Sierra Wireless™ 4G LTE Tri-Fi Hotspot

User Guide

Table of Contents

Get Started

This section gives you all the information you need to set up your device and Sprint service the first time.

Your Device

System Requirements

Setting Up Your Device

Getting Help

Your Device

The following illustrations show your device's primary external features and buttons:

Front View
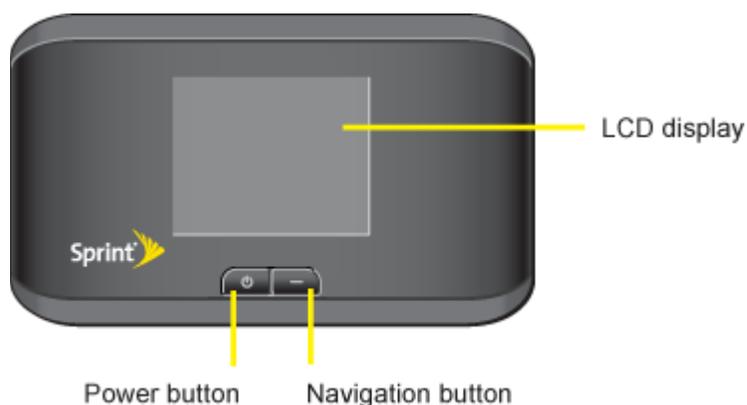
Bottom View (Battery Cover Removed)

Top View

Mute switch   WPS button
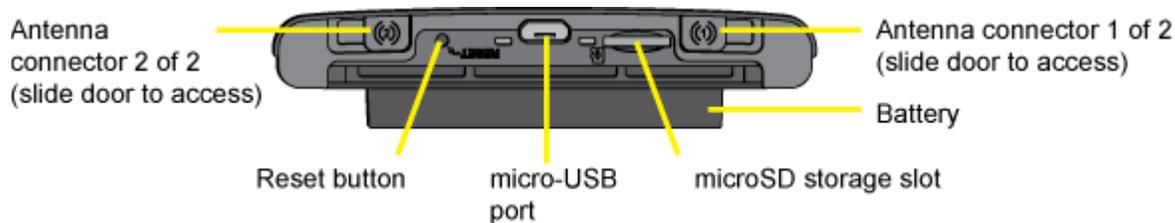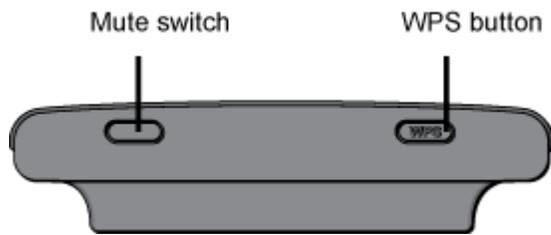
Package Contents

Your package includes several items.

- Sierra Wireless 4G LTE Tri-Fi Hotspot

- Battery compartment cover

- Rechargeable battery

- AC charger with micro-USB port

- Micro-USB cable

- Get Started guide

Care and Maintenance

As with any electronic device, you should handle this device with care to ensure reliable operation. Follow these guidelines in using and storing the device.

- Protect the device from liquids, dust, and excessive heat.

- Do not handle or operate the device while driving or operating a vehicle. Doing so may distract you from properly operating the vehicle. In some jurisdictions, operating communication devices while in control of a vehicle is a criminal offense.

- Do not apply adhesive labels to the device. They may cause the device to overheat and may alter the antenna's performance.

System Requirements

This section lists items that are required to use your Sierra Wireless™ 4G LTE Tri-Fi Hotspot.

- One or more computers that support Wi-Fi (802.11b/g/n)

- Web browser (required if you'll be using the browser interface to view status and to configure settings). The following browsers are supported:

  - Internet Explorer (version 6.0 or higher)

  - Mozilla Firefox (version 2.0 or higher)

  - Google Chrome (version 2.0.172.28 or higher)

  - Apple Safari (version 2.0 or higher)

  - Opera version 9.64

- If you'll be connecting the device through USB:

  - Computer running Windows 7, Windows Vista, Windows XP, or Mac (OS X 10.4.x or higher)

  - USB 2.0 slot

Setting Up Your Device

Read step-by-step instructions for setting up the device.

Device Setup

Activating Your Device

Device Setup

This section describes how to set up your device.

1. Install the battery, as described in Installing the Battery.

2. Connect the device to the AC charger, as described in "Using the AC Charger with Your Device's micro-USB Port" in Charging the Battery.

3. Plug the AC charger into an electrical outlet.

4. **Important:** Charge the device until the battery icon is full ( ).

Connecting to the Network

1. Make sure you are in a Sprint 4G, 4G LTE, or 3G coverage area (not roaming).

2. If you have a LAN connection, disconnect it.

3. Make sure your computer's Wi-Fi is turned on.

4. If the device LCD displays "Charging," "Charged," or "Powered off," press and hold the power button for two seconds.
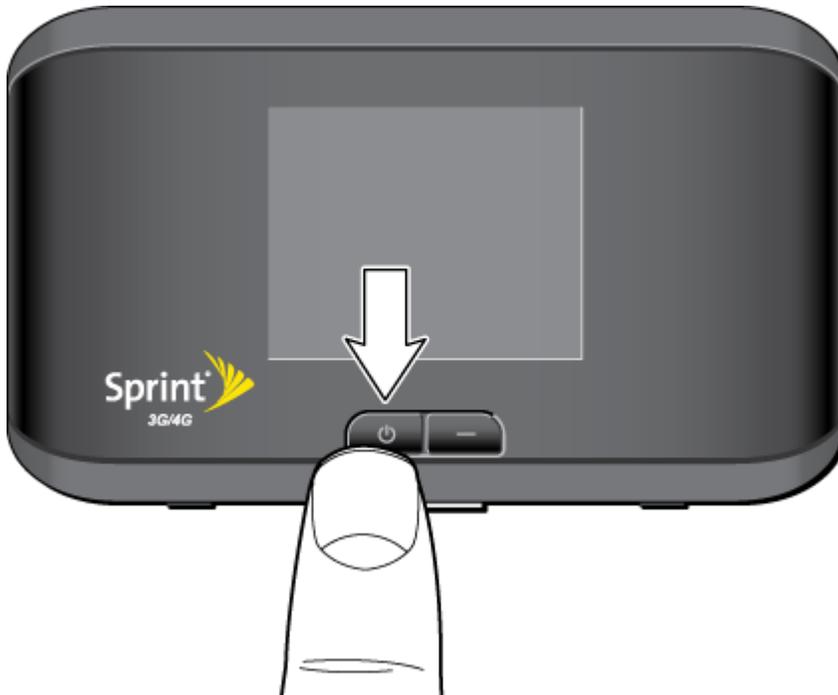
5. Wait until the device LCD displays "Connect your computer to Wi-Fi network," followed by the network name (SSID) and password. This may take several seconds.

6. On your computer, connect to the Wi-Fi network listed on the device LCD. If you don't know how to do this, see How Do I Connect to Wi-Fi? After you've connected to the Wi-Fi network, the device LCD displays "Open any web page to continue setup."

7. Open your Web browser. The "Welcome to your Sierra Wireless™ 4G LTE Tri-Fri Hotspot" window opens.

Note: This window displays the administrator password and the address of the device home page. Please remember this information or write it down in a safe place.

This window provides several options.

- To keep the default settings of the device, click one of the following:

  - **The Internet** (to connect immediately to the Internet)

  - **My Sierra Wireless™ 4G LTE Tri-Fri Hotspot's home page** (to view the device status, customize settings). Proceed to Activating Your Device.

  - To change security settings, click **Set up my Sierra Wireless™ 4G LTE Tri-Fri Hotspot**.

Changing the Password and Settings

During the device setup, you can select **Set up my Sierra Wireless™ 4G LTE Tri-Fri Hotspot** to change the following settings:

- **Administrator password** — This password is used to log in to the home page, where you can view and customize your device settings. The default password is "password." Choose something easy-to-remember (yet not easily guessed by others). If you forget this password, you'll need to reset the device to its default settings and go through the device setup (as described in Device Setup).

  Your administrator password must be 1–20 characters long.

- **Wi-Fi network name (SSID)** — This name is visible to other Wi-Fi-enabled devices, and is used to identify your Wi-Fi network. The length of the Wi-Fi network name (SSID) depends on other settings of the browser interface. (See the Help bubble that's displayed when you move the cursor to the SSID input field.)

- **Wi-Fi security** — The default setting is WEP 64 Bit Open. To select another option, click **More options**. (See "Wi-Fi Security Options", below.)

- **Wi-Fi password** — The maximum length of this field is determined by the **Wi-Fi security** option (the previous item). (See the Help bubble that's displayed when you move the cursor to the **Wi-Fi password** field.)

  If you'll be sharing your Internet connection, you may need to give the Wi-Fi password to other users; don't use your banking or other important passwords. Also, don't use a password that's easily guessed by others.

From this window you can also enable the Password Reminder feature, which is useful if you forget the Wi-Fi password (**Show Wi-Fi password on your device**). (See "Wi-Fi Password Reminder" in Wi-Fi Password.)

Tip: Help information on each field appears (in a bubble) when you move the cursor into the field.

Tip: You can display this window any time, by clicking **Admin Setup** ( ) in the home page. (See Displaying the Home Page of the Device.)

After you change the settings and click **Submit**, the device restarts and displays updated information on its LCD. Follow the instructions on the LCD, and proceed to "Your Device is Now Restarting" (below).

Wi-Fi Security Options

If you click **More options** (after having clicked **Set up my Sierra Wireless™ 4G LTE Tri-Fri Hotspot**, during the device setup), a window with several Wi-Fi security options opens.

Note: All the devices used with the Sierra Wireless 4G LTE Tri-Fi Hotspot must support the selected security type.

Note: WPS is available only if you select either a WPA2 Personal option (including **WPA/WPA2 Personal**) or (not recommended) no security. (See Connecting Through WPS.)

The options displayed depend on the **Basic Rate** setting (in **Advanced Settings > Wi-Fi > Security**; see Wi-Fi Tab: Security Panel).

If **Basic Rate** is "802.11b/g compatibility" or "802.11g only," these options are shown:

- **WPA-Personal** — This is a strong security standard, supported by most Wi-Fi devices.

- **WPA2-Personal AES** — This is a stronger, newer security standard that is limited to newer Wi-Fi devices.

- **WEP-64 Bit** — This option provides security, but it's relatively weak. This option works with older and newer Wi-Fi devices, and is recommended only if any of your devices don't support WPA or WPA2.

- **None** — No security is used (no password is required to access the Wi-Fi network); this setting is not recommended. Anyone may access your device and use your Internet connection. (You are responsible for payment for data usage fees.)

If **Basic Rate** is "802.11b/g/n compatibility," these options are shown:

- **WPA2 Personal - AES** — This is a stronger, newer security standard that is limited to newer Wi-Fi devices.

- **WPA/WPA2 Personal** (recommended setting if any of your devices are more than two years old) — Wi-Fi devices that use either WPA or WPA2 can connect to the Sierra Wireless 4G LTE Tri-Fi Hotspot. Most Wi-Fi devices support this type of security.

- **None** — No security is used (no password is required to access the Wi-Fi network); this setting is not recommended. Anyone may access your device and use your Internet connection. (You are responsible for payment for data usage fees.)

If the above options don't meet your requirements, click **I don't see what I want....** (This link might not be displayed, depending on the **Basic Rate** setting.)

Expanded Wi-Fi Security Options

If you click **I don't see what I want...** (from the Wi-Fi Security Options window during the device setup), a window with an expanded list of Wi-Fi security options opens.

Note: All the devices used with the Sierra Wireless 4G LTE Tri-Fi Hotspot must support the selected security type.

Note: WPS is available only if you select either a WPA2 Personal option (including **WPA/WPA2 Personal**) or (not recommended) no security. (See Connecting Through WPS.)

Note: You can also view the expanded list of Wi-Fi security options in the **Security** panel of the **Wi-Fi** tab of the **Advanced Settings** window. (See "Accessing the Advanced Settings Window" in Advanced Settings.)

Some of the following options may be displayed, depending on the **Basic Rate** setting (see Wi-Fi Tab: Security Panel):

- **None** — No security is used (no password is required to access the Wi-Fi network); this setting is not recommended. Anyone may access your device and use your Internet connection. (You are responsible for payment for data usage fees.)

- **WEP 64 Bit - Shared** — This option provides security, but it's relatively weak. This option works with older and newer Wi-Fi devices, and is recommended only if any of your devices don't support WPA or WPA2.

  Shared WEP uses the same key for encryption and authentication; some consider shared WEP to be less secure than open WEP.

- WEP 128 Bit - Shared — This option provides security, but it's relatively weak (but stronger than **WEP 64 Bit - Shared**). This option works with older and newer Wi-Fi devices, and is recommended only if any of your devices don't support WPA or WPA2.

  Shared WEP uses the same key for encryption and authentication; some consider shared WEP to be less secure than open WEP.

- WEP 64 Bit - Open — This option provides security, but it's relatively weak. This option works with older and newer Wi-Fi devices, and is recommended only if any of your devices don't support WPA or WPA2.

  Open WEP uses the key for encryption, but not for authentication.

- WEP 128 Bit - Open — This option provides security, but it's relatively weak (but stronger than WEP 64 Bit - Open). This option works with older and newer Wi-Fi devices, and is recommended only if any of your devices don't support WPA or WPA2.

  Open WEP uses the key for encryption, but not for authentication.

- WPA Personal - TKIP — This is a strong security standard that is supported by most Wi-Fi devices.

- WPA Personal - TKIP/AES — This is a strong security standard that is supported by most Wi-Fi devices.

- WPA2 Personal - AES — This is a stronger, newer security standard that is limited to newer Wi-Fi devices.

- WPA2 Personal - TKIP/AES — This is a stronger, newer security standard that is limited to newer Wi-Fi devices.

- WPA/WPA2 Personal (recommended setting if any of your devices are more than two years old) — Wi-Fi devices that use either WPA or WPA2 can connect to the Sierra Wireless 4G LTE Tri-Fi Hotspot. This setting is supported by most Wi-Fi devices.

Your Device is Now Restarting

The "Your device is now restarting" window opens if you've clicked **Set up my Sierra Wireless™ 4G LTE Tri-Fri Hotspot** and then clicked **Submit**.

The changes take effect after the device restarts automatically.

You should write down the following information that's displayed in the window:

- Wi-Fi network name

- Wi-Fi password

To complete the process:

1. Wait until the device LCD displays "Connect your computer to Wi-Fi Network."

2. Connect your computer to the Wi-Fi network, using the information you've written down. (If you don't know how to do this, see How Do I Connect to Wi-Fi?)

3. After the Wi-Fi connection was successfully established, click the **Click here** text in the window.

Activating Your Device

Normally your device will be set up on your account at the time of purchase. If this has not happened, the browser interface will prompt you to activate your device.

The process of setting up an account is called **activation**. When the device starts up, it will detect whether the device has been configured with an account ("preactivated"). If it has not, the activation process starts automatically.

Note: If you're able to connect to 3G, you are already set up to use Sprint service on the 3G network; no further action is needed. Proceed to Connecting Through USB.

In some cases, the activation process will be seamless, not requiring any action from your part; you might not even see any activation-related messages displayed on the device LCD.

In other cases, your computer will display one of the following:

- "3G Activation Required" alert (displayed on the home page; available if you have already set up with Sprint a wireless account that is associated with your Sierra Wireless 4G LTE Tri-Fi Hotspot)

- Device Self-Activation wizard (displayed if you haven't yet set up a wireless account that is associated with your Sierra Wireless 4G LTE Tri-Fi Hotspot)

Activating Your Device Through the "3G Activation Required" Alert

In rare cases, the device LCD and the home page may indicate that activation is required:

- The LCD displays "3G Activation failed."

- The home page displays the alert "3G Activation Required."

Note: You will still be able to connect to the Internet when you have 4G coverage. (You won't be able to connect to the Internet if you have only 4G LTE coverage.) Once you initiate the activation process, you won't be able to connect to the Internet through 4G or 4G LTE, until the activation process has completed.

To activate your device:

1. Make sure you're in 3G coverage and the signal strength is strong.

2. In the address bar of your Web browser, type **http://192.168.0.1** to display the home page.

3. In the **Admin Login** section (in the upper left area of the home page), enter the administrator password (1–20 characters/numbers). (The default password is "password".)

4. Click **OK**.

5. Click the alerts icon ▯ to display the alert window.

6. If more than one alert is available, use the ◁ and ▷ buttons (at the top of the alert window) to browse to the "3G Activation Required" alert.

7. In the alert, click **Activate now**.

If you haven't successfully completed the activation, contact Sprint Customer Service and have the following available:

- Your billing information.

- MEID of the device (displayed on the packaging and inside the battery compartment).

Activating Your Device Through the Activation Wizard

If you haven't set up with Sprint a wireless account that is associated with your Sierra Wireless 4G LTE Tri-Fi Hotspot, the Device Self-Activation wizard is automatically displayed.

To activate your device through the Device Self-Activation wizard:

1. Make sure you're in 3G coverage and the signal strength is strong.

2. Follow the onscreen instructions displayed in the Device Self-Activation wizard.

   If the activation fails, the following options may be presented:

   ▪ Retry the activation.

   ▪ Reset the device to its default settings (after which the device will restart) and then retry the activation.

   ▪ Cancel. You should retry the activation at a later time.

If, after trying the above options, you haven't successfully completed the activation, contact Sprint Customer Service and have the following available:

● Your billing information.

● MEID of the device (displayed on the packaging and inside the battery compartment).

To manually start the Device Self-Activation wizard (for example, at a later time):

1. Make sure you're in 3G coverage and the signal strength is strong.

2. In the address bar of your Web browser, type **http://192.168.0.1** to display the home page.

3. In the **Admin Login** section (in the upper left area of the home page), enter the administrator password (1–20 characters/numbers). (The default password is "password".)

4. Click **OK**.

5. Click **Advanced settings** ( ).

6. Click **Device > About**.

7. Click **Launch Activation Wizard**.

Getting Help

Learn where you can get more information or assistance.

Visiting the Sprint Website

Sign on to sprint.com to get up-to-date information on Sprint services, options, and more.

You can also:

- Review coverage maps.

- Access your account information.

- Add additional options to your service plan.

- Purchase accessories.

- Check out frequently asked questions.

- And more.

Contacting Sprint Customer Service

You can reach Sprint Customer Service by:

- Logging on to your account at www.sprint.com.

- Calling us toll-free at **1-888-788-4727** (business use) or **1-888-211-4727** (personal use).

Online Help

In the browser interface, click **Help** and, from the menu, select **Online Help**.

The Help system opens in a new Web browser window or tab.

You have several options to find the information you need:

- Browse the Table of Contents.

- Use the Index or Search feature: click the appropriate button in the lower left part of the help window, and type the information you're looking for.

Other Ways to View Help Information

- Some windows have a icon. Click the icon to view Help information.

- When you move the cursor over an item in **Advanced Settings**, help information, if available, appears to the right of the window.

Contextual Help in the Advanced Settings Window

When you move the cursor over an item in **Advanced Settings**, help information on this item, if available, appears to the right of the window.

To turn this feature on or off:

1. Make sure you're logged in to the home page.

2. Click **Advanced settings > Device > Basic**.

3. Set **Help for Advanced Settings** to **Show** or **Hide**.

4. Click **Save**.

Device Basics

Learn about the buttons, connectors, and other components of your Sierra Wireless 4G LTE Tri-Fi Hotspot.

Components of Your Device

3G and 4G Networks

Battery

Power Button

Other Buttons and Switches

Reset Button

LCD

microSD Card Slot

Your device provides a simple way to use your 3G or 4G Internet connection with any Wi-Fi-enabled device, and to share your Internet connection with friends and family.
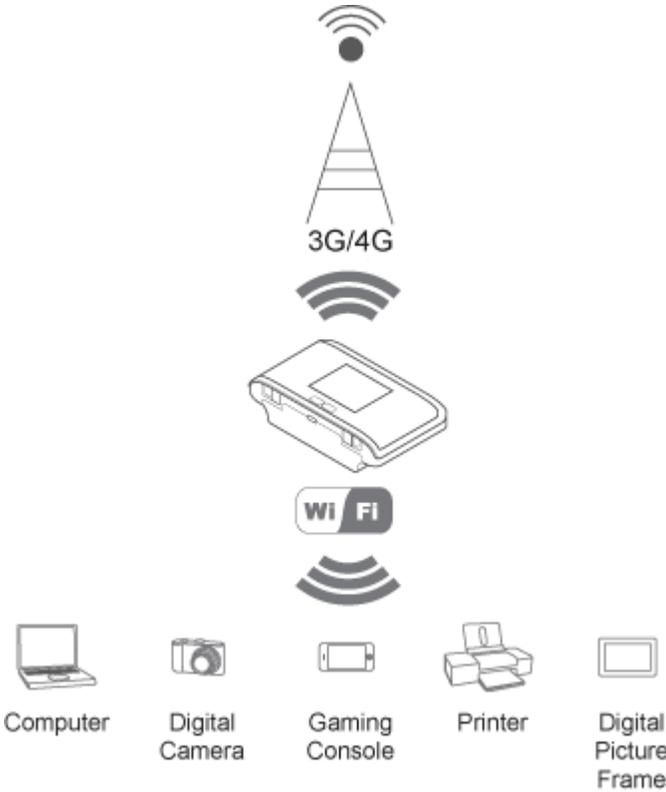
Components of Your Device

Your device consists of several main components.

- Wi-Fi access point
  The Wi-Fi access point connects your computers and other Wi-Fi-enabled devices to your device.

- 3G modem
  The 3G modem connects your device to the Internet via the 3G (CDMA 1X/EVDO) network (more widely available, compared with 4G).

- 4G modem
  The 4G modem connects your device to the Internet via the 4G WiMAX network (newer technology and faster speeds, compared with 3G).

- 4G LTE modem
  The 4G LTE modem connects your device to the Internet via the 4G LTE network (newer technology and faster speeds, compared with 3G).

- Routing hardware
  The routing hardware handles traffic between the 3G or 4G LTE/4G modems, the Wi-Fi access point, and the Wi-Fi network.

3G and 4G Networks

These wireless networks connect you to the Internet.

Depending on your coverage area, you may have:

- Both 3G and 4G coverage

- Only 3G coverage

- Only 4G coverage.

Your device automatically connects to the fastest network that is available to you. If you have both 3G and 4G coverage and your connection happens to get disrupted, your device can automatically switch to the other network. (For more information, see "Configuring the 3G/4G Connection Preferences" in Mobile Broadband Information and Settings.)

Download speeds

Actual speeds depend on several factors, including network conditions.

Wireless mode	Maximum downlink speeds	Typical downlink speeds
3G (EV-DO Rev. 0)	2.4 Mbps	400–700 kbps
3G (EV-DO Rev. A)	3 Mbps	0.6–1.4 Mbps

4G (LTE)	20 Mbps	TBD Mbps
4G (WiMAX)	10 Mbps	3–6 Mbps

Battery

The battery compartment is on the back of the device. The battery is replaceable. If you need a new battery, visit the Sierra Wireless online store at sierrawireless.com/eStore. Chargers and other accessories are also available from the Sprint Store at sprint.com.

Installing the Battery

Before you use your device, install the battery.

1. Using slight finger pressure, slide the battery compartment cover towards you to remove it.
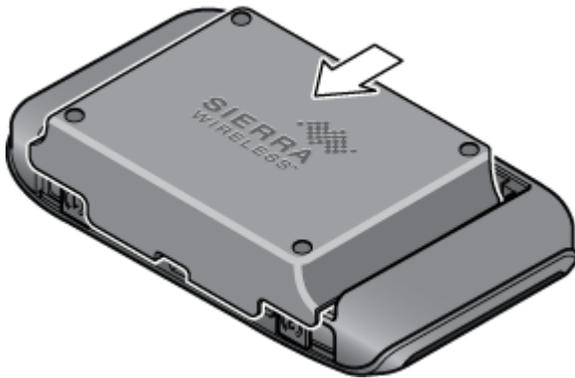
2. Insert the battery into the device, contacts end first. Make sure the battery contact points are aligned with those inside the battery compartment.

3. Replace the battery compartment cover.
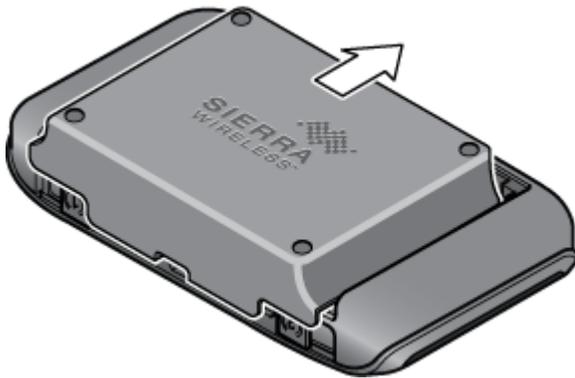
Charging the Battery

You need to recharge your device's battery periodically. You can continue using your device while it is charging.

The faster method is to connect the device to the AC charger. (See "Using the AC Charger with Your Device's micro-USB Port", below.) Alternatively, you can connect the device to your computer, although this charges more slowly. (See "Charging Through Your Computer", below.)

Using the AC Charger with Your Device's micro-USB Port
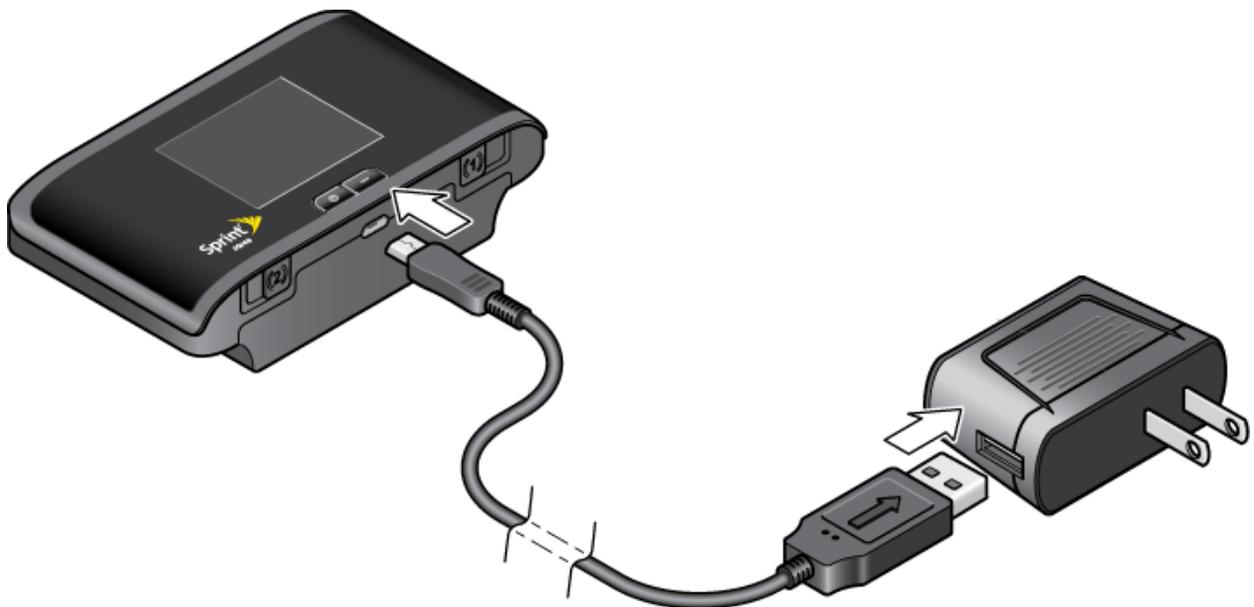
1. Insert the larger end of the micro-USB cable into the AC charger.

2. Insert the other end of the cable into the micro-USB port on the side of your device.

3. Insert the AC charger into an electrical outlet.

When charging, the LCD shows [battery charging icon] and, if the device is off, displays a message "Charging... xx% complete" (where "xx" is a number value).

When the device is charged, the LCD shows:

- [battery full icon] (if the device is on)

- [battery charging icon] and the message "Fully charged" (if the device is off).

Charging Through Your Computer
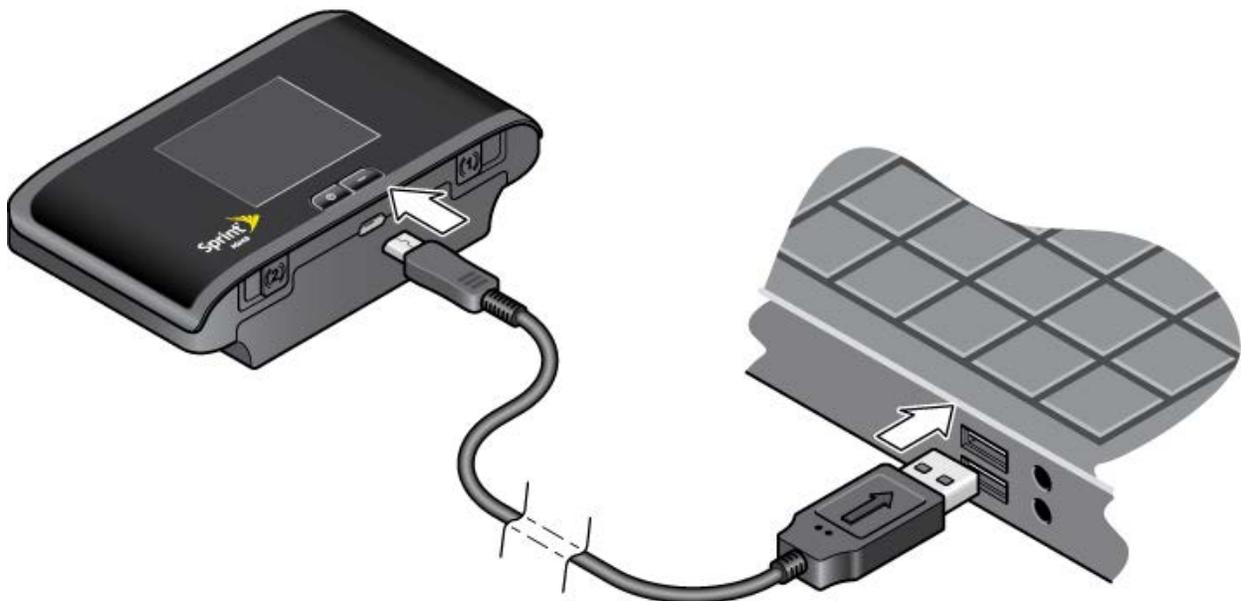
Note: If you'll be using USB for data transfer (and not just for charging the device), you must install the device driver. (See Making a Tethered Connection.)

Note: If you're using Mac OS X 10.4.x, after you connect the device you may see a warning message that your computer is running on UPS backup battery and that you should perform a computer shutdown. You can continue with your work. To prevent this message from being displayed, install the device driver. (See Making a Tethered Connection.)

1. Make sure your computer is turned on.

2. Insert the larger end of the micro-USB cable into your computer.

3. Insert the other end of the cable into the micro-USB port on the side of your device.

When charging, the LCD shows [USB] .

When the device is charged, the LCD shows ▮▮▮▮.

Power Button

Use the power button to turn your device on and off. The power button also is a status indicator.

Turning Your Device On and Off

Using the Power Button to Determine the Device State

Controlling the Device Using the Power Button

Turning Your Device On and Off

Use the power button on your device to turn it on and off.

Turning Your Device On

1. Make sure that:

   ▪ The device has a charged battery inserted.

     — or —

   ▪ The device is connected to the AC charger or a computer (through the micro-USB cable).

2. If the LCD is blank, press and hold the power button ⏻ until the device turns on.
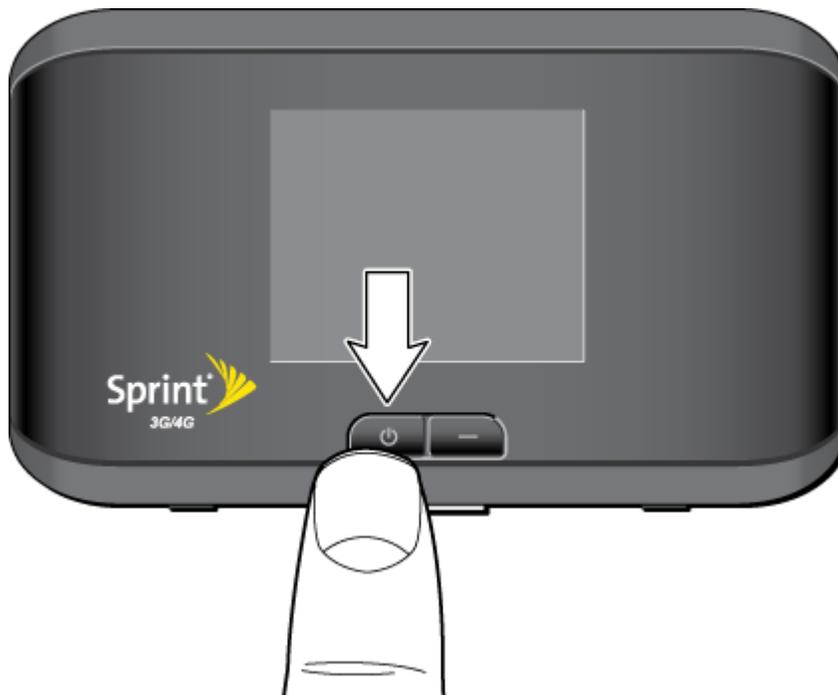
Turning Your Device Off

► Press and hold the power button ⏻ until the device turns off.

Using the Power Button to Determine the Device State

The power button on the device also indicates the device's status. See the following table:

Power button ⏻	Description	Your action
Not lit	The device is turned off.	To turn the device on, press and hold the power button ⏻ until the device turns on.
	The device is turned on, but the LED is turned off.	Optionally, turn on the LED. (See Enabling and Disabling the Power Button LED.)
Lit, flashing (approximately every 4 seconds)	The device is turned on, and the LED is turned on.	No action required.
Lit, flashing (approximately every 8 seconds)	The device is in standby (low power) mode. The following are off: LCD, Wi-Fi radio, 3G/4G radios. (For more information, see "Standby (Low Power) Mode" in Battery Information and Settings.)	To exit standby mode: Connect the device to the AC charger or computer through the micro-USB cable. — or — Press the power button ⏻.

Controlling the Device Using the Power Button

The power button supports two types of presses.

Type of press	Result
Quick press	Removes device from standby (low power) mode. Wakes up (turns on) the LCD if the LCD was enabled but dormant. (The LCD turns dark, after a configurable time of inactivity.) Confirms or acknowledges a displayed message. Turns off display of the Wi-Fi network name and password.
Long press (press and hold for two seconds)	Turns the device on or off.

Device Basics   28

Other Buttons and Switches

This section describes the navigation button, WPS button, and the mute switch.

Navigation Button

The navigation button ▭ is next to the power button ⏻. Briefly press the navigation button to go to the next information screen, if available. (See LCD Information Screens.)

WPS Button

Wi-Fi Protected Setup™ (WPS) provides a fast, simple, and secure way to connect WPS-enabled devices to your Wi-Fi network. You don't have to give the name (SSID) and Wi-Fi password of your network to other users.

The WPS button WPS is on the top of the device, as shown in the figure in Top View. Press this button if you want to connect a device that supports WPS to your network. (See Connecting Through WPS.)

Mute Switch

The mute switch is used to turn device sounds on or off. The mute switch is located on the top of your device, to the left of the WPS button, as shown in the following drawing:
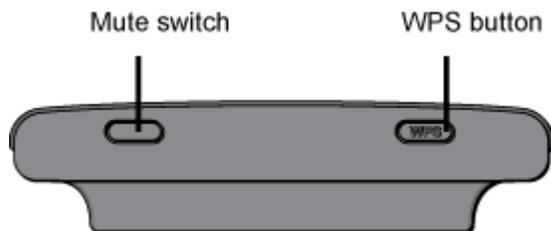
Tip: You can also disable sounds through the home page. (See Sounds Information and Settings.)

Reset Button

If the device or the home page seems to stop responding, you can reset (restart) the device.

The reset button is inside the hole located near the battery compartment as shown below (after the battery compartment cover has been removed).
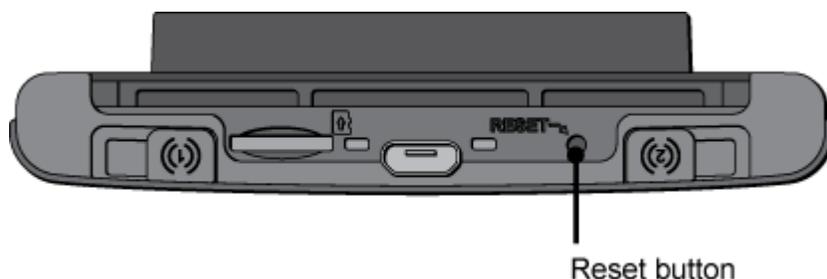
For information on using this button, see Restarting the Device and Resetting the Software to Default Settings: Using the Reset Button.

Restarting the Device

If the device or the home page seems to stop responding, you can reset (restart) the device by pressing the reset button.

Tip: Alternatively, you may be able to restart the device by pressing and holding the power button on the device for three to four seconds.

To restart the device:

1. Using slight finger pressure, slide the battery compartment cover towards you to remove it.
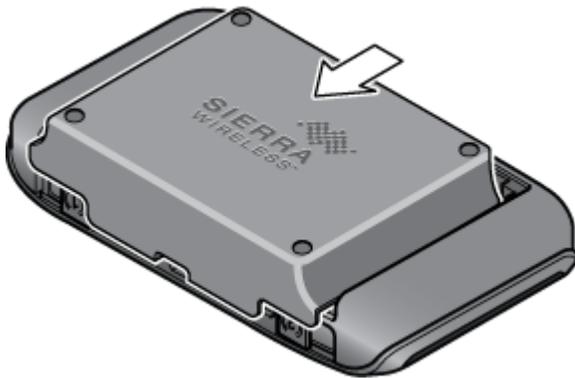
2. Locate the small hole labeled "RESET" (near the micro-USB port). The reset button is inside this hole.

Reset button

3. Insert a thin object (for example, the end of a paper clip) into the hole, and press down for about a second.

4. Replace the battery compartment cover.
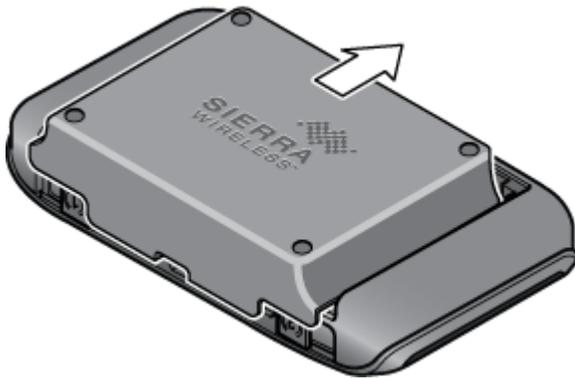
LCD

The LCD has several icons that help you determine the status of your device and its connections.

If the LCD is not lit, see "Turning Your Device On" in Turning Your Device On and Off.

Interpreting the LCD

LCD Information Screens

Interpreting the LCD

The LCD shows icons and text that reflect the status of the device and your connection.
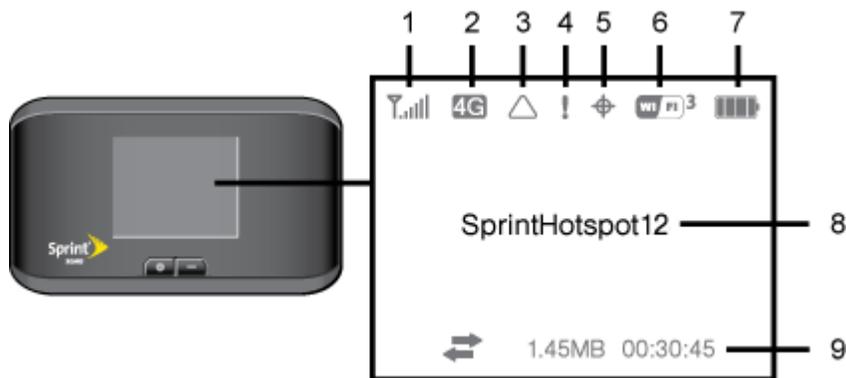
Item	Description
1	Signal strength
2	3G or 4G status
3	Roaming indicator
4	Alerts
5	GPS
6	Number of Wi-Fi users

7	Battery status
8	Device name. Message area.
9	Amount of data transferred; connection duration. Message area.

Tip: Most of the LCD icons and messages are also shown on the Virtual Device and Mini Window. (See "Virtual Device" and "Mini Window" in Device Views, and Messages Displayed on the Device LCD.)

The LCD can also display various information screens and messages, as described in LCD Information Screens and in Messages Displayed on the Device LCD.

LCD Information Screens

The LCD of the Sierra Wireless 4G LTE Tri-Fi Hotspot can display, on separate screens, summary information.

- Connection information (the Wi-Fi network name [SSID] and password [if the Wi-Fi Password Reminder feature is enabled])

- Alerts

- Data usage (displayed on the "Billing Info" LCD information screen)

- Network status

- Device information (for example, MEID or whether an update is available) (displayed on the "About..." LCD information screen)

- Software update status

When more than one information screen is available, the upper right corner of the LCD displays "(x/y)," where x and y represent "screen x out of y screens." For example, (1/6) means that the first of six LCD information screens is shown.

To view the first LCD information screen or to go to the next screen, press the navigation button ▬ on the device.

microSD Card Slot

Your device supports a microSD™ card (not included) for file sharing and transfer or storage. The microSD slot is located on the same side of the device as the micro-USB port (to access the slot, you must remove the battery cover). Your computer recognizes the microSD card as a removable storage device. The device supports microSD cards up to 32 GB.

Note: Using microSD cards larger than 32 GB can cause data loss and damage your device.

Your Network Connection

Find out how to launch, share, and end your network connection.

Launching and Ending A Network Connection

Sharing Your Connection

Connecting Through USB

Launching and Ending A Network Connection

Learn how to manually launch a connection, and how to end it.

Launching Your Network Connection

Ending Your Network Connection

Launching Your Network Connection

After the device powers on and boots up, a connection to the 3G or 4G network is launched automatically, unless you've disabled **Connect Automatically**.

You will need to manually launch a connection if:

- The connection was not successful.

- You've disabled auto-connect.

- You've enabled auto-connect and also **Disable when roaming**, and have lost the connection while roaming.

- You've manually ended a connection (by clicking **Disconnect**).

To launch a connection:

► Click **Connect** on the Virtual Device on the home page. (You must be logged in.)

— or —

Click **Connect** in the Mini Window. (You must be logged in.)

— or —

If the device LCD displays "Disconnected from 3G/4G network. Connect now?", press the power button ![power button] on the device.

See also:

- Internet Connection Information.

- Mobile Broadband Information and Settings

- Roaming Information and Settings

- Signal Information

- "Scan for Private Network" in WAN Tab: 4G Panel

Ending Your Network Connection

Learn how to end your network connection.

1. Make sure you're logged in to the home page.

2. Click **Disconnect** on the Virtual Device or in the Mini Window. (See "Virtual Device" and "Mini Window" in Device Views.)

Note: The Wi-Fi connection is still available, so users can, for example, share files by using a microSD card.

Sharing Your Connection

Your Sierra Wireless 4G LTE Tri-Fi Hotspot provides two ways of sharing your network connection with other users.

- User manually enters the Wi-Fi information

- User connects by using WPS

Manually Entering the Wi-Fi information

Connecting Through WPS

Manually Entering the Wi-Fi information

One option for connecting to the network is for users to manually enter the Wi-Fi information.

For other users to share your network connection:

1. Provide the Wi-Fi network name and password to them.

2. On their computer, users must open the Wi-Fi network manager and connect to the Wi-Fi network of the Sierra Wireless 4G LTE Tri-Fi Hotspot. (See How Do I Connect to Wi-Fi?)

Connecting Through WPS

Wi-Fi Protected Setup (WPS) provides a fast, simple, and secure way to connect WPS-enabled devices to your Wi-Fi network. You don't have to give the name (SSID) and Wi-Fi password of your network to other users.

The WPS feature is available on certain cameras, printers, smartphones, and laptops. These devices have either a hardware button or a WPS-related option in the software. Please consult the user documentation of your device.

To turn this feature on or off:

1. Make sure you're logged in to the home page.

2. Click **WPS** (below the Virtual Device).

3. In the WPS Setup window, select **Enable** or **Disable**.

4. Click **Save**.

WPS is not available in any of these situations:

● Wi-Fi is not enabled. (See Wi-Fi Tab: Network Panel.)

● The Wi-Fi security option is WPA Personal, WEP, or WEP-related (for example, "WEP 64 Bit Open"). (**Note:** WPS is available if the Wi-Fi security option is WPA/WPA2 Personal.)

● SSID Broadcast is not enabled. (See Wi-Fi Tab: Network Panel.)

● WPS is turned off (from the WPS Setup window).

● MAC filter mode is "Allow all in list", but no computers have been added to the list. (See "Specifying Computers That Can Access the Network" in Allowing or Denying Computers Access to the Network.)

If the maximum number of connected devices has already been met, an error message "Max connected devices" or "Max Wi-Fi users" is displayed when you attempt WPS. Disconnect one of the connected devices and then retry.

Using the LCD of your Sierra Wireless 4G LTE Tri-Fi Hotspot

1. Press the WPS button ⬚WPS⬚ on your Sierra Wireless 4G LTE Tri-Fi Hotspot.

2. When the LCD of your Sierra Wireless 4G LTE Tri-Fi Hotspot displays "WPS Started", press (within 2 minutes) the WPS button on the wireless device you want to connect or select the WPS-related option in the device's software.

Your Sierra Wireless 4G LTE Tri-Fi Hotspot and the wireless device will communicate and establish the connection. If no problems are encountered, the LCD of your Sierra Wireless 4G LTE Tri-Fi Hotspot displays "WPS in Progress. Adding Device..." and then "WPS Session Complete." If problems are encountered, see WPS-Related Messages.

Using the home page of your Sierra Wireless 4G LTE Tri-Fi Hotspot

1. Make sure you're logged in to the home page.

2. Click **WPS** (below the Virtual Device).

3. In the WPS Setup window, make sure **Enable** is selected.

4. Perform one of the following, depending on whether the Wi-Fi device you are adding to your Wi-Fi network supports the PBC (Push Button Configuration) method or the PIN (Personal Information Number) method.

   If the Wi-Fi device supports the PBC (Push Button Configuration) method:

   ▪ In the WPS Setup window, select **Use PBC method**.

- Click **Connect**.

- Within 2 minutes, press the WPS button on the wireless device you want to connect or select the WPS-related option in the device's software.

— or —

If the Wi-Fi device has a PIN associated with it:

- Find out the PIN for the Wi-Fi device you're adding. To do this, use the PIN option in the device's software. Alternatively, use the Wi-Fi Protected Setup Wizard that may be available, depending on the manufacturer of the device.

- In the WPS Setup window, select **Use PIN method**.

- Enter the PIN for the Wi-Fi device.

- Click **Connect**.

- Within 2 minutes, start connecting from the WPS-related PIN option in the device's software or from the Wi-Fi Protected Setup Wizard.

Your Sierra Wireless 4G LTE Tri-Fi Hotspot and the wireless device will communicate and establish the connection. The status is displayed in the WPS Setup window (below the **Connect** button) and also on the LCD of the Sierra Wireless 4G LTE Tri-Fi Hotspot.

Connecting Through USB

Use the micro-USB cable (included) to connect the device to your computer.
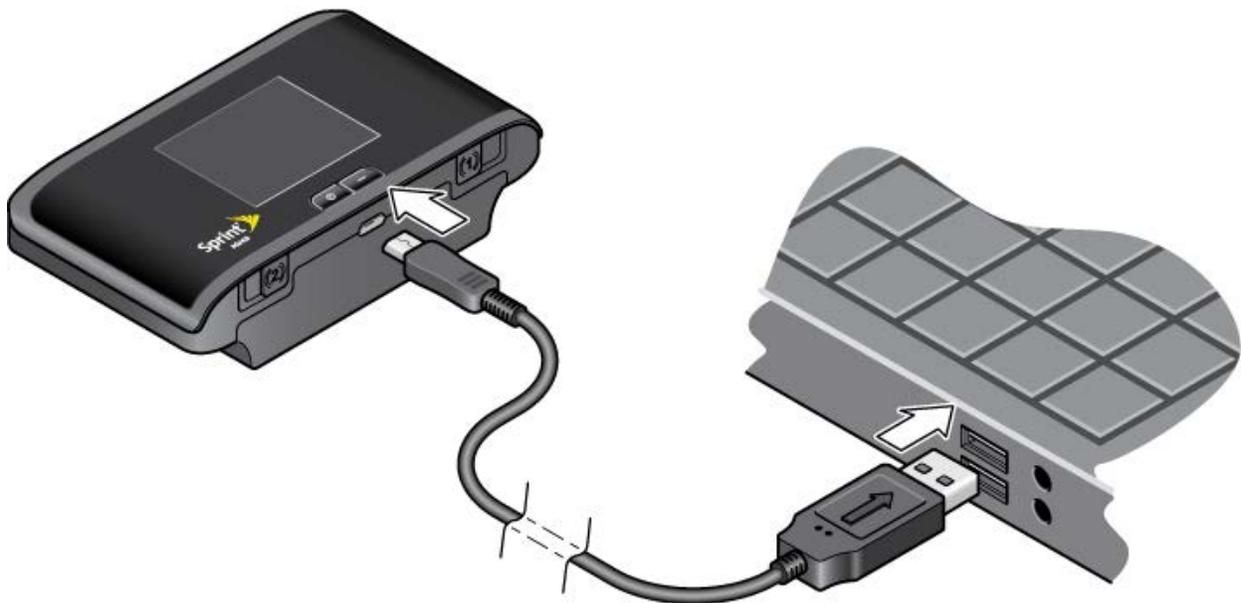
Note: If you'll be using USB for data transfer (and not just for charging the device), you must install the device driver. (See Making a Tethered Connection.)

Use the micro-USB cable when:

- You want to charge the device, but you don't want to use the AC charger, or the AC charger is not available.

- Your computer does not have Wi-Fi.

- You want to block others from using the device. (See Disabling Wi-Fi When Connected Through USB.)

To connect the device to your computer:

1. Insert the larger end of the micro-USB cable into your computer.

2. Insert the other end of the cable into the micro-USB port on the side of your device.

Note: If you're having problems, see Cannot Connect Through USB.

Making a Tethered Connection

Your device supports a direct connection through a USB cable to a Windows or Mac computer. (This is commonly referred to as a "tethered" connection.)
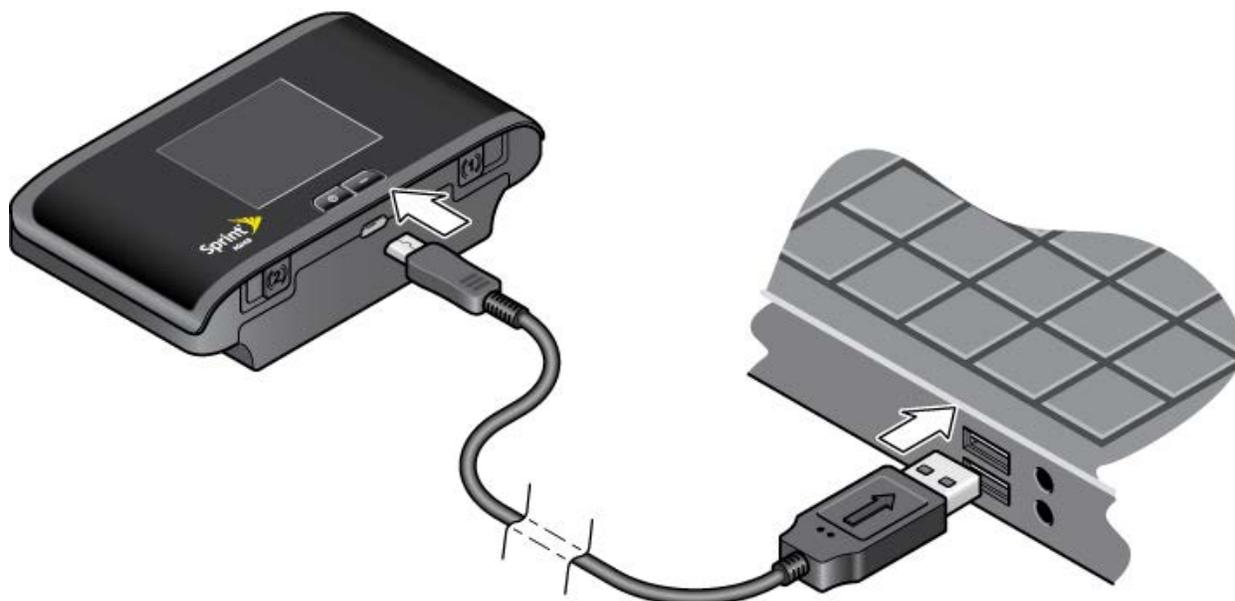
Note: If you'll be using USB for data transfer (and not just for charging the device), you must install the device driver (see "Windows" or "Mac", below). No installation CD is required — the device supports the TRU-Install feature.

Note: If you're using Mac OS X 10.4.x, after you connect the device you may see a warning message that your computer is running on UPS backup battery and that you should perform a computer shutdown. You can continue with your work. To prevent this message from being displayed, install the device driver (see "Mac", below).

Windows

To install the device driver on Windows:

1. Make sure the device is turned on.

2. Connect the device to your computer through the micro-USB cable.

3. If the TRU-Install window is not displayed, in Windows Explorer browse to the TRU-Install entry (under My Computer), then browse to the Win folder and run **Setup.exe**.

   — or —

   If you're running Windows Vista and the AutoPlay window opens, click **Run setup.exe**.

4. In the TRU-Install window, click **OK**.

5. Install the Sierra Wireless USB driver. (Follow the onscreen instructions.)

Mac

To install the device driver on Mac:

1. Make sure the device is turned on.

2. Connect the device to your computer through the micro-USB cable.

3. In the window that appears, double-click the **.pkg** file.

4. Install the Sierra Wireless USB driver. (Follow the onscreen instructions.)

5. When prompted for your password, enter your Mac password.

TRU-Install

TRU-Install is a feature that installs the necessary drivers the first time you connect your device to your Windows or Mac computer through the micro-USB cable. (For details, see Making a Tethered Connection.) An installation CD is not required.

TRU-Install is enabled by default.

To change the setting:

1. In the address bar of your Web browser, type **http://192.168.0.1** to display the home page.

2. Make sure you're logged in to the home page (the text "Admin Logged in" is displayed near the upper left corner of the home page). If you're not logged in, in the **Admin Login** section (in the upper left area of the home page), enter the administrator password (1– 20 characters or numbers). (The default password is "password.")

3. Click **Advanced settings > Device > Basic**.

4. Select a value for **TRU-Install**.

Browser Interface Home Page

Access your device and connection information, and configure device settings from the browser interface home page.

Home Page Basics

Home Page Buttons

Icons and Text

Alerts

Viewing Device Information

Updates

The home page is the entry page of the browser interface that lets you:

● Display status information for your device and your data connection.

● Launch and end a network connection.

● Change the settings for your device and your data connections (if you're logged in).

● Access additional resources (the user guide and the Important Information document).
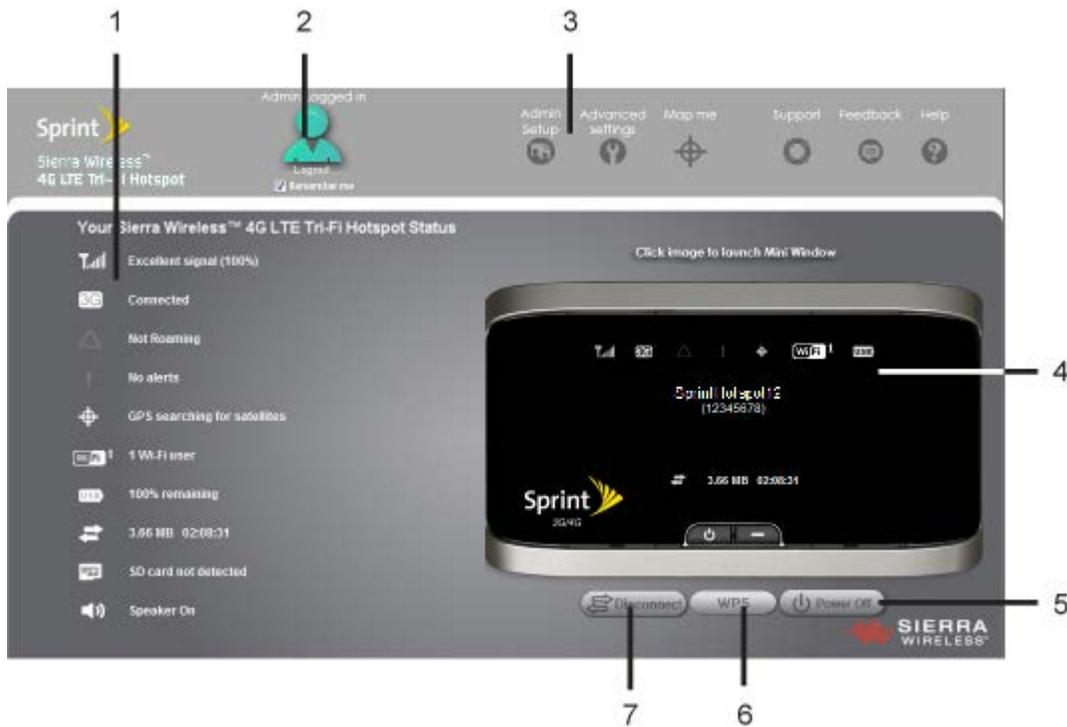
Callout item	Description
1	When you click an icon or the text next to it, a window opens to the right. The window contains additional status information and, if you're logged in, commonly-used configurable settings. (See Icons and Text.)
2	Use this area to enter the administrator password and log in. When you're logged in, you can change settings. (See Logging On as an Administrator.)
3	Clicking one of these buttons displays a window or a menu. (See Home Page Buttons.)
4	This is the Virtual Device; it reflects the status of your device. If you click the image, a movable Mini Window is opened. (See "Virtual Device" and "Mini Window" in Device Views.)
5	A handy way to turn the device off, especially if, for example, you're in an airplane before takeoff, and the device is in your overhead bag. (This button is available only if you're logged in.)
6	Start a WPS session (to add to your network a device that supports WPS), or enable or disable WPS. (See Connecting Through WPS.)
7	Disconnects a connection, or connects (if currently there's no connection). (This button is available only if you're logged in.)

Home Page Basics

Learn how to display the home page, log on as administrator, and more.

Displaying the Home Page of the Device

Logging On as an Administrator

Device Views

Turning Your Device Off

Setup Pages

Displaying the Home Page of the Device

There are several ways you can display the home page of the device.

Note: You can display the home page only when your device is turned on and you have established a connection to it (through Wi-Fi or through the micro-USB cable).

To display the home page, type one of the following in the address bar of your Web browser:

- **http://SprintHotspot**

- **http://192.168.0.1**

- **SSID** value (field in **Advanced settings > Wi-Fi > Network** and also in **Advanced settings > Router > LAN**)

Note: If you're using the Google Chrome Web browser, after typing in the address bar, press the Down Arrow key and then the Enter key. (If you press only the Enter key, a Google search is started, using the information you typed in.)

If your Web browser displays an error message, see Cannot Display the Home Page.

Logging On as an Administrator

You don't need to log in to access and use the home page. However, logging in provides several benefits.

When you log in:

- Additional information appears in the window that opens when you click an item on the left side of the home page. (See Icons and Text.)

- You can access the **Advanced Settings** window, where you can modify additional settings.

- You can rerun the device setup, if required (**Admin Setup** [ ]).

- You can install updates.

To log in:

1. Make sure that nobody else is already logged in — other people can use the home page at the same time, but only one user can be logged in.

2. In the **Admin Login** section (in the upper left area of the home page), enter the administrator password (1–20 characters or numbers). (The default password is "password." It's recommended you change the password, if you haven't already.)

3. Click **OK**.

After a period of inactivity, you will be automatically logged off (timeout security feature), unless you select **Remember me** (below the password field). (For more information, see Automatic Login ("Remember Me").)

Device Views

The virtual device and the Mini Window reflect most of the icons and text displayed on the real device, and are a convenient way to easily see the device status.

Virtual Device

The right half of the home page contains an image of your device. This is a "virtual device" — it reflects most of the icons and text displayed on the real device.

Mini Window

If you click the virtual device in the home page, the Mini Window opens — an image of the device in a separate Web browser window.

Similar to the virtual device, the Mini Window reflects most of the icons and text displayed on the real device.

To save space on your monitor, you can close the home page and move the Mini Window to the side of your monitor. Then you can use the window to keep an eye on the status of your device and connection. (To reopen the home page, click the **Home** link.)

If you're logged in, the window has a **Connect** or **Disconnect** button, and a **Power Off** button.

Turning Your Device Off

There are several ways you can turn your device off.

- From the home page:

  - Make sure you're logged in to the home page.

  - Click **Power Off** (below the Virtual Device).

- From the Mini Window:

  - Make sure you're logged in to the home page.

  - Click **Power Off**.

Tip: You can also turn the device off by pressing and holding the power button until the device turns off.

Setup Pages

At any time, you can rerun the device setup, if required.

The Welcome to your Sierra Wireless™ 4G LTE Tri-Fri Hotspot window opens in two cases.

- Automatically, as part of the initial setup of your newly purchased device.

- When you click **Admin Setup** ( ) from the home page, make changes (if applicable) and then click **Submit** (you must be logged in).

Note: This window displays the administrator password and the address of the device home page. Please remember this information or write it down in a safe place.

This window provides several options.

- To keep the default settings of the device, select one of the following:

  - **The Internet** — This connects you immediately to the Internet.

  - **My Sierra Wireless™ 4G LTE Tri-Fri Hotspot's home page** — From the home page you can view the device status and customize settings.

- To change security settings, select **Set up my Sierra Wireless™ 4G LTE Tri-Fri Hotspot**.

Home Page Buttons

The home page has several buttons that open a browser window or perform certain actions on the device.

The top horizontal part of the home page has several buttons.

- **Admin Login** — Click this button to log on as administrator. (See Logging On as an Administrator.)

- **Admin Setup** — Click this button to rerun the device setup, for example, after you've reset the software to default settings. (See Setup Pages.)

- **Advanced settings** — Click this button to display a window from which you can configure all the settings of the device and the browser interface. (See Advanced Settings.)

- **Map me** — Use this button to do one of the following:

  - Open a Web browser window that shows your current location. (See Viewing Your Current Location in a Web Browser.)

  - Search for the closest gas station, restaurant, other points of interest, or do a custom search. (See Performing a Location Search.)

- **Support** — This button opens the online support site in a new Web browser window or tab. (See Support Button.)

- **Feedback** — Use this button to send your comments on the device. (See Feedback.)

- **Help** — This button displays a menu with options to open online help, the user guide, or the important information booklet.

When you're logged in, several buttons are displayed below the Virtual Device.

- Connect/Disconnect — This button connects or disconnects your device from the 3G or 4G network.

- WPS — This button starts a WPS (Wi-Fi Protected Setup) session. (See Connecting Through WPS.)

- Power Off — This button turns the device off.

Admin Setup Button

This button displays a window where you can change the administrator password, Wi-Fi network name (SSID), Wi-Fi security type, and Wi-Fi password.

For more information, see Setup Pages.

Advanced Settings

From the Advanced Settings window you can configure all the settings of the device and the browser interface.

The Advanced Settings window has the following tabs, each with several panels:

- Device tab. (See Device Tab.)

- WAN tab. (See WAN Tab.)

- Wi-Fi tab. (See Wi-Fi Tab.)

- Router tab. (See Router Tab Settings.)

For most fields and buttons, contextual help, if enabled, appears to the right of the window when you move the cursor over an item. (For more information, see "Contextual Help in the Advanced Settings Window" in Online Help.)

To access the Advanced Settings window:

1. Make sure you're logged in to the home page.

2. Click **Advanced settings** ( ).

Map me Button

The **Map me** button is used for GPS/Location Based Services: you can, for example, search for the closest gas station, restaurant, other points of interest, or do a custom search.

See Sprint Location Services.

Support Button

The **Support** button opens the online support site in a new Web browser window or tab.

Note: This button is available only when you're connected to the Internet.

Feedback

The **Feedback** button opens the online feedback site in a new Web browser window or tab.

Note: This button is available only when you're connected to the Internet.

Help Button

This button displays a menu with several options.

- Display the online Help.

- Download the user guide.

- View the important information booklet. This booklet contains regulatory notices, warranty, and other information.

Connect/Disconnect Button

This button connects or disconnects your device from the 3G or 4G network.

Note: This button appears only when you're logged in.

WPS Button

This button starts a WPS (Wi-Fi Protected Setup) session. (See Connecting Through WPS.)

Note: This button appears only when you're logged in.

Power Off Button

This button turns the device off.

Note: This button appears only when you're logged in.

Note: You can turn the device on only by using the physical power button on the device or by disconnecting and reconnecting the micro-USB cable.

Icons and Text

Learn about the various icons and text that provide status information.

Signal Information

Mobile Broadband Information and Settings

Roaming Information and Settings

Alert Information

GPS Information and Settings

Wi-Fi Users Information and Settings

Battery Information and Settings

Internet Connection Information

microSD Card Information and Settings.

Sounds Information and Settings

The left part of the home page has a vertical row of icons and text, starting with the signal strength indicator .

Y.ıl	Good signal (40%)
3G	Connected
△	Not Roaming
!	No alerts
⊕	GPS searching for satellites
WiFi ¹	1 Wi-Fi user
USB	100% remaining
⇄	42.5 KB 00:05:41
micro SD	Shared access; Security enabled
◀))	Speaker On
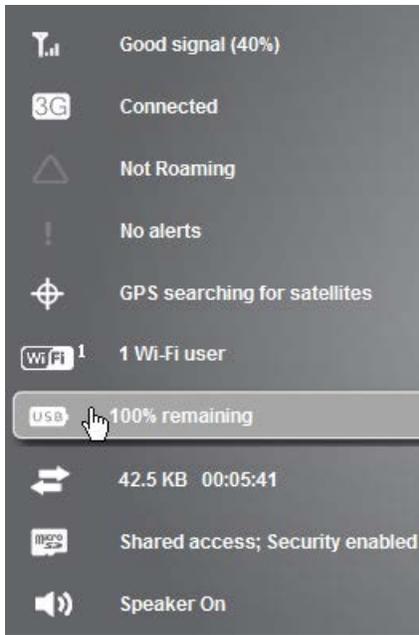
Most of these icons are also shown on the physical device and Virtual Device (Virtual Device). When you hold the mouse over an icon, the corresponding icon on the Virtual Device is highlighted.

If you click an icon or the text, a window opens with additional information, as shown in the following screenshot:

Your Sierra Wireless™ 4G LTE Tri-Fi Hotspot Status

Y.ıl	Good signal (40%)
3G	Connected
△	Not Roaming
!	No alerts
⊕	GPS searching for satellites
WiFi ¹	1 Wi-Fi user
USB	100% remaining
⇄	42.5 KB 00:05:41
micro SD	Shared access; Security enabled
◀))	Speaker On

Battery Information and Settings
Battery Level: 100% remaining

Battery or USB powered:
Wi-Fi Performance: ○ Short Range ● Long Range
Standby Timer: 20 minutes ▾

AC powered:
Wi-Fi Performance: ○ Short Range ● Long Range

Save   Cancel

If you're logged in, the window may also display configurable settings.

Note: A more complete set of configurable settings is available in the **Advanced Settings** window. (See Advanced Settings.)

Signal Information

Learn how to determine the signal strength and get detailed 3G/4G status information.

Icon	Description
	No signal
	Very weak signal
	Excellent signal

Click the signal strength icon to display the Signal Quality window. The window displays:

- The active network — the network that is currently being used for your data connection. For example, "3G (EVDO Rev A)."

- 3G or 4G status:

  - Connection status. For example, "Connected."

  - Tables that show the coverage type, RSSI and Ec/Io (for 3G), RSSI and CINR (for 4G WiMAX), and RSRP and RSRQ (for 4G LTE).

    RSSI reflects the signal strength of the network.

    Ec/Io is a dimensionless ratio of the average power of a channel, typically the pilot channel, to the total signal power.

    RSRP stands for Reference Signal Received Power and reflects the LTE signal strength.

    CINR stands for Carrier to Interference-plus-Noise Ratio and is a measurement of signal effectiveness.

    RSRQ stands for Reference Signal Received Quality and reflects the LTE signal quality. RSRQ is the ratio between the RSRP and the Received Signal Strength Indicator (RSSI).

    The first table also shows the type(s) of 3G service you have: 1X, 1xEV-DO, or both. (To determine whether you have EV-DO Rev. 0 or Rev. A service, use the text near the 3G icon; see Mobile Broadband Information and Settings.)

- **Scan for 4G** button (available only if 4G is in power save mode — the LCD of the device displays "Power Save Mode. 4G Network not found"). Click this button to search for and attempt to connect to a 4G network. (Whether or not a connection to 4G occurs depends on the WAN Mode setting; see WAN Tab: Setup Panel.)

Tip: If 4G is in power save mode, you can also scan for 4G from the "Network Status" LCD information screen. (See LCD Information Screens.)

See also Improving Signal Strength.

Mobile Broadband Information and Settings

The 3G or 4G icon indicates the service and connection state. Note that only one icon is shown (the active network).

Icon	Description
3G or 4G	You have no service. Try the suggestions in Cannot Connect to the 3G or 4G Network.
3G or 4G	You have service but are not connected.
3G or 4G	You have service and are connected.

The text next to the icon displays the connection status, for example, "No service," or "Connected."

Click the icon to display the Mobile Broadband Information window. The window displays:

- The active network — the network that is currently being used for your data connection. For example, "4G", "4G LTE", or "3G (EVDO Rev A)."

- 3G and 4G status. For example, "Connected."

- **Connection Preferences** (if you're logged in).

Configuring the 3G/4G Connection Preferences

The value determines which network(s) to connect to, and in what order:

- **3G Preferred** — Connection can be established to either 3G or 4G; if both are available, 3G is used.

- **4G Preferred** — Connection can be established to either 3G or 4G; if both are available, 4G is used. This setting is recommended if your service provider has no data limit for 4G and 4G LTE, but does for 3G, or you want to take advantage of the faster data transfer speeds of 4G/4G LTE.

- **3G Only** — Connection can be established only to 3G.

- **4G Only** — Connection can be established only to 4G or 4G LTE. (If you don't have 4G or 4G LTE coverage, you can save power by selecting **3G Only**.)

Note: The following options are not available if **3G Only** is selected.

- **LTE + WiMAX** — When connecting to 4G, connection can be established to either 4G WiMAX or 4G LTE; if both are available, 4G LTE is used (unless the 4G WiMAX signal is significantly better than the 4G LTE signal).

- **LTE Only** — When connecting to 4G, connection can be established only to 4G LTE.

- **WiMAX Only** — When connecting to 4G, connection can be established only to 4G WiMAX.

To automatically connect to the network upon loss of connection or when the device powers on, select **Connect Automatically**. To prevent this from happening when you're roaming, also select **Disable when roaming**.

Note: **Disable when roaming** does not prevent you from roaming; it only prevents a connection (that was lost while roaming) from automatically being reestablished.

Roaming Information and Settings

The roaming indicator shows whether you are roaming. The text near the icon may indicate additional details.

Icon	Description
	Not roaming
	Roaming
[flashing]	Enhanced roaming indicator

Note: Roaming on 4G is not supported.

Click the roaming indicator to display the Roaming Information window. The window displays:

- Roaming status.

- **Allow 3G roaming** field (if you're logged in).

  - If you select this field, you can roam and connect when outside of Sprint coverage, but additional charges may occur. (To roam outside of the United States and Puerto Rico, you must also select **Allow 3G international access**.)

- If you do not select this field, you can connect only when you're inside a Sprint coverage area.

Note: If you change the value of this field, the device restarts (after you click **Save**).

- **Allow 3G international access** field (if you're logged in) — allows 3G roaming outside of the United States and Puerto Rico (for example, in Canada).

  If this field is not displayed, select **Allow 3G roaming**.

Alert Information

The alerts icon indicates whether there are any alerts (situations that require your attention).

Note: To view alert information, you must be logged in. New alerts are checked upon device power-up. That is, if an event occurs, you won't be notified until the device is restarted.

Icon	Description
	No alerts are available.
	One or more alerts are available.

The text next to the icon indicates the number of alerts.

Click the icon to display the Alert window. (For more information, see Alerts.)

GPS Information and Settings

The GPS icon indicates whether GPS is off, available, or active.

Icon	Description
	GPS is off (not enabled). Before you can use GPS, you must accept the GPS privacy agreement and enable GPS. (See GPS Privacy Agreement and Enabling GPS.)
	GPS is on and available. (The GPS privacy agreement has been accepted, and GPS is enabled.)
(flashing)	GPS is active (acquiring a location fix).

The text next to the icon displays the GPS status, for example, "GPS not enabled" or "GPS searching for satellites."

Click the icon to display the GPS Information and Settings window. The window shows the GPS status and, if available, location information, including:

- **HEPE** — The Horizontal Estimated Position Error reflects accuracy (horizontal/vertical precision).

Note: For best results, minimize the number of obstructions between your device and the GPS satellites.

- **Timestamp** — This indicates the time of the last fix.

Configuring the Settings

When you're logged in, the following settings are available:

View privacy agreement (link displayed if you haven't yet accepted the GPS privacy agreement). You cannot enable and use GPS until you accept this agreement. Click the link to view and then accept the agreement.

Enable GPS — To use GPS and to configure other GPS settings, this check box must be selected.

GPS Mode — This setting determines how often the device should obtain a fix.

- **One-time** — A single fix is used. Use this option if you'll be using your device at the same location.

- **Continuous** — Fixes are obtained on a regular basis; also known as auto-tracking. This is useful for turn-by-turn (TBT) navigation applications, such as driving directions.

Get fix now — This button starts a one-time fix (not displayed if **GPS Mode** is **Continuous** or a GPS session is already in progress). If you change the value from **Continuous** to **One-time**, you must click **Save** before your changes take effect and the fix becomes possible.

Mapping service — This determines the mapping service (for example, Google Maps or MapQuest) that displays the GPS results (in a separate browser window).

Metric units — This setting specifies whether to use metric when displaying the GPS results (for example, the altitude, speed, HEPE).

Note: Additional settings are available at **Advanced settings > WAN > GPS**. (See GPS Settings.)

Wi-Fi Users Information and Settings

The Wi-Fi users icon provides information about the status of Wi-Fi and the number of connected users.

- Number of Wi-Fi users are connected to the device — for example, shows that no (zero) users are connected.
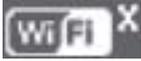
- — Wi-Fi of the Sierra Wireless 4G LTE Tri-Fi Hotspot has been disabled through the browser interface. (To enable Wi-Fi, change the **Disable Wi-Fi** setting in the Wi-Fi Users window [see "Connected Users Information", below].)

The icon is on the left side of the home page.

Click the icon to display the Wi-Fi Users window.

Connected Users Information

When you're logged in, the Wi-Fi Users window shows a table with information on computers currently connected to the device.

A row may show one or both of these icons:

- — The user of this computer is logged in as administrator.

- — This computer is connected to the device through the micro-USB cable.

MAC Address — Each wireless device has a unique MAC address (assigned by its manufacturer). On Windows PCs, the MAC address is called the "physical address;" on a Mac computer, it is called the "Ethernet ID." (See Finding the MAC Address.)

Block — Use this to block a computer's access to the device. You might want to do this if:

- You don't recognize a listed computer.

- You have lots of data to transfer (you want to be the sole user of the bandwidth).

- You're approaching the data limit on your account.

Max Wi-Fi users — You can limit the number of Wi-Fi users (maximum of eight) that can connect to the device. A smaller number improves performance and security.

Disable Wi-Fi — This setting specifies when to turn off the Wi-Fi of the device.

- **Never** — Select this value if you want to make sure the device is always broadcasting Wi-Fi signals.

- **Always** — Select this value if you always want to use the device in tethered mode and you want to make sure the device is never broadcasting any Wi-Fi signals. With this option, WPS won't be available. (See Connecting Through WPS.)

- **When connected to USB** — Only a computer connected through the micro-USB cable to the device will be able to use it. With this option, WPS won't be available. (See Connecting Through WPS.)

Battery Information and Settings

The battery icon indicates the state of the battery of the device.

The text next to the icon displays additional information, for example, the charging status (% remaining or % complete). If "Charging paused" is displayed, see What Do I Do if the Home Page Displays "Charging paused"?

Tip: You can also check the battery icon from the Home page, Mini Window, and device LCD.

Icon	Description
	Battery level is critical. Charge the device immediately. (See Charging the Battery.)
	No battery; connected to an electrical outlet (through the AC charger).
	Connected to USB. Battery is either charging or is not inserted.
	Charging through the AC charger.
	Battery is low. Charge the device. (See Charging the Battery.)
	Battery is charged.

Click the icon to display the Battery Information and Settings window.

When you're logged in, you can set the behavior for when the device is:

- **Battery or USB powered**. Choose one of the following:

  - **Short Range** — This setting improves battery life, at the cost of shorter Wi-Fi range.

  - **Long Range** —This setting allows you to use your wireless devices farther from your Sierra Wireless 4G LTE Tri-Fi Hotspot, at the cost of shorter battery life and the increased possibility of interference with/from other nearby Wi-Fi devices.

- **AC powered**. Choose one of the following:

  - **Short Range** — Choose this setting if you have a designated wireless area and you need to minimize the effect of your network on other networks in the vicinity.

  - **Long Range** — This setting allows you to use your wireless devices farther from your Sierra Wireless 4G LTE Tri-Fi Hotspot but increases the possibility of interference with or from nearby wireless networks.

Standby (Low Power) Mode

When the device is in standby (low power) mode, the 3G/4G modem radios, the Wi-Fi radio, and the LCD are off, and the power button ⏻ is flashing (approximately every 8 seconds).

When you're logged in, you can set how soon the device goes into standby mode when no Wi-Fi users are connected to it (**Standby Timer**).

You can specify different settings for battery power and AC power. (See Device Tab: Basic Panel.)

Note: This setting has no effect when the device is connected to a computer through the micro-USB cable.

To exit standby mode:

► Connect the device to the AC charger or computer through the micro-USB cable.

— or —

Press the power button ⏻.

Internet Connection Information

Click the data icon to display the Internet Connection Information window.

Note: Data usage amounts are approximate and should not be used for billing purposes. For accurate data usage amounts, check with Sprint or click the **check carrier usage** link.

When you click ⇄ the Internet Connection Information window displays:

- Data statistics for the current connection session:

  - Data sent

  - Session duration

  - Data received

  - Total transferred

- **WWAN IP Address** — This is the external IP address of the modem [3G or 4G] (that is, the IP address of the modem as seen from the Internet).

- **More info** — Click this link to display, when you're connected to the network, the following information:

  - **WAN DNS Primary** — This is the address of the Internet system used to translate names (for example, sprint.com) into IP addresses.

- **WAN DNS Secondary** — This is the address of the Internet system used to translate names (for example, sprint.com) into IP addresses. The secondary DNS is used when there is a problem with the primary DNS.

- **Default Gateway** — This is the address of the node on the computer network that the network software uses when an IP address does not match any other routes in the routing table (that is, when an IP packet's destination address is outside of the local subnet).

- **WAN MTU size** — This is the size of the largest packet ("Maximum Transmission Unit") that a network protocol can transmit.

Viewing and Configuring Detailed Internet Connection Information

When you're logged in, the Internet Connection Information window displays a table showing data use:

- In the current cycle or since you last reset the data usage figures — whichever occurred more recently. These numbers get automatically reset to 0 on the day selected in the **Starts on day list**.

- Over the lifetime of the device.

- By network [3G, 4G, and 4G LTE], and by sent, received, and total.

From this window you can:

- Reset the data usage figures for the current billing cycle. (Click **Reset**.)

- Change the start day of the billing cycle (in the **Starts on day** list).

- See the number of days left in the cycle.

- Check the data usage as tracked by Sprint. (When you're connected to the network, click the link **check carrier usage**.)

microSD Card Information and Settings

The text next to the microSD icon indicates the status of the card.

The card may be:

- Enabled

- Detected

- Accessible by all ("shared") or only the administrator

- Accessible with or without a password (security)

Click the microSD icon ( ) to display the SD Card Information and Settings window. The window displays:

- The card status (see the list above)

- Storage capacity of the card, and space available (displayed only if a card is detected)

- A button to safely eject the card (**Safe-Eject SD Card**; displayed only if a card is detected))

When you're logged in, you can:

- Enable or disable the microSD card slot. (See Enabling the microSD Card Slot.)

- Set up access to the card. (See Setting Up Access to the microSD Card.)

Sounds Information and Settings

The sounds icon shows whether the device speaker is on.

Icon	Description
	The device speaker is on.
	The device speaker is off.

Click the sounds icon ( ) to display the Sounds window. The window displays:

- Status of the device speaker (on or off).

- If you're logged in, check boxes to enable or disable sounds for the following events:

  - **Internet connected** — A sound is played when you connect to the Internet.

  - **Low battery** — A sound is played when the battery is low. This is useful as a reminder to charge the device.

  - **Internet disconnected** — A sound is played when you lose the connection to the Internet.

  - **System alerts** — A sound is played when a system alert occurs. You can then use the device LCD or the Alerts window to get information about the alert. (See Alert Information.)

Note: System alerts include several types of events, for example:
  - Critical battery
  - Critical temperature
  - Software update available

- Routing hardware settings reset
- Device startup failure

  - **Wi-Fi user has joined** — A sound is played when a Wi-Fi user connects to your network. This is useful, for example, to detect an unwelcome Wi-Fi user if you're the only one using the device.

  - **Enter standby mode** — A sound is played when the device enters standby mode. (See "Standby (Low Power) Mode" in Battery Information and Settings.)

  - **Wi-Fi user has left** — A sound is played when a Wi-Fi user disconnects from your network.

  - **Last user has left** — A sound is played when the last Wi-Fi user disconnects from your network. You can turn the device off if nobody will be using it for awhile.

- If you're logged in, for each of the above events, click ▶ to play each corresponding sound.

Tip: You can also disable all sounds through the mute switch on the device. (See "Mute Switch" in Other Buttons and Switches.) If you've enabled the sounds through the home page, but there are no sounds when an event occurs, check the position of the mute switch.

Alerts

Alerts notify you about situations that require your attention.

3G Activation Required

GPS Privacy Agreement

SD Card Error

Software Update Available

The alerts icon ▯ indicates whether there are any alerts (messages that require your attention).

The icon is on the left side of the home page.

Click the icon to display the Alert window. If more than one alert is available:

- The higher priority alert opens.

- When you close an alert, the next alert opens.

- You can use the ◀ and ▶ buttons (at the top of the alert window) to view other alerts.

The options and instructions shown in the alert window depend on the alert event. Please read the instructions carefully. They may state, for example, that you have to reconnect to Wi-Fi after an update is installed.

Tip: You can view a list of available alerts on the "Alerts" LCD information screen. (See LCD Information Screens.)

3G Activation Required

If only 3G coverage is available, you won't be able to connect to the Internet until 3G activation has been completed.

To activate 3G on your device:

1. Make sure you have 3G coverage.

2. Make sure you're logged in to the home page.

3. Click the alerts icon ▯ to display the alert window.

4. If more than one alert is available, use the ◁ and ▷ buttons (at the top of the alert window) to browse to the alert.

5. In the 3G Activation Required alert window, click **Activate now**.

- If activation is successful, "Activation complete!" is displayed. You can now connect to the 3G network. If the connection is not established automatically, click **Connect** on the home page or Mini Window.

- If activation was not successful, "Activation failed" is displayed. Retry the activation. If it is not successful, contact Sprint Customer Service and have the following available:

  ▪ Your billing information.

  ▪ IMEI of the device (displayed on the packaging and inside the battery compartment).

GPS Privacy Agreement

The GPS Privacy Agreement alert appears if you haven't accepted the GPS privacy agreement. (You cannot use GPS until you accept the GPS privacy agreement and then enable GPS.)

To accept the GPS privacy agreement:

1. Make sure you're logged in to the home page.

2. In the vertical row of icons (down the left side of the home page), click the GPS icon (⊕) and, in the window that's displayed, click **View privacy agreement**.

   — or —

Display the GPS Privacy Agreement alert window. (See Alert Information.)

3. Read the agreement, and select **I have read the foregoing and hereby agree to ...**.

SD Card Error

Learn about recommended steps if you're having problems reading from the microSD card, or if the SD Card Error alert window opens or the device LCD displays "SD Card error."

1. Remove and reinsert the microSD card.

2. If the card is still not working, try it in the microSD slot of another computer.

   If it works in the other device, the card slot on your device may have a problem.

   If the card doesn't work in the other computer, try one of the following:

   ▪ Use a different microSD card.

     — or —

   ▪ Reformat your card.

Note: The formatting procedure erases all the data on the microSD card, after which the files CANNOT be retrieved. To prevent the loss of important data, please check the contents before you format the microSD card.

Software Update Available

The update may improve performance and add or modify features.

Note: During installation of the update, your Internet and Wi-Fi connections won't be available. When the installation is complete, you will need to reconnect to Wi-Fi.

To install the update:

1. Make sure your device is connected to the AC charger or computer through the micro-USB cable.

Note: If you'll be using USB for data transfer (and not just for charging the device), you must install the device driver. (See Making a Tethered Connection.)

2. Make sure you're logged in to the home page.

3. Click the alerts icon ▯ to display the alert window.

4. If more than one alert is available, use the ◁ and ▷ buttons (at the top of the alert window) to browse to the alert.

5. In the Software Update Available alert window, click **Update Options**.

6. Read the information in the Software Installation Options window.

7. To install the update, click **Download and install now**.

— or —

If you are not in a strong signal area, make a note of the URL displayed in the window and click **I'll get the update later**. At a later time, access the URL to download the update to your computer, and then follow the steps in Upgrading Firmware From a File.

When the installation is complete, reconnect to Wi-Fi. (See How Do I Connect to Wi-Fi?)

Viewing Device Information

View information about your device and lifetime data usage.

1. Log in to the home page.

2. Click **Advanced settings** ( ).

3. Click **Device > About**.

Note: 4G and 4G LTE information is not available if **WAN Mode** is "3G Only." (**WAN Mode** is in **Advanced settings > WAN > Setup**.)

The following information is displayed:

● **Model Number** — This is the manufacturer's model of your device.

● **Network Operator** — This field shows the carrier that your device was activated with.

● **Manufacturer** — This is the company that made your device.

● **Wi-Fi Firmware Version** — This is the firmware version for the Wi-Fi access point of the device.

● **Software Version** — This is the firmware version for the routing hardware of the device.

● **Router PRI Version** — This is the PRI version for the routing hardware of the device. The PRI (Product Release Instructions) is a file that contains the settings used to configure wireless products for a particular service provider, customer, or purpose.

● **Wi-Fi MAC Address** — This is the MAC address of the 4G module. Each wireless device has a unique MAC address (assigned by its manufacturer).

● **Activation** — This field reflects whether 3G is activated.

- **Reconditioned** — This field indicates whether your device has been returned for service or repair and reconditioned (if applicable).

- **Total Bytes** — This is the amount of data transferred over the 3G network during the lifetime of the device.

- **MDN** (Mobile Directory Number) — This is a 10-digit phone number.

- **ESN** or **MEID** (3G).

  The ESN (Electronic Serial Number) is the unique first-generation serial number assigned to the 3G component of the device.

  The MEID (Mobile Equipment Identifier) is the unique second-generation serial number assigned to the 3G component of the device.

- **PRL Version** — The PRL (Preferred Roaming List) is an account configuration item set by your service provider. It controls the radio channels and network carrier used by the 3G modem. An updated PRL may improve your 3G network service.

- **PRI Version** — This is the PRI version of the 3G component of the device.

- **Firmware Version** — This is the firmware version of the 3G component of the device.

- **Total Bytes** — This is the amount of data transferred over the 4G network during the lifetime of the device.

- **Firmware Version** — This is the firmware version of the 4G component of the device.

- **MAC Address** — This is the MAC address of the 4G module. Each wireless device has a unique MAC address (assigned by its manufacturer).

- **DDF ID** — This is the version information of your 4G channel plan, which determines the frequencies to scan and 4G networks to detect.

- **Total Bytes** — This is the amount of data transferred over the 4G LTE network during the lifetime of the device.

- **Firmware Version** — This is the firmware version of the 4G LTE component of the device.

- **MAC Address** — This is the MAC address of the 4G LTE module. Each wireless device has a unique MAC address (assigned by its manufacturer).

- **Driver Version** — This is the version of the 4G LTE driver of the device.

The window also has buttons to:

- Save the information to a text file.

- Reset the 3G and 4G configuration of the device to default settings (**Reset Device to Factory Defaults**). (See Resetting the 3G and 4G Configurations to Default Settings.)

- Reset the 3G and 4G configuration of the radios of the device to default settings (**Reset Radios to Factory Defaults**). (See Resetting the 3G and 4G Radio Configurations to Default Settings.)

Tip: You can view some of the above information on the "About..." LCD information screen. (See LCD Information Screens.)

Updates

From time to time, updates may become available for your device. You can download and apply updates through the **Advanced settings > Device > Basic** page.

Automatically Checking for Updates

Manually Checking for Updates

Upgrading Firmware From a File

Note: If a software update is available, the device LCD displays a message, and an alert is available from the home page. (See Software Update Available.)

The updates may improve performance and add or modify features. The updates may include the following:

- Device firmware

- The browser interface

- Help files

- Other files

You can:

- Set the browser interface to automatically check for updates (see Automatically Checking for Updates).

- Manually check for updates. (See Manually Checking for Updates.)

Tip: You can view the update availability and status on the "Software Updates" LCD information screen. (See LCD Information Screens.)

Automatically Checking for Updates

You can specify how often the browser interface checks for updates.

1. Log in to the home page.

2. Click **Advanced settings** ().

3. Click **Device > Basic**.

4. In the **Check for Updates** list, click a value.

Note: If the **Check for Updates** list is not available, your device supports the Guaranteed Update feature, which automatically checks for updates, at a pre-determined frequency. This feature requires 4G or 4G LTE coverage.

Tip: When updates are available, an alert is shown in the browser interface. (See Alert Information.)

Manually Checking for Updates

At any time, you can manually check for updates.

Note: During installation of the update:
- DO NOT turn off or unplug the device.
- Your Wi-Fi and Internet connections won't be available.

When the installation is complete, you will need to reconnect to Wi-Fi. (See How Do I Connect to Wi-Fi?)

1. Log in to the home page.

2. Make sure you're connected to 3G or 4G.

3. Click **Advanced settings** ().

4. Click **Device > Basic**.

5. Click **Check for updates now**. (The message next to the button indicates whether updates are available.)

Installing the updates

To install available updates, after you've manually checked for updates:

1. Make sure your device is connected to the AC charger or computer through the micro-USB cable.

Note: If you'll be using USB for data transfer (and not just for charging the device), you must install the device driver. (See Making a Tethered Connection.)

2. Click **Update options**.

3. Read the information in the Software Installation Options window.

4. To install the update, click **Download and install now**.

— or —

If you are not in a strong signal area, make a note of the URL displayed in the window and click **I'll get the update later**. At a later time, access the URL to download the update to your computer, and then follow the steps in Upgrading Firmware From a File.

5. When the installation is complete, reconnect to Wi-Fi. (See How Do I Connect to Wi-Fi?)

Upgrading Firmware From a File

Use this option when you have an updated firmware file that you've, for example, downloaded from the Sprint or Sierra Wireless website.

Note: During installation of the update:
- DO NOT turn off or unplug the device.
- Your Wi-Fi and Internet connections won't be available.

When the installation is complete, you will need to reconnect to Wi-Fi. (See How Do I Connect to Wi-Fi?)

To upgrade the device firmware from a file:

1. Log in to the home page.

2. Make sure **When connected to USB** is selected (for **Disable Wi-Fi**). (See Disabling Wi-Fi When Connected Through USB.)

3. Make sure your device is connected to the AC charger or computer through the micro-USB cable.

4. Click **Advanced settings** ( ).

5. If you want to later confirm that the upgrade was successful, write down the current version information (shown in **Device > About**):

   ▪ Software version

   ▪ Firmware version (in the 3G Information section)

   ▪ Firmware version (in the WiMAX Information section)

   ▪ Firmware version (in the LTE Information section)

6. Click **Device > Basic**.

7. Optionally, save the current configuration (recommended).

   ▪ Click **Export**.

- Save the file. Note the filename and path.

8. Click the **Browse** button next to the **Update Firmware From File** field, and click the firmware file to upload to the device.

9. Click **Update**.

    Please wait while the upgrade occurs; this may take several minutes. The device LCD shows the upgrade status. The device will restart (possibly several times).

    Once the upgrade is complete, the LCD device shows the usual icons and text (for example, the device name).

10. Compare the current version information (in **Device > About**) to the values you wrote down in step 5 to confirm that the upgrade was successful.

11. If you've saved the current configuration, reload it.

    - Click the **Browse** button next to the **Import Router Settings** field, and click the file you've saved.

    - Click **Import**.

12. Reconnect to Wi-Fi. (See How Do I Connect to Wi-Fi?)

Device Settings

The Advanced settings menu controls many of the device's settings and can be accessed by clicking **Advanced settings** in the browser interface home page.

Power Settings

Login Settings

Display Settings

Sound Settings

Advanced Settings

Router Tab Settings

Exporting and Importing Settings

Device Logs

Power Settings

Control your device's battery usage through these settings.

Battery and USB Power Settings

AC Power Settings

Battery and USB Power Settings

You can specify the settings for battery power and USB power.

- Short Range — This setting improves battery life, at the cost of a shorter Wi-Fi range.

- Long Range — This setting allows you to use your wireless devices farther from your Sierra Wireless 4G LTE Tri-Fi Hotspot, at the cost of shorter battery life and the increased possibility of interference with/from other nearby Wi-Fi devices.

To choose an option:

1. Make sure you're logged in to the home page.

2. Click the battery icon   . The Battery Information and Settings window opens.

   — or —

   Click **Advanced settings > Wi-Fi > Network**.

3. Select an option in the **Battery or USB Powered** section.

AC Power Settings

You can specify the settings for AC power.

- **Short Range** — Choose this setting if you have a designated wireless area and you need to minimize the effect of your network on other networks in the vicinity.

- **Long Range** — This setting allows you to use your wireless devices farther from your Sierra Wireless 4G LTE Tri-Fi Hotspot but increases the possibility of interference with or from nearby wireless networks.

To choose an option:

1. Make sure you're logged in to the home page.

2. Click the battery icon   . The Battery Information and Settings window opens.

   — or —

   Click **Advanced settings > Wi-Fi > Network**.

3. Select an option in the **AC Powered** section.

Login Settings

You can change the administrator password, and also enable automatic login.

Changing the Administrator Password.

Automatic Login ("Remember Me").

Changing the Administrator Password

For security reasons, change the administrator password on a regular basis.

Note: If you forget the Admin Login password, you'll need to reset the device to its default settings and go through the device setup. (See What Do I Do if I Forget the Administrator Password?)

1. Log in to the home page.

2. Click **Advanced settings > Device > Basic**.

3. In the **Admin Password** field, type the new password (1–20 letters, numbers, or symbols).

Automatic Login ("Remember Me")

For convenience, you can enable automatic login.

If you enable automatic login:

- Anyone who uses the computer will automatically be logged in to the home page (as long as no one else has already logged in from another computer); entering the administrator password is not required.

- The timeout security feature is disabled — you will never be automatically logged off.

To enable automatic login:

1. From the computer that you want to enable automatic login, log in to the home page.

2. In the login area, select the **Remember me** check box.

You can repeat the above steps on other computers; however, since only one administrator can be logged in at a time, only the first person to display the home page will be logged in.

Viewing Computers That Are Set to Automatically Log In as Administrator

1. Log in to the home page.

2. Click **Advanced settings > Device > Basic**.

3. Next to **Remember me Client List**, click **show list**.

Disabling Automatic Login For a Specific Computer

1. Log in to the home page.

2. Click **Advanced settings > Device > Basic**.

3. Next to **Remember Me Client List**, click **show list**.

4. In the row for the computer that you want to disable automatic login, click **Remove**.

Display Settings

Adjust your screen's settings to suit your surroundings and to prolong the battery life; you can also enable the power button LED to act as a status indicator.

Turning the LCD On or Off

Setting the LCD Timeout

Setting the LCD Brightness

Enabling and Disabling the Power Button LED

Turning the LCD On or Off

Turning the LCD off helps prolong the battery life, but you can't check the LCD for status icons and messages.

1. Log in to the home page.

2. Click **Advanced settings > Device > Display**.

3. Set the **LCD Backlight** field to **On** or **Off**.

Setting the LCD Timeout

Use this feature to select the delay time before the LCD automatically turns off.

Tip: Alternatively, you can permanently turn the LCD off, in which case it will never become lit and will not display text and icons. (See Turning the LCD On or Off.)

To set the amount of time, after which the LCD of the device temporarily turns off:

1. Make sure you're logged in to the home page.

2. Click **Advanced settings > Device > Display**.

3. Make sure **LCD Backlight** is set to **On**.

4. In the **Turn Backlight Off** list, click a value. (A smaller value helps prolong the battery life.)

Note: The LCD turns on if an important system event occurs.

Setting the LCD Brightness

Adjust your screen's settings to suit your surroundings.

1. Make sure you're logged in to the home page.

2. Click **Advanced settings > Device > Display**.

3. Make sure **LCD Backlight** is set to **On**.

4. Select a value for **On Battery/USB Power**. (A lower brightness prolongs the battery life.)

5. Select a value for **On AC Power**.

Enabling and Disabling the Power Button LED

The power button LED on the device acts as a status indicator. (For more information, see Using the Power Button to Determine the Device State.)

To enable or disable the power button LED:

1. Log in to the home page.

2. Click **Advanced settings > Device > Display**.

3. Set the **Power Button LED** field to **On** or **Off**.

Sound Settings

You can enable or disable sounds for various events.

Enabling and Disabling Sounds for Specific Events.

Low Battery Alert

Critical Battery Level Alert

You can enable or disable sounds of the device through:

- The mute switch on the device (disables all sounds). (See "Mute Switch" in Other Buttons and Switches.)

- The browser interface (selectively disables sounds). (See Sounds Information and Settings and Enabling and Disabling Sounds for Specific Events.)

Enabling and Disabling Sounds for Specific Events

For certain types of events, sounds can be individually enabled or disabled.

1. Log in to the home page.

2. Click **Advanced settings > Device > Sounds**.

3. Next to each of the event types, select **Enable** or **Disable**.

Sounds for the following events can be individually enabled or disabled:

- **Low Battery** — A sound is played when the battery is low. This is useful as a reminder to charge the device. In the **Alert When** list, you can select a battery level to trigger the alert.

- **System Alerts** — A sound is played when a system alert occurs. When you hear the device beep, use the device LCD or the Alerts window to get information about the alert. (See Alert Information.

Note: System alerts include several types of events, for example:
- Critical battery
- Critical temperature
- Software update available
- Routing hardware settings reset
- Device startup failure

- **Internet Connected** — A sound is played when you connect to the Internet.

- **Internet Disconnected** — A sound is played when you lose the connection to the Internet.

- **Wi-Fi User Has Joined** — A sound is played when a Wi-Fi user connects to your network. This is useful, for example, to detect an unwelcome Wi-Fi user if you're the only one using the device.

- **Wi-Fi User Has Left** — A sound is played when a Wi-Fi user disconnects from your network.

- **Last User Has Left** — A sound is played when the last Wi-Fi user disconnects from your network. You can turn the device off if nobody will be using it for awhile.

- **Enter Standby Mode** — A sound is played when the device enters standby mode. (See "Standby (Low Power) Mode" in Battery Information and Settings.)

Low Battery Alert

You can set an alert to sound when the battery level is low.

Setting the Alert From the Home Page

1. Make sure you're logged in to the home page.

2. Click the Sounds icon ( ).

3. In the Sounds window, select **Low battery**.

Setting the Alert From the Advanced Settings Window

1. Log in to the home page.

2. Click **Advanced settings > Device > Sounds**.

3. For the **Low Battery** field, select **Enable**.

4. In the **Alert When** list, select the battery level to trigger the alert.

Critical Battery Level Alert

You can enable an alert to sound when the battery level is critical (that is, dangerously low).

To enable this alert:

1. Log in to the home page.

2. Click **Advanced settings > Device > Sounds**.

3. For the **System Alerts** field, select **Enable**.

Note: System alerts include several types of events, for example:
- Critical battery
- Critical temperature
- Software update available
- Routing hardware settings reset
- Device startup failure

Advanced Settings

Learn about advanced configuration of the device and the browser interface.

From the Advanced Settings window you can configure all the settings of the device and the browser interface.

The Advanced Settings window has the following tabs, each with several panels:

- Device tab. (See Device Tab.)

- WAN tab. (See WAN Tab.)

- Wi-Fi tab. (See Wi-Fi Tab.)

- Router tab. (See Router Tab Settings.)

For most fields and buttons, contextual help, if enabled, appears to the right of the window when you move the cursor over an item. (For more information, see "Contextual Help in the Advanced Settings Window" in Online Help.)

Accessing the Advanced Settings Window

1. Make sure you're logged in to the home page.

2. Click **Advanced settings** ( ).

Device Tab

Use the **Device** tab to access and configure options for the device, including updates, display, microSD card, sounds, logging.

Device Tab: Basic Panel

Device Tab: Display Panel

Device Tab: microSD Card Panel

Device Tab: Sounds Panel

Device Tab: About Panel

Device Tab: Log Panel

Device Tab: Basic Panel

Use the **Basic** panel of the **Device** tab to access and configure general options for the device.

1. Log in to the home page.

2. Click **Advanced settings** ( ).

3. Click **Device > Basic**.

From this window, you can view or adjust these settings, or perform the following actions:

- **Admin Password** — This is the password used to login as administrator. (See Changing the Administrator Password.)

- **Remember Me Client List** — You can view and specify computers that are set to automatically log in. (See Automatic Login ("Remember Me").)

- **Help for Advanced Settings** — You can enable or disable contextual help for the Advanced Settings window. (See "Contextual Help in the Advanced Settings Window" in Online Help.)

- **Import Router Settings** — You can import configuration settings. (See Importing Settings.)

- **Export Router Settings** — You can export configuration settings. (See Exporting Settings.)

- **Update Firmware from File** — You can upgrade the device firmware from a file. (See Upgrading Firmware From a File.)

- **Standby Timer on Battery** and **On AC Power** — You can enable standby (low power) mode. (See "Standby (Low Power) Mode" in Battery Information and Settings.)

- **TRU-Install** — This feature installs the necessary drivers the first time you connect your device to your Windows or Mac computer through the micro-USB cable. (For information on this feature, see TRU-Install.)

- **Check for Updates** and **Check for updates now** — You can check for updates to your device. (See Automatically Checking for Updates and Manually Checking for Updates.)

- **Last checked** — This is the date that the update server was last checked.

Device Tab: Display Panel

From the **Display** panel of the **Device** tab, you can configure settings for the device LCD.

To access this panel:

1. Log in to the home page.

2. Click **Advanced settings** ( ).

3. Click **Device > Display**.

From this window, you can view or adjust these settings:

- **Power Button LED** — You can enable the power button light on the device. (See Enabling and Disabling the Power Button LED.)

- **LCD Backlight** — You can turn the LCD on or off. (See Turning the LCD On or Off.)

- **Turn Backlight Off** — This setting specifies how soon the LCD goes dormant. (See Setting the LCD Timeout.)

- **Backlight Settings** — You can adjust the brightness of the LCD. (See Setting the LCD Brightness.)

Device Tab: microSD Card Panel

From the **microSD Card** panel of the **Device** tab, you can enable the microSD card slot and configure settings used for access.

1. Log in to the home page.

2. Click **Advanced settings** ( ).

3. Click **Device > microSD Card**.

From this window, you can view or adjust these settings, or perform the following actions:

- **Status** — This field reflects the status of the microSD card slot (for example, the slot is disabled, or a card is detected).

- **SD-Card Slot** — Before you can use the microSD Card slot, you must enable it. (See Enabling the microSD Card Slot.)

- microSD Shared Folder Name — This is the name of the folder that the microSD card shows up as (in the file browser program). (See microSD Shared Folder Name.)

- Username and Password Security — You can specify whether a username and password are required to access the microSD Card. (See Setting Up Access to the microSD Card.)

- Guest Username — This is the username that non-administrators must enter before using the card.

- Guest Password — This is the password that non-administrators must enter before using the card.

Device Tab: Sounds Panel

From the **Sounds** panel of the **Device** tab, you can enable or disable sounds for specific types of events.

1. Log in to the home page.

2. Click **Advanced settings** ( ).

3. Click **Device > Sounds**.

4. Next to each of the event types, select **Enable** or **Disable**.

Sounds for the following events can be individually enabled or disabled:

- **Low Battery** — A sound is played when the battery is low. This is useful as a reminder to charge the device. In the **Alert When** list, you can select a battery level to trigger the alert.

- **System Alerts** — A sound is played when a system alert occurs. You can then use the device LCD or the Alerts window to get information about the alert. (See Alert Information.)

Note: System alerts include several types of events, for example:
- Critical battery
- Critical temperature
- Software update available
- Routing hardware settings reset
- Device startup failure

- **Internet Connected** — A sound is played when you connect to the Internet.

- **Internet Disconnected** — A sound is played when you lose the connection to the Internet.

- **Wi-Fi User Has Joined** — Useful, for example, if you're the only one using the device, to detect an intruder.

- **Wi-Fi User Has Left** — A sound is played when a Wi-Fi user disconnects from your network.

- **Last User Has Left** — A sound is played when the last Wi-Fi user disconnects from your network. You can turn the device off if nobody will be using it for awhile.

- **Enter Standby Mode** — A sound is played when the device enters standby mode. See "Standby (Low Power) Mode" in Battery Information and Settings.)

To play the sound for an event, click its ▶ button.

Device Tab: About Panel

View information about your device.

1. Log in to the home page.

2. Click **Advanced settings** (   ).

3. Click **Device > About**.

Note: 4G and 4G LTE information is not available if **WAN Mode** is "3G Only." (**WAN Mode** is in **Advanced settings > WAN > Setup**.)

The following information is displayed:

- **Model Number** — This is the manufacturer's model of your device.

- **Network Operator** — This field shows the carrier that your device was activated with.

- **Manufacturer** — This is the company that made your device.

- **Wi-Fi Firmware Version** — This is the firmware version for the Wi-Fi access point of the device.

- **Software Version** — This is the firmware version for the routing hardware of the device.

- **Router PRI Version** — This is the PRI version for the routing hardware of the device. The PRI (Product Release Instructions) is a file that contains the settings used to configure wireless products for a particular service provider, customer, or purpose.

- **Wi-Fi MAC Address** — This is the MAC address of the 4G module. Each wireless device has a unique MAC address (assigned by its manufacturer).

- **Activation** — This field reflects whether 3G is activated.

- **Reconditioned** — This field indicates whether your device has been returned for service or repair and reconditioned (if applicable).

- **Total Bytes** — This is the amount of data transferred over the 3G network during the lifetime of the device.

- **MDN** (Mobile Directory Number) — This is a 10-digit phone number.

- **ESN** or **MEID** (3G).

    The ESN (Electronic Serial Number) is the unique first-generation serial number assigned to the 3G component of the device.

The MEID (Mobile Equipment Identifier) is the unique second-generation serial number assigned to the 3G component of the device.

- **PRL Version** — The PRL (Preferred Roaming List) is an account configuration item set by your service provider. It controls the radio channels and network carrier used by the 3G modem. An updated PRL may improve your 3G network service.

- **PRI Version** — This is the PRI version of the 3G component of the device.

- **Firmware Version** — This is the firmware version of the 3G component of the device.

- **Total Bytes** — This is the amount of data transferred over the 4G network during the lifetime of the device.

- **Firmware Version** — This is the firmware version of the 4G component of the device.

- **MAC Address** — This is the MAC address of the 4G module. Each wireless device has a unique MAC address (assigned by its manufacturer).

- **DDF ID** — This is the version information of your 4G channel plan, which determines the frequencies to scan and 4G networks to detect.

- **Total Bytes** — This is the amount of data transferred over the 4G LTE network during the lifetime of the device.

- **Firmware Version** — This is the firmware version of the 4G LTE component of the device.

- **MAC Address** — This is the MAC address of the 4G LTE module. Each wireless device has a unique MAC address (assigned by its manufacturer).

- **Driver Version** — This is the version of the 4G LTE driver of the device.

The window also has buttons to:

- Save the information to a text file.

- Reset the 3G and 4G configuration of the device to default settings (**Reset Device to Factory Defaults**). (See Resetting the 3G and 4G Configurations to Default Settings.)

- Reset the 3G and 4G configuration of the radios of the device to default settings (**Reset Radios to Factory Defaults**). (See Resetting the 3G and 4G Radio Configurations to Default Settings.)

Tip: You can view some of the above information on the "About..." LCD information screen. (See LCD Information Screens.)

Device Tab: Log Panel

Configure settings related to the logging of events.

1. Log in to the home page.

2. Click **Advanced settings** ( ).

3. Click **Device > Log**.

From this window, you can:

- Enable logging of system events. (See "Enabling and Disabling Logging of System Events" in System Events.)

- Export logs. (See "Exporting System Events" in System Events and "Exporting the Connection History" in Connection History.)

- Clear logs. (See "Clearing the System Events Log" in System Events and "Clearing the Connection History" in Connection History.)

- Enable logging of connects and disconnects. (See "Enabling and Disabling Logging of Connects and Disconnects" in Connection History.)

- Set the method used for time acquisition. (See Setting the Method Used for Time Acquisition.)

WAN Tab

Configure your 3G, 4G, 4G LTE, and GPS settings.

WAN Tab: Setup Panel

WAN Tab: 3G Panel

WAN Tab: 4G Panel

WAN Tab: 4G LTE Panel

WAN Tab: GPS Panel

WAN Tab: Setup Panel

From the **Setup** panel of the **WAN** tab you can configure 3G/4G/4G LTE network preferences.

1. Log in to the home page.

2. Click **Advanced settings** ( ).

3. Click **WAN > Setup**.

From this window, you can view or adjust these settings, or perform the following actions:

- **Active Network** — This is the network that is currently being used for your data connection: 3G, 4G, 4G LTE, or none.

- **Network Operator** — This field shows the carrier that your device was activated with.

- **Session Duration** — The session duration indicates how long you've been connected to the network.

- **Session Total Data** — This indicates the amount of data transferred over the lifetime of the device (by network type) and in the current session.

- **Work Mode** — This indicates the 3G and 4G activation/provisioning status of your device and account. Technical support staff may request this value from you.

- **LTE Enabled** — This indicates whether 4G LTE is enabled on the device.

- **WAN Mode** — This setting specifies the network(s) to connect to, and in what order.

  - **3G Preferred** — The connection can be established to either 3G or 4G; if both are available, 3G is used.

  - **4G Preferred** — The connection can be established to either 3G or 4G; if both are available, 4G is used. This setting is recommended if your service provider has no data limit for 4G, but does for 3G, or you want to take advantage of the faster data transfer speeds of 4G.

  - **3G Only** — The connection can be established only to 3G. (If you don't have 4G or 4G LTE coverage, you can save power by selecting **3G Only**.)

  - **4G Only** — The connection can be established only to 4G.

Note: The following options are not available if **3G Only** is selected.

- **4G Mode** — This setting specifies the 4G network(s) to connect to.

  - **LTE + WiMAX** — When connecting to 4G, connection can be established to either 4G WiMAX or 4G LTE; if both are available, 4G LTE is used (unless the 4G WiMAX signal is significantly better than the 4G LTE signal).

  - **LTE Only** — When connecting to 4G, connection can be established only to 4G LTE.

  - **WiMAX Only** — When connecting to 4G, connection can be established only to 4G WiMAX.

- **Connect Automatically** — You can set your device to connect to the network when the device powers on. To prevent this from happening when you're roaming, also select **Disable when roaming**.

- **Failover Wait-time** — This setting specifies how long the device should wait, after it loses the connection with the preferred network, before it attempts to connect to the other network (not available if **WAN Mode** is "3G Only" or "4G Only").

- **Switchback Wait-time** — This setting specifies how long the device should wait, when the less-preferred network is connected and the preferred network becomes available, before switching to the preferred network (not available if **WAN Mode** is "3G Only" or "4G Only").

- **Update 3G PRL** — You can check whether an updated PRL is available.

  The PRL (Preferred Roaming List) is an account configuration item set by your service provider. It controls the radio channels and network carrier used by the 3G modem. An updated PRL may improve your 3G network service.

Note: A 3G connection to the Internet won't be available until the update is complete. (The 4G connection won't be affected.)

- **Update 3G Profile** — You can check whether an updated profile for your 3G connection is available. An updated profile may improve your 3G network service.

- **Active IP Addresses** — These are the IP addresses of the 4G LTE connection.

- **Channel UL** — This is the channel that is used to upload data to the 4G LTE network.

- **Channel DL** — This is the channel that is used to download data from the 4G LTE network.

- **Configure APN** — Click the link to display the APN Settings window. You will be prompted to enter the Service Programming Code (SPC). (If you don't know your SPC, contact Sprint.)

- **Channel List** — These are the channels used by the 4G LTE radio. Enter two numbers, separated by a comma, only if instructed by a Sprint representative, and then click the Save button. (When prompted, enter the MSL [Master Subsidy Lock].)

WAN Tab: 3G Panel

From the **3G** panel of the **WAN** tab you can view various 3G information.

1. Log in to the home page.

2. Click **Advanced settings** (   ).

3. Click **WAN > 3G**.

From this window, you can view this information:

- **Connection Status** — This field reflects the status of the 3G connection: connected, not connected, or dormant.

  Dormant means a connection is established, but no data is being transferred.

- **Service Type** — This is the network that is currently being used for your data connection (1xRTT, EVDO, or EVDO Rev. A).

- **Coverage Type** — This is a list of the types of 3G networks that are available. The **RSSI** and **Ec/Io** for each type are shown.

  RSSI reflects the signal strength of the network.

  Ec/Io is a dimensionless ratio of the average power of a channel, typically the pilot channel, to the total signal power.

- **MDN** (Mobile Directory Number) — This is a 10-digit phone number.

- **SID** (System ID) — The System ID identifies your home network area and is used in conjunction with your phone number to determine if you are "home" or "roaming."

- **MSID** (Mobile Station ID) — Also known as IMSI (International Mobile Station Identity), the MSID is an identifier of a device on the 3G network.

- **NAI** (Network Access Identifier) — This is your User ID for accessing the 3G network.

- **DRC Cover** — Technical support staff may request this value from you.

- **PN 1xRTT** — Technical support staff may request this value from you.

- **DRC Value** — Technical support staff may request this value from you.

- **PN EVDO** — Technical support staff may request this value from you.

- **Channel** — Technical support staff may request this value from you.

- **Roaming Status** — This indicates whether you are home or roaming (outside of Sprint coverage).

- **PRL Version** — The PRL (Preferred Roaming List) is an account configuration item set by your service provider. It controls the radio channels and network carrier used by the 3G modem. An updated PRL may improve your 3G network service.

Tip: You can view the 3G connection status on the "Network Status" LCD information screen. (See LCD Information Screens.)

WAN Tab: 4G Panel

From the **4G** panel of the **WAN** tab you can view various 4G information.

1. Log in to the home page.

2. Click **Advanced settings** ( ).

3. Click **WAN > 4G**.

Note: 4G information is not available if **WAN Mode** is "3G Only or **4G Mode** is "LTE Only."
(**WAN Mode** and **4G Mode** are in **Advanced settings > WAN > Setup**.)

From this window, you can view this 4G information, or perform the following actions:

● **Connection Status** — This field reflects whether you are connected to 4G.

● **Service Type** — This field reflects the 4G service type: 4G, 4G Off, power save mode, or no service.

● **Scan for Private Network** — Click this link if you have been informed that a private network might be available to you. (See "Scan for Private Network" in WAN Tab: 4G Panel.)

● **RSSI** and **CINR**.

RSSI reflects the signal strength of the network.

CINR stands for Carrier to Interference-plus-Noise Ratio and is a measurement of signal effectiveness. For the receiver to decode the carrier signal, the latter must be in an acceptable CINR range.

● **TX Power** — This number indicates the transmitter power. A higher number is better.

● **Center Frequency** — This number indicates the frequency of the 4G channel used for the data connection.

● **NSP-ID** — This number is the ID of the 4G Network Service Provider.

● **NAP-ID** — This number is the ID of the 4G Network Access Provider.

● **BSID** — This number is the ID of the Base Station.

● **Preamble** — This number is the preamble ID of the current base station that the modem is listening to.

● **Realm** — This login address is used for 4G service (user@realm).

● **Certificate Information** — Click the link to display information in a popup window. You will be prompted to enter the Service Programming Code (SPC). (If you don't know your SPC, contact Sprint.)

Scan for Private Network

In some cases, a private network may be available in your location. Such a network may be provided, for example, on a college or university campus (to extend access to campus network resources) or in a large building complex (to improve network service).

To access a private network:

1. Make sure you're logged in to the home page.

2. Make sure that, in **Advanced settings > WAN > Setup**:

   - **4G Preferred** or **4G Only** is selected, and

   - **LTE + WiMAX** or **WiMAX only** is selected.

3. Click **Advanced settings > WAN > 4G**.

4. Select **Scan for Private Network**.

5. If prompted to enter your login information, enter it. (If you don't know this login information, contact the network administrator.)

WAN Tab: 4G LTE Panel

From the **4G LTE** panel of the **WAN** tab you can view various 4G LTE information.

1. Log in to the home page.

2. Click **Advanced settings** ().

3. Click **WAN > 4G LTE**.

Note: 4G LTE information is not available if **WAN Mode** is "3G Only" or **4G Mode** is "WiMAX Only." (**WAN Mode** and **4G Mode** are in **Advanced settings > WAN > Setup**.)

From this window, you can view this 4G LTE information:

- **Connection Status** — This field reflects whether you are connected to 4G LTE.

- **Service Type** — This field reflects the 4G service type: 4G, 4G Off, power save mode, or no service.

- **RSRP** and **RSRQ**.

   RSRP stands for Reference Signal Received Power and reflects the signal strength of the 4G LTE network.

   RSRQ stands for Reference Signal Received Quality and reflects the signal quality of

the 4G LTE network. RSRQ is the ratio between the RSRP and the Received Signal Strength Indicator (RSSI).

- **PLMN ID** — This information identifies the Public Land Mobile Network that is currently serving the Sierra Wireless 4G LTE Tri-Fi Hotspot.

- **IMSI** — The International Mobile Station Identity (IMSI) uniquely identifies a wireless device within the service provider's network. The IMSI is also known as MSID by some service providers.

- **Serving Cell** — This information identifies the 4G LTE cell that is currently serving the Sierra Wireless 4G LTE Tri-Fi Hotspot.

- **Band** — This is the frequency band number for 4G LTE.

- **TX Power** — This number indicates the transmitter power. A higher number is better.

- **Last Error Code** — This is the error code for the most recent 4G-related error.

WAN Tab: GPS Panel

From the **GPS** panel of the **WAN** tab you can enable GPS and configure GPS settings.

1. Log in to the home page.

2. Click **Advanced settings** ( ).

3. Click **WAN > GPS**.

From this window, you can view or adjust these settings, or perform the following actions:

- **Enable GPS** — To use GPS, and to configure other GPS settings, this check box must be selected. If the GPS privacy agreement opens, you must accept it before you can use GPS.

- **GPS Mode** — This setting determines how often the device should obtain a fix.

  - **One-time** — A single fix is used. Use this option if you'll be using your device at the same location.

  - **Continuous** — Fixes are obtained on a regular basis; also known as auto-tracking. Useful for turn-by-turn (TBT) navigation applications, such as driving directions.

- **Get fix now** — This button starts a one-time fix (not displayed if **GPS Mode** is **Continuous** or a GPS session is already in progress). If you change the value from **Continuous** to **One-time**, you must click **Save** before your changes take effect and the fix becomes possible.

- **Mapping Service** — This determines the mapping service (for example, Google Maps or MapQuest) that displays the GPS results (in a separate browser window).

- **Performance Value** — This specifies the amount of time the device should wait for a satellite to be discovered.

  - **Automatic** — The device automatically determines the most appropriate setting to use.

  - **Manual** — In the input field, enter the number of seconds the device should wait for a satellite to be discovered. If this time is exceeded, an error is reported.

- **Accuracy**

  - **Automatic** — The device automatically determines the most appropriate setting to use.

  - **Manual** — In the input field, enter the number of meters to which the data must be accurate. **Note:** If the value is very small (that is, very high accuracy), the fix may fail.

- **Fix Rate** — The smaller the number, the more up-to-date the location tracking will be, at the cost of shorter battery life of the device. This setting is available only if **GPS Mode** is set to **Continuous**.

- **Metric Units** — This specifies whether to use the metric system when displaying the GPS results (for example, the altitude, speed, HEPE).

- **Show GPS Data** or **Hide GPS Data** — This specifies whether the GPS data should be shown in the lower part of the window.

Wi-Fi Tab

From the **Wi-Fi** tab you can configure the Wi-Fi network, including Wi-Fi security.

Wi-Fi Tab: Network Panel

Wi-Fi Tab: Security Panel

Wi-Fi Tab: MAC Filter Panel

Wi-Fi Tab: Network Panel

From the **Network** panel of the **Wi-Fi** tab you can configure general settings of the Wi-Fi network.

1. Log in to the home page.

2. Click **Advanced settings** ().

3. Click **Wi-Fi > Network**.

From this window, you can view or adjust these settings, or perform the following actions:

- **Disable Wi-Fi** — This setting specifies when to turn off the Wi-Fi of the device.

  - **Never** — Select this value if you want to make sure the device is always broadcasting Wi-Fi signals.

  - **Always** — Select this value if you always want to use the device in tethered mode and you want to make sure the device is never broadcasting any Wi-Fi signals. With this option, WPS won't be available. (See Connecting Through WPS.)

  - **When connected to USB** — Only a computer connected through the micro-USB cable to the device will be able to use it. With this option, WPS won't be available. (See Connecting Through WPS.)

- **SSID** — This is the Wi-Fi network name; it identifies your Wi-Fi network and is visible to other Wi-Fi-enabled devices. (See SSID (Wi-Fi Network Name).)

- **Hostname** — This is, in essence, a name you're giving the device. (See Host Name (Device Name) and Displaying the Home Page of the Device.)

- **Link SSID and Hostname** — See Linking the SSID and the Host Name.

- **SSID Broadcast** — If broadcast is enabled, the wireless network is displayed in the list of Wi-Fi networks available in the local area. For increased security, set this field to **Disable**. You will need to give the SSID to the people who will be accessing your network; WPS won't be available.

- **Max Number of Users** — You can limit the number of Wi-Fi users (maximum of eight) that can connect to the device. A smaller number improves performance and security.

- **Battery or USB Powered** (power settings)

  - **Short Range** — This setting improves battery life, at the cost of a shorter Wi-Fi range.

  - **Long Range** — This setting allows you to use your wireless devices farther from your Sierra Wireless 4G LTE Tri-Fi Hotspot, at the cost of shorter battery life and the increased possibility of interference with/from other nearby Wi-Fi devices.

- **AC Powered** (power settings)

  - **Short Range** — Choose this setting if you have a designated wireless area and you need to minimize the effect of your network on other networks in the vicinity.

  - **Long Range** — This setting allows you to use your wireless devices farther from your Sierra Wireless 4G LTE Tri-Fi Hotspot but increases the possibility of interference with or from nearby wireless networks.

- **Wi-Fi Channel** — This is the active channel of the Wi-Fi access point. If your network is having performance issues (possibly caused by other Wi-Fi networks in the vicinity using the same channel), try a different Wi-Fi channel.

- **RTS Threshold** — This setting specifies the smallest packet size, in bytes, for which RTS/CTS (Request to Send/Clear to Send) handshaking is used. The recommended value is 2347. Change this value only if you're experiencing inconsistent data flow. Make only minor changes to this value.

- **Fragmentation Threshold** — This setting specifies the largest allowable size, in bytes, for a packet. If the packet is larger than this, it is fragmented into multiple packet before it is transmitted. To prevent poor network performance, it's recommended to keep this value as large as possible (up to 2346).

- **Wi-Fi Power Save Mode** — If this field is set to "On," the Wi-Fi component of the Sierra Wireless 4G LTE Tri-Fi Hotspot enters power save mode, when possible. If your computer tends to lose the Wi-Fi connection and stops responding, set this field to "Off."

- **Wi-Fi Age Out Time** — This is the amount of time of inactivity (no traffic), after which the Sierra Wireless 4G LTE Tri-Fi Hotspot drops the connection to a device.

- **WMM Support** — Wi-Fi Multimedia (WMM) is a standard that defines quality of service (QoS) in Wi-Fi networks. WMM improves the performance of audio, video and voice applications transmitted over Wi-Fi.

- **List of connected devices** — You can display a window that shows connected computers. A table row may show one or both of these icons:

  - —The user of this computer is logged in as administrator.

  - —This computer is connected to the device through the micro-USB cable.

Wi-Fi Tab: Security Panel

From the **Security** panel of the **Wi-Fi** tab you can configure Wi-Fi security.

1. Log in to the home page.

2. Click **Advanced settings** ( ).

3. Click **Wi-Fi > Security**.

From this window, you can set the:

- **Security** — This specifies the security used by Wi-Fi. (See Wi-Fi Security.)

- **Wi-Fi Password** — This password is used to connect to the Wi-Fi network. (See Wi-Fi Password.)

- **Password Reminder** — This feature displays the Wi-Fi password on the LCD of the device. (See "Wi Fi Password Reminder" in Wi-Fi Password.)

- **Basic Rate** — This setting determines the type of wireless devices that can connect to your network.

  - If you're certain that all of the Wi-Fi devices used with your device support 802.11g, then select **802.11g only** (this ensures faster Wi-Fi speeds); otherwise, select **802.11b/g/n compatibility** or **802.11b/g compatibility**.

  - If you change this value to **802.11b/g/n compatibility** and the specified Wi-Fi security type is not supported by this value, the security type may change to WPA/WPA2 Personal.

Wi-Fi Tab: MAC Filter Panel

MAC (Media Access Control) filtering can prevent unauthorized wireless devices from connecting to your network.

The MAC filter is used to grant ("whitelist") or block ("blacklist") wireless devices access to the Wi-Fi, 3G, and 4G networks. Access is based on the MAC address of each wireless device.

MAC filtering increases security of your network. You can give access to your network, based on the MAC address of the wireless devices. This makes it harder for a hacker to use a MAC address to access your network.

To access this panel:

1. Log in to the home page.

2. Click **Advanced settings** (   ).

3. Click **Wi-Fi > MAC Filter**.

From this window, you can:

- Turn off MAC filtering (**MAC Filter Mode** = "No filtering")

- Display a list of computers that are:

  - Allowed to access the network (**MAC Filter Mode** = "Allow all in list")

  - Not allowed to access the network (**MAC Filter Mode** = "Block all in list")

- Add or remove a computer from the lists. (See "Specifying Computers That Can Access the Network" and "Specifying Computers That Are Not Allowed to Access the Network" in Allowing or Denying Computers Access to the Network.)

- Display a list of computers that are currently connected through Wi-Fi (**List of connected devices**). (See Displaying a List of Currently Connected Computers.)

Router Tab Settings

From the **Router** tab you can enable or disable various features, as well as configure their settings.

Basic Panel: General

Basic Panel: UPnP (Universal Plug and Play)

Basic Panel: SPI (Stateful Packet Inspection)

LAN Panel: General

LAN Panel: DHCP

LAN Panel: DNS Mode

Port Forward Panel: General

Port Forward Panel: Enabling Port Forwarding

Port Forward Panel: Enabling Port Forwarding for an Application

Port Forward Panel: Disabling Port Forwarding for an Application

Port Trigger Panel: General

Port Trigger Panel: Enabling Port Triggering

Port Trigger Panel: Enabling Port Triggering for Specified Protocols and Ports

Port Trigger Panel: Removing Ports From the Port Triggering List

DMZ Panel: General

DMZ Panel: Enabling DMZ

DMZ Panel: Configuring DMZ

Resetting the Software to Default Settings: General

Resetting the Software to Default Settings: Using the Reset Button

Resetting the Software to Default Settings: Using the Browser Interface

1. Log in to the home page.

2. Click **Advanced settings** ( ).

3. Click **Router**.

4. Depending on the settings you want to configure, click one of the panels:

   - **Basic**. (See Basic Panel: General.)

   - **LAN**. (See LAN Panel: General.)

   - **Port Forward** — Port forwarding lets you forward incoming traffic to specific ports and devices (per their local IP address) on your network. (See Port Forward Panel: General.)

   - **Port Trigger** — You can set the device to monitor outgoing data on specific port numbers (trigger ports). (See Port Trigger Panel: General.)

   - **DMZ** — You can select one computer to receive all unsolicited incoming connections. (See DMZ Panel: General.)

Basic Panel: General

You can enable or disable various features of the router component of your device.

To access this panel:

1. Log in to the home page.

2. Click **Advanced settings** (   ).

3. Click **Router > Basic**.

From this window, you can enable or disable these features, and perform these actions:

- **USB Tethered Networking** — To prevent an unauthorized user from using the device through the micro-USB cable, set this field to **Disable**. Users will be able to connect only through Wi-Fi and only after they provide the correct Wi-Fi password (if Wi-Fi security is enabled).

  This setting does not affect the ability to charge the Sierra Wireless 4G LTE Tri-Fi Hotspot through the micro-USB cable.

- **Port Forwarding** — Port forwarding lets you forward incoming traffic to specific ports and devices (per their local IP address) on your network. (See Port Forward Panel: General.)

- **Port Triggering** — You can set the device to monitor outgoing data on specific port numbers (trigger ports). (See Port Trigger Panel: General.)

- **DMZ** — You can select one computer to receive all unsolicited incoming connections. (See DMZ Panel: General.)

- **UPnP** (universal plug and play). (See Basic Panel: UPnP (Universal Plug and Play).)

- **SPI** (stateful packet inspection). (See Basic Panel: SPI (Stateful Packet Inspection).)

- **Router Settings Reset**. (See Resetting the Software to Default Settings: Using the Browser Interface.)

Basic Panel: UPnP (Universal Plug and Play)

UPnP provides simple and robust connectivity among consumer electronics, intelligent appliances, and mobile devices from many different vendors. (For more information, see upnp.org.)

Note: If UPnP is enabled, there are potential security risks.

Enabling UPnP

Before you can use UPnP, you must enable it.

1. Log in to the home page.

2. Click **Advanced settings > Router > Basic**.

3. Next to **UPnP**, select **Enable**.

Basic Panel: SPI (Stateful Packet Inspection)

SPI, also known as "dynamic packet filtering," helps to prevent cyber attacks by validating that the traffic passing through a session conforms to the protocol used for this type of session. Packets that are not conforming get rejected.

Enabling SPI

Before you can use SPI, you must enable it.

1. Log in to the home page.

2. Click **Advanced settings > Router > Basic**.

3. Next to **SPI**, select **Enable**.

LAN Panel: General

Configure LAN-related settings of the routing hardware.

1. Log in to the home page.

2. Click **Advanced settings** ( ).

3. Click **Router > LAN**.

From this window, you can view or adjust these settings, or perform the following actions:

- **Router IP Address** — This is the routing hardware's IP address on the LAN.

- **Subnet Mask** — This is the routing hardware's internal LAN subnet mask.

- **Hostname** — This is, in essence, a name you're giving the device. (See Host Name (Device Name).)

- **Link SSID and Hostname** — With this feature you only need to remember one name when selecting the Wi-Fi network, accessing the browser interface, or accessing the microSD card. (See Linking the SSID and the Host Name.)

- **SSID** — This is the name of the Wi-Fi network. (See SSID (Wi-Fi Network Name).)

- **MTU** — This specifies whether optimization is used.

  - **Auto** — Optimization is not used.

  - **Optimized** (recommended setting) — Optimization is used; this may improve data transmission.

  - **Manual** — Optimization is used; this may improve data transmission. After selecting the radio button, enter the value to use (1200–1500).

- **DHCP Server** — This field enables DHCP.

Note: The following settings are displayed only when DHCP is enabled.

- **DHCP IP Address Range** — This specifies the starting and ending address of the range of IP addresses available for the device to dynamically (that is, not permanently) assign to computers connected to it.

- **DHCP Lease Time** — This is the amount of time, in minutes, a computer can use its assigned IP address before it is required to renew the lease. After this time is up, the computer is automatically assigned a new dynamic IP address.

  Enter a number between 2 and 10080.

- **Max DHCP Clients** — This is the number of DHCP addresses that can be assigned and active at one time. It's recommended you set this to a number greater than the number of Wi-Fi users.

- **DNS Mode** — This specifies how the DNS servers (that the DHCP clients are to communicate with) are obtained.

  - **Auto** — The DNS server specified by Sprint is used. **DNS Relay** is enabled by default.

- **Manual** — The routing hardware assigns DHCP clients the DNS servers specified in the **Manual DNS Server #1** and **#2** fields.
  Use this option to access a DNS server that provides customized addressing or if you have a local DNS server on your network.
  If **DNS Relay** is disabled, the routing hardware rejects DNS requests targeting the internal DNS proxy.

- **Manual DNS Server #1** and **#2** — These are the static IP addresses to use for the DNS servers (if **DNS Mode** is Manual); available only if **DNS Mode** is Manual.

- **DNS Relay** — If enabled, and if **DNS Mode** (see above) is Manual, the routing hardware assigns DHCP clients the DNS servers specified in the **Manual DNS Server #1** and **#2** fields.

  If **DNS Relay** is set to Disable, the routing hardware rejects DNS requests targeting the internal DNS proxy.

  The **DNS Relay** field is configurable and displayed only if **DNS Mode** is Manual. If **DNS Mode** is Auto, DNS Relay is enabled by default.

- **DHCP Static IP Assignment List** — You can assign a permanent IP address to a MAC address, and view the static IP assignment list. (See "DHCP Static IP Assignment List" in LAN Panel: DHCP.)

LAN Panel: DHCP

DHCP (Dynamic Host Control Protocol) automatically assigns an IP address to each device on the network and manages other network configuration information for devices connected to your network. You do not need to manually configure the IP address on each device that's on your network.

The assigned IP addresses are not permanent (as opposed to when using static IP).

Most ISPs (Internet Service Providers) use DHCP.

Normally, you should enable DHCP, in which case you must configure each device on the network with one of the following:

- TCP/IP settings set to "Obtain an IP address automatically."

- TCP/IP bound to the Ethernet connection with DHCP.

If DHCP is disabled, you must configure each device on the network with:

- Fixed (permanent/static) IP address.

- DNS server addresses (provided by Sprint).

Enabling DHCP

1. Log in to the home page.

2. Click **Advanced settings > Router > LAN**.

3. Next to **DHCP Server**, select **Enable**.

Configuring DHCP

To configure DHCP settings, DHCP must be enabled (**Advanced settings > Router > LAN > DHCP Server**).

You can set the following DHCP settings in **Advanced settings > Router > LAN**:

- **DHCP IP Address Range** — This is the starting and ending address of the range of IP addresses available for the device to dynamically (that is, not permanently) assign to computers connected to it.

  The start address must be 192.168.0.10 or above.

  The ending address must be 192.168.0.50 or below.

- **DHCP Lease Time** — This is the amount of time, in minutes, a computer can use its assigned IP address before it is required to renew the lease. After this time is up, the computer is automatically assigned a new dynamic IP address.

  Enter a number between 2 and 10080.

- **Max DHCP Clients** — This is the number of DHCP addresses that can be assigned and active at one time. It's recommended you set this to a number greater than the number of Wi-Fi users.

- **DNS Mode** — This specifies how the DNS servers (that the DHCP clients are to communicate with) are obtained. (See LAN Panel: DNS Mode.)

- **DHCP Static IP Assignment List** — You can assign a permanent (static) IP address to a device on your network, and view the static IP assignment list. (See "DHCP Static IP Assignment List", below.)

DHCP Static IP Assignment List

With DHCP, IP addresses are assigned dynamically; devices typically don't have a permanent IP address.

However, in some cases you might want to assign a static (permanent) IP address to a device, while still using DHCP for the rest of the devices on your network. This is also known as "DHCP

reservation." You might want to do this with, for example, a Web server, FTP server, or media server.

Viewing the Static IP Assignment List

1. Log in to the home page.

2. Click **Advanced settings > Router > LAN**.

3. Make sure DHCP is enabled (**DHCP Server**).

4. Click **DHCP Static IP Assignment List**.

Assigning an IP Address Based on a MAC Address

1. Follow the above steps to display the DHCP Static IP Assignment List window.

2. In the **Hostname** field, enter a meaningful description of the device.

3. In the **MAC Address** field, enter the MAC address of the device. (If you don't know this address, see Finding the MAC Address.)

4. In the **IP Address** field, enter the IP address you want to assign to the device.

5. Select the **Enable** check box to have the device use the designated IP address.

6. Click **Add**.

7. Click **Save**.

Removing an IP Address Based on a MAC Address

1. Click **DHCP Static IP Assignment List** on the **LAN** panel of the **Router** tab.

2. To keep the device information in the list (in case you want to re-enable DHCP for this MAC address later on), clear the **Enable** check box.

   — or —

   To remove the device from the list:

   - Click the row that you want to remove. A row of buttons (**Delete**, **OK**, **Cancel**) appears.

   - Click **Delete**.

LAN Panel: DNS Mode

The **DNS Mode** setting specifies how the DNS servers (that the DHCP clients are to communicate with) are obtained.

1. Log in to the home page.

2. Click **Advanced settings** ( ).

3. Click **Router > LAN**.

4. Set **DNS Mode** to one of the following:

   ▪ **Auto** — The DNS server specified by Sprint is used. **DNS Relay** is enabled by default.

   ▪ **Manual** — The routing hardware assigns DHCP clients the DNS servers specified in the **Manual DNS Server #1** and **#2** fields.
   Use this option to access a DNS server that provides customized addressing or if you have a local DNS server on your network.
   If **DNS Relay** is disabled, the routing hardware rejects DNS requests targeting the internal DNS proxy.

For information on DNS Relay, see LAN Panel: General.

Port Forward Panel: General

Port forwarding lets you forward incoming traffic to specific ports and devices (per their local IP address) on your network. (Normally, incoming traffic [from the Internet] is blocked.)

For example, you can configure port forwarding so that:

● You can access your Remote Desktop from the Internet (by specifying the WAN [public] IP address that the device is using).

● Internet users can access a Web, FTP, or email server, or gaming or Internet application hosted by your computer.

Note: Port forwarding creates a security risk. When not required, port forwarding should be disabled.

Note: Port forwarding does not apply to normal browsing, file downloading, running most online games or other applications hosted on the Internet. (Some online games require port forwarding.)

Before you can use or configure port forwarding, you must enable it, as explained in Port Forward Panel: Enabling Port Forwarding.

From the **Port Forward** panel of the **Router** tab of the **Advanced Settings** window, you can:

● Enable port forwarding for an application. (See Port Forward Panel: Enabling Port Forwarding for an Application.)

- Remove an application from the port forwarding list. (See Port Forward Panel: Disabling Port Forwarding for an Application.)

Port Forward Panel: Enabling Port Forwarding

Before you can use or configure Port Forwarding, you must enable it.

1. Log in to the home page.

2. Click **Advanced settings > Router > Basic**.

3. Next to **Port Forwarding**, select **Enable**.

4. Click **Save**.

Port Forward Panel: Enabling Port Forwarding for an Application

You can enable port forwarding for certain application types.

1. Make sure you've enabled port forwarding. (See Port Forward Panel: Enabling Port Forwarding.)

2. Click **Advanced settings > Router > Port Forward**.

3. In the last row of the table, click the **Application** field, and select the application type from the list.

   The values for **Start** and **End** ports are automatically filled in.

4. If necessary, change the range of port numbers associated with the application. Traffic will be allowed (not blocked) if its destination port number is in the specified range.

   - In the **Start** field, enter the number that starts the port range.

   - In the **End** field, enter the number that ends the port range.
     If the range consists of only one port, enter the number that you entered in the **Start** field.

5. In the **Protocol** list, click the protocol(s) used for this application (TCP, UDP, or both).

6. In the **IP Address** field, enter the IP address of the server to be accessed.

7. Make sure **Enable** is selected.

8. Click **Add**.

9. Click **Save**.

Port Forward Panel: Disabling Port Forwarding for an Application

You can disable port forwarding for certain application types.

1. Make sure you've enabled port forwarding. (See Port Forward Panel: Enabling Port Forwarding.)

2. Click **Advanced settings > Router > Port Forward**.

3. To keep the application in the list (in case you want to re-enable port forwarding later on), clear the **Enable** check box.

   — or —

   To remove the application from the list:

   ▪ Click the row that you want to remove. A row of buttons (**Delete**, **OK**, **Cancel**) appears.

   ▪ Click **Delete**.

Port Trigger Panel: General

Some applications require multiple ports open for communication, many of which may be initiated by a computer on the WAN. Examples of this include video conferencing, VoIP (Internet telephony), and Internet gaming.

With port triggering, the device monitors outgoing data on specific port numbers (trigger ports).

The device keeps track of the IP address of the computer that sends data on these trigger ports, so that when incoming data on the forward ports arrives, the device sends the incoming data to the same computer.

Before you can use or configure port triggering, you must enable it, as explained in Port Trigger Panel: Enabling Port Triggering.

From the **Port Trigger** panel of the **Router** tab of the **Advanced Settings** window, you can:

● Enable port triggering for specified protocols and ports. (See Port Trigger Panel: Enabling Port Triggering for Specified Protocols and Ports.)

● Remove protocols and ports from the port triggering list. (See Port Trigger Panel: Removing Ports From the Port Triggering List.)

Port Trigger Panel: Enabling Port Triggering

Before you can use or configure Port Triggering, you must enable it.

1. Log in to the home page.

2. Click **Advanced settings > Router > Basic**.

3. Next to **Port Triggering**, select **Enable**.

Port Trigger Panel: Enabling Port Triggering for Specified Protocols and Ports

After you've enabled port triggering, you can enable it for specified protocols and ports.

1. Make sure you've enabled port triggering. (See Port Trigger Panel: Enabling Port Triggering.)

2. Click **Advanced settings > Router > Port Trigger**.

3. In the last row of the table, in the first **Protocol** list, click the protocol(s) used by the application for outgoing traffic (to the Internet, sent through the trigger ports).

4. In the **Trigger Ports** field, enter the port number(s) used to determine that the application is in use. (That is, specify the port number or range of port numbers that the application uses for outgoing traffic. Check the user documentation for the application.)

   To specify a range of port numbers, separate the start and end port number with a hyphen.

5. In the second **Protocol** list, click the protocol(s) used by the application for incoming traffic (from the Internet).

6. In the **Forward Ports** field, enter the ports to forward to the computer that triggered the rule. (That is, specify the port number or range of port numbers that the application uses for incoming traffic. Check the user documentation for the application.)

7. To specify a range of port numbers, separate the start and end port number with a hyphen.

8. Make sure **Enable** is selected.

9. Click **Add**.

10. Click **Save**.

Port Trigger Panel: Removing Ports From the Port Triggering List

If you no longer require port triggering on certain ports, you can remove the ports from the port triggering list.

1. Make sure you've enabled port triggering. (See Port Trigger Panel: Enabling Port Triggering.)

2. Click **Advanced settings > Router > Port Trigger**.

3. To keep the entry in the list (in case you want to re-enable this entry later on), clear the **Enable** check box.

— or —

To remove the entry from the list:

- Click the row that you want to remove. A row of buttons (**Delete**, **OK**, **Cancel**) appears.

- Click **Delete**.

DMZ Panel: General

You can select one computer to receive all unsolicited incoming connections.

The IP address of the DMZ ("demilitarized zone") is the default recipient of incoming packets (from the Internet) that are not handled by port forwarding rules, port triggering rules, or NAT'd connections:

1. If port forwarding, port triggering, or both are enabled, incoming traffic is routed according to the port forwarding rules, port triggering rules, or NAT'd connections.

2. If incoming traffic was not routed as a result of the above:

   - If DMZ is enabled, then incoming traffic is routed to the computer that uses the IP address specified by the DMZ settings.

   - If DMZ is not enabled, the incoming traffic is blocked.

Note: Putting a computer in the DMZ opens all the ports of that computer, and exposes that computer to various security risks. Use this option only as a last resort — if possible, use other options instead (for example, port forwarding or port triggering).

DMZ Panel: Enabling DMZ

Before you can use or configure DMZ, you must enable it.

1. Log in to the home page.

2. Click **Advanced settings > Router > Basic**.

3. Next to **DMZ**, select **Enable**.

4. Click **Save**.

DMZ Panel: Configuring DMZ

Specify which computer is to receive all unsolicited incoming connections.

1. Make sure you've enabled DMZ. (See DMZ Panel: Enabling DMZ.)

2. Click **Advanced settings > Router > DMZ**.

3. Specify the computer that you want exposed to the Internet: in the **Destination IP Address** field, enter the IP address of the computer. (If you don't know how to find the IP address, see Finding the IP Address.)

4. In the **Source IP Address** section, specify what incoming traffic (not handled by port forwarding, port triggering, or NAT) to forward to this computer.

   To forward all incoming traffic, click **Any**.

   — or —

   To forward incoming traffic from certain IP addresses:

   ▪ Click **Restriction**.

   ▪ In the two additional fields that are displayed, enter the start and end IP addresses of a range.

5. Using the DHCP Static IP Assignment List, assign an IP address based on the MAC address of the computer that is in the DMZ. (See "Assigning an IP Address Based on a MAC Address" in LAN Panel: DHCP.)

   — or —

   On the computer that is in the DMZ, disable DHCP, and manually assign the IP address, gateway, and DNS server.

Resetting the Software to Default Setting: General

In some cases you will need to reset the software to default settings.

WARNING: If you reset the software to default settings:
• You must go through the device setup, as if you've just purchased the device. (See Device Setup.)
• Any changes you've made to the settings are lost.
Your 3G and 4G account information is not affected; after reset, the device remains provisioned for service.

You'll need to reset the software to default settings if:

● You've forgotten the administrator password.

● You've changed the DHCP settings such that the device is inoperable (for example, there's no communication with the device).

You have two options to initiate the reset:

- Through the software. (See Resetting the Software to Default Settings: Using the Browser Interface.)

- Through the reset button on the device. (See Resetting the Software to Default Settings: Using the Reset Button.)

Resetting the Software to Default Settings: Using the Reset Button

You can reset the software to default settings from the device itself, without having to use the browser interface.

1. Using slight finger pressure, slide the battery compartment cover towards you to remove it.
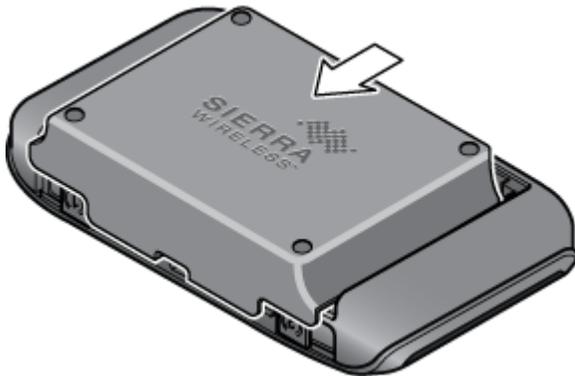
2. Locate the small hole labeled "RESET" (near the micro-USB port). The reset button is inside this hole.

Reset button
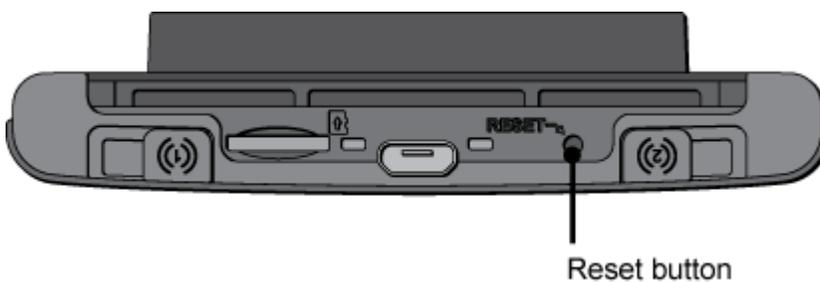
3. Insert a thin object (for example, the end of a paper clip) into the hole, and press down **for five or more seconds**.

4. Replace the battery compartment cover.

5. Check the device LCD. If it displays "Reset to factory defaults? Press ⏻ to accept," press the power button [⏻] on the device.

6. Follow the instructions on the device LCD.

Resetting the Software to Default Settings: Using the Browser Interface

It's easy to reset the software to default settings through the browser interface.

WARNING: If you reset the software to default settings:
  • You must go through the device setup, as if you've just purchased the device. (See Device Setup.)
  • Any changes you've made to the settings are lost.
  Your 3G and 4G account information is not affected; after reset, the device remains provisioned for service.

1. Log in to the home page.

2. Click **Advanced settings > Router > Basic**.

3. Click **Router Settings Reset**.

4. Check the device LCD. If it displays "Reset to factory defaults? Press ⏻ to accept," press the power button [⏻] on the device.

5. Follow the instructions on the device LCD.

Exporting and Importing Settings

These features let you, for example, save the current configuration, make some changes and test them, and then restore the original configuration.

Exporting Settings

Exporting Settings

Settings include configuration information for the device, network, and browser interface.

You can, for example, save the current configuration, then make some changes and test them. You can then use the **Import** button to restore (load) the saved configuration.

To export the settings to a text file:

1. Log in to the home page.

2. Click **Advanced settings > Device > Basic**.

3. Click **Export**.

Importing Settings

This feature lets you restore a saved configuration.

1. Log in to the home page.

2. Click **Advanced settings > Device > Basic**.

3. Browse to and click the file with the saved settings.

4. Click **Import**.

Note: Your device may reset, and you may need to reconnect to Wi-Fi and the Internet. (See How Do I Connect to Wi-Fi? and Launching Your Network Connection.)

Device Logs

Learn how to configure settings related to the logging of events, export and clear logs.

Connection History

The connection history shows the time of connections to and disconnections from the Internet.

Note: The connection history does not log the amount of data transferred. In the Internet Connection Information window, you can view information on the current billing cycle and lifetime of the device. (See Internet Connection Information.)

Enabling and Disabling Logging of Connects and Disconnects

1. Log in to the home page.

2. Click **Advanced settings > Device > Log**.

3. In the **Connect/Disconnect** section, select **Enable** or **Disable**.

4. Click **Save**.

Exporting the Connection History

1. Log in to the home page.

2. Click **Advanced settings > Device > Log**.

3. Make sure **Connect/Disconnect** is set to **Enable**.

4. Click **Export**.

Clearing the Connection History

1. Log in to the home page.

2. Click **Advanced settings > Device > Log**.

3. In the **Connect/disconnect** section, click **Clear log**.

System Events

You can enable or disable, as a group, the logging of the several kinds of system events.

- Software update available

- Network update available

- Primary WAN failover

- Primary WAN switchback

- Unexpected data connection loss

- Changes to miscellaneous settings

The following system events are always logged:

- Intrusion alerts

- Unexpected power loss

- Critical battery

- Critical temperature

- Routing hardware settings reset

- Firmware update

Enabling and Disabling Logging of System Events

1. Log in to the home page.

2. Click **Advanced settings > Device > Log**.

3. In the **Verbose System Event Logging** section, select **Enable** or **Disable**.

4. Click **Save**.

Note: Certain events are always logged. (See System Events.)

Exporting System Events

1. Log in to the home page.

2. Click **Advanced settings > Device > Log**.

3. Make sure **Verbose System Event Logging** is set to **Enable**.

4. Click **Export**.

Clearing the System Events Log

1. Log in to the home page.

2. Click **Advanced settings > Device > Log**.

3. Make sure **Verbose System Event Logging** is set to **Enable**.

4. Click **Clear log**.

Setting the Method Used for Time Acquisition

Time information is stored in the connection history log and system events log.

To set the method used for obtaining the time:

1. Log in to the home page.

2. Click **Advanced settings > Device > Log**.

3. Select the **3G** or the **NTP** check box.

   - **3G** — Time information is obtained from the 3G (CDMA) network; this is more accurate than NTP, but requires 3G coverage.

- **NTP** — The device's clock is synchronized to a Network Time Protocol server on the Internet; not as accurate as when using the **3G** setting, but doesn't require 3G coverage. Use this setting if you have 4G or 4G LTE but no 3G coverage.

Configuring the Wi-Fi Network

Learn how to configure the Wi-Fi network, including its security and range.

SSID (Wi-Fi Network Name)

Wi-Fi Security

Host Name (Device Name)

Setting the Maximum Number of Wi-Fi Users

Wi-Fi Channel

Disabling Wi-Fi When Connected Through USB

You can configure basic settings of the Wi-Fi network through the setup pages. To display the setup pages:

1. Make sure you're logged in to the home page.

2. Click **Admin Setup** ( ).

For more information, see "Changing the Password and Settings" in Device Setup.

You can configure basic and advanced settings of the Wi-Fi network through the **Advanced Settings** window. To display the **Advanced Settings** window:

1. Log in to the home page.

2. Click **Advanced settings** ( ).

3. Click **Wi-Fi > Network**.

For more information, see Wi-Fi Tab: Network Panel.

See also:

- Disabling Wi-Fi When Connected Through USB.

- Battery and USB Power Settings

- AC Power Settings

SSID (Wi-Fi Network Name)

The SSID identifies your Wi-Fi network and is visible to other Wi-Fi-enabled devices. It appears on your device's LCD screen; if more than one Sierra Wireless 4G LTE Tri-Fi Hotspot is available, you can use this name to tell the devices apart.

You can display the home page by typing the SSID in your Web browser (if **Link SSID and Hostname** is selected. (See Linking the SSID and the Host Name.)

You should make the SSID unique and change it on a regular basis for optimal security.

To change the SSID:

1. Log in to the home page.

2. Click **Advanced settings > Wi-Fi > Network**.

3. In the **SSID** field, enter the new name.

   If the SSID field is not available, Link SSID and Hostname is enabled. You must either edit Hostname (and the SSID will get the same value), or disable Link SSID and Hostname and edit the SSID.

4. Click **Save**.

5. Follow the onscreen instructions to reconnect to Wi-Fi. (See How Do I Connect to Wi-Fi?)

Note: If you're sharing your connection, other users must also reconnect to Wi-Fi; provide them with the new SSID.

Note: For security reasons, it's recommended you disable SSID Broadcast. (See Wi-Fi Tab: Network Panel.) WPS won't be available. (See Connecting Through WPS .)

Linking the SSID and the Host Name

You may find linking the **SSID** and the **Hostname** to be a handy feature.

If you link the **SSID** (Wi-Fi network name) and the **Hostname** (name of your device):

● The SSID becomes whatever the Hostname is (you cannot change the SSID — only the Hostname).

● You only need to remember one name when selecting the Wi-Fi network, accessing the browser interface, or accessing the microSD card.

To link the SSID and the Hostname:

1. Log in to the home page.

2. Click **Advanced settings** ( ).

3. Click **Wi-Fi > Network** or **Router > LAN**.

4. Select the **Link SSID and Hostname** check box.

   The **SSID** field gets the value of **Hostname** and becomes unavailable (grayed out).

5. Click **Save**.

   The device resets, after which you must reconnect to Wi-Fi. (See How Do I Connect to Wi-Fi?

Wi-Fi Security

Learn about the various Wi-Fi security options available to you.

By default, Wi-Fi security is enabled for your device and the Wi-Fi network.

Note: All the devices used with the Sierra Wireless 4G LTE Tri-Fi Hotspot must support the selected security type.

Note: WPS is available only if you select either a WPA2 Personal option (including **WPA/WPA2 Personal**) or (not recommended) no security. (See Connecting Through WPS.)

To change the security used by Wi-Fi:

1. Log in to the home page.

2. Click **Advanced settings > Wi-Fi > Security**.

3. Select one of the following options. Note that not all options may be displayed, depending on the **Basic Rate** setting.

   - **None** — No security is used (no password is required to access the Wi-Fi network); this setting is not recommended. Anyone may access your device and use your Internet connection. (You are responsible for payment for data usage fees.)

   - **WEP 64 Bit - Shared** — This option provides security, but it's relatively weak. This option works with older and newer Wi-Fi devices, and is recommended only if any of your devices don't support WPA or WPA2.

     Shared WEP uses the same key for encryption and authentication; some consider shared WEP to be less secure than open WEP.

   - **WEP 128 Bit - Shared** — This option provides security, but it's relatively weak (but stronger than **WEP 64 Bit - Shared**). This option works with older and newer Wi-Fi

devices, and is recommended only if any of your devices don't support WPA or WPA2.

Shared WEP uses the same key for encryption and authentication; some consider shared WEP to be less secure than open WEP.

- **WEP 64 Bit - Open** — This option provides security, but it's relatively weak. This option works with older and newer Wi-Fi devices, and is recommended only if any of your devices don't support WPA or WPA2.

  Open WEP uses the key for encryption, but not for authentication.

- **WEP 128 Bit - Open** — This option provides security, but it's relatively weak (but stronger than **WEP 64 Bit - Open**). This option works with older and newer Wi-Fi devices, and is recommended only if any of your devices don't support WPA or WPA2.

  Open WEP uses the key for encryption, but not for authentication.

- **WPA-Personal TKIP** — This is a strong security standard that is supported by most Wi-Fi devices.

- **WPA-Personal TKIP/AES** — This is a strong security standard that is supported by most Wi-Fi devices.

- **WPA2-Personal AES** — This is a stronger, newer security standard that is limited to newer Wi-Fi devices.

- **WPA2-Personal TKIP/AES** — This is a stronger, newer security standard that is limited to newer Wi-Fi devices.

- **WPA/WPA2 Personal** (recommended setting if any of your devices are more than two years old) — Wi-Fi devices that use either WPA or WPA2 can connect to the Sierra Wireless 4G LTE Tri-Fi Hotspot. Supported by most Wi-Fi devices.

4. Click **Save**.

The option you select determines the Wi-Fi security used and also the maximum length of the Wi-Fi password.

Wi-Fi Password

If Wi-Fi security is enabled, a Wi-Fi password is required to connect to the Wi-Fi network.

To make your password more secure:

- Use letters and numbers

- Use special characters (for example, @)

● Use both uppercase and lowercase letters

To change the Wi-Fi password:

1. Log in to the home page.

2. Click **Advanced settings > Wi-Fi > Security**.

3. In the **Wi-Fi Password** field, type the password; the maximum length depends on the Wi-Fi security type that you've selected.

   ▪ **None** — No security is used (no password is required to access the Wi-Fi network); this setting is not recommended. Anyone may access your device and use your Internet connection. (You are responsible for payment for data usage fees.)

   ▪ **WEP 64 bit - Shared** — The password must be 5 ASCII characters.

   ▪ **WEP 128 bit - Shared** — The password must be 13 ASCII characters.

   ▪ **WEP 64 bit - Open** — The password must be 5 ASCII characters.

   ▪ **WEP 128 bit - Open** — The password must be 13 ASCII characters.

   ▪ **WPA-Personal TKIP** — The password must be 8 to 63 ASCII characters.

   ▪ **WPA-Personal TKIP/AES** — The password must be 8 to 63 ASCII characters.

   ▪ **WPA2-Personal AES** — The password must be 8 to 63 ASCII characters.

   ▪ **WPA2-Personal TKIP/AES** — The password must be 8 to 63 ASCII characters.

   ▪ **WPA/WPA2 Personal** — The password must be 8 to 63 ASCII characters.

4. Click **Save**.

Wi-Fi Password Reminder

To display the Wi-Fi password on the LCD of the device when the Wi-Fi Password Reminder feature is enabled:

1. If the LCD is dark (no text or icons are displayed):

   ▪ Make sure the LCD is enabled. (See Turning the LCD On or Off.)

   ▪ Briefly press the power button [⏻] on the device.

2. Press the navigation button [—] on the device.

The information is displayed for approximately 20 seconds. To clear the information before that, briefly press the power button [⏻] on the device.

Enabling the Wi-Fi Password Reminder

1. Log in to the home page.

2. Click **Advanced settings > Wi-Fi > Security**.

3. In the **Password Reminder** section, select **On**.

4. Click **Save**.

Allowing or Denying Computers Access to the Network

MAC (Media Access Control) filtering can prevent unauthorized wireless devices from connecting to your network.

The MAC filter is used to grant ("whitelist") or block ("blacklist") wireless devices access to the Wi-Fi, 3G, and 4G networks. Access is based on the MAC address of each wireless device.

In the **MAC Filter** panel of the **Wi-Fi** tab (**Advanced Settings > Wi-Fi > MAC Filter**), you can choose one of three modes:

- **No filtering** — All computers are allowed to access the network.

- **Allow all in list** — Only computers that are in this list are allowed to access the network.

- **Block all in list** — All computers are allowed to access the network, unless they're in this list.

In any case, a user still needs to provide the correct Wi-Fi password to access the network.

Specifying Computers That Can Access the Network

1. Log in to the home page.

2. Click **Advanced settings > Wi-Fi > MAC Filter**.

3. In the **MAC Filter Mode** list, click **Allow all in list**.

4. Do one of the following:

   - If the computer you want to allow access is currently connected to the Sierra Wireless 4G LTE Tri-Fi Hotspot, click **List of connected devices**. In the row for the computer, click **Add**.

     — or —

   - Click **Add**. In the **MAC Address** field, enter the MAC address of the computer you're adding to the list. (If you don't know this address, see Finding the MAC Address.) In the **Name** field, enter a name, for example "Amy's PC."

5. Repeat step 4 for each computer for which you want to allow access.

Specifying Computers That Are Not Allowed to Access the Network

1. Log in to the home page.

2. Click **Advanced settings > Wi-Fi > MAC Filter**.

3. In the **MAC Filter Mode** list, click **Block all in list**.

4. Determine and block an undesired user of your network.

   - Click the **List of connected devices** link.

   - If you see a device you don't recognize, you can compare its MAC address to the MAC address of each of the devices on your network.

     To determine the MAC address of each device you have, see Finding the MAC Address. If none of your devices have this MAC address, that device might be an intruder.

   - In the row for the device you want to block, click **Add**.

5. For each computer you want to block, repeat step 4.

Tip: The Wi-Fi Users window has a **Block** check box, available for each currently connected user. (See Wi-Fi Users Information and Settings.)

Removing a Computer From the Allowed or Disallowed Lists

1. Log in to the home page.

2. Click **Advanced settings > Wi-Fi > MAC Filter**.

3. In the **MAC Filter Mode** list, click either **Allow all in list** or **Block all in list**.

4. Click the row that you want to remove. A row of buttons (**Delete**, **OK**, **Cancel**) appears.

5. Click **Delete**.

Displaying a List of Currently Connected Computers

To detect a potential intruder, you may want to display a list of currently connected computers.

1. Make sure you're logged in to the home page.

2. Click the [WiFi] icon to display the Wi-Fi Users window.

   — or —

Click **Advanced settings > Wi-Fi > Mac Filter**, and click **List of connected devices**.

A row displays the icon if the user is logged in as administrator.

Host Name (Device Name)

The host name is, in essence, a name you're giving the device.

The host name is shown on your device's LCD screen; if more than one device is available, you can use this name to tell the devices apart. (See Linking the SSID and the Host Name.)

This name is also used when you type a command to access the:

- Home page. (See Displaying the Home Page of the Device.)

- microSD card. (See Accessing the microSD Card.)

To change the host name:

1. Log in to the home page.

2. Click **Advanced settings** ( ).

3. Click **Wi-Fi > Network** or **Router > LAN**.

4. In the Hostname field, enter a name for your device.

    The name must be 1–15 ASCII characters. Valid characters are:

    ▪ a-z

    ▪ A-Z

    ▪ 0-9. Note that the host name cannot be all numbers.

    ▪ - (hyphen). Note that the host name cannot start or end with a hyphen.

Setting the Maximum Number of Wi-Fi Users

If your network is having performance issues, you might want to decrease the number of Wi-Fi users allowed to connect to the device. To do this:

1. Make sure you're logged in to the home page.

2. Click the icon and, in the Wi-Fi Users window, click a value in the **Max Wi-Fi users** list.

    — or —

Click **Advanced settings > Wi-Fi > Network**, and click a value in the **Max Number of Users** list.

Wi-Fi Channel

The Wi-Fi channel is the active channel of the Wi-Fi access point. If your network is having performance issues (possibly caused by other Wi-Fi networks in the vicinity using the same channel), try a different Wi-Fi channel. To use a different Wi-Fi channel:

1. Log in to the home page.

2. Click **Advanced settings > Wi-Fi > Network**.

3. Click a channel number in the **Wi-Fi Channel** list, or, to have the device automatically determine the channel to use, click **Auto**.

Disabling Wi-Fi When Connected Through USB

You can optionally turn off the device's Wi-Fi when connected via the micro-USB cable.

In this case:

- ● Only a computer that is connected to the device through the micro-USB cable can use the device.

- ● You can prolong the battery life of the device.

- ● The battery charges faster.

- ● WPS won't be available. (See Connecting Through WPS.)

To enable this feature:

1. Make sure you're logged in to the home page.

2. Click the Wi-Fi Users icon (for example,) and set **Disable Wi-Fi** to **When connected to USB**.

    — or —

    Click **Advanced settings > Wi-Fi > Network** and set **Disable Wi-Fi** to **When connected to USB**.

Configuring 3G, 4G, and 4G LTE

Learn about configuring network settings and also resetting the configurations to default settings.

Viewing 3G Activation Information

Resetting the 3G and 4G Configurations to Default Settings.

Resetting the 3G and 4G Radio Configurations to Default Settings

See also:

- WAN Tab: 3G Panel

- WAN Tab: 4G Panel

- WAN Tab: 4G LTE Panel

Viewing 3G Activation Information

You can check whether 3G is activated and view related information.

1. Log in to the home page.

2. Click **Advanced settings** ( ).

3. Click **Device > About**.

The following fields are related to 3G activation:

- **Activation Status** — This field reflects whether 3G is activated.

- **Activation Date** — This is the date that the 3G modem was first activated.

- **Network Operator** — This field shows the carrier that your device was activated with.

Resetting the 3G and 4G Configurations to Default Settings

You may need to reset the 3G and 4G configurations to their default settings.

Note: Reset the configurations only if instructed by a Sprint representative.

Note: After a configuration reset:
• You must go through the device setup (see Device Setup) and 3G activation. (The

latter starts automatically.)

- Any changes you've made to the settings are lost.

1. Log in to the home page.

2. Click **Advanced settings > Device > About**.

3. Click **Reset Device to Factory Defaults**.

4. When prompted, enter the SPC (Service Programming Code). (If you don't know your SPC, contact Sprint.)

To be able to establish a data connection after you've reset the device to factory defaults, you must first:

1. Go through the device setup. (See Device Setup.)

2. Go through 3G activation or, if using 4G, use pay-as-you-go.

Resetting the 3G and 4G Radio Configurations to Default Settings

You may need to reset the 3G and 4G radio configurations to their default settings.

Note: Reset the configurations only if instructed by a Sprint representative.

Note: After a radio configuration reset, you must go through 3G activation, which starts automatically.

1. Log in to the home page.

2. Click **Advanced settings > Device > About**.

3. Click **Reset Radios to Factory Defaults**.

To be able to establish a data connection after you've reset the radios to factory defaults, you must first:

► Go through 3G activation or, if using 4G, use pay-as-you-go.

Location Services and Settings

This section describes how to use and configure location-based navigation.

Sprint Location Services

GPS Settings

Sprint Location Services

Your device offers location-based navigation to help you figure out where you are and get you where you're going.

Requirements for GPS Service

Enabling GPS

Displaying Your Location Information

Viewing Your Current Location in a Web Browser

Performing a Location Search

Requirements for GPS Service

There are a couple of requirements to access GPS services.

- ● You must accept the GPS privacy agreement.

- ● GPS must be enabled.

GPS services may not be available if you are indoors. (You may be able to get a GPS lock if your device is very close to a window.) GPS receivers must be able to lock onto the global positioning satellites to accurately determine position. The number of obstructions present indoors often makes accurate position determination impossible.

Enabling GPS

Before you can access GPS services, you must enable GPS.

1. Make sure you're logged in to the home page.

2. Click the GPS icon (on the left side of the home page) and select **Enable GPS**.

   — or —

   Click **Advanced settings > WAN > GPS** and select **Enable GPS**.

Note: If **Enable GPS** is not available, you must accept the GPS privacy agreement. (See GPS Privacy Agreement.)

3. If the GPS privacy agreement opens, you must read and accept it.

Displaying Your Location Information

You can easily display your location information.

1. Make sure you're logged in to the home page.

2. Make sure GPS is enabled.

3. For best results, minimize the number of obstructions between your device and the GPS satellites.

4. Click the GPS icon on the left side of the home page.

5. In the GPS Information and Settings window, set **GPS Mode** to **One-time**, and click **Get fix now**. (The top part of the window shows your location information.)

Tip: You can also display location information from **Advanced settings > WAN > GPS** — click **Get fix now**. Alternatively, you can view your current location in a Web browser. (See Viewing Your Current Location in a Web Browser.)

Viewing Your Current Location in a Web Browser

You can easily display your current location in a Web browser.

1. Make sure GPS is enabled and you're connected to the 3G or 4G network.

2. For best results, minimize the number of obstructions between your device and the GPS satellites.

3. In the horizontal row of buttons (across the top of the home page), click **Map me** ( ).

Performing a Location Search

You can search for a variety of types of establishments near your current location.

1. Make sure GPS is enabled and you're connected to the 3G or 4G network.

2. In the horizontal row of buttons (across the top of the home page), move the mouse over **Map me** ( ) to display a row of icons:

3. Click one of these icons to search for items of interest, as shown in the following table:

Icon	Click to search for:
	Text (search string) that you enter.
	Electronics-related businesses
	Restaurants
	Local hotels
	Local banks (ATM machines)
	Local gas stations
	Local coffee shops

The results of the search are displayed in a new browser window or tab.

Note: If a window displays "GPS Fix in Progress," please wait while your device obtains a GPS location fix.

Note: When a location fix has been acquired, your Web browser will display the mapping results.

GPS Settings

This section provides an overview of GPS-related items you can change.

Setting the GPS Mode

Setting the GPS Fix Rate

Using Metric Units

Changing Your Mapping Service

Performance Setting: GPS

Accuracy

Basic GPS settings can be changed in the GPS Information and Settings window. (See GPS Information and Settings.)

Additional settings are available at **Advanced settings > WAN > GPS**.

Setting the GPS Mode

GPS mode determines how often the location fix is done.

The location fix can be done:

- Once ("one-time"), or

- Periodically ("continuous") — used, for example, for turn-by-turn (TBT) navigation applications.

To set the GPS mode:

1. Make sure you're logged in to the home page.

2. Click **Advanced settings > WAN > GPS**.

3. Select the **Enable GPS** check box if it is not selected.

4. Select one of the following:

    - **One-time** — A single fix is used. Use this option if you'll be using your device at the same location.

Tip: If you want to get a fix immediately, click **Get fix now**.

    - **Continuous** — Fixes are obtained on a regular basis; also known as auto-tracking. Useful for turn-by-turn (TBT) navigation applications, such as driving directions.

Setting the GPS Fix Rate

The GPS fix rate determines how often GPS fixes are obtained. This option is available only if the fix mode (**GPS Mode**) is set to **Continuous**.

1. Log in to the home page.

2. Click **Advanced settings > WAN > GPS**.

3. Make sure **GPS Mode** is set to **Continuous**.

4. In the **Fix Rate** field, enter a number of seconds between 1 and 999. (The smaller the number, the more up-to-date the location tracking will be, at the cost of shorter battery life of the device.)

Using Metric Units

You can use metric units in the display of location information (for example, speed and altitude).

1. Make sure you're logged in to the home page.

2. Click the GPS icon on the left side of the home page.

3. In the GPS Information and Settings window, select the **Metric** units check box.

Changing Your Mapping Service

You can change the mapping service (for example, Google Maps or MapQuest) that displays the GPS results (in a separate browser window).

1. Make sure you're logged in to the home page.

2. Click the GPS icon ⊕ on the left side of the home page.

3. Click a service in the **Mapping service** list in the GPS Information and Settings window.

Performance Setting: GPS

The performance setting determines the amount of time the device waits for a satellite to be discovered when obtaining GPS information.

1. Log in to the home page.

2. Click **Advanced settings > WAN > GPS**.

3. In the **Performance Value** section, select one of the following:

   - **Automatic** — The device automatically determines the most appropriate setting to use.

   - **Manual** — In the input field, enter the number of seconds the device should wait for a satellite to be discovered. If this time is exceeded, an error is reported.

Accuracy

The accuracy setting determines how accurate the location information is.

1. Log in to the home page.

2. Click **Advanced settings > WAN > GPS**.

3. In the **Accuracy** section, select one of the following:

   - **Automatic** — The device automatically determines the most appropriate setting to use.

   - **Manual** — In the input field, enter the number of meters to which the data must be accurate. **Note:** If the value is very small (that is, very high accuracy), the fix may fail.

Using the microSD Card Slot

Your device is equipped with a microSD (Secure Digital) memory card slot that allows you to store and share images, videos, music, and documents. A microSD memory card (not included) is required.

The device supports microSD cards up to 32 GB.

Note: Using microSD cards larger than 32 GB can cause data loss and damage your device.

Before Using the microSD Card Slot

Inserting a microSD Card

Removing a microSD Card

Accessing the microSD Card.

Before Using the microSD Card Slot

Perform the following steps before using the microSD Card slot.

1. Enable the slot. (See Enabling the microSD Card Slot.)

2. Optionally, enable DLNA Media Server. (See Enabling DLNA Media Server.)

3. Set up access to the slot. (See Setting Up Access to the microSD Card.)

4. Optionally, rename the **microSD Shared Folder Name**. (See microSD Shared Folder Name.)

5. Make sure the microSD card is inserted into the slot.

6. Let other users know how they can access the card. (See Accessing the microSD Card.)

Enabling the microSD Card Slot

Before computers can recognize the microSD card, you must enable the microSD slot on the device.

1. Make sure you're logged in to the home page.

2. In the SD Card Information and Settings window, select **Enable SD Card**. (See microSD Card Information and Settings.)

    — or —

Click **Advanced settings > Device > microSD Card** and set the **SD-Card Slot** field to **Enable**.

Enabling DLNA Media Server

Your Sierra Wireless 4G LTE Tri-Fi Hotspot can serve as a Digital Media Server (DMS), providing content to networked digital media players (DMP) and digital media renderers (DMR). You can, for example, play audio or movie files (stored on the microSD card inserted in your hotspot) on a computer, tablet, mobile phone, or TV that supports DLNA. (**Note:** The software on the device must support the types of files you're trying to play. If you're having problems, check the user documentation of the software.)

Before your devices can play the files, you must enable Digital Media Server on your hotspot.

1. Make sure you're logged in to the home page.

2. In the SD Card Information and Settings window, select **Enable DLNA Media Server**. (See microSD Card Information and Settings.)

When a microSD card is inserted in the hotspot, it is shown in the DMP/DMR's media software, with the same name as the name of your hotspot. If it's not shown in the media software, check that:

● The device and software support DLNA. (For a list of products that support DLNA, see www.dlna.org/consumer-home/look-for-dlna/product-search.)

● DLNA is enabled on the device and in the software. See the user documentation of your device.

Setting Up Access to the microSD Card

If you've enabled access to the microSD card, you must also specify whether a username and password are required to access the card.

1. Make sure you're logged in to the home page.

2. In the SD Card Information and Settings window or from **Advanced settings > Device > microSD Card**, under **Username and Password Security**, select one of the values:

▪ To have no security, select **None**.

Anyone can use the card; no username or password is required.

▪ To allow only the administrator to use the card, select **Administrator Only**.

When prompted for the username (when you try to use the card), enter "admin". For the password, enter the home page login password.

▪ To allow non-administrators to use the card, select **Administrator + Guest**.

3. If you've selected **Administrator + Guest**:

   ▪ Optionally, change the **Set Guest Username** and **Set Guest Password** fields (up to 20 characters each with spaces allowed).

   ▪ Give the guest username and password to people whom you want to allow access to the card.

microSD Shared Folder Name

You can optionally change the name of the folder that the microSD card shows up as (in the file browser program); the default folder name is "shared."

1. Make sure you're logged in to the home page.

2. Click **Advanced settings > Device > MicroSD Card**.

3. In the **microSD Shared Folder Name** field, type the new name. (You can use up to 32 letters, numbers, and spaces in any combination.)

For information on how this folder name is used, see Accessing the microSD Card.

Inserting a microSD Card

Remove the battery compartment cover to insert a compatible microSD card into your device.

1. Using slight finger pressure, slide the battery compartment cover towards you to remove it.
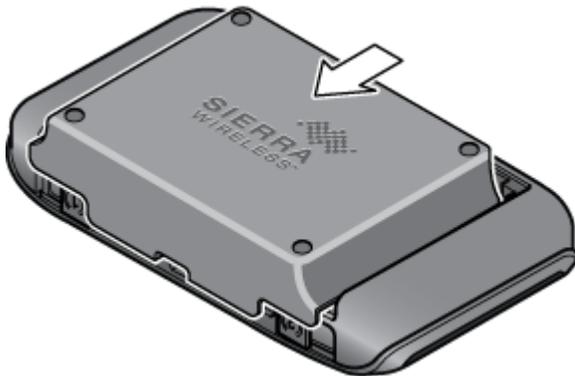
2. Carefully insert the microSD card (label facing up) into the slot on your device (near the micro-USB port), until the microSD card clicks into place.

3. Check the status of the microSD card. (See microSD Card Information and Settings.)

Removing a microSD Card

Before removing your device's microSD card, use the **Safe-Eject SD Card** button.

1. Make sure you and other users have completed any file transfers.

2. In the microSD Card Information and Settings window, click **Safe-Eject SD Card** and wait until a message is displayed, stating it is safe to remove the card. (See microSD Card Information and Settings.)

3. Using your fingernail or a thin blunt object, gently press the microSD card in and then release; it should partially pop out of its slot.

4. Remove the microSD card and store it in a safe place.

5. Replace the battery compartment cover.

Accessing the microSD Card

If the microSD slot is enabled, an inserted card appears in your file browser as a shared network drive.

The way to access the card varies, depending on your operating system.

Note: In the information that follows, **<Hostname>** is the value of the Hostname field (in **Advanced settings > Wi-Fi > Network** and also in **Advanced settings > Router > LAN**).

Windows

1. In Windows Explorer or Internet Explorer, type one of the following:

   - **\\SprintHotspot**

   - **\\<Router IP Address>** (field in **Advanced settings > Router > LAN**)

     For example, \\192.168.0.1\

   - **\\<Hostname>** (For example, \\MyDeviceName\)

   — or —

   From the Windows **Start** menu, click **Run**, and then type one of the following:

   - **\\SprintHotspot**

   - **\\<Hostname>**

2. Double-click the shared folder.

Mac

1. In Finder, select **Go > Connect to Server**.

2. Type one of the following:

   - **smb://SprintHotspot/**

   - **smb://<Router IP Address>/** (For example, smb://192.168.0.1/)

   - **smb://<Hostname>** (For example, smb://MyDeviceName)

3. When prompted, select the shared drive as the folder to mount.

Linux

1. Open the run menu (Alt+F2) or a file browser, and type one of the following:

   - **smb://SprintHotspot**

   - **smb://<Router IP Address>/** (For example, smb://192.168.0.1/)

   - **smb://<Hostname>/** (For example, smb://MyDeviceName)

2. Double-click the shared folder.

Other operating systems

Please see the user documentation for your operating system or computer.

If security has been enabled for the microSD card, you will be prompted to enter the username and password for the microSD card. (See Setting Up Access to the microSD Card.)

Frequently Asked Questions

Find out answers to questions you may have.

How Can I Tell I'm Connected to 3G or 4G?

How Do I Connect to Wi-Fi?

Is Roaming on 4G Supported?

What Do I Do if I Forget the Wi-Fi Password?

What Do I Do if I Forget the Administrator Password?

What Do I Do if the Home Page Displays "Charging paused"?

If the Connection is "Always On," Am I Always Being Billed?

How can I Stream Files to my Computer, Tablet, or Mobile Phone?

Questions About GPS and Sprint Location Services

Questions About WPS

How Do I Access My Corporate Network Through a VPN?

Are Terminal Sessions Supported?

How Can I Tell I'm Connected to 3G or 4G?

There are several ways you can tell you're connected to 3G or 4G.

When you're connected:

- The 3G or 4G icon (on the left side of the home page) is solid. For example, 4G .

- The bottom area of the device LCD, the Virtual Device, and the Mini Window show the data transfer icon and data transfer information (amount of data; connection duration).

How Do I Connect to Wi-Fi?

You may have to manually connect to Wi-Fi after certain events — for example, as part of the initial device setup, or after a software update.

Tip: The Wi-Fi network name and password are displayed on one of the LCD information screens of the Sierra Wireless 4G LTE Tri-Fi Hotspot. (See LCD Information Screens.)

To connect to Wi-Fi:

1. Do one of the following, depending on your operating system.

    Windows 7: Right-click the ⬛ icon in the system tray.

    Windows Vista: Click **Control Panel > Network and Internet > Network and Sharing Center > Connect to a network**.

    Windows XP: Click **Control Panel > Network Connections > Wireless Network Connections > View available wireless networks**.

    Mac: Click the AirPort icon 📶 (in the upper right corner of your screen).

    Linux: Please see the user documentation of the Linux distribution.

    Other operating systems: Please see the user documentation for your operating system or computer.

2. Select the Wi-Fi network provided by the Sierra Wireless 4G LTE Tri-Fi Hotspot and connect to it. (If prompted for a network key/security key/password, enter the Wi-Fi password.)

Is Roaming on 4G Supported?

At the time of this release, roaming (that is, using a network other than Sprint) on 4G or 4G LTE is not supported.

Your device can roam on 3G and also automatically switch, in Sprint coverage, between 4G and 4G LTE. (To change the roaming setting, see Roaming Information and Settings. To change the 3G/4G connection settings, see "Configuring the 3G/4G Connection Preferences" in Mobile Broadband Information and Settings.)

What Do I Do if I Forget the Wi-Fi Password?

There are a couple of things you can do if you forgot the Wi-Fi password.

- If the Wi-Fi Password Reminder feature is enabled, display the password on the device. (See "Wi Fi Password Reminder" in Wi-Fi Password.)

- Connect the device to your computer through USB, then log in and view the Wi-Fi password (in **Advanced settings > Wi-Fi > Security**). Write the password down in a safe place. (See Connecting Through USB.)

What Do I Do if I Forget the Administrator Password?

Here's what to do if you forgot the Administrator Password.

1. Reset the software to default settings. (See Resetting the Software to Default Settings: General.)

2. Go through the device setup, during which the administrator password will be displayed; write it down in a safe place. (See Device Setup.)

What Do I Do if the Home Page Displays "Charging paused"?

If the text after the battery icon (on the home page) includes "Charging paused" (as shown in the screenshot below), there are several things you can try.

● Connect your device through the micro-USB cable.

● Disconnect from the 3G or 4G network.

● Turn the device off and wait until it no longer feels warm to the touch.
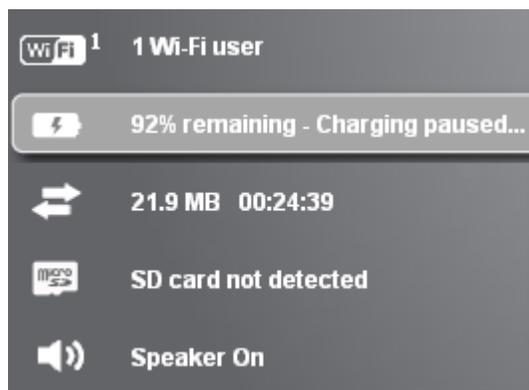
If the Connection is "Always On," Am I Always Being Billed?

No; the connection to the network goes dormant after a period of inactivity, but the connection can be re-established faster than having to reconnect. Billing occurs only when data is passed across the network.

How can I Stream Files to my Computer, Tablet, or Mobile Phone?

Your Sierra Wireless 4G LTE Tri-Fi Hotspot can serve as a Digital Media Server (DMS), providing content to networked digital media players (DMP) and digital media renderers (DMR). You can, for example, play audio or movie files (stored on the microSD card inserted in your hotspot) on a computer, tablet, mobile phone, or TV that supports DLNA. (**Note:** The software on the device must support the types of files you're trying to play. If you're having problems, check the user documentation of the software.)

If your device supports DLNA, see Enabling DLNA Media Server. (For a list of products that support DLNA, see www.dlna.org/consumer-home/look-for-dlna/product-search.)

Questions About GPS and Sprint Location Services

Find answers to common questions about GPS and Sprint Location Services.

What is LBS?

What is GPS?

What is Enhanced Local Search?

How Do I Use the Enhanced Local Search Feature?

Where Can I Use GPS?

How Do I Enable or Disable GPS?

Location-Based Services Limitations

How Can I Stream GPS Data to Use With a Third-party GPS Application?

What is LBS?

LBS (Location-Based Services) is used to provide enhanced Local Search feature via internet mapping services. (For more information, see Performing a Location Search.)

What is GPS?

GPS stands for Global Positioning System, which is a system that uses a series of 24 geosynchronous satellites to provide location data.

GPS satellites transmit signals to equipment on the ground. GPS receivers passively receive satellite signals, but do not transmit.

What is Enhanced Local Search?

Enhanced Local Search is a quick, easy method to run, via the browser interface, local search queries to find locations and directions to locations and businesses.

The enhanced Local Search feature uses LBS and allows you to search for Sprint stores, restaurants, banks, hotels, or other points of interest. (For more information, see Performing a Location Search.)

How Do I Use the Enhanced Local Search Feature?

See Performing a Location Search.

Where Can I Use GPS?

GPS works wherever you have line-of-sight access to the GPS satellites.

How Do I Enable or Disable GPS?

By default, Sprint Location Services are disabled. To enable Sprint Location Services, see Enabling GPS.

Location-Based Services Limitations

Weather conditions may affect your ability to get a clear view of the satellites and thus to acquire a GPS fix.

How Can I Stream GPS Data to Use With a Third-party GPS Application?

Follow these steps to stream GPS data for a third-party GPS application.

1. Install the device driver. (See Making a Tethered Connection.)

2. Set **GPS Mode** (in **Advanced settings > WAN > GPS**) to **Continuous**.

3. Determine the COM port number that your Sierra Wireless device (that is, your Sierra Wireless 4G LTE Tri-Fi Hotspot) is using.
   In the following example for Windows, the Device Manager shows that COM 18 is used. In your case, the COM port number might be different.
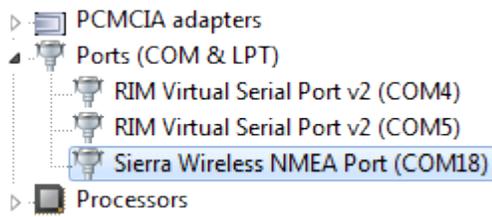
    (If you don't know how to access the Device Manager, see
http://sierrawireless.custhelp.com/app/answers/detail/a_id/698.)

4. Configure your GPS application to use the same COM port. For help, see the documentation of the GPS application.

Questions About WPS

Find answers to common questions about WPS.

What is WPS?

How do I Use WPS?

If a Wireless Device has a WPS Button or a WPS Software Option, Must I Use it to Connect Via Wi-Fi?

What is WPS?

Wi-Fi Protected Setup (WPS) provides a fast, simple, and secure way to connect WPS-enabled devices to your Wi-Fi network. You don't have to give the name (SSID) and Wi-Fi password of your network to other users.

The WPS feature is available on certain cameras, printers, smartphones, and laptops. These devices have either a hardware button or a WPS-related option in the software. Please consult the user documentation of your device.

How do I Use WPS?

Please see Connecting Through WPS.

If a Wireless Device has a WPS Button or a WPS Software Option, Must I Use it to Connect Via Wi-Fi?

If this is the only way your device provides to connect through Wi-Fi, then you must use the WPS button or the WPS software option. Some laptops support two methods — a WPS button or software option, and Wi-Fi network manager software where you can connect by entering the Wi-Fi network name (SSID) and password, as described in How Do I Connect to Wi-Fi?

Please consult the user documentation of your device.

How Do I Access My Corporate Network Through a VPN?

The answer to this question depends on whether you're using Sprint Data Link^{SM}.

Using Sprint Data Link

Sprint Data Link is a network feature that allows you to directly connect to your corporate VPN.

With Data Link, you and your mobile workforce can maintain a secure, seamless VPN connection between your enterprise network and the advanced Sprint Mobile Broadband Network.

To learn more about Data Link, to arrange a connectivity solution that works for you, or to configure Data Link, please contact Sprint.

If You're Not Using Sprint Data Link

Once you complete a wireless connection, you may need to launch an extranet client provided by your company and supply the appropriate user name and password to gain access. For support, contact your company help desk.

Are Terminal Sessions Supported?

Terminal sessions (for example, via telnet or ssh) are not supported.

Tips

This section provides information on getting the most out of your device and your network connection.

Extending Battery Life

Device Location

Improving Signal Strength

Improving 3G Network Service

Improving Wi-Fi Performance

Security Tips

Finding the MAC Address

Finding the IP Address

Extending Battery Life

There are several ways you can extend the battery life.

- When you're not using the device, turn it off, or end the 3G/4G connection. (Click **Disconnect** on the home page or in the Mini Window.)

- Connect the device through the micro-USB cable to your computer, and disable Wi-Fi. (See Disabling Wi-Fi When Connected Through USB.)

- Adjust the LCD — do one or more of the following:

  - Turn the LCD off (**Advanced settings > Device > Display > LCD Backlight**).

  - Decrease the brightness of the LCD (**Advanced settings > Device > Display > Backlight Settings > On Battery/USB Power**).

  - Set the LCD to turn off sooner. (See Setting the LCD Timeout.)

- Configure the setting (for when battery powered or connected via USB) to "Short Range" (**Advanced settings > Wi-Fi > Network > Battery or USB Powered**).

- Enable standby (low power) mode. (See "Standby (Low Power) Mode" in Battery Information and Settings.)

- Turn off the lighting of the power button (that is, LED) (**Advanced settings > Device > Display > Power Button LED**).

- Limit the number of Wi-Fi users (**Advanced settings > Wi-Fi > Network > Max Number of Users**).

- If you have 3G but not 4G or 4G LTE coverage, set **WAN Mode** to "3G Only" (**Advanced settings > WAN > Setup > WAN Mode**).

- Set **Wi-Fi > Network > Wi-Fi Power Save Mode** to "On." (If your computer tends to lose the Wi-Fi connection and stops responding, set this field to "Off.")

- If GPS is enabled and you're using your device from the same location, set **GPS Mode** to "One-time." (See Setting the GPS Mode.)

Device Location

Follow these guidelines in placing your device.

- Avoid moisture or extreme temperatures.

- For improved reception, place the device near a closed window.

- Place your device within easy reach of a reliable power supply and the computer to which it will be connected.

Improving Signal Strength

There are several ways you can improve the signal strength.

- Make sure you're inside a 4G, 4G LTE, or 3G coverage area.

- Try reorienting your device.

- Move the device and your computer to another location — you may be in or near a structure that is blocking the signal. Every obstacle (for example, walls, ceilings, furniture) between the Sierra Wireless 4G LTE Tri-Fi Hotspot and other wireless devices decreases the signal strength.

- Place the device in a centralized location, as high as possible in the room.

- Make sure there's plenty of space around your device to provide the best signal reception.

- Keep the device at least 3–6 feet away from electrical devices that generate RF interference (for example, microwaves, TVs, 2.4 GHz cordless phones, cellular phones, baby monitors, wireless speakers). If you're not using these electrical devices, turn them off.

- If possible, place your devices so that the signal passes through open doorways or drywall, as opposed to concrete, brick, metal, walls with insulation, and so on.

- If you cannot obtain service, contact Sprint — a network or account problem may be preventing you from obtaining service.

- Consider purchasing the desktop cradle for the Sierra Wireless 4G LTE Tri-Fi Hotspot from the Sprint Store at sprint.com or from the Sierra Wireless online store at sierrawireless.com/eStore.

Improving 3G Network Service

To improve your network service, periodically check for PRL and profile updates.

The PRL (Preferred Roaming List) is an account configuration item set by your service provider. It controls the radio channels and network carrier used by the 3G modem.

To check for these updates:

1. Log in to the home page.

2. Click **Advanced settings** ( ).

3. Click **WAN > Setup**.

4. Click **Update 3G PRL**.

5. After the update checking is completed, click **Update 3G Profile**.

Improving Wi-Fi Performance

There are several ways you can improve Wi-Fi performance.

- Try a different channel number. (See Wi-Fi Channel.)

- Check whether any device updates are available. (See Updates.)

- See the tips in Improving Signal Strength.

- Limit the number of Wi-Fi users (**Advanced settings > Wi-Fi > Network > Max Number of Users**).

- Select a longer Wi-Fi range (**Advanced settings > Wi-Fi > Network > Long Range > Battery or USB Powered** or **AC Powered**).

Windows XP Users

1. Open the Device Manager.

  - Click **Start > Settings > Control Panel**.

  - Double-click **System**.

- Click **Hardware**.

- Click **Device Manager**.

2. Double-click **Network adapters**.

3. Double-click the Wi-Fi client network adapter of your computer — for example, "Intel(R) WiFi Link 5100 AGN" in the screenshot below.
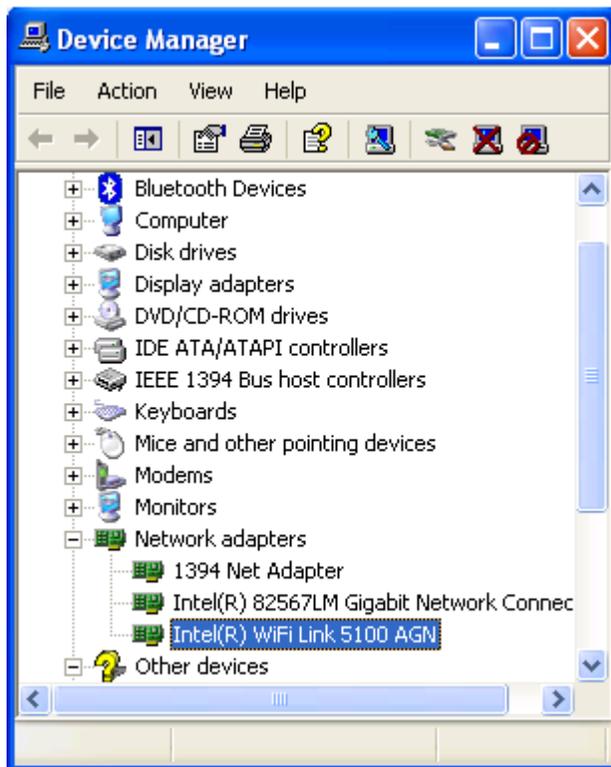
4. If the Wi-Fi client network adapter is by Intel, click **Advanced** and, in the **Property** list, click **Power Management** and move the slider all the way to the right (to **Highest**). Click **OK**.

— or —

If the Wi-Fi client network adapter is not by Intel, select a configuration with minimal power savings (to maximize throughput).

Note: The above settings are often controlled by 3rd-party value-add applications and may be automatically changed. If Wi-Fi performance improves for a while after performing the above steps, but then declines, recheck the above settings.

Security Tips

Follow these tips to minimize security risks.

- Change the Wi-Fi network name (SSID) and Wi-Fi password on a regular basis. (See SSID (Wi-Fi Network Name) and Wi-Fi Password.)

- Disable SSID Broadcast. (See Wi-Fi Tab: Network Panel.)

- Use the highest level of Wi-Fi security that your devices support. (See Wi-Fi Security.)

- Change the login password. (See Changing the Administrator Password.)

- Use MAC filtering to specify computers that are or aren't allowed to connect to the network. (See Wi-Fi Tab: MAC Filter Panel.)

Finding the MAC Address

You'll need to know the MAC address of a device in a couple of cases.

- Assigning an IP address based on a MAC address (when using DHCP). (See "DHCP Static IP Assignment List" in LAN Panel: DHCP.)

- Allowing or denying computers access to the network. (See Allowing or Denying Computers Access to the Network.)

Tip: You can display a list of connected devices, including the MAC address of each device: click **List of connected devices**, available from **Advanced settings > Wi-Fi > MAC Filter** or from **Advanced settings > Wi-Fi > Network**.

The steps to finding the MAC address of a device vary, depending on your operating system.

Windows

1. Open a command prompt window.

   - Click **Start** and **Run**.

   - Type **cmd** or **command**, and click **OK**.

2. At the command prompt, type **ipconfig/all** and press **Enter**.

3. Write down the Physical Address for the entry that relates to the wireless network connection; it appears as a series of numbers and letters — this is the MAC address of your wireless adapter.

Mac OS X

1. From the Apple menu ( ), select **System Preferences**.

2. Select **Network**.

3. Select the adapter that is connecting to the routing hardware.

4. Select **Advanced**.

5. Select **Ethernet**. The Ethernet ID is listed. This is the same as the MAC address.

Linux

Please see the user documentation of the Linux distribution.

Other operating systems

Please see the user documentation for your operating system or computer.

Finding the IP Address

You'll need to know the IP address of a device when configuring certain features.

- Port forwarding

- Port triggering

- DMZ

- Static DHCP features

The steps to finding the IP address of a device vary, depending on your operating system.

Windows

1. Open a command prompt window.

    ▪ Click **Start** and **Run**.

    ▪ Type **cmd** or **command**, and click **OK**.

2. At the command prompt, type **ipconfig** and press **Enter**.

3. Write down the IP Address for the entry that relates to the wireless network connection. (The IP address might be listed under "Ipv4 Address," or something similar.)

Mac OS X

1. From the Apple menu ( ), select **System Preferences**.

2. Select **Network**.

3. Select the wireless adapter. The IP address is displayed in the right pane.

Other operating systems

Please see the user documentation for your operating system or computer.

Troubleshooting

Learn about various troubleshooting tips, and what to do when a specific message is displayed.

General Tips

Connection Errors

LCD Is Dark

Insufficient Signal Strength

Messages Displayed on the Device LCD

Cannot Connect to Wi-Fi

WPS-Related Messages

Cannot Connect Through USB

Cannot Display the Home Page

Cannot Connect to the 3G or 4G Network

The Device Seems to Have Stopped Charging

Sprint Location Services Aren't Working or Don't Seem to Be Available

GPS Fix Not Available

Cannot Check for Updates

Sounds Are Enabled, but the Device Doesn't Generate Any Sounds

General Tips

Here are some general tips to get you started.

- If the LCD shows "Connection Error", followed by a number, see Connection Errors.

- Check the system events log. (See "Exporting System Events" in System Events.)

- If some settings are preventing you from connecting to Wi-Fi, connect to the device through the micro-USB cable, and then change the settings. (See Connecting Through USB.)

- Go to sprint.com/support to access troubleshooting and other resources.

- The knowledge base at the Sierra Wireless website (www.sierrawireless.com/support/customer_help.aspx) may also be useful.

Connection Errors

If any of the following 4G LTE connection errors are displayed on the LCD, on the Mini Window, or on the Virtual Device, contact Sprint and provide them with the name and number of the error.

Error number	Description
2	IMSI unknown in HSS
3	Illegal UE
6	Illegal ME
7	EPS services not allowed
8	EPS services and non-EPS services not allowed
9	UE identity cannot be derived by the network
10	Implicitly detached
11	PLMN not allowed
12	Tracking Area not allowed
13	Roaming not allowed in this tracking area
14	EPS services not allowed in this PLMN
15	No Suitable Cells In tracking area
16	MSC temporarily not reachable
17	Network failure
18	CS domain not available
19	ESM failure
20	MAC failure
21	Synch failure
22	Congestion
23	UE security capabilities mismatch
24	Security mode rejected, unspecified
25	Not authorized for this CSG
26	Non-EPS authentication unacceptable
39	CS domain temporarily not available
40	No EPS bearer context activated
95	Semantically incorrect message
96	Invalid mandatory information
97	Message type non-existent or not implemented

98	Message type not compatible with the protocol state
99	Information element non-existent or not implemented
100	Conditional IE error
101	Message not compatible with the protocol state
111	Protocol error, unspecified
133	Error unknown
138	Lower layer failure
150	T3410 timeout
151	T3420 timeout
153	T3418 timeout
256	NAS EMM not registered
257	Service loss
Other value	Protocol error, unspecified

LCD Is Dark

The following table describes situations that can cause the LCD to be dark (that is, not displaying any text or icons), and recommends actions.

Device state	LCD state	Your action
On	Off (**Advanced settings > Device > Display > LCD Backlight** is set to "Off")	Turn on the LCD: set **LCD Backlight** to "On."
On	On, but dormant (inactivity timeout)	Briefly press the power button on the device.
Off	Off	Turn the device on: Make sure a battery is inserted into the device. Press the power button on the device until the device turns on.

If the LCD is still dark, use the micro-USB cable to connect the device to the AC charger or to a computer.

Insufficient Signal Strength

If you have insufficient signal strength, an icon is displayed on the left side of the home page.

Insufficient signal strength, indicated by , may occur because:

- You are outside a 4G, 4G LTE, or 3G coverage area.

- Your device's internal antenna is pointing in the wrong direction.

- You are in or near a structure that is blocking the signal.

- You are near a device that is causing radio signal interference.

- A network or account problem is preventing you from obtaining service.

See also Improving Signal Strength.

Messages Displayed on the Device LCD

Use this section to look up a specific message displayed on the LCD and find out what steps to take.

3G Activation Failed

Connecting to 3G/4G

Connection Error

Device Activation Required

Searching for Network

Update Failed

See also SD Card Error.

3G Activation Failed

See "Activating Your Device Through the "3G Activation Required" Alert" in Activating Your Device.

Connecting to 3G/4G

If the device LCD displays "Connecting to 3G/4G", go through the following steps.

1. Check the signal strength. If it is weak, try the tips in Improving Signal Strength.

2. Try a different Connection Preferences setting. (See Mobile Broadband Information and Settings.)

3. Turn the device off and on. (See "Turning Your Device Off" and "Turning Your Device On" in Turning Your Device On and Off.)

4. Update the 3G profile: click **Advanced settings > WAN > Setup > Update 3G Profile**.

5. If you're still unable to connect to 3G or 4G, contact Sprint.

Connection Error

If the device LCD displays "Connection Error", go through the following steps.

1. Log in to the home page.

2. Click **Advanced settings** (   ).

3. Click **WAN > Setup > Update 3G Profile**.

4. If an error message and number are displayed on the LCD after the update:

   ▪ Note the information.

   ▪ Check the table in Connection Errors.

   ▪ Contact Sprint.

Device Activation Required

See "Activating Your Device Through the "3G Activation Required" Alert" in Activating Your Device.

Searching for Network

The LCD displays this message until a 3G or 4G network is acquired.

If this message persists, see the tips in Cannot Connect to the 3G or 4G Network.

Update Failed

If this message appears on the device LCD or in the Software Update Available alert window (after you've attempted the update), go through the following steps:

1. Make sure your device is connected to the AC charger or computer through the micro-USB cable.

Note: If you'll be using USB for data transfer (and not just for charging the device), you must install the device driver. (See Making a Tethered Connection.)

2. Retry the update.

3. If the "Update failed" message is still displayed, contact Sprint.

Cannot Connect to Wi-Fi

If your computer cannot connect to the Wi-Fi network of the Sierra Wireless 4G LTE Tri-Fi Hotspot, there are several things you should check.

Make sure that:

- The maximum number of Wi-Fi users has not been reached. (To determine the number of connected Wi-Fi users and set the maximum, see Wi-Fi Users Information and Settings.)

- You're connecting to the correct Wi-Fi network (SSID), and you're using the correct Wi-Fi password. If the Wi-Fi Password Reminder feature is enabled, you can use it to display the SSID and Wi-Fi password on the device LCD. (See "Wi-Fi Password Reminder" in Wi-Fi Password.)

- Nobody has changed the name or password of the Wi-Fi network. If the Wi-Fi Password Reminder feature is enabled, you can use it to display the SSID and Wi-Fi password on the device LCD. (See "Wi-Fi Password Reminder" in Wi-Fi Password.)

- Nobody is connected through the micro-USB cable when **When connected to USB** is selected (for **Advanced settings > Wi-Fi > Network > Disable Wi-Fi**).

- **Always** is not selected (for **Advanced settings > Wi-Fi > Network > Disable Wi-Fi**).

- Your computer supports the type of Wi-Fi security that the network is set to use.

Note: All the devices used with the Sierra Wireless 4G LTE Tri-Fi Hotspot must support the selected security type.

- Your computer supports Wi-Fi 802.11g (if **Basic Rate** is set, in **Advanced settings > Wi-Fi > Security**, to **802.11g only**).

- Your computer has not been blocked through MAC filtering. (See "Specifying Computers That Are Not Allowed to Access the Network" in Allowing or Denying Computers Access to the Network.)

Tip: If some settings are preventing you from connecting to Wi-Fi, connect to the device through the micro-USB cable, and then change the settings. (See Connecting Through USB.)

WPS-Related Messages

Use this section to look up a specific WPS-related message and find out what steps to take.

WPS Failed. WPS could not add the device to the network

WPS Not Available. WPS feature not enabled

WPS Not Available. SSID Broadcast disabled

WPS Not Available. Wi-Fi currently disabled

WPS Not Available. WEP or WPA security not allowed

WPS Not Available. Max connected devices

WPS Not Available. MAC Filter list empty

WPS PIN Chksum Error

WPS PIN Mismatch. The PIN used did not match the PIN of the device

WPS Timeout. The WPS session was terminated. Press WPS button to try again

WPS Multiple Sessions Error

WPS Failed. WPS could not add the device to the network

If the LCD of your Sierra Wireless 4G LTE Tri-Fi Hotspot displays this message, the device you are trying to connect may not be WPS-enabled. Use the manual method to connect the W-Fi device to your Wi-Fi network, as described in Manually Entering the Wi-Fi information.

WPS Not Available. WPS feature not enabled

If the LCD of your Sierra Wireless 4G LTE Tri-Fi Hotspot displays this message, go through the following steps.

1. Click **WPS** (below the Virtual Device).

2. In the WPS Setup window, select **Enable**.

3. Click **Save**.

4. Retry the WPS process.

WPS Not Available. SSID Broadcast disabled

If the LCD of your Sierra Wireless 4G LTE Tri-Fi Hotspot displays this message, go through the following steps.

1. Click **Advanced settings** ( ).

2. Click **Wi-Fi > Network**.

3. Set **SSID Broadcast** to **Enable**.

4. Click **Save**.

5. Retry the WPS process.

6. After you've finished using WPS, for security reasons it's recommended you change **SSID Broadcast** back to **Disable**.

WPS Not Available. Wi-Fi currently disabled

If the LCD of your Sierra Wireless 4G LTE Tri-Fi Hotspot displays this message, go through the following steps.

1. Click **Advanced settings** ( ).

2. Click **Wi-Fi > Network**.

3. Set **Disable Wi-Fi** to **Never**.

4. Click **Save**.

5. Retry the WPS process.

WPS Not Available. WEP or WPA security not allowed

If the LCD of your Sierra Wireless 4G LTE Tri-Fi Hotspot displays this message, go through the following steps.

1. Click **Advanced settings** ( ).

2. Click **Wi-Fi > Security**.

3. Select either a WPA2 Personal option (including **WPA/WPA2 Personal**) or (not recommended) no security.

4. Click **Save**.

5. Retry the WPS process.

WPS Not Available. Max connected devices

If the LCD of your Sierra Wireless 4G LTE Tri-Fi Hotspot displays this message, go through the following steps.

1. Disconnect one of the devices that is currently connected through Wi-Fi.

2. Retry the WPS process.

WPS Not Available. MAC Filter list empty

This message occurs when you try WPS while MAC filter mode is "Allow all in list", but no computers have been added to the list.

Do one of the following:

► Add one or more computers to the list of computers that can access the network. (See "Specifying Computers That Can Access the Network" in Allowing or Denying Computers Access to the Network.)

— or —

► Turn off MAC filtering. (See Wi-Fi Tab: MAC Filter Panel.)

WPS PIN Chksum Error

This message may occur when the PIN that you've entered (after having selected **Use PIN method**) is incorrect. Make sure you have the correct PIN for the device you're adding to the network.

WPS PIN Mismatch. The PIN used did not match the PIN of the device

This message may occur when the PIN that you've entered (after having selected **Use PIN method**) is incorrect. Make sure you have the correct PIN for the device you're adding to the network.

WPS Timeout. The WPS session was terminated. Press WPS button to try again

WPS did not start in the expected time. Make sure you start WPS on both the wireless device and the Sierra Wireless 4G LTE Tri-Fi Hotspot. (See Connecting Through WPS.)

WPS Multiple Sessions Error

This message occurs when more than one WPS session is in progress.

Note: For security reasons, only one device is allowed to join, through the PBC (Push Button Configuration) method, the network at a time. If the Sierra Wireless 4G LTE Tri-Fi Hotspot detects simultaneous PBC connection requests from multiple devices in the past two minutes, it blocks PBC.

If you're using WPS to add more than one device to your network, finish adding one device before you add the next one.

Cannot Connect Through USB

If your computer cannot connect to the Sierra Wireless 4G LTE Tri-Fi Hotspot through the micro-USB cable, go through the following steps.

1. Make sure that you've installed the device driver, as described in Making a Tethered Connection.

2. Connect to the Sierra Wireless 4G LTE Tri-Fi Hotspot through Wi-Fi.

3. Make sure that **USB Tethered Networking** is set, in **Advanced settings > Router > Basic**, to **Enable**.

4. Restart the device.

Cannot Display the Home Page

Your Web browser may display an error message when you try to display the home page. The error message depends on your Web browser.

- "Could not connect to remote server" (Opera)

- "Internet Explorer cannot display the webpage" (Internet Explorer)

- "Oops! This link appears to be broken" (Google Chrome)

- "Safari can't open the page" (Safari)

- "The connection has timed out" (FireFox)

Check the following:

- The device is turned on. (See "Turning Your Device On" in Turning Your Device On and Off.)

- You have established a connection to the device (through Wi-Fi or through the micro-USB cable).

- Make sure you're typing the correct address in the Web browser.

  - Try **http://<SSID>**, where <SSID> is as displayed on the device LCD. (See LCD Information Screens.)

  - If the home page is still not displayed, try **http://192.168.0.1** or, if you're using custom routing settings, replace "192.168.0.1" with the appropriate IP address.

- The Web browser is a recent version, and Java-enabled. The following are recommended:

  - Internet Explorer (version 6.0 or higher)

  - Mozilla Firefox (version 2.0 or higher)

  - Google Chrome (version 2.0.172.28 or higher)

  - Apple Safari (version 2.0 or higher)

  - Opera version 9.64

- If your computer has other adapters (for example, Ethernet) connected to other networks, disable or remove them from your computer.

- If Internet security software is running on your computer, disable it and see whether the error message still occurs. Some firewall software may block access to the home page.

- If DHCP is enabled on the device, make sure DHCP is enabled on your computer. (See LAN Panel: DHCP.)

- Check your Web browser settings.

  - Open the Control Panel in Windows.

  - Double-click **Internet Options**.

  - From the **Security** tab, restore the default settings.

  - From the **Connections** tab, select **Never dial a connection**.

  - From the **Advanced** tab, restore the default settings.

  - Close and reopen your Web browser.

- Disconnect the device from your computer (if you're using the micro-USB cable). Remove the battery from the device. Reinsert the battery.

If, after checking all of the above, you still cannot display the home page, consider resetting the software to default settings. (See Resetting the Software to Default Settings: General.)

Cannot Connect to the 3G or 4G Network

If this message is displayed, go through the following steps.

- Make sure your computer is connected to the device (through the micro-USB cable or Wi-Fi). (See How Do I Connect to Wi-Fi? or Making a Tethered Connection.)

- Make sure you're in 4G, 4G LTE, or 3G coverage.

- Try the tips in Improving Signal Strength.

- Check the **WAN Mode** setting (**Advanced settings > WAN > Setup**). For example, if it's set to **4G Only**, you won't be able to connect if you don't have 4G or 4G LTE coverage.

- If you're roaming on 3G, make sure that 3G roaming is enabled. (In the Roaming Information window, select **Allow 3G Roaming**.)

Note: Roaming charges may apply.

- If you're roaming internationally, make sure that **Allow 3G international access** is selected (on the Roaming Information window).

- Check whether 4G is in power save mode — the LCD of the device displays "Power Save Mode. 4G Network not found." If this is the case, press the power button on the device or click the **Scan for 4G** button in the Signal Quality window.

- Check with Sprint — a network or account problem may be preventing your device from obtaining service.

The Device Seems to Have Stopped Charging

If the "About..." LCD information screen shows "chrg paused" or the text after the battery icon (on the home page) includes "Charging paused," see What Do I Do if the Home Page Displays "Charging paused"?

(For more information on the LCD information screens, see LCD Information Screens.)

Sprint Location Services Aren't Working or Don't Seem to Be Available

Make sure that GPS is enabled. (See Enabling GPS.)

For best results, minimize the number of obstructions between your device and the GPS satellites.

GPS Fix Not Available

Make sure you have a clear view of the sky; if you're in a forested area, or in or near tall buildings, move to another location.

To retry a fix, click **Retry Now**. Otherwise, click **Cancel**.

Cannot Check for Updates

Make sure your device is connected to the AC charger or computer through the micro-USB cable.

Note: If you'll be using USB for data transfer (and not just for charging the device), you must install the device driver. (See Making a Tethered Connection.)

Sounds Are Enabled, but the Device Doesn't Generate Any Sounds

Check that sounds are not turned off through the mute switch on the device. (See "Mute Switch" in Other Buttons and Switches.)

Technical Specifications

This section lists the electrical, radio frequency, and other parameters of the device for those who require technical information.

LED Operation

Radio Frequency and Electrical Specifications

Software Specifications

Environmental Specifications

Mechanical Specifications

LED Operation

See Using the Power Button to Determine the Device State.

Radio Frequency and Electrical Specifications

This section lists the radio frequency and electrical parameters of the device.

Item	Description
Approvals	FCC
Battery	Size: 3600 mAh Duration for full charge: AC charger: 7 hours PC USB cable: 8 hours Charge life: 10 hours under standard use 8 hours of continuous use
Current	Maximum: 1400 mA Standby current: 4 mA (1xEV-DO/IS2000 hybrid mode) 3 mA (LTE) 5 mA (WiMAX)
Transmit	PCS: 1850 to 1910 MHz Cellular: 824 to 849 MHz LTE: 1910 to 1915 MHz WiMAX: 2495 to 2690 MHz
Receive	PCS: 1930 to 1990 MHz Cellular: 869 to 894 MHz LTE: 1990 to 1995 MHz

	WiMAX: 2495 to 2690 MHz GPS: 1575.42 MHz

Software Specifications

This section lists the specifications that the device supports.

Item	Description
CDMA (3G) specification	IS-2000 Release 0
Data service	IS-707A
LTE (4G) specification	3GPP Release 9
WiMAX (4G) specification	IEEE 802.16e-2005
Wi-Fi specification	IEEE 802.11b IEEE 802.11g IEEE 802.11n
Wi-Fi security and encryption protocols	WEP Open & Shared WEP-64 WEP-128 WPA-Personal TKIP & AES (Pre-Shared Key or WPA-PSK) WPA2-Personal TKIP & AES (WPA2-PSK) WPA+WPA2-Personal (WPA+WPA2 PSK)
WPS	Wi-Fi Simple Configuration 2.0 (WSC 2.0) based Wi-Fi Protected Setup (WPS)
SMS (IS-637)	Not supported
FAX	Not supported
IOTA	Supported
OTASP (IS-683A, IS-683B, IS-683C)	Supported
OTAPA	Supported
PRL (Preferred Roaming List)	Supported
Authentication	Supported
Voice	Not supported
NAM	Single
Position Location	Standalone
TTY/Accessibility	Not supported
Mobile IP	Supported
Network protocols (routing hardware)	TCP, UDP, ARP, RARP, ICMP

VPN	Pass-through of the following VPN types: PPTP IPSec Tunneling of multiple VPN sessions simultaneously is supported.

Environmental Specifications

This section describes the environmental conditions that the device can be used in.

Item	Description
Operating temperature	32 to 95°F
Storage temperature	-4 to +140°F
Humidity	90% at +140°F
Drop	1.5 m (approx. 59") on granite

Mechanical Specifications

This section describes the dimensions and physical features of your device.

Item	Description
Dimensions (W x L x H)	3.84" x 2.25" x 0.95"
Power button	Supported
Headset jack	Not supported
LED	White

Safety Information

Read important safety information about your device.

Important Notice

Safety and Hazards

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the Sierra Wireless 4G LTE Tri-Fi Hotspot are used in a normal manner with a well-constructed network, the device should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. Sierra Wireless accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the device, or for failure of the device to transmit or receive such data.

Safety and Hazards

Do not operate your device under the following conditions.

- In areas where blasting is in progress

- Where explosive atmospheres may be present

- Near medical equipment

- Near life support equipment, or any equipment that may be susceptible to any form of radio interference.

In such areas, your device MUST BE POWERED OFF. The device can transmit signals that could interfere with this equipment.

Do not operate the device in any aircraft, whether the aircraft is on the ground or in flight. In aircraft, the device MUST BE POWERED OFF. When operating, the device can transmit signals that could interfere with various onboard systems.

Note: Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. The device may be used at this time.

The driver or operator of any vehicle should not operate the device while in control of a vehicle. Doing so will detract from the driver or operator's control and operation of that vehicle. In some jurisdictions, operating such communications devices while in control of a vehicle is an offense.

Proper Battery Use and Disposal

Follow these guidelines to ensure safe and responsible battery use.

- Do not open, disassemble, puncture, crush, bend, or shred.

- Do not expose to water or other liquids, fire, explosion, or other hazards.

- Use the battery only in the Sierra Wireless 4G LTE Tri-Fi Hotspot.

- If using with a charger, use only the AC charger supplied with the device.

- Do not short circuit the battery.

- When replacing a battery, use the same model of battery that was supplied with the device.

- Follow local regulations when disposing of a used battery.

- Avoid dropping the device or the battery. If dropped and you suspect damage, take it to a service center for inspection.

Note: Improper battery use may result in a fire, explosion, or other hazard.

Regulatory Notices

This section contains regulatory information for your device.

The design of the Sierra Wireless 4G LTE Tri-Fi Hotspot complies with U.S. Federal Communications Commission (FCC) guidelines respecting safety levels of radio frequency (RF) exposure for mobile devices, which in turn are consistent with the following safety standards previously set by U.S. and international standards bodies:

- ANSI / IEEE C95.1-1999, **IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3kHz to 300 GHz**

- National Council on Radiation Protection and Measurements (NCRP) Report 86, 1986, **Biological Effects and Exposure Criteria for Radio Frequency Electromagnetic Fields**

- International Commission on Non-Ionising Radiation Protection (ICNIRP) 1998, **Guidelines for limiting exposure to time-varying electric, magnetic, and electromagnetic fields (up to 300 GHz)**

FCC ID: N7NAC803S.

RF Exposure - The Sierra Wireless 4G LTE Tri-Fi Hotspot has been tested for compliance with FCC RF exposure limits in a portable configuration. At least 1.0 cm of separation distance between the Sierra Wireless 4G LTE Tri-Fi Hotspot and the user's body must be maintained at all times. This device must not be used with any other antenna or transmitter that has not been approved to operate in conjunction with this device.

WARNING (EMI) - United States FCC Information - This equipment has been tested and found to comply with the limits for a Class B computing device peripheral, 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.

CAUTION: Any changes or modifications not expressly approved by Sierra Wireless could void the user's authority to operate the equipment.

This device complies with Parts 15, 24, and 27 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.

Legal

This section contains important license and legal information.

[Patents](#)

[Licenses](#)

[Trademarks](#)

[Copyright](#)

[Limitation of Liability](#)

[Additional Information and Updates](#)

Patents

This product may contain technology developed by or for Sierra Wireless Inc.

This product includes technology licensed from QUALCOMM® 3G.

This product is manufactured or sold by Sierra Wireless Inc. or its affiliates under one or more patents licensed from InterDigital Group.

Licenses

A large amount of the source code to this product is available under licenses which are both free and open source. Most is available under the GNU General Public License.

The remainder of the open source software which is not under the GPL is available under one of a variety of more permissive licenses. Those that require reproduction of the license text in the distribution are listed in the sections that follow (starting with [iPerf License](#)).

[GNU General Public License](#)

[iPerf License](#)

[miniupnpd License](#)

[OpenSSL License](#)

[Original SSLeay License](#)

[PPPD License](#)

[PPPStats License](#)

[PPPDump License](#)

SSH2 License

UUID License

Zlib License

GNU General Public License

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect

making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions: a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change. b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License. c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following: a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or, c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However,

parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program 'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

iPerf License

Copyright (c) 1999-2007, The Board of Trustees of the University of Illinois

All Rights Reserved.

Iperf performance test

Mark Gates

Ajay Tirumala

Jim Ferguson

Jon Dugan

Feng Qin

Kevin Gibbs

John Estabrook

National Laboratory for Applied Network Research

National Center for Supercomputing Applications

University of Illinois at Urbana-Champaign

http://www.ncsa.uiuc.edu

Permission is hereby granted, free of charge, to any person obtaining a copy of this software (Iperf) and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimers.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimers in the documentation and/or other materials provided with the distribution.

Neither the names of the University of Illinois, NCSA, nor the names of its contributors may be used to endorse or promote products derived from this Software without specific prior written permission. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF

MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE CONTIBUTORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

miniupnpd License

Copyright (c) 2006-2008, Thomas BERNARD

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

- The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenSSL License

Copyright (c) 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed. I.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

PPPD License

Copyright (c) 1984-2000 Carnegie Mellon University. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name "Carnegie Mellon University" must not be used to endorse or promote products derived from this software without prior written permission. For permission or any legal details, please contact

    Office of Technology Transfer
    Carnegie Mellon University
    5000 Forbes Avenue
    Pittsburgh, PA 15213-3890
    (412) 268-4387, fax: (412) 268-7395
    tech-transfer@andrew.cmu.edu

4. Redistributions of any form whatsoever must retain the following acknowledgment:

    "This product includes software developed by Computing Services at Carnegie Mellon University (http://www.cmu.edu/computing/)."

CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Copyright (c) 1999-2004 Paul Mackerras. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. The name(s) of the authors of this software must not be used to endorse or promote products derived from this software without prior written permission.

3. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by Paul Mackerras <paulus@samba.org>".

THE AUTHORS OF THIS SOFTWARE DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

PPPStats License

Copyright (c) 1989 Regents of the University of California.

All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

PPPDump License

Copyright (c) 1999 Paul Mackerras. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name(s) of the authors of this software must not be used to endorse or promote products derived from this software without prior written permission.

4. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by Paul Mackerras <paulus@samba.org>".

THE AUTHORS OF THIS SOFTWARE DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL THE AUTHORS BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

SSH2 License

Copyright (c) 2004-2007 Sara Golemon <sarag@libssh2.org>

Copyright (C) 2006-2007 The Written Word, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Neither the name of the copyright holder nor the names of any other contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING

NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

UUID License

Copyright (c) 2004-2008 Ralf S. Engelschall <rse@engelschall.com>

Copyright (c) 2004-2008 The OSSP Project <http://www.ossp.org/>

This file is part of OSSP uuid, a library for the generation of UUIDs which can found at http://www.ossp.org/pkg/lib/uuid/

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THIS SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.

IN NO EVENT SHALL THE AUTHORS AND COPYRIGHT HOLDERS AND THEIR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Zlib License

Copyright (C) 1995-2010 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly

Mark Adler

Trademarks

SPRINT and the logo are trademarks of Sprint.

Sierra Wireless, the Sierra Wireless logo, TRU-Locate, and the red wave design are trademarks of Sierra Wireless.

Windows® is a registered trademark of Microsoft Corporation.

Mac and Mac OS are trademarks of Apple Inc., registered in the U.S. and other countries.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Wi-Fi, WPA, and WPA2 are registered marks of the Wi-Fi Alliance.

QUALCOMM® is a registered trademark of QUALCOMM Incorporated.

Other trademarks are the property of the respective owners.

Copyright

©2012 Sprint. All rights reserved. No reproduction in whole or in part without prior written approval.

Limitation of Liability

The information in this manual is subject to change without notice and does not represent a commitment on the part of Sierra Wireless. SIERRA WIRELESS AND ITS AFFILIATES SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUE OR ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE ANY SIERRA WIRELESS PRODUCT, EVEN IF SIERRA WIRELESS AND/OR ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR THEY ARE FORESEEABLE OR FOR CLAIMS BY ANY THIRD PARTY.

Notwithstanding the foregoing, in no event shall Sierra Wireless and/or its affiliates aggregate liability arising under or in connection with the Sierra Wireless product, regardless of the number of events, occurrences, or claims giving rise to liability, be in excess of the price paid by the purchaser for the Sierra Wireless product.

Additional Information and Updates

For up-to-date product descriptions, documentation, application notes, firmware upgrades, troubleshooting tips, and press releases, visit sierrawireless.com.

Index