JEXtream®

5G Home Router

User Manual

Model: CG890

NOTE: All pictures and drawings shown in this document are for illustration purpose only. Actual product may vary due to product variant and enhancement.

Contents

1

Getting Started

Overview
Components
Device Display

Overview

Thank you for choosing 5G Home Router CG890.

CG890 device will allow you to access the latest 5G and LTE networks for faster uploads and downloads. You can connect up to 32 Wi-Fi client devices to the Internet at once - laptops, tablets, smartphones and more via 2.4GHz and 5GHz Wi-Fi network. Also, ethernet ports are available for LAN or WAN connection.

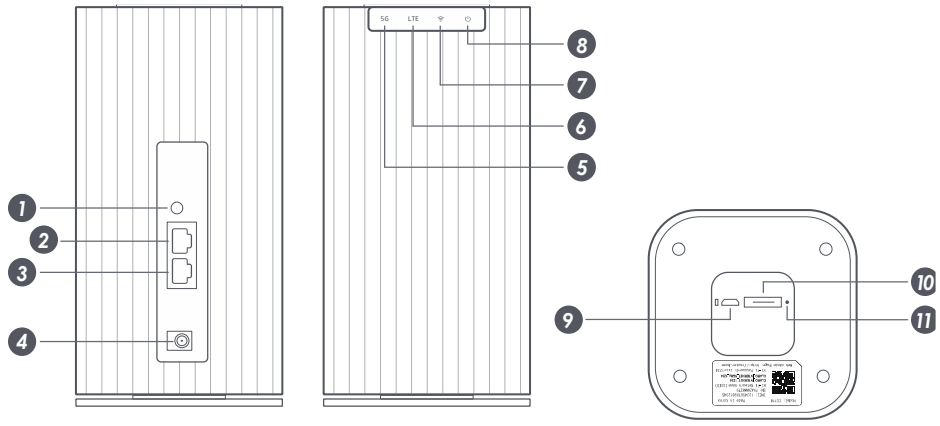
System Requirements

- Compatible with all IEEE802.11b/g/n/ac/ax Wi-Fi client devices.
- Works with the latest versions of most browsers*.

** It is recommended to use the latest versions of Internet browsers. Outdated versions may not be compatible with the CG890 Web Admin Home page, http://router.home*

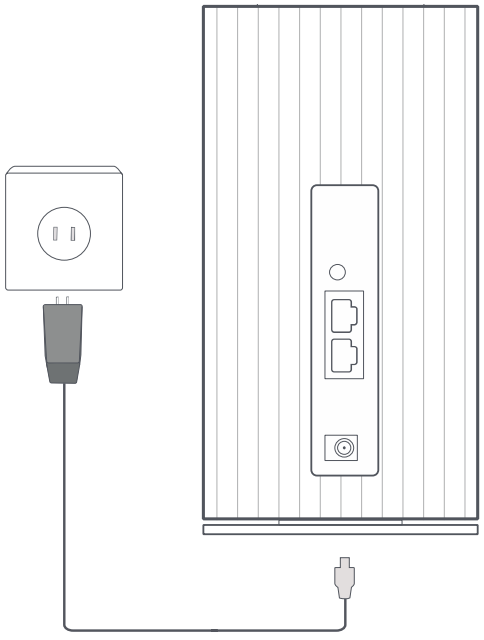
Components

Component Names



1. Power Button
2. WAN/LAN Port
3. LAN Port
4. Power Adapter Port
5. 5G Signal Indicator
6. LTE Signal Indicator
7. Wi-Fi Indicator
8. Power Indicator
9. Micro USB
10. Sim Card Slot
11. Reset Button

Status Indicators



Status Indicators		
5G Indicator	On	In Service
	Off	Not in 5G Coverage
LTE Indicator	On	In Service
	Off	LTE Not Available or 5G in Service
Wi-Fi Indicator	On	WiFi On
	Off	WiFi Off
Power Indicator	On	Power On
	Off	Power Off

2

Using Your CG890

Accessing the Network

Work effectively at your home or office with reliable broadband speed that the 5G and LTE service provides. You can connect to the internet at speeds fast enough to keep up to date on all your email correspondence, download attachments, and access your corporate intranet.

Using Your CG890 for the First Time

System Requirements

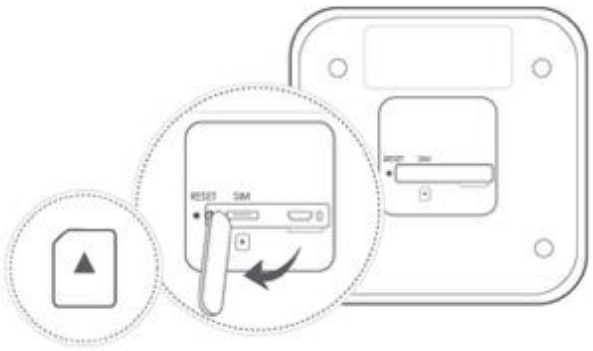
Your computer, tablet, or other wireless devices need Wi-Fi capability and Internet browser software only. Your CG890 is compatible with most major operating systems and the latest versions of browsers.

Installing the SIM Card

Your SIM (Subscriber Identity Module) card is a small rectangular plastic card that stores important information about your wireless service and activation plan.

1. Prepare appropriate SIM card size.

2. Open the rubber cover on the bottom of the device, insert the SIM card with a proper direction shown on the device until it clicks.



* To remove the SIM card, press it down once gently. The SIM card will pop out.

IMPORTANT! Do not bend or scratch your SIM card. Avoid exposing your SIM card to static electricity, water, or dirt. Whenever you insert or remove the SIM card, ensure your CG890 is powered off and is not connected to any power source. Never use tools, knives, keys, or any type of object to force the door open or to remove the SIM card.

Connecting to Your CG890

Power On/Off your CG890

- Power On: Press and hold the power button on the backside of the device, then release the button when the power indicator LED on the front side comes on.
- Power Off: Press and hold the power button on the backside of the device, then release the button when all 4 LED indicators on the front side blinks once.

Wi-Fi Name (SSID) and Password

You can find your device default Wi-Fi Name (SSID) and Password on the device label located on the bottom of the device.

Connecting to the Internet via Wi-Fi

1 Open the Wi-Fi application or controls on your computers or other Wi-Fi client devices that you want to connect to your CG890. Then find your CG890's Wi-Fi name.
2 Click **Connect** and enter the Password.

Connecting to the Internet via Ethernet

1 Connect an Ethernet Cable between CG890 Ethernet port (RJ45) and your computer or other Ethernet capable devices you want to connect.
2 Devices will be automatically connected to the Internet.

NOTE: For the best performance, we recommend using CAT6 (or above) Ethernet cables.

Using Your CG890 after Setup is Complete

Web Admin Home (http://router.home)

Your CG890 comes from the factory with security turned on. The default **Web Admin Home** page password is '**admin**'.

You can create your own **Web Admin Home** page password by signing into the **Web Admin Home** page. After you change your own **Web Admin Home** page password, you will be required to use the new password to log in the **Web Admin Home** page.

To change your **Web Admin Home** page password:

1 Connect your Wi-Fi client devices or Ethernet capable device to your CG890.
2 Run a web browser and open http://router.home
3 Click **Settings > Device > Web Interface**.

3

CG890 Settings

Managing Your Device Settings
Web Admin Home
Messages
Settings
About
Support

Managing Your Device

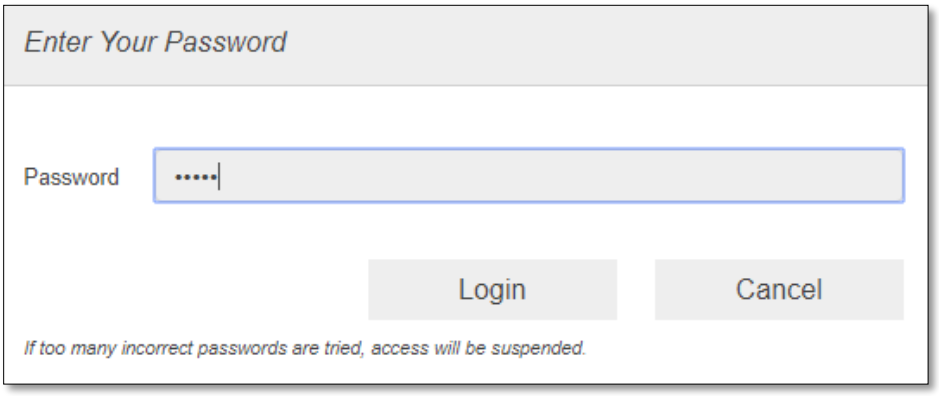
Access CG890 Router **Web Admin Home** page

You can access your router device information using an internet browse.

Access CG890 Router Web Admin Home page via internet browsers.

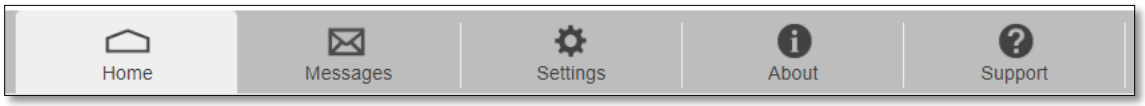
1 Connect your Wi-Fi client devices to the CG890.
2 Run an internet browser on your connected devices and open the **Web Admin Home** page by entering http://router.home
3 Click **Login** and enter the password**.** If you entered the correct password, the **Web Admin Home** page screen appears.

NOTE: The default password is '**admin**'. On your first login, you will be directed to change the password.



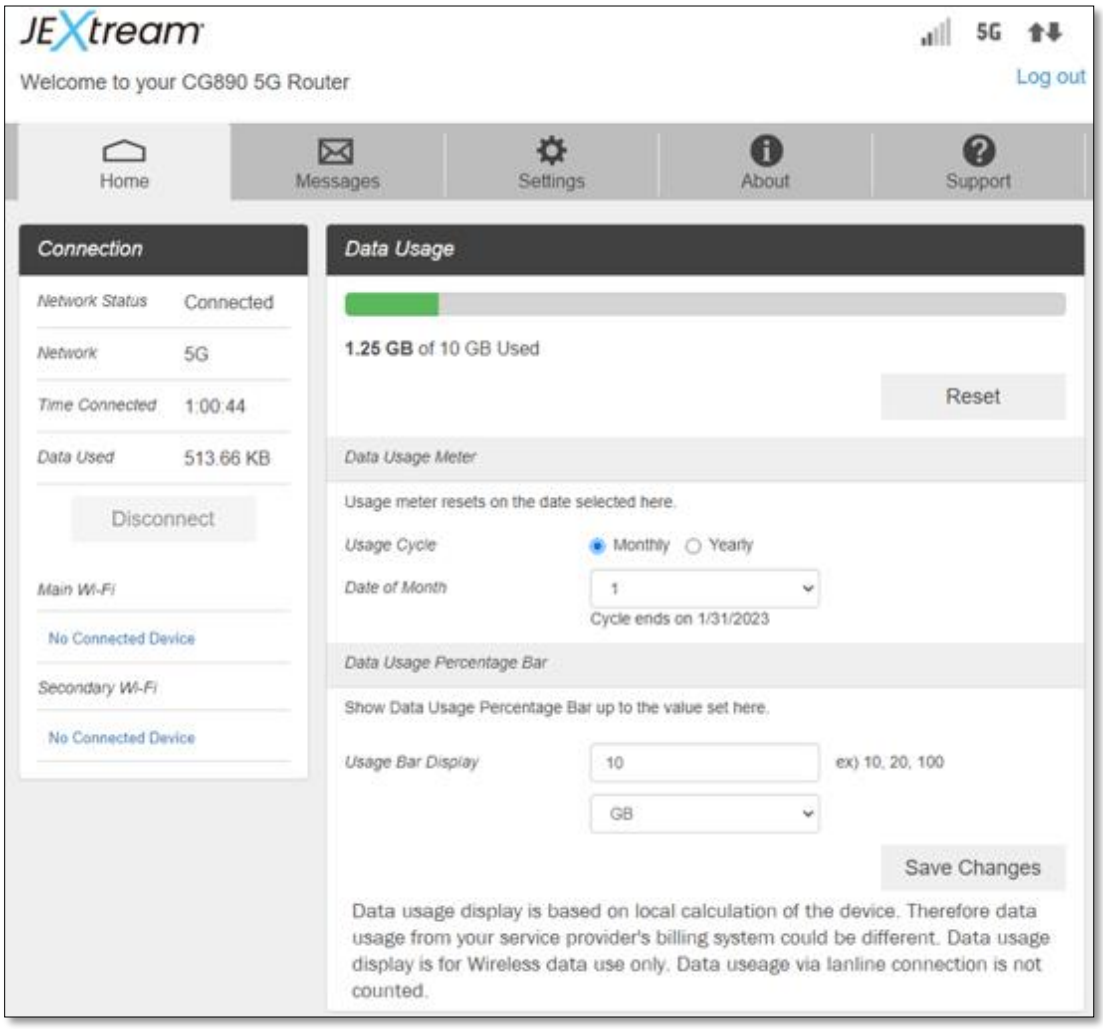
The **Web Admin Home** page allows you to quickly access all menu options for your CG890.

- **Home**
- **Messages**
- **Settings**
- **About**
- **Support**



Home

Check status of network connection and data usage on the **Web Admin Home** page.



Connection:

- Disconnect: Click Disconnect to disconnect the Internet. This button works only when **Auto Connect** function is disabled (**Settings > Mobile Network > Mobile Settings**). **NOTE**: **Auto Connect** function is enabled by default. If disabled, you need to login **Web Admin Home** page and press **Connect** button every time you power on the device.

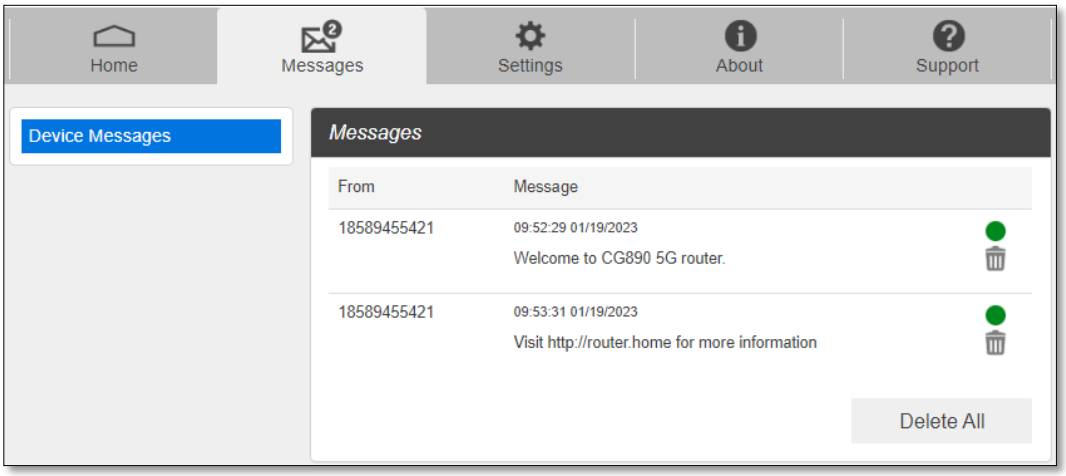
Data Usage:

- Reset: Click **Reset** to run data usage meter from zero again.
- Usage Cycle: Select Monthly or Yearly date for data usage meter to reset periodically. Press **Save Changes** to save the change made.
- Usage Bar Display: Enter the total amount of data for the data usage bar to display. Press **Save Changes** to save the change made. The data usage bar will be enabled and shows the data used / total amount of data. This is for display only and does not limit data usage.

Messages

Messages page displays SMS messages received.

To see the message received, click the message line. To delete a message, click the trash bin icon to the right of the message. To delete all messages, click **Delete All** button.



Settings

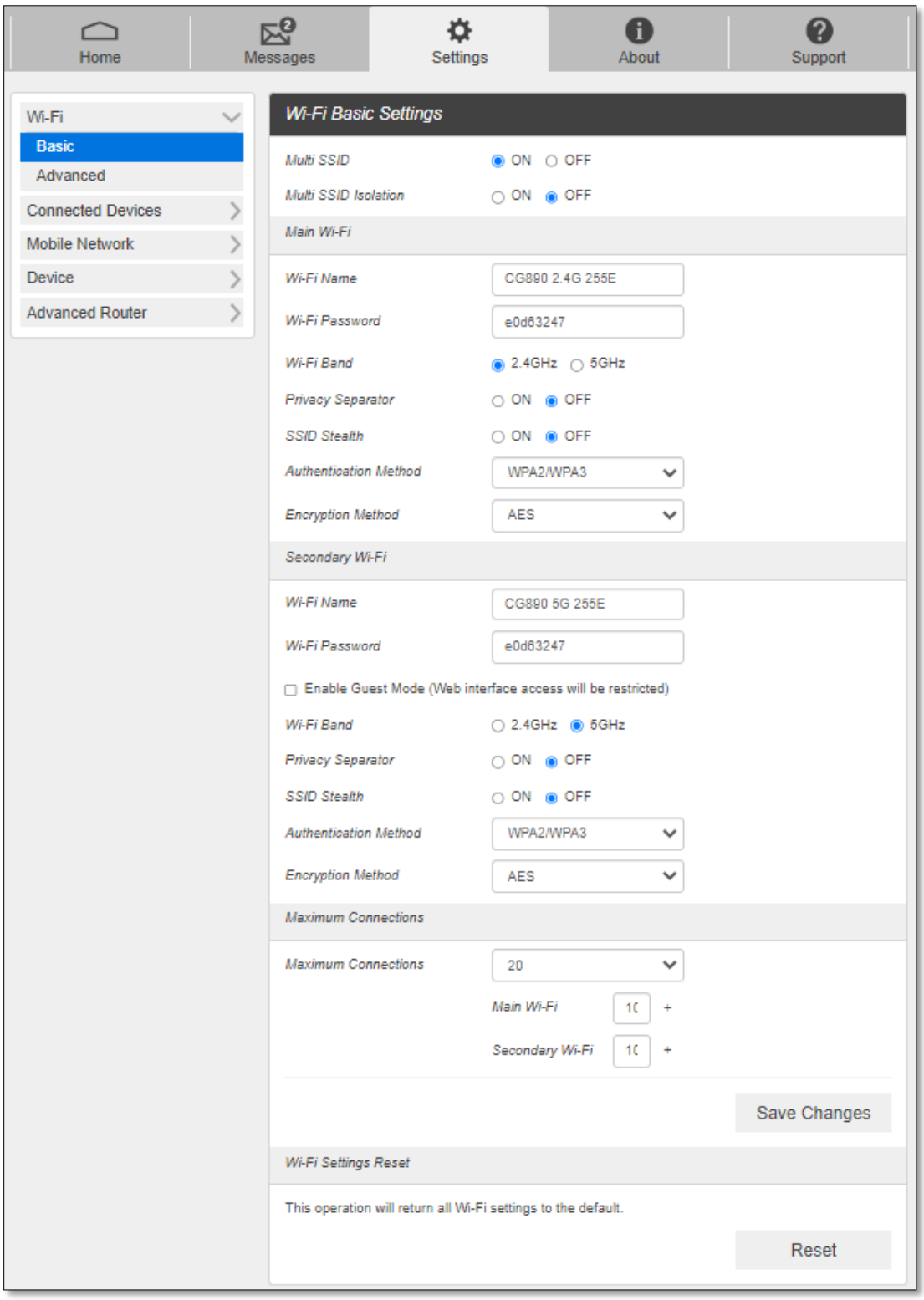
The **Settings** page has the following menu options.

- **Wi-Fi**
  - **Basic**
  - **Advanced**
- **Connected Devices**
  - **Wi-Fi**
  - **Ethernet**
- **Mobile Network**
  - **Mobile Settings**
  - **APN**
  - **SIM**
- **Device**
  - **Preferences**
  - **Web Interface**
  - **Software Update**
  - **Backup and Restore**
  - **System Logs**
- **Advanced Router**
  - **LAN settings**
  - **DNS Mode**
  - **MAC Filtering**
  - **Firewall IPv4**
  - **Firewall IPv6**

Wi-Fi

The **Wi-Fi** menu contains the following options:

- **Basic**: You can change basic Wi-Fi network settings.



- Multi SSID: Device is broadcasting Main Wi-Fi and Secondary Wi-Fi. Selecting OFF set the device to broadcast only Main Wi-Fi.

- Multi SSID Isolation: If On is selected, it prevents your devices from communicating across the Main Wi-Fi and Secondary Wi-Fi access points.

- Wi-Fi Name: Service Set Identifier (SSID). This is the Wi-Fi network name your router is broadcasting.

- Wi-Fi Password: The password needs to be at least 8 characters long.

- Wi-Fi Band: CG890 router supports both the 2.4 and 5GHz bands of Wi-Fi spectrum. Choose Wi-Fi Band depends on your Wi-Fi client device capability. 5GHz normally provides faster data speed than 2.4Ghz.

- Privacy Separator: If ON is selected, connected devices on the same Wi-Fi network cannot make Local Area Network communication.
  NOTE: if you connect WLAN printer to your CG890, Privacy Separator should be OFF to send file from a connected device to the printer

- SSID Stealth: If ON is selected, the Wi-Fi name will not be broadcasted. You need to manually enter the Wi-Fi name and the Password from your connected device to connect.

- Authentication Method: The authentication methods are described below. Default is WPA2/WPA3.

Mode	Description
WPA3	WPA3 is the latest, updated implementation of WPA2
WPA2/WPA3	Apply both the WPA2 and WPA3 scheme.
WPA/WPA2-PSK	Apply both the WPA-PSK and WPA2-PSK scheme.
WPA2-PSK	WPA-PSK is the securer version of WPA with implementation of the 802.11i standard.
OPEN	Authentication and encryption won't be performed. There are risks that private info will be intercepted or network will be used by unauthorized individuals.

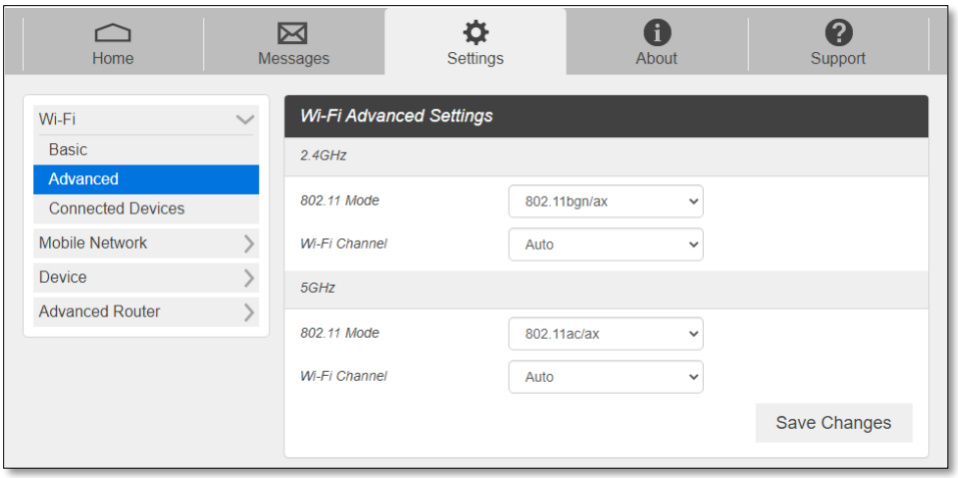
- Encryption Method: Select an encryption method from the drop-down list.
  NOTE: Changes to Authentication Method and Encryption Method could result in loss of Wi-Fi connection depending on your connected devices' Wi-Fi client security capabilities. Consult with your connected devices' user manuals before changing.

- Enable Guest Mode: Check this box to use the Secondary Wi-Fi as a Guest Wi-Fi network. If checked, devices connected to this Secondary Wi-Fi network are not able to access the **Web Admin Home** page

- Maximum Connections: Set the maximum number of the Wi-Fi connections Main and Guest Wi-Fi network allow simultaneously.

- Wi-Fi Settings Reset: Click the Reset button to reset all Wi-Fi settings to the default set.

- **Advanced**
  These advanced settings should only be changed for specific circumstances. Changes to the advanced settings could result in loss of Wi-Fi connection with your devices. Consult your devices' manuals for Wi-Fi specifications.



- 802.11 Mode: Select an 802.11 mode from the drop-down list.

- Wi-Fi Channel: Select a Wi-Fi channel from the drop-down list.

Connected Devices

The Connected Devices show the list of devices connected to your CG890 router.

- **Wi-Fi**

- Main Wi-Fi Devices – Names of the connected devices to the Main Wi-Fi network.

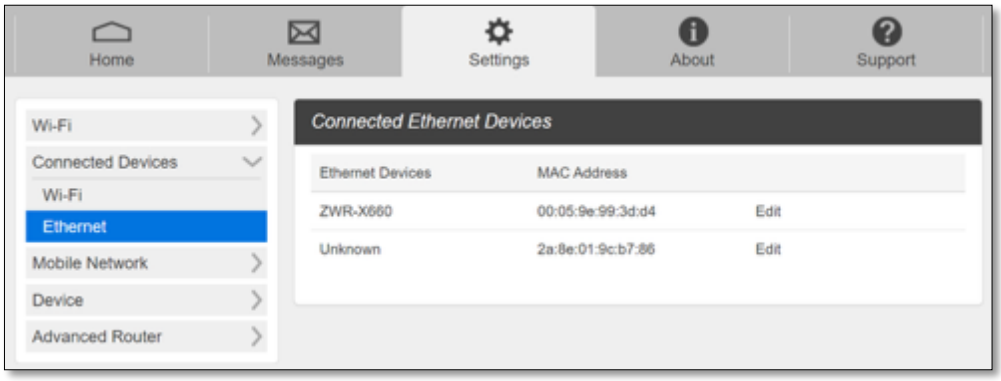
- Secondary Wi-Fi Devices – Names of the connected devices to the Secondary Wi-Fi network.

- MAC Address – The MAC address is a unique network identifier for this connected device.

To Edit a Connected Device Name:
1. Click on the **Edit**.
2. Update the name of the device and click **OK**.

To block connection:
1. Press **Block** on the device you want to block connection.
2. The devices blocked will be listed on the Blocked Devices. The blocked devices will not be allowed to connect to your CG890.
3. To unlock the device, press **Unblock**.

- **Ethernet**



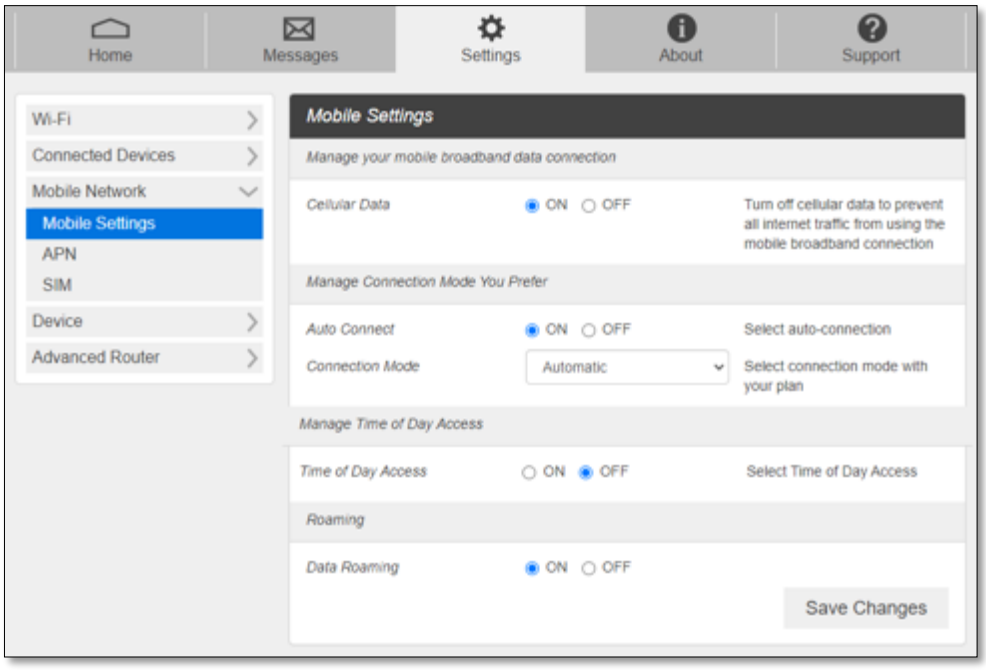
- Ethernet Devices – Names of the connected devices to the CG890 via Ethernet

- MAC Address – The MAC address is a unique network identifier for this connected device.

To Edit a Connected Device Name:
1. Click **Edit**.
2. Update the name of the device and click **OK**.

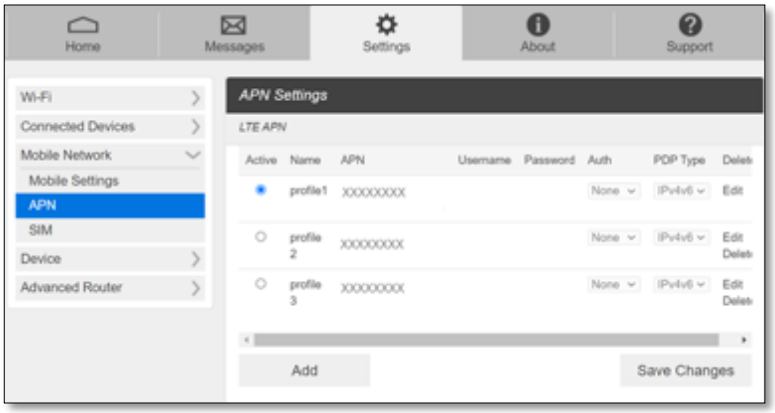
Mobile Network

Mobile Network menu help you to manage your wireless network settings.



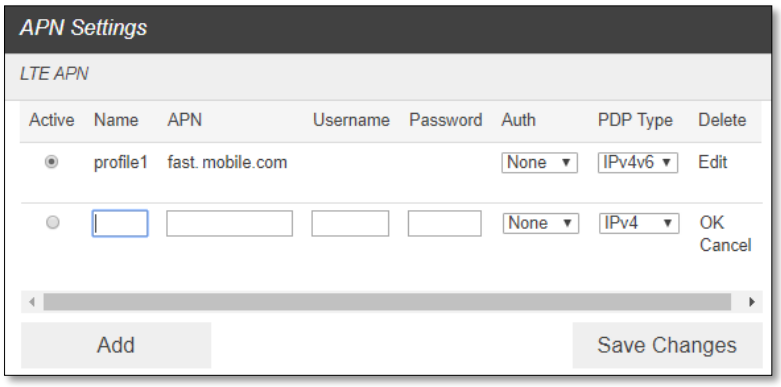
- **Mobile Settings**
  - Cellular Data: Selecting OFF disconnects all wireless data traffic to the network.
  - Auto Connect: Select ON to make your device automatically connects to the network when it is powered on. If OFF is selected, you need to login the **Web Admin Home** page to connect to the network next time the device is powered on.
  - Connection Mode: Select network type (5G, LTE, 3G) to connect to.
  - Time of Day Access: You can set the time span per day to allow data connection.
  - Data Roaming: Turn Data Roaming on or off.
    CAUTION! Allowing roaming could result in additional service charges. Please contact your service provider for more details.

- **APN**
  APN menu displays current APN settings. You can add/edit/delete APNs.



To add a new APN, follow the steps below:

1. Click **Add** to access the following page.



2. Enter the related parameters as described in the following table.

Parameters	Description
Name	Type the profile name.
APN	The Access Point Name (APN) is the name to set up a connection to the gateway between your service provider's cellular network and the public Internet.
Username	Username is used to obtain authentication from the ISP when the connection is established.
Password	Password is used to obtain authentication from the ISP when the connection is established.
Auth (Authentication)	Password Authentication Protocol (PAP) provides a simple method without encryption for the peer to establish its identity using a 2-way handshake. Challenge-Handshake Authentication Protocol (CHAP) is used to periodically verify the identity of the peer using a 3-way handshake.
PDP Type	PDP Type must be selected. IPv4, IPv6, IPv4v6.

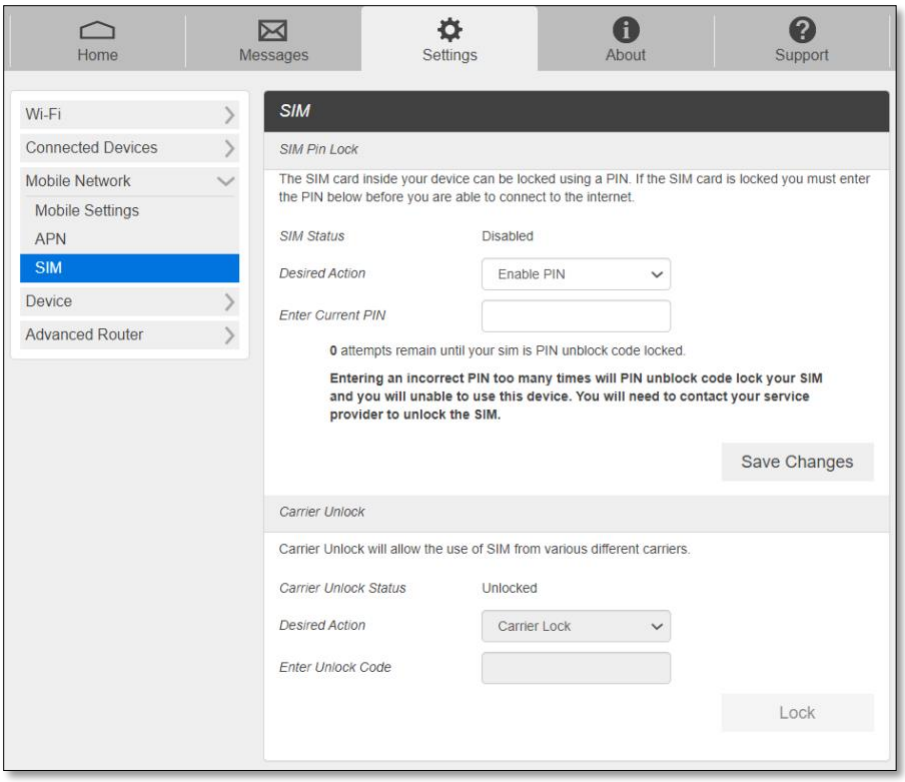
3. Click **Save Changes** to add the new APN.

Additional APN Options
- To select APN to use, click **Active** circle, then click **Save Changes**.
- To edit APN info, click **Edit**, change the settings, and then click **OK**.
- To delete APN, click Delete.

CAUTION! Changing APN information could result in connection failure. Please contact your service provider before changing APN only when needed.

- **SIM**
  - SIM Pin Lock

The SIM PIN Lock allows you to lock the SIM (Subscriber Identity Module) card in your device for additional security. If locked, the PIN code must be entered before the device can connect to the Internet whenever you power on your router.

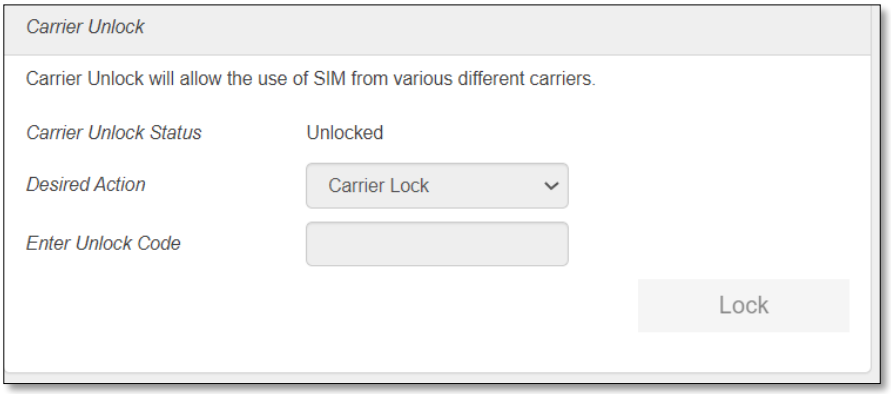


To set SIM Pin Lock, enter the current PIN and press **Save Changes**. The SIM Status will be changed to Enabled. Once the SIM PIN Lock is enabled, you need to login the **Web Admin Home** page and enter SIM PIN to connect to the mobile broadband network each time you power on your CG890.

NOTE: If you enter the wrong SIM PIN three times, your SIM will be disabled permanently until you enter the PUK code from your service provider.

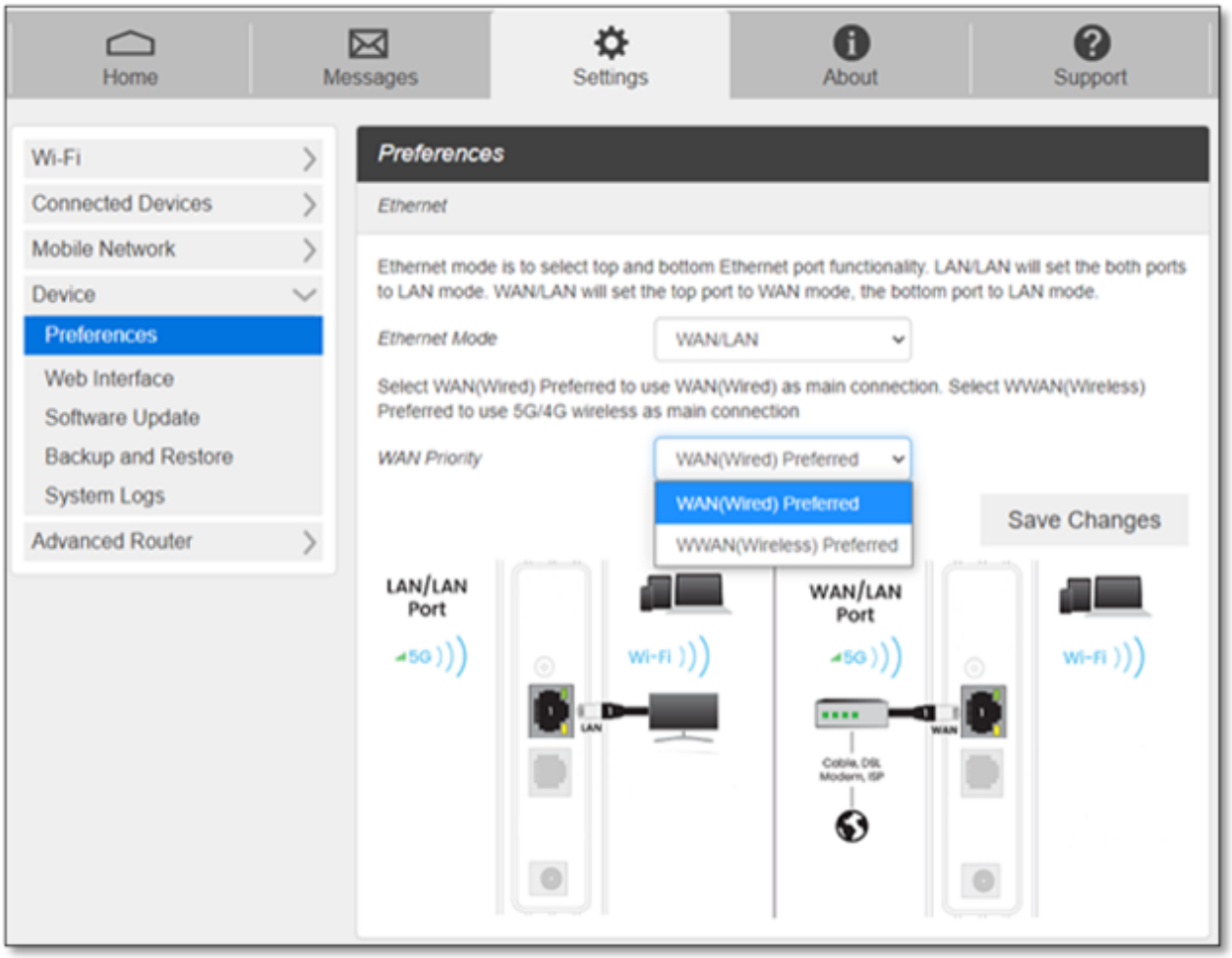
- Carrier Unlock

Your CG890 could be locked to recognize the SIM from your wireless service provider only. To use other SIMs from other wireless service provider, you need to unlock the carrier setting. The unlock code can be provided by your current wireless service provider.



Device

- **Preferences**



- Ethernet Mode: CG890 has two Ethernet ports. The top and bottom Ethernet Ports can be set as LAN/LAN mode (default) or WAN/LAN mode.
  - LAN/LAN mode**:** Default setting. CG890 will provide internet connection (LAN) to both Ethernet Ports.
  - WAN/LAN mode: CG890 will provide WAN connection to the top Ethernet Port. Users can connect Ethernet cable from other internet service provider (for example, landline ISP modem) to the top Ethernet Port.

- WAN Priority: This option appears only when Ethernet Mode is set to WAN/LAN mode to decide which connection to be used primarily. If the primary connection fails, it will be switched to the secondary connection.
  - WAN(Wired) Preferred**:** CG890 will provide internet connection primarily from the WAN port connection (Other modems connected to CG890) to its Wi-Fi and LAN networks.
  - WWAN(Wireless) Preferred: CG890 will provide internet connection primarily from your wireless service providers to its Wi-Fi and LAN networks.

- **Web Interface**

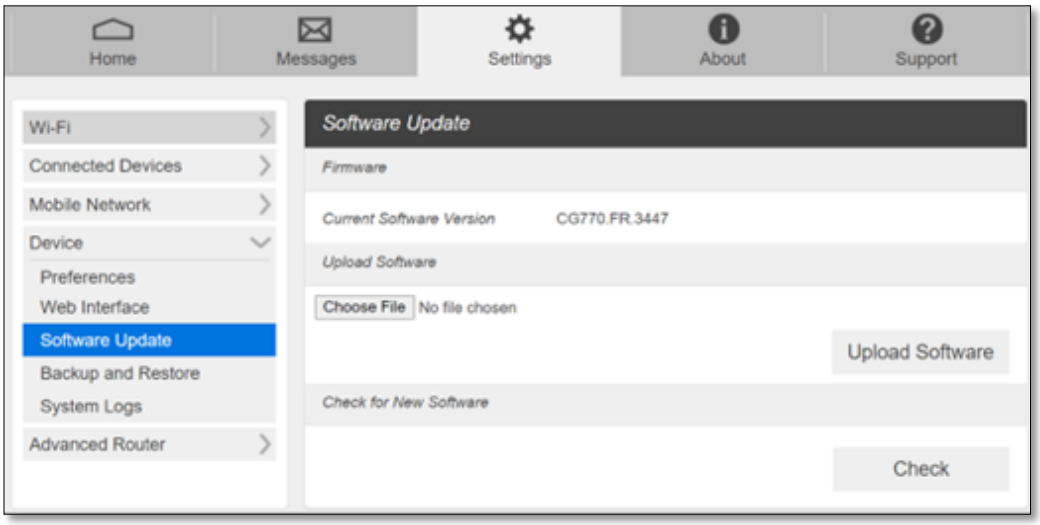
You can change **Web Admin Home** page login password.

How to change the password.

1. Enter the current password. (Default password is “admin”)
2. Enter the new password.
3. Enter the new password again.
4. Press **Save Changes**.

- **Software Update**

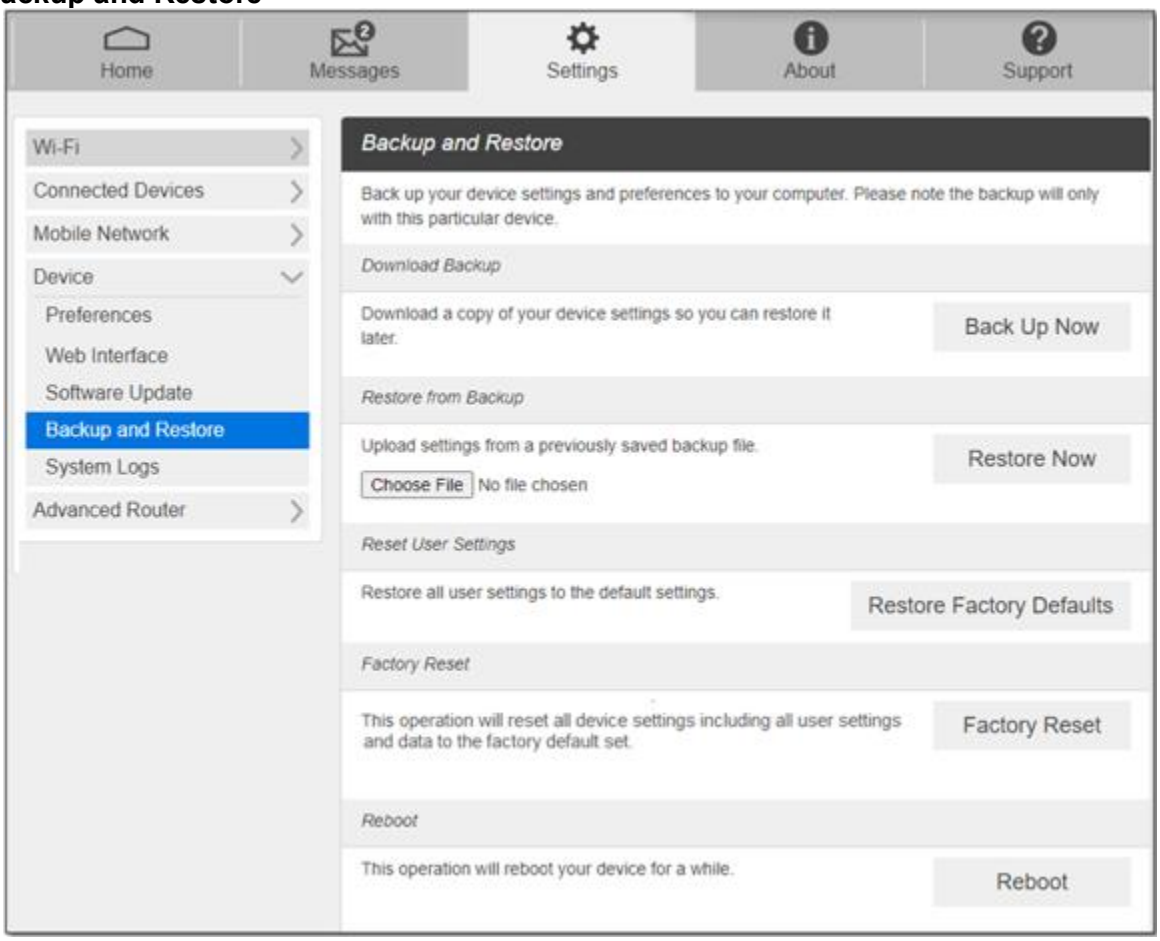
You can check current software version and check if there is a new update is available.



- Upload Software: Manual Update. In case you have a new software file provided by your service provider, save the file in your connected device, select the file by pressing **Choose File**, then press **Upload Software** to update your device software.

- Check for New Software: Automatic Update. Click **Check** button. Message windows will pop up and guide you through the update process.

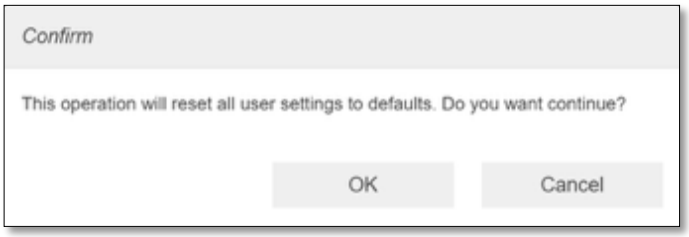
- **Backup and Restore**



- Download Backup: Click **Back Up Now**. The backup file automatically saved on your computer in Downloads folder.

- Restore from Backup: To restore the device settings from the backup file, follow the steps below:
  1. Click **Choose File** to select the backup file save in your computer.
  2. Click **Restore Now**. Your router will restart.

- Reset User Settings: To reset all user settings to its default settings, follow the steps below:
  1. Click **Restore Factory Defaults**.
  2. Click **OK** to confirm. Your router will restart.

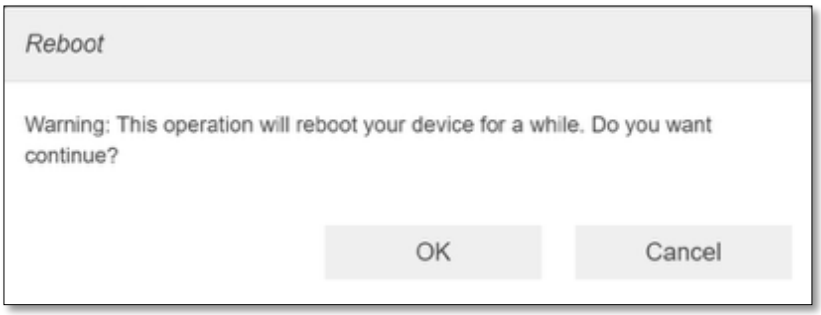


NOTE: This operation will reset all setting changes users made on the router.

- Factory Reset: To restore your device to its factory default settings, follow the steps below:
  1. Click **Factory Reset**.
  2. Click **OK** to confirm. Your router will restart.

NOTE: This operation will reset all device configuration settings and other setting changes users made on the router.

- Reboot: To restart your device, follow the steps below:
  1. Click **Reboot**.
  2. Click OK to confirm. Your router will restart.



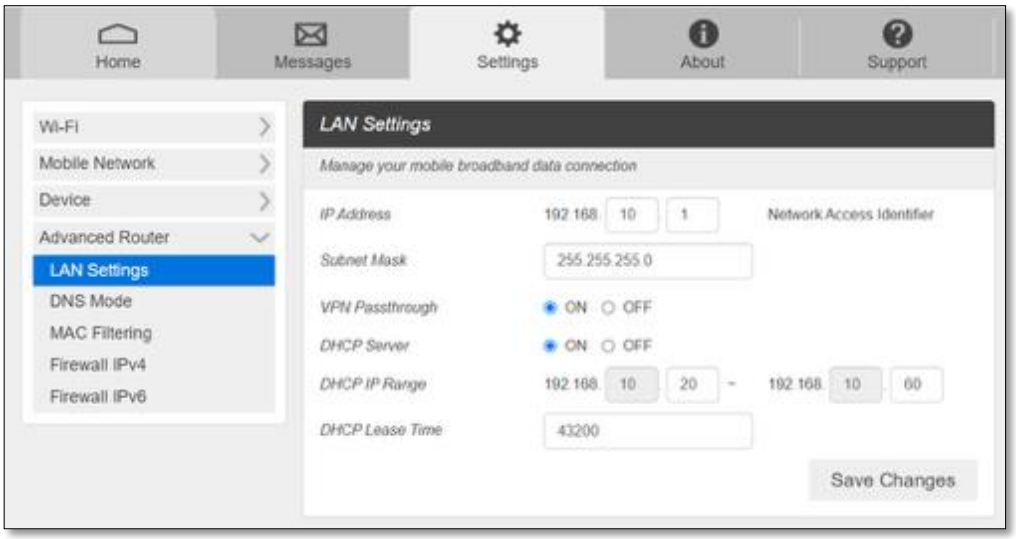
NOTE: This operation will just restart your router. No settings change.

Advanced Router

Configure LAN, DNS Mode, MAC Filtering, Firewall settings.

- **LAN Settings**

  LAN Settings shows current Local Area Network settings. You can change CG890 local network settings as needed.



- IP address – The IP address of the default gateway and your device **Web Admin Home** page.

- Subnet mask – The Subnet mask network setting for your device. The default value 255.255.255.0 is standard for small (class “C”) networks. If you change your LAN IP Address, ensure that you use the correct Subnet mask for the IP address range containing the LAN IP address.

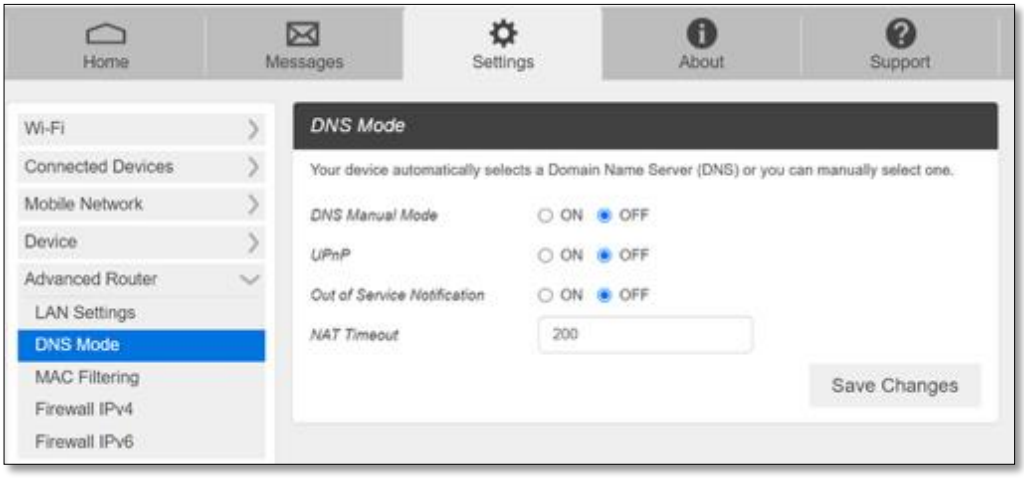
- VPN Passthrough– Allowing or preventing connected devices to establish a secure VPN connection. When turned **ON,** this feature allows VPN clients on your connected device to connect through your device to remote VPN servers. The default setting for this feature is **ON.** When turned **OFF**, the VPN clients are not allowed to connect.

- DHCP (Dynamic Host Configuration Protocol) server – The DHCP server is **ON** by default. When turned **ON**, your router automatically assigns local IPs to connected devices. When turned **OFF**, you will need to set it up manually from the device you want to connect to your router.

- DHCP IP Range – Defines the local IP range that DHCP server can assign to connected devices.

- DHCP Lease Time - DHCP lease time represents the period between when your connected device obtained its IP address from your device and the time when it expires. When the DHCP lease time expires, your connected device automatically releases IP address and asks your device to give it a new one.

- **DNS Mode**
  - DNS Manual Mode
    Your device automatically selects a Domain Name Server (DNS) assigned by your service provider. **DNS Manual Mode** option allows you to manually set up two DNS IP addresses you want to use instead.



To manually set a Domain Name Server:

1. Click the **ON** button to enable **Manual DNS**.
2. Enter the IP address of the first DNS in the **DNS Address 1** field.
3. Enter the IP address of the second DNS in the **DNS Address 2** field.
4. Click **Save Changes** button.

- UPnP: When it is ON, the devices connected to CG890 seamlessly discover each other's presence on the network and establish functional network services.

- NAT Timeout: The device will keep NAT entries in the translation table for this configurable length of time.

- **MAC Filtering**

The MAC filtering allows only selected devices to access your router's Wi-Fi network.

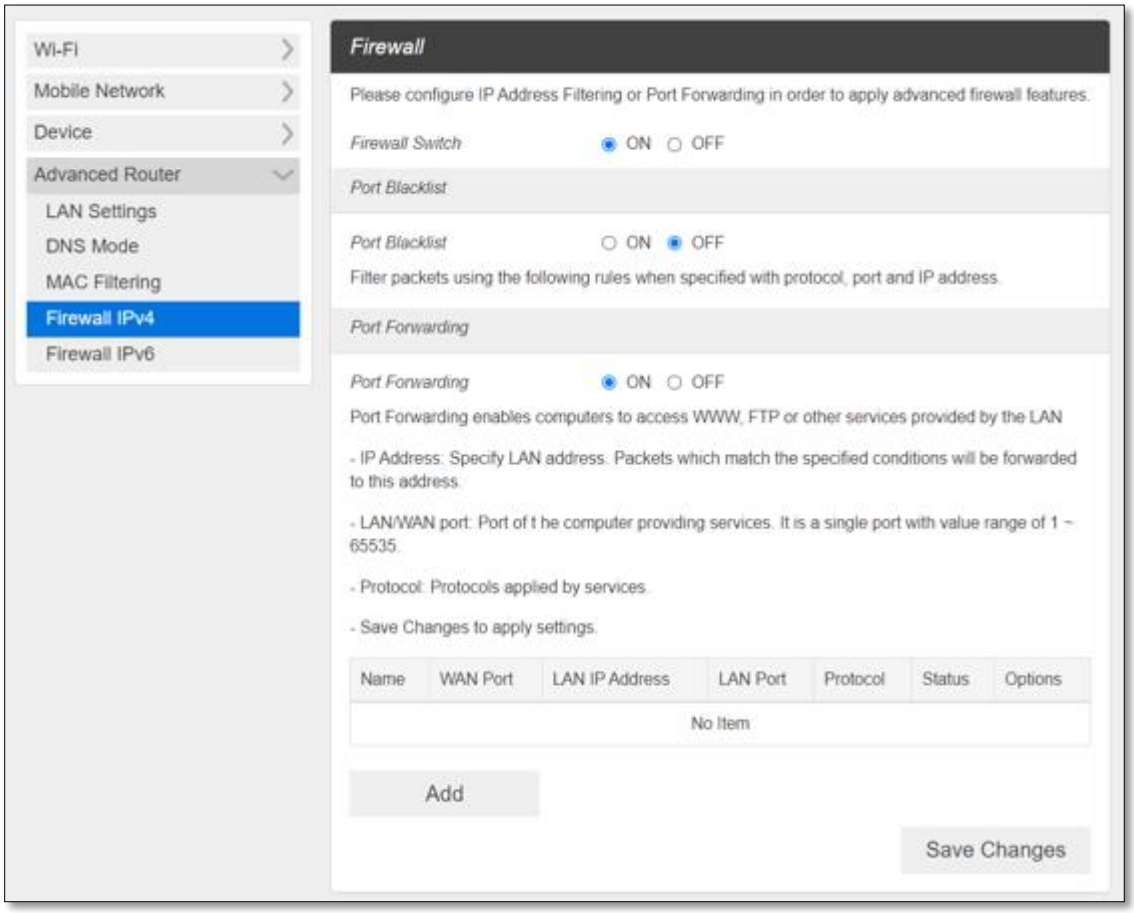
To enable MAC Filtering,

1. Select **ON**.
2. Press **Add** to add a line to enter permitted device name and MAC address, then click **OK**. When entering MAC addresses, use ":" as the separators (for example, c2:b5:d7:27:fb:9b). To add more, press **Add** to add another line.
3. When completed adding devices, press **Save Changes**.

NOTE: Once MAC filtering is set up, only listed device can access your router's Wi-Fi network. The MAC filtering has no effect on devices connected via Ethernet connection.

- **Firewall IPv4**

You may set up firewall rules to protect your network from virus and malicious activity on the Internet.



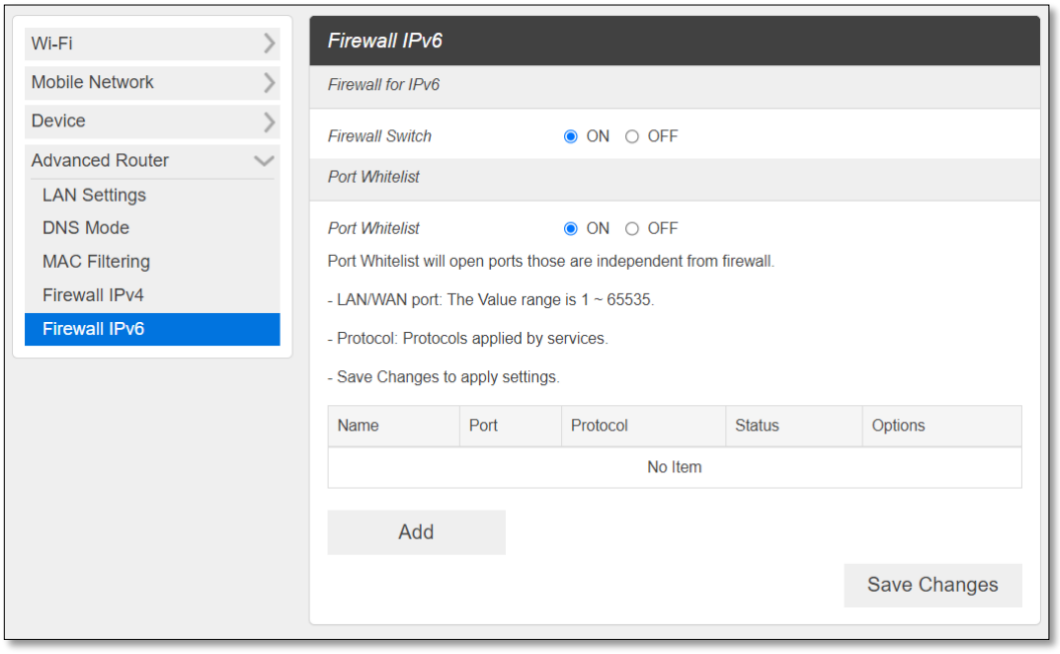
- Firewall Switch – To set up Port Blacklist and Port Forwarding, turn Firewall Switch **ON**. If Firewall Switch is **OFF**, both Port Blacklist and Port Forwarding settings are not active.

- Port Blacklist – You can block outbound forward packet by setting up a rule in the blacklist. To set up the rule,
  1. Turn **ON** Port Blacklist.

2. Press **Add** to create a line to setup a rule.
3. Enter the name of the rule you want to set up.
4. Enter IP address of the site you want to restrict outbound forward packet.
5. Enter Port number of the outbound forward packet.
6. Select Protocol and Status **ON/OFF**: **ON** means the rule is in active. **OFF** means the rule is not active.
7. Press **OK** to complete set up, then press **Save Changes**.

- Port Forwarding – You can allow inbound packet for specific port number by setting up port forwarding rule. To set up Port Forwarding,
  1. Turn **ON** Port Forwarding.
  2. Press **Add** to create a line to set up a rule.
  3. Enter the name of the rule you want to set up.
  4. Enter WAN port number of allowed inbound forward packet.
  5. Enter LAN IP address your connected device that is assigned by your device.
  6. Enter LAN port number of allowed inbound forward packet.
  7. Select Protocol and Status **ON/OFF**: **ON** means the rule is in active. **OFF** means the rule is not active.
  8. Press **OK** to complete set up, then press **Save Changes**.

- **Firewall IPv6**



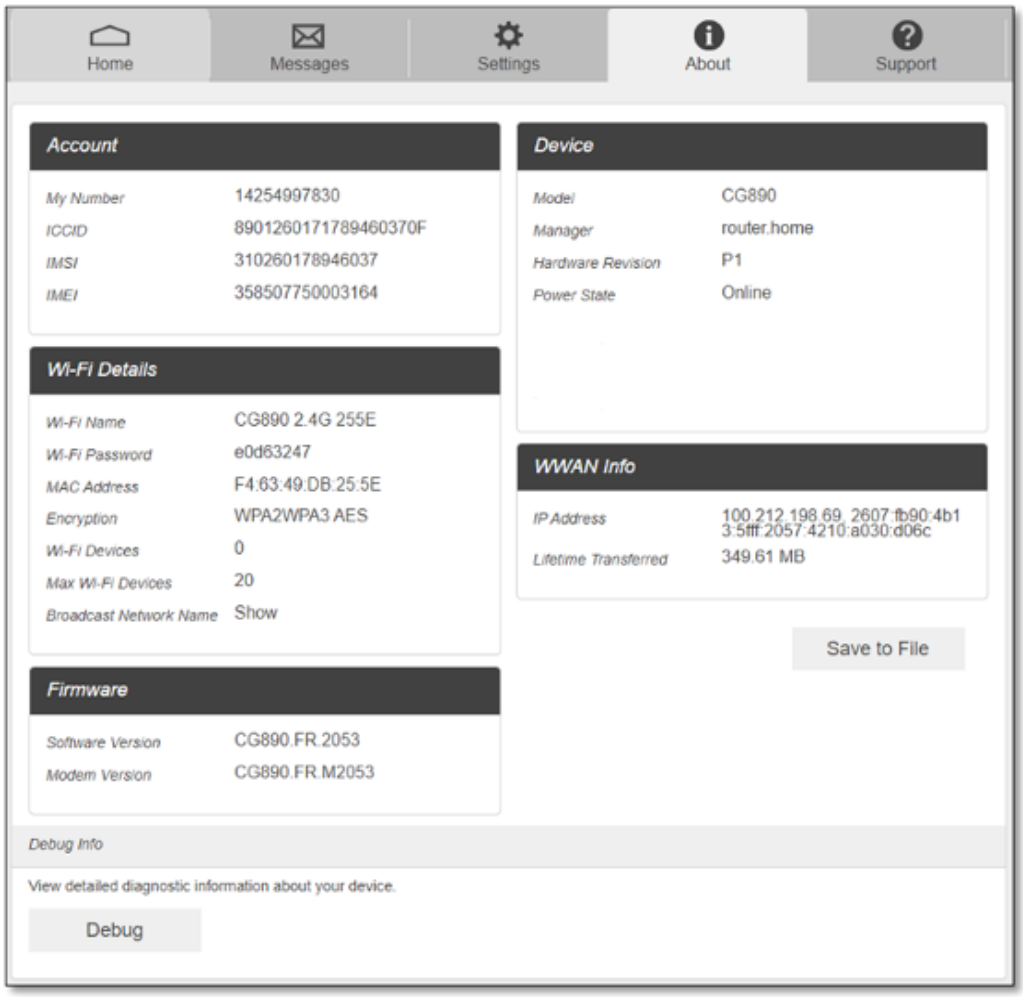
- Firewall Switch – To set up Port Whitelist, turn Firewall Switch **ON**. If Firewall Switch is **OFF**, Port Whitelist settings is not active. By default, the Firewall Switch for IPv6 is **ON** to restrict inbound forward packet from outside.

- Port Whitelist – You can allow inbound forward packet of specific port number by setting up Port Whitelist. To set up Port Whitelist,
  1. Turn **ON** Port Whitelist.
  2. Press **Add** to create a line to set up a rule.
  3. Enter the name of the rule you want to create.
  4. Enter the port number you want to allow inbound forward packet.
  5. Select Protocol and Status **ON/OFF**: **ON** means the rule is in active. **OFF** means the rule is not active.
  6. Press **OK** to complete set up, then press **Save Changes**.

About

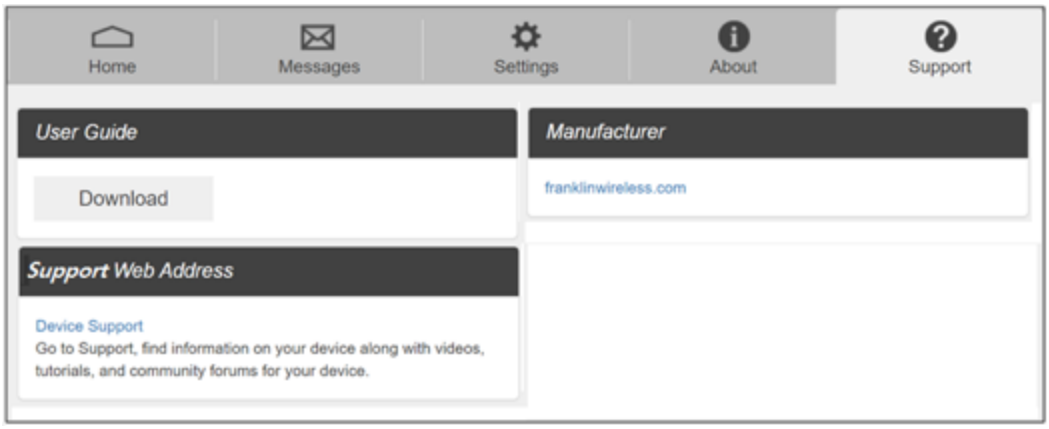
View your device's connection information, firmware information, WWAN information, Wi-Fi details and device information.

From the **Web Admin Home** page main screen, click the **About** tab to view the available information.



Support

Obtain support information from the **Web Admin Home** page Support Tab.



4

Troubleshooting

Overview
First Steps
Common Problems and Solutions

Overview

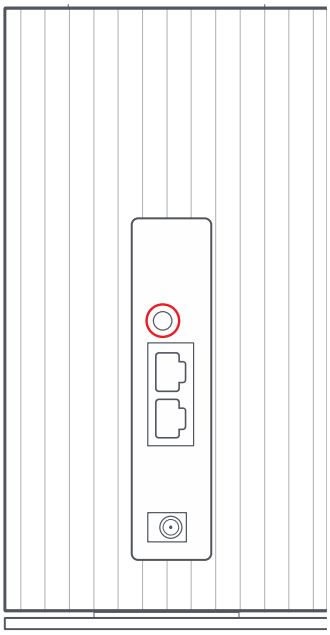
The following tips can help solve many common problems encountered while using the CG890.

First Steps

1 Make sure you are using your CG890 in the correct geographic region (within coverage).
2 Ensure that your wireless coverage extends to your current location by using the interactive Wireless Carrier's coverage map tool.
3 Ensure that you have an active service plan.
4 Restarting your computer and your CG890 device can resolve many issues.

Common Problems and Solutions

How do I perform Factory Reset?
Using the power button: Locate the power button on the backside of the device. Press the power button for about 10 seconds and release when the 4 LED indictors on the front side start blinking. Press the button one more time to confirm. Then, your CG890 will perform the factory reset and restart automatically.



Using **Web Admin Home** Page: Connect to your CG890, open **Web Admin Home** page (http://router.home) and log in. Select **Settings > Device > Backup and Restore** and Click **Factory Reset**.

Note: The CG890 router must be powered on when you perform factory reset. Factory reset will remove all your personal settings and turn your router to the factory default settings.

My CG890 got completely freeze and not responding. How do I perform hard reset?
Locate the reset button (small hole) on the bottom of the device. Using a sharp object such as a paper clip, press the reset button for more than 15 seconds and release. Then, your CG890 will perform hard reset and restart automatically.

Note: Hard reset is for rare cases that your router freezes and is not responding for unexpected errors. Hard reset just restarts your router and won't change any device setting you have made before.

I cannot connect to Wi-Fi after changing Wi-Fi password.
Your Wi-Fi client devices save the previously used Wi-Fi names associated with the passwords used to access the Wi-Fi name. When you change the Wi-Fi password only and keep the same Wi-Fi Name, the client devices try to connect to your CG890 using the Wi-Fi name and previous Wi-Fi password saved, causing Wi-Fi authentication error. Try to forget the Wi-Fi credentials saved in your client device and try again. It will prompt entering the new password.

I cannot access the Web Admin Home page, http://router.home
Ensure that Wi-Fi or Ethernet connection is established on your client device. Also, make certain that you are entering the correct full address of the **Web Admin Home** page, http://router.home correctly on your browser. If the problem still exists, try http://192.168.10.1.
If you changed the default gateway IP address from **Web Admin Home > Settings > Advanced Settings > LAN Settings** before, you need to use the default gateway IP address you changed to access the **Web Admin Home** page.

I cannot log into the Web Admin Home page, http://router.home
Ensure that you are entering the correct password to sign in. The default **Web Admin Home** page login password is "**admin**" unless you have previously changed. If your browser has cache memory or history login to same IP address, please clear the browser cache.
If you forgot the **Web Admin Home** page login password, perform factory reset by pressing the reset button on the bottom of the device.

5

Regulatory Information

Regulatory Statements
Safety Hazards

Regulatory Statements

FCC Equipment Authorization ID: XHG-CG890

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

SAR Information

The exposure standard for your device uses a unit of measurement called the Specific Absorption Rate ("SAR").

SAR is the unit of measurement for the amount of RF energy absorbed by the body when using a mobile device. Although the SAR is determined at the highest certified power level, the actual SAR value of the device while in operation can be well below the level reported to the FCC. This is due to a variety of factors including its proximity to a base station, the design of the device and other factors. What is important to remember is that each device meets strict Federal Government guidelines. Variations in SARs do not represent a variation in safety. All devices must meet the federal standard, which incorporates a substantial margin of safety. SAR values at or below the federal standard of 1.6 watts/kg (W/kg) are considered safe for use by the public. This product meets current FCC Radio Frequency Exposure Guidelines.

Additional details at FCC website:

www.fcc.gov/oet/ea

Body-Worn Operation

Please note this important safety information regarding radio frequency (RF) radiation exposure and near-body operation. To ensure compliance with RF exposure guidelines, the device must be used at least 10 mm from your body. Failure to observe this warning could result in RF exposure exceeding the applicable guideline limits.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the 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.

FCC CAUTION: Any changes or modification not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

NOTE: The Radio Frequency (RF) emitter installed in your modem must not be located or operated in conjunction with any other antenna or transmitter, unless specifically authorized by Franklin Wireless.

Safety Hazards

Follow Safety Guidelines
Always follow the applicable rules and regulations in the area in which you are using your device. Turn your device off in areas where its use is not allowed or when its use may cause interference or other problems.

Electronic Devices
Most modern electronic equipment is shielded from radio frequency (RF) signals. However, inadequately shielded electronic equipment may be affected by the RF signals generated by your device.

Medical and Life Support Equipment
Do not use your device in healthcare facilities or where medical life support equipment is located as such equipment could be affected by your device's external RF signals.

Pacemakers

- The Health Industry Manufacturers Association recommends that a minimum separation of six inches must be maintained between a device and a pacemaker in order to avoid potential interference with the pacemaker. These recommendations are consistent with the independent research by and recommendations of Wireless Technology Research. Persons with pacemakers should always follow these guidelines:
- Always keep the device at least six inches away from a pacemaker when the device is turned on.
- Place your device on the opposite side of your body where your pacemaker is implanted in order to add extra distance between the pacemaker and your device.
- Avoid placing a device that is on next to a pacemaker (e.g., do not carry your device in a shirt or jacket pocket that is located directly over the pacemaker).
- If you are concerned or suspect for any reason that interference is taking place with your pacemaker, turn your device OFF immediately.

Hearing Devices
When some wireless devices are used with certain hearing devices (including hearing aids and cochlear implants) users may detect a noise which may interfere with the effectiveness of the hearing device.

Use of Your Device while Operating a Vehicle
Please consult the manufacturer of any electronic equipment that has been installed in your vehicle as RF signals may affect electronic systems in motor vehicles.
Please do not operate your device while driving a vehicle. This may cause a severe distraction and, in some areas, it is against the law.

Use of Your Device on an Aircraft
Using your device during flight may violate FAA regulations. Because your device may interfere with onboard electronic equipment, always follow the instructions of the airline personnel and turn your device OFF when instructed to do so.

Blasting Areas
In order to avoid interfering with blasting operations, your device should be turned OFF when in a blasting area or in an area with posted signs indicating that people in the area must turn off two-way radios. Please obey all signs and instructions when you are in and around a blasting area.

Proper Battery & Adapter Use and Disposal

- Do not disassemble or open crush, bend or deform, puncture or shred.
- Do not modify or remanufacture, attempt to insert foreign objects into the battery, immerse or expose to water or other liquids, expose to fire, explosion or another hazard.
- Only use the battery for the system for which it is specified.
- Only use the battery with a charging system that has been qualified with the system per CTIA Certification Requirements for Battery System Compliance to IEEE 1725. Use of an unqualified battery or charger may present a risk of fire, explosion, leakage, or another hazard.
- Do not short circuit a battery or allow metallic conductive objects to contact battery terminals.
- Replace the battery only with another battery that has been qualified with the system per this standard, IEEE-Std-1725. Use of an unqualified battery may present a risk of fire, explosion, leakage or other hazard. Only authorized service providers shall replace the battery.
- Promptly dispose of used batteries in accordance with local regulations.
- Battery usage by children should be supervised.
- Avoid dropping the battery. If the battery is dropped, especially on a hard surface, and the user suspects damage, take it to a service center for inspection.
- Improper battery use may result in a fire, explosion or another hazard.
- The host device shall only be connected to CTIA certified adapters, products that bear the USB-IF logo or products that have completed the USB-IF compliance program.

Document Revision History

Revision: Rev.1.2
January 25, 2023

6

Glossary

Glossary

Term	Definition
LTE	Long-Term Evolution
5G	The 5th Generation Wireless Communication
802.11(b/g/n/ac/ax)	A set of WLAN communication standards in the 2.4GHz and 5Ghz frequency band.
Bps	Bits per second
Broadband	High capacity, high-speed transmission channel with a wider bandwidth than conventional modem lines.
DHCP	Dynamic Host Configuration Protocol
DHCP Server	A server or service with a server that assigns IP addresses.
DNS	Domain Name System
Firmware	A computer program embedded in electronic devices. Firmware usually contains operating code for the device.
GB	Gigabyte
Hotspot	A Wi-Fi (802.11b/g/n/ac) access point or the area covered by an access point.
HTTP	Hyper Text Transfer Protocol
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IP Type	The type of service provided over a network.
IP Address	The address of a device attached to an IP network.
ISP	Internet Service Provider
Kbps	Kilobits per second
LAN	Local Area Network
MAC Address	Media Access Control address
Mbps	Megabits per second
MSID	Mobile Station Identifier
Network Operator	The vendor who provides your wireless access.
Port	A virtual data connection used by a program to exchange data.
Port Forwarding	A process that allows remote devices to connect to a specific computer within a private LAN.
Port Number	A 16-bit number used by the TCP and UDP protocols to direct traffic.
PRL	Preferred Roaming List
Protocol	A standard that allows connection, communication, and data transfer between computing endpoints.
Proxy	A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address.
Router	A device that directs traffic from one network to another.
SIM	Subscriber Identification Module
SSID	Service Set Identifier
TCP/IP	Transmission Control Protocol/Internet Protocol
USB	Universal Serial Bus
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WWAN	Wireless Wide Area Network