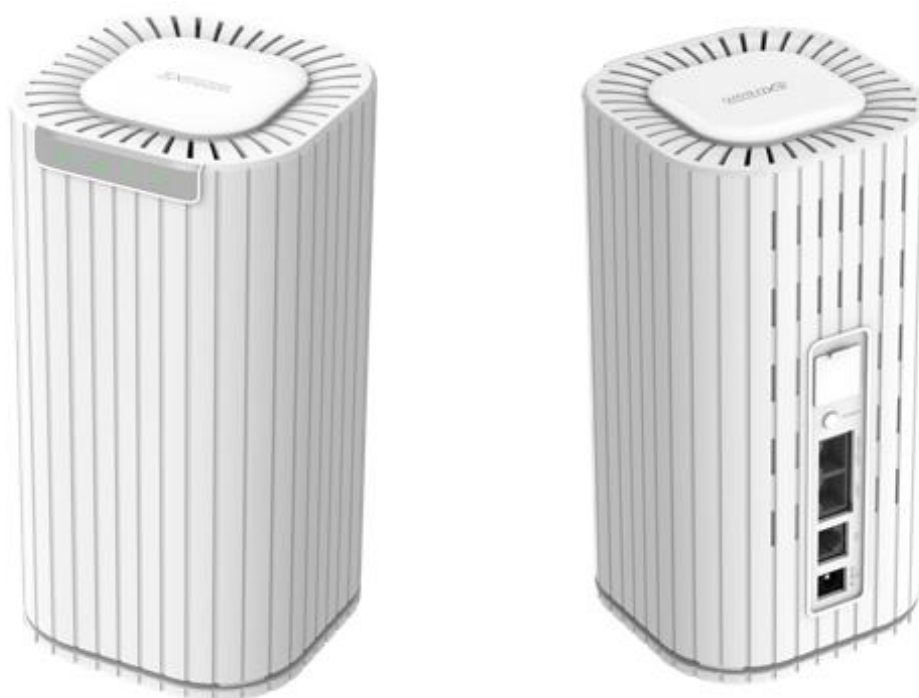


JEXtream®

5G Home Router

User Manual

Model: CG770



Claro

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

Contents

Getting Started	1
<i>Overview</i>	2
System Requirements.....	2
<i>Components</i>	3
<i>Battery Management</i>	4
Using Your CG770	5
<i>Accessing the Network</i>	6
<i>Using Your CG770 for the First Time</i>	6
System Requirements.....	6
Installing the SIM Card.....	6
Charging the Battery.....	7
<i>Connecting to Your CG770</i>	8
Wi-Fi Name (SSID) and Password.....	8
Connecting to the Internet via Wi-Fi.....	8
Connecting to the Internet via Ethernet.....	8
<i>Using Your CG770 after Setup is Complete</i>	9
<i>Updating Your CG770 software</i>	9
CG770 Settings	10
<i>Managing Your Router Device</i>	11
<i>Web Admin Home</i>	12
<i>Messages</i>	13
<i>Settings</i>	13
Wi-Fi.....	14
Connected Devices.....	16
Mobile Network.....	17
Device.....	21
Advanced Router.....	25
<i>About</i>	30
<i>Support</i>	31
Troubleshooting	32
<i>Overview</i>	33
<i>First Steps</i>	33
<i>Common Problems and Solutions</i>	33
Regulatory Information	35
<i>Regulatory Statements</i>	36
FCC Equipment Authorization ID: XHG-CG770.....	36
Body-Worn Operation.....	37

<i>Safety Hazards</i>	37
Glossary	40
<i>Glossary</i>	41

1

Getting Started

Overview
Components
Device Display
Battery Management

Overview

Thank you for choosing JEXtream® 5G Home Router CG770.

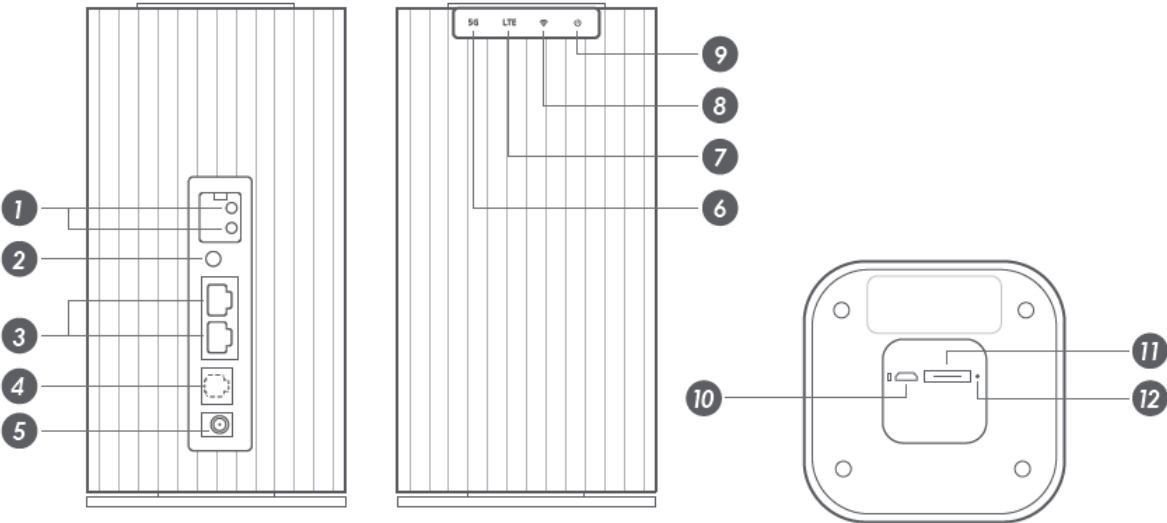
CG770 device will allow you to access the latest 5G and LTE networks for faster uploads and downloads. You can connect up to 20 Wi-Fi capable devices to the Internet at once - laptops, tablets, Smartphones and more via 2.4GHz and 5GHz Wi-Fi. Also, ethernet ports are available for LAN or WAN connection.

System Requirements

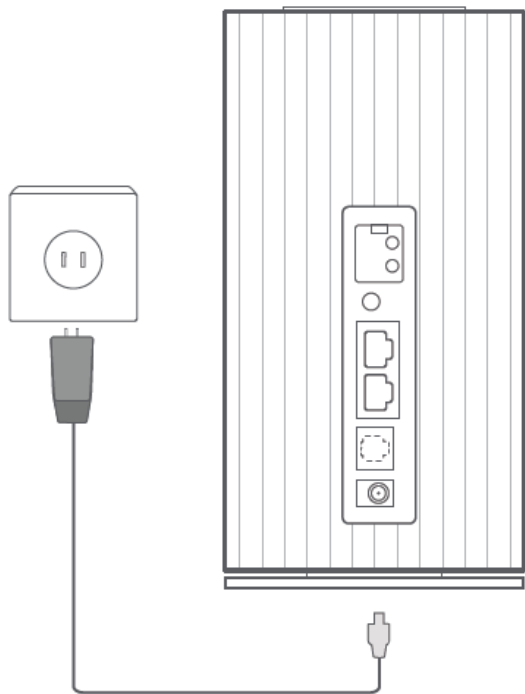
- Compatible with all IEEE802.11b/g/n/ac/ax Wi-Fi enabled devices.
- Works with the latest versions of most browsers*.

** It is recommended to use the latest versions of Internet browsers. Outdated versions may not be compatible with the CG770 Web Admin User Interface, <http://192.168.1.1> or <http://router.home>*

Components



- 1. External Antenna Port (TS-9B)
- 2. Power Button
- 3. RJ45 (LAN Port)
- 4. RJ11 (Telephone Port)
- 5. Power Adapter Port
- 6. 5G Signal Indicator
- 7. LTE Signal Indicator
- 8. Wi-Fi Indicator
- 9. Power/Battery Indicator
- 10. Micro USB
- 11. Sim Card Slot
- 12. Reset Button



CG770 LED		
5G Indicator	Green	In Service
	Off	Not in 5G Coverage
LTE Indicator	Green	In Service
	Off	No Service
Wi-Fi Indicator	Green	WiFi On
	Off	WiFi Off
Power/Battery Indicator	Green	Power On
	Blinking	Battery in use or charging

Battery Management

CG770 is equipped with a non-removable and rechargeable battery. It works from its charged battery alone, or when the device is plugged into a power source.

Note: Please do not attempt to open or disassemble your router device. Doing so may cause damage that voids your warranty.

IMPORTANT! Please use only an approved charger to charge your device. Improper handling of the charging port, as well as the use of an incompatible charger, may cause damage to your device and void the warranty.

2

Using Your CG770

Accessing the Network
Using Your CG770 for the First Time
Connecting to Your CG770
Using Your CG770 After Setup is Complete

Accessing the Network

Work effectively at your home or office with the 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 CG770 for the First Time

System Requirements

Your computer, tablet, or other wireless devices need Wi-Fi capability and Internet browser software only. Your CG770 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



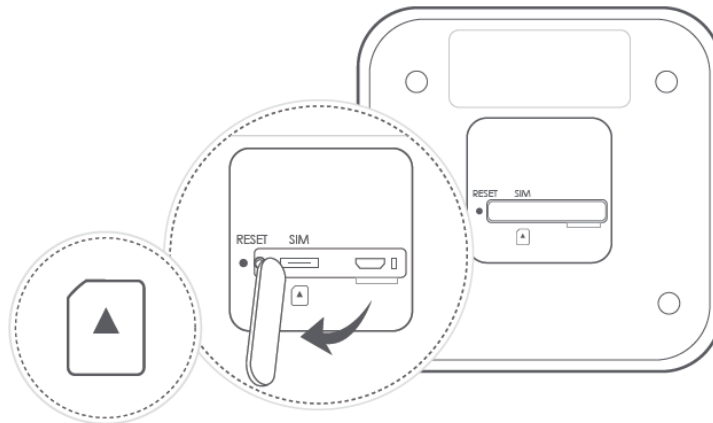
mini-SIM (2FF)



micro-SIM (3FF)



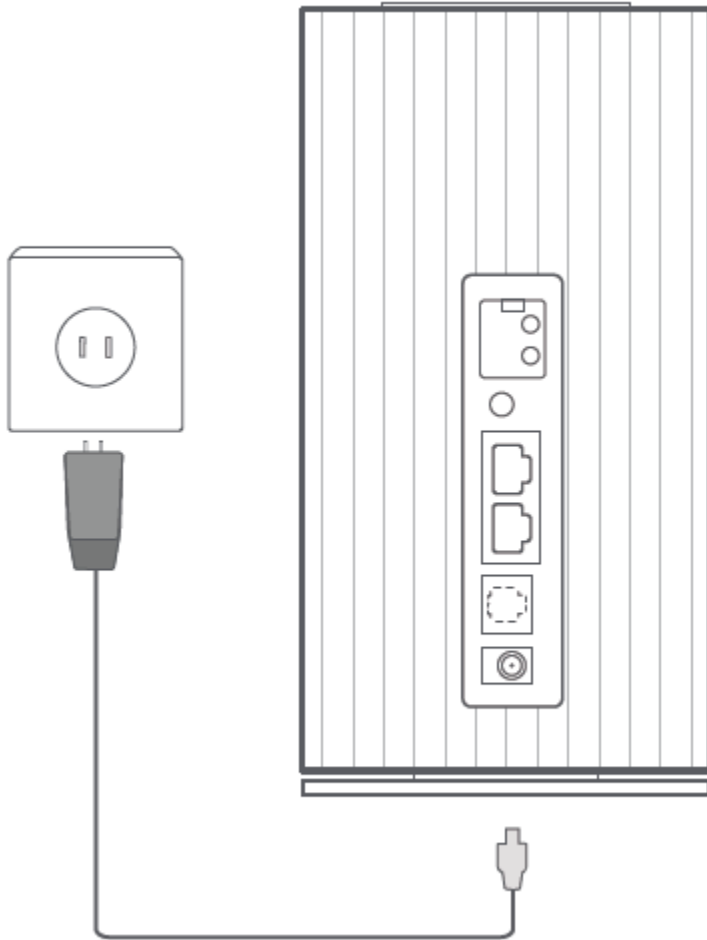
nano-SIM (4FF)



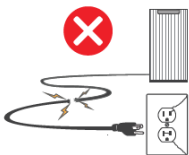
IMPORTANT! Do not bend or scratch your SIM card. Avoid exposing your SIM card to static electricity, water, or dirt. Whenever you insert or remove the SIM card, ensure your CG770 is powered off and is not connected to any power source. Never use tools, knives, keys, or any type of object to force the door open or to remove the SIM card.

Charging the Battery

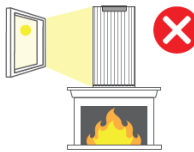
Long Press the power button after power adaptor is connected to wall plug. LED indicator should be on for status update. Please use a proper wall charger at all time.



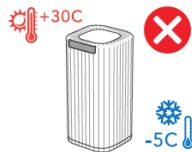
Avoid using damaged charger, cables or plugs.



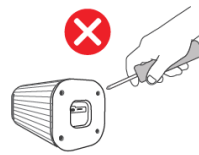
Avoid direct sunlight on device or placement near fire (i.e. heaters, fireplace or candles).



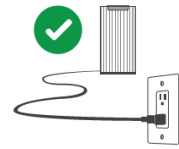
Avoid placing device where extreme temperatures are experienced.



Do not modify the hardware.



Please plug into the wall properly.



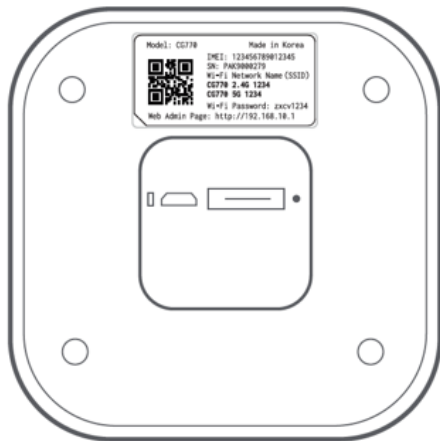
NOTE: Your CG770 is equipped with a non-removable rechargeable battery. Do not use any tools, sharp objects or any utensils when dealing with the battery. Doing so may cause damage that voids your warranty.

- It normally takes 3~5 hours, depending your power sources and device status to fully charge the battery.
- Battery life depends on the network, signal strength, temperature, features, and active connection time.
- When charging, keep your device near room temperature. Avoid placing device where extreme temperatures are experienced.
- Never leave the CG770 in an unattended vehicle due to uncontrolled temperatures that may be outside the desired temperatures for your device.

Connecting to Your CG770

Wi-Fi Name (SSID) and Password

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



Connecting to the Internet via Wi-Fi

- 1 Open the Wi-Fi application or controls on your laptop or Wi-Fi capable device that you want to connect to your CG770. Then find your CG770's Wi-Fi name.
- 2 Click **Connect** and enter the Password (located on the bottom of device or floating sticker)

Connecting to the Internet via Ethernet

- 1 Connect Ethernet Cable (RJ45) between CG770 and your laptop or Ethernet capable device.
- 2 Device will be automatically connected to internet

Using Your CG770 after Setup is Complete

Wi-Fi (or Ethernet) and Web Admin Page (<http://192.168.1.1> or <http://router.home>)

Your CG770 comes from the factory with security turned on. The default **Web Admin** page password is '**ClienteCLARO**'.

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

To change your **Web Admin** home password:

- 1 Connect your Wi-Fi capable device or Ethernet capable device to your CG770.
- 2 Open a web browser and enter <http://192.168.1.1> or <http://router.home>
- 3 Click **Settings > Device > Web Interface**.

Updating Your CG770 software

New software is updated automatically in the following scenarios.

- 1) If a new update is available, it will be downloaded in the background and wait to be applied on the next power off.
- 2) The device must have at least 40% battery or 20% on charger to apply an update.
- 3) If the device is on AC power all the time and an update is available, the device will download and wait to apply the update in 48 hours between the hours of 2 - 4am.
- 4) If there is traffic or data activity for at least 1 minute at the 2 - 4am window the device will wait until next day 2 - 4am window (24 hours later) to apply the update.

3

CG770 Settings

Managing Your Device Settings

Web Admin Home

Messages

Settings

About

Support

Managing Your Router Device

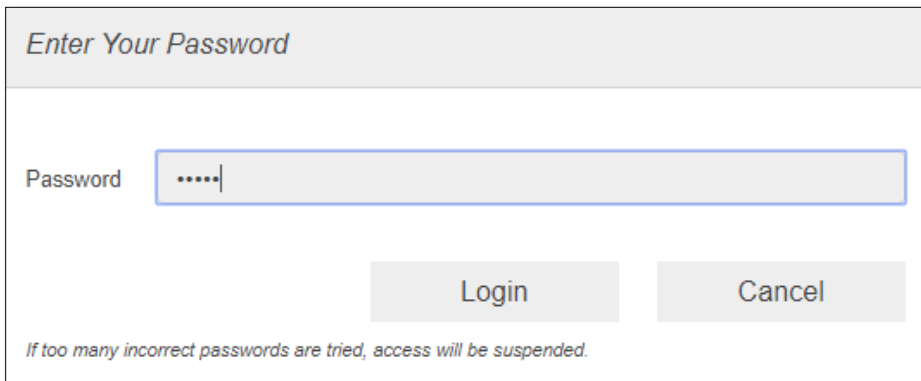
Access the CG770 Router **Web Admin** page

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

Access CG770 Router Web Admin page via internet browsers.

- 1 Connect your Wi-Fi capable device to the CG770.
- 2 Open a web browser on your connected device and open the Web Admin home page by entering <http://192.168.1.1> or <http://router.home>
- 3 Click **Login** and enter the password. If you entered the correct password, the Web Admin screen appears.

NOTE: The default password is 'ClienteCLARO'. On your first login, you will be directed to 'Change password'



The screenshot shows a login form titled "Enter Your Password". It features a text input field labeled "Password" containing five dots and a cursor. Below the input field are two buttons: "Login" and "Cancel". At the bottom of the form, there is a warning message: "If too many incorrect passwords are tried, access will be suspended."

Web Admin Home

The **Web Admin** page allows you to quickly access all menu options for your CG770.

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

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

- Disconnect: Click Disconnect to disconnect the Internet.
- Reset: Reset data usage.

The screenshot shows the JEXtream Web Admin interface for a CG770 5G Router. At the top, there is a navigation bar with icons for Home, Messages, Settings, About, and Support. The main content area is divided into two columns: Connection and Data Usage. The Connection column shows the network status as Connected, the network type as 5G, the time connected as 0:00:29, and the data used as 20.90 KB. There is a Disconnect button. The Data Usage column shows a progress bar and 20.90 KB Used, with a Reset button. Below the Data Usage section, there is a disclaimer about data usage calculation and a link to the settings page. The footer contains the copyright information: ©2021 Franklin Wireless Corp. All Rights Reserved.

Connection	
Network Status	Connected
Network	5G
Time Connected	0:00:29
Data Used	20.90 KB
Disconnect	
Main Wi-Fi	
No Connected Device	
Secondary Wi-Fi	
No Connected Device	

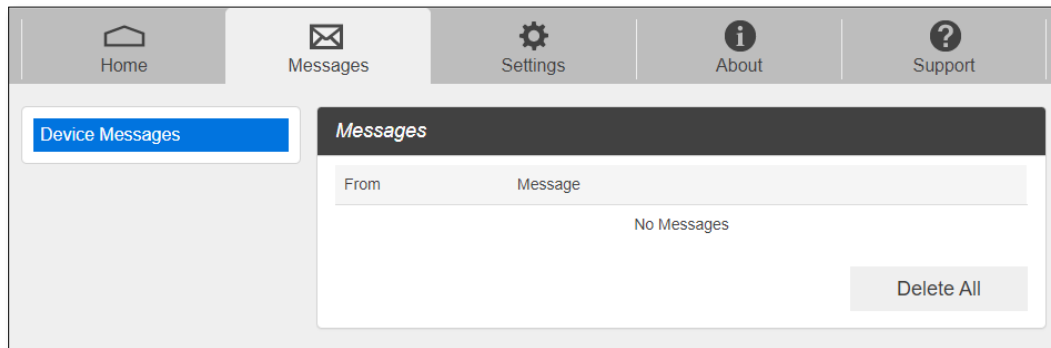
Data Usage
20.90 KB Used
Reset
Data usage calculation is based on the local device usage. Therefore, data usage might be different from billing system provided by the operator.
You can reset usage or change usage meter from settings page .

©2021 Franklin Wireless Corp. All Rights Reserved.

Messages

Messages page displays SMS messages sent to you by Wireless Carrier.

You can see the message contents by pressing the **Messages** menu on your **Web Admin** home page. To delete a selected message, click the trash bin icon to the right of the message date and timeline. To delete all messages, click **Delete All Messages** 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**
 - **Data Usage**
 - **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.

The screenshot displays the 'Wi-Fi Basic Settings' interface. At the top, there are navigation tabs: Home, Messages, Settings, About, and Support. A left sidebar menu shows 'Wi-Fi' expanded with 'Basic' selected, along with 'Advanced', 'Connected Devices', 'Mobile Network', 'Device', and 'Advanced Router'. The main content area is titled 'Wi-Fi Basic Settings' and is divided into several sections:

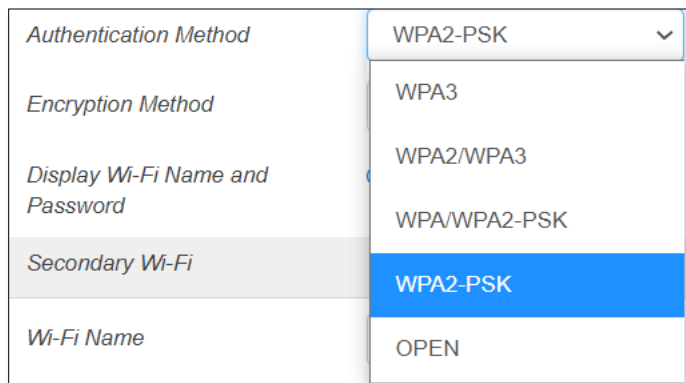
- Multi SSID:** ON OFF
- Multi SSID Isolation:** ON OFF
- Main Wi-Fi:**
 - Wi-Fi Name: CG770 2.4G 0800
 - Wi-Fi Password: 59806244
 - Wi-Fi Band: 2.4GHz 5GHz
 - Privacy Separator: ON OFF
 - SSID Stealth: ON OFF
 - Authentication Method: WPA2-PSK
 - Encryption Method: AES
- Secondary Wi-Fi:**
 - Wi-Fi Name: CG770 5G 0800
 - Wi-Fi Password: 59806244
 - Enable Guest Mode (Web interface access will be restricted)
 - Wi-Fi Band: 2.4GHz 5GHz
 - Privacy Separator: ON OFF
 - SSID Stealth: ON OFF
 - Authentication Method: WPA2-PSK
 - Encryption Method: AES
- Maximum Connections:**
 - Maximum Connections: 20
 - Main Wi-Fi: 10 +
 - Guest Wi-Fi: 10 +

At the bottom right, there is a 'Save Changes' button. Below this, a section titled 'Wi-Fi Settings Reset' contains the text 'This operation will return all Wi-Fi settings to the default.' and a 'Reset' button.

- **Multi SSID:** Device is broadcasting Main Wi-Fi and Secondary Wi-Fi as default. User can stop the Multi-SSID broadcasting by selecting No.
- **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). To change it, enter a string less than 32 characters as the name for your wireless local area network (WLAN).
- **Wi-Fi Password:** To change, enter the new Wi-Fi password. The password needs to be at least 8 characters long.
- **Wi-Fi Band:** It supports both the 2.4 and 5GHz bands of Wi-Fi spectrum for top throughput. You can choose Wi-Fi Band depends on your preference.
- **Privacy Separator:** If ON is selected, your devices on the same Wi-Fi Name can't make Local Area Network communication.

NOTE: if you connect WLAN printer to your CG770, Privacy Separator should be OFF to send file from your PC 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 connect.
- **Authentication Method:** The authentication methods are described below.



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.

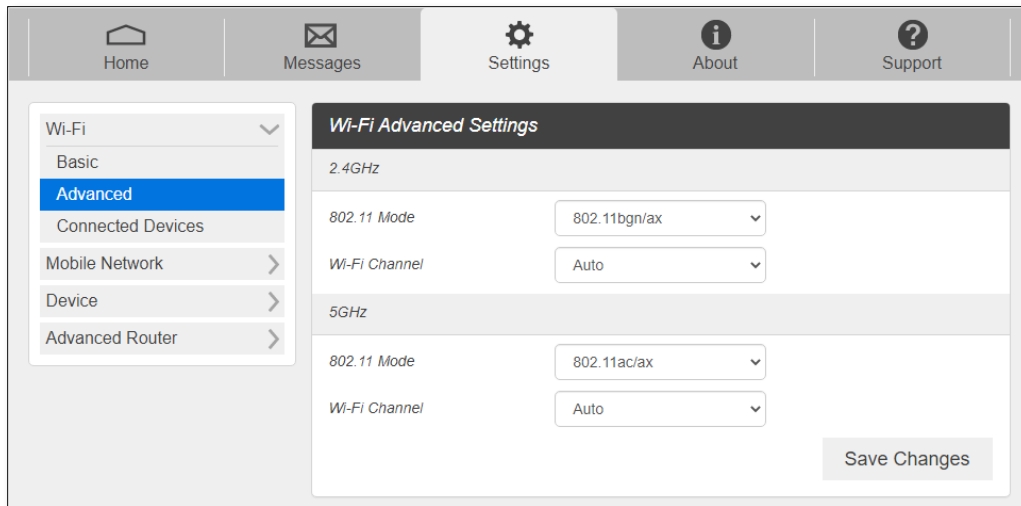
- **Encryption Method:** Select an encryption method from the drop-down list.
- **Maximum Connections:** Choose the maximum number of the devices which connect to your device simultaneously. You can also click the right or left arrow to distribute

the maximum number of the connected devices between the Main Wi-Fi and the Guest Wi-Fi.

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

- **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.

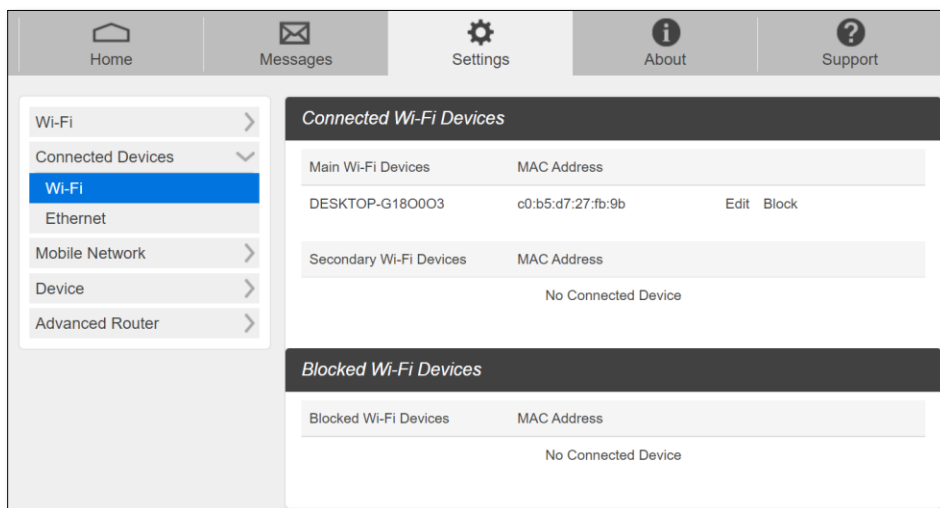


- **802.11 Mode:** Select an 802.11 mode from the drop-down list.
- **Wi-Fi Channel:** Select a Wi-Fi channel from the drop-down list.

Connected Devices

The Connected Devices menu contains the following options:

- **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.

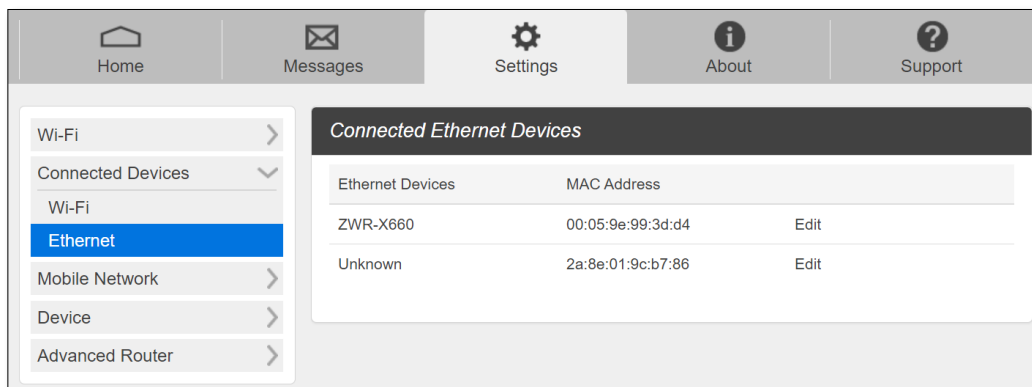
To Edit a Connected Device:

1. Click on the **Edit**. A page opens, allowing you to edit the name of the device.
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 device blocked will be listed on the Blocked Devices. The blocked devices will not be allowed to connect to your CG770.
3. To unlock the device, press **Unblock**.

- Ethernet



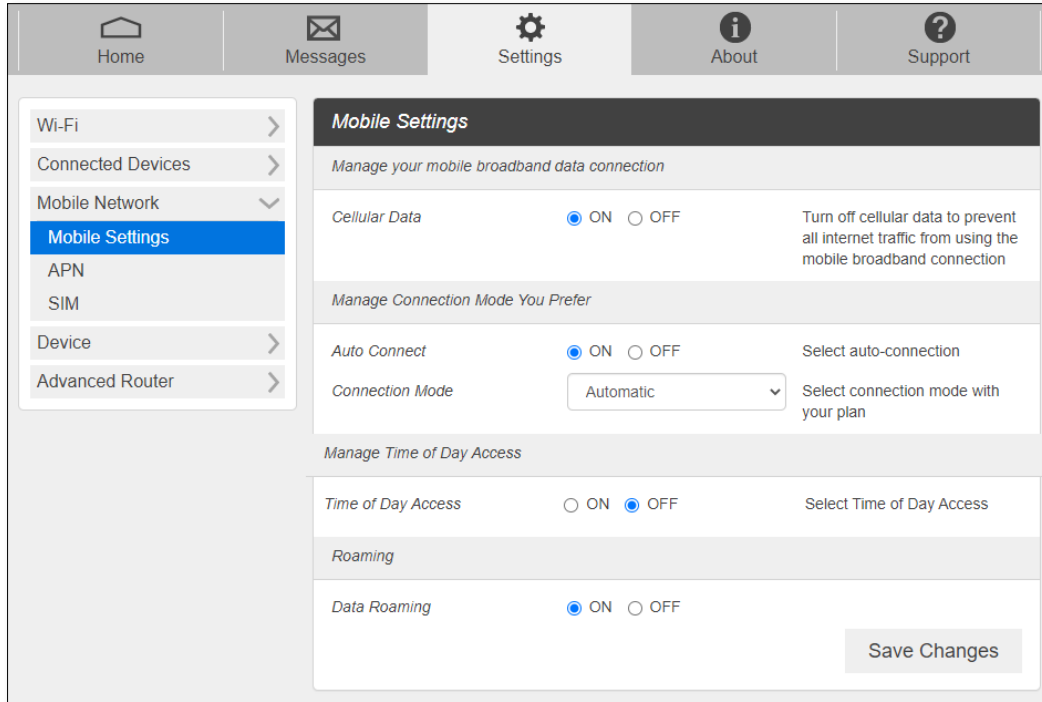
- Ethernet Devices – Names of the connected devices to the CG770 via Ethernet
- MAC Address – The MAC address is a unique network identifier for this connected device.

To Edit a Connected Device:

1. Click on the **Edit**. A page opens, allowing you to edit the name of the device.
2. Update the name of the device and click **OK**.

Mobile Network

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



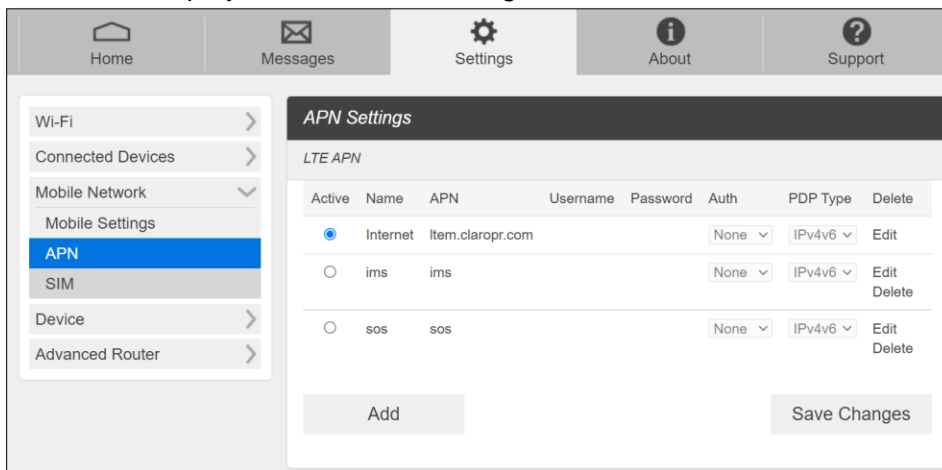
- **Mobile Settings**

- Cellular Data: Selecting OFF disconnect all data traffic to the network.
- Auto Connect: Select ON or OFF 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 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 new APNs.



To add a new APN, follow the steps below:

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

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.

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

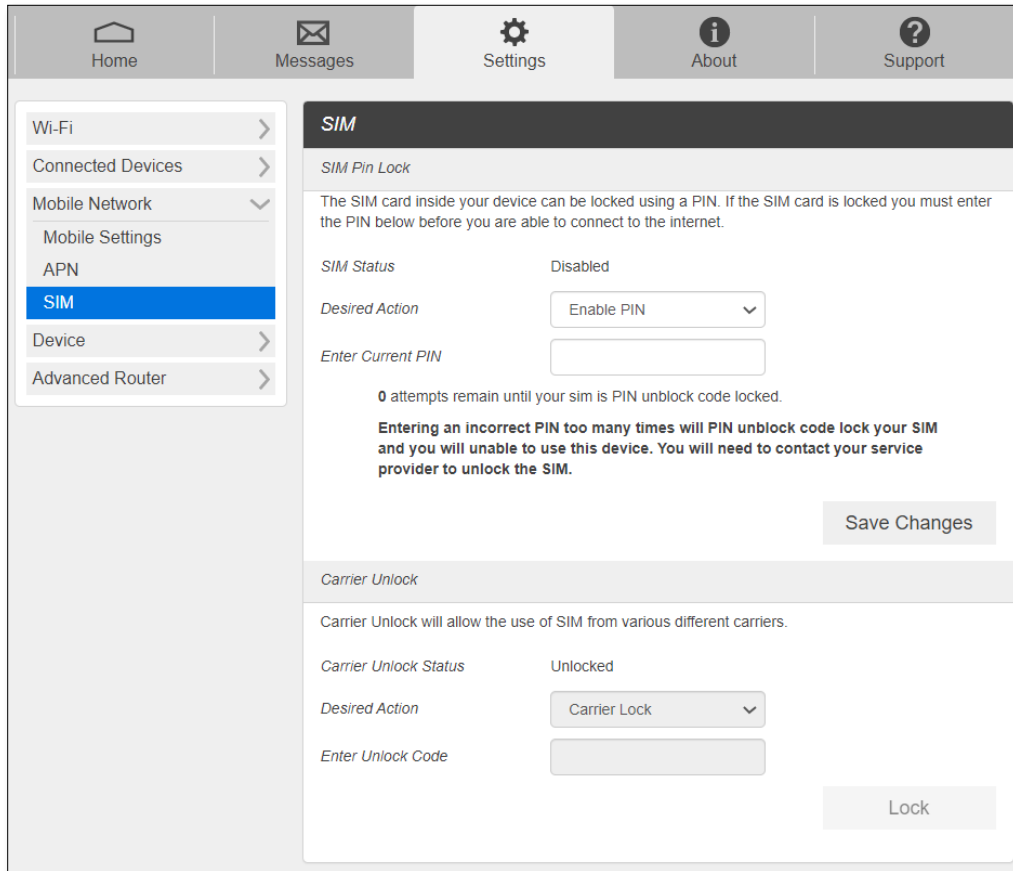
Additional APN Options

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

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

- **SIM**
SIM Pin Lock

The **SIM** menu allows you to lock the SIM (Subscriber Identity Module) card in your device. The SIM card inside your device can be locked with a PIN code for additional security. If locked, the PIN code must be entered before the device can connect to the Internet whenever you turn on your device. You can also change the SIM PIN.



Enter the SIM PIN and press **Save Changes** to save your settings. The SIM Status will be changed to Enabled. Once the SIM PIN Lock is enabled, you need to enter SIM PIN to connect to the mobile broadband network each time you power on your CG770.

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 CG770 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.

Carrier Unlock

Carrier Unlock will allow the use of SIM from various different carriers.

Carrier Unlock Status Unlocked

Desired Action Carrier Lock ▾

Enter Unlock Code

Device

- Preferences

The screenshot displays the 'Preferences' page for the CG770 device. The 'Ethernet' section is active, showing 'Ethernet Mode' set to 'WAN/LAN'. The 'WAN Priority' dropdown is set to 'WAN(Wired) Preferred'. A diagram below illustrates two configurations: 'LAN/LAN Port' where both Ethernet ports are used for LAN, and 'WAN/LAN Port' where the top port is used for WAN (connected to a modem) and the bottom port is used for LAN. A 'Save Changes' button is visible in the top right of the diagram area.

- **Ethernet Mode:** CG770 has two Ethernet ports. Users can select top and bottom Ethernet Port functionality. LAN/LAN mode and WAN/LAN mode.

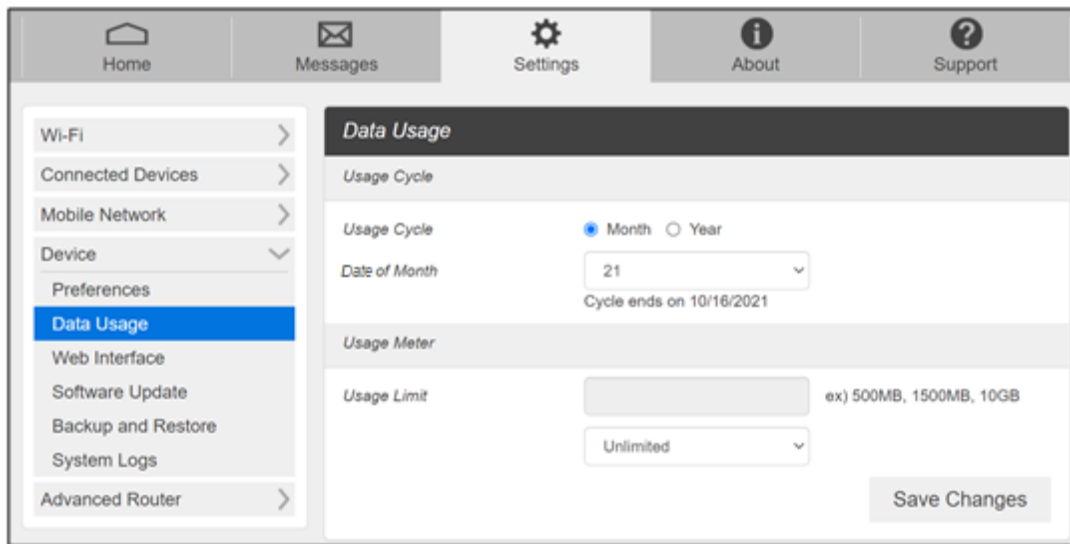
- **LAN/LAN mode:** CG770 will provide internet connection (LAN) to both Ethernet Ports.

- WAN/LAN mode: CG770 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.

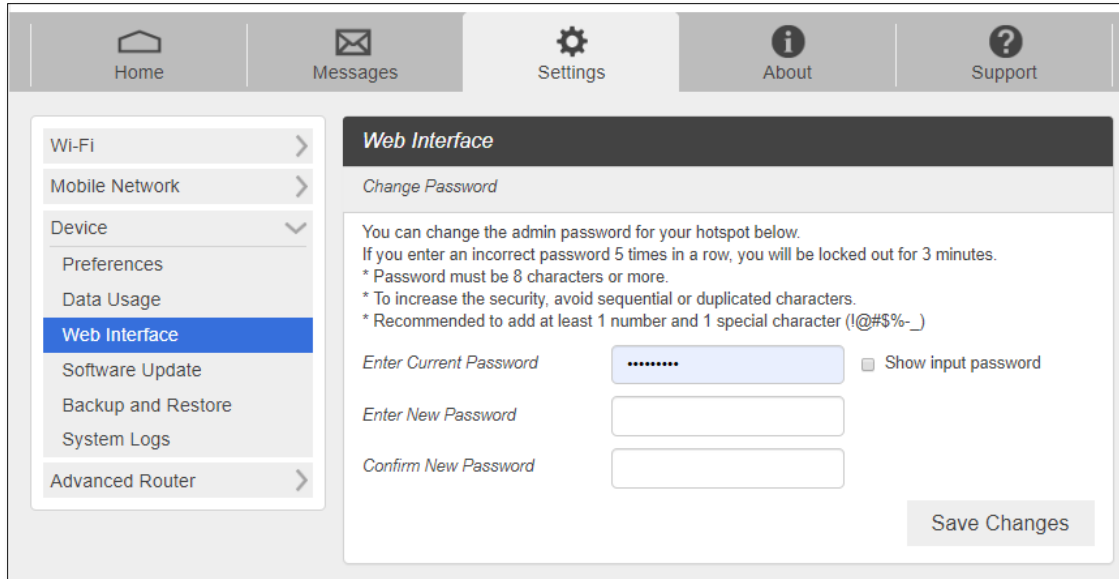
-WAN Priority: Users can select “WAN (Wired) preferred” or “WWAN (Wireless) preferred” to decide which WAN connection to be used primarily. If the primary connection fails, it will be switched to the second WAN connection.

- WAN(Wired) Preferred: CG770 will provide internet connection from the WAN port connection to its Wi-Fi and LAN network.
- WWAN(Wireless) Preferred: CG770 will provide internet connection from your wireless service (5G, 4G) providers to its Wi-Fi and LAN network.

- **Data Usage**: You can select date of month or date of year to reset data usage meter monthly or yearly.



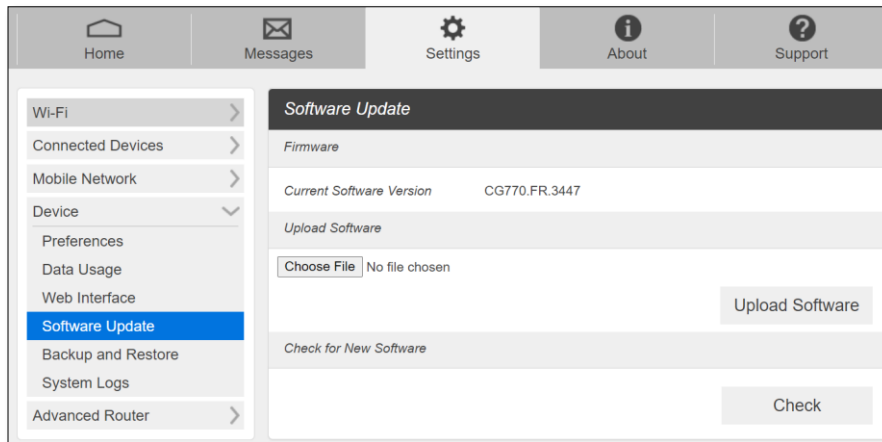
- **Web Interface**
You can change Web Admin login password.



- Current Password: Enter the current password. (Default password is “ClienteCLARO”)
- New Password: Enter the new password.
- Confirm New Password: Enter the new password again.

- **Software Update**

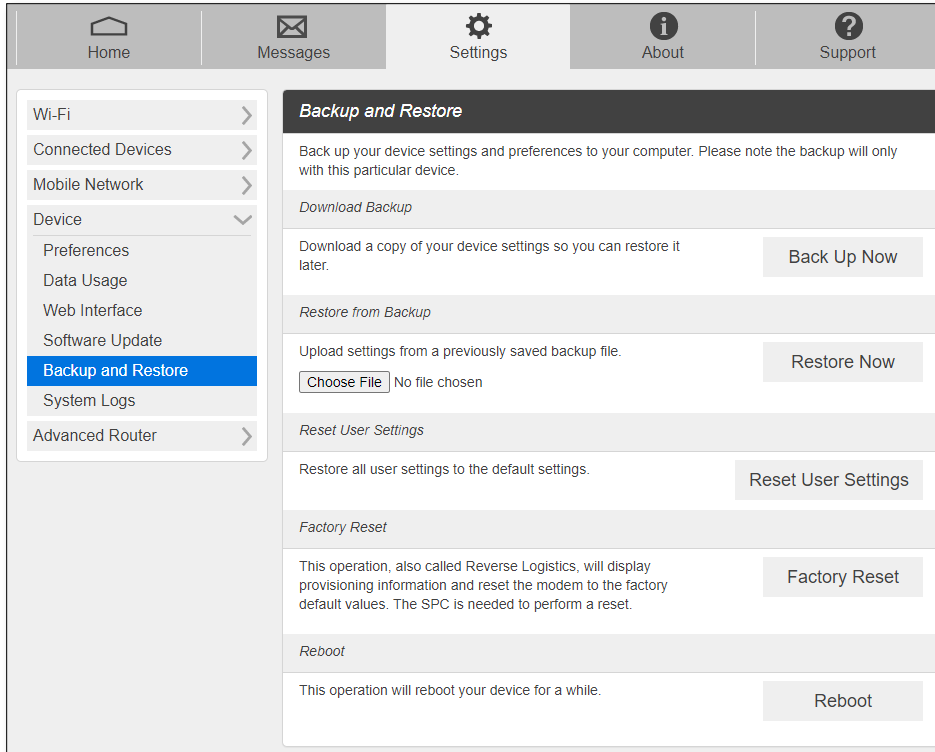
You can check current software version or check if there is a new update is available.



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

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

- **Backup and Restore**



Download Device Setting Backup file

To back up your device settings to your computer, follow the steps below:

- a. Click **Back Up Now**.
- b. Click **Save** on the pop-up window.
- c. Choose a location on your computer to save the backup file.
- d. Click **Save**.

Restore Device Settings from the Backup file

To restore the device settings from the backup file, follow the steps below:

- a. Click **Choose File** to select the backup file in your computer.
- b. Click **Restore now**.

Reset User Settings

To reset all user settings to its default settings, follow the steps below:

- a. Click **Reset User Settings**.
- b. Click **OK** to confirm the command.

Restore Device to Factory Defaults

To restore your device to its factory default settings, follow the steps below:

- c. Click **Restore Factory Defaults**.
- d. Click **OK** to confirm the command.

Reboot

To restart your device, follow the steps below:

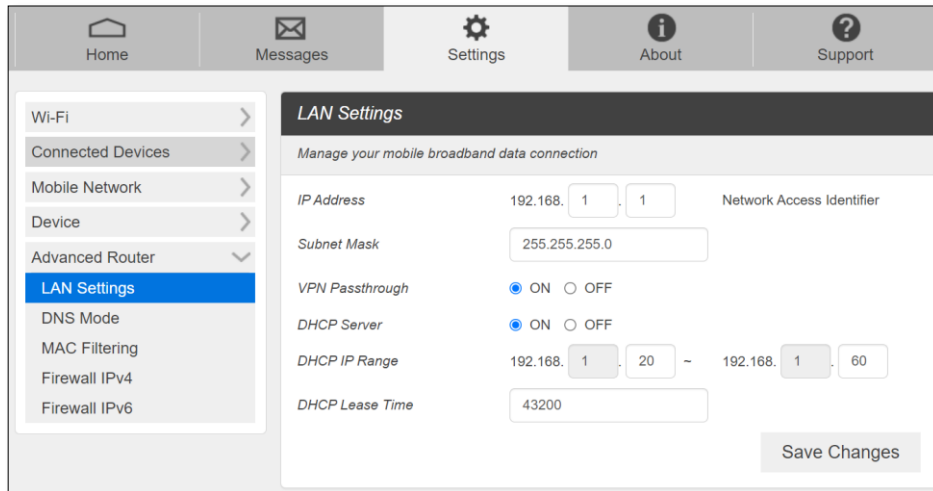
- a. Click **Reboot**.
- b. It will take 2~3 min the device reboot.

Advanced Router

Configure LAN, Firewall, and Customization settings.

- LAN Settings

From the Web UI, click Settings > Advanced Router > LAN Settings to display the router information shown in the following figure.

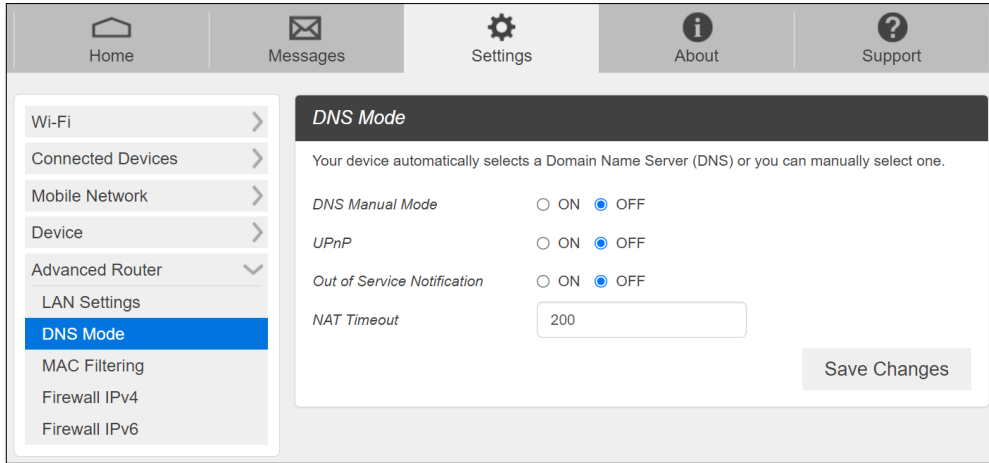


- **IP address** – The IP address of the default gateway and for your device Web Admin
- **Subnet mask** – The Subnet mask network setting for your device. The default value 255.255.255.0 is standard for small (class “C”) networks. If you change your LAN IP Address, ensure that you use the correct Subnet mask for the IP address range containing the LAN IP address.
- **VPN Passthrough ON/OFF** – 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 device automatically assigns local IPs to your other devices you connect to your device. When turned **OFF**, you will need to set it up manually from the device you want to connect to your device.
- **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 network. The **DNS Mode** option allows you to manually set up two DNS IP addresses.



To manually set a Domain Name Server:

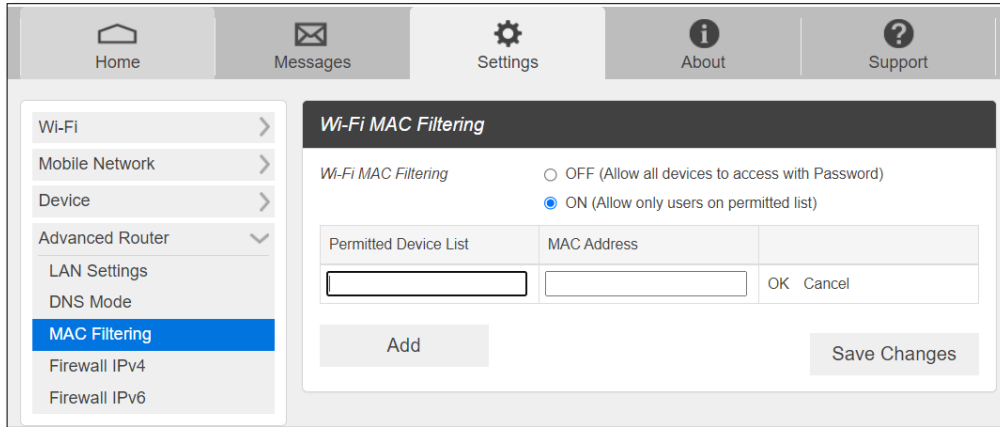
- 1 Click the **ON** button to enable **Manual DNS**.
- 2 Enter the IP address of the first DNS in the **DNS Address 1** field.
- 3 Enter the IP address of the second DNS in the **DNS Address 2** field.
- 4 Click **Save Changes** button.

- UPnP: When it is ON, the devices connected to CG770 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 device Wi-Fi network. By default, MAC filtering is turned **OFF**.



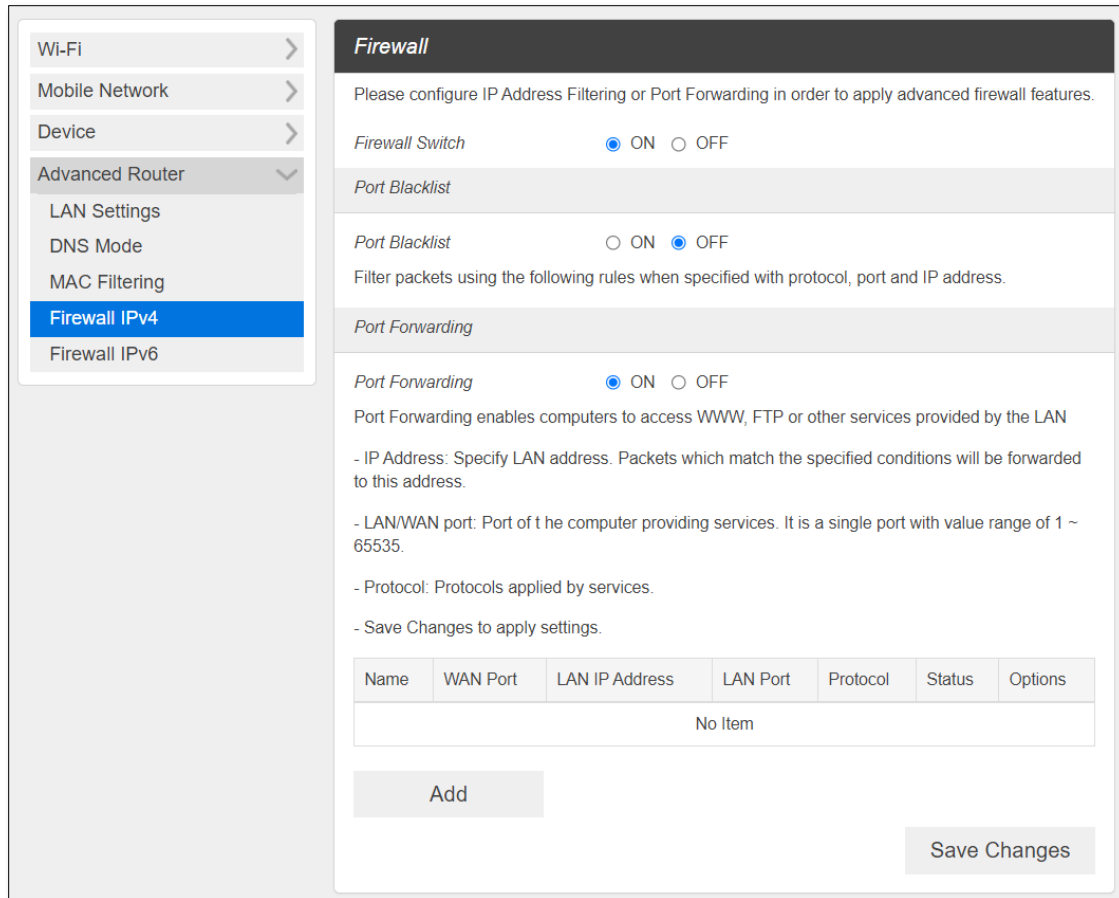
To enable MAC Filtering,

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 device Wi-Fi network. The MAC filtering has no effect on devices connected via Ethernet connection.

- **Firewall IPv4**

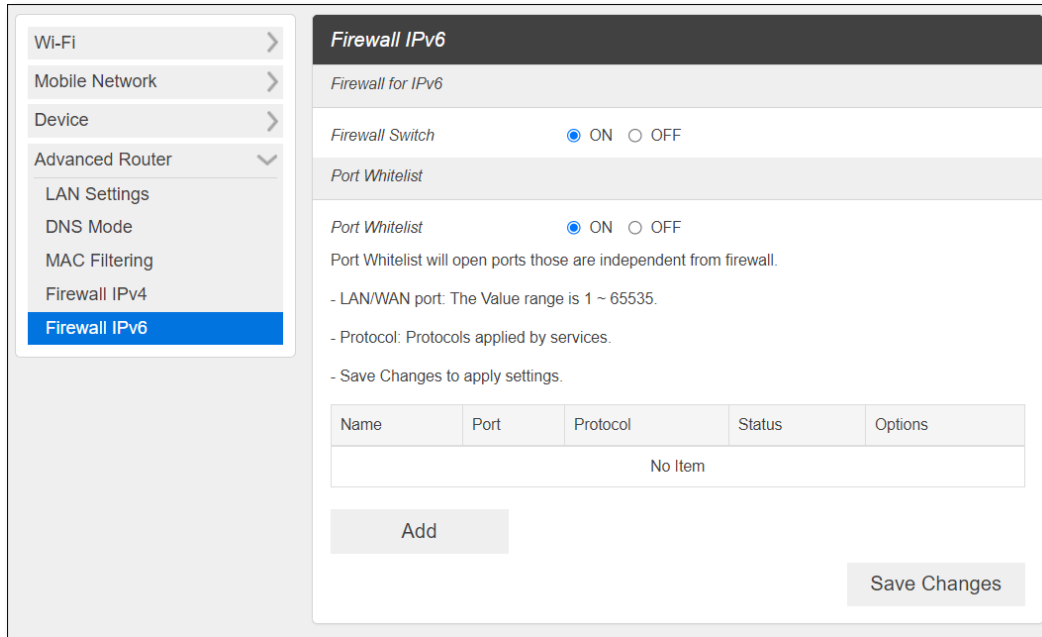
From the Web UI, click **Settings > Advanced Router > Firewall IPv4**. You may set up firewall rules to protect your network from virus and malicious activity on the Internet.



- **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 UI main screen, click the **About** tab to view the available information.

The screenshot shows a web interface with a top navigation bar containing five tabs: Home, Messages, Settings, About (selected), and Support. The main content area is divided into several sections:

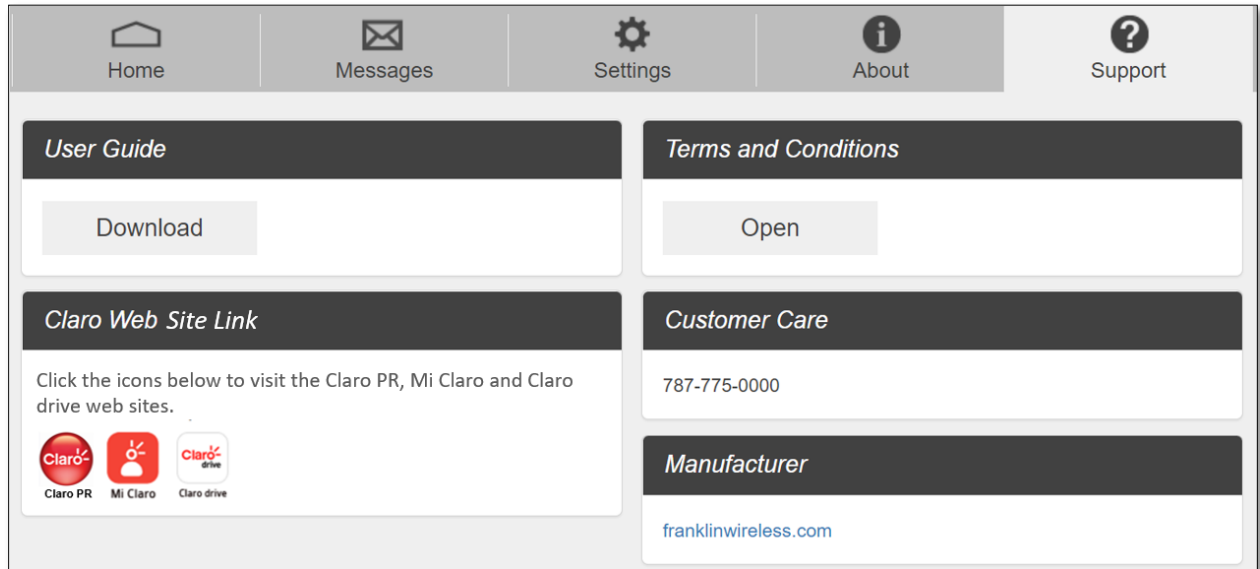
- Account**:
 - My Number: 14254997830
 - ICCID: 8901260171789460370F
 - IMSI: 310260178946037
 - IMEI: 358507750002729
- Device**:
 - Model: CG770
 - Manager: router.home
 - Hardware Revision: P2
 - Power State: Online
 - Current Voltage: 4.215V
 - Battery Charge Level: 83%
 - Battery Status: Charging
- Wi-Fi Details**:
 - Wi-Fi Name: CLARO_INTERNET_5GHz_39 CA
 - Wi-Fi Password: 12345678
 - MAC Address: F4:63:49:BC:39:CA
 - Encryption: WPA2 AES
 - Wi-Fi Devices: 1
 - Max Wi-Fi Devices: 20
 - Broadcast Network Name: Show
- WWAN Info**:
 - IP Address: 26.122.88.171, 2607:fb90:4af6:83cc:6954:8844:18e3:d345
 - Lifetime Transferred: 11.07 GB
- Firmware**:
 - Software Version: CG770.FR.3447
 - Modem Version: CG770.FR.M3447

At the bottom right of the main content area, there is a "Save to File" button. Below the main content is a "Debug Info" section with the text "View detailed diagnostic information about your device." and a "Debug" button.

Support

Obtain support information from the Web UI Support Tab.

From the Web UI main screen, click the **Support** tab to view the available options.



4

Troubleshooting

Overview
First Steps
Common Problems and Solutions

Overview

The following tips can help solve many common problems encountered while using the CG770.

First Steps

- 1 Make sure you are using your CG770 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 CG770 device can resolve many issues.

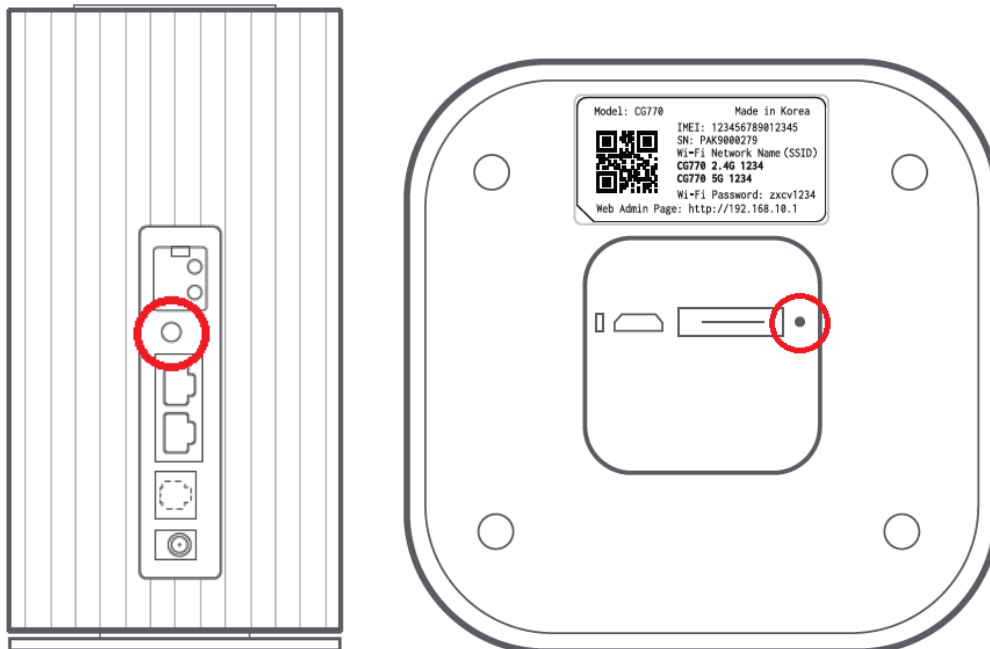
Common Problems and Solutions

How do I perform a Power Reset on CG770?

Using the power button: Press and hold the power button for 10 seconds until the CG770 restarts.

How do I perform a Reset?

Using the factory reset button: Press the reset button for 3 ~ 5 seconds and release. Then, your CG770 will perform the reset and restart automatically.



How do I perform a Factory Reset?

Using **Web Admin Page**: Connect to your CG770 and then open **Web Admin** home page (<http://192.168.1.1> or <http://router.home>). Select **Settings > Device > Backup and Restore** and Click **Factory Reset**.

I cannot connect to Wi-Fi after changing Wi-Fi password.

Your Wi-Fi 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 for your CG770 and keep the same Wi-Fi Name, the devices try to connect to your CG770 using the Wi-Fi name and previous Wi-Fi password saved, causing Wi-Fi authentication error. Delete or Forget the Wi-Fi name from the Wi-Fi controls of your device.

I cannot access the Web Admin, <http://192.168.1.1> or <http://router.home>

Ensure that Wi-Fi connection is enabled on your device and that you have selected the correct Wi-Fi name (SSID) for your CG770 connection. Also, make certain that you are entering the correct full URL address as <http://192.168.1.1> or <http://router.home>.

If you changed the IP address from **Web Admin, Settings > Advanced Router > LAN Settings**, you need to use the IP address you changed to access the **Web Admin** page.

I cannot log into Web Admin, <http://192.168.1.1> or <http://router.home>

Ensure that you are entering the correct password to sign in. The default **Web Admin** login password is "ClienteCLARO" unless you have previously changed. If your browser has cache memory or history login to same IP address, please clear the browser cache.

5

Regulatory Information

Regulatory Statements
Safety Hazards

Regulatory Statements

FCC Equipment Authorization ID: XHG-CG770

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.

Federal Communication Commission Interference Statement

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 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 modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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.

This device is restricted for indoor use.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance **20cm** between the radiator & your body.

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 20 cm 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.1.4

Date: June 2022

6

Glossary

Glossary

Term	Definition
LTE	Long-Term Evolution
802.11(b/g/n/ac)	A set of WLAN communication standards in the 2.4GHz 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