Table of Contents

Purpose ........................................................................................................................................ 1
Gateway Components .................................................................................................................. 2
  Front Panel ............................................................................................................................... 2
  Rear Panel ................................................................................................................................ 5
  Bottom Panel ............................................................................................................................. 6
Preparing for Installation ........................................................................................................... 7
  Wireless Connection ................................................................................................................ 7
  Wired Connection .................................................................................................................... 7
  Start with the Installation ....................................................................................................... 7
Setup ............................................................................................................................................ 8
  Connect the Gateway to Your Service Provider’s Network .................................................... 8
  Power on the Gateway ............................................................................................................. 9
  Connect Your Wired Devices ................................................................................................... 10
    Requirements ....................................................................................................................... 10
    How to Connect Your Wired Devices ................................................................................... 10
  Connect Your Wireless Devices .............................................................................................. 11
    Requirements ....................................................................................................................... 11
    How to Connect Your Wireless Devices ............................................................................... 11
  How to Configure the Gateway Push Button ......................................................................... 13
    Manually Connect Your Wireless Client ............................................................................ 14
    How to Connect the Gateway to a PC ................................................................................ 15
    How to Connect the Gateway to a Mac ............................................................................. 16
  How to Connect Your Phone .................................................................................................. 17
Administrator Tool ................................................................................................................... 18
  Accessing the Wireless Gateway Administrator Tool .......................................................... 18
  Admin Tool Menu .................................................................................................................. 19
  How to Change the Default Admin Tool Password .............................................................. 20
  How to Backup or Restore a Configuration ......................................................................... 21
    Configure Gateway Settings in Cox Business MyAccount ................................................. 22
Gateway Wireless Access Point .................................................................................................. 25
  Wireless Access Point ........................................................................................................... 25
  Wireless Client ....................................................................................................................... 25
    How to Configure a Wireless Client ................................................................................... 26
# Table of Contents

**How to Set the Wireless Security** ........................................................................................................... 28
**How to Start a WPS Session** ..................................................................................................................... 29
**How to Prevent Devices from Accessing Your Wireless Network** .......................................................... 31
  - MAC Address ............................................................................................................................................ 31
  - MAC Filtering............................................................................................................................................ 31
  - Security Tab / Device Filter ....................................................................................................................... 32
  - Enable Device Filter ................................................................................................................................. 32
  - Block All.................................................................................................................................................. 32
  - Allow All.................................................................................................................................................. 32
  - Options for Time of the Day Filters – When Block .................................................................................. 32

**Terms of Use and Guest Splash Page** ..................................................................................................... 33

**Internet Security** ....................................................................................................................................... 34
**Access Control** .......................................................................................................................................... 34

**Manage Sites and Devices** ..................................................................................................................... 34
  - Security Tab / Access Control .................................................................................................................. 34
  - Blocked Sites .......................................................................................................................................... 35
  - Trusted Devices ...................................................................................................................................... 35

**Manage Devices** ....................................................................................................................................... 35
  - Security Tab / Device Filter ..................................................................................................................... 35
  - Enable Device Filter ................................................................................................................................ 36
  - Block All.................................................................................................................................................. 36
  - Allow All.................................................................................................................................................. 36
  - Options for Time of the Day Filters – When Block .................................................................................. 37

**Managed Services (Port Blocking)** ......................................................................................................... 37
  - Security Tab / Service Filter .................................................................................................................... 37
  - Blocked Services ...................................................................................................................................... 38
  - Trusted Devices ...................................................................................................................................... 38

**Firewall** ...................................................................................................................................................... 38
  - Changing the Security Level .................................................................................................................... 40

**Reports** ..................................................................................................................................................... 41

**Advanced Configuration** ......................................................................................................................... 42
**Port Configuration for Applications and Services** ................................................................................. 42
  - Issue....................................................................................................................................................... 42
  - Solutions.................................................................................................................................................. 43

**UPnP (Universal Plug and Play)** ................................................................................................................ 43
<table>
<thead>
<tr>
<th>Supported Operating Systems</th>
<th>44</th>
</tr>
</thead>
<tbody>
<tr>
<td>UPnP and the Gateway</td>
<td>44</td>
</tr>
<tr>
<td>Enable UPnP on the Gateway</td>
<td>44</td>
</tr>
<tr>
<td><strong>Port Forwarding</strong></td>
<td>44</td>
</tr>
<tr>
<td>Use a Reserved IP Address</td>
<td>44</td>
</tr>
<tr>
<td><strong>Port Triggering</strong></td>
<td>46</td>
</tr>
<tr>
<td><strong>Port Filtering</strong></td>
<td>47</td>
</tr>
<tr>
<td><strong>Configure a DMZ Host</strong></td>
<td>47</td>
</tr>
<tr>
<td>Application Tab/DMZ</td>
<td>48</td>
</tr>
<tr>
<td><strong>Dynamic DNS</strong></td>
<td>48</td>
</tr>
<tr>
<td><strong>Assigning a Reserved IP (static IP) to a Device</strong></td>
<td>50</td>
</tr>
<tr>
<td><strong>Support</strong></td>
<td>51</td>
</tr>
<tr>
<td><strong>Wireless Connection Troubleshooting</strong></td>
<td>51</td>
</tr>
<tr>
<td>No Wireless Connectivity</td>
<td>51</td>
</tr>
<tr>
<td>Poor Wireless Connectivity or Range</td>
<td>52</td>
</tr>
<tr>
<td>Change the Wireless Channel</td>
<td>52</td>
</tr>
<tr>
<td>Make Sure That the Wireless Access Point Is Enabled</td>
<td>53</td>
</tr>
<tr>
<td>Cannot Connect via WPS</td>
<td>54</td>
</tr>
<tr>
<td><strong>Network Diagnostic Tools</strong></td>
<td>54</td>
</tr>
<tr>
<td><strong>Gateway Reboot and Reset Options</strong></td>
<td>56</td>
</tr>
<tr>
<td>Reset/Restore the Gateway via the Reset Button</td>
<td>57</td>
</tr>
</tbody>
</table>
Purpose

This guide instructs you on how to:

- Set up your gateway and local network for use with Cox Business Internet and Cox Fiber Internet
- Configure and use the main features of your gateway
- Configure Internet security
Gateway Components

This section displays different views of the Gateway 4131 model and describes the LEDs, ports, and buttons on the device for your reference.

Front Panel

The following images represent the front panel view of the CGA4131.

**Figure 1. Front Panel**

![Gateway 4131 Front Panel Image]

**Figure 2. Front Panel with LEDs**

![Gateway 4131 Front Panel with LEDs Image]
Ethernet LED (Item A)

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid on</td>
<td>Ethernet is enabled with AC power</td>
</tr>
<tr>
<td>Off</td>
<td>Ethernet is not enabled</td>
</tr>
</tbody>
</table>

Ethernet Ports 1-8 LEDs (Items B – I)

The CGA4131 has 8 Ethernet ports. The status of each port is shown by its LED state. If Port 1 is used with the CBIG eWAN configuration, the port is not available for LAN connections.

<table>
<thead>
<tr>
<th>Port 1</th>
<th>LED B</th>
<th>Port 2</th>
<th>LED C</th>
<th>Port 3</th>
<th>LED D</th>
<th>Port 4</th>
<th>LED E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port 5</td>
<td>LED F</td>
<td>Port 6</td>
<td>LED G</td>
<td>Port 7</td>
<td>LED H</td>
<td>Port 8</td>
<td>LED I</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid on</td>
<td>The port is connected.</td>
</tr>
<tr>
<td>Off</td>
<td>The port is not connected</td>
</tr>
<tr>
<td>Blinking</td>
<td>Data is being transferred</td>
</tr>
</tbody>
</table>

Internet LED (Item J)

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid on</td>
<td>Internet Service is active</td>
</tr>
<tr>
<td>Off</td>
<td>There is no Internet Service</td>
</tr>
</tbody>
</table>

WiFi LED (Item K)

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blinking</td>
<td>Data (2.4GHz or 5GHz) is active over the wireless connection</td>
</tr>
<tr>
<td>Off</td>
<td>WiFi access point is not enabled</td>
</tr>
</tbody>
</table>

Online LED (Item L)

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid on</td>
<td>Connected to the service provider’s network. Even when Internet is not active, LED is on. Data traffic can be used.</td>
</tr>
<tr>
<td>Blinking</td>
<td>Trying to acquire Upstream, Downstream frequencies</td>
</tr>
</tbody>
</table>
Telephone Lines 1-8 LEDs (Items M – T)
The CGA4131 has 8 telephone lines. The status of each telephone line is shown by its LED state.

<table>
<thead>
<tr>
<th>Telephone Line</th>
<th>LED M</th>
<th>Telephone Line</th>
<th>LED N</th>
<th>Telephone Line</th>
<th>LED O</th>
<th>Telephone Line</th>
<th>LED P</th>
</tr>
</thead>
<tbody>
<tr>
<td>Line 1</td>
<td></td>
<td>Line 2</td>
<td></td>
<td>Line 3</td>
<td></td>
<td>Line 4</td>
<td></td>
</tr>
<tr>
<td>Line 5</td>
<td>LED Q</td>
<td>Line 6</td>
<td>LED R</td>
<td>Line 7</td>
<td>LED S</td>
<td>Line 8</td>
<td>LED T</td>
</tr>
</tbody>
</table>

State Description

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid on</td>
<td>Telephone line is registered successfully with the call manager</td>
</tr>
<tr>
<td>Blinking</td>
<td>Telephone line has either gone off-hook or is in active call</td>
</tr>
<tr>
<td>Off</td>
<td>Telephone line is not registered with the call manager</td>
</tr>
</tbody>
</table>

Reset Button (Item U)
Press the Reset button to reset the box. Press the Reset button approximately 12-13 seconds to restore to factory settings.

For more information, see Reset/Restore the Gateway via the Reset Button.

Telephone Line LED (Item V)

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid on</td>
<td>MTA Voice interface is operational</td>
</tr>
<tr>
<td>Off</td>
<td>MTA Voice interface is not operational</td>
</tr>
</tbody>
</table>

WPS (Item W)
The LED blinks when the WPS button is pressed. It will blink for 2 minutes or until the wireless client WiFi is connected to the gateway, whichever is earlier. The LED will then turn solid white for 2 minutes and will turn Off thereafter.

For more information about WPS, see How to Connect Your Wireless.

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blinking</td>
<td>WPS Process initialized (lasts for 2 minutes)</td>
</tr>
<tr>
<td>Off</td>
<td>No WPS activity</td>
</tr>
</tbody>
</table>

Battery LED (Item X)

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Off</td>
<td>Device is off, or AC power is on or Battery is not installed</td>
</tr>
<tr>
<td>Solid on</td>
<td>On Battery Power</td>
</tr>
<tr>
<td>Blinking</td>
<td>Battery needs replacement</td>
</tr>
</tbody>
</table>
Rear Panel

The following image shows the back-panel view of the CGA4131.

**Figure 3. Rear Panel View**

![Rear Panel View](image)

**Telephone port (Item A)**

The CGA4131 supports up to eight traditional phones or DECT base station to connect to the Gateway. Single-line customers can use the Tel 2/Alarm port to connect an auto dial alarm system.

**Ethernet switch (Item B)**

The CGA4131 supports up to eight Ethernet connections (for example, a computer) to your local network. For more information, see *Connect Your Wired Devices*.

The first four (4) Ethernet ports each can transfer up to 1 Gbps data, while ports 5 - 8 can have a combined data transfer speed of 1 Gbps.

When the device is configured in eWAN mode, port 1 is used to connect to the ONT and/or Nokia Model 7210 SAS-Mxp. Other Nokia models that may be used are the 7210 SAS-K30 and the 7210 SAS-5.

Each Ethernet port has two LEDs:

<table>
<thead>
<tr>
<th>LED</th>
<th>LED Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Left LED (Green)</td>
<td>Solid on</td>
<td>Connected to a Gigabit Ethernet device</td>
</tr>
<tr>
<td></td>
<td>Blinking</td>
<td>Connected to a Gigabit Ethernet device and sending/receiving</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>Not connected to a Gigabit Ethernet device</td>
</tr>
<tr>
<td>Right LED (Amber)</td>
<td>Solid on</td>
<td>Connected to a 100Mbps/10Mbps device</td>
</tr>
<tr>
<td></td>
<td>Blinking</td>
<td>Connected to a 100Mbps/10Mbps device and sending/receiving</td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>Not connected to a 100Mbps/10Mbps device</td>
</tr>
</tbody>
</table>

**Cable Port (Item C)**

The CGA4131 complies with DOCSIS 3.0 and 3.1 standards along with PacketCable™ specifications to deliver high-end performance and reliability.
USB Port (Item D)
USB port connects to USB devices.

Power Inlet (Item E)
Plug the power cord in the Power slot.

Bottom Panel

*Figure 4* shows the CGA4131 bottom panel and Battery Compartment with door on (Item A).

Battery Slot (Optional) (Item A)
During a power failure, the Gateway can automatically switch to the auxiliary emergency power through the rechargeable battery (if installed). The following capabilities are supported during a loss of power:

- The connected phones or dial function for a connected alarm system
- Basic voice features.

⚠️ **Caution:** Do not remove the battery unless instructed by your service provider.

**Figure 4. Bottom Panel View**

Product Label (Item B)
Setup information, including the Gateway SSID, Passphrase, MAC addresses and Serial Number can be found here.
Preparing for Installation

Wireless Connection
If you want to connect your computer using a wireless connection, your computer must be equipped with a WiFi Certified wireless client adapter.

Wired Connection
If you want to connect a computer using a wired connection, your computer must be equipped with an Ethernet Network Interface Card (NIC).

Start with the Installation
You are now ready to begin installing your Gateway.
Setup

Complete the following to set up the Gateway:

1. CBIG eWAN customers – toggle device to eWAN mode before you connect it to the network via Ethernet. *(Note: CBIG eWAN customers connect the ONT or WAN Ethernet Handoff to Port #1.)*

2. Connect your Gateway to your service provider’s network. For more information, see *Power on the Gateway.*

3. Connect your wireless devices to the Gateway. For more information, see *Connect Your Wireless Devices.*

4. Connect your phones. For more information, see
5. *How to Connect Your* Phone.

After completing the setup procedure, the Gateway is ready for use. You may elect to make additional configurations to the Gateway based on your business needs; e.g., change wireless security using the Gateway’s Admin Tool.

**Connect the Gateway to Your Service Provider’s Network**

Use the following steps to connect the Gateway to your service provider’s network.

1. Take one end of the coaxial cable and connect it to the cable splitter.
2. Connect the other end to the Cable port on the Gateway.

![Back Panel – Cable Port](image1)

![4131 Gateway Connected to Active CPE (Customer Premise Equipment) (example)](image2)
Power on the Gateway

Use the following steps to turn on the gateway:

1. Use the power cord that is included with your gateway.

2. Connect the small end of the power cord to the Power port on the back of the Gateway (see Figure 8).

3. Plug the other end of the power cord into an electrical outlet.

4. Wait at least two (2) minutes to allow the Gateway to complete the startup phase.

Connect Your Wired Devices

All Ethernet ports on the Gateway are Gigabit Ethernet ports and have a maximum speed of 1 Gbps (gigabit per second).
Requirements

- Your network device, such as a computer or point of sale terminal and the Gateway must have a free Ethernet port.
- Your network device must be configured to obtain an IP address automatically. (This is the default setting.)

How to Connect Your Wired Devices

**Recommendation:** Use Category 5e or Category 6 Ethernet cables with the Gateway.

1. Plug one end of the Ethernet cable into one of the RJ-45 Ethernet ports on the back of the Gateway. (See Figure 9). *(Note: CBIG eWAN customers do not use Port 1.)*
2. Plug the other end of the Ethernet cable into the Ethernet port of your local area network device.
   
   **Result:** Your local area network device is now connected to your network. Use the same procedure to connect other Ethernet devices; e.g., computers and network printers.

**Figure 9.** Back Panel – Ethernet Ports

Connect Your Wireless Devices

The Gateway has two access points that allow you to connect wireless devices to your network:

- The 5 GHz IEEE 802.11a/n/ac access point offers superior transfer rates, is less sensitive to interference, and allows you to connect IEEE 802.11a/n/ac wireless clients.
- The 2.4 GHz IEEE 802.11b/g/n access point allows you to connect IEEE 802.11b/g/n wireless clients. Use this access point for wireless clients that do not support 5 GHz.

**Caution:** If you want to connect your wireless client to the 5 GHz access point, check that your wireless client supports 5 GHz connections.
Requirements

- Your wireless client must support WPS. Check the documentation of your wireless client to confirm.

- Your Gateway must use WPA/WPA2-PSK (TKIP/AES) encryption (default encryption) or WPA2-PSK (AES) encryption.

How to Connect Your Wireless Devices

WiFi Protected Setup (WPS) allows you to add new wireless clients to your local network quickly and easily without the need to enter any of your wireless settings; e.g., network name, wireless network key, encryption type.

The 2.4 GHz and the 5 GHz access points of your Gateway support WPS.

Use either option below to connect your wireless device:

- Follow the steps listed in the
- How to Configure a Wireless Client section.
- Follow the steps listed in the Manually Connect Your Wireless Client section.
WPS Methods

The following WPS methods are supported by your Gateway:

- **Push Button Configuration (PBC):** Place both the wireless client and the Gateway in registration mode by pushing a hardware or software button.
- **PIN code entry on the wireless client:** Enter the Gateway’s WPS PIN code on the wireless client. For more information, see *Manually Connect Your Wireless Client.*
- **PIN code entry on the Gateway:** Enter the wireless client’s WPS PIN code on the Admin Tool. For more information, see *How to Start a WPS Session.*

**How to Configure the Gateway Push Button**

Use the following steps to configure the gateway Push Button.

1. Start the wireless protected setup (WPS) on your wireless client.
2. On the Gateway, press and hold the WPS button for at least 5 seconds and then release. Result: The WPS button LED will start blinking. This indicates that the Gateway is now searching for wireless clients that are in registration mode.

![Figure 10. WPS Button](image)

The Gateway will configure security settings with the wireless client. Your wireless client will prompt you when it is connected to the access point.

**Troubleshooting**

If you are having trouble connecting your wireless client via WPS, this may be caused by one of the following reasons:

WPS cannot be correctly executed: Configure your wireless manually. For more information, see *Manually Connect Your Wireless Client.*

Your wireless client is out of range: If possible, move your wireless client closer to your Gateway or use a wireless repeater to extend the range of your wireless network.
Manually Connect Your Wireless Client

Requirements

- Your network device must be equipped with a WiFi Certified wireless client.
- Your network device must be configured to obtain an IP address automatically. This is the default setting.

How to Manually Connect Your Wireless Client

If you want to connect a computer using the wireless network, configure the wireless client on your computer with the wireless settings printed on the Gateway's back panel label.

The Gateway's back panel contains two items needed to establish a WiFi connection:

- **SSID** ("Network Name") is the name of the network. You may use the 2.4GHz or 5GHz network name. Note the following requirements for SSIDs:
  - The CGA4131 only allows the first 3 Guest SSIDs to be used per radio
  - One (1) primary and three (3) Guest SSIDs are visible to the customer
  - One (1) primary and seven (7) Guest SSIDs are visible to Cox
    - The last four (4) are reserved for Cox; e.g., this is where CoxWiFi displays.

- **Passphrase** is the password used for the network name selected.

Refer to *How to Connect the Gateway to a PC* for instructions.

Refer to *How to Connect the Gateway to a Mac* for instructions.
How to Connect the Gateway to a PC

Use the following steps to connect your PC.

1. Click the wireless network icon in the notification area.  
   Result: A list of available wireless networks appears.
   
   **Figure 11. Available Wireless Networks**

2. Double-click the Gateway's Network Name (SSID). Use the Gateway’s Network Name (SSID) printed on the panel label on the gateway. For more information, see *Bottom Panel*.
   
   **Result:** Windows prompts you to enter the security key.

3. Type the Passphrase from the Gateway's bottom panel label in the *Enter the network security key* box and click the Next button.
   **Result:** Windows prompts you to identify sharing needs.

   **Figure 12. Enter Network Security Key**

4. Click Yes to turn on sharing.
How to Connect the Gateway to a Mac

Use the following steps to connect your Mac computer.

1. Click the WiFi icon on the menu bar.
   Result: A list of available wireless networks appears.
   ![Available Wireless Networks](image)

2. Double-click the Gateway’s Network Name (SSID). (Note: The Gateway’s Network Name (SSID) is printed on the Gateway’s side or back panel label.)
   Result: The WiFi window prompts you to enter your WPA password.
   ![Enter WPA Password](image)

3. In the Password box, type the Passphrase, which is printed on the label located on the bottom of the Gateway.

4. Select the Remember this network checkbox and click OK.
   Result: You are now connected to the Gateway network.
How to Connect Your Phone

This section describes how to connect single line phone.

1. Connect your traditional phone, external DECT base station or fax to an active RJ-11 Telephone jack on the back panel of your Gateway.

   Note: You must connect Alarm dialers to either port 1 or 2. Be sure the Alarms dialer is connected to an active telephone port connected to the phone network.

2. Plug the other end of the telephone cable into the telephone device.

3. Verify that each phone line is active by first checking for dial tone, and then by placing a call to an active telephone number and checking that both parties can properly hear one another.
Administrator Tool

The Administrator (Admin) tool allows you to configure the settings of your Gateway through your web browser, using a computer or device that is currently connected to your Gateway (either wired or wirelessly).

**Note:** The Admin Tool web pages are displayed differently for smaller screens if you connect using a mobile device. The example in this guide shows the screens as accessed using a computer.

**Accessing the Wireless Gateway Administrator Tool**

Use the following steps to access the Wireless Gateway Admin tool.

1. Enter http://192.168.0.1 in your web browser. (**Note:** You must use a computer or device that is currently connected to your Gateway either wired or wirelessly to access the site).

   On Windows, it is possible to access the Admin Tool using UPnP. For more information, see **UPnP (Universal Plug and Play)**.

   **Note:** 192.168.0.1 is the default IP address of the Gateway. If the IP address of the Gateway has changed, use the new IP address.

2. The Gateway prompts you to enter the username and password. Enter your username (default: blank) and password (default: blank).

   **Result:** The Gateway admin main page appears.

   **Figure 16. Gateway Admin main page**
## Admin Tool Menu

The Gateway admin tool menu consists of the following first-level menu items. Based on your service provider’s network, some screens listed in the “Sub Menu” column may not be available to you.

<table>
<thead>
<tr>
<th>Top Level Menu</th>
<th>Sub Menus</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Overview</td>
<td>The <strong>Status</strong> screens provide basic information about the Gateway, including information on the Local Network, the Wireless Networks, and the DOCSIS Network to your Service Provider.</td>
</tr>
<tr>
<td></td>
<td>Gateway</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Local Network</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Wireless</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DOCSIS Status</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DOCSIS Signal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DOCSIS Log</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Spectrum Analyzer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>System</td>
<td></td>
</tr>
<tr>
<td>Connection</td>
<td>Devices</td>
<td>The <strong>Connection</strong> screens show devices that are connected to your gateway on various Local Networks provided by your Gateway as well as options to enable eWAN Mode and Bridge Mode Routing. There are also options to configure your Gateway using a Static IP address.</td>
</tr>
<tr>
<td></td>
<td>LAN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WAN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Routing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Modem</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MTA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Time</td>
<td></td>
</tr>
<tr>
<td>Wireless</td>
<td>Radio</td>
<td>The <strong>Wireless</strong> screens show options related to the wireless network, including radio parameters and wireless security.</td>
</tr>
<tr>
<td></td>
<td>Security</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Advanced</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Guest Network</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MAC Control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WPS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>QoS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hotspot</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>Firewall</td>
<td>The <strong>Security</strong> screens provide options to manage and filter Internet access provided by the Gateway.</td>
</tr>
<tr>
<td></td>
<td>IP Filter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Device Filter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access Control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Service Filter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VPN</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Email Settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Report</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>Port Forward</td>
<td>Options related to Port Forwarding and other features are found in the <strong>Application</strong> menu.</td>
</tr>
<tr>
<td></td>
<td>Port Trigger</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Port Filter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DDNS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DMZ</td>
<td></td>
</tr>
<tr>
<td></td>
<td>UPnP</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IP Passthrough</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SIP ALG</td>
<td></td>
</tr>
</tbody>
</table>
### Top Level Menu

<table>
<thead>
<tr>
<th>Sub Menus</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration</td>
<td>The <strong>Administration</strong> screens present options to change the username and password, add users, and reset the device.</td>
</tr>
<tr>
<td>User</td>
<td></td>
</tr>
<tr>
<td>Remote Access</td>
<td></td>
</tr>
<tr>
<td>Backup &amp; Restore</td>
<td></td>
</tr>
<tr>
<td>Reboot &amp; Reset</td>
<td></td>
</tr>
<tr>
<td>Troubleshooting</td>
<td></td>
</tr>
<tr>
<td>Remote Log</td>
<td></td>
</tr>
<tr>
<td>Diagnostic</td>
<td><strong>Diagnostic</strong> screens provide some utilities to troubleshoot your network connection or Gateway.</td>
</tr>
<tr>
<td>System</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td></td>
</tr>
<tr>
<td>Wireless</td>
<td></td>
</tr>
<tr>
<td>Clients</td>
<td></td>
</tr>
<tr>
<td>Internet</td>
<td></td>
</tr>
</tbody>
</table>

### How to Change the Default Admin Tool Password

We recommend changing the default password of the Gateway the first time it is used. The username and password fields are empty by default.

Use the following steps to access the Wireless Gateway Admin tool.

1. Enter `http://192.168.0.1` in your web browser. **(Note: You must use a computer or device that is currently connected to your Gateway either wired or wirelessly to access the site).**
2. Enter the default username and password.
3. A pop-up message displays, prompting you to change the password.
4. Follow the prompts.
How to Backup or Restore a Configuration

The backup feature saves the current Gateway configuration to a local PC. These settings can be restored later if a configuration needs to be restored, or to recover from changes that have had an undesirable effect.

To back up the current configuration, click Administration on the Admin Tool menu, and then click Backup on the sub-menu. Follow the onscreen instructions.

Figure 17.  Backup and Restore Options

To restore a previous configuration, click Browse and use the navigation window to locate the file. The default file name is in the following format: filename_YY_MM_DD_HOUR_MINUTES.gwc.

When the file has been located, click Restore to restore the settings. When the settings are restored, the device will reboot to the restored settings.

Important: Do not edit the backup files; this may result in corrupt files making them worthless as configuration backup.

Caution: Restoring a saved configuration will require the Gateway to restart. The reboot will cause a short service interruption of the services provided by the Gateway.
Configure Gateway Settings in Cox Business MyAccount

Your Cox Internet Gateway was installed with unique settings according to the specifications. To store your settings securely, select the device from the drop-down and use the fields provided. Should you need to restore your router, this information will allow you to apply your latest configurations. **Note**: The information stored here will not alter the configurations or behavior of your gateway/router.

**Figure 18.** MyAccount
Use the following steps to save your gateway settings in MyAccount.

1. Enter myaccount.coxbusiness.com in your web browser.
2. Enter your MyAccount Username and Password in the fields and click the **Sign In** button.
   - **Result:** The MyAccount Welcome page appears.
3. Scroll to the My Services section and click the **Internet** tab. (See **Figure 18**.)
4. Click the **Internet Gateway** icon.
5. Click the **Gateway/Guest WiFi Reference Info** box and click the **Next** button. (See **Figure 19**.)
6. Choose the device you want to configure from the **Select a Device** drop-down menu. (See **Figure 20**.)
   - **Result:** The **Internet Gateway Settings** window appears. (See **Figure 21**.)
7. Populate the fields appropriately. (Tip: Click the question mark icon to see a description of the field.

8. Click the Save button.
Gateway Wireless Access Point

This section will help you set up your wireless network. To set up a wireless network, you need the following components:

- Wireless access point (already integrated into your gateway)
- Wireless client (for example, a computer, smartphone, network printer)

**Wireless Access Point**

The wireless access point is the heart of your wireless network. The wireless access point:

- Connects different wireless clients
- Secures the data sent over wireless connection

The Gateway has two access points:

- The 5 GHz access point enables superior transfer rates for 802.11a/n/ac wireless devices that are closer to the AP.
- The 2.4 GHz access point provides connectivity to 802.11b/g/n wireless clients that are farther from the AP. Use this access point for legacy wireless clients.

**Note:** If you are connecting the wireless client to the 5 GHz access point, make sure the wireless client supports 5 GHz connections.

**Wireless Client**

The wireless client allows you to connect a wireless client to a wireless access point. Both built-in and external (for example via USB) wireless clients are available.

Devices like tablets, smart TVs and smartphones usually have a built-in wireless client. Check the documentation of your device for more information.
How to Configure a Wireless Client

1. Go to the Admin Tool (http://192.168.0.1) using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *Accessing the Wireless Gateway Administrator Tool*.

2. Click the **Wireless** tab then click the **Radio** sub-tab.

   **Result:** The screen displays Radio setup information at 2.4GHz and 5GHz:

   ![Wireless – Radio Settings](image)

   The following fields are available for configuration:

   - **Wireless Interface:** The wireless interface can be enabled or disabled with this option.
   - **Network Name:** The Network Name (SSID) can either be set or displayed under this option. The user can also prevent the network name (SSID) from being broadcast by selecting the **Hide** radio button.
**Network Mode:** The Network Mode determines which 802.11 wireless protocols will be used. The Network Mode has different options available according to the wireless interface:

For 2.4GHz:
- 802.11b only
- 802.11g only
- 802.11n only
- Mixed (802.11b and 802.11g)
- Mixed (802.11g and 802.11n)
- Mixed (802.11b, 802.11g and 802.11n)

For 5GHz:
- 802.11a only
- 802.11n only
- 802.11ac only
- Mixed (802.11a and 802.11n)
- Mixed (802.11n and 802.11ac)
- Mixed (802.11a, 802.11n and 802.11ac).

**Channel Width:**

The channel bandwidth can be selected manually for Wireless-N connections. For best performance in a network using Wireless-N, Wireless-G, and Wireless-B devices, it is suggested to use the AUTO (20 or 40MHz) channel setting.

Wireless-N connections will use the 40MHz channel if there is no interference, while Wireless-G and Wireless-B will still use the 20MHz channel.

For Wireless-G and Wireless-B networking only, select 20MHz only. Then, only the 20MHz channel will be used.

For 5GHz, the options include AUTO 20 or 40 or 80MHz. The 80MHz will only be used for AC.

**Channel:**

If AUTO (20 or 40MHz) is selected for the Radio Band setting the appropriate Standard Channel setting will be automatically selected, depending on the Wide Channel setting.

If only 20MHz is selected as the Radio Band setting, select the appropriate channel from the list provided to correspond with the network settings. All devices in the wireless network must broadcast on the same channel to communicate.

**MAC Address:** The wireless MAC Address is displayed in this field.

**Scan Nearby AP:** The Scan button provides a mechanism for the AP to scan for neighboring APs and provides various statistics on neighbors.
**Note:** Enabling Network Name (SSID) broadcast does not mean that everyone can connect to your network. They must have the correct wireless network key (password) to connect to the Gateway network. It only informs them that your network is present.

**Important:** Network Name (SSID) broadcasting is required for WPS.

**How to Set the Wireless Security**

It’s recommended to set a password on the WiFi networks you set up.

1. Go to the Admin Tool (http://192.168.0.1) using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see Accessing the Wireless Gateway Administrator Tool.

2. Click the **Wireless** tab then click the **Security** sub-tab. Here, you can set and display Wireless Network (2.4GHz and 5GHz) security information including the Network Name, Security Mode, Encryption, Network Password, and Key Interval.

   **Figure 23. **[Wireless Security Settings](#)

   Available settings include:

   **Network Name:** The Network Name is displayed here.

   **Security Mode:** Options for security settings include:

   - **2.4GHz:** Open, WPA2 Personal, WPA or WPA2 Personal
   - **5GHz:** Open, WPA2 Personal, WPA or WPA2 Personal

   The default setting is WPA or WPA2 Personal.

   **Encryption:** For ease of use, the encryption mode changes according to the selected security mode. For example: If the security mode is selected to be “WPA2 Personal”, the selected encryption mode will be AES. Similarly, if the security mode being used is WPA or WPA2 Personal, the encryption mode will be AES and TKIP.
Network Password: You must select a password that meets the requirements of the encryption type being used:

- **Open**: No password needed
- **WPA2 Personal**: at least 8 characters
- **WPA or WPA2 Personal**: at least 8 characters

**Key Interval**: The default is 3600 seconds.

Be sure to click the Save button at the bottom of the screen after making any changes.

### How to Start a WPS Session

WiFi Protected Setup (WPS) allows users to easily connect to the wireless network by simply pushing a button or entering a PIN code. WPS permits home users to easily connect to a secure network without any complex configuration and eliminates the need to remember or store their security information in an unsafe way.

The CGA4131 supports the WPS Push-Button Configuration (PBC). In this method, the user pushes a button, either an actual or a virtual one, on both the access point and the new wireless client device.

The CGA4131 provides two WPS PBC buttons:

- Hardware button on the front panel
- Software button on the Web UI

Pressing either PBC button on the CGA4131 will flash the WPS LED and initiate the WPS PBC operation. Then, press the software PBC button on the client device (some clients use a hardware button). The two buttons must be pushed within 60 seconds of each other.

Using the Admin Tool, click the Wireless tab and then click the WPS control tab. The screen displays WPS setup information. Here a user can set and display WPS parameters including the Access Point PIN and Connection Method (Push Button / PIN Number).
**Figure 24. WPS Settings**

![Gateway Wireless Access Point Diagram]

- **Wi-Fi Protected Setup (WPS)**: On
- **Access Point PIN**: 35973416
- **Connection Method**: Push Button (recommended)

**2.4GHz Wireless Network**
- **Network Name**: UAT_cWAN_2.4GHz
- **Security Mode**: None

**5GHz Wireless Network**
- **Network Name**: UAT_cWAN_5GHz
- **Security Mode**: None
How to Prevent Devices from Accessing Your Wireless Network

MAC Address

A MAC (Media Access Control) address is a unique hexadecimal code that identifies a device on a network. Each network-enabled device has at least one unique MAC address.

For example, if your computer is equipped with an Ethernet and a wireless network adaptor, each of these interfaces will have its own MAC address.

MAC Filtering

When using MAC filtering, you allow or deny devices to access your network based on their MAC address.

1. Go to the Admin Tool (http://192.168.0.1), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see Accessing the Wireless Gateway Administrator Tool.

2. Click the Security tab then click the Device Filter tab.

Result: The Device Filter settings screen displays.

Figure 25. Device Filter Settings

The Device Filter screen is used to allow or block devices connecting to the router, for both LAN and WiFi clients. The devices are allowed or blocked with respect to their MAC address, which is added in the allowed devices list in this screen. You can add devices through auto-learned devices under the device list or add a device manually under the Allowed Devices list.
Security Tab / Device Filter

Device Filter setup information includes:

- **Device Filter Status** – Enabled / Disabled
- **Access Type** – Allow All / Block All
- **Blocked Devices List** – Computer Name, MAC Address, When Block, and Delete
- **Devices List** – List of auto-learned devices (Computer Name, MAC Address, Status, and Operation)

You can enable or disable this feature, select the filter type (Allow All or Deny All) and add devices into the Blocked List.

**Enable Device Filter**

Device Filter can be enabled with Access Type set to either Block All devices or Allow All devices status.

**Block All**

When the Block All option is selected, all devices except in the Allowed Devices list are blocked for Internet access.

**Allow All**

When the Allow All option is selected, all devices except in the Blocked Devices list are allowed for Internet access.

**Options for Time of the Day Filters – When Block**

When you configure the When Block option to select the day of the week and the time of the day, the device filter is activated only for the selected time of the day.
Terms of Use and Guest Splash Page

In accordance with the Digital Millennium Copyright Act of 1998, an auto-enabled Terms of Use splash page permits Cox Business Internet Gateway customers to offer their guests a more secure WiFi experience.

Customers who wish to use a business’s Guest WiFi must check the box indicating you have read and agree to the WiFi Terms of Service and Acceptable Use Policy box and click the Submit button before they can access the Internet. Failure to do so will prevent access.

Figure 26. Internet Access Terms of Use splash page
Internet Security

The Gateway offers the following options to secure your Internet connection:

- Access Control
- Manage sites and devices
- Manage devices
- Managed services (Port Blocking)
- Firewall
- Reports

Access Control

The Access Control function:

- Prevents access to specific websites based on the URL or keywords.
- Prevents access requests from certain devices.
- Prevents access to specific applications or services (for example, FTP).

There are options within this feature to trust certain devices that are permitted to bypass these rules.

Manage Sites and Devices

The Access Control screen is used to block websites based on their URL and add devices which can be considered as “Trusted”. Trusted devices can access all websites.

Security Tab / Access Control

Click the Security tab then click Access Control tab.

This screen displays the following Site Filter setup information which can be viewed and set:

- **Site Filter Status** – Enabled / Disabled
- **List of Blocked Sites** – with Content, Type, When, Delete information
- **Trusted Devices** – List of devices auto-learned in the gateway with Computer Name, MAC Address, IP Address, Trusted information
Figure 27. Access Control Settings

**Blocked Sites**

To create a new entry in the Blocked Sites list, add the URL details, type and time of day for the filter. There is an option to delete the URLs from the Blocked Sites list.

**Trusted Devices**

You can override the URL blocking feature for specific devices. They need to be added in the Trusted Devices list with Trusted button enabled.

**Manage Devices**

The Device Filter screen is used to allow or block devices connecting to the router, for both LAN and WiFi clients. The devices are allowed or blocked based on their MAC address. There are flexible rules that allow devices to be blocked based on the time of day.

**Security Tab / Device Filter**

Click the Security tab then click the Device Filter tab. The screen displays following Device Filter setup information:

- **Device Filter Status** – Enabled / Disabled
- **Access Type** – Allow All / Block All
- **Blocked Devices List** – Computer Name, MAC Address, When Block, and Delete
- **Devices List** – List of auto-learned devices (Computer Name, MAC Address, Status, and Operation)

**Figure 28. Device Filter Settings**

On this screen, you can enable or disable the feature, select the filter type (**Allow All** or **Deny All**) and add devices into the Blocked List. Each option is explained below.

**Enable Device Filter**

Device Filter can be enabled with Access Type set to either **Block All** devices or **Allow All** devices status.

**Block All**

When the **Block All** option is selected, all devices except in the Allowed Devices list are blocked for Internet access.

**Allow All**

When the **Allow All** option is selected, all devices except in the Blocked Devices list are allowed for Internet access.
Options for Time of the Day Filters – When Block

When you configure the **When Block** option to select the day of the week and the time of the day, the device filter is activated only for the selected time of the day.

**Managed Services (Port Blocking)**

The **Service Filter** screen is used to block certain service requests coming from the LAN to WAN devices connected through the router. You can block the desired service port range by adding it to Blocked Services.

**Security Tab / Service Filter**

Click the **Security** tab then click the **Service Filter** tab. The screen displays the following Service Filter setup information:

- **Service Filter** – Enable / Disable
- **Blocked Services** – The specific traffic / service that is blocked using the Service Filter. This could be protocols or port numbers. The name of the service can be set by the user, along with TCP/UDP, the Start Port, and the End Port. The service can be blocked or allowed according to the time using the **When** field.
- **Trusted Devices** – List of auto-learned devices in the LAN. Service filter can be enabled or disabled for these devices by selecting the **Trusted** option.

**Figure 29. Service Filter Settings**

Slide the **Service Filter** toggle to the right to enable this option.
**Blocked Services**

Creating the list of blocked services can be done by adding an entry and selecting the protocol and port information. You can configure the time of the day configurations when using the option (the time when the filter should be enabled).

**Trusted Devices**

Trusted devices can bypass the list of services that are blocked. The devices are identified by their MAC address.

**Firewall**

The Gateway comes with an integrated firewall that helps you protect your network from attacks from the Internet. This firewall has several predefined levels to allow you to adjust the firewall to your needs.

The following table explains the traffic restrictions while setting the firewall level to various levels – **High**, **Medium**, **Low** and **Off**.

<table>
<thead>
<tr>
<th>Firewall level</th>
<th>Restrictions on inbound traffic</th>
<th>Restrictions on outbound traffic</th>
<th>Remarks</th>
</tr>
</thead>
</table>
| High          | All unsolicited inbound traffic is blocked, and Intrusion Detection is enabled. | All traffic except the following are restricted:  
  - HTTP and HTTPS (TCP ports 80, 443)  
  - DNS (TCP/UDP port 53)  
  - NTP (UDP ports 119, 123)  
  - Email (TCP ports 25, 110, 143, 465, 587, 993, 995)  
  - VPN (GRE, UDP port 500, TCP port 1723)  
  - iTunes (TCP port 3689) | Both inbound and outbound traffic are restricted |
| Medium        | Inbound traffic is blocked for the following services:  
  - IDENT protocol (TCP port 113)  
  - ICMP request  
  - Peer-to-Peer applications  
  - Kazaa (TCP/UDP port 1214)  
  - BitTorrent (TCP ports 6881-6999)  
  - Gnutella (TCP/UDP port 6346) | No restrictions – Outbound connections are allowed by the firewall regardless of the service or port(s) being used for the connection. |
<table>
<thead>
<tr>
<th>Firewall level</th>
<th>Restrictions on inbound traffic</th>
<th>Restrictions on outbound traffic</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Vuze (TCP ports 49152-65534)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intrusion Detection is enabled in</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>the Medium operating level. All</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>other inbound traffic is allowed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>by the firewall. Please note that</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>unsolicited inbound traffic will</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>not be forwarded to devices on</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>home network unless they match a</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>port forwarding / triggering rule,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>or a DMZ host has been configured.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>Inbound traffic is blocked for the</td>
<td>No restrictions - outbound</td>
<td></td>
</tr>
<tr>
<td></td>
<td>following services:</td>
<td>connections are allowed by the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• IDENT protocol (TCP port</td>
<td>firewall regardless of the service</td>
<td></td>
</tr>
<tr>
<td></td>
<td>113)</td>
<td>or port(s) being used for the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intrusion Detection is enabled in</td>
<td>connection.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the Low operating level. All other</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>inbound traffic is allowed by the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>firewall. Please note that</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>unsolicited inbound traffic will</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>not be forwarded to devices on</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>home network unless they match a</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>port forwarding / triggering rule,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>or a DMZ host has been configured.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Off</td>
<td>No restrictions. Can be enabled</td>
<td>No restrictions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>through port forward/ port</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>trigger/DMZ rule</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The default Firewall setting is **Minimum Security (Low)**. This means that **all** traffic passing through the Gateway (from and to the Internet) is allowed.
Changing the Security Level

Proceed as follows:

1. Go to the Admin Tool (http://192.168.0.1), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see Accessing the Wireless Gateway Administrator Tool. On the menu, click Security and then Firewall.

   Figure 30. Firewall Settings

![Firewall Settings Diagram](image_url)
Reports

The report screen displays all events generated by firewall rules. For example, if the firewall breach attempt was registered, the same would be logged as a firewall breach attempt and shown under firewall logs. Similarly, if there were incidents for Device filter, Service filter or Site filter restrictions, they would be shown in the respective logs. Each line item in the report display has the timestamp of the last such occurrence, with number of attempts and the incident type with a brief description.

To display security reports, select the Security tab in the Gateway screen and then select the Report tab. The following types of reports are available:

- Device Filter logs
- Site Filter logs
- Service Filter logs
- Email Settings logs
- Firewall Logs

![Security Reports](image-url)
Advanced Configuration

This chapter covers more advanced features. The following topics are covered:

- Port configuration for applications and services
- UPnP (Universal Plug and Play)
- Port Forwarding
- Port Triggering
- Port Filtering
- Configure a DMZ Host
- Dynamic DNS
- Assigning a Reserved IP (static IP) to a Device

**Port Configuration for Applications and Services**

The Gateway allows you to use one Internet connection for multiple computers. This means that all your computers share one public IP address, as if only one computer were connected to the outside world.

**Issue**

When the Gateway receives an incoming message, the Gateway must decide to which computer it should send this message. If the incoming message is a response to an outgoing message originating from one of your computers, the Gateway sends the incoming message to this computer.

*Figure 32. Gateway Message Handling – Incoming Response to Outgoing Message*
The Gateway will not be able to resolve the destination if:

- The incoming message arrives on a different port as the outgoing message. The Gateway will not know that the two messages are related.
- There is no outgoing message.

**Figure 33. Gateway Message Handling – Incoming Message Arrives on a Different Port or There is no Outgoing Message**

**Solutions**

To avoid this problem, the Gateway offers the following solutions:

- The Gateway supports automatic device discovery and port configuration for UPnP-enabled devices. For more information, see *UPnP (Universal Plug and Play)*.
- The Gateway allows you to assign a port to a device. For more information, see *Port Forwarding*.
- The Gateway allows you to define multiple trigger ports. When a device sends data over one of these ports, the Gateway will automatically assign several related ports to the device. For more information, see
• *Port* Triggering.

**UPnP (Universal Plug and Play)**

UPnP is designed to automate the installation and configuration of a (small) network as much as possible. This means that UPnP-capable devices can join and leave a network without any effort of a network administrator.
Supported Operating Systems
The following operating systems support UPnP:

UPnP and the Gateway
UPnP offers you the following benefits:

- You do not have to manually create port mappings to run services on a computer. The automatic port configuration mechanism for UPnP-enabled applications will do this for you. If the application is UPnP-enabled, UPnP will create these entries automatically.
- You can access the Admin Tool without having to remember the address of the Gateway.

Enable UPnP on the Gateway
1. Go to the Admin Tool (http://192.168.0.1), using a computer or device that is currently connected to your Gateway (either wired or wirelessly).
2. Click the Application menu and click the UPnP toggle to turn on.
   Result: The UPnP screen appears.

Figure 34. UPnP Settings

3. Click the toggle button to enable UPnP.
4. Click Save.

Port Forwarding
Port forwarding allows you to forward incoming Internet traffic arriving on a specific port to an internal IP address. For example, if you are running a web server and the Gateway receives a request on port 80, this request should be forwarded to your web server.

Use a Reserved IP Address
The target device of the port forwarding rules will be specified by an IP address. Make sure that your device uses a fixed (static) IP address. If you don’t, the device might receive a new IP
address later and the port forwarding rule will no longer be applied to the device. For more information, see *Assigning a Reserved IP (Static IP) to a Device*.

Proceed as follows:

1. Go to the Admin Tool (http://192.168.0.1), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *Accessing the Wireless Gateway Administrator Tool*.

2. Click the Application tab and then the Port Forward sub tab. **Result:** The Port Forward screen appears.

3. Click the Port Forward toggle to turn on the function.

4. Enter the range of ports and the types of traffic to forward to an IP address. The range information can be configured in Start Port and End Port fields; and you can select either TCP traffic only or UDP traffic only or BOTH.

5. The Server IP should be the IP address of the target device. In *Figure 35*, the gateway is configured to forward TCP traffic on ports 2-20 to IP address 192.168.0.10.

6. Click the Enable toggle to turn on Port Forwarding. (To disable the port, click the Enable toggle so that it moves to the left.)

7. Click the Save button.

8. *(Optional)* Click the green X under the Delete column to remove the port and click the Save button.

*Figure 35. Port Forward Table Settings*
Port Triggering

Port triggering allows you to define a set of dynamic port forwarding rules that will be activated as soon as a device sends traffic to the Internet over a specific port(s), the trigger port(s).

The differences compared to the Port Forwarding function are:

- Port triggering rules will only be activated if a local device is sending traffic over one of the trigger ports. There must be outbound traffic first.
- Port triggering rules forward the traffic to any device that has initiated the communication while port forwarding only forwards to a specific fixed IP.
- Port triggering rules allow you to translate the port numbers. This means that the incoming port can differ from the target port.
- If no outgoing traffic is detected on the Trigger Range ports for 10 minutes, the Target Range ports will close.

This is a safer method for opening specific ports for special applications such as, video conferencing programs, interactive gaming, file transfer in chat programs, etc. They are dynamically triggered and not held open constantly or erroneously left open via the router administrator and exposed for potential hackers to discover.

1. Go to the Admin Tool (http://192.168.0.1), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see Accessing the Wireless Gateway Administrator Tool.
2. On the Application menu, click Port Trigger.

Result: The Port Triggering screen appears.

Figure 36. Port Triggering Settings
**Port Filtering**

The Port Filter screen is used to block certain port requests coming from outside (WAN) devices to the devices on your local network (LAN) connected through the router. You can set the range of ports to be blocked by this feature.

1. Go to the Admin Tool (http://192.168.0.1), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *Accessing the Wireless Gateway Administrator Tool*.

2. On the Application menu, click **Port Filter**.

   **Result:** The Port Filter screen appears (see *Figure 37*).

The screen displays the following Port Filter setup information, which can be viewed and modified by the user:

- Range of Ports
- Traffic / Protocol
- Enable the filter
- Delete the filter entry

![Figure 37. Port Filter Settings](image)

**Configure a DMZ Host**

The DMZ feature exposes the network user to the Internet for using special-purpose services such as Internet Gaming or Video Conferencing. DMZ hosting forwards all the ports at the same time to one computer. The Port Forwarding feature is more secure because it only opens the ports the user wants to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer to the Internet. This is generally used if PCs are running specific applications that use random unknown port numbers and do not function correctly with specific port triggers or port forwarding setups.

It is advisable not to have any PCs/Servers as DMZ hosts because of exposure to the public Internet which results from this configuration. Remember to disable this setting if this is enabled temporarily for any specific application.
Any computer whose port is being forwarded must have its DHCP client function disabled and should have a static IP address assigned to it. Its IP address may change when it is using the DHCP function.

**Application Tab/DMZ**

Click the Application tab then click the DMZ tab. This screen displays DMZ setup information. Here, a user can enable the DMZ feature, enter the host address (both IPv4 and IPv6) and save the configuration.

![DMZ Settings](image)

**Dynamic DNS**

Dynamic DNS (DDNS) configures the Gateway's router functionality as a Dynamic DNS client. Dynamic DNS allows a dynamic IP address to be aliased to a static, predefined host name so that the host can be easily contacted by other hosts on the Internet, even if its IP address changes. The CGA4131 supports a dynamic DNS client compatible with the Dynamic DNS service (http://www.dyndns.com/).

1. Go to the Admin Tool (http://192.168.0.1), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see **Accessing the Wireless Gateway Administrator Tool**.

2. On the Application menu, click **DDNS**.
   **Result:** The Dynamic DNS screen appears. (See **Figure 39**.)

This screen displays DDNS setup information. Here, you can set and display DDNS (Disable, DynDns.org, TZO.com, Changeip.com, and Freedns.afraid.org), Username, Password and Hostname.
Figure 39. Dynamic DNS Settings

![Dynamic DNS Settings screenshot]
Assigning a Reserved IP (Static IP) to a Device

By default, each device will get an IP address from the Gateway’s DHCP server. When a device leaves, is turned off or the lease time of the address has expired, the IP address becomes available and can be re-used for other devices.

When you want to run a service on a network device (for example, a web server, network printer, etc.), it is advised to assign a “static IP” to the device. This way, the device will always be reachable on the same address and there is no risk that you are accessing the wrong device.

You can add a static IP through the LAN Setup screen. Click Connection and LAN to access this screen and then click Add Static IP.

Figure 40. LAN Setup: IPv4
Support

This section suggests solutions for issues that you may encounter while installing, configuring or using your Gateway. If the suggestions do not resolve the problem, look at the support screens on www.technicolor.com or contact your service provider.

This section describes the following topics:

- Wireless Connection Troubleshooting
- Network Diagnostic Tools
- Gateway Reboot and Reset Options

**Wireless Connection Troubleshooting**

**No Wireless Connectivity**

Try the following:

- Make sure that the wireless client is enabled (message like “radio on”).
- Make sure that the wireless client is configured with the correct wireless settings (network name, security settings).
- If the signal is low or not available, try to reposition the Gateway.
- Make sure that the wireless client supports the wireless band, protocol and the selected wireless security that are currently used by the access point.
• Change the wireless channel. See Change the Wireless Channel.
• Make sure that the access point is enabled. For more information, see Make Sure That the Wireless Access Point Is Enabled.

Poor Wireless Connectivity or Range

Try the following:
• Check the signal strength on the wireless client. If the signal is low, try to reposition the Gateway.
• If you are connected to the 5 GHz access point, try connecting to the 2.4 GHz access point instead.
• Change the wireless channel.
• Use WPAWPA2-PSK (TKIP/AES) as encryption.

For more information, see How to Configure a Wireless Client.

Change the Wireless Channel

Proceed as follows:
1. Go to the Admin Tool (http://192.168.0.1), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see Accessing the Wireless Gateway Administrator Tool.
3. In the Channel Width list, click 20MHz.
4. In the Channel dropdown, click one of the channels.
5. Click Save.
**Figure 42. Change the Wireless Channel: 2.4GHz Wireless Network**

![2.4GHz Wireless Network Diagram]

**Figure 43. Change the Wireless Channel: 5GH Wireless Network**

![5GH Wireless Network Diagram]

**Make Sure That the Wireless Access Point Is Enabled**

Proceed as follows:

1. Go to the Admin Tool (http://192.168.0.1), using a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *Accessing the Wireless Gateway Administrator Tool*.

2. Under **Wireless**, click **Radio**.

3. The Wireless Network screen appears. Ensure that the Wireless Interface toggle is set to enabled.
Cannot Connect via WPS
If you are having trouble connecting your wireless client via WPS, try to configure it manually. For more information, see


**Manually Connect Your Wireless** Client.

**Network Diagnostic Tools**

The Admin Tool offers the following diagnostic tools:

- **Ping**: Checks the network connectivity to a specific IPv4 or IPv6 address
- **Traceroute**: Displays the route/path and measures transit delays of packets across the network

Use the following steps to review the diagnostic tools.

1. Enter [http://192.168.0.1](http://192.168.0.1) in your web browser to access the admin site. You must use a computer or device that is currently connected to your Gateway (either wired or wirelessly). For more information, see *Accessing the Wireless Gateway Administrator Tool*.

2. On the Administration menu, click the **Troubleshooting** tab.

![Troubleshooting](image)

**Figure 44. Troubleshooting**
**Gateway Reboot and Reset Options**

The Gateway includes diagnostic tools that allow you to reboot the gateway or reset certain settings in it. The following tools are provided:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboot WiFi module</td>
<td>This function turns off the WiFi radio and then turns it back on. Choosing</td>
</tr>
<tr>
<td></td>
<td>“Reboot WiFi Module” will result in temporary loss of Internet access.</td>
</tr>
<tr>
<td>Reboot WiFi Router</td>
<td>This is the same as rebooting a wireless router attached to a cable</td>
</tr>
<tr>
<td></td>
<td>gateway. Choosing “Reboot WiFi Router” will result in temporary loss of</td>
</tr>
<tr>
<td>Reboot System</td>
<td>This reboots the entire system.</td>
</tr>
<tr>
<td>Reset Username &amp; Password</td>
<td>The Web UI username and password will be reset to default values.</td>
</tr>
<tr>
<td>Reset WiFi Settings</td>
<td>This restores WiFi parameters (e.g., SSID/WiFi network name, WiFi password)</td>
</tr>
<tr>
<td></td>
<td>to the factory set values. This operation results in clients being</td>
</tr>
<tr>
<td></td>
<td>disconnected from the WiFi network. The clients need to be reconnected</td>
</tr>
<tr>
<td></td>
<td>with the default network name (SSID) and password.</td>
</tr>
<tr>
<td>Reset Factory Settings</td>
<td>This resets all Gateway settings to Factory Default settings.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: A reset to factory default settings deletes all configuration</td>
</tr>
<tr>
<td></td>
<td>changes you made. Therefore, after the reset a reconfiguration of your</td>
</tr>
<tr>
<td></td>
<td>Gateway or a restore of a previously saved configuration. See *How to</td>
</tr>
<tr>
<td></td>
<td>Backup or Restore a Configuration*.</td>
</tr>
<tr>
<td></td>
<td>Also, your wireless clients will have to be re-associated, as described</td>
</tr>
<tr>
<td></td>
<td>in <em>Connect Your Wireless Devices</em>.</td>
</tr>
</tbody>
</table>

1. Click the **Administration** tab and then the **Reboot & Reset** tab.

**Result**: The screen displays Reboot and Reset options.
Figure 45. **Reboot and Reset Options**

![Gateway Administration Interface](image)

**Reset/Restore the Gateway via the Reset Button**

Proceed as follows:

1. Make sure that the Gateway is turned on.
2. If you want to:
   - **Reset the Gateway**, use a pen or an unfolded paperclip to push the recessed Reset button on the front panel of the Gateway for approximately five (5) seconds and then release.
   - **Restore the factory default settings of the Gateway**, use a pen or an unfolded paperclip to push the recessed Reset button on the front panel of the Gateway for at least 15 seconds and then release.
3. Restart the Gateway.

End of Document