COX BUSINESS®

Small Business Gateway

Technicolor model 4332

User Guide

Table of Contents

Overview

The Cox Business Internet Small Business Gateway (later referenced as "Gateway") provides seamless network management from the MyAccount portal. You can view and modify a connected wireless client, such as a tablet, smart TV, or smartphone to a wireless access point.

Check your device's documentation for more information.

This guide instructs you to:

- Set up your gateway and local network to use with Cox Business Internet
- Configure and use the main features of your gateway
- Configure Internet security

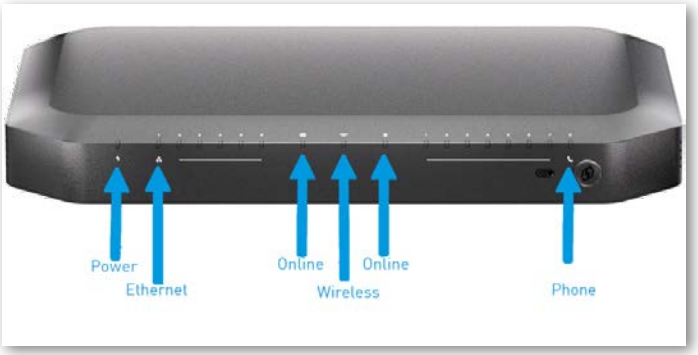

Figure 1. Technicolor 4332 gateway: front view

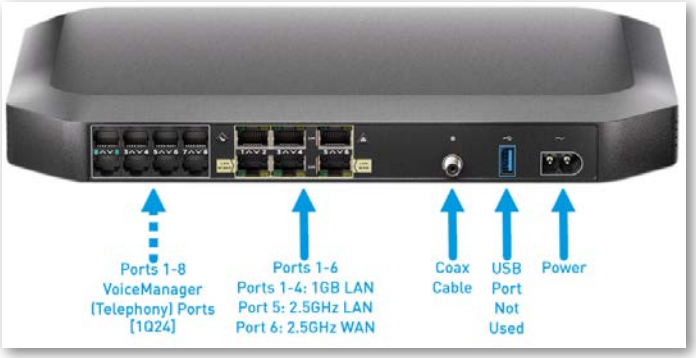

Figure 2. Ports on 4332

How to Configure a Static IP

Single Static IP address

Important: You will need a Static IP address from Cox Business before you proceed with the next set of steps. If you do not have a Cox Static IP address, please call us at 866-456-9944.

The gateway defaults to a Dynamic IP that changes regularly. If you require a Static IP, typically for your web/email server and security system, you can apply the Cox-assigned IP address to your gateway.

1. Log in to your MyAccount profile at myaccount.coxbusiness.com.
2. From the Welcome page, scroll to the My Services section and click the **Internet** sub-link.
3. Click the **View IP Addresses** icon. (See Figure 3)
4. Click the **Print PDF** button to capture your **Assigned Static IPs, Gateway, Netmask,** and **Primary** and **Secondary Name Server** values.
5. To get started, please connect to your SMB Gateway using either an Ethernet cable or WiFi.

   Enter http://192.169.0.1 in your web browser to open the Cox Wireless Cable Voice Gateway portal.

   - Locate Your Login Credentials: Your initial login details can be found on the label located on the bottom of the Small Business Gateway.
     - Username: admin
     - Password: Use the WiFi passphrase printed on the label.
   - Log In: Enter the username and password to access your gateway.
   - Change Your Password: You will be prompted to change the default password. Choose a password that you prefer and make it memorable.

6. Re-login: After updating your password, use the same username (admin) and the new password you just created to log in.
7. Select the Internet Configuration tile which will open the Internet Configuration page.
8. Please select the small pencil icon in the upper right hand corner of this page to enter Edit mode for your Internet Configuration. (See Figure 4)
9. Under the section labels WAN Connection Mode please select Static from the drop down menu. (See Figure 5)
10. Enter the values that Cox Business assigned your **WAN IPv4 Address** ("**Assigned Static IPs**" in MyAccount), **Subnet Mask** ("**Netmask**" in MyAccount), **Default Gateway** ("**Gateway**" in MyAccount), **Primary DNS** ("**Primary Name Server**" in MyAccount), and **Secondary DNS server** ("**Secondary Name Server**" in MyAccount).
11. Once you have completed these fields please select the Save button.

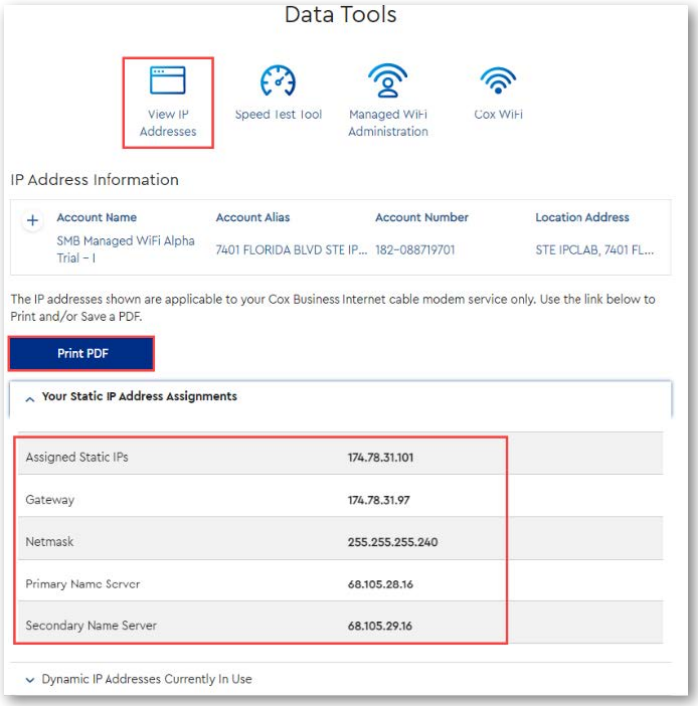

Figure 3. IP Address Assignments: MyAccount

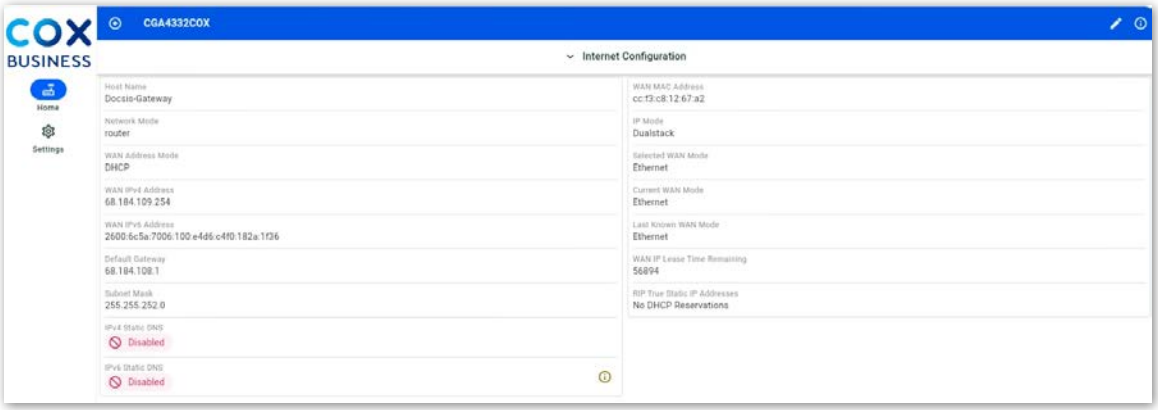

Figure 4. Connection/WAN: Gateway Portal

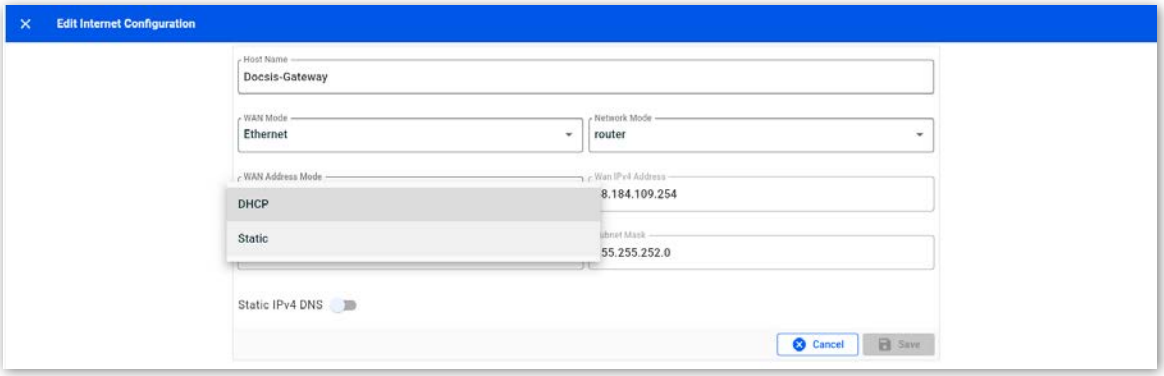

Figure 5. Wan Connection Mode

If you are adding multiple Static IP addresses, proceed to the next section.

Multiple Static IP Addresses—4332

To ensure that the routes are indeed being added to the routing table of your gateway we have 2 methods by which you can verify the correct CIDR block is ready for use.

MyAdmin

Look up the customer as you normally would and then proceed to click the Internet card at the top of the screen.

Select the 4332 by clicking the card and then clicking the link that is exposed at the bottom of the information that says Device Configuration:

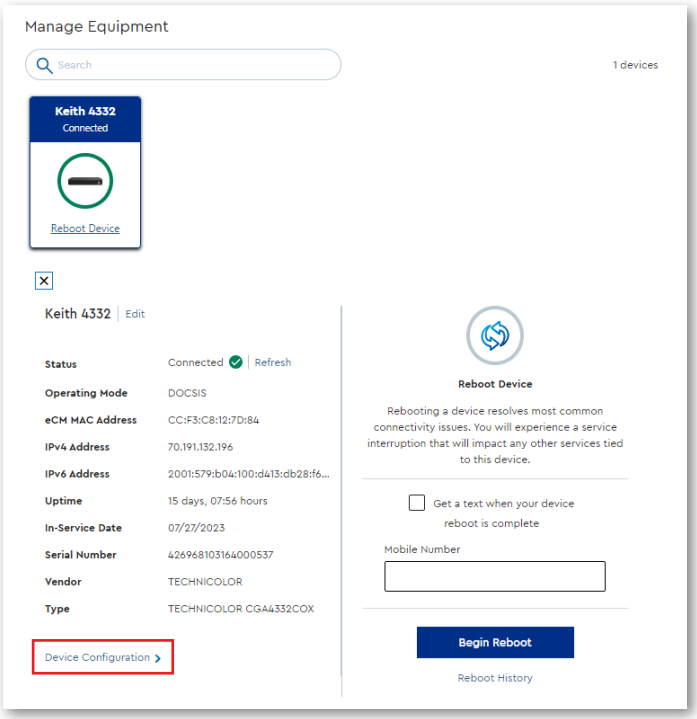

Figure 6.

Once in this menu you can select the Advanced Settings Tab and then click the Advanced Gateway Services Portal link.

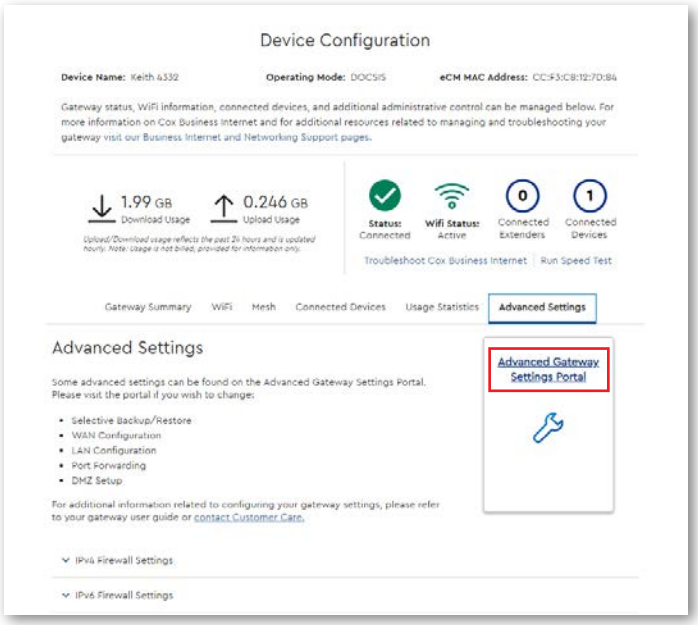

Figure 7.

This will open another tab and sign you into the Advanced Services Portal. Click the 4332 which will take you into the configuration menu. Click the Internet Configuration card and you will the see the CIDR blocks that have been assigned to this gateway:

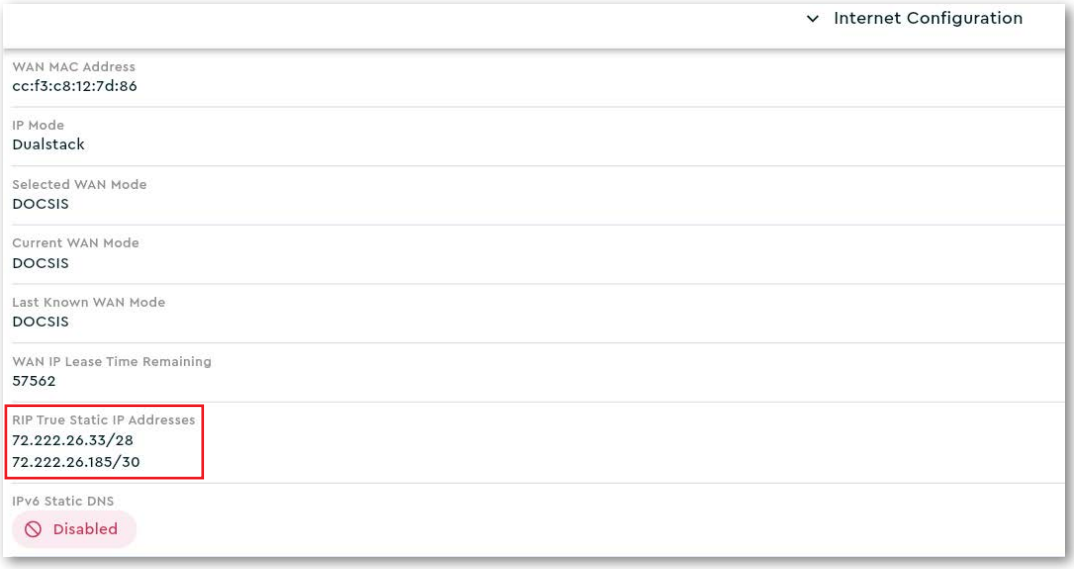

Figure 8.

Logging in to MyAccount

The Gateway portal is accessible through Cox Business MyAccount. Here, you can view the status of your gateway device, review general information about your WiFi, and manage your device's settings.

For more information on Cox Business Internet and for additional resources related to managing and troubleshooting your gateway, visit the Business Internet and Networking Support pages.

Use the following steps to access the Gateway portal through MyAccount.

1. Enter myaccount-business.cox.com in your web browser.
2. Enter your MyAccount email address in the **User ID** field.
3. Enter your MyAccount password in the **Password** field.
4. Click the **Log In** button.
5. Click the **Internet** tile.

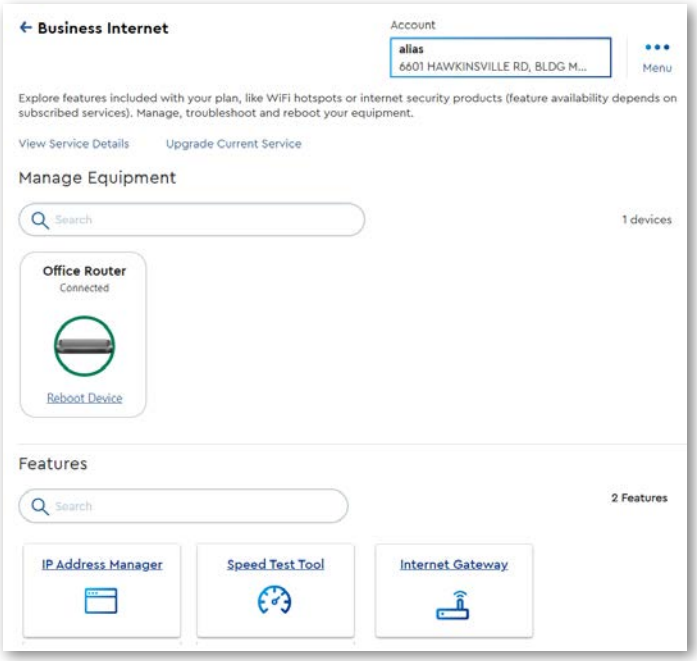

Figure 9. Business Internet Homepage

Modifying Gateway Settings via the MyAccount Portal

Your Gateway has been installed with unique settings based on your business needs. Should you require the configurations to be modified or restored determines the tile you click in the "Manage Equipment" section on the Business Internet page.

Two of the most common changes users make are renaming the **network (SSID)** and restoring the gateway's **configuration file**.

Changing the Device Name

Use the following steps to rename the SSID (the name of your business's network). (See Figure 6)

1. Repeat steps 1–5 in Logging in to MyAccount.
2. From the Business Internet page, scroll to the "Manage Equipment" section and click the device you want to rename. (**Note:** In the image below, the selected device is highlighted.)
3. Click the **Edit** link at the right of the existing name. The current name is "TECHNICOLOR CGA4332COX."
4. Enter the new name in the field provided and click the **Save** link.

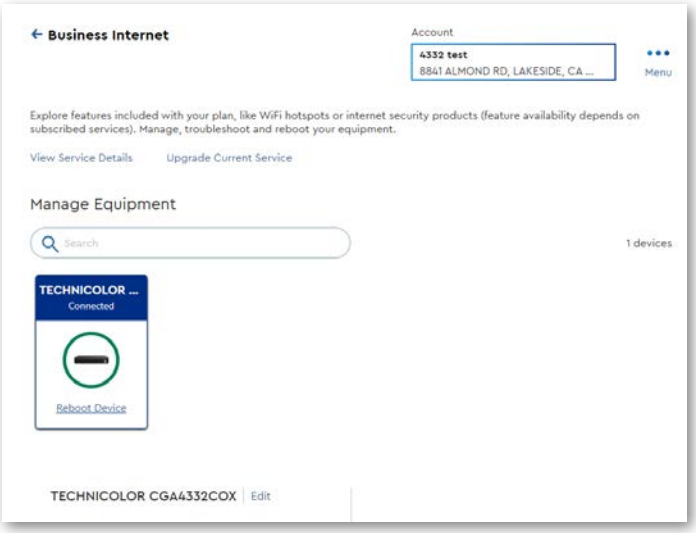

Figure 10. Gateway Name Change

Restoring the Gateway's Configuration

Before you restore your gateway's configuration, remember that **a backup of your WiFi and Firewall settings automatically generates every day between midnight and 8:00 a.m.** Therefore, unless you need to restore the gateway's configuration outside of these hours, you may elect to wait for it to happen automatically.

Use the following steps to restore the gateway settings.

1. Repeat steps 1–5 in Logging in to MyAccount.
2. From the Business Internet page, scroll to the "Manage Equipment" section and click the device you want to reconfigure.
3. Scroll to the bottom of the page and click the **Device Configuration** link.
4. Scroll to the middle of the page and click the **Advanced Settings** link in the toolbar.
5. Scroll to the "Advanced Settings" section.
6. Click the **Advanced Gateway Settings Portal** tile.
7. Click the image of the device you want to restore if there are multiple devices. (See Figure 8)
8. Scroll down the page and click the **Backup and Restore** tile. (See Figure 9)

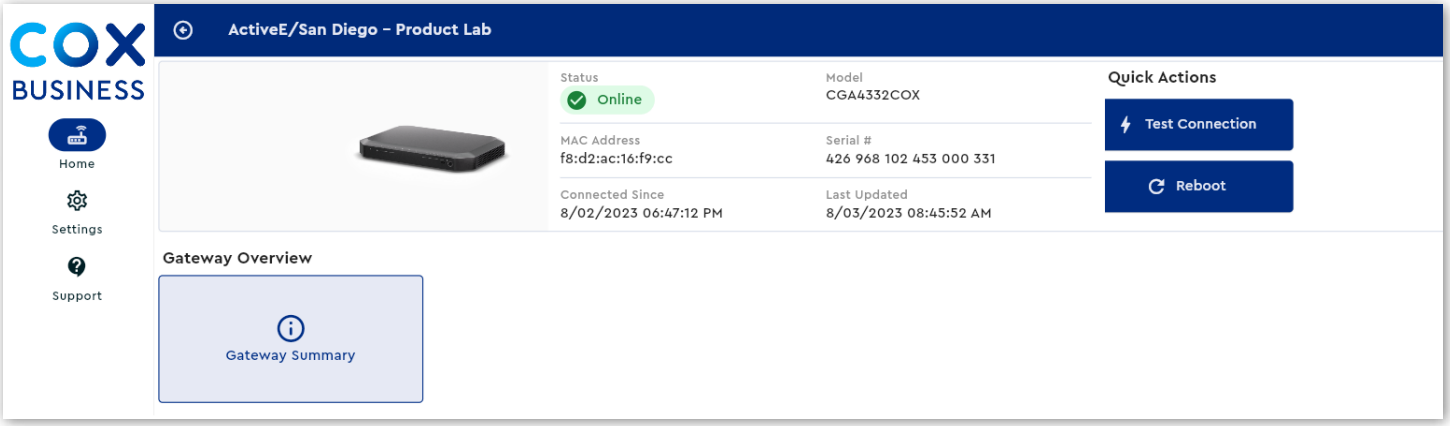

Figure 11. Small Business Gateway Portal: Main Page

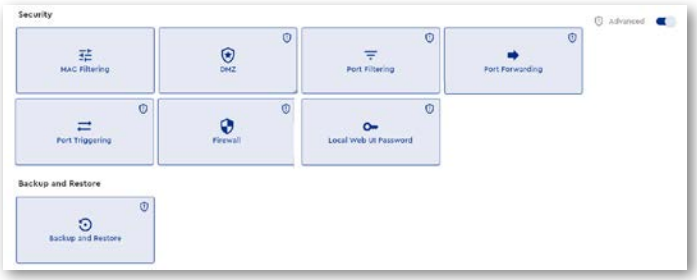

Figure 12. Security Backup and Restore

The following section instructs you to set up your wireless network. You will need a wireless access point (already integrated into your gateway) and a wireless client (a computer, smartphone, network printer, etc.)

Configuring Primary and Guest WiFi Settings

Connecting the 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 2.4 GHz access point provides connectivity to 802.11b/g/n wireless clients that are farther from the access point. Use this access point for legacy wireless clients.

– The 5 GHz access point provides superior transfer rates for 802.11a/n/ac wireless devices that are closer to the access point.

Figure 13. Network Configuration

Note: To connect the wireless client to the 5.0 GHz access point, confirm the wireless client supports 5.0 GHz connections.

Configuring 2.4 GHz and 5.0 GHz Frequency Bands for Primary WiFi

When you connect to a 2.4 GHz WiFi access point, you have fewer channels available from which to choose. As a result, WiFi tends to have more susceptibility to interference and lower connection speed. However, you have a greater range of geographical coverage.

When you connect to a 5.0 GHz WiFi access point, you have more channels available from which to choose. As a result, the frequency band may cut through network clutter and interference to maximize network performance. However, you have a decreased range of geographical coverage.

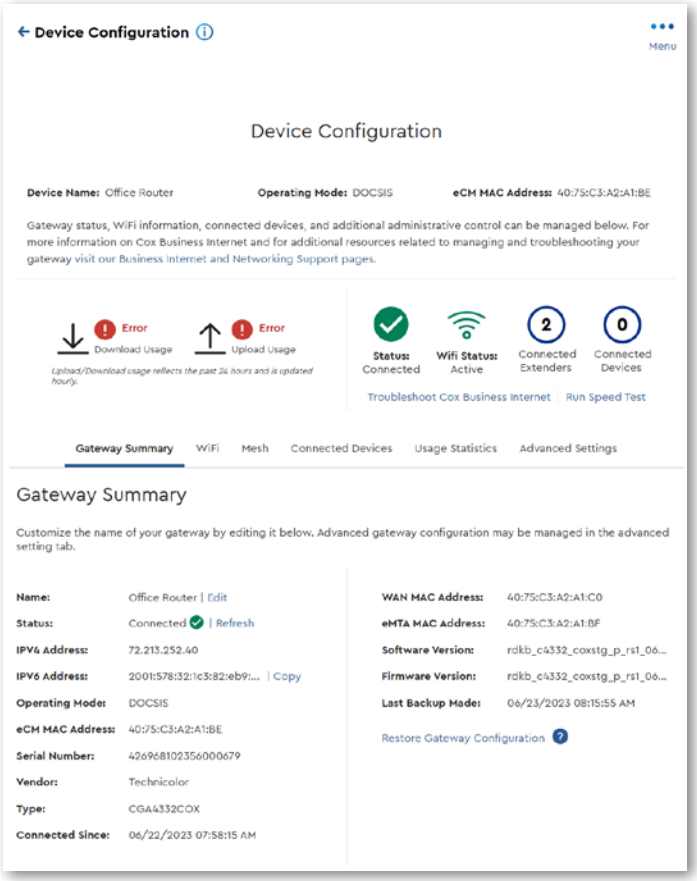

Figure 14. Device Configuration

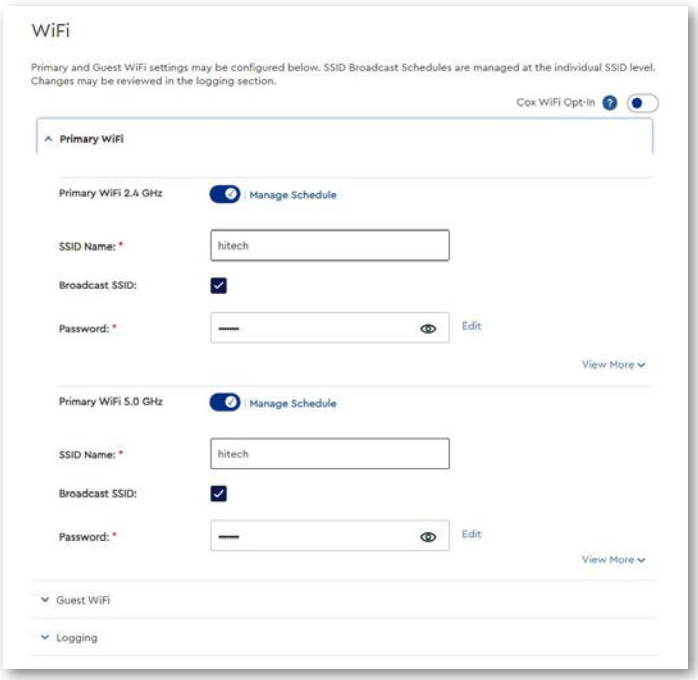

Figure 15. Primary WiFi 2.4 GHz

Use the following instructions to set up a 2.4 GHz or 5.0 GHz radio frequency for your primary (private) network.

1. Repeat steps 1–5 in Logging in to MyAccount.
2. Click the equipment tile that has an image of the device you want to configure.
3. Scroll to the bottom of the "Manage Equipment" section and click the **Device Configuration** link.
4. Scroll to the middle of the page and click the **WiFi** heading link in the toolbar.
5. Click the **Primary WiFi** down arrow to expand and the **View More** link on the right side of the page.
6. Click the **Primary WiFi 2.4** GHz toggle right to manage that frequency's settings. (**Note:** The **Manage Schedule** link at the right of the toggle enables you to set up an on/off schedule for your networks' broadcast availability.)
7. Enter the name of your ***primary*** (private) network, e.g., "OfficeRouter."

Important:
One benefit of our gateway is it performs band steering; however, this feature works only if your 2.4 GHz and 5.0 GHz SSIDs have the same name.

Should you create a different name for each band, gateway performance will likely be impacted.

8. Check the **Broadcast SSID** box if you want the name of the WiFi to display on the list of networks. Enter (or edit) the **Password** you want to use for your primary WiFi.
9. The **Channel Selection** drop-down menu offers two options: **Automatic** and Manual. The network selection process typically defaults to Automatic, which means your device will connect to the strongest network signal available. (**Note:** If you select "**Manual**," your device will detect if there are multiple, available networks and it will remain connected to it regardless of whether other networks become available.)
10. From the **Security** drop-down menu, select the option that best suits your business's needs. The options are:
    - 2.4GHz: Open, WPA2-Personal (AES), WPA3-Personal (AES) and WPA3-Personal-Transition (AES). **The default value for 2.4 GHz is WPA2-Personal (AES).**
    - 5GHz: Open, WPA2-Personal (AES), WPA3-Personal (AES) and WPA3—Personal-Transition (AES). **The default setting for 5.0 GHz is WPA3-Personal-Transition (AES).**

Note: Descriptions for each type of security are as follows:
- Open: no password needed
- WPA2 Personal: at least 8-character password
- WPA2-Transition: at least 8-character password
- WPA-WPA3

11. The **Encryption** mode defaults to AES and cannot be changed.

Note: The device's **WiFi Mode** determines which frequency range it uses to broadcast and receives signals, as well as its maximum download and upload speeds. The WiFi mode defaults to n, g for a 2.4 GHz speed. The WiFi mode defaults to a, n for a 5.0 GHz speed.

12. Expand the **WiFi Mode** drop-down and select the WiFi standard for your primary WiFi. The options are:
    - **802.11a** (for 5.0 GHz only)
    - **802.11ac** (for 5.0 GHz only)
    - **802.11g** (for 2.4 GHz speed only)
    - **802.11n** (for 2.4 and 5.0 GHz) supports several computers and other electronic devices at one time, so the router

continues to perform even when running computers, entertainment systems, and other peripheral items simultaneously. Operates on 2.4 GHz and 5.0 GHz at 600 Mbps.

- **802.11ax** (for 2.4 and 5.0 GHz) reduces the effects of interference and increase throughput in crowded urban and suburban environments.

Configuring 2.4 GHz and 5.0 GHz Radio Frequency Bandwidths for Guest WiFi

Wireless settings for Guest WiFi networks mirror the Primary WiFi setup for the respective GHz band.

Remember: The device's **WiFi Mode** determines which frequency range WiFi uses to broadcast and receive signals, as well as its maximum download and upload speeds.

You can set up to three (3) guest networks for 2.4 GHz and 5.0 GHz.

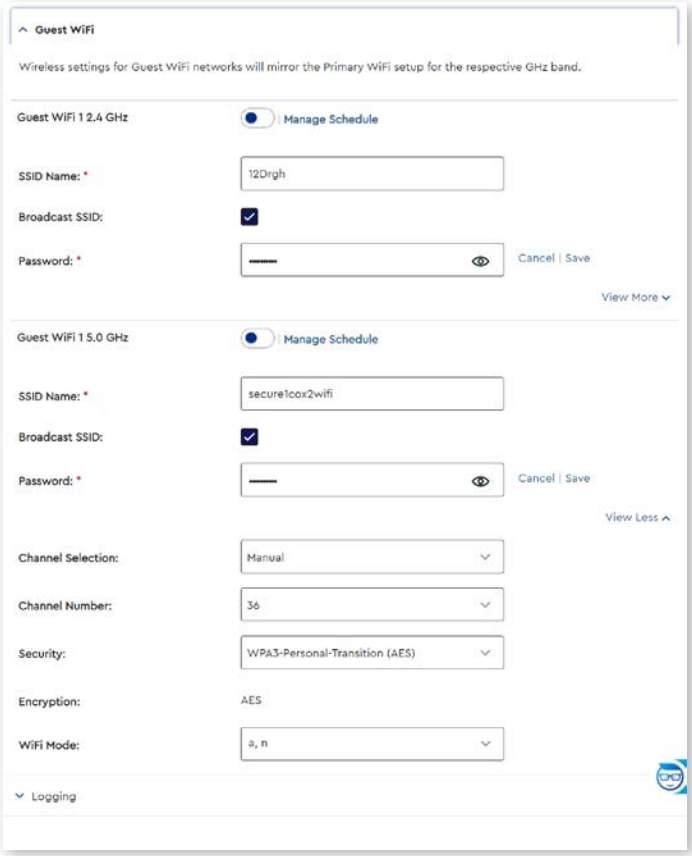

Figure 16. Guest WiFi Settings page

Use the following instructions to set up a 2.4 GHz or 5.0 GHz radio frequency for your guest (public) network.

1. Repeat steps 1–5 in Logging in to MyAccount.
2. Click the equipment tile that has an image of the device you want to configure.
3. Scroll to the bottom of the "Manage Equipment" section and click the **Device Configuration** link.
4. Scroll to the middle of the page and click the **WiFi** heading link in the toolbar.
5. Click the **Guest WiFi** down arrow to expand and the **View More** link.
6. Click the **Guest WiFi 2.4 GHz** toggle right to manage that frequency's settings. (**Note:** The **Manage Schedule** link at the right of the toggle enables you to set up an on/off schedule for your network's broadcast availability.
7. Enter the name of your guest (public) network.
8. Check the **Broadcast SSID** box if you want the name of your WiFi to display on the list of networks. Enter (or edit) the **Password** you want guests to use for guest WiFi.
9. The **Channel Selection** drop-down menu offers two options: **Automatic** and **Manual**. The network selection process typically defaults to Automatic, which means your device will connect to the strongest network signal available. (**Note:** If you select "**Manual**," your device will detect if there are multiple available networks, and it will remain connected to it regardless of whether other networks become available.)
10. Click the **Channel Number** drop-down and select the number of bands you need for your business. (Note: If you have a lot of congestion (usage) on a particular channel, choose a higher number to increase download and upload speed).

11. From the Security drop-down menu, select the option that best suits your business's needs. The options are:
    - 2.4GHz: Open, WPA2-Personal (AES), WPA3-Personal (AES) and WPA3-Personal-Transition (AES). **The default value for 2.4 GHz is WPA2-Personal (AES).**
    - 5GHz: Open, WPA2-Personal (AES), WPA3-Personal (AES) and WPA3-Personal-Transition (AES). **The default setting for 5.0 GHz is WPA3-Personal-Transition (AES)**

Note: Descriptions for each type of security are as follows:
- **Open:** no password needed
- **WPA2 Personal:** at least 8-character password
- **WPA2-Personal:** at least 8-character password
- **WPA**-WPA3

12. The **Encryption** mode defaults to AES and cannot be changed.

Note: The device's **WiFi Mode** determines which frequency range is used to broadcast and receive signals, as well as maximum download and upload speeds. The WiFi mode defaults to n, g for a 2.4 GHz speed. The WiFi mode defaults to a, n for a 5.0 GHz speed.

13. Expand the WiFi Mode drop-down and select the WiFi standard for your guest WiFi. Expand the WiFi mode drop down and select the WiFi standard for your guest WiFi. (See step 12 on the previous page for descriptions of each.)
14. Click the **Logging** drop-down to see the last 60 days (or 100 changes) made to advanced settings, such as changing the WiFi password, the name of the WiFi, the security option and channel selection.

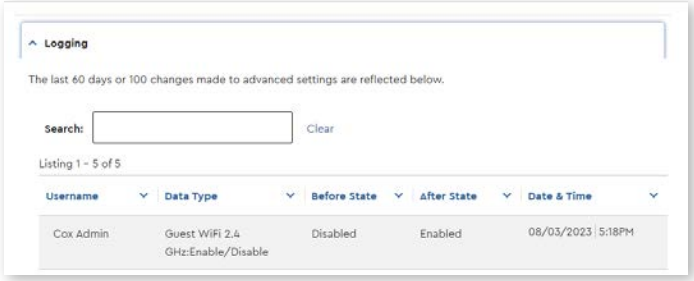

Figure 17. Logging sample

Viewing the Gateway's Connected Devices

Devices connected to the gateway in the last seven (7) days are captured in both a list and map view. Custom groups may be created and managed for quick access.

You can view information about a specific device in the table at the bottom of the page, create or manage search filters, and select a specific device to further customize the network map.

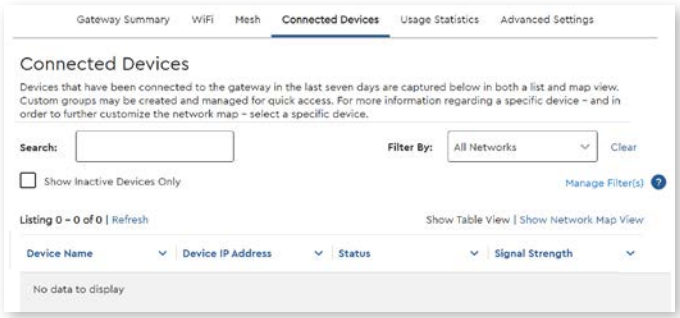

Figure 18. Connected Devices page

Use the following steps to view a device's IP address, status, and signal strength. You can also add up to 10 sort filters if you need to search through multiple devices.

1. Repeat steps 1–5 in Logging in to MyAccount.
2. Click the equipment tile that has an image of the device you want to configure.
3. Scroll to the bottom of the "Manage Equipment" section and click the **Device Configuration** link.
4. Scroll to the middle of the page and click the **Connected Devices** tab in the toolbar.

   Result: The Connected Devices page appears and displays a table of all devices that are connected to a specific network.

5. (Optional): If you want to create groups to better organize and manage devices connected to your network, click the **Manage Filters** link in the "Connected Devices" section of the page.
6. Click the **Add Filter** button to create another search field OR click the **Delete Filter** link to the right of the field you want to remove.
7. Click the **Save** button.

Viewing a Network's Usage Statistics

The Gateway Usage Statistics page displays how much a specific network has been used over the last 30 days and the previous 24 hours. It includes all wired and wireless connected devices.

Use the following steps to view a network's usage statistics.

1. Repeat steps 1–5 in Logging in to MyAccount.
2. Click the equipment tile that has an image of the device you want to configure.
3. Scroll to the bottom of the "Manage Equipment" section and click the **Device Configuration** link.
4. Click the **Usage Statistics** tab in the toolbar

Accessing Advanced Settings

The **Advanced Settings** tab enables you to configure or perform the following tasks:

- Selective backup/restore of the configuration
- WAN configuration
- LAN configuration
- Port forwarding
- DMZ setup

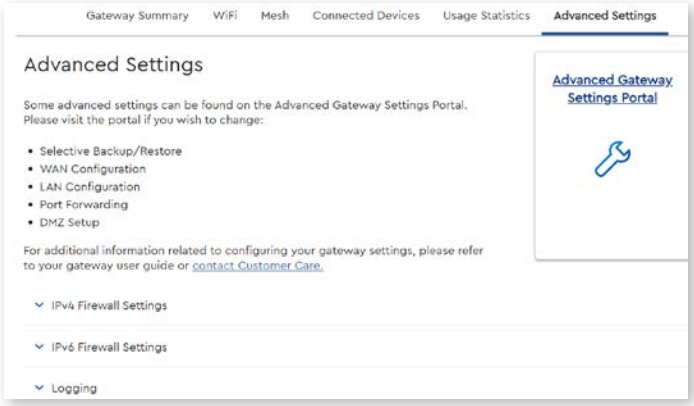

Figure 19. Advanced Settings page

Use the following settings to access the advanced gateway settings portal.

1. Repeat steps 1–5 in Logging in to MyAccount.
2. Click the equipment tile that has an image of the device you want to configure.
3. Scroll to the bottom of the "Manage Equipment" section and click the **Device Configuration** link.
4. Click the **Advanced Settings** tab in the toolbar.
5. (Optional): If you want to modify the **IPV4** and **IPV6 Firewall Settings**, click the respective drop-down arrows.

Modifying IPv4 Firewall Settings

6. From the Advanced Settings page, shown above, click the **IPv4 Firewall Settings** drop-down arrow.

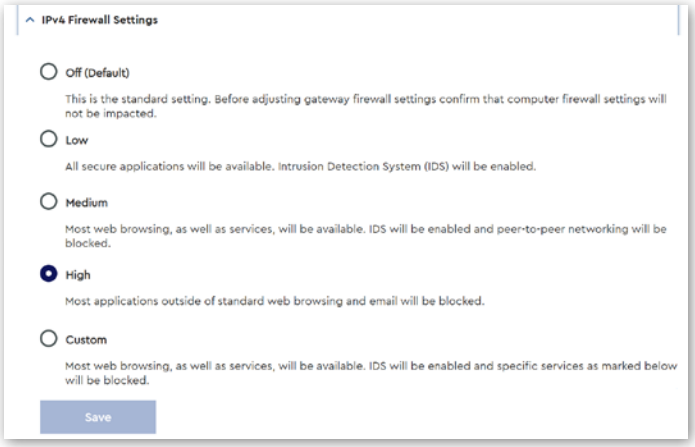

Figure 20. IPv4 firewall settings

7. Select the security level you want to use for your public or private network.
8. Click the **Save** button.

Modifying IPv6 Firewall Settings

Figure 21. IPv6 firewall settings

Use the following steps to modify the level of protection you want for your IPv6 firewall.

1. Repeat steps 1–5 in the "Accessing Advanced Settings" section above.
2. From the Advanced Settings page, shown above, click the **IPv6 Firewall Settings** drop-down arrow.
3. Select the security level you want to use for your public or private network.
4. Click the **Save** button.

Accessing the Advanced Gateway Settings Portal

The advanced gateway settings portal contains multiple options you may use to view and/or modify configuration settings.

Use the following steps to access the gateway portal.

1. Repeat steps 1–5 in Logging in to MyAccount.
2. Click the equipment tile that has an image of the device you want to configure.
3. Scroll to the bottom of the "Manage Equipment" section and click the **Device Configuration** link.
4. Click the **Advanced Settings** tab in the toolbar.
5. Click the **Gateway Advanced Settings Portal** tile.

Section heading	Advanced setting component(s)	
Gateway Overview	Gateway summary	
Network	Connected clients	Local network
	Internet configuration	Ethernet configuration
	Static addresses	NTP services
	DOCSIS summary	
WiFi	WiFi configuration	Add extender
	Mesh	
Security	MAC filtering	Port triggering
	DMZ	Firewall
	Port filtering	Local web UI password
	Port forwarding	
Backup and restore	Backup and restore	
Troubleshooting	Self care	Gateway logging
	SSID scanner	Networking troubleshooting

Accessing Gateway and Network Settings and Configurations

The **gateway** section is a view-only snapshot of the device's technical specifications, such as the vendor, serial number, hardware version, WAN MAC version, memory analytics and more.

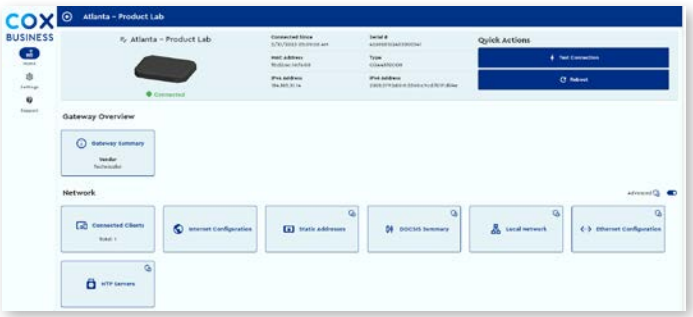

Figure 22. Gateway Overview and Network sections

Use the following steps to access the **gateway** summary.

1. Repeat steps 1–5 in Logging in to MyAccount.
2. From the Business Internet page, scroll to the "Manage Equipment" section and click the device you want to reconfigure.
3. Scroll to the bottom of the page and click the **Device Configuration** link.
4. Scroll to the middle of the page and click the **Advanced Settings** link in the toolbar.
5. Click the **Gateway Summary** tile.
6. Click the **DOCSIS Summary** tile to view technical specifications, such as the MAC address, CM status, IPv4 subnet mask, default gateway IP address and DHCP settings.
7. Click the **Local Network** tile to multiple IP address types and information about the IPv4 and IPv6 status.
8. Click the **Ethernet Configuration** tile to view the alias names, up/down status, MAC address and activation status.
9. Click the **Network Time Protocol (NTP) Services** tile to view the enablement status, synchronization status, time and time zone where the network is located.

Accessing WiFi/Security Settings and Configuration

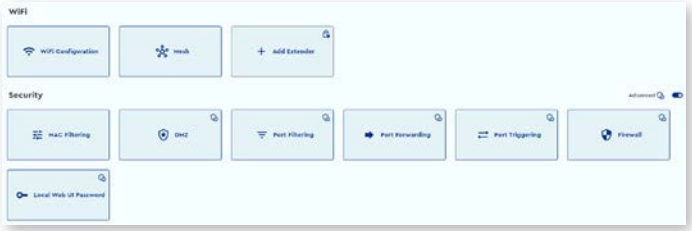

Figure 23. WiFi and Security sections

Use the following steps to access the WiFi section.

1. Repeat steps 1–5 in Logging in to MyAccount.
2. From the Business Internet page, scroll to the "Manage Equipment" section and click the device you want to reconfigure.
3. Scroll to the bottom of the page and click the **Device Configuration** link.
4. Scroll to the middle of the page and click the **Advanced Settings** link in the toolbar.
5. Click the **WiFi Configuration** tile.

   Result: You can view and edit settings for both the 2.4 GHz and 5.0 GHz primary (private) and guest networks. (**Note:** Click the **Access Schedule** link to enable or disable the time schedule, which means setting the days and times that your WiFi network turns off automatically)
6. Click the **Mesh** tile to join two or more WiFi access points together to create and share a single, seamless WiFi network.
7. Click the **Add Extender*** tile to increase the Internet range throughout areas of your business.

*The Add Extender feature is on the 2024 development roadmap.

Use the following steps to access the **Security** section.

1. Repeat steps 1–5 in Logging in to MyAccount.
2. Click the **Mac Filtering** tile to configure a security access control method. A MAC address assigned to each network interface controller is used to determine access to the network.
3. Click the **Port Filtering** tile to block certain port requests that arrive from outside (WAN) devices to the devices on your local area network (LAN) connected through the router. You can set the range of ports to be blocked by this feature.
4. Click the **Port Forwarding** tile 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.
5. Click the **Port Triggering** tile to define a set of dynamic port forwarding rules that are activated as soon as a device sends traffic to the Internet over a specific port(s) and/or trigger port(s).

The differences compared to the **Port Forwarding** function are:

- Port triggering rules are activated only if a local device sends 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 outgoing traffic is not detected on the Trigger Range ports for 10 minutes, the Target Range ports close. (**Note:** 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.)

6. Click the **Firewall** tile to view and modify the levels of security for both the IPv4 and IPv6. There are multiple levels: a low level for the Internet may be used for guest WiFi. A medium level should be for DMZ a high level should be used for your primary (private) WiFi.
7. Click the **Local Web UI Password** tile to set or modify an administrator's password. Click the **Confirm** button to save.

Accessing Backup/Restore and Troubleshooting Sections

Use the following steps to access the **Troubleshooting** section.

1. Repeat steps 1–5 in Logging in to MyAccount.
2. From the MyAccount homepage, click the **Internet** tile.
3. From the Business Internet page, scroll to the "Manage Equipment" section and click the device you want to investigate.
4. Scroll to the bottom of the page and click the **Device Configuration** link.
5. Scroll to the middle of the page and click the **Advanced Settings** link in the toolbar.
6. From the gateway portal page, scroll to the "Troubleshooting" section.
7. Click the **SSID Scanner** tile to begin a network scan on your Internet.
8. Click the **Gateway Logging** tile to view information about events, such as the name of the filter, a description of the event, the severity, the category and time of the event. You may view this information over the last 24 hours, three (3) days or seven (7) days.
9. Click the **Network Troubleshooting** tile to ping the network.

Extender(s) Installation Process

You can add WiFi Radio Network Extender(s) (referred to as Extenders) to your Small Business Gateway to increase the coverage area of your WiFi network. This low-cost enhancement to the dynamic Small Business Gateway can help customers like you who need WiFi coverage assistance, without requiring an upgrade to a more expensive and managed solution.

Our Cox Business WiFi Extenders are easy to install, troubleshoot, and manage through the MyAccount customer portal or our Cox Business WiFi Mobile App.

Both platforms offer customers a self-guided approach to connecting the Extender to your Cox Small Business Gateway. The guided digital experience includes recommendations for where and how to set up your new Extender, and informs you when the installation is optimized to improve WiFi network coverage.

An Extender can help in multiple scenarios, but it is important to understand what an Extender provides and what it doesn't. The Cox Business WiFi ecosystem continually monitors the health of your Extender, and makes adjustments to ensure your business-critical WiFi network is working as optimally as possible.

Extenders can assist and improve the reach and availability of your WiFi network in scenarios such as:

- **Obstacles:** Walls, hallways, and other architectural features that inhibit your Gateway from reaching certain areas of your business
- **Large Open Rooms:** Dining areas, warehouses, or patios that present challenges with coverage

Extenders cannot solve some issues that arise with WiFi networks such as:

- **Interference** from motors, machinery, or appliances such as microwaves
- **Older Devices:** Customers with older WiFi devices may not be able to take advantage of the benefits of newer Wifi standards
- **Multiple floors** or **multiple buildings**

For those challenges that an Extender doesn't resolve, our WiFi Cloud Optimization feature can curate and recommend changes to allow WiFi connection to your network in the best way possible. The following are automated changes, seamlessly dispatched to customers:

- Overloaded WiFi channels or those affected by outside interference are removed from the list of WiFi channels a client can use to connect. This ensures your WiFi clients are using the best path for optimal performance.
- Our WiFi mesh architecture ensures WiFi clients are always routed over the best possible WiFi Radio path for optimal performance. This assists with devices that roam or move about your WiFi network.

Installation

Extenders are packaged with all of the items you need for installation:

- Airties 4985 WiFi Radio Network Extender
- Power supply
- Ethernet cable
- A QR code to download the Cox Business WiFi Mobile App
  - Also, you can use our Cox Business MyAccount web portal.

Once you enter the MyAccount web portal or Cox Business WiFi Mobile App, you should see your Extender in a state *ready for setup*.

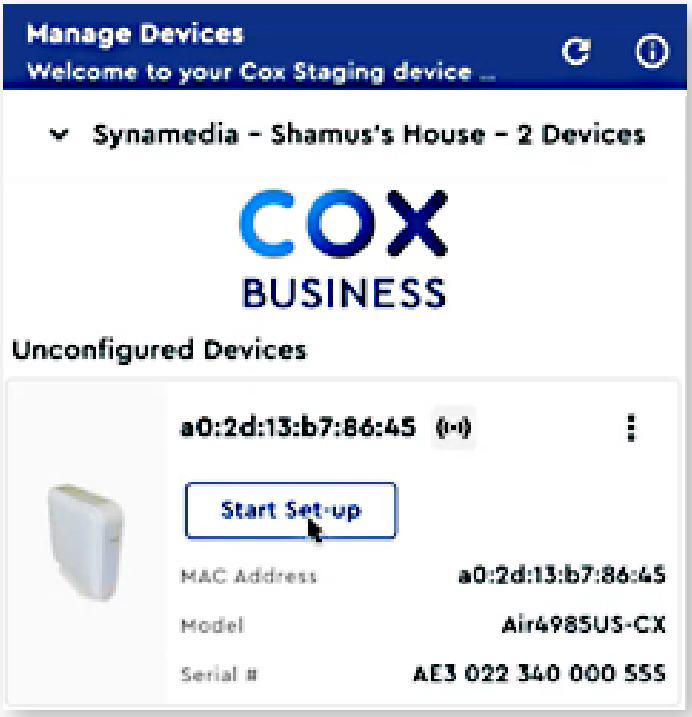

Figure 24. Start Set-up

Click the **Start** *Set-up* button to initiate the Extender configuration and placement wizard.

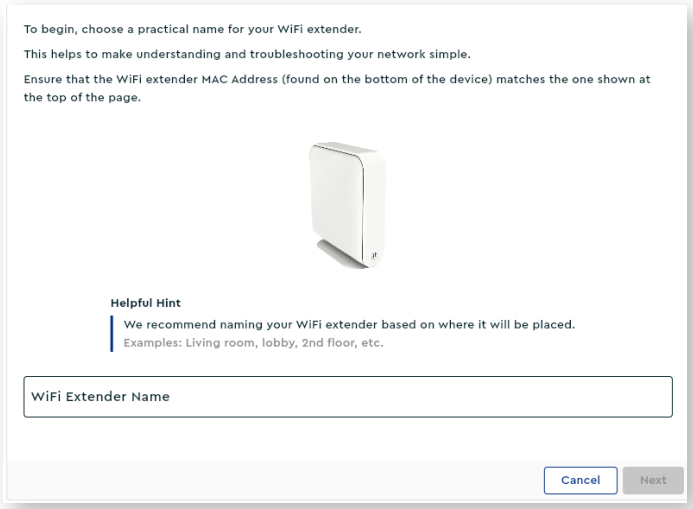

Figure 25. Naming Extender

Wiring the Extender

After you name your Extender, there are two methods to install and connect it:

Wiring Directly to Your Small Business Gateway via the Included Ethernet Cable

- Recommended.
- This is a step for connecting your Extender to the gateway. You will not need to keep it connected via Ethernet for the Extender to work as designed.

WPS (WiFi Protected Setup)

- There is a WPS button on the gateway that will initiate this connection.
- This method can be used when connecting via Ethernet for initial installation is not possible.

Connection Methods

Both methods are initially used for connecting your Extender to the Gateway. After completing the initial connection process, you can move the Extender to your desired location and finalize the placement.

- The Extender can be used wirelessly or wired via Ethernet, as both methods are utilized in the mesh network for optimal traffic flow.

After a successful connection has been established, it's time to place your Extender.

Placement

Once you have decided which method to use for installation, you can follow the step-by-step instructions in either the Cox Business WiFi Mobile App or the Cox Business MyAccount customer portal:

- Once connected, the wizard will provide suggestions on placement, such as placing the Extender halfway between the gateway and your problem area.

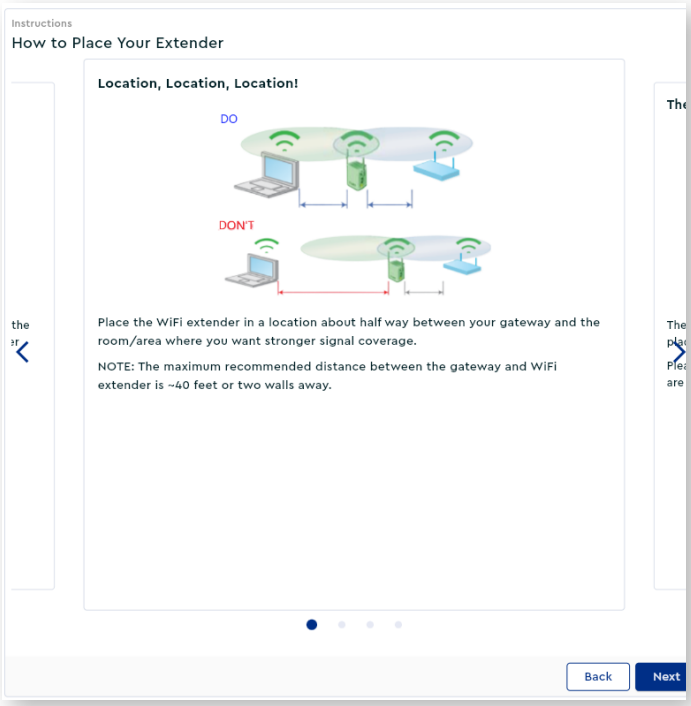

Figure 26. Extender Placement Suggestions

- After you have decided on placement, the wizard can analyze its position and give you a score indicating how well the Extender will work in this location and whether it's too close or too far from the gateway for optimal performance.

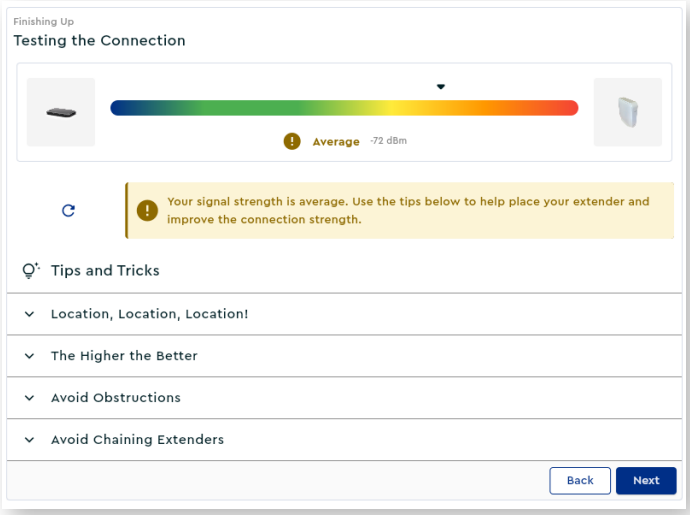

Figure 27. Extender Placement Score

Management

Now that you have placed your Extender in its optimal location, our Cox Business WiFi Cloud Optimization feature will monitor the performance of your Extender 24/7 to ensure its performance and stability remain constant.

Our customers can reboot their Extender, check its status (online/offline), and more.

You can continue to use the Cox Business WiFi Mobile App or MyAccount web portal to monitor the health of your network and Extender, see what's connected to your network, and access all of the other features described in this guide.

Once your Extender is successfully online and placed properly, our web portal/mobile app can you help you manage your Extender. Clicking on your Extender will open up a menu just for this device.

Figure 28. Network Device Status

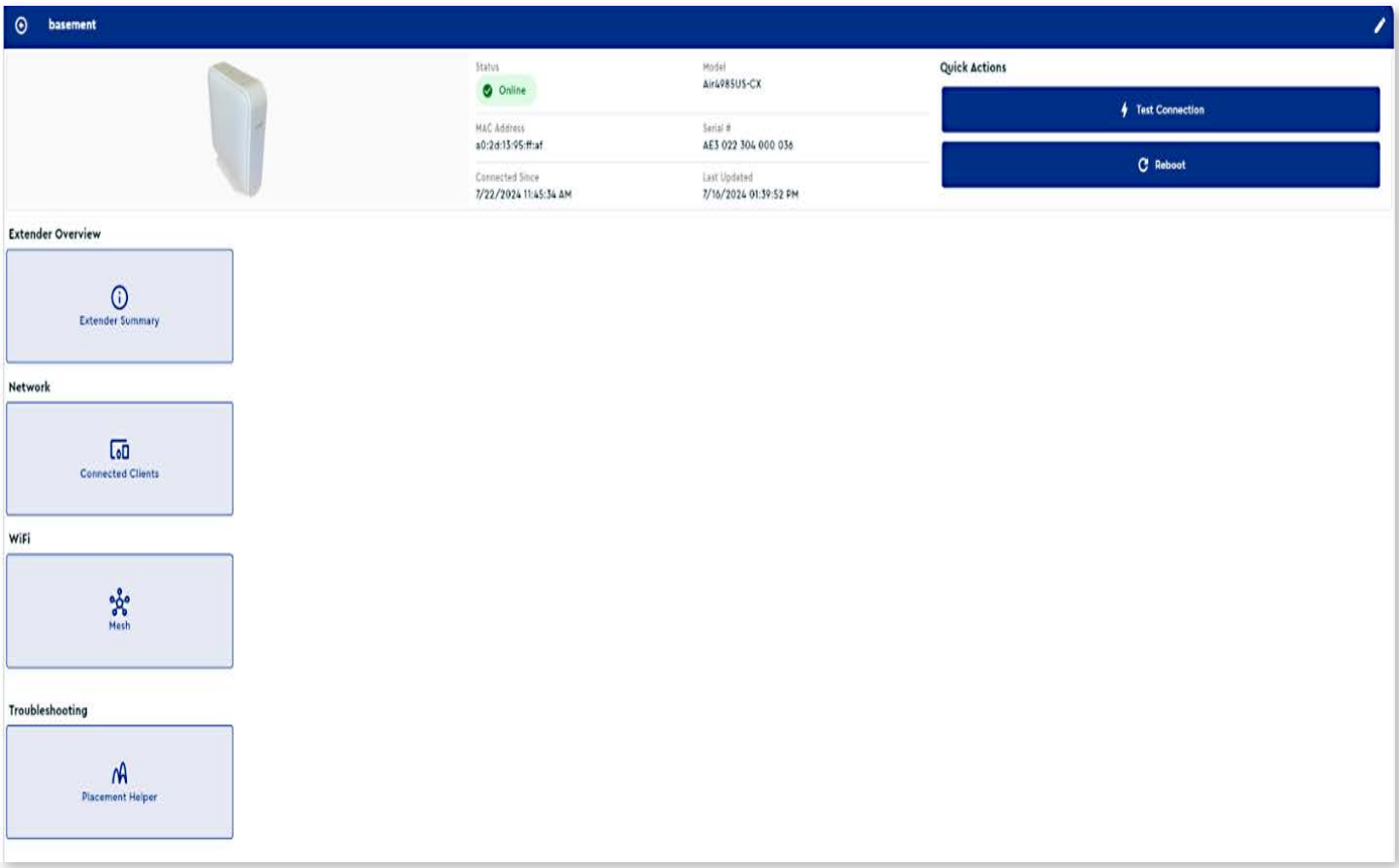

Figure 29. Extender Status

You can view general info about your Extender, see what is connected to your Extender, review your overall WiFi network topology, and even re-run the placement helper wizard for your Extender.

The Mesh card will open up a graphical visual of your Extender:

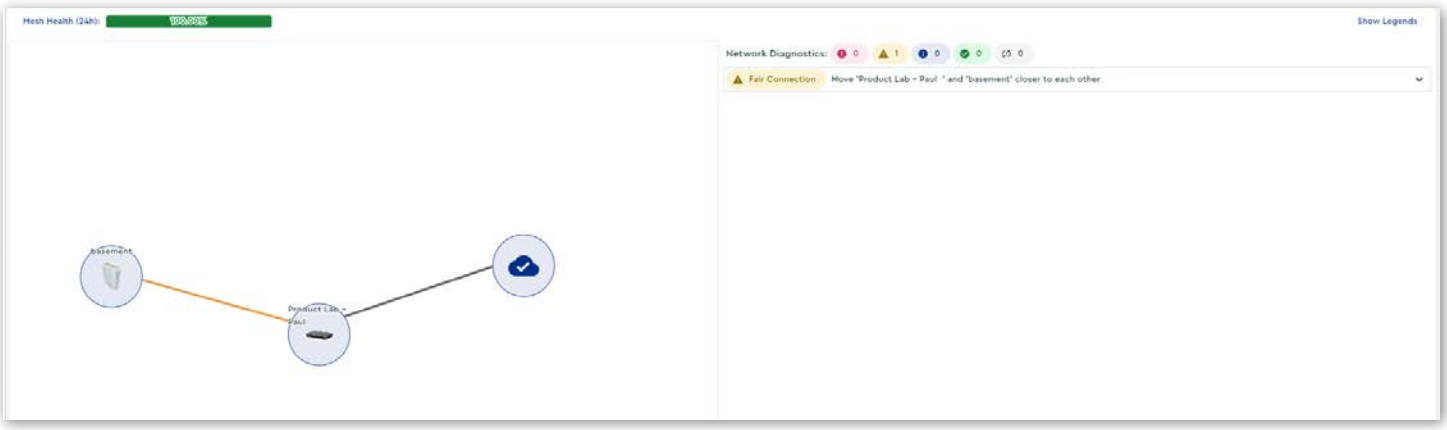

Figure 30. Mesh Network Status

This visual shows the gateway in your network, any connected WiFi Extenders, and any recommendations regarding your Extender—this is the same information you receive after the placement wizard is complete.

Double-clicking on your Extender will open up more detailed information about your Extender.

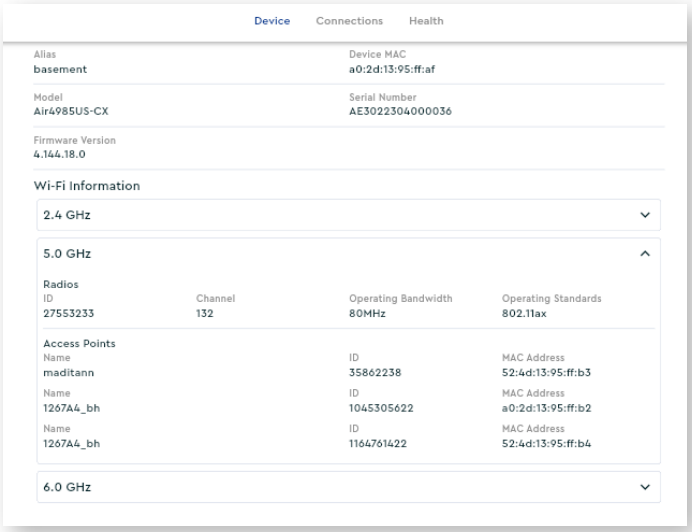

Figure 31. Device Info

You can view each frequency used in your network, their associated SSIDs, and other network health stats.

View the connection quality between your Extender and the gateway:

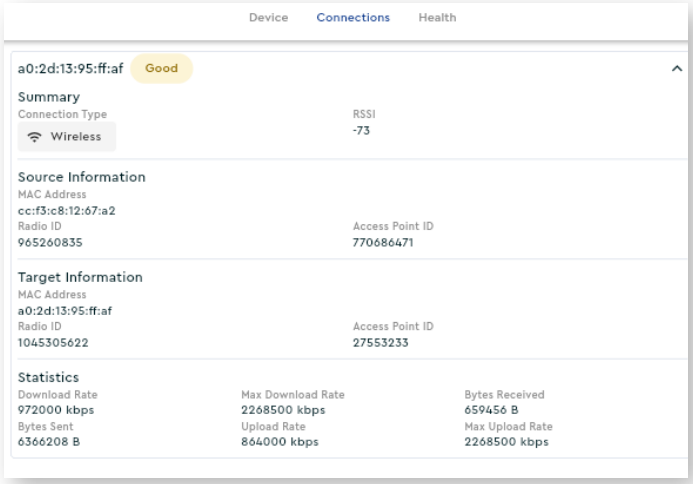

Figure 32. Extender Gateway Connection Status

Finally, view the health of all of the frequencies broadcast from the Extender:

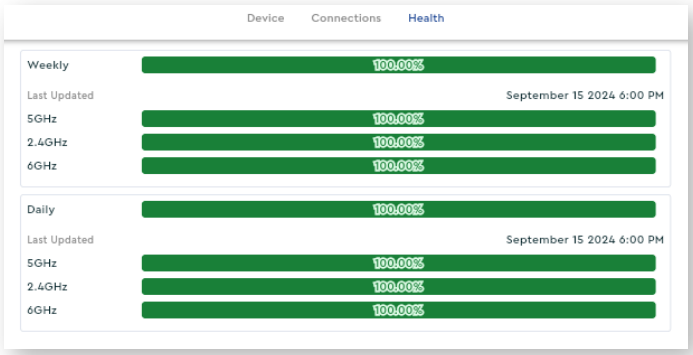

Figure 33. WiFi Radio Frequency Status

CB-775-231456-04 03/25