



CommandIQ Help

May 2024

#220-01342-11

Contents

About CommandIQ Help	6
Bottom Menu	7
Icons	8
Initial Router Management Setup	9
Step 1: Launch and User Setup	10
Step 2: Configure Router	13
Step 3: Configure the Wi-Fi Network	17
Zero Touch Satellite Onboarding	19
Add Mesh (Satellites).....	19
Dashboard (Home Screen)	23
Alerts	25
My Networks	29
Networks	31
Network Tools	33
Share Network Access	37
Equipment	39
Add Equipment	43
Replace a Router.....	43
Services	46
Usage	47

Add a Network	49
Edit a Network	53
Things	53
Add Things	57
Edit Things	59
People	59
Add People	60
Edit/Delete People	61
Places	62
Add Places	63
Edit/Delete Places	64
ExperienceIQ	65
My Priorities	66
Traffic Priorities.....	68
Device Priorities.....	69
Parental Control Profiles	70
Parental Control Settings	71
Pause Network Access	78
DNS over HTTPS Content Blocking	80
ProtectIQ	82
Trusted List	84
Skip Devices	85
Intrusion Prevention System (IPS) Settings	86

Additional Details..... 90

ProtectIQ Alerts..... 91

Arlo..... 91

Servify..... 94

Settings..... 95

Update Account 96

Delete Account 97

Set Passcode 98

Secondary Account Support..... 100

Contact Support..... 101

Language..... 102

Alerts..... 103

Terms and Conditions..... 105

Privacy Policy..... 106

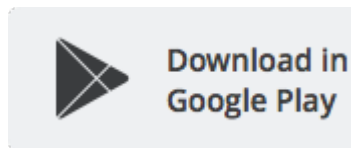
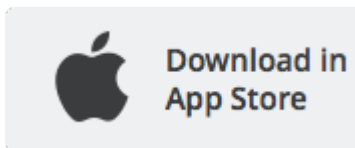
About..... 108

About CommandIQ Help

Welcome to the CommandIQ® Help!

Use this Help information to assist with setting up and managing your BLAST router's home Wi-Fi network from your smart phone or tablet using the CommandIQ mobile application.

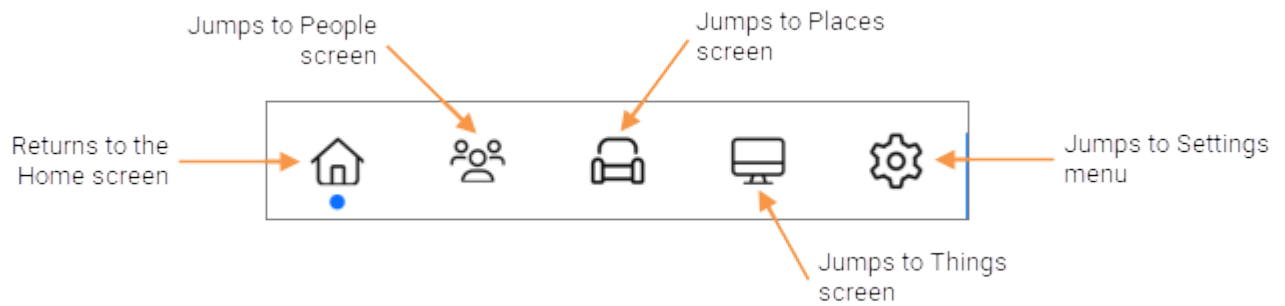
CommandIQ is available for Apple® iOS and Android™ mobile devices. If you have not already done so, download the app to your phone or tablet to get started.



Calix releases an updated CommandIQ app, Calix Service Cloud and EXOS software on a quarterly cadence. This means that every three months, both service providers and their subscribers will have an up-to-date application. While CommandIQ and Service Cloud are updated automatically, providers must manually upgrade GigaSpire systems. This means that new software features available in CommandIQ may not be available on the subscribers GigaSpire. This guide is written to reflect the most current software release and applies to both iOS and Android devices. Note that full feature support requires both CommandIQ and the GigaSpire be running the current software release.






Bottom Menu

The bottom menu provides quick access to all CommandIQ components and settings and is available throughout the app. A blue dot under an icon in the bottom menu indicates your current location within the app.



Icons

The CommandIQ app uses the following settings and navigation icons.

	Add a new item (e.g., network, person, place, thing).
	Edit an item.
	Return to the previous screen.
	Show/hide password.
	Open the CommandIQ Help documentation.

Chapter 1

Initial Router Management Setup

The first time you open CommandIQ, you are prompted to enter some information to allow CommandIQ to manage the BLAST system. This information includes establishing your user login credentials for management, identifying the router to manage, and setting up the Wi-Fi SSID and password. This is a one-time setup activity to be completed only at initial launch.

Continue to the following topics for instructions on completing the initial router management setup with CommandIQ. Or, check out [this video](#) for guidance.

1. *Launch and user setup*
2. *Add router*
3. *Configure Wi-Fi network*

Guidelines

- Service providers have the option to enable Secure Onboarding. If enabled, CommandIQ will request your account number during the setup process. Contact your service provider for additional account information.
- During the onboarding process, CommandIQ checks the Primary SSID. If the SSID starts with CXNK, the option to configure Wi-Fi is presented, with the option to skip this step. If the SSID does not start with CXNK, an assumption is made that the SSID has already been customized and the user is not prompted to setup Wi-Fi.

Step 1: Launch and User Setup

The first time you open CommandIQ, the app guides you through an initial setup to manage the BLAST router. The setup begins with setting yourself up as an authorized CommandIQ user by establishing a personal login ID and password. This is a one-time activity only.

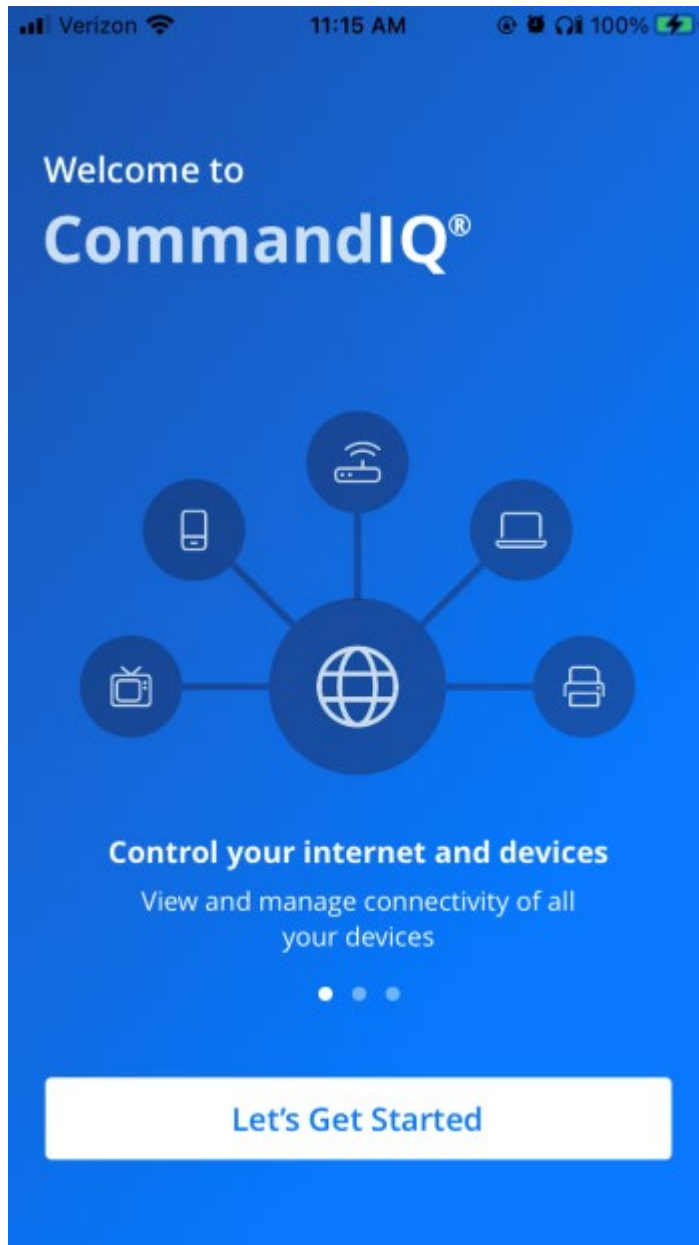
To launch CommandIQ and set up your user account

1. On your mobile device's app launcher screen, tap the CommandIQ app icon to open the app.



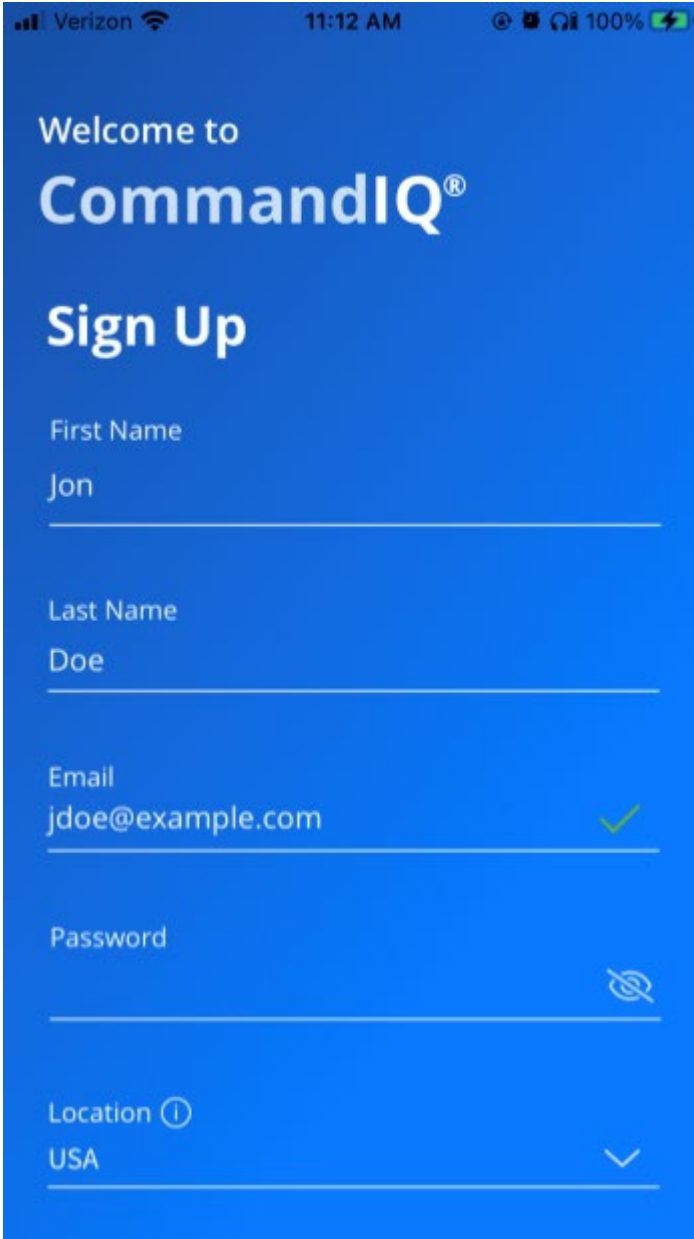
2. Tap **Let's Get Started**.
3. If you have an existing CommandIQ account, enter your login email address and password, then tap **Log in**.

4. If you are new to CommandIQ, tap the Sign Up link, then proceed to create your account and onboard your equipment.



5. On the Account creation screen, tap each field and type to input the following information:
 - First Name: Your first name
 - Last Name: Your last name
 - Email: Your email address, which serves as your app login username
 - Password: Create a password to log in to the app on this device

Note: The password must be at least 8 characters in length. Tap the eyeball icon to see the characters as you type.



6. In the **Location** field, tap and scroll to select the appropriate location for the ORG that services the GigaSpire:
 - USA for US based systems
 - CA for international systems
7. Tap to select the checkbox for the **I Accept the Terms & Conditions** acknowledgment (required to proceed).
8. Tap the **Create Account** button to save your inputs and continue.

Step 2: Configure Router

The next screens offer a customized experience to guide you through setting up your router so that it can be identified by cloud services. CommandIQ collects a unique serial number and MAC address, which can be found printed on the product label on the bottom of the router.

You can collect this information conveniently and error-free by using the QR-code scanning function via your mobile device's camera. Or as an alternative, you can input the information manually by typing into the respective fields.

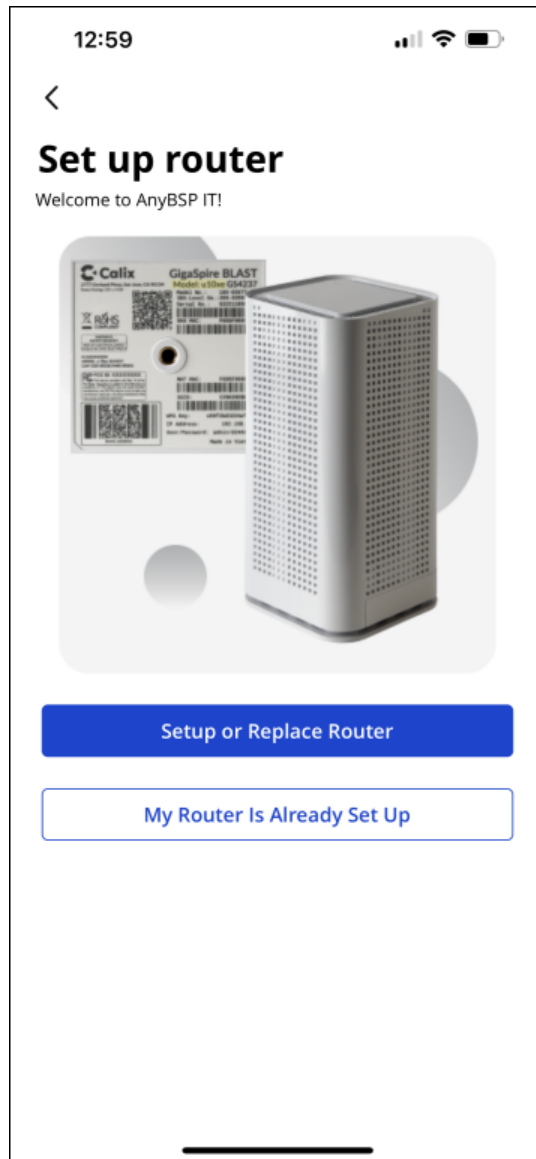
Guidelines

- Your service provider must remotely initiate router replacement sessions from Calix Service Cloud. If you plan to swap your GigaSpire, contact your service provider prior to completing a replacement.
- Guided router replacement currently supports swaps from a GigaSpire to a GigaSpire only.
- The QR-code scanning function requires a camera with auto-focus.

To configure a router with CommandIQ

1. On the *Set up router* screen, do one of the following:
 - To set up a new router and receive model-specific guidance on placement, power, and ethernet connection, tap **Setup or Replace Router** and select **Set up a new router** from the pop-up menu.
- or -
 - If applicable, tap **My Router is Already Set Up** to bypass the guided setup.
- or -
 - To replace a router, tap **Setup or Replace Router** and select **Replace an existing router with a new one** from the pop-up menu.

Note: You can replace a router as an existing CommandIQ user. See *Replace a Router* for more information.



2. On the *Scan device* screen, input the router's MAC address and serial number using one of the following methods:
 - **Scan QR code:**
 - a. Point the camera viewfinder at the QR code printed on the router's product label, located on the bottom of the unit.
 - b. Center the QR code in the middle of the viewfinder frame, and then zoom in or out until the QR code fills the frame and the camera automatically captures the identifier information (where the MAC address and serial number values auto-populate into the respective fields upon capture).
After the capture occurs, proceed to setup. If the capture fails after multiple attempts, use the manual type-in method.

Proprietary Information: Not for use or disclosure except by written agreement with Calix.

© Calix. All Rights Reserved.

- **Type:**
 - a. From the *Scan device* screen, tap **Manually Enter Device Details**.
 - b. Select your router model from the **Model** drop-down menu.
 - c. Tap the **MAC Address** field, and then type in the router's MAC address as seen on the label on the bottom of the unit.
 - d. Tap the **Serial Number** field, and then type in the router's serial number as seen on the label on the bottom of the unit.
 - e. Tap **Start Setup**.

1:51

<

Step 1 of 6

Device Details

Enter device details manually

Model

Select GigaSpire or GigaPro model

MAC Address

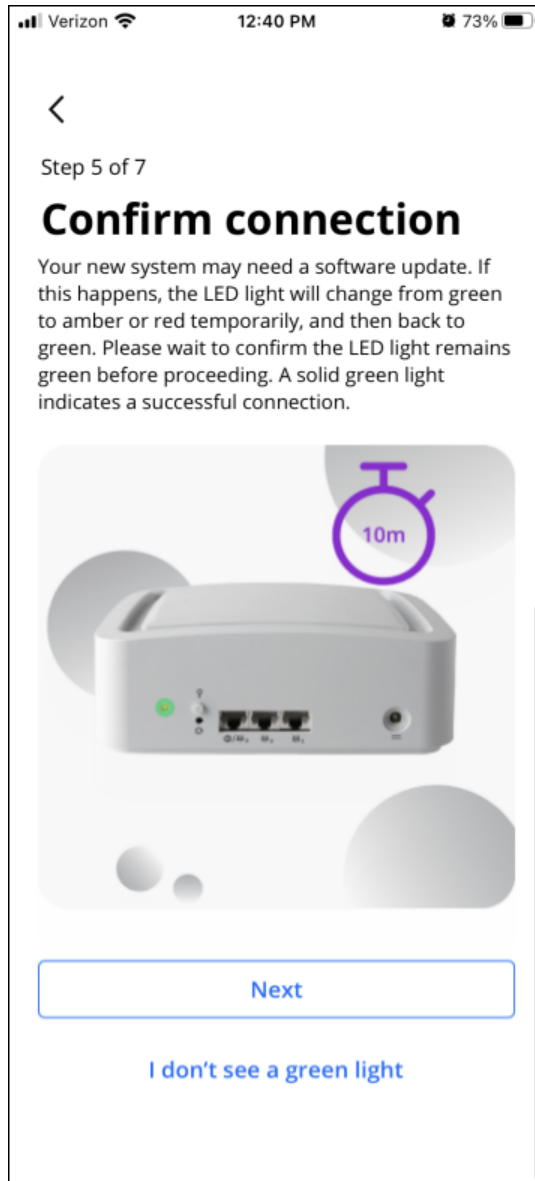
Serial Number

Start Setup

Calix GigaSpire BLAST Model G4227

3. Tap **Next** on the *Router placement* screen.
4. Follow the on-screen instructions to plug in your router, then tap **Next**.
5. Follow the on-screen instructions to connect an ethernet cable, then tap **Next**.

6. Follow the on-screen instructions to confirm a successful connection, then tap **Next**.
For common troubleshooting tips, tap **I don't see a green light**.



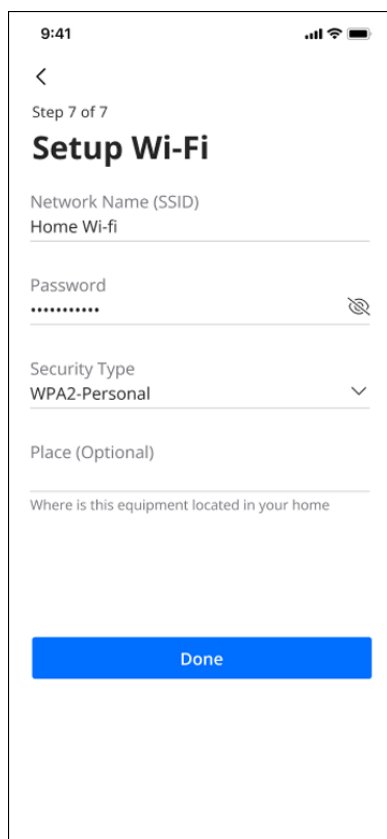
7. Tap the **Next** button to save your inputs and continue.

Step 3: Configure the Wi-Fi Network

The next screen in the setup sequence helps you set up your home's primary Wi-Fi network, including assigning a name to your BLAST router (the name that appears in the CommandIQ app).

To configure the BLAST router's Wi-Fi network

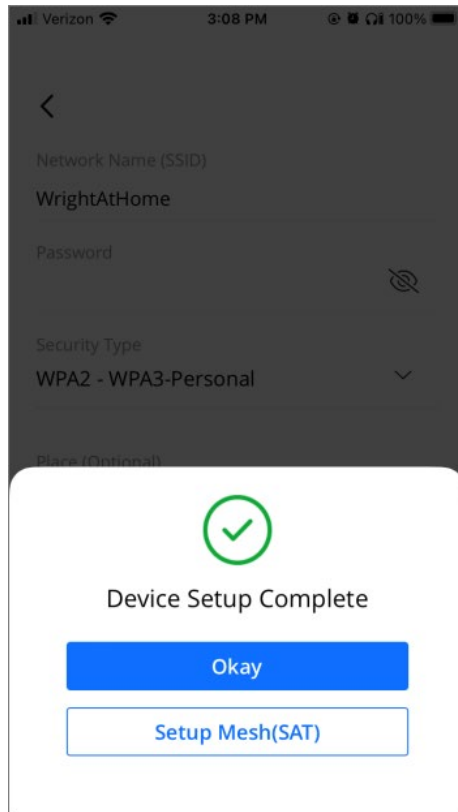
1. On the *Setup Wi-Fi* screen, tap the **Network Name (SSID)** field, and then type in a name for your Wi-Fi network. This name value is what Wi-Fi client devices will see when they scan for available Wi-Fi networks.



2. Tap the **Password** field and enter the password for the wireless network.
3. Tap the **Security Type** selection list to select a security option for the Wi-Fi network:
 - **WPA2-Personal**
 - **WPA - WPA2-Personal**
 - **WPA2 - WPA3-Personal**
 - **WPA3-Personal**

Note: WPS is disabled when the WPA3-Personal security type is enabled.

4. (Optional) Tap the **Place** field, and then type in the location of the router in your home (e.g., Living Room).
5. Tap the **Done** button to save your inputs and continue.
6. A confirmation displays. Tap **Okay** to view the CommandIQ Home screen or tap **Setup Mesh(SAT)** to add another network device.



To set up a Mesh(SAT) device

After completing the initial router onboarding and Wi-Fi setup, you have the option to onboard additional mesh (satellite) units.

Note: The desired mesh device must have no prior RG pairing. If your mesh satellite has previously been paired to an RG, factory reset the mesh by holding the hardware reset button for 30 seconds.

1. Tap **Setup Mesh(SAT)**.
2. Scan the QR code to automatically populate the device details. Alternately, tap **Issues Scanning?** to manually enter the MAC address and serial number.
3. Tap **Next**.
4. Enter a **Name** for the device.
5. Tap **Done** to complete the onboarding. If you have additional devices to add, tap **Save and add another Mesh(SAT)** to onboard another mesh device.

Zero Touch Satellite Onboarding

Zero touch onboarding allows a satellite to be discovered by the router (RG) without using WPS. Addition of the satellite is managed via CommandIQ. This works for all GigaSpire and GigaMesh models.

Guidelines

- The desired mesh device must have no prior RG pairing. If your mesh satellite has previously been paired to an RG, factory reset the mesh by holding the hardware reset button for 30 seconds.
- Zero Touch Onboarding requires EXOS R21.1 or higher on both the satellite and the RG.
- The 2.4 GHz radio on the Residential Gateway must be enabled.
- The QR-code scanning function requires a camera with auto-focus.

Onboarding Steps

- Within CommandIQ, the user is prompted to identify the satellite:
 - Scan the QR code on the satellite label, -or-
 - Manually enter the FSAN ID, MAC Address, and Serial Number
- Command prompts from CommandIQ provides a step by step tutorial of the on-boarding process.
- Security is assured in that the QR code or MAC/SN/FSAN proves that physical access to the satellite is validated.
- Once satellites are scanned, they will appear in the network topology, regardless of whether the satellite has paired.
- The satellite can be scanned with the power on or off.
- Even with Zero Touch OnBoarding, satellites can still be paired via ethernet or WPS.

Note: WPS is disabled for the 6 GHz radio.

Add Mesh (Satellites)

In order to add a satellite, a user can either scan the QR Code located on the bottom of the BLAST unit or manually enter the information. The steps detailed below can be performed with or without power being applied. Upon completing the steps below, the gateway controller enables the bootstrap satellite discovery option for ten minutes. After 10 minutes, if the satellite has not been powered up and successfully paired, the connection will move to expired.

Guidelines

- The desired mesh device must have no prior RG pairing. If your mesh satellite has previously been paired to an RG, factory reset the mesh by holding the hardware reset button for 30 seconds.

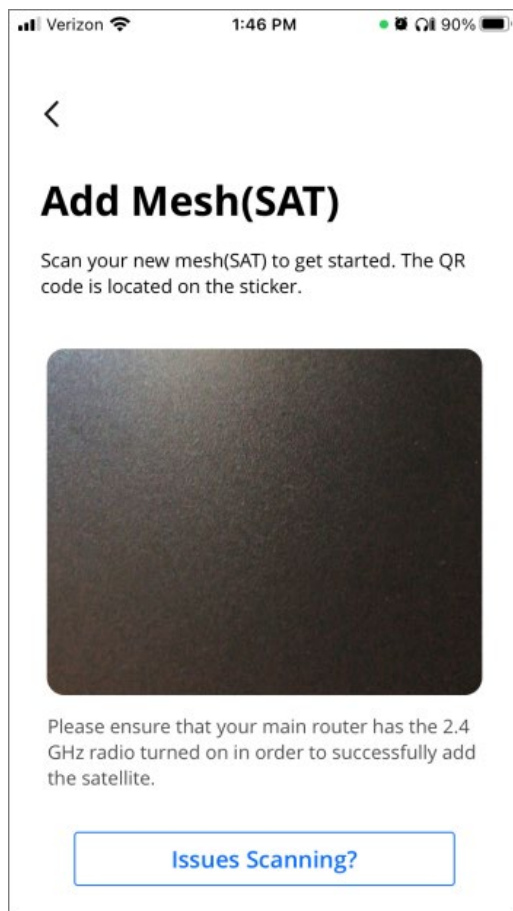
Note: Users can view satellites that have been installed or are in the process of being installed. CommandIQ provides the pairing status of systems paired or in the process of pairing.

Under the Satellite name, the connection status is displayed:

- Online: The controller is paired with the satellite.
- Offline: The controller has previously been paired with the satellite, but the satellite is off-line.
- Pending: The controller has started the pairing process but has not yet been completed.
- Expired: The satellite failed to pair during the allotted 10 minute window.

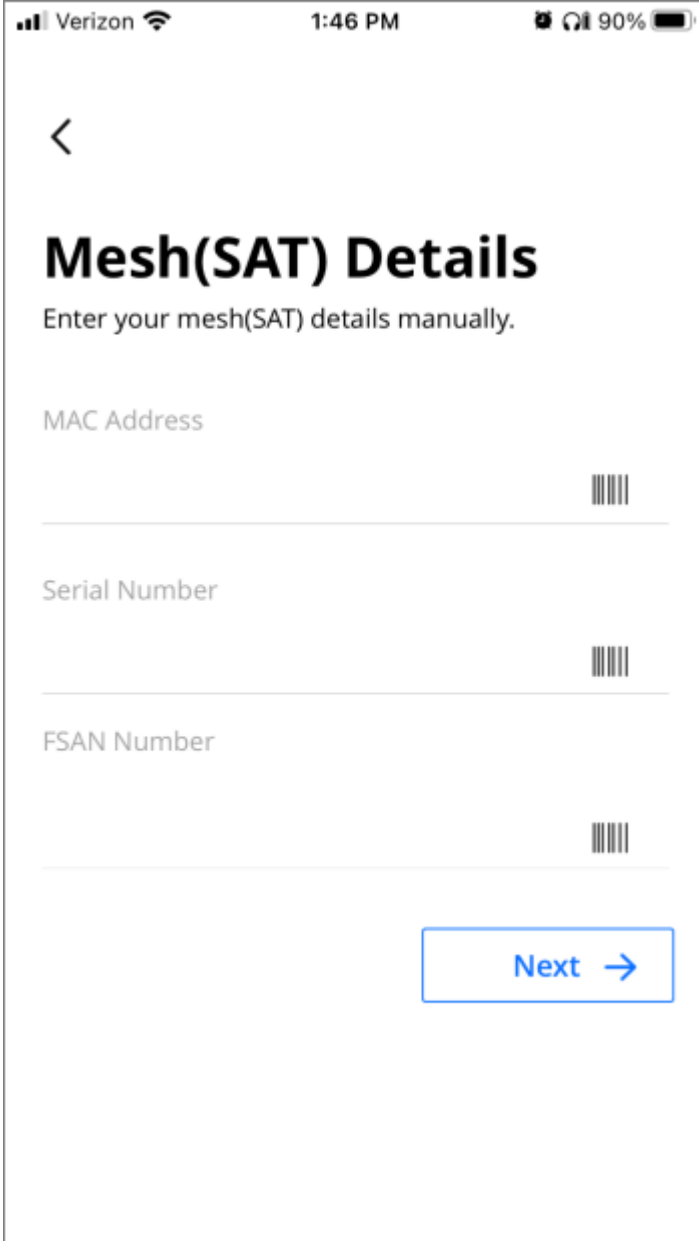
To add a Satellite to the network

1. From the Home screen, tap **My Network**.
2. Tap the *plus sign* and select **Add Equipment**.
The **Add Mesh(SAT)** screen opens.
3. Scan the QR code located on the bottom end label of the BLAST router. When the scan is successful, the needed information is stored within the network.



4. If the scan is not successful, tap the **Issue scanning?** button to manually enter the required system information.
5. Enter the **MAC Address**, **Serial Number**, and **FSAN Number** of the BLAST router.

Note: All three fields above can be found on the product label located on the bottom of the BLAST.



The screenshot shows a mobile application interface for entering mesh(SAT) details. At the top, the status bar displays 'Verizon', signal strength, Wi-Fi, time '1:46 PM', and battery '90%'. Below the status bar is a back arrow icon. The main heading is 'Mesh(SAT) Details' in bold black text, followed by the instruction 'Enter your mesh(SAT) details manually.' There are three input fields, each with a label and a barcode icon on the right: 'MAC Address', 'Serial Number', and 'FSAN Number'. At the bottom right, there is a blue 'Next' button with a right-pointing arrow.

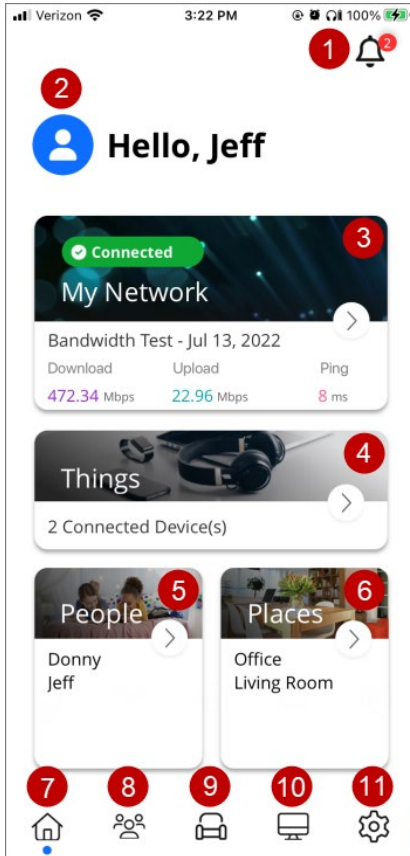
6. Tap **Next** to complete the onboarding process.

Chapter 2

Dashboard (Home Screen)

The home screen for CommandIQ is called the dashboard. The CommandIQ dashboard provides quick access to all of the app's functions and ties them together in a convenient single screen.

Check out the dashboard's element map below to familiarize yourself with the element names. See the linked Help topics for detailed instructions on how use each feature.



1. **Notifications:** Tap the notifications icon to see all system generated push notification alerts.
2. **Profile:** Tap your profile icon to edit your profile, including avatar image, name, email address, and password. Your full name as provided during initial setup appears here, so you know that CommandIQ is personalized for you and your home network. You can modify the account name that appears here as needed.
3. **My Network:** (on page [29](#)) Provides status of Residential Gateways in the network as well as last measured result of a speed test. Upon drilling down, displays equipment, services, and usage statistics for devices and equipment associated with the network chosen.
4. **Things:** (on page [53](#)) Tap to view a list of all devices on the network. Tap an individual device to change network priority and network path information. All devices are placed into category types making it easier to access how each is connected to your network. As new devices are added, there may be additional categories created. Tapping on any category type provides a more detailed view of the individual device category.
5. **People:** Tap to view a list of all users on the network.
6. **Places:** Tap to view a list of places in the network.

Bottom Menu

The bottom menu appears on every screen within the CommandIQ app. A dot under an icon in the menu bar indicates which screen you are currently viewing.

7. **Home:** Tap to return to the Home screen.
8. **People:** Tap to view the People screen.
9. **Places:** Tap to view the Places screen.
10. **Things:** Tap to view the Things screen.
11. **Settings:** (on page [95](#)) Tap to view and modify CommandIQ app settings.

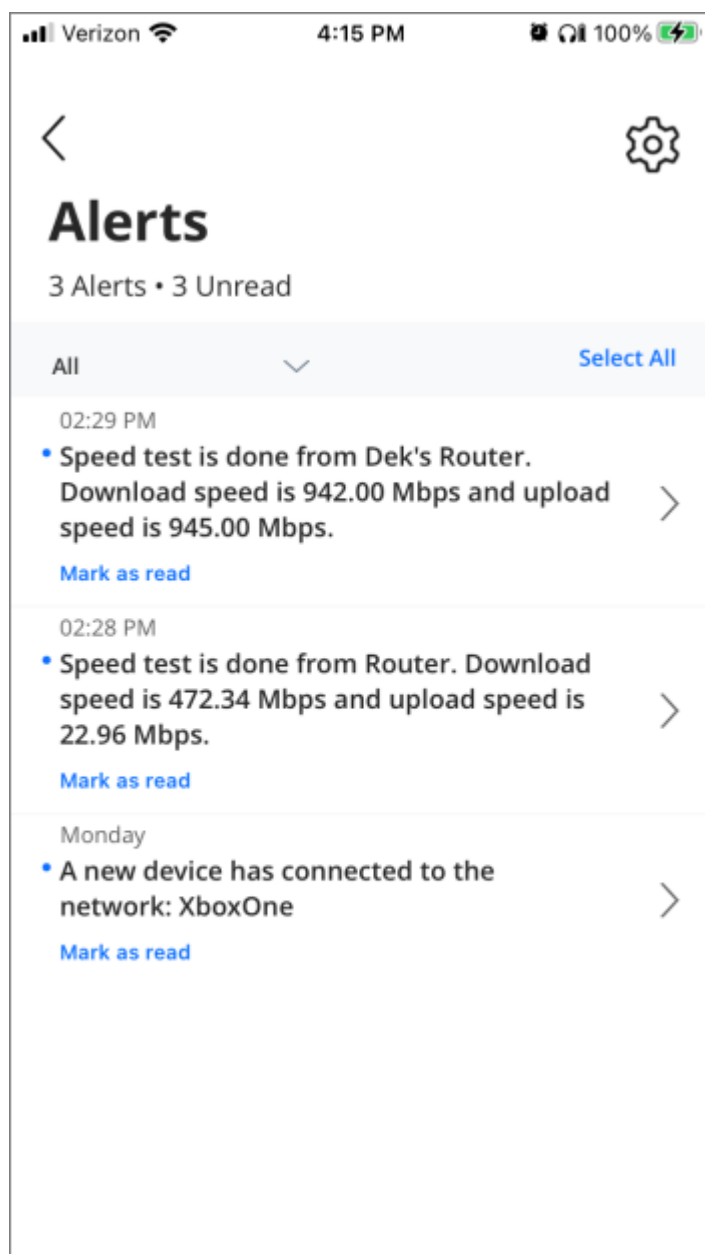
Alerts

Tap the *Alerts* icon on the Home screen to view a list of notifications applicable to this network. From the **Alerts** screen, you can mark all, delete all, or cancel the delete request.

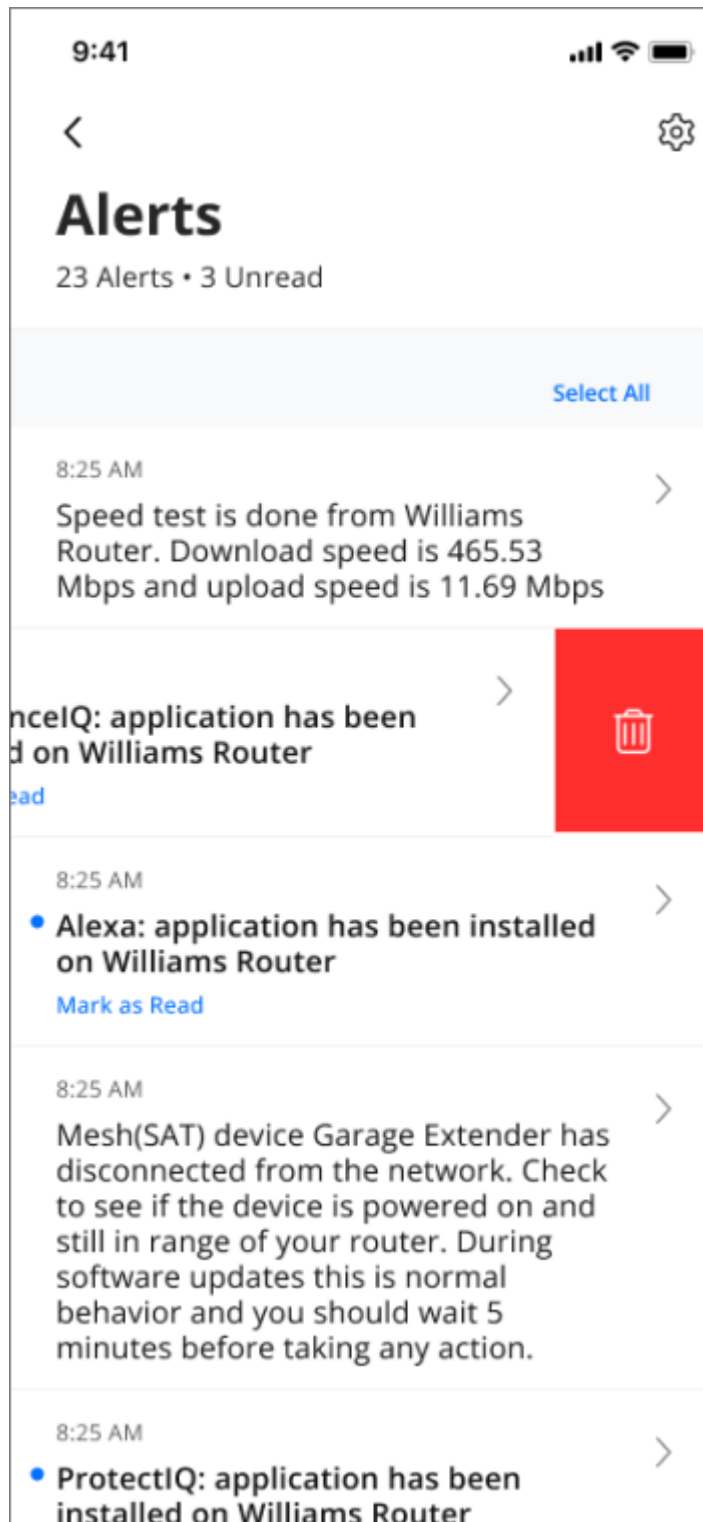
To manage alerts

1. From the Home screen, tap the *Alerts* icon. Alternately, navigate to **Settings > Alerts**.

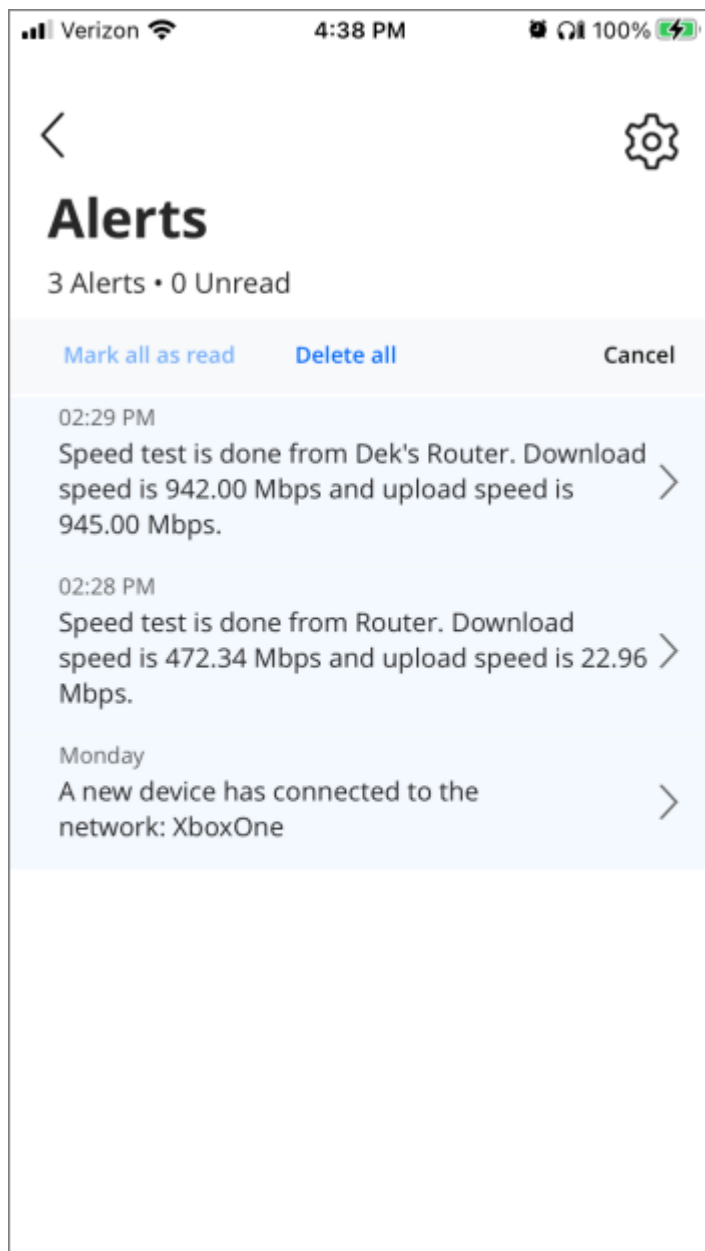
View your alerts. Tap on an alert in the list to view more information and to delete the alert.



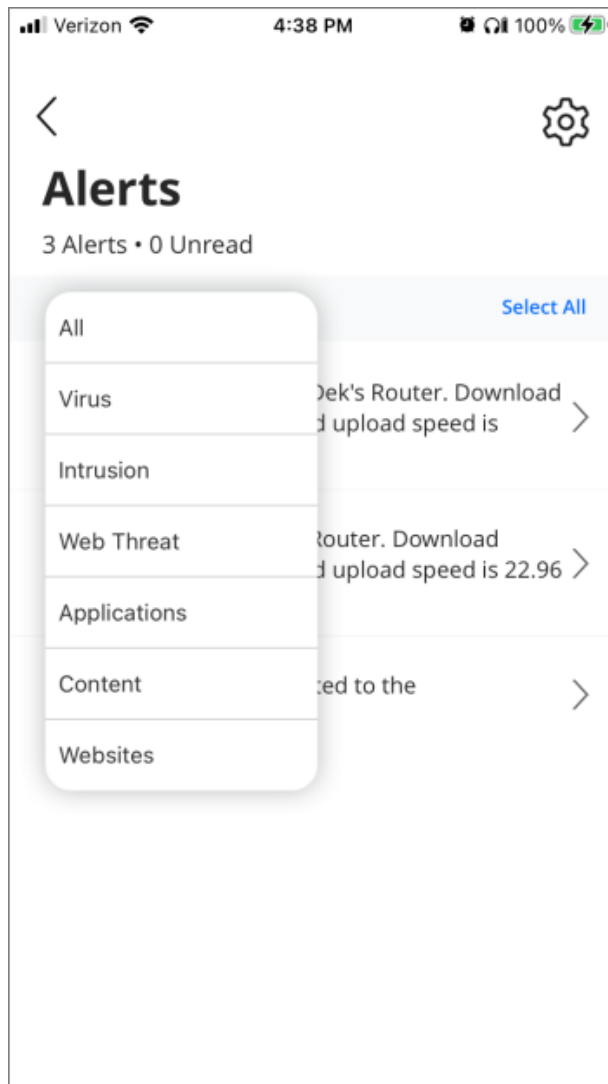
To delete an alert, swipe the alert to the left and tap the *trashcan* icon.



To mass-edit alerts, tap **Select All**, then tap either **Mark all as read** or **Delete all**.



Tap **All** to filter the alerts list by alert type.



Note: When viewing a filtered list of alerts, the "Delete All" function deletes all alerts encountered on the network, not just those exclusive to the applied filter.

To manage CommandIQ alert settings

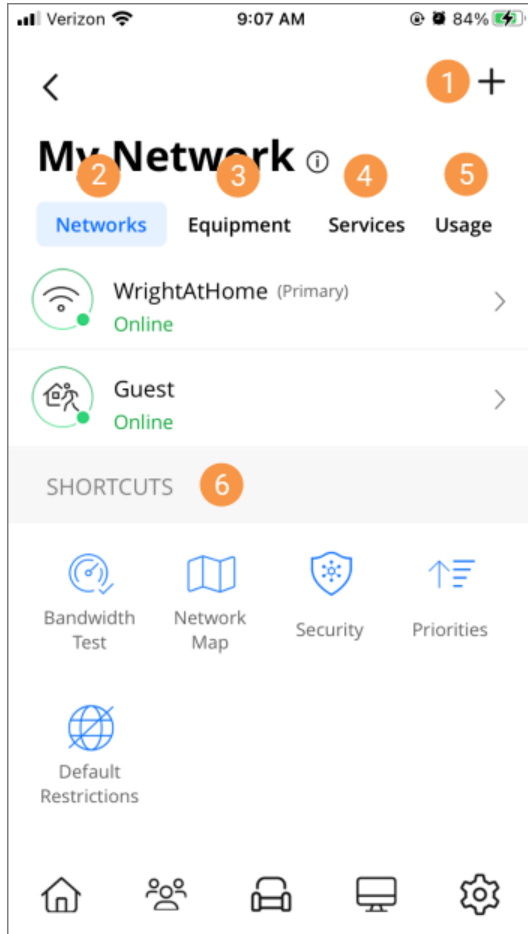
1. Navigate to **Settings > Alerts**. Alternately, from the Home screen, tap the *Alerts* icon, then tap the *Settings* icon.
2. Select the toggle to enable (green) or disable push notifications to your mobile device.
3. In the CommandIQ section, select the toggles for which CommandIQ alerts you would like to receive.

Chapter 3

My Networks

The **My Networks** screen provides access to information and settings for your wireless network(s), network equipment, and Things.

From the **My Networks** screen, the following controls/indicators are displayed:

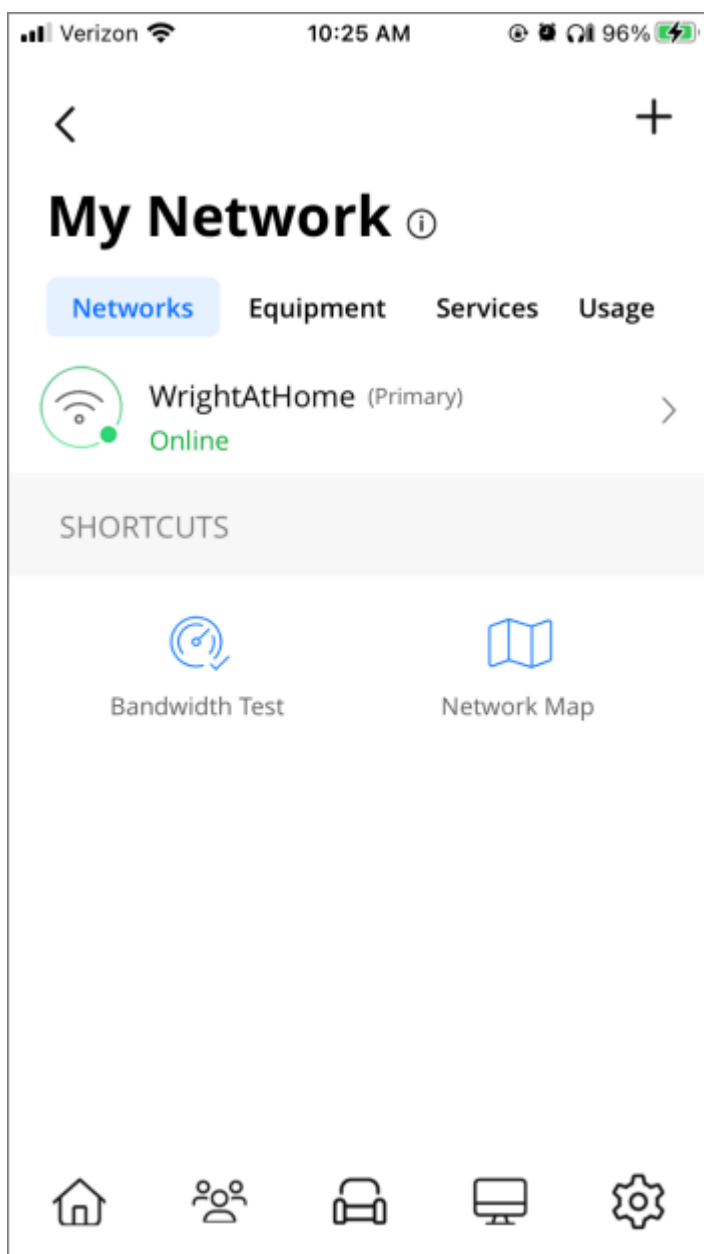


1. **Add:** Tap to *add a new network* (on page [49](#)), *add new network equipment*, or *replace an existing router*.
2. **Networks:** Tap to view a list of your network SSIDs and to view additional network details.
3. **Equipment (on page [39](#)):** Tap to view a list of your network equipment (e.g., routers, mesh satellites).
4. **Services (on page [46](#)):** Tap to view your services (e.g., ExperienceIQ, ProtectIQ) and manage services settings.
5. **Usage (on page [47](#)):** Tap to view bandwidth usage data for Things connected to your network.
6. Shortcuts to Network Tools:
 - **Bandwidth Test (on page [33](#)):** Tap to run a bandwidth test.
 - **Network Map (on page [34](#)):** Tap to view the Network Map.
 - **Security:** Tap to view threat data and configure additional security settings. Requires ProtectIQ.
 - **Priorities:** Tap to set device and traffic priorities.
 - **Default Restrictions:** Tap to view and configure global browser, content, application, and website restrictions.

Networks

The **My Network > Networks** tab lists your wireless networks and provides access to network tools such as the Bandwidth Test and the *Network Map* (on page [34](#)).

To access this screen, you can either tap the **My Network** tile on the Home screen or tap the **Networks** icon in the bottom menu bar. Then, tap **Networks**.

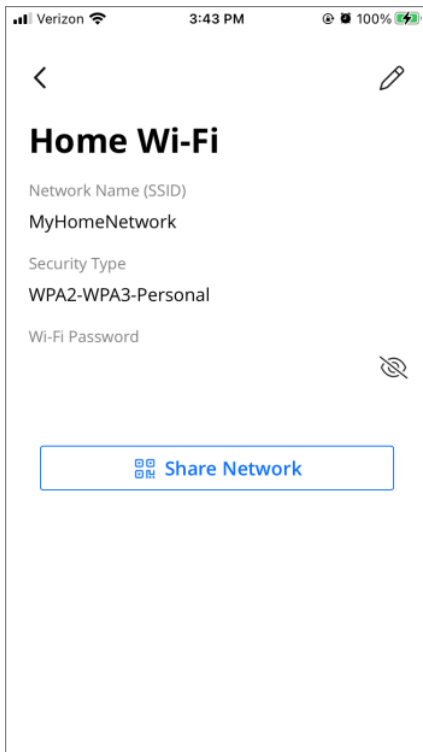


To view network details

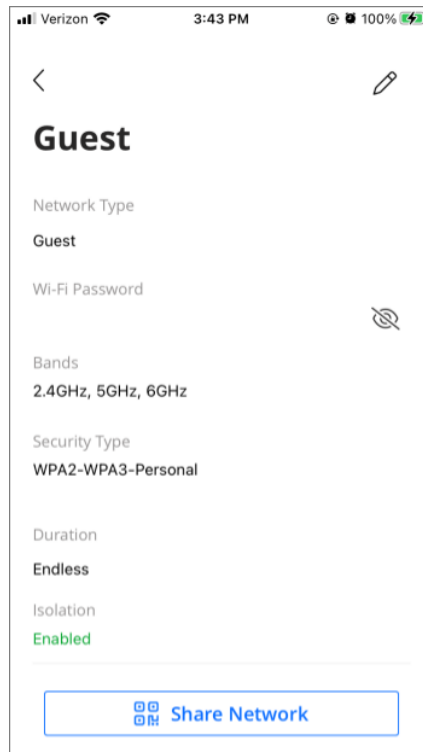
1. From the **My Network > Networks** tab, tap on the desired network.

View the network information and *share network access* (on page [37](#)).

Example Primary Network Details



Example Guest Network Details



To edit network details

1. From the **My Network > Networks** tab, tap on the network you would like to edit.
2. Tap the *pencil* icon.
3. Edit the SSID, password, and security type as desired.

Note: WPS is disabled if the WPA3-Personal security type is selected.

4. Tap **Save**.
5. Tap **OK** to confirm and return to the My Network screen.

Network Tools

Bandwidth Test

The **Bandwidth Test** screen displays the latest bandwidth test results, including download/upload speeds and latency. Note that the numbers displayed reflect the previous bandwidth test.

To run a bandwidth test

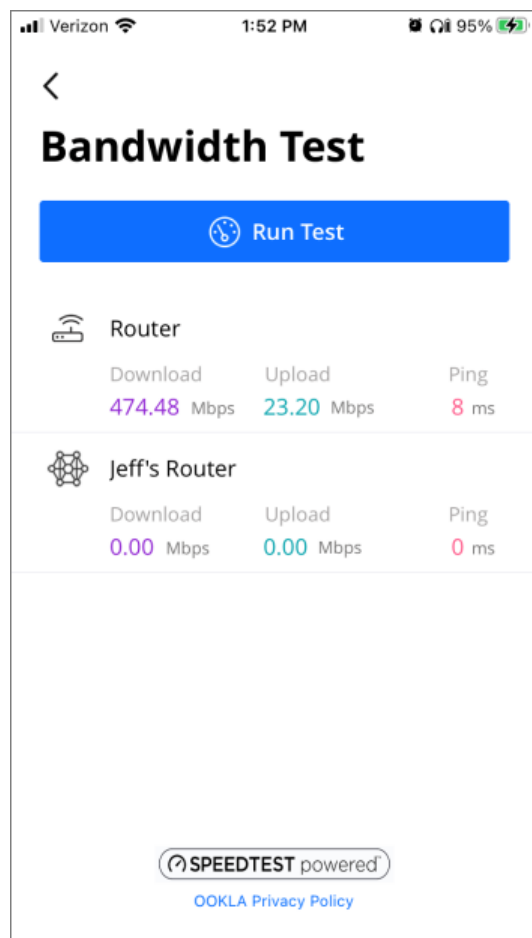
1. From the My Network screen, tap **Bandwidth Test**.

2. Tap **Run Test**.

Note: The Run Test button text changes to indicate test progress.

3. After the test completes, results for all equipment in the network are displayed.

- a. Download Speed
- b. Upload Speed
- c. Ping Time



Additional Notes

1. The blue Run Test button provides visual confirmation that the bandwidth test is in progress.
2. Results for the bandwidth test are used for setting bandwidth queues used for My Priorities.
3. Bandwidth testing is capped at 2.5 Gbps.
4. Satellite speed is measured to the RG, not to the internet and can vary based on wireless conditions. If satellite speed is low, try moving the satellite to get a better Wi-Fi connection to the RG. Check **My Network > Equipment > Mesh(SAT) > Additional Details** to see the Wi-Fi signal strength and backhaul PHY rates.

Note: Bandwidth testing may not be available in all countries. Check with your service provider for details.

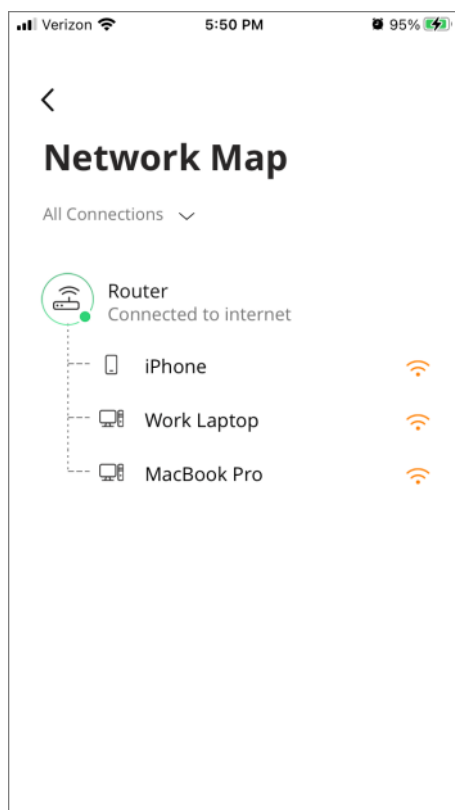
Network Map

The Network Map provides a visual indication of what Things (devices) are connected to what equipment.

To view the network map

1. From the Home screen, tap on the **My Network** tile.
2. Tap **Network Map**.
3. The network map displays the following information:
 - The RG, any satellites, and their current connection strength.
 - A list of Things connected to the RG and each satellite.
 - Connection type of the Things on the network (Wi-Fi or Ethernet)

Note: Each device in the network shows a relative signal strength to the right of each device.



Private Ookla Server Support

CommandIQ supports bandwidth testing to a private Ookla server. The provider must designate a private server endpoint and enable the feature in Calix Service Cloud. CommandIQ automatically selects the private server if configured.

By using a private server, a BSP outside the US can enable on-demand Ookla testing. Rest of world countries (countries outside of US and eight non-GDPR countries) do not have access to an OOKLA public server and so may only run private server speed tests.

Criteria for Acceptance of Ookla Speed Tests

- Acceptance Criteria 1: Any subscriber in Rest of World countries should only be able to run private server speed test when setup in OPS cloud.
- Acceptance Criteria 2: Any subscriber in SUPPORTED countries should be able to run private server speed test when setup in OPS cloud.
- Acceptance Criteria 3: Any subscriber in Rest of World countries should continue to have speedtest hidden if there is no private server configured.

Service Cloud Configuration for Ookla Private Server

NetOps

Subscriber Management

Reports

Operations

Configurations

Configuration

Dial Plan External File Server Secure Onboarding Self Heal Stale System Purge Subnet Configuration **Speed**

Background Testing

On-demand Latency Test PING Target

Test Configuration for TR143-capable third party CPE

Download URL

Upload URL

Upload Size

Test Configuration for Ookla capable CPE

Ookla Private Server Endpoint

Only Use Ookla Private Server for GigaSpire Speed Tests

Ookla On Demand Testing Update

Ookla on-demand speed test results (from CommandIQ) on GigaSpire systems are capped at a maximum rate for display to the subscriber.

- Tests on systems with a DHCP or a static IP uplink will display actual results up to the maximum of 2.5 Gbps.
- Tests that achieve > 2.5 Gbps will report **Your measured speed exceeds 2.5 Gbps**.
- Testing in Calix Service Cloud (CSC) will show the actual speed test result and it could be more than the 2.5 Gbps rate reported in CommandIQ.
- Tests on systems with a PPPoE uplink will display actual results up to the maximum of 1 Gbps.
- Tests on PPPoE systems that achieve > 1 Gbps will report **Your measured speed exceeds 1 Gbps**.
- Testing in CSC on PPPoE systems will show the actual speed test result and it could be more than the 1 Gbps rate reported in CommandIQ.
- Client devices connected to a LAN port on a Gigaspire can achieve 1 Gbps speed test results if the Gigaspire supports an uplink in excess of 1 Gbps, even on systems with a PPPoE uplink.
- For systems with 10 GE, 10 GE AE, or XGS-PON, on-demand test results are capped at 2.5 Gbps regardless of the bandwidth profile applied to the system but it is possible to connect multiple client devices and achieve > 1 Gbps on simultaneous tests (up to 4 Gbps)

Proprietary Information: Not for use or disclosure except by written agreement with Calix.

© Calix. All Rights Reserved.

- Some systems using PPPoE will may not reach the 1 Gbps maximum speed test, even if the uplink is 1 Gbps depending on the Ookla server and network conditions.

Share Network Access

You can share network access information with users via QR code or text message.

Share network access via QR code

1. Navigate to **My Network > Networks**.
2. Tap on the network you want to share.
3. Tap **Share Network**.

A QR code displays on the screen. Scan the QR code to join a mobile device to the network.



Join a mobile device to the network via QR code

1. From the device you wish to join to the network, scan the QR code.
The wireless network SSID and passphrase appear on screen.
2. Tap **Connect** to join the network.

Share network access via text message

1. Navigate to **My Network > Networks**.
2. Tap on the network you want to share.
3. Tap **Share Network**.
4. Tap **Share via Text**.
5. Select the desired contact and send the message. The message includes the QR code, links to iOS and Android scanner applications, and the network SSID and passphrase.

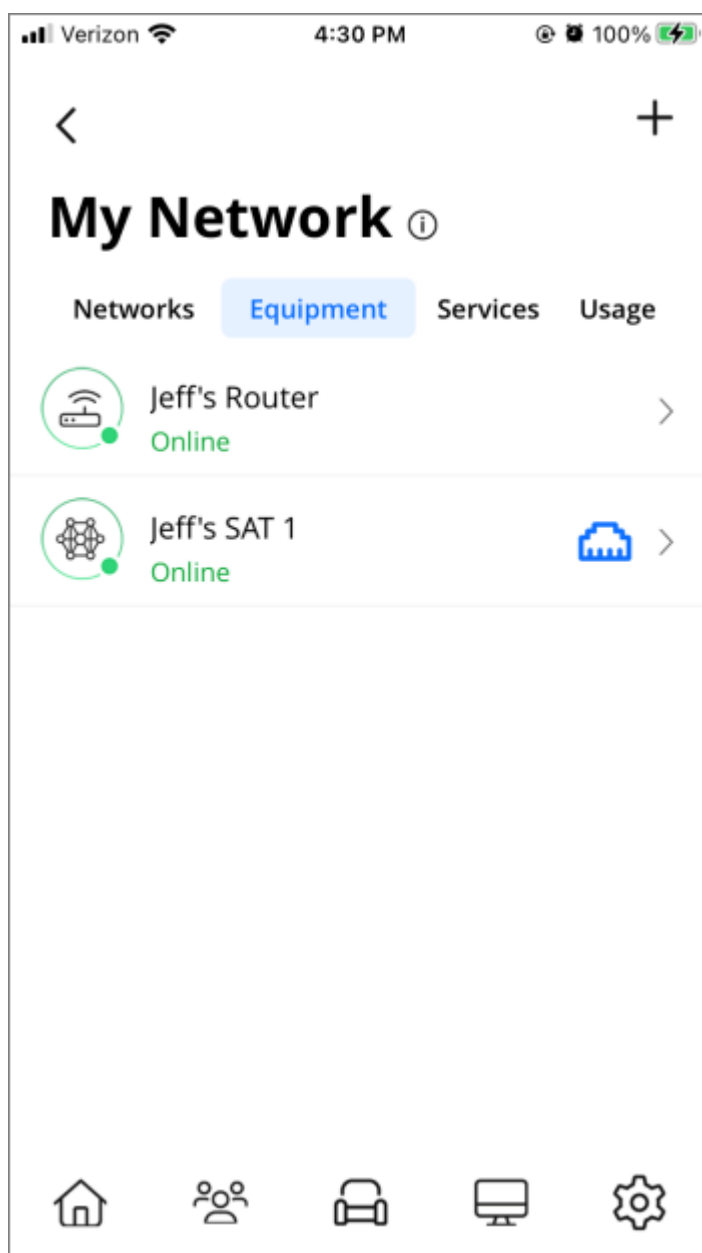
Join a mobile device to the network via text message

1. Open the text message and note the wireless SSID and password.
2. From your device's wireless settings, connect to the SSID using the password provided.

Equipment

The **My Network > Equipment** tab provides a list of Calix RG and mesh (SAT) systems that make up the network. From the Equipment tab, you can view a system's connection type (wired or wireless) and component status (Online/Offline). By default, CommandIQ assigns the name "<your name's> Router" to RG systems and "<your name's> SAT 1" to mesh (SAT) systems.

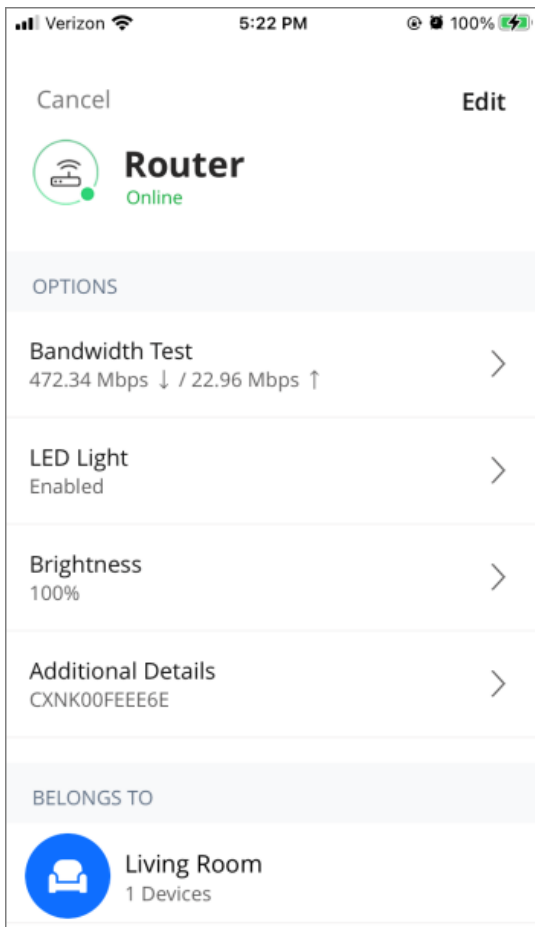
To access this screen, you can either tap the **My Network** tile on the Home screen or tap the **Networks** icon in the bottom menu bar. Then, tap **Equipment**.



To view residential gateway (Router) system details

1. From the Home screen, tap on the **My Network** tile.
2. Select the **Equipment** tab.
3. Tap on the Router.

The following information displays.



- **System type:** Displays the system type (RG or mesh).
- **System name:** Displays the system name (Router by default).
- **Connection status:** Displays the connection status (Online/Offline).

OPTIONS

- **Bandwidth Test:** Displays the most recent bandwidth test results. Tap to view additional speed test data and to run a speed test.
- **LED Light (all equipment):** Displays whether the system's LED light is enabled (default) or disabled. Tap to enable or disable the LED light on the system.
- **Brightness:** Displays the brightness level of the system's LED light (100% by default). Tap to adjust the LED brightness.
- **Additional Details:** Display's the router's FSAN serial number.

Tap to view the following information:

- Router name
- WAN IP address(es)
- LAN IP address
- MAC address
- FSAN serial number
- Device serial number
- Firmware version
- Model number

BELONGS TO

- **Place(s):** Displays the place(s) associated with the router.

To edit router details

1. From the Home screen, tap on the **My Network** tile.
2. Select the **Equipment** tab.
3. Tap on the Router.
4. Tap **Edit**.
5. Edit the router's **Name**.
6. Associate the router with a new **Place**.
7. Tap **Submit** to save your changes.

To view mesh system details

1. From the Home screen, tap on the **My Network** tile.
2. Select the **Equipment** tab.
3. Tap on the mesh system.

The following information displays.

- **System type:** Displays the system type (RG or mesh).
- **System name:** Displays the system name (Router by default).
- **Connection status:** Displays the connection status (Online/Offline).

CONNECTION

- **Router:** Displays the name and connection status of the router the mesh system is connected to.

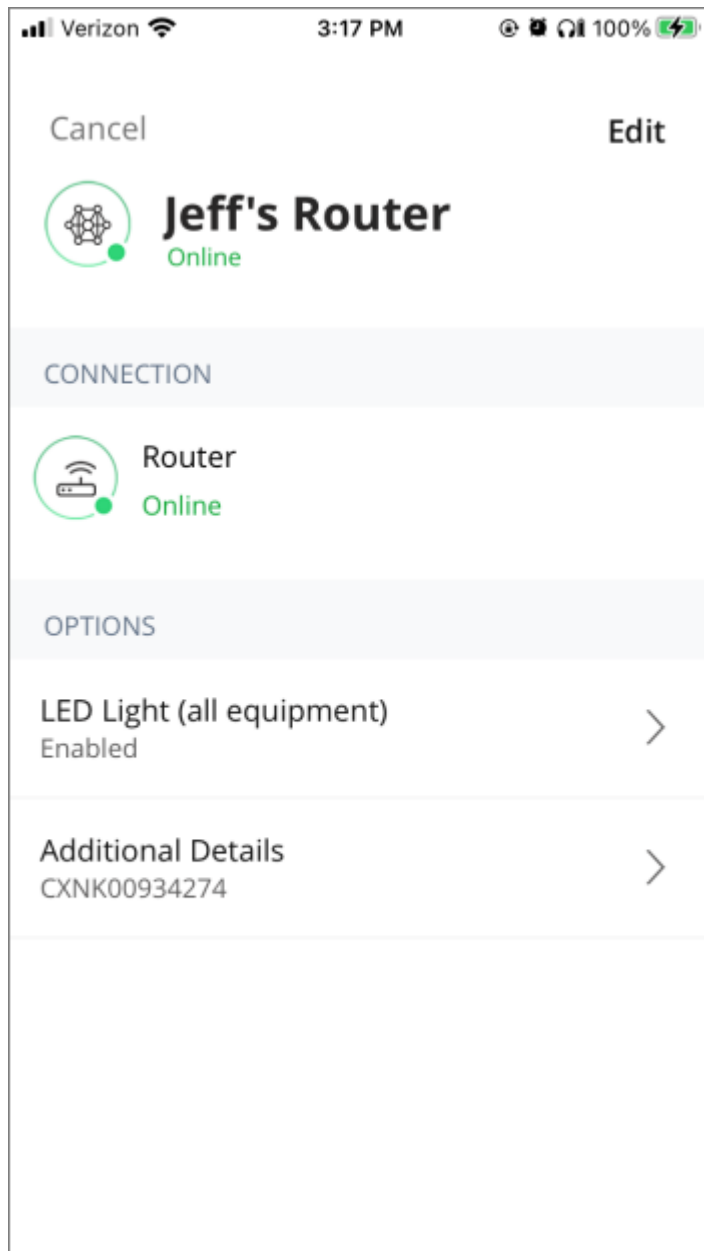
OPTIONS

- **LED Light (all equipment):** Displays whether the system's LED status light is enabled (default) or disabled. Tap to enable to or disable the LED light on the system.
- **Additional Details:** Display's the mesh system's FSAN serial number.

Tap to view the following additional information:

- Router name
- LAN IP address
- MAC address
- FSAN serial number
- Serial number
- Firmware version

- Model number



To edit mesh (SAT) details

1. From the Home screen, tap on the **My Network** tile.
2. Select the **Equipment** tab.
3. Tap on the mesh system.
4. Tap **Edit**.
5. Edit the system **Name**.

6. Associate the system with a new **Place**.
7. Tap **Submit** to save your changes.

Add Equipment

You can add new mesh units to your network from the **My Network** screen.

Guidelines

- The desired mesh device must have no prior RG pairing. If your mesh satellite has previously been paired to an RG, factory reset the mesh by holding the hardware reset button for 30 seconds.

To add equipment

1. From the Home screen, tap on the **My Network** tile.
2. Tap the *plus sign* and select **Add Equipment**.
The **Add Mesh(SAT)** screen opens.
3. Scan the QR code located on the sticker that came with the device.
Alternately, tap **Issues Scanning?** to enter the device info manually. Device information, including MAC address and serial number, can be found on the sticker applied to the bottom of the unit.
4. Tap **Next**.
5. Enter a **Name** for the device.
6. Tap **Done** to complete the onboarding. If you have additional devices to add, tap **Save and add another Mesh(SAT)** to onboard another mesh device.

Replace a Router

You can upgrade or replace an existing GigaSpire unit from the **My Network** screen.

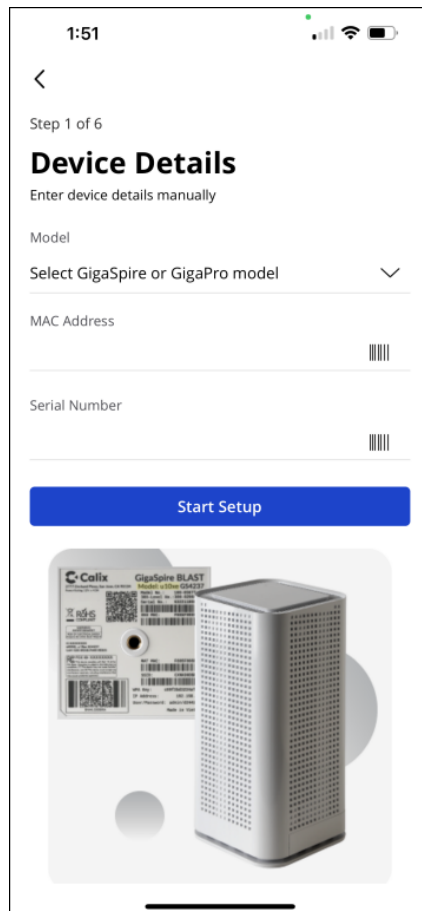
Guidelines

- Your service provider must remotely initiate router replacement sessions from Calix Service Cloud. If you plan to swap your GigaSpire, contact your service provider prior to completing a replacement.
- Guided router replacement currently supports swaps from a GigaSpire to a GigaSpire only.
- The QR-code scanning function requires a camera with auto-focus.

To replace a router

1. From the Home screen, tap on the **My Network** tile.
2. Tap the *plus sign* and select **Replace Router**.

3. On the *Scan device* screen, input the router's MAC address and serial number using one of the following methods:
 - **Scan QR code:**
 - a. Point the camera viewfinder at the QR code printed on the router's product label, located on the bottom of the unit.
 - b. Center the QR code in the middle of the viewfinder frame, and then zoom in or out until the QR code fills the frame and the camera automatically captures the identifier information (where the MAC address and serial number values auto-populate into the respective fields upon capture).
After the capture occurs, proceed to setup. If the capture fails after multiple attempts, use the manual type-in method.
 - **Type:**
 - a. From the *Scan device* screen, tap **Manually Enter Device Details**.
 - b. Select your router model from the **Model** drop-down menu.
 - c. Tap the **MAC Address** field, and then type in the router's MAC address as seen on the label on the bottom of the unit.
 - d. Tap the **Serial Number** field, and then type in the router's serial number as seen on the label on the bottom of the unit.
 - e. Tap **Start Setup**.



-
4. Tap **Next** on the *Replace router* screen.
 5. Follow the on-screen instructions to disconnect your existing router, then tap **Next**.
 6. Follow the on-screen instructions to plug in your new router, then tap **Next**.
 7. Follow the on-screen instructions to connect an ethernet cable, then tap **Next**.
 8. Follow the on-screen instructions to confirm a successful connection, then tap **Next**.
For common troubleshooting tips, tap **I don't see a green light**.
 9. On the *Setup Wi-Fi* screen, tap the **Network Name (SSID)** field, and then type in a name for your Wi-Fi network. This name value is what Wi-Fi client devices will see when they scan for available Wi-Fi networks.
 10. Tap the **Password** field and enter the password for the wireless network.
 11. Tap the **Security Type** selection list to select a security option for the Wi-Fi network:
 - **WPA2-Personal**
 - **WPA - WPA2-Personal**
 - **WPA2 - WPA3-Personal**
 - **WPA3-Personal**
- Note:** WPS is disabled when the WPA3-Personal security type is enabled.
12. (Optional) Tap the **Place** field, and then type in the location of the router in your home (e.g., Living Room).
 13. Tap the **Done** button to save your inputs.

Services

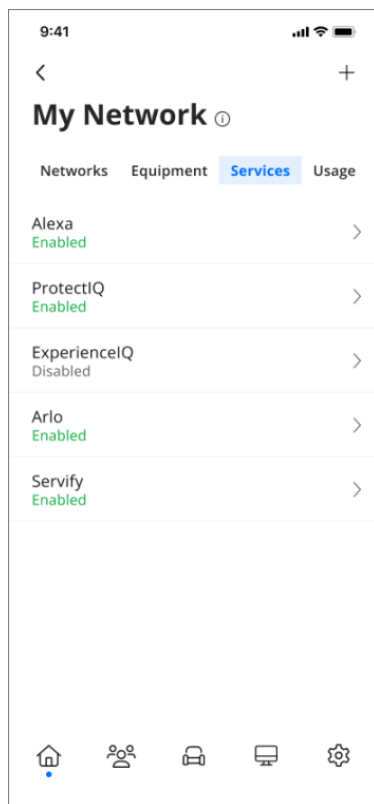
The **My Network > Services** tab provides access to the following container-based applications and service delivery platforms:

- *ProtectIQ* (on page [82](#))
- *ExperiencIQ*
- *Arlo*
- *Servify*

To access this screen, you can either tap the **My Network** tile on the Home screen or tap the *Networks* icon in the bottom menu bar. Then, tap **Services**.

To view Services

1. From the My Network page, tap **Services**.
2. A list of the services installed on the RG is displayed. Each service includes network status (enabled, disabled).
3. Tap on a service to view and configure settings for the service.



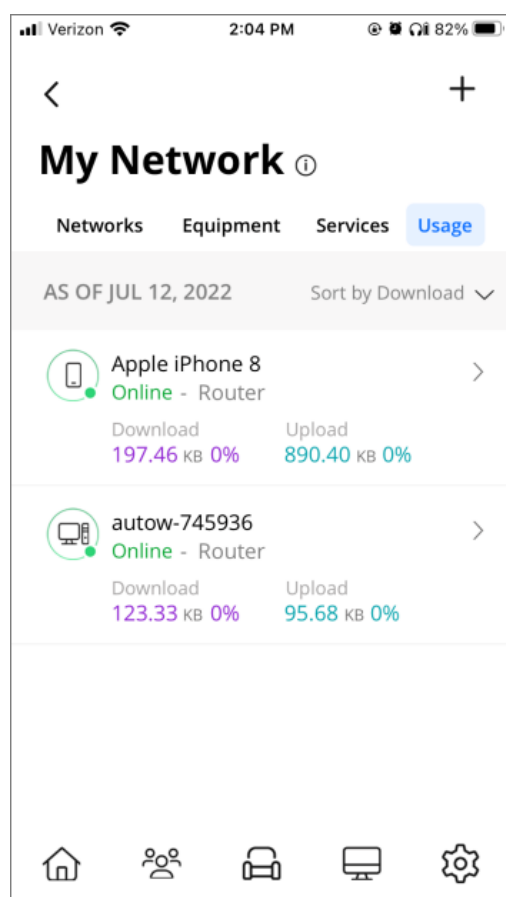
Usage

The **Usage** page provides usage statistics for devices in the network.

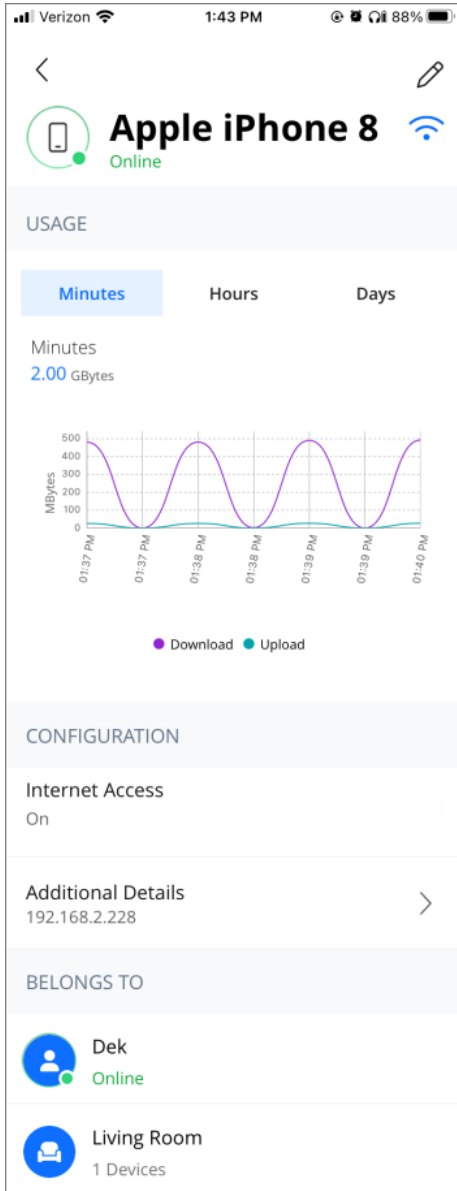
To access this screen, you can either tap the **My Network** tile on the Home screen or tap the **Networks** icon in the bottom menu bar. Then, tap **Usage**.

To view device usage

1. Tap **Usage** from the **My Network** screen. The following usage statistics display for each device:
 - a. Device name
 - b. Device connection status (Online/Offline)
 - c. Router the device is connected to
 - d. Download and Upload usage
 - e. Download and upload percent usage for each device



2. Tap on a device to view additional details.



- Device type (e.g., Phone, Computer)
- Device name
- Connection status (Online, Offline)
- Connection type

USAGE

- Speed test results
- Total data usage
- Latest speed test results

Select a timeframe to view data for the previous day, the previous seven days, or the previous month.

OPTIONS

- Internet Access (On, Off)

Note: See the *Pause Internet Access* article for more information on restricting internet access.

- Additional Details

Tap to view detailed device information:

- Device Type (tap to change)
- Connected to
- Download speed
- Upload speed
- Wi-Fi protocol
- Efficiency
- Radio band
- Radio channel
- Device IP address
- Device MAC address
- Device vendor
- Device model

BELONGS TO

Lists People and Places associated with the thing.

Add a Network

You can set up additional secondary Wi-Fi network from the Add Network menu selection. Creating a secondary Wi-Fi network allows you to provide Wi-Fi internet access to visitors without providing the credentials to your home's primary Wi-Fi network.

Secondary networks can be configured to support a wide range of network types. By default, three secondary network types are listed in the secondary networks table:

- Guest Network
- Work From Home
- Custom Network

Guest Network Attributes

A guest network allows your friends and family temporary access to the internet. Guest Networks are isolated and prevent access to any other devices connected to your primary network.

- The Guest Network option is dual band only, no band splitting.
- WPA3 Authentication mode is fully supported however network prioritization is not.
- Subnet isolation is supported and **enabled** by default. When subnet isolation is enabled, members of the guest network will be unable to access the primary network on this device. Enter the subnet's Gateway Address, beginning and ending IP, and subnet mask to define isolation properties.

Work From Home Network Attributes

A Work From Home (WFH) network allows a limited number of devices that require high-priority access to the internet. Work From Home networks are isolated and prevent access to any other other devices connected to your primary network.

Custom Network Attributes

A custom network allows for the most flexible configuration to best fit your internet access needs.

- The Custom Network option can be single, dual, or tri band, allowing the subscriber to create 2.4 GHz only, 5 GHz only, or 6 GHz only SSIDs.
- WPA3 Authentication mode is fully supported.

Note: The 6 GHz SSID only supports the WPA3-Personal, WPA2-WPA3-Personal, and Enhanced Open security types.

- Subnet isolation is supported and **disabled** by default.

To add a guest Wi-Fi network

1. From the My Network screen, tap the *plus sign*.
2. Tap **Add Network**.
3. Select **Guest** from the **Wireless Network Type** drop-down menu.

Note: The Isolation option provides added security in that you can choose to isolate this network from other networks as appropriate. Guest networks default to On.

4. Enter a new **Network Name (SSID)**.
5. Select a **Security Type**:
 - None
 - WPA2-Personal
 - WPA-WPA2-Personal
 - WPA2-WPA3-Personal (default)
 - WPA3-Personal
6. Enter the **Wi-Fi Password**.
7. Tap to disable Isolation. By default, this option is enabled for guest networks.

Note: The Isolation option provides added security in that you can choose to isolate this network from other networks as appropriate.

8. Set the access duration time for this network. Being this is a guest network, normally the duration will tend to be quite short.
 - **Endless:** For guest networks that are permanent in nature. All guests entering the network will use the Guest SSID and password. The guest network will always be on and anyone within range can access this network.
 - **Custom:** Establish a start time and a stop time for this network.
9. Tap **Save** when finished.
10. Tap **OK**.

Note: For detailed information on establishing secondary networks and assigning security types, refer to the [GigaSpire BLAST Service Providers Guide](#) for assistance.

Upon completion, a pop-up message displays asking whether you would like to share the guest network SSID and password.

Tap **Share** to share the network details.

Tap **Skip** to complete the guest network setup and return to the My Networks screen.

To add a Work From Home network

1. From the My Network screen, tap the *plus sign*.
2. Tap **Add Network**.
3. Select **Work From Home** from the **Wireless Network Type** drop-down menu.
4. Enter a new **Network Name (SSID)**.
5. Select a **Security Type**:
 - None
 - WPA2-Personal
 - WPA-WPA2-Personal
 - WPA2-WPA3-Personal (default)
 - WPA3-Personal
6. Enter the **Wi-Fi Password**.
7. The Prioritization and Isolation options are enabled by default and cannot be disabled.

Note: The Isolation option provides added security in that you can choose to isolate this network from other networks as appropriate.

8. Tap **Save** when finished.
9. Tap **OK**.

To add a custom Wi-Fi network

1. From the My Network screen, tap the *plus sign*.
2. Tap **Add Network**.
3. Select **Custom** from the **Wireless Network Type** drop-down menu.

Note: The Isolation option provides added security in that you can choose to isolate this network from other networks as appropriate. Custom networks default to Off.

4. Enter the **Network Name (SSID)**.
5. Select the **Band**:
 - All (default)
 - 2.4G
 - 5G
 - 6G
6. Select the **Security Type**:
 - None

- WPA2-Personal
 - WPA-WPA2-Personal
 - WPA2-WPA3-Personal (default)
 - WPA3-Personal (default for 6G band)
7. Tap to enable **Prioritization**.
 8. Tap to enable **Isolation**. By default, this option is disabled for custom networks.


Note: The Isolation option provides added security in that you can choose to isolate this network from other networks as appropriate.

9. Tap **Save** when finished.


Edit a Network

From the **My Network** screen, you can edit a network's SSID, password, and security type.

To edit primary network settings

1. From the **Home** screen, tap on the **My Network** tile.
2. Tap on the desired network.
3. Tap on the *pencil*  icon.
4. Edit the network name (SSID), password, and security type.
5. Tap **Save**.

To edit secondary network settings

1. From the **Home** screen, tap on the **My Network** tile.
2. Tap on the desired network.
3. Tap on the *pencil*  icon.
4. Edit the network settings as desired.
5. Tap **Save**.

Things

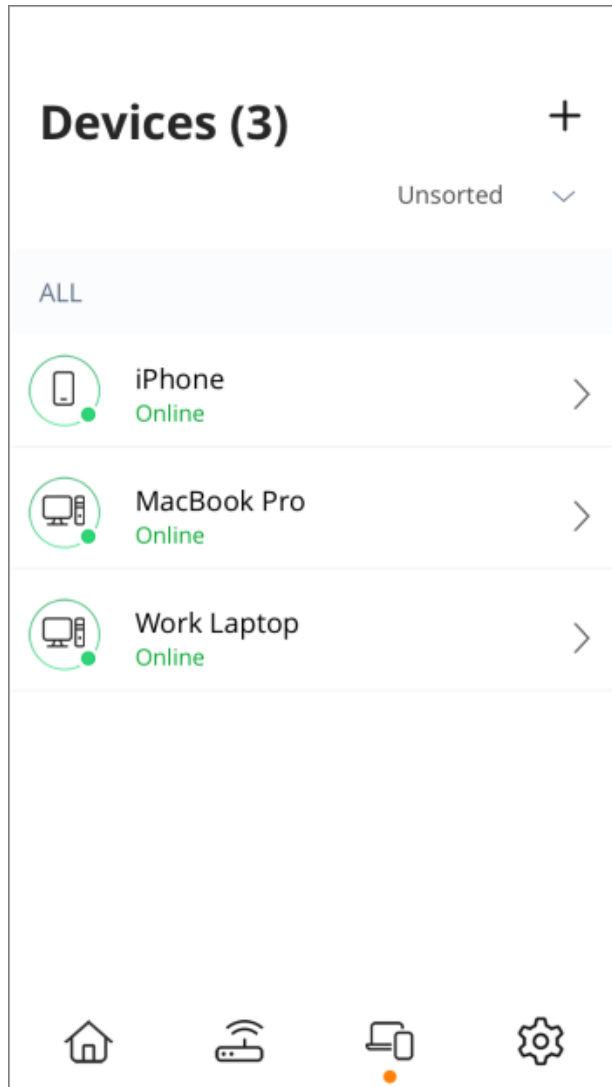
The Things tab stores information on all components connected to the network. Each thing displays its network status (On or Offline) and connection type (Wireless or Ethernet). When querying any device in the network, easy to read statistics and graphs are provided to facilitate network optimization. Tapping any subheadings (All, Type, People, Place) sorts the results as indicated.

Note: Listed devices can be sorted by Type, People, and Place.

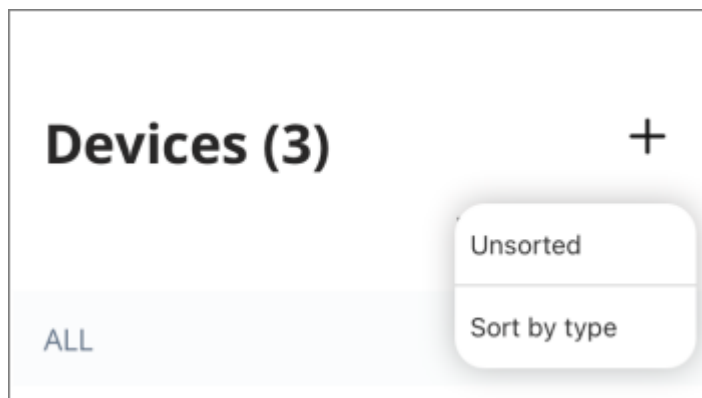
To view things

1. Tap the *Things* icon in the bottom menu bar. Alternately, tap the **Things** tile on the Home screen.

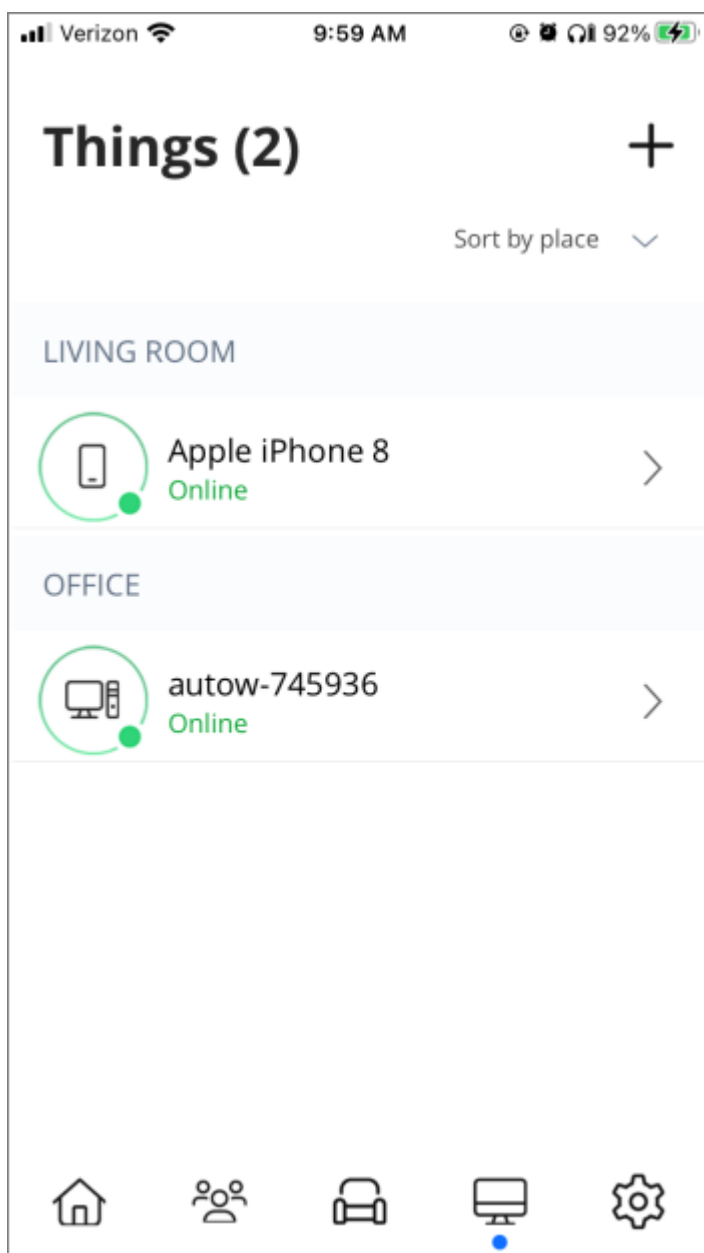
The list of things connected to your network displays.



Sort the list to view devices by type, people, and places.

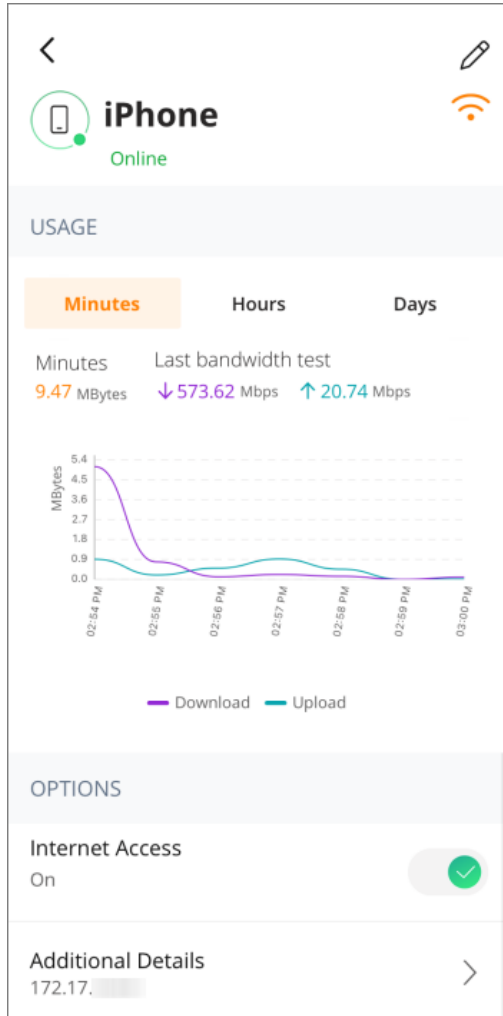


Example things sorted by Place



To view thing details

1. From the **Things** screen, tap the desired device.
The following information displays.



- Device type (e.g., Phone, Computer)
- Device name
- Connection status (Online, Offline)
- Connection type

USAGE

- Speed test results
- Total data usage
- Download speed
- Upload speed

Select a timeframe to view data for the previous three minutes, the previous six hours, or the previous seven days.

CONFIGURATION

- Internet Access (On, Off)

Note: The Internet Access toggle for Things is unavailable when the system lacks an ExperienceIQ container or when the device is assigned under People without ExperienceIQ.

- Additional Details

Tap to view detailed device information:

- Device Type (tap to change)
- Connected to
- Download speed
- Upload speed
- Signal strength
- Radio band
- Device IP address
- Device MAC address
- Device vendor
- Device model

BELONGS TO

Lists People and Places associated with the thing.

Add Things

You can add a Thing to your network by either connecting the Thing to the wireless SSID or by connecting via WPS. Please note that the WPS option is disabled if the wireless network security type is set to WPA3-Personal.

To add a Thing by connecting to the wireless SSID

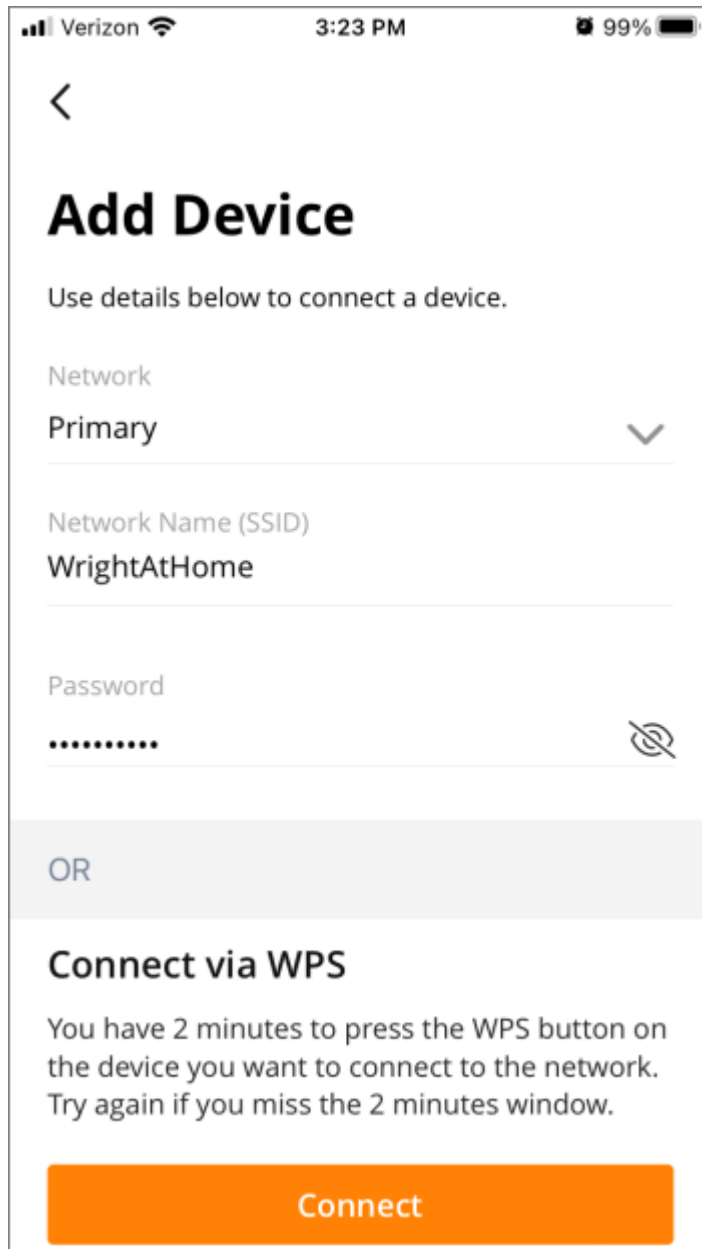
1. Tap the *Things* icon in the bottom menu bar. Alternately, tap the **Things** tile from the Home screen.
2. Tap the plus sign.
The wireless network information are displayed.
3. Connect the Thing to the network using the provided SSID and password.
After the Thing connects to the network, it appears in the Things list.

To add a Thing via WPS

Note: The WPS connection option is disabled if the wireless security type is set to WPA3-Personal.

1. Tap the *Things* icon in the bottom menu bar. Alternately, tap the **Things** tile from the Home screen.
2. Tap the plus sign.
3. Tap the **Connect** button on the bottom of the screen to begin a two-minute WPS session. The device to be connected will listen for a signal from the network and will continue to try to connect.

Note: If a connection is not established within two minutes, tap the Connect button again to retry.



The screenshot shows an iPhone interface for adding a device. At the top, the status bar displays 'Verizon', signal strength, Wi-Fi, the time '3:23 PM', and a battery level of '99%'. Below the status bar is a back arrow. The main heading is 'Add Device'. Underneath, it says 'Use details below to connect a device.' There are three input fields: 'Network' with a dropdown menu currently showing 'Primary', 'Network Name (SSID)' with the text 'WrightAtHome', and 'Password' with a masked field of dots and a visibility toggle icon. A grey bar with the text 'OR' separates this from the 'Connect via WPS' section. This section includes the text 'You have 2 minutes to press the WPS button on the device you want to connect to the network. Try again if you miss the 2 minutes window.' At the bottom of this section is a large orange button labeled 'Connect'.

Edit Things

From the Things screen, you can edit a Thing's name and associate the Thing with people and places.

To edit a Thing

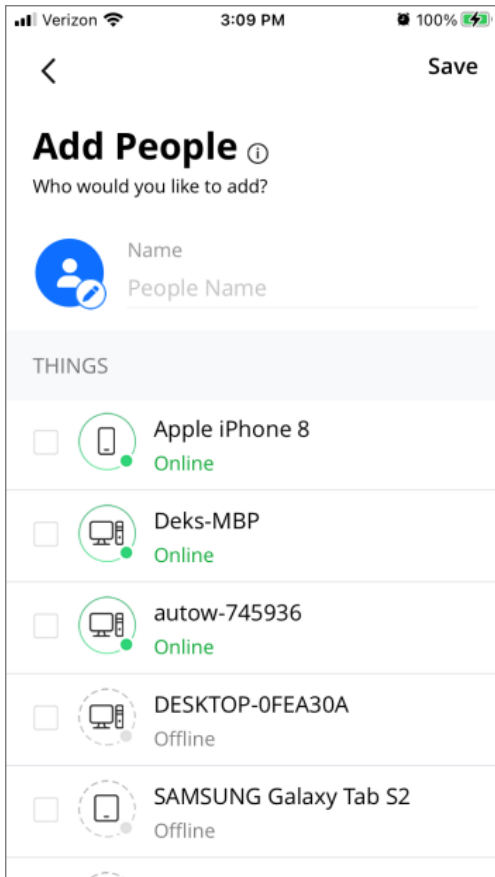
1. Tap the *Things* icon in the bottom menu bar. Alternately, tap the **Things** tile from the Home screen.
2. Tap the desired Thing.
3. Tap the *pencil* icon to view the Things details.
4. Tap into the **Name** field to edit the Thing name.
5. Tap **Apply**.
6. Tap on a Person or a Location to associate the Thing with a new person or place.
7. Tap **OK** to confirm.
8. Tap the *back arrow* to save your changes and return to the Thing details screen.

People

From the People screen of the CommandIQ app, you can view and manager your network users.

Add People

User profiles are designed to store network preferences pertaining to parental controls and equipment/services usage.



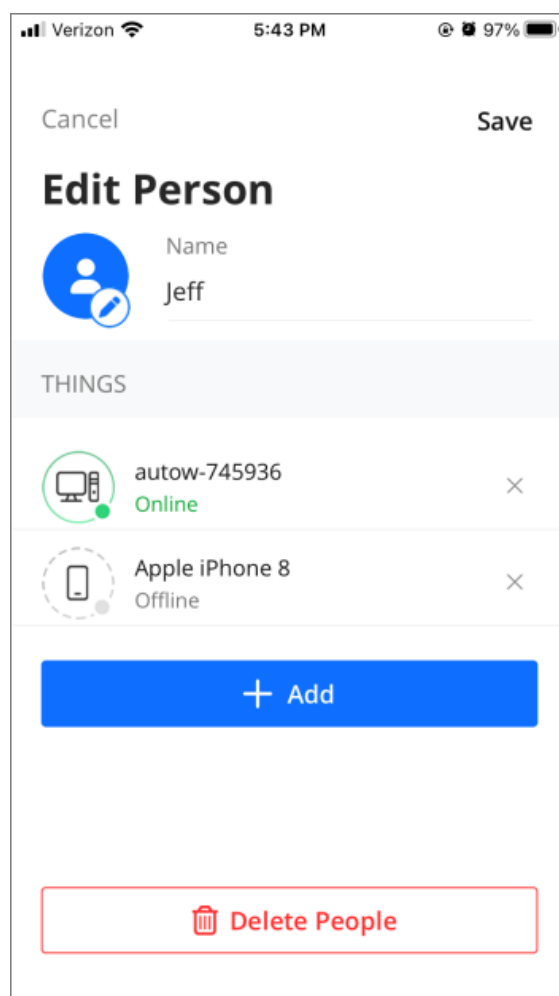
To add a person

1. Tap the *People* icon in the bottom menu bar. Alternately, tap the **People** tile from the Home screen.
2. Tap the *plus sign* icon to add a new person.
3. Tap into the **Name** field to add the person's name.
4. Tap the *pencil* icon the profile avatar to add a profile image.
5. Select the checkbox for each Thing you would like to associate with the person.
6. Tap **Save**.
A confirmation window displays.
7. Tap **OK** to return to the People screen.

Edit/Delete People

To edit a person

1. Tap the *People* icon in the bottom menu bar. Alternately, tap on the **People** tile from the Home screen.
2. Tap on the desired person.
3. Tap the *pencil* icon.
4. Edit the person's information.
 - Tap into the **Name** field to edit the person's name.
 - Tap the *pencil* icon to change the person's profile image.
 - Tap **+ Add** to associate a thing with the person.



5. Tap **Save** to save your changes and return to the People screen.

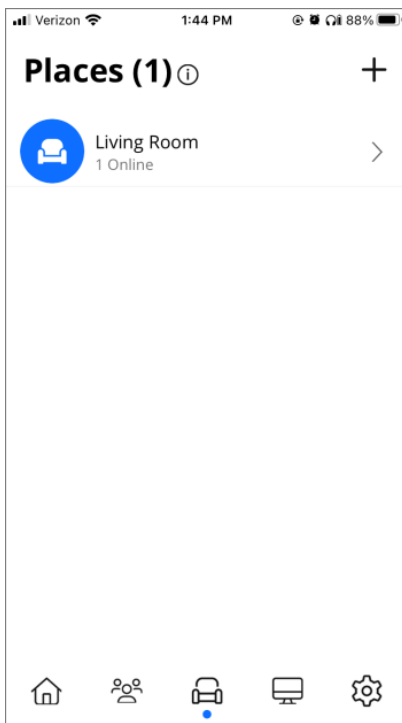
To delete a person

1. Tap the *People* icon in the bottom menu bar. Alternately, tap on the **People** tile from the Home screen.
2. Tap on the desired person.
3. Tap the *pencil* icon.
4. Tap **Delete People**.
5. Tap **Yes** to confirm.
6. Tap **OK** to return to the People screen.

Places

From the Places screen of the CommandIQ app, you can view and manage your network places. To access the Places screen:

1. Tap the **Places** tile from the Home screen.
- or -
2. Tap the *Places* icon in the bottom menu bar.



Add Places

Places can be configured from the home page allowing Things to be attached to a place with it's own rules and features.

To add a Place

1. Tap the *Places* icon in the bottom menu bar. Alternately, tap the **Places** tile from the Home screen.
2. Tap the *plus sign*.
3. Enter a name for the place.
4. Tap the *pencil* icon on the profile image to add an image.
 - a. Tap **Camera** to take a new photo or tap **Gallery** to select an existing photo from your device.
5. Select the checkbox for each Thing you would like to associate with the Place.
6. Tap **Save**.

Edit/Delete Places

To edit a Place

1. Tap the *Places* icon in the bottom menu bar. Alternately, tap the **Places** tile from the Home screen.
2. Tap on the desired Place.
3. Tap the *pencil* icon.
4. Edit the Place's name and profile image.
5. Tap **+ Add Thing** to associate a Thing with the Place.
6. Tap the x to disassociate a Thing from the Place.
7. Tap **Save**.

To delete a Place

1. Tap the *Places* icon in the bottom menu bar. Alternately, tap the **Places** tile from the Home screen.
2. Tap on the desired Place.
3. Tap the *pencil* icon.
4. Tap **Delete Place**.
5. Tap **Yes** to confirm.
The Place is deleted.
6. Tap **OK** to return to the Places screen.

Chapter 4

ExperiencelQ

ExperiencelQ provides provisioning access to a container-based application for parental control and network priority.

Note: For container-based applications (e.g., ProtectIQ, ExperiencelQ), if the application has not been subscribed, the application and its options will not be displayed.

With user profiles, ExperiencelQ readily facilitates:

- *Setting time limits*
- *Setting account restrictions*
- *Application and/or website blocking*

The above facilities ensure age-appropriate content and screen time limits are observed.

To enable ExperiencelQ

1. From the **My Network** screen, tap the **Services** tab.
2. Tap **ExperiencelQ**.
3. Tap the **Enable service** toggle to enable (turn the toggle green).

My Priorities

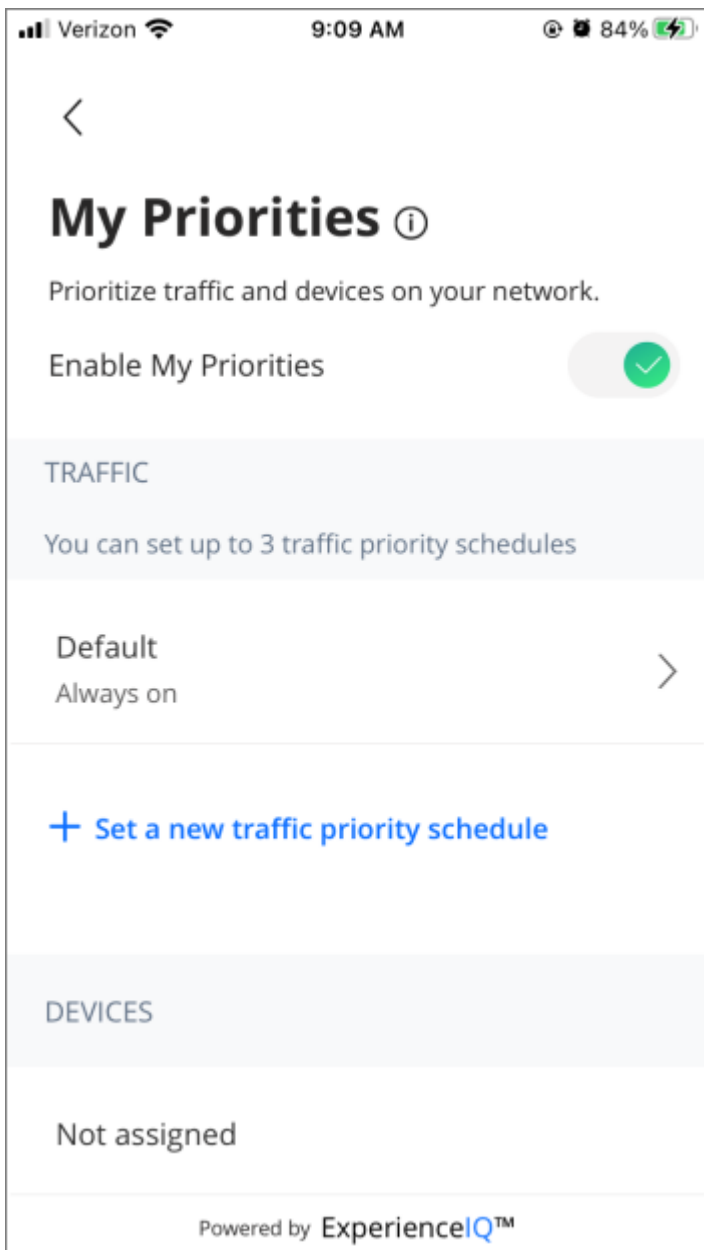
My Priorities allows a user to prioritize network traffic based on application type and prioritize devices on the network. Before enabling My Priorities, a bandwidth test must be run on the BLAST system. The results of this test are used to set the upstream and downstream bandwidth limits for each queue used by My Priorities. The user can then rank the priority of applications on the network.

Application categories, with specific examples, include the following:

- **Work:** Zoom, Microsoft Teams®, Microsoft Office 365®, etc.
- **Browsing:** HTTP, SMTP, POP3, DNS, etc.
- **File Transfers:** FTP, iCloud®, Dropbox®, etc.
- **Video & Music:** Netflix®, Spotify®, Hulu®, etc.
- **Gaming:** Call of Duty®, Diablo®, Counter Strike®, etc.
- **P2P File Sharing:** BitTorrent™, eDonkey, etc.

Schedules can be created to prioritize applications based on the time of day and day of the week. A user can have a workday schedule where Work & Browsing have the highest priority and then an evening schedule where Video & Gaming get a higher priority.

Individual client devices (up to five) can be added to a device priority list. Client devices in this list will have all traffic, regardless of application, set with the highest priority.

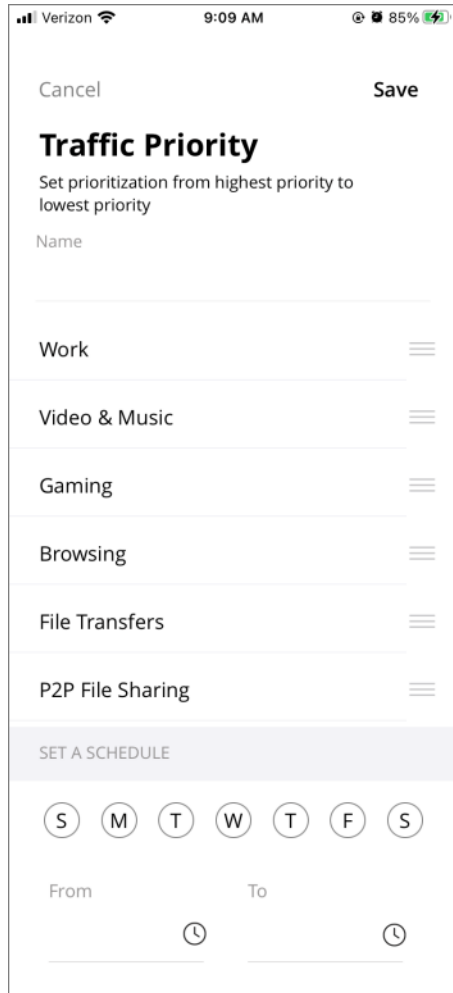


Traffic Priorities

Additional priorities can be included based on your specific environment.

To set a traffic priority

1. From the My Network screen, tap **Priorities**.
2. Tap **Set a new traffic priority schedule**.



3. Enter a name for the traffic priority into the **Name** field.
4. Drag and drop the various categories of traffic to reflect the priority you wish to give them.
5. Select the day(s) of the week that you want the traffic priority applied.
6. Tap into the **From** field to set the start time.
7. Tap into the **To** field to set the end time.
8. Tap **Save**.
9. Tap **OK**.

To delete a priority

1. From the My Network screen, tap **Priorities**.
2. Select the desired schedule.
3. Tap **Delete Priority**.
4. Tap **OK**.

Device Priorities

Individual devices can harbor their own priorities. Up to five devices can share the same priorities (the default priorities has no limit).

To set a device priority

1. From the My Network screen, tap **Priorities**.
2. Tap **Set device priorities**.
3. Select either **Always On** or **Set Duration**.
 - If Set Duration is selected, tap into the **Duration** field to set the length of time the traffic will be affected.
4. Tap **+ Add Device**.
5. Select the device(s), than tap **Save**.
6. Tap **OK**.
7. Tap **Save** after all selections are complete.

Parental Control Profiles

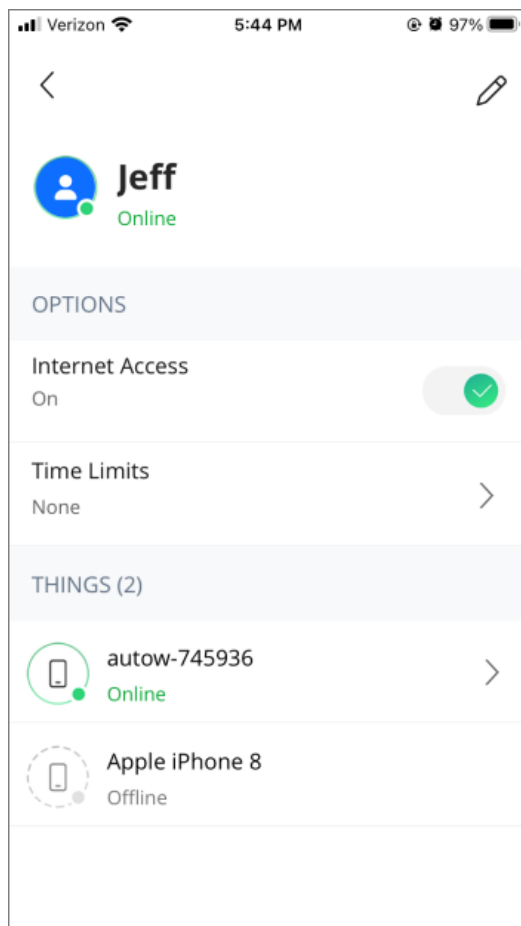
After creating user profiles, time limits, account restrictions, and content/website restrictions can be configured to ensure age-appropriate and screen time limits are observed.

Parental control profiles allow the user to configure user profiles with time limits and content restrictions.

To enable or disable internet access for a person

1. Tap the *People* icon in the bottom menu bar. Alternately, tap the **People** tile from the Home screen.
2. Tap on the desired person.
3. Tap the toggle to enable (On) or disable (Off) internet access for the person.

After internet access is disabled for a person, none of the devices associated with the person will be able to access the internet.



To set internet time limits for a person

1. Tap the *People* icon in the bottom menu bar. Alternately, tap the **People** tile from the Home screen.
2. Tap on the desired person.
3. Tap **Time Limits**.
4. Select one of the following options:
 - **None (default)**: Allows the person unrestricted internet access.
 - **Everyday**: Set a daily time limit for internet access. Any thing(s) associated with the person will not be able to access the internet outside of the selected hours. For example, if you select 7:00am to 9:00pm, the person has internet access every day from 7:00am to 9:00pm. Between the hours of 9:00pm and 7:00am, none of the things associated with the person will be able to access the internet.
 - a. Select a **Start Time** and an **End Time**.
 - b. Tap **Save**.
 - **Custom**: Set a different time limit for each day of the week.
 - a. Tap on a day.
 - b. Tap **+ Add Time Range**.
 - c. Select a **Start Time** and an **End Time**.
 - d. Tap **Submit**.
 - e. Repeat for the remaining days.
5. Tap **Save**.

Parental Control Settings

You can configure global or user-specific restrictions that affect content, applications, and websites.

The SafeSearch and YouTube Restricted Mode feature provides additional filtering of inappropriate content. Developed by major search engines vendors (including Google and Bing), SafeSearch blocks explicit images, videos, and websites. This filtering is especially useful when applied to user profiles within the CommandIQ system. This same filtering applies to any devices that are associated with those user profiles.

The SafeSearch features utilize detailed algorithms to filter out inappropriate content. Although these algorithms do an excellent job of finding and blocking this content, this feature will not catch everything since new sites and content will always find new ways to by-pass these filters. For this reason, consider the SafeSearch feature as an extra layer of protection against unwanted content coming through.

If inappropriate content escapes these filters and is shown in your search results, you can click the following links to re-define the algorithm:

- Use the following link for reporting inappropriate content (Google):
<https://support.google.com/websearch/answer/510>
- Use the following link for reporting inappropriate content (Bing):
<https://www.microsoft.com/en-us/concern/bing>

DNS over HTTPS and Apple iCloud Private Relay are new network options available on devices and in applications which could enable a user to bypass a content control. By blocking these two options, parents can be assured that their children are not bypassing restrictions by using encrypted DNS or relaying traffic via the Apple iCloud.

Encrypted DNS can be enabled by both operating system and web browser. DNS over HTTPS (DoH) is a protocol to enable DNS name resolution via HTTPS rather than traditional UDP DNS. It is used to increase privacy and prevent manipulation of DNS data by "man in the middle" attacks. By using HTTPS, DNS queries are encrypted which prevents snooping. Other options include DNS over TLS (DoT) and DNS over QUIC (DoQ).

Browsers such as Chrome, Edge, and Firefox all support DoH, some by default. Apple, Android, and Windows also support DoH.

Current operating systems and web browsers claim support for encrypted DNS to increase privacy and security. However, this approach will bypass most parental control functions. Stopping users from using this method will enable parental controls functions.

Note: When DoH is applied, the Safe Search and YouTube Restriction are automatically disabled.

Restrictions in ExperienceIQ work in part by inspecting the DNS queries from client devices. If a client device is using DoH, they can possibly bypass content, application, and website restrictions. Parents can now block DoH on EXOS systems running R22.2 and higher.

Client devices/browsers that are set with the automatic DoH settings should revert to classic DNS behavior if DoH is blocked. Clients that have had DoH settings manually changed may simply fail DNS resolution, at which point they will need to be reverted to automatic DoH settings or the block lifted.

To prevent flooding a user with alerts, when DoH is detected and blocked on a client device, only one alert per device, per 24 hours will be sent. For testing purposes, rebooting the RG will reset the 24-hour timer.

Apple iCloud Private Relay is a service for iCloud+ subscribers which acts as both an encrypted DNS relay and a VPN/Proxy. When Private Relay is enabled, traffic requests are sent to two separate internet relays. The user's IP address is visible to the first relay (Apple). The second relay generates a temporary IP address, decrypts the DNS, and connects the user to the requested site. The requested site sees the temporary address as the source of the request.

The Private Relay service would defeat parental controls by both encrypting the DNS (DoH) and acting as a VPN/Proxy.

CommandIQ supports blocking iCloud Private Relay. This triggers the VPN notification in CommandIQ and blocks the initial connection to the Private Relay server. After two minutes, the device reports the network is not compatible with Private Relay and reverts to standard behavior.

Some devices configured with iCloud Private Relay may take longer than two minutes to revert to standard behavior. For these devices, if blocking iCloud Private Relay is a requirement for other devices on the network, then disable the feature on the problem device.

Validate Settings

There are a couple of different ways to determine whether these filters are in effect:

1. Go to **My Network > Default Restrictions**.
2. Tap the **Safe Search** and **YouTube Restriction** toggles to ensure the current algorithms are in effect.
3. Users can validate the settings for identified devices within a given profile by surfing to the following locations:
 - a. YouTube: https://www.youtube.com/check_content_restrictions – Tap the LEARN MORE link for instructions.
 - b. SafeSearch: <https://www.google.com/preferences>
 - c. Bing Safesearch:
 - Navigate to bing.com
 - Tap on the hamburger menu. The SafeSearch knob is visible
 - Tap the SafeSearch button and verify that Bing reflects a strict status.

Tap the info ⓘ icon for additional information on default restriction settings.

Configure Global Restrictions

CommandIQ provides a Default Restrictions profile that allows you to apply global content, application, and website restrictions to all devices not associated with a user profile. By default, the Default Restrictions profile is disabled. You can enable and configure the Default Restrictions profile from **My Networks > Default Restrictions**.

The Default Restrictions profile includes recommended settings for different age groups, including:

- Child (0-8 yrs old)
- Pre-teen (9-12 yrs old)
- Teen (13-18 yrs old)

After you select an age group, you can modify the recommended settings as desired.

Guidelines

- Default restrictions apply to all wired and wireless devices connected to the router.

- Default restrictions do not apply to RG or mesh systems, STB or phone services, or devices in a profile applied to a person.
- Restrictions applied to a person override global restrictions set through the Default Restrictions profile.

To configure global content, application, and website restrictions

1. Select the toggles to enable or disable the following options:
 - Safe Search
 - YouTube Restriction
 - Block DNS over HTTPS
 - Block iCloud Private Relay
2. Tap **Content Restrictions**.
3. Select an age group from the drop-down menu. Settings update according to the selected age group.
4. Modify the settings as desired.
5. Tap the *back arrow* to return to the Default Restrictions screen.
6. Tap **Applications**.
 - a. Begin typing the name of the app. The system auto-completes the word you are typing. When a match is found, select the app.
 - b. After the application is displayed, choose whether you want to block the app, always allow, or allow for a specific amount of time. To restrict access to a certain length of time, type in the amount of time allowed (in hours and minutes).
 - c. Continue adding additional applications until done.
 - d. Tap the *back arrow* to return to the Default Restrictions screen.
7. Tap **Websites**.
 - a. Begin typing the name of the website you wish to block.
 - b. Tap **Done** when complete. The new site appears in the list of restricted websites.
 - c. Tap **Block** or **Always allow** to filter this specific website.
 - d. Tap the *back arrow* to return to the Default Restrictions screen.

Configure Restrictions for a Person

CommandIQ allows you to apply content, application, and website restrictions to a user's profile. For example, you can limit access to social media applications to between 7:00am and 8:00pm for children in your household. Restrictions applied to a person override global restrictions set in the Default Restrictions profile.

To configure content restrictions for a person

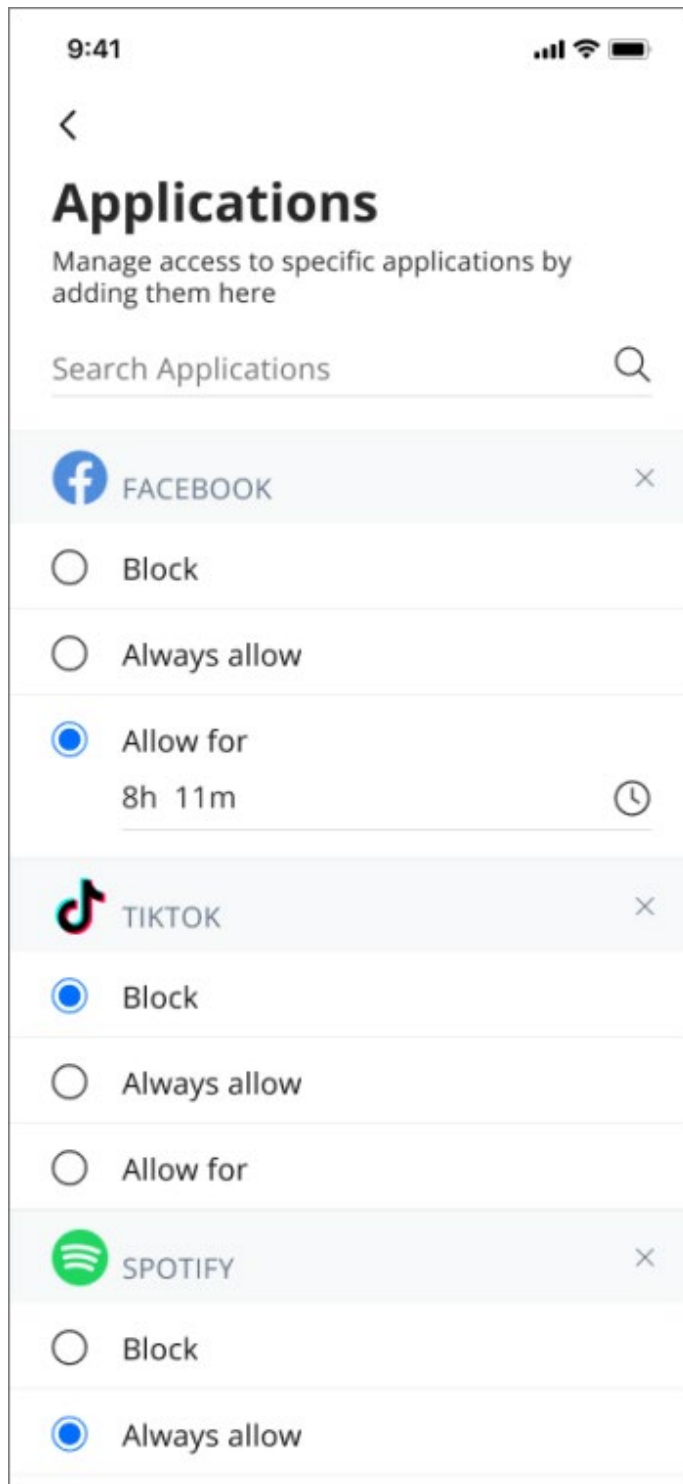
1. From the **People** screen, select the desired user.
2. Ensure the **Internet Access** toggle is set to on (slider is green).
3. Under **Time Limits**, update the time of day where internet access is allowed. After you tap the start time or end time, a time line displays on the bottom of the screen for establishing the exact time.
4. Tap **Save** after time limits are established. Time limits are created.
5. Tap the *back arrow* to return to the Restrictions page.
6. Select **Restrictions > Content Restrictions**. A list of options is displayed based on age group.
7. To apply age group specific filtering, select the appropriate group from the menu:
 - No Restrictions
 - Child (0-8 yrs old)
 - Pre-teen (9-12 yrs old)
 - Teen (13-18 yrs old)

The content restrictions update based on your selection. Scroll down and check the content type that will be filtered for this user.

To configure application restrictions for a person

1. From the **People** screen, select the desired user.
2. Tap **Applications**.
3. Begin typing the name of the app. The system auto-completes the word you are typing. When a match is found, select the app.
4. After the application is displayed, choose whether you want to block the app, always allow, or allow for a specific amount of time. To restrict access to a certain length of time, type in the amount of time allowed (in hours and minutes).

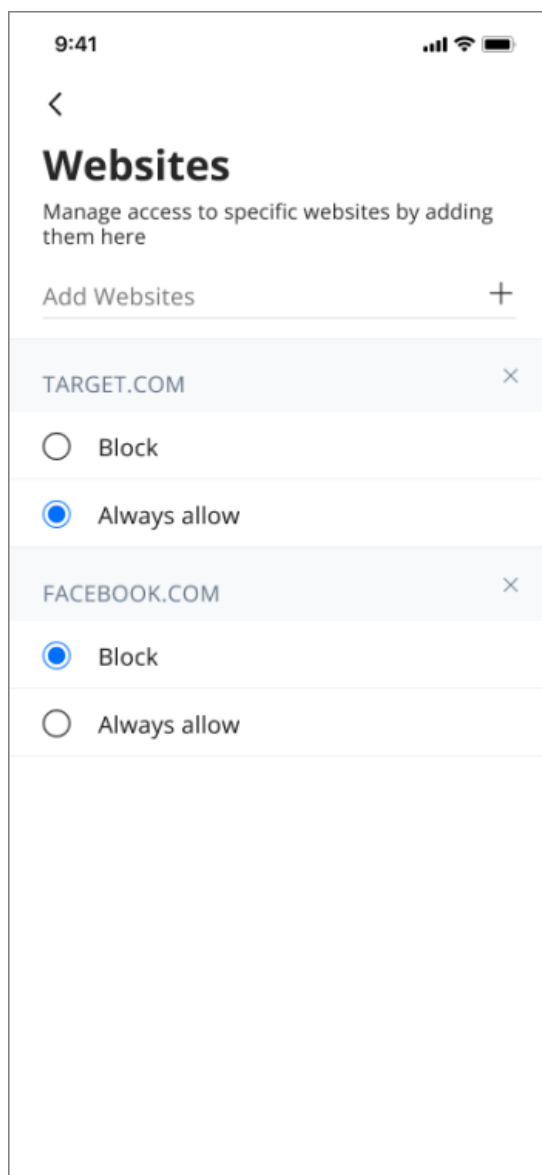
Note: Additions to the Applications filter are always allowed and saved automatically.



5. Continue adding additional applications until done.

To configure website restrictions for a person

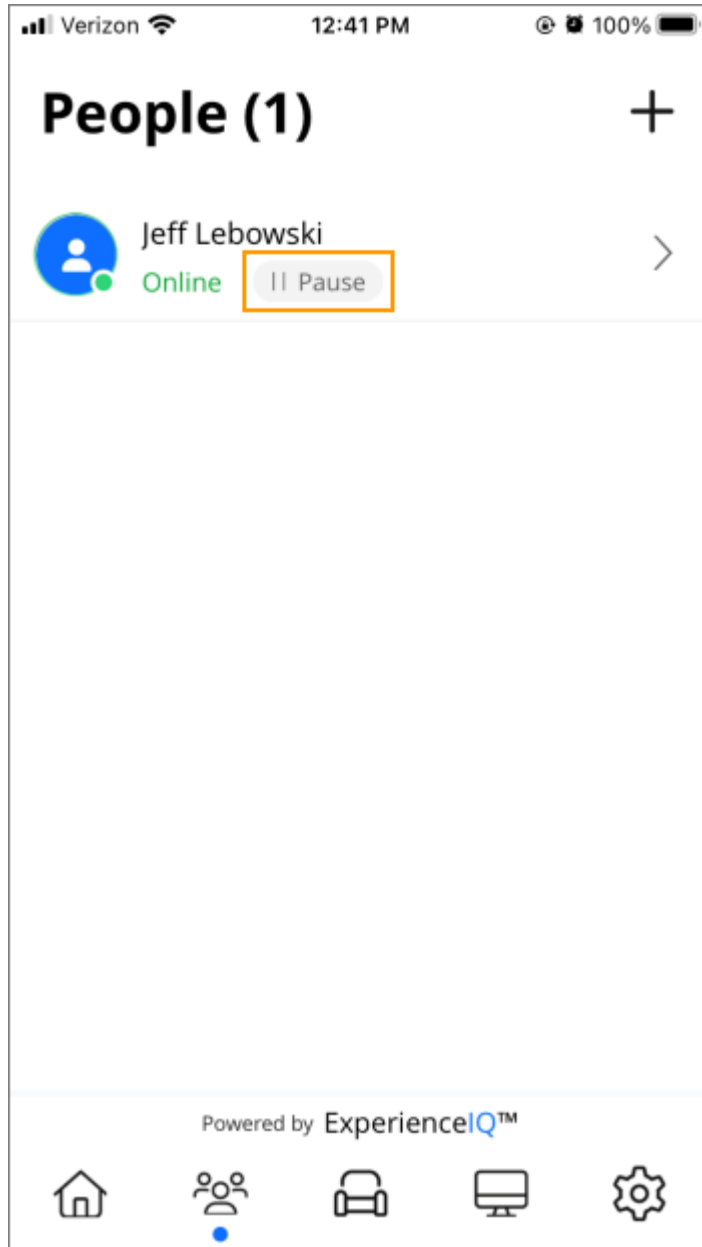
1. From the **People** screen, select the desired user.
2. Tap **Websites**.
3. Begin typing the name of the website you wish to block.
4. Tap **Done** when complete.
The new site appears in the list of restricted websites.
5. Tap **Block** or **Always allow** to filter this specific website.



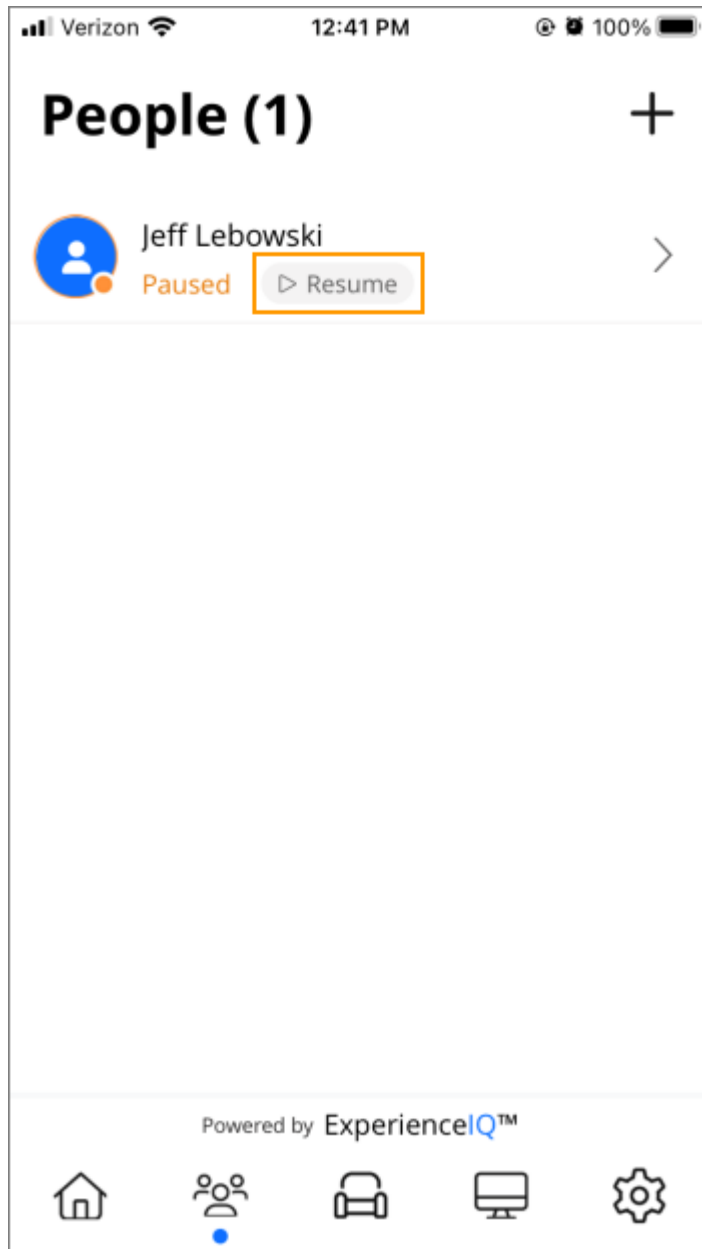
Pause Network Access

A user with a Parental Control profile can have service paused or resumed from the main People screen.

- Tap the **Pause** button to pause service.



- Profiles that are paused remains in that state until manually resumed. To resume service, tap the **Resume** button.



- Add additional time for a blocked profile that has exceeded their access time (in 30-minute increments).
- Specific applications cannot be paused; only the user profile can be paused.

DNS over HTTPS Content Blocking

ExperienceIQ adds support for blocking DNS over HTTPS and Apple iCloud Private Relay. For these features to be functional in CommandIQ, the Gigaspire must be running EXOS 22.2 or newer. In addition:

- DoH will be detected, blocked and an alert sent. (1 per device per 24 hours)
- iCloud Private Relay will be treated as a VPN and VPN detection/blocked alerts will be sent if it is detected.
- Both features are off by default.

Encrypted DNS can be enabled by operating system and web browser. DNS over HTTPS (DoH) is a protocol to enable DNS name resolution via HTTPS rather than traditional UDP DNS. It is used to increase privacy and prevent manipulation of DNS data by "man in the middle" attacks. By using HTTPS, DNS queries are encrypted which prevents snooping. Other options include DNS over TLS (DoT) and DNS over QUIC (DoQ).

Browsers such as Chrome, Edge, and Firefox all support DoH, some by default. Apple, Android and Windows also support DoH.

Note: For the Firefox browser, if DNS over HTTPS is blocked, Firefox reverts to standard DNS to resolve.

Current operating systems and web browsers claim support for encrypted DNS to increase privacy and security. However, this approach will bypass most parental control functions. Stopping users from using this method will enable parental controls functions. In details, the Safe Search and YouTube Restriction are affected.

Note: When DoH is applied, the Safe Search and YouTube Restriction are automatically disabled.

Restrictions in ExperienceIQ work in part by inspecting the DNS queries from client devices. If a client device is using DoH, they can possibly bypass content, application, and website restrictions. Parents can now block DoH on EXOS systems running R22.2 and higher. The system blocks DoH by adding the encrypted DNS server IP addresses to a DB and blocking queries to these addresses via the DPI engine.

Client devices/browsers that are set with the automatic DoH settings should revert to classic DNS behavior if DoH is blocked. Clients that have had DoH settings manually changed may simply fail DNS resolution, at which point they will need to be reverted to automatic DoH settings or the block lifted.

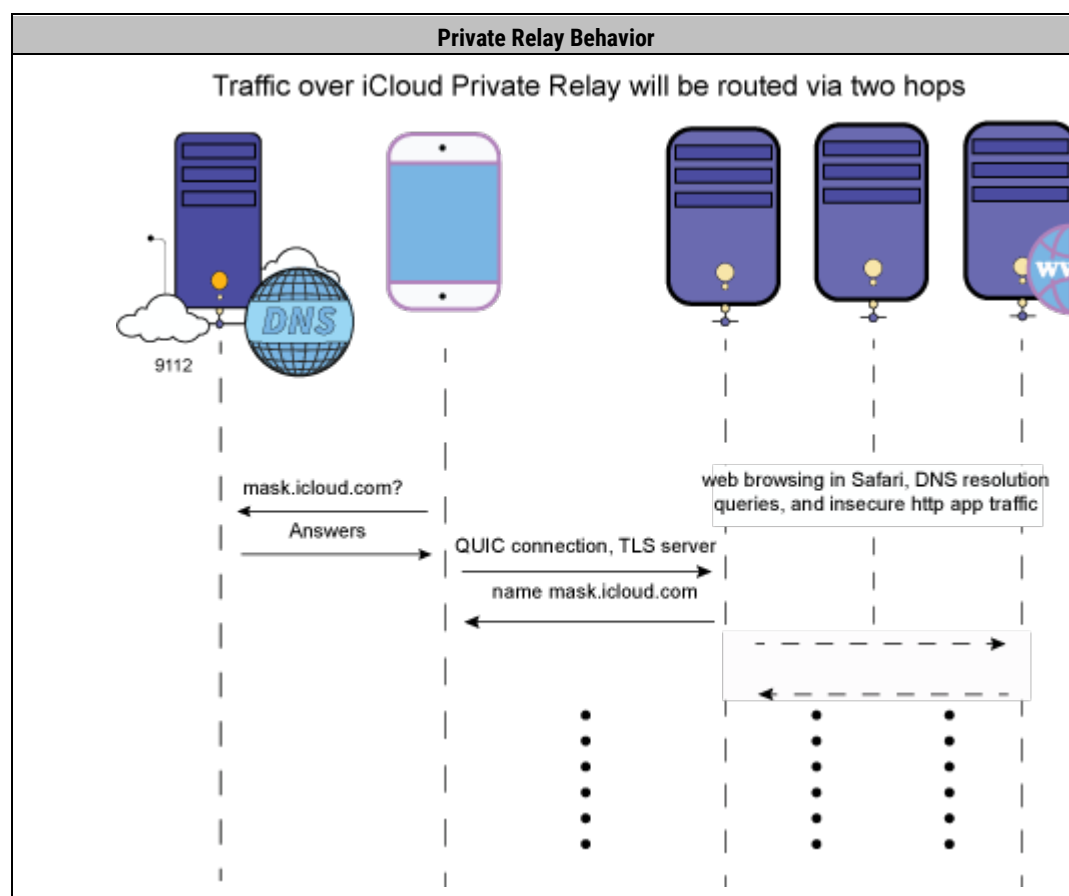
To prevent flooding a user with alerts, when DoH is detected and blocked on a client device, only one alert per device, per 24 hours will be sent. For testing purposes, rebooting the RG resets the 24-hour timer.

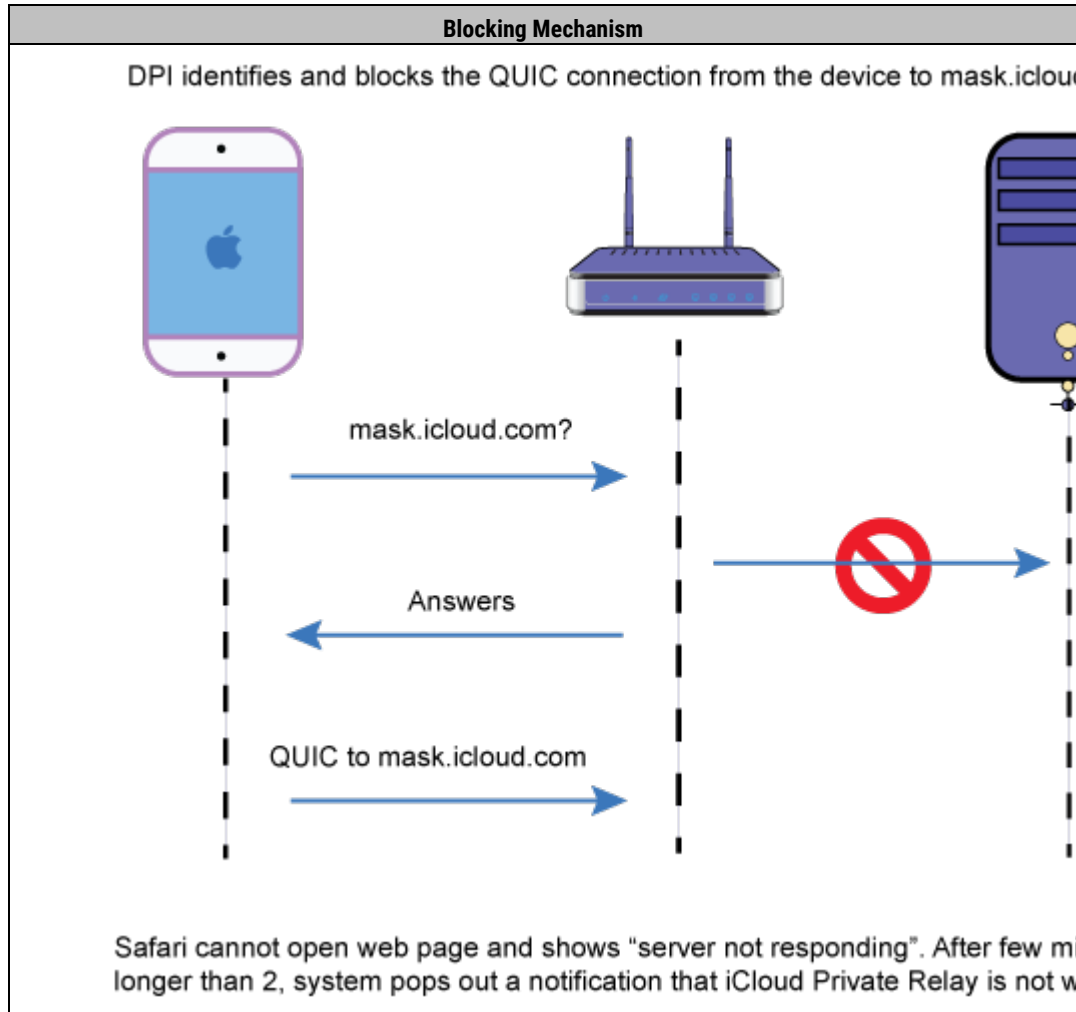
iCloud Private Relay Behavior

CommandIQ supports blocking iCloud Private Relay by detecting the initial DNS query to the private relay DNS server and classifying that connection with an AVC signature of being a VPN/Proxy/Anonymizer. This triggers the VPN notification in CommandIQ and block the initial connection to the Private Relay server. After two minutes, the device reports the network is not compatible with Private Relay and revert to standard behavior.

Some devices configured with iCloud Private Relay may take longer than two minutes to revert to standard behavior. For these devices, if blocking iCloud Private Relay is a requirement for other devices on the network, then disable the feature on the problem device.

Note: iCloud Private Relay is not available in all countries or regions and is currently in beta in iOS 15, iPadOS 15, and macOS Monterey.





ProtectIQ

ProtectIQ is a container-based application that provides network security by scanning for viruses, malware, malicious web sites, and intrusion attempts. From the **My Network > Security** screen, you can manage the following network security settings:

- *Trusted websites*
- *Skip devices for security scanning*
- *Intrusion settings*
- *Additional details*

Before you can view and use ProtectIQ settings, you must first enable the ProtectIQ service.

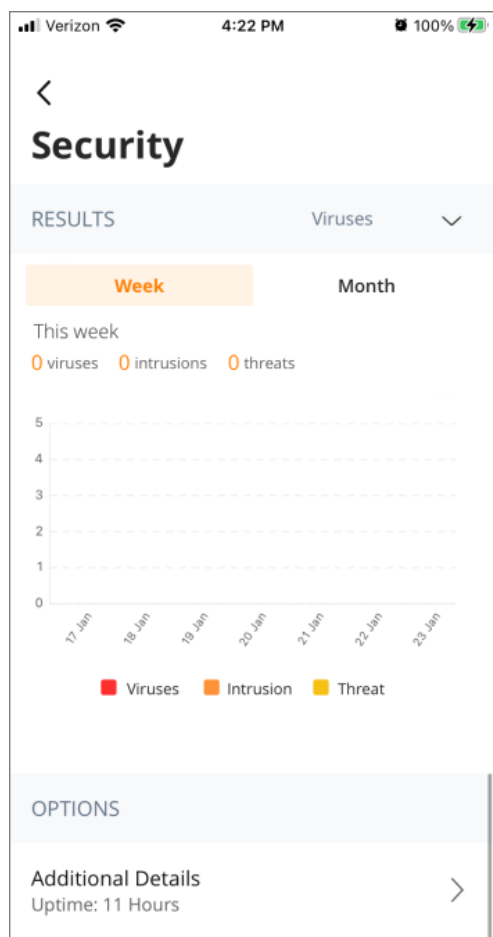
Note: For container-based applications (e.g., ProtectIQ, ExperienceIQ), if the application has not been subscribed, the application and its options will not be displayed.

To enable ProtectIQ

1. From the **My Network** screen, tap the **Services** tab.
2. Tap **ProtectIQ**.
3. Tap the **Enable service** toggle to enable (turn the toggle green).

To view Security data

1. From the Home screen, tap on the **My Network** tile.
 2. Tap **Security**.
 3. Select **Day**, **Week**, or **Month** to view historical security data for the selected time period.
- Filter the results to view virus, intrusion, and threat data.

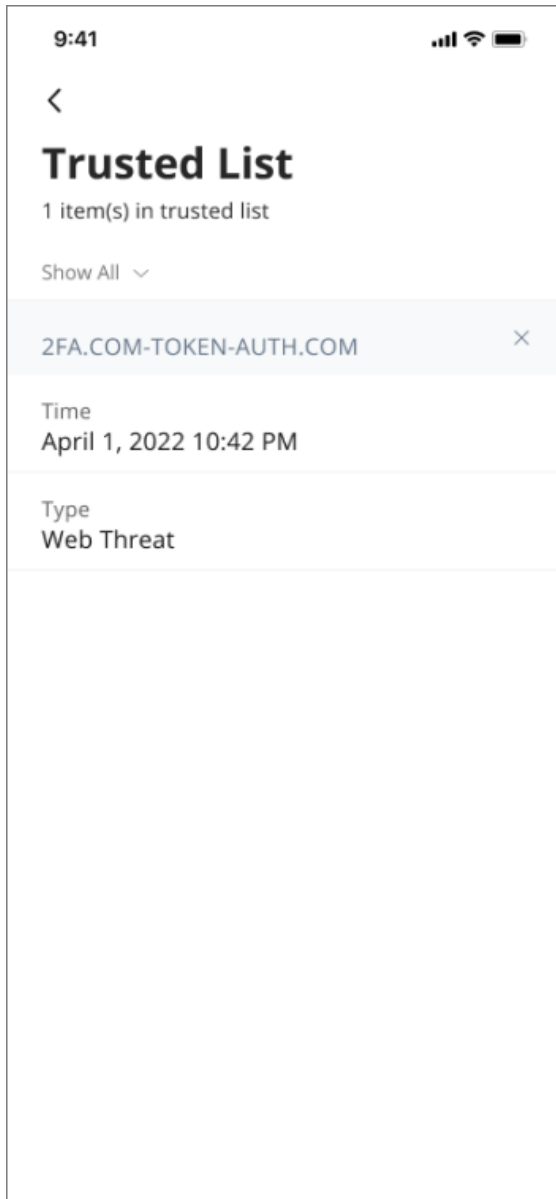


Trusted List

When a GigaSpire BLAST flags a security issue, the user can add it to a Trusted List from the Alert tab.

If a threat is detected that you know is safe, you can add or remove sites from the Trusted List.

CommandIQ displays sites or services based on security notifications.



Note: Intrusion settings continue to monitor websites on the Trusted List.

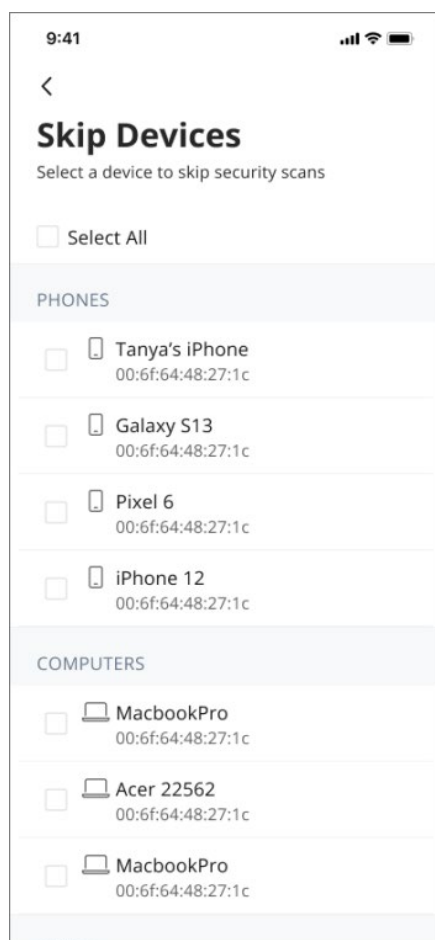
Skip Devices

The Skip Devices feature allows you to turn off ProtectIQ scans based on selected client devices. The Skip Devices screen displays a list of devices connected to and learned by the BLAST system. These devices are arranged into device type categories. After initial detection and scan, you can add learned device to the appropriate category so that network traffic coming to or from the device is no longer scanned again by ProtectIQ.

To skip security scans

1. From the My Network screen, tap **Security**.
2. Tap **Skip Devices**.

A list of network devices displays.



3. Select the checkbox for each device you wish to skip security scans. For convenience, you can tap **Select All** to select and skip all devices at once.

Note: Intrusion settings continue to monitor skipped devices.

Intrusion Prevention System (IPS) Settings

Intrusion Prevention System (IPS) Protocol Anomaly blocks traffic that violates standard TCP/UDP/IP behavior when enabled. Examples include:

- IPv4 header length exceeds packet length
- Bad IP checksum
- IPv4 zero address
- Bad ICMP checksum
- Bad TCP checksum
- GRE checksum error
- HTTP double encoding

IPS Port Scan Defense detects TCP & UDP port scans on the WAN and LAN interfaces and will block the scans when enabled. Port scans are commonly used by bots on the internet to look for vulnerable services on a network. Blocking a port scan attempt is just one layer of network security. The following types of scans are supported:

- TCP RST Scan
- TCP Flood Scan
- UDP Scan

Intrusion settings are handled by two security options in ProtectIQ which can be enabled or disabled individually and include:

- **IPS Protocol Anomaly** is used for detecting both network and computer intrusions and potential misuse by monitoring system activity and classifying traffic as either normal or anomalous. To identify attacking kind of traffic, the system learns what normal traffic looks like and applies the protocol anomaly feature as needed.
- **IPS Port-Scan-Defense** provides an additional layer of security to thwart would be attackers who run port scans looking for open windows (ports) into a computer. The port-scan-defense feature employs various methods to recognize unwelcome port scan attempts and blocks the scan.

Note: When enabled, intrusion settings monitor trusted and skipped devices.

Verizon 2:08 PM 91%

< Save

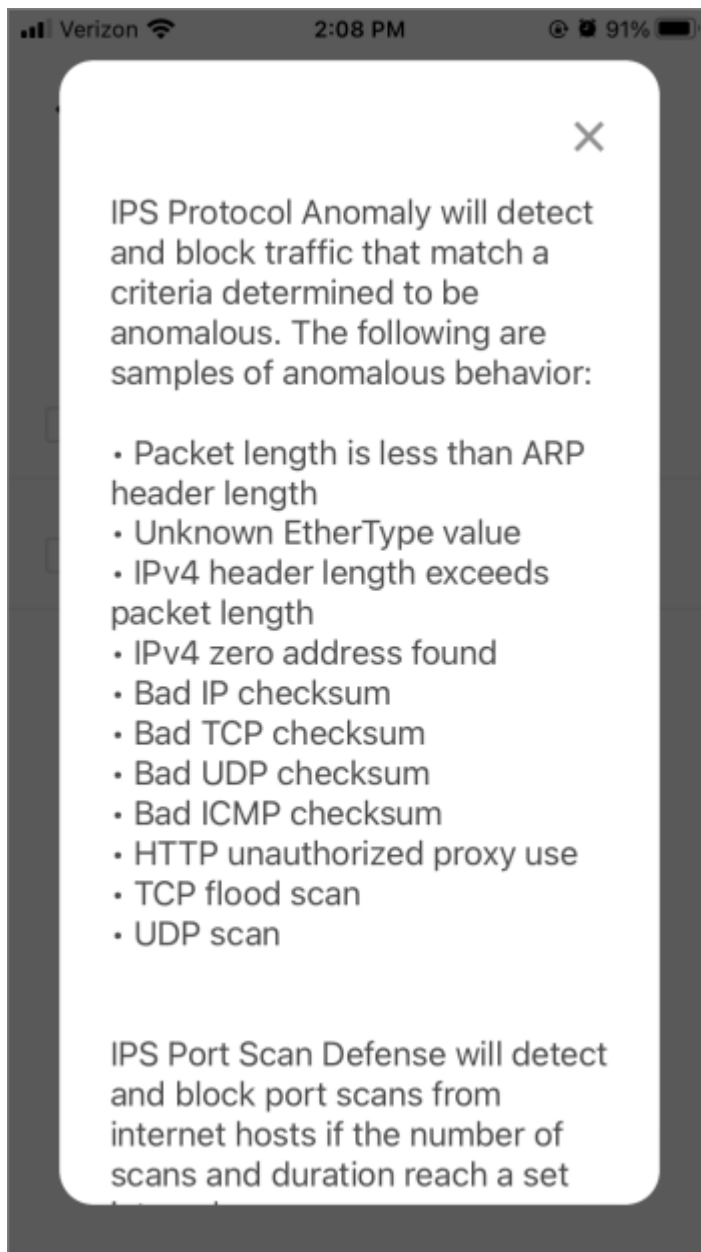
Intrusion Settings ⓘ

Intrusion prevention system settings: select the box for these security features if you want to enable them.

IPS Protocol Anomaly

IPS Port-Scan-Defense

For more information on IPS settings, tap the info ⓘ icon.



LAN Threat Detection and Notification

ProtectIQ supports port scan defense, although it is disabled by default. The port scan defense monitors for TCP Flood Scans, TCP RST Scans, and UDP Scans.

In earlier releases, only the WAN interface of the Gigaspire was monitored for port scans. With EXOS R22.2, the LAN ports and Wi-Fi are also monitored.

ProtectIQ can detect the port scan from WAN, and self protection. However, LAN side devices have not been added to the watchlist which misses some attack info from LAN side. Adding br-lan to the watch list can protect devices from LAN side attack to WAN side.

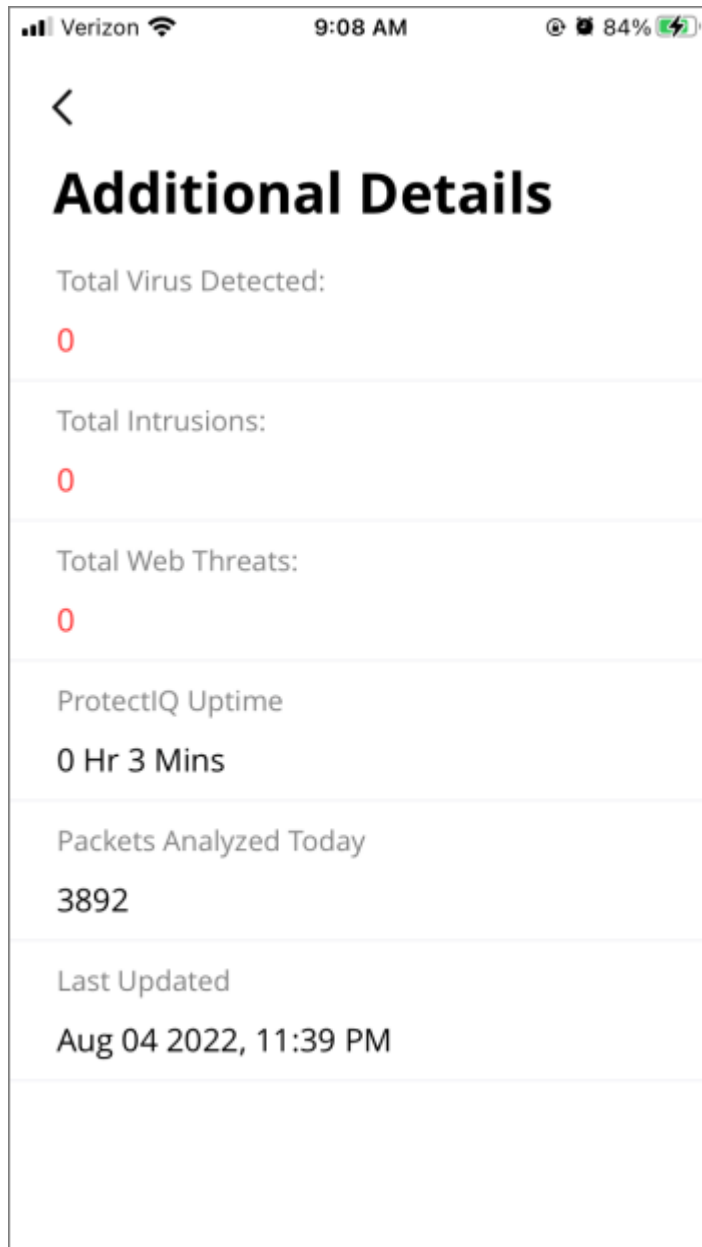
TCP & UDP Port scans from a LAN host will now be blocked and logged if IPS Port-Scan-Defense is enabled. This includes scans of hosts on the LAN and hosts outside on the WAN.

The LAN port scan defense is enabled by default when IPS Port-Scan-Defense is enabled and cannot be disabled via CommandIQ.

Additional Details

To view additional Security details

1. From the home page, tap **My Network**.
2. Tap **Security**.
3. Tap **Additional Details**. Details concerning ProtectIQ uptime, last firmware update, packets analyzed, and virus/intrusions/threats are displayed.



ProtectIQ Alerts

When threats are detected by ProtectIQ, an alert is generated detailing the specific threat, when it occurred, and the source IP of the threat.

Note: For erroneous ProtectIQ alerts that are displayed, an option exists on the bottom of the page to add the offending address to the trusted list.

To edit ProtectIQ alert settings

1. Navigate to **Settings > Alerts**. Alternately, from the Home screen, tap the *Alerts* icon, then tap the *Settings* icon.
2. Scroll to the ProtectIQ section.
3. Tap the toggles to enable (green) or disable ProtectIQ alert notifications.

Arlo

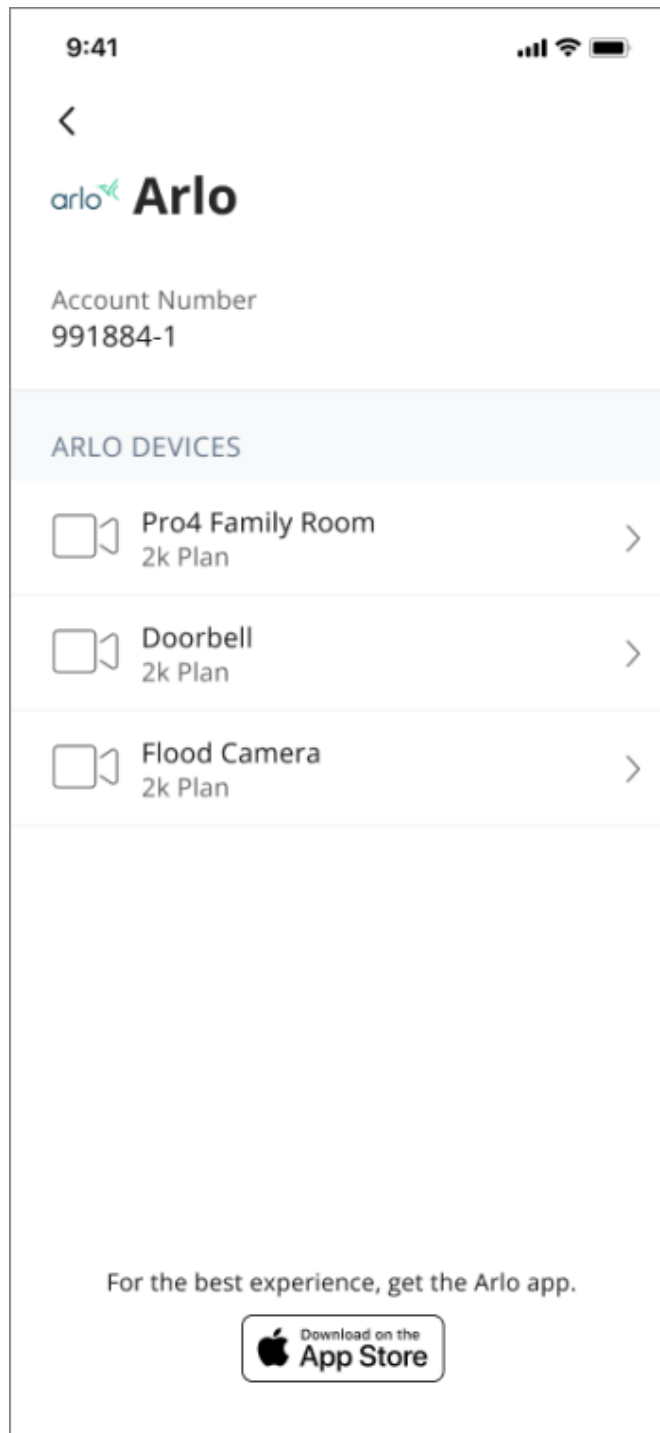
From CommandIQ, you can view a list of your Arlo devices and Arlo device details.

Note: This feature requires an active Arlo entitlement.

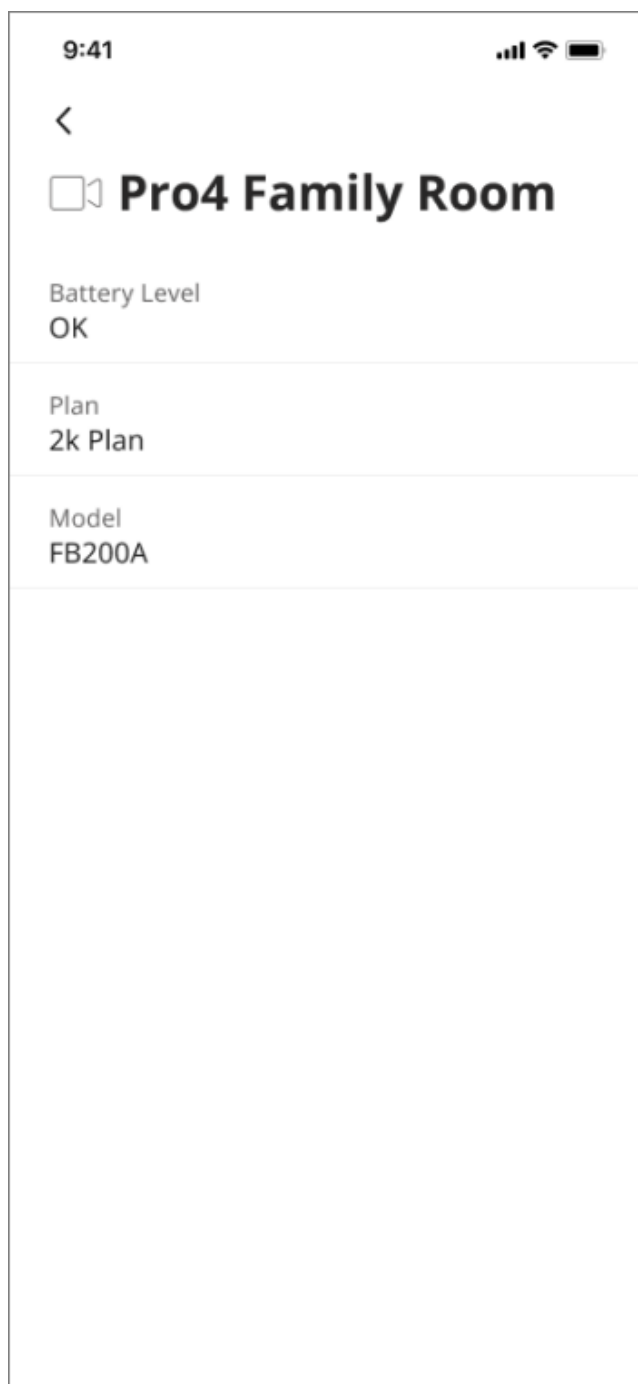
To view Arlo devices

1. Navigate to **My Network > Services > Arlo**.

Your Arlo account number and devices are displayed.



2. Tap on a device to view device details.



Servify

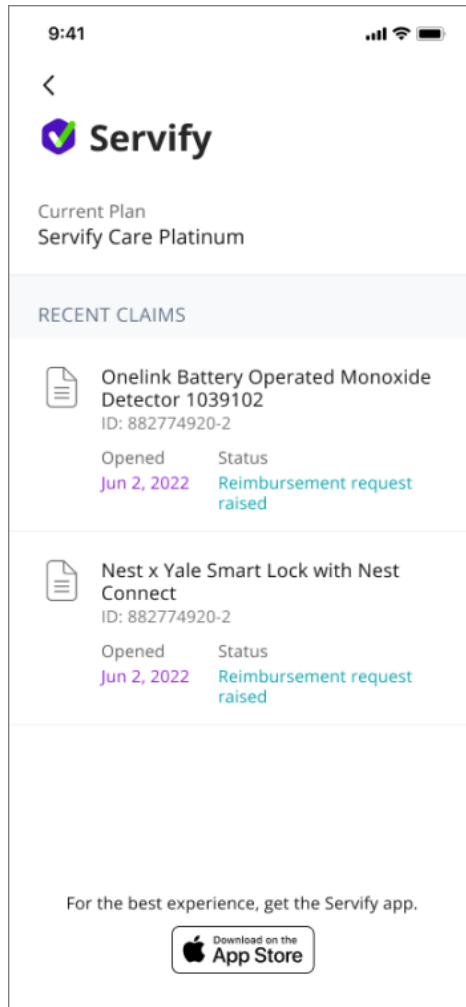
Servify is a container-based application that allows you to view your Servify claims and claim status from CommandIQ.

Note: This feature requires an active Servify Bronze or Servify Platinum subscription.

To view Servify claims

1. Navigate to **My Network > Services > Servify**.

View your Servify plan, claims, and claim status. If you have the Servify app installed on your device, you can open Servify from CommandIQ.



Chapter 5

Settings

From the Settings menu, you can modify and personalize app settings and your home broadband Wi-Fi experience. The Settings menu is accessible directly from the bottom menu bar.

To view selection options on the Settings tab

1. From the home screen, tap the *Settings* icon in the bottom menu bar.
2. Tap to select from the available options:
 - **Account:** You can change the account (user) name, email address, and password by tapping the Avatar image or the email address at the top of the screen. Options exist for updating account information as well as adding or removing accounts.
 - **Set Passcode:** CommandIQ supports the use of a numeric Personal Identification Number (PIN) option in lieu of a password to log into the app. Select this menu item to establish or update a PIN for login.
 - **Language:** CommandIQ supports screen display language in English, French Canadian, Spanish, and German, with English as the default. You can switch the display language from the Language screen.
 - **Terms & Conditions:** View the developer's current End User License Agreement (EULA) from the Terms and Conditions screen.
 - **Privacy Policy:** View the developer's privacy policy for the CommandIQ application
 - **Contact Support:** View support contact options—including phone, email, and web—and access the billing portal.
 - **About:** See the developer's high-level description of the CommandIQ app on the About screen as well as the current CommandIQ release version.
 - **Log out:** Tap the Log out button to log out from the CommandIQ app.

Update Account

From **Settings > Account and Admins**, you can change key account data or remove accounts from the CommandIQ app.

To update or remove the CommandIQ user account and reset the router configuration

1. Navigate to **Settings > Account and Admins**.
2. Tap **Edit**.
3. To update the avatar, tap the *pencil* icon and download a new avatar from your photo library.
4. Update the first name, last name, and email address, and password fields as necessary.
 - a. The email address used to log into CommandIQ, established during initial setup, can be changed at any time. Select this item to modify the app login password.
 - b. The password to log into CommandIQ that you established during initial setup can be changed at any time. Select this item to modify the app login password. Update the password and toggle the viewable password option as needed.

Delete Account

On occasion, the account that manages the GigaSpire BLAST and or its satellites needs to be reset (deleted). Perform the steps below to execute the account deletion.

To delete an account

1. Navigate to **Settings > Account and Admins**.
2. Tap **Edit**.
3. Tap **Remove Account**.

A warning message displays ensuring that you do not inadvertently remove this account.

4. Tap **Yes, Remove**.

The account is removed and all account information, including routers and mesh systems, is deleted from the app. After you remove the primary account, you must complete the router onboarding process the next time you sign in to the app.

Set Passcode

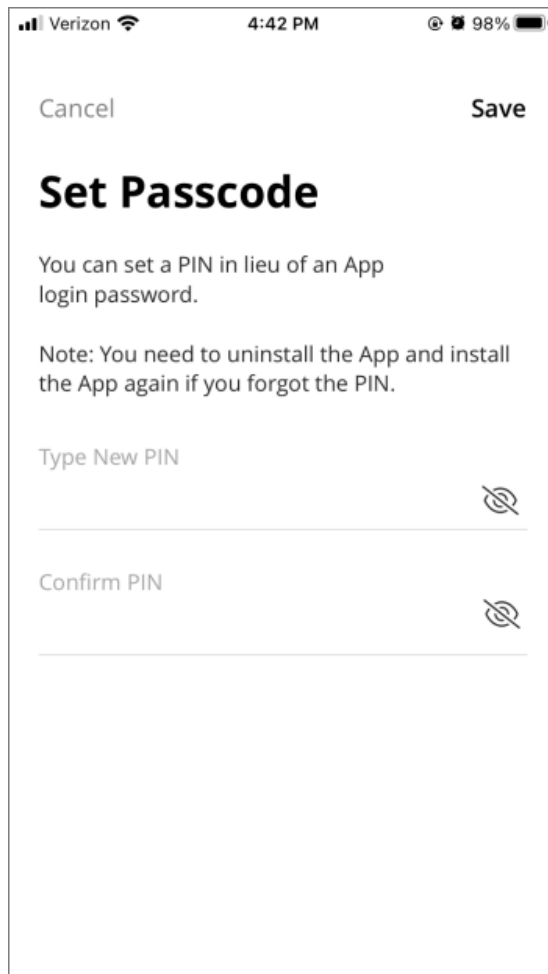
CommandIQ supports the optional use of a numeric Personal Identification Number (PIN) to log into the app, in lieu of an alphanumeric password. If you prefer to use a PIN code instead of a password for login, you can establish a PIN code from the Set Passcode screen.

A PIN code replaces the login password that was established during initial setup. The PIN code can be up to six digits long. After you set a PIN, the option to enable biometric login (fingerprint or facial recognition).

Note: There is no way to recover a forgotten PIN. After establishing a PIN, if you later forget the PIN, you must un-install and then re-install the CommandIQ app to resume use.

To set passcode for login

1. Navigate to **Settings > Set Passcode**.
2. Tap into the **Type New PIN** field and type to enter a PIN code (up to six digits in length).



3. Tap into the **Confirm PIN** field and re-type the PIN code to confirm a match.
4. Tap **Save** to return to the Settings menu.

After you set a PIN, the following Settings menu options become available:

- Reset Passcode
- Enable/Disable Passcode
- Enable/Disable Biometric Login

To enable biometric login

Note: To enable biometric login, you must set a PIN.

1. From the **Settings** menu, select the **Biometric Login** toggle to enable (turn the toggle green).

To reset a passcode

1. From the **Settings** menu, tap **Reset Passcode**.
2. Tap into the **Type Current PIN** field to enter your current PIN.
3. Tap into the **Type New PIN** field to enter your new PIN.
4. Tap into the **Confirm PIN** field to confirm the PIN.
5. Tap **Save**.

To disable passcode login

1. From the **Settings** menu, tap the **Passcode** toggle to disable (turn the toggle gray).
By default, disabling passcode login also disables biometric login.

Secondary Account Support

You can add a secondary (administration) account to the network.

To create a secondary account

1. Navigate to **Settings > Account and Admins**.
2. Tap **Invite Admin**.
3. Input the user's first name, last name, and email address.

Note: Email addresses must be unique. If your email address is already in use, enter a known unused address.

4. Tap **Send Invite**. An email is sent to the secondary account asking for verification of acceptance.

Note: After the email is sent, the secondary account status switches to Pending until the Invitee accepts.

To delete the secondary account as the primary admin

1. Swipe left on the secondary account to reveal the *trashcan* icon.
2. Tap the *trashcan* icon and confirm the account is to be deleted.
An **Are you Sure?** message displays prior to deletion.
3. Confirm the deletion.

To delete the secondary account as the secondary admin

The secondary account user may also delete their own account.

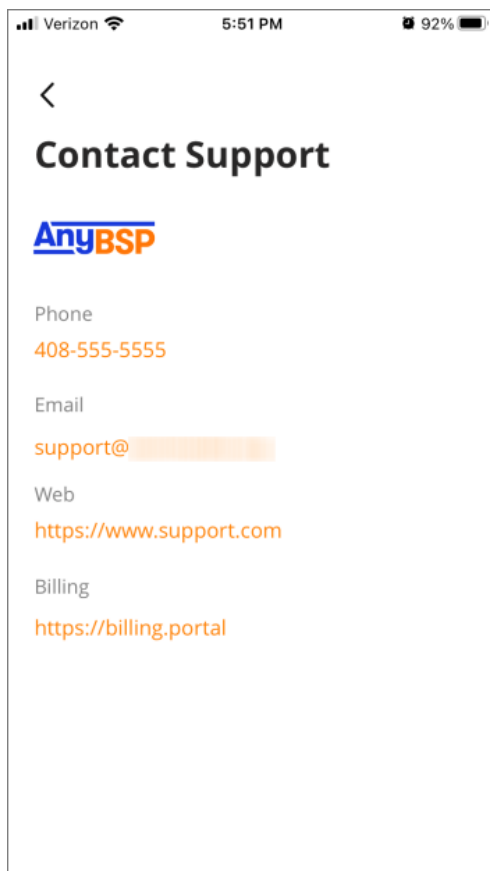
1. Go to **Settings > Account and Admins**.
2. Tap **Edit**.
3. Tap **Delete**.
4. Confirm the deletion.

Contact Support

Broadband Service Providers (BSP) can embed their support contact information into CommandIQ. For CommandIQ to receive this data, the BSP must first populate the support information in Calix Cloud. See the Add CommandIQ Support Information topic for more information.

From the **Settings > Contact Support** screen, users can access the following support information:

- Phone number
- Email
- URL
- Billing portal

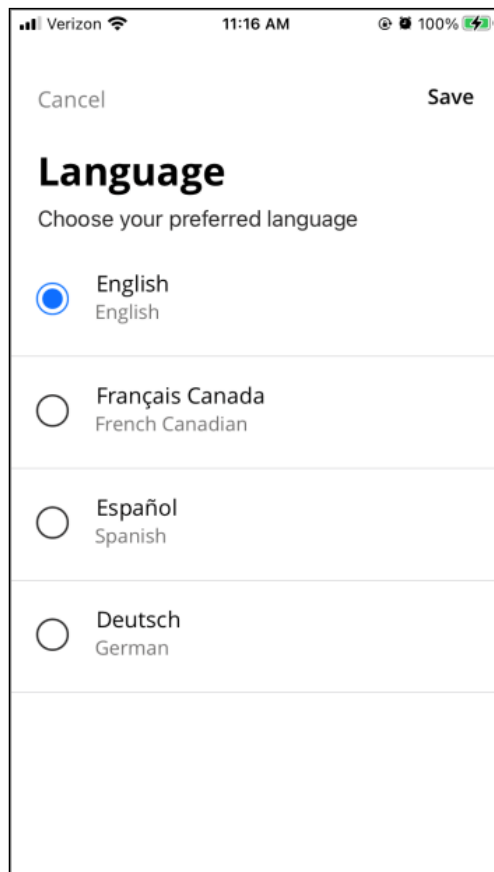


Language

The CommandIQ app screens are presented in the English language by default, but the app also supports presentation in French Canadian, Spanish, and German. You can switch the display to any language by choosing the desired option.

To change the language

1. Navigate to **Settings > Language**.
2. Tap on your desired language:
 - English (default)
 - French Canadian
 - Spanish
 - German
3. Tap **Save**. The screen text throughout the app changes to the selected language.



Alerts

CommandIQ can notify users for many network related events. An alert can be raised when a new device connects, when a satellite is disconnected, when a website or application is blocked or when a web threat is detected. Users can fine tune which alerts will be pushed through as a notification.

VPN detection allows the administrator of the system to monitor VPN connections, thereby bypassing the standard security settings for each user. This feature is passive in nature in that the system doesn't change anything other than logging the connection.

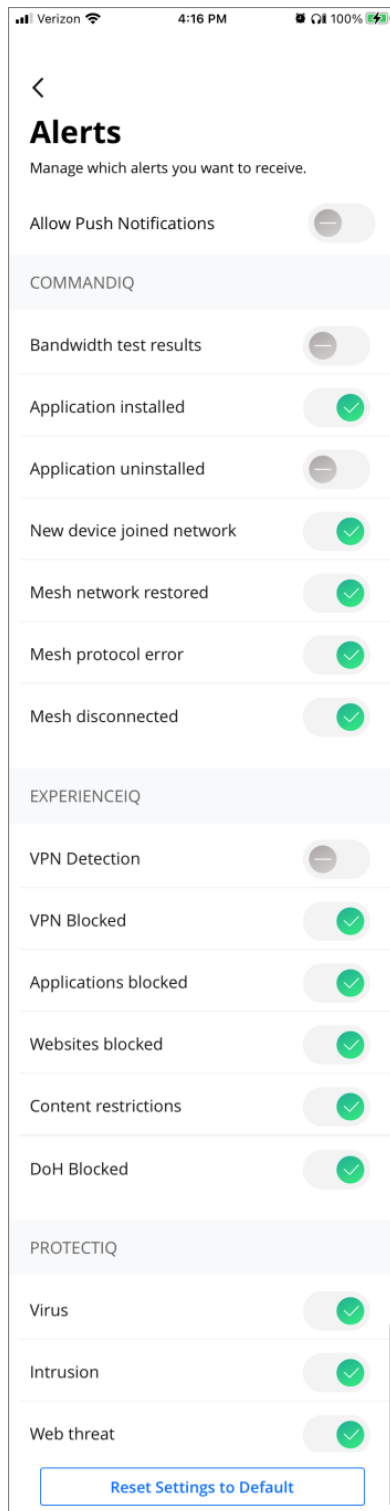
If VPN Detection is enabled, an alert is generated and saved in the Notifications folder within CommandIQ.

Note: For VPN Detection to be present, the ExperienceIQ application must be present and enabled.

To edit alert settings

1. From the Home screen, tap the *Alerts* icon.
2. Tap the *Settings* icon. Alternately, navigate to **Settings > Alerts**.
3. Select the toggle to enable or disable alert push notifications.

4. Select the toggle to configure alert settings for CommandIQ, ExperienceIQ, and ProtectIQ.



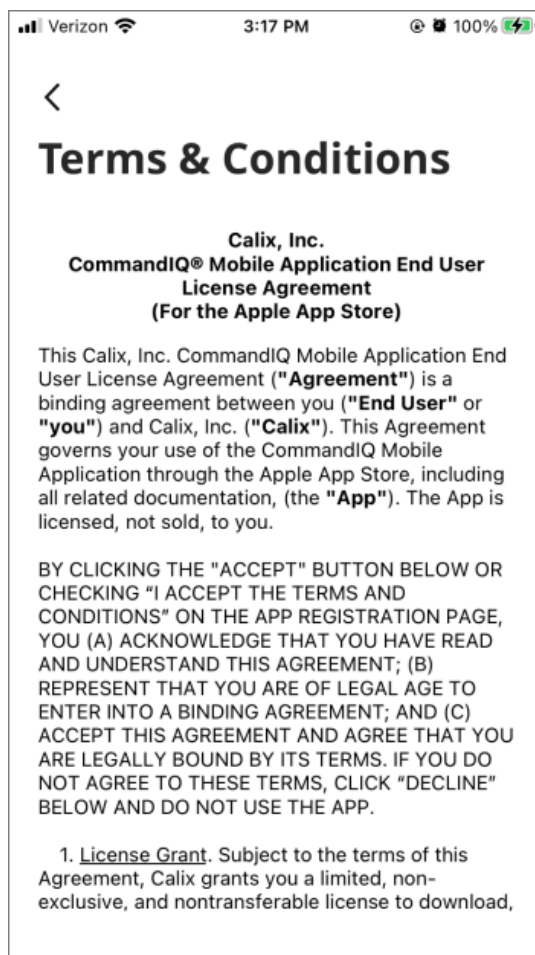
Terms and Conditions

The Terms and Conditions screen shows the developer's End User License Agreement (EULA) for using the CommandIQ app.

If you did not read the Terms and Conditions presented on the user setup screen during initial app setup, you can review those terms at any time from this screen.

To view the app's Terms and Conditions

1. Navigate to **Settings > Terms & Conditions**.
2. Tap the < (back) icon at the top of the screen to return to the Settings menu.

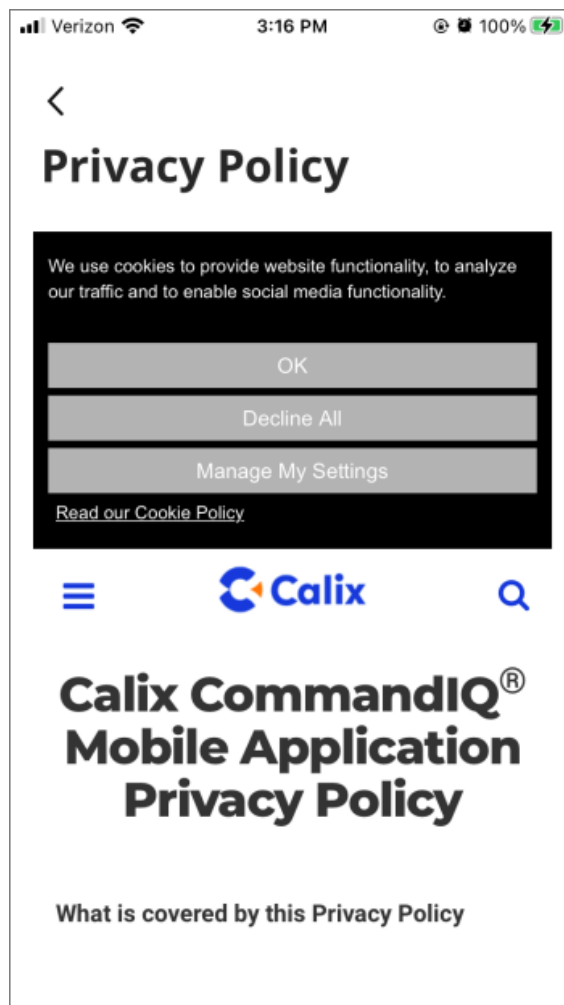


Privacy Policy

The Calix Privacy Policy is available for viewing and printing from the CommandIQ app.

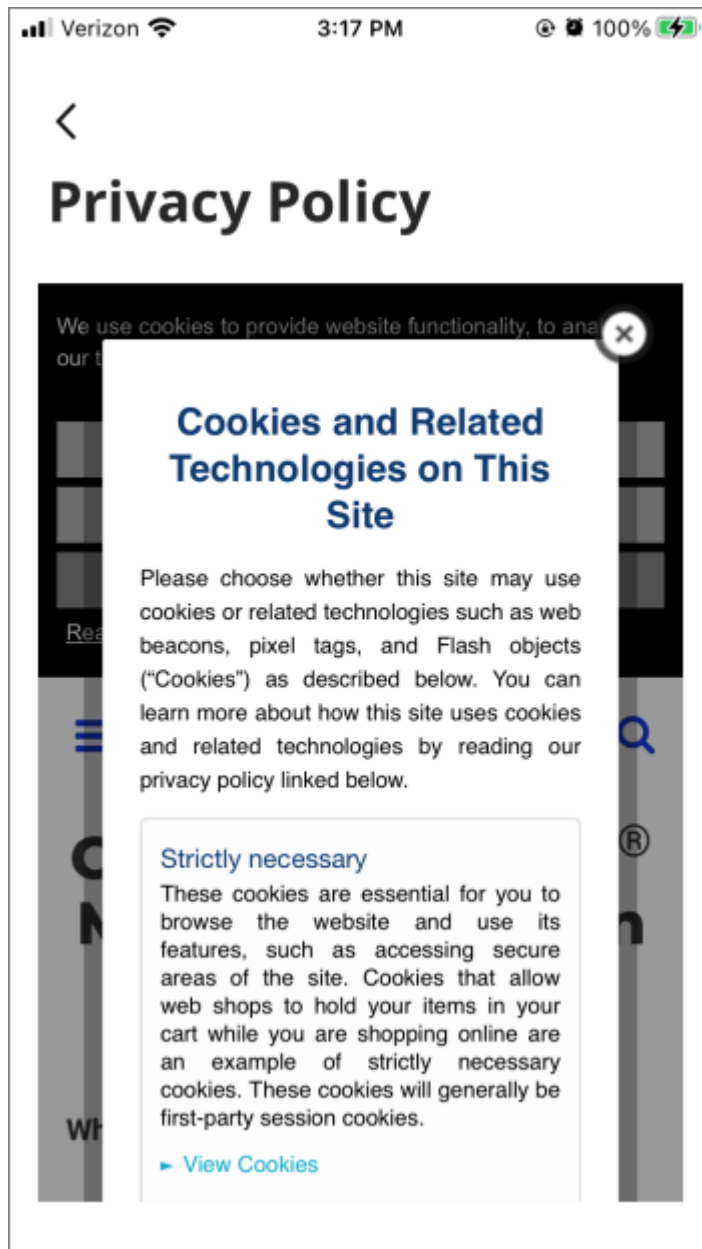
To view the Calix Privacy Policy

1. Navigate to **Settings > Privacy Policy**.
2. A dialogue box is displayed asking you to agree with the Calix cookies policy.
3. Tap **OK** or **Manage My Settings** to view the policy in its entirety.
4. If choosing **Manage My Settings**, a new dialogue box is displayed showing how cookies are managed on this site
5. Tap the **Done** button to return to the dashboard.



6. A brief summary of how cookies are handled in CommandIQ.
7. If you agree, tap **Agree and Proceed**.

8. Tap **View Cookie Settings** to make further changes.

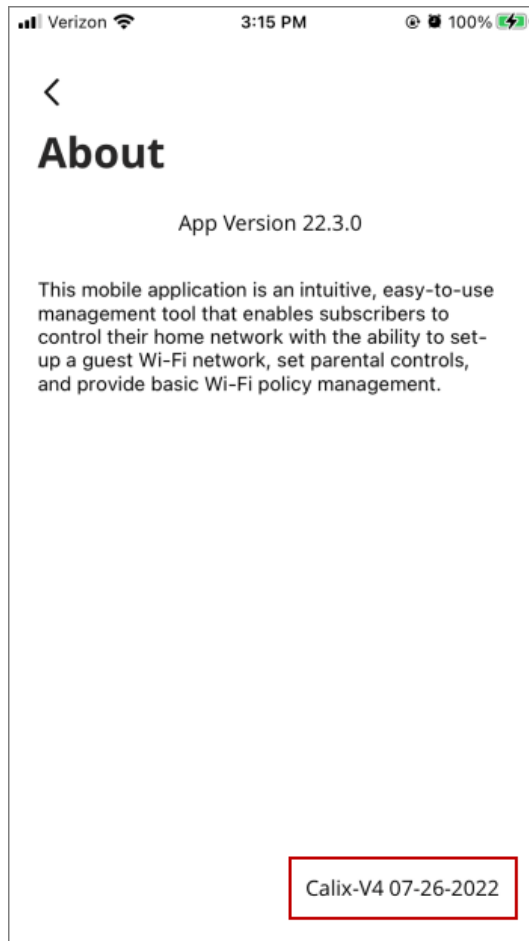


About

The About screen shows the developer's description of the CommandIQ app.

To view the app's About information

1. Navigate to **Settings > About**.



2. Tap the *back arrow* icon to return to the Settings menu.

Important: CommandIQ auto-updates to the latest version when it becomes available on the appropriate app store.

Note: The most up-to-date ProtectIQ and ExperienceIQ components are tied directly to the EXOS firmware. To ensure that the latest features are available, EXOS systems should be running the most current firmware.