FAQ: CommandIQ

Last Updated: May 2024

Overview

This document provides answers to frequently asked questions about Command**IQ** and Command**IQ** services including Experience**IQ**, and Protect**I**Q.

Contents

Overview 1

Command**IQ** 3

- Where can I download the Command**IQ** app? 3
- What should my Wi-Fi name and password be? 3
- Are the Wi-Fi names (SSID) case sensitive? 3
- How do I check my app version? 3
- Do I need to upgrade my app? 3
- What languages does Command**IQ** support? 3
- What are the information icons I see on some screens within the app? 4
- Can I password protect the app? 4
- How do I add a new person to my network? 5
- What are Places? 6
- How do I create a Place? 6
- How do I add a new Thing (device)? 7
- How do I add a network device? 8
- How can I establish or set network priorities? 10
- How can I set up an additional wireless network, such as a guest network? 12
- How can I check my internet connection speeds or run a bandwidth test with Command**IQ**? 13
- I see three wireless network options (guest, work-from-home, and custom) when adding an additional wireless network. What are they and how do they differ? 14
- How do I rename a thing? 15
- How can I change my SSID settings with Command**IQ**? 16
- Can I turn off Wi-Fi access for a specific device? 16
- What is a dBm? 16
- How can I identify a device that just shows numbers and/or letters as the identifier? 16
- How do I enable or disable a service within Command**IQ**? 17
- How do I set up Alexa? 18

How do I view how devices are mapped in my network? 18
Protect**IQ** 19
How do I get started with Protect**IQ**? 19
What does the Additional Details section within Security settings tell me? 20
What happens when I get a security notification? Should I be worried? 21
What does a security alert tell me? 21
What is the Trusted List in Protect**IQ**? 21
In Protect**IQ**, what are Intrusion Settings? 21
My device appears to be working normally, but I keep seeing a security alert. What do I do? 22
Experience**IQ** 22
How do I get started with Experience**IQ**? 22
What's next after I enable Experience**IQ**? 23
How do I set time network limits? 23
How do I restrict access to specific content, applications, and websites? 26
What are the options to filter content? 27
How can I view device usage from a person's profile? 26
I accidentally put my phone into a parental control profile and turned it off, now I cannot turn it back on. What should I do? 28
What are VPN detection alerts? 28

CommandIQ

Where can I download the CommandIQ app?

Download the Command**IQ** app from either the Google Play store or Apple App Store. Search for Command**IQ** to find the correct app.

What should my Wi-Fi name and password be?

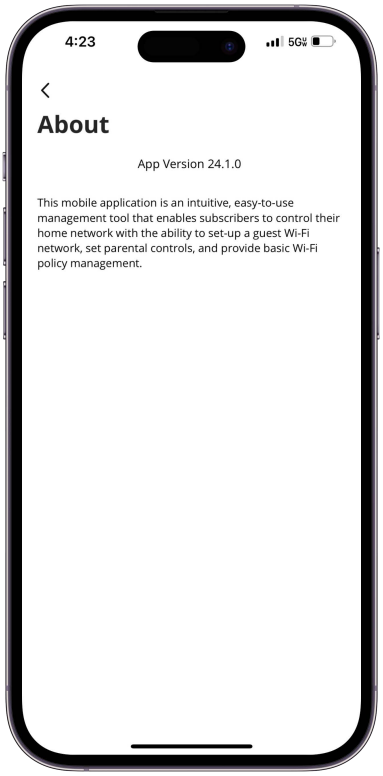
Your Wi-Fi (SSID) name should be something unique and that you remember. You will likely not want to change your Wi-Fi name and password often as you would have to reconnect all the devices in your home after changing the name.

Are the Wi-Fi names (SSID) case sensitive?

Yes, Wi-Fi SSID names are case sensitive.

How do I check my app version?

Tap **Settings**, then tap **About**. The app version displays in the bottom-right corner of the screen.



Do I need to upgrade my app?

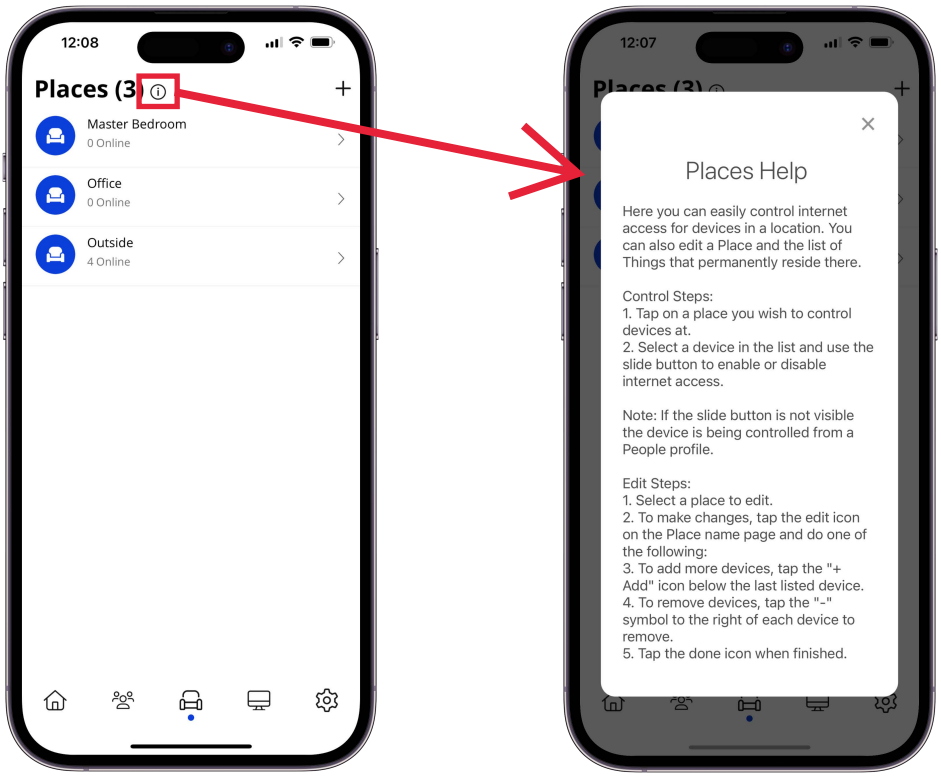
If you have automatic app updates set on your device, the app will automatically pull in any new versions. If you do not have this set up, you can manually check for an update. Or finally, you can uninstall the current app, find it in the app store, and install the newest version.

What languages does CommandIQ™ support?

Command**IQ** support English (default), French Canadian, German, and Spanish. To change the language, go to **Settings > Language** and select your desired language.

What are the information icons I see on some screens within the app?

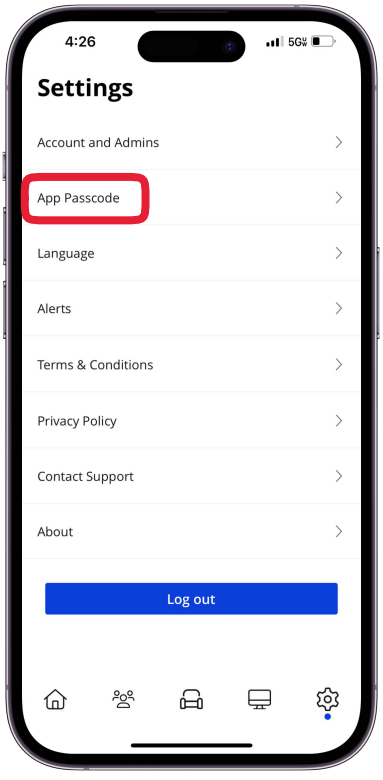
Specific screens within the app feature information ⓘ icons. Tap the icon when you need a basic description or assistance to understand an app feature within the respective screen panel.



Can I password protect the app?

Yes, you set a PIN that must be entered any time you launch the app. The PIN must contain at least 4 characters. After you configure a PIN, it can be enabled or disabled from the **Settings** menu.

To set a passcode, go to **Settings > App Passcode**. See the Set Passcode Help article for more information.

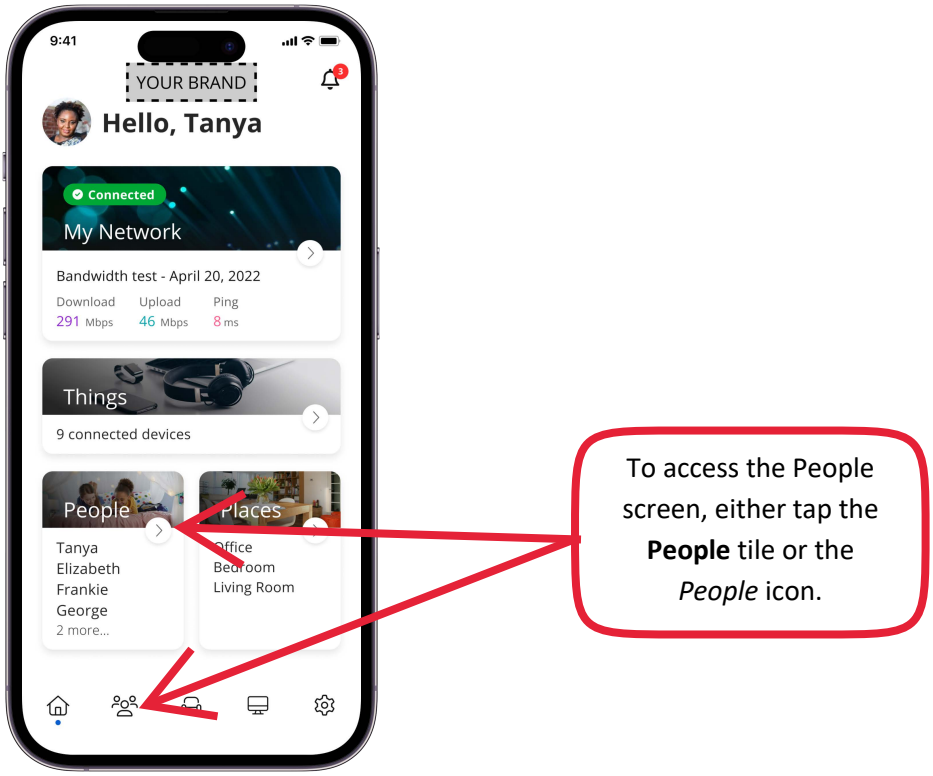


How do I add a new person to my network?

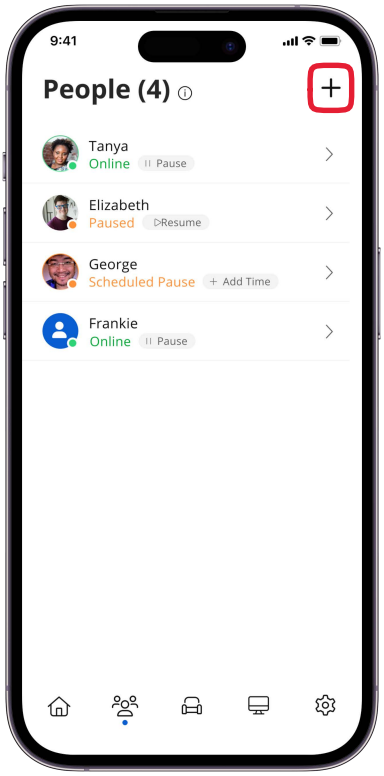
You can add people from the **People** screen.

To access the **People** screen, you can either:

- Tap the **People** tile on the Home screen.
  OR
- Tap the *People* icon in the bottom menu bar.

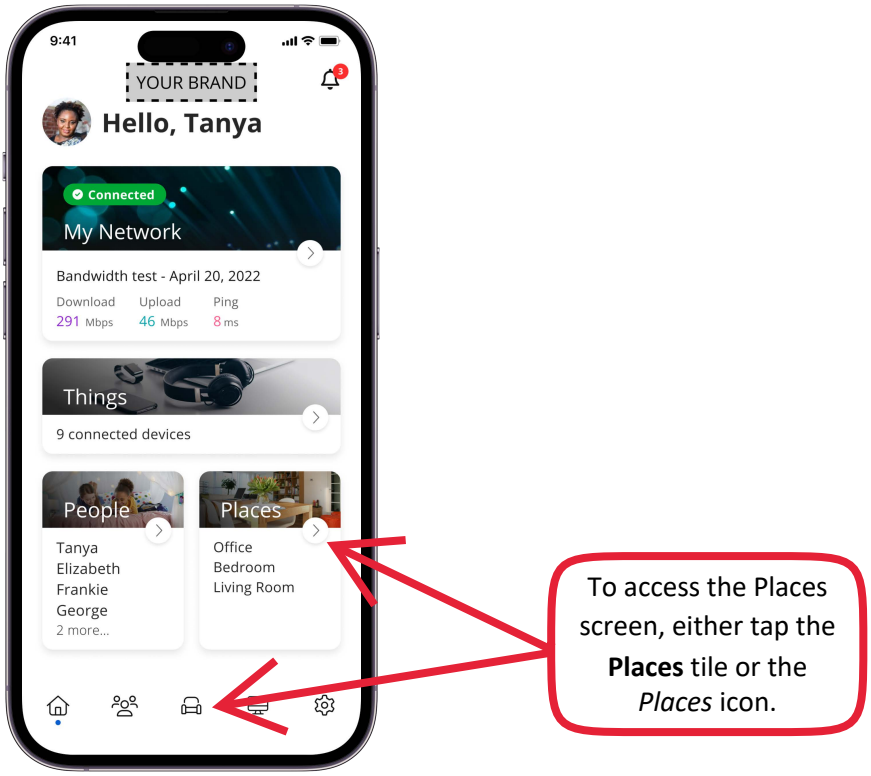


Once on the People screen, tap the plus sign in the upper-right corner to add a person. See the Add People Help article for more information.



What is Places?

Places allow you to assign a group of devices to specific locations within your home. For example, you might have a home office where you want to assign your laptop, printer, or other office equipment. Your gaming devices or home fitness equipment (e.g., Peloton) might be assigned to another place. Your outdoor security cameras might be assigned to a place you name “Outdoors”.

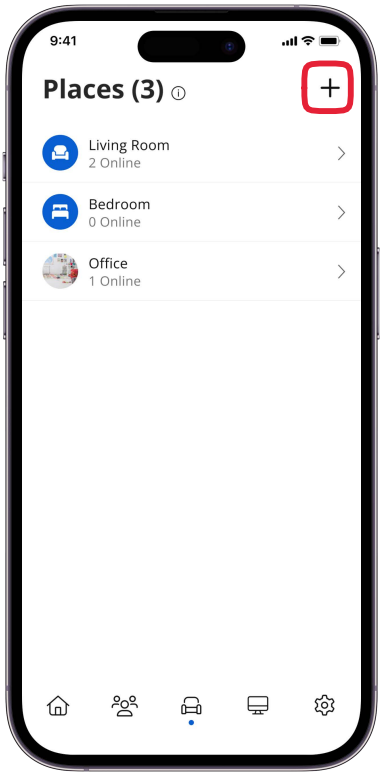


How do I create a Place?

You can add places from the **Places** screen.

To access the **Places** screen, you can either:

- Tap the **Places** tile on the Home screen.
  OR
- Tap the *Places* icon in the bottom menu bar.



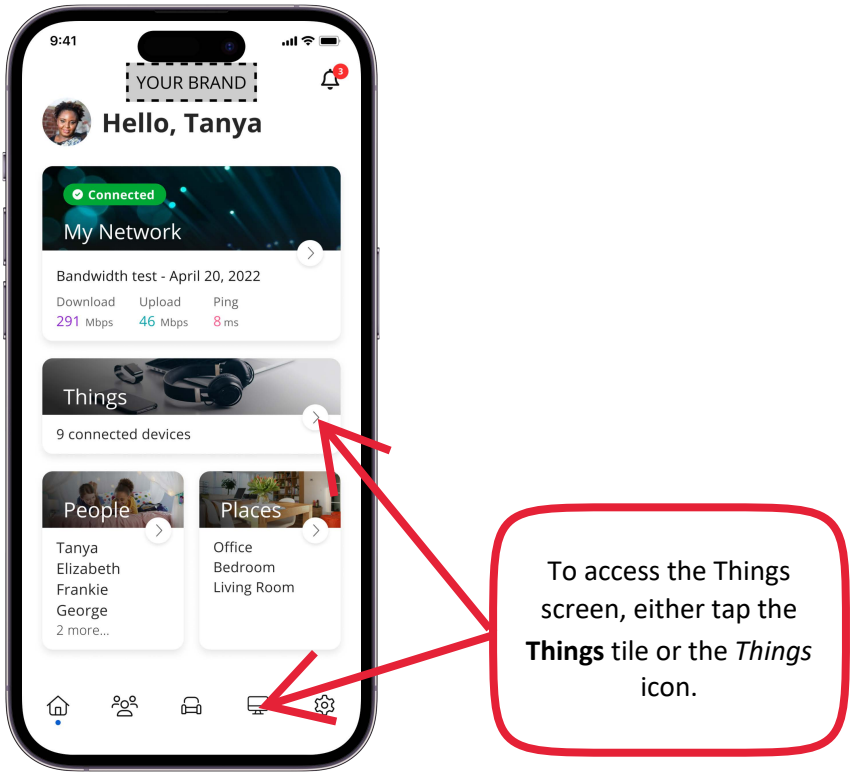
Once on the **Places** screen, tap the *plus sign* in the upper-right corner to add a place. See the Add Places Help article for more information.

How do I add a new Things/devices?

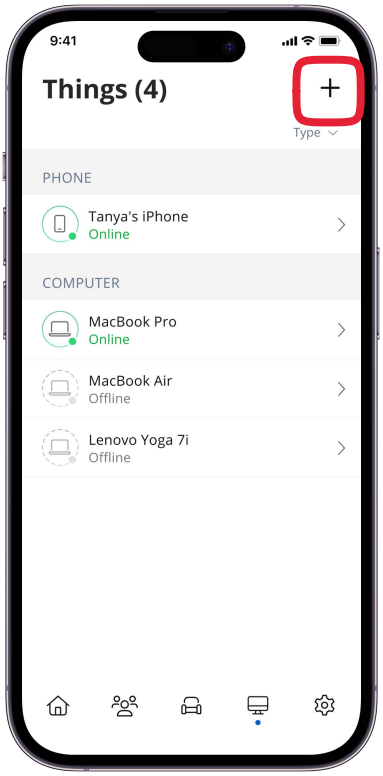
In Command**IQ**, devices are referred to as Things. You can add things from the **Things** screen.

To access the **Things** screen, you can either:

- Tap the **Things** tile on the Home screen.
  OR
- Tap the *Things* icon in the bottom menu bar.



Once on the **Things** screen, tap the *plus sign* in the upper-right corner to add a thing. See the Add Things Help article for more information.

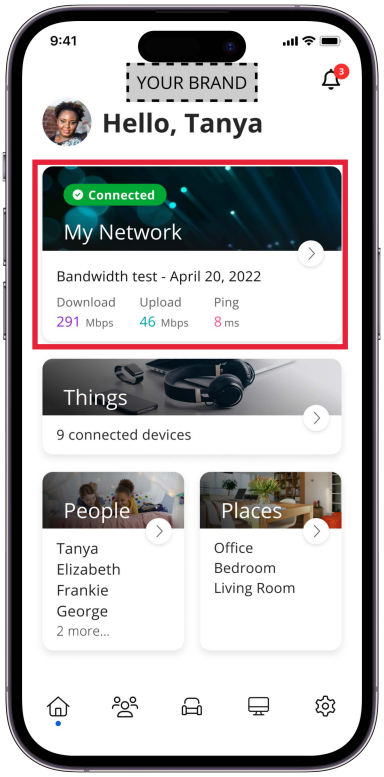


How do I add a network device?

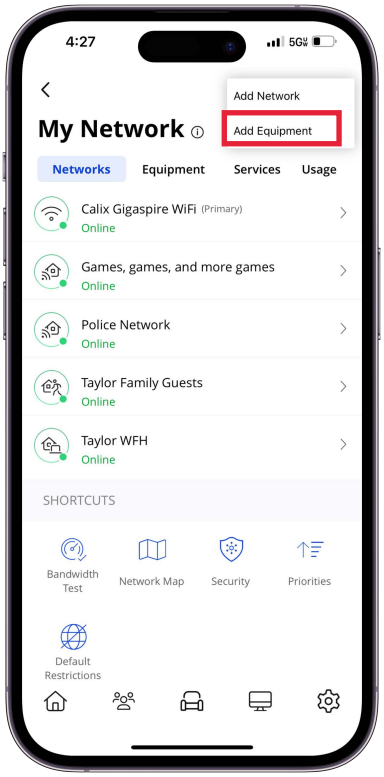
After you complete your initial router onboarding, you can add additional mesh systems.

To add a mesh system:

1. From the **Home** screen, tap on the **My Network** tile.



2. Click the *plus sign* in the upper-right corner of the screen and select **Add Equipment**.



3. Continue to onboard the mesh system.

See the Add Equipment Help article for more information.

How do I assign things to person or a place?

There are two ways to assign a connected device to a person or a place:

- **From a person or a place**:
  a) Go to either the **People** or the **Places** screen.
  b) Tap on the desired person or place, then tap the *pencil* icon.
  c) Tap **Edit**
  d) Tap "**+ Add**" and add Thing(s).
- **From the thing**:
  a) Go to the **Things** screen.
  b) Tap on the desired thing.
  c) Tap the *pencil* icon.
  d) Select the desired person or place.

See the Edit/Delete People and Edit/Delete Places Help topics for more information.

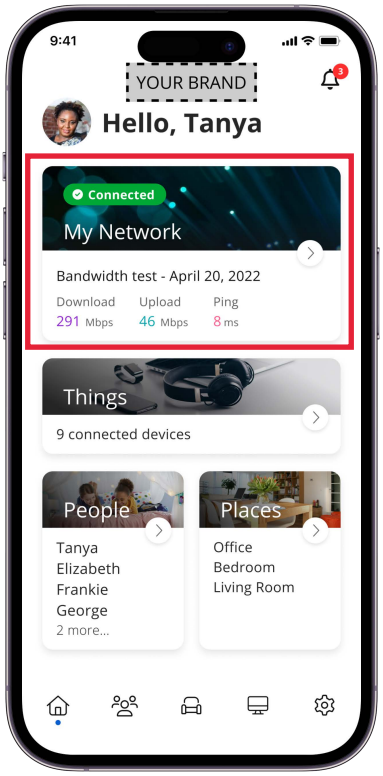
Note: One thing to keep in mind is that you should not add the device with the Command**IQ** app (i.e. the admin's mobile phone that manages Command**IQ**) to a profile. In doing so, it is possible to inadvertently cut off your own access to these controls. Should this occur, switch to mobile data to restart the profile that contains your app device.

How can I establish or set network priorities?

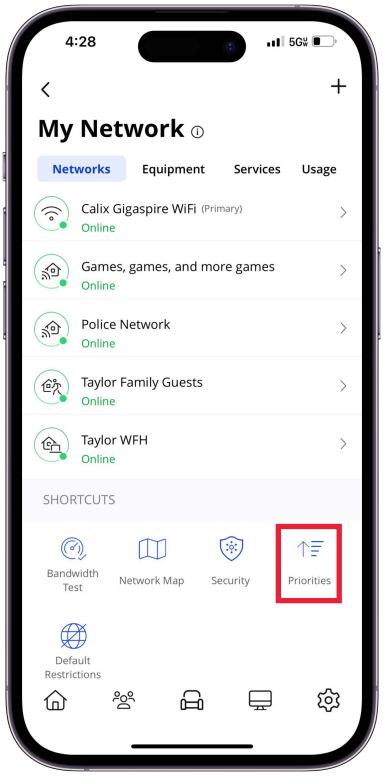
You can prioritize traffic and devices on your network. This feature is very useful, for example, when you want to prioritize traffic to your work devices versus your gaming devices during your normal work hours or if you want to prioritize traffic to music and videos during the weekend.

To set priorities:

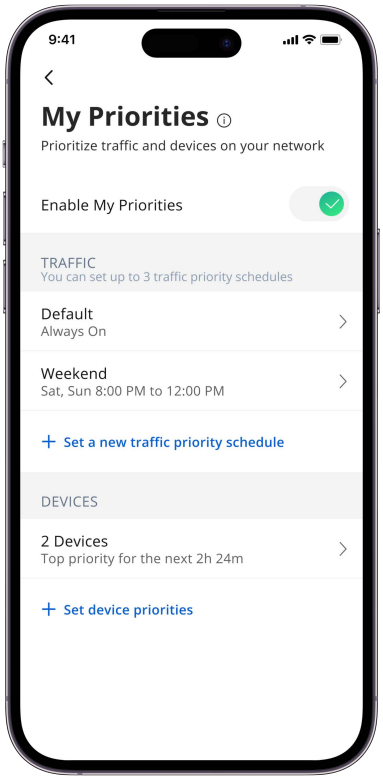
1. Tap **My Network** from the Home screen.



2. Tap **Priorities**.



3. Continue to edit or set Traffic and Device priorities as desired.



A default priority is set, which you can edit.

In total, you can set up to three traffic priority schedules. The app allows you to name your traffic priority and set a time schedule.

You can also set device priorities, assigning up to five devices on a priority schedule.

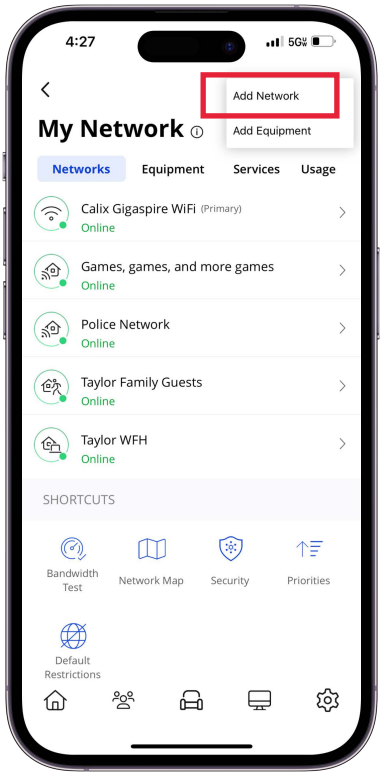
See the My Priorities Help topics for more information.

How can I set up an additional wireless network, such as a guest network?

To add a network:

How can I set up an additional wireless network, such as a guest network?
To add a network:

1. From the **Home** screen, tap on the **My Network** tile.
2. Tap the *plus sign* in the upper-right corner and select **Add Network**.



3. Select the **Wireless Network Type**:
    - Guest
    - Work From Home
    - Customer
4. Enter a **Network Name (SSID)**. This is the name you and your guests will see when attempting to connect from a device.
5. It's highly recommended that you select a security type to protect your network.
6. **For guest networks**, you can optionally set a start and end time. If family is visiting for the weekend, set the network for the time they'll be in your home. If you have guests coming over for a party, set your network only during the time of the party so it automatically shuts off at the desired time. If you toggle the on button for Endless, your guest SSID will broadcast indefinitely, until you manually delete or edit the network.
7. **For custom networks**, you have the option of selecting the band type. The options are All Bands, 2.4G, 5G, and 6G (if supported by device hardware). This is ideal for when you want to assign devices of a certain band to its own custom network.
8. For both guest and custom networks, you can also select if you want devices added to either network to be isolated from other devices within your overall network.
9. After you configure your settings, you'll be given the option to send a text notification to your guest if they are stored as a contact in your mobile device. The notification will presents users with the wireless network information.

See the Add A Network Help topic for more information.

I see three wireless network options (guest, work-from-home, and custom) when adding an additional wireless network. What are they and how do they differ?

In additional to your primary network, you can create multiple secondary wireless networks that run simultaneously.

A **guest network** is an isolated network that you can create when you want to provide visitors in your home or business Wi-Fi access. The devices that your guests add to your guest network are isolated from your connected devices. You can create a time schedule for the guest network, which is ideal when you want to provide visitors access to your network for a limited time.

A **work-from-home network** is another isolated network where you can assign devices (e.g., your work laptop, printer) that require network prioritization. Devices added to this network are classified as “top devices” in the home and will receive bandwidth priority over other devices within your overall home network.

You can create a **custom network** when you want more flexibility and want to create a network where isolation and prioritization are optional. In addition, you can choose the band type you want to assign to the custom network. The options are All Bands, 2.4G, 5G, and 6G (if supported by device hardware).

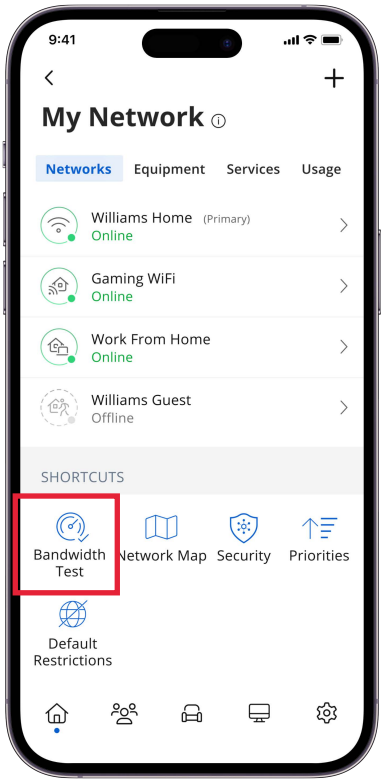
See the Add a Network Help topic for more information.

How can I check my internet connection speeds or run a bandwidth test with CommandIQ?

With a GigaSpire, you can initiate a speed test directly from the Command**IQ** app to test the speed from your GigaSpire to the internet.

To run a speed test:

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



3. Tap **Run Test**. After the speed test completes, the results appear in the My Network tile on the Home screen. You'll also see a new notification. Tap the Notification icon to review the speed test results.

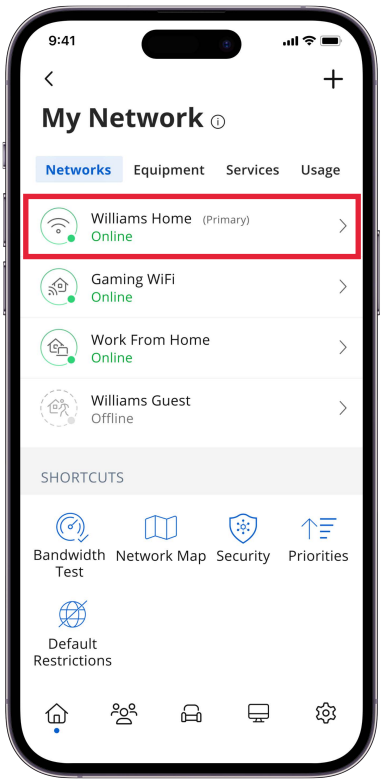
Note: GigaSpire satellites run bandwidth tests between themselves and the primary GigaSpire system (acting as the residential gateway). You may notice that the rates between the primary system and the satellite(s) are higher than your subscription rate.

See the Bandwidth Test Help article for more information.

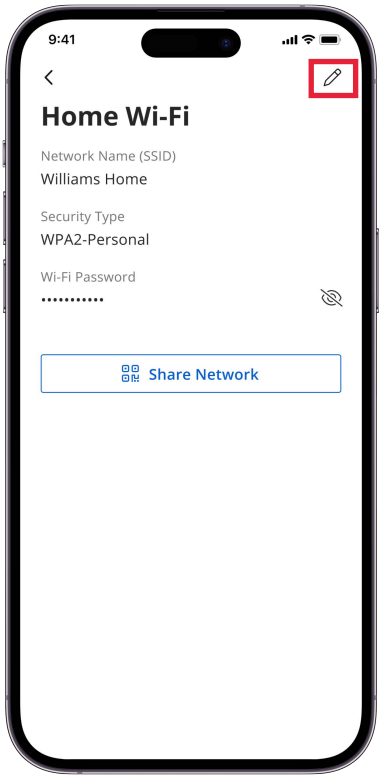
How can I change my SSID settings with CommandIQ?

To edit your network's SSID settings:

1. From the **Home** screen, tap on the **My Network** tile.
2. Tap on your primary network.



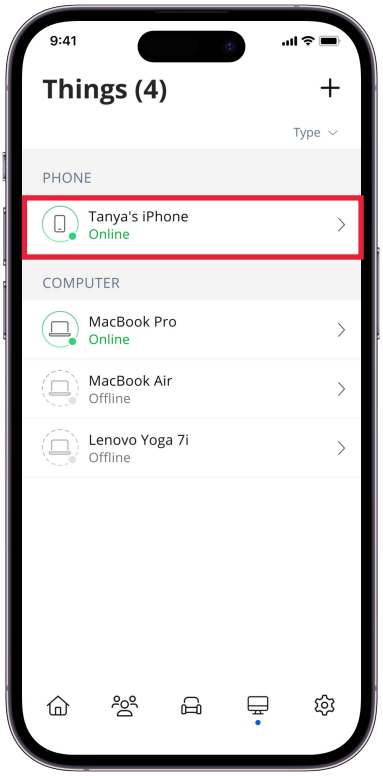
3. Tap the Edit.
4. Edit your network SSID, password, and security type as desired.
5. Tap **Save** when finished.



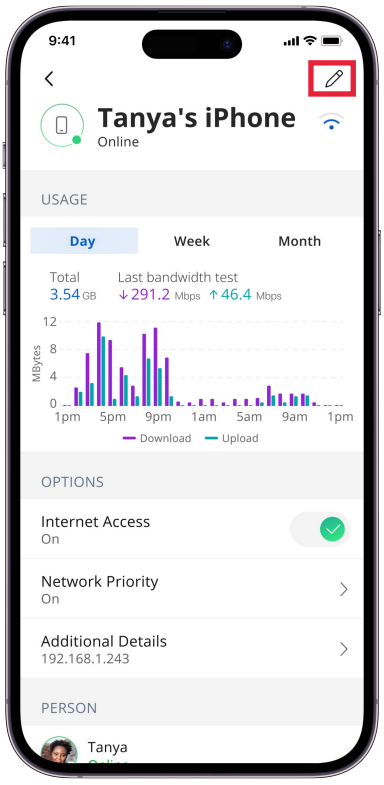
How do I rename a thing?

It's easy to rename a connected device on your network:

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

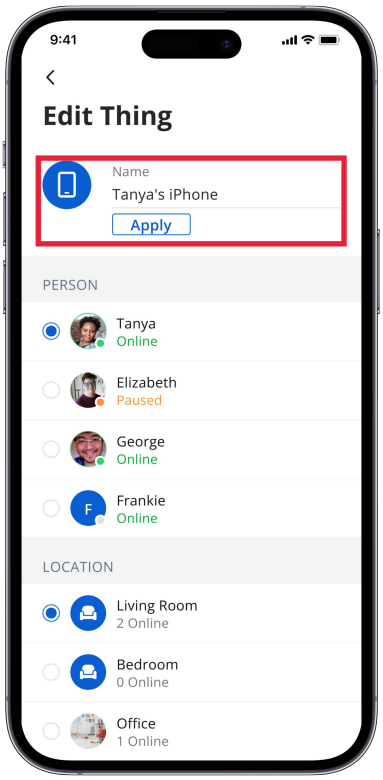


3. Tap the *Edit* icon.



4. Edit the thing **Name** and tap **Apply**.

From this screen, you can also assign the device to a person or a place within your home.



See the Edit Things Help topic for more information.

Can I turn off Wi-Fi access for a specific device?

Yes, you can disable Wi-Fi access for a specific device on your network.

To disable network access for a thing:

1. Go to the **Things** screen.
2. Tap on the desired thing.
3. Toggle the **Internet Access** toggle to Off (toggle is gray).

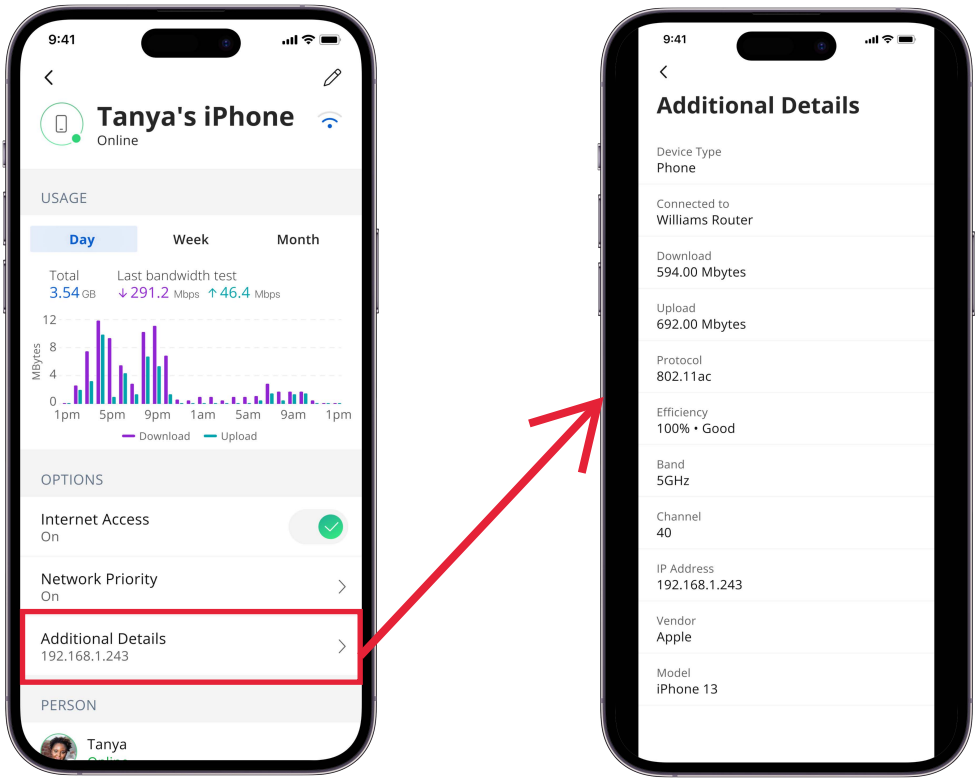
What is a dBm?

This stands for decibel-milliwatts. It is a measure of how strong your signal strength is to a specific device. A general range is that -50 to -70dBm is considered strong, while anything over -100 would be weak. However, this also depends on the capabilities of the device, so you may have a weak signal indicated and have absolutely no problem using your device.

How can I identify a device that just shows numbers and/or letters as the identifier?

You may see entries in your Things that consist of a string of numbers and/or letters. This may happen for devices that do not send identifying information to the GigaSpire when they join the network. Typically, the string of numbers and/or letters displayed in the Command**IQ** app is the hardware address (also known as the MAC address of the device. The MAC address is typically found on a sticker on the device or, if the device has a management interface, somewhere in the network settings.

To properly identify the device, compare the device MAC address to the string of numbers/letters listed in the Command**IQ** app. To locate the MAC address in Command**IQ**, go to **Things**, select the device, then tap **Additional Details**.

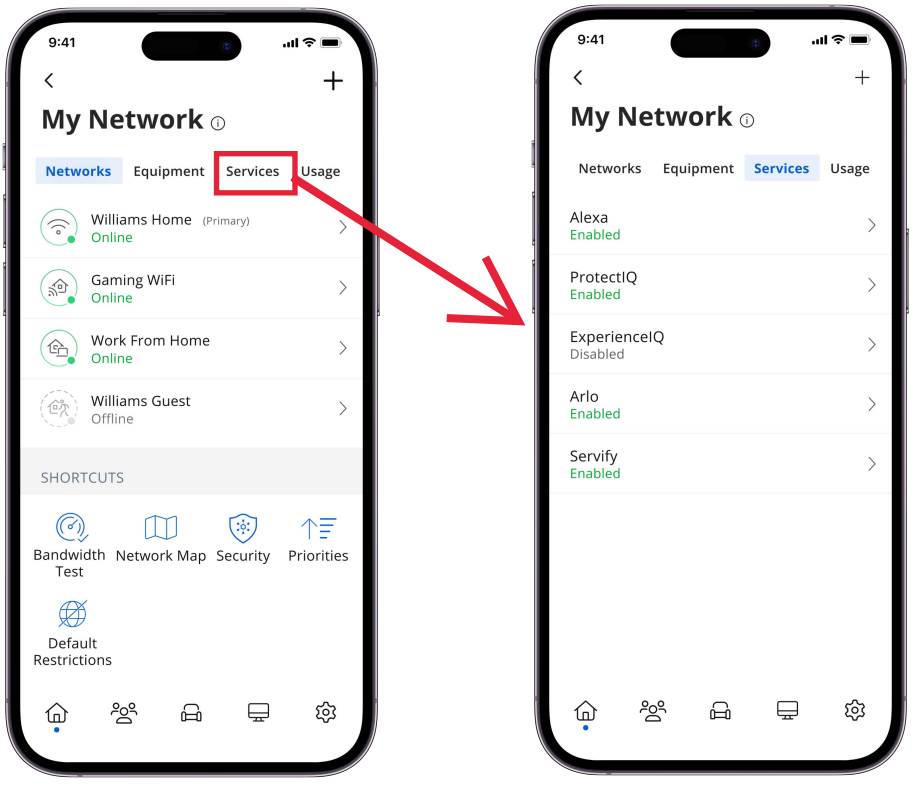


How do I enable or disable a service within CommandIQ?

Part of managing your network involves being able to enable and disable added value services (ProtectIQ, ExperienceIQ, etc.).

To disable services:

1. From the **Home** screen, tap on the **My Network** tile.
2. Tap on the **Services** tab, then tap on the desired service.



3. Tap on the toggle to turn the service on (green toggle) or off (gray toggle).

How do I set up Alexa?

Part of the joy of having a connected home is being able to control things with just the sound of your voice. And thankfully, the GigaSpire BLAST systems connect with Amazon Alexa. And setting it up is a simple process. Let's get started.

To begin, you will need to go into your Alexa app, in the main menu from the top left, select Skills & Games. Search for and enable the Calix Smart Router skill.

After the skill is enabled, you'll be able to say things like:

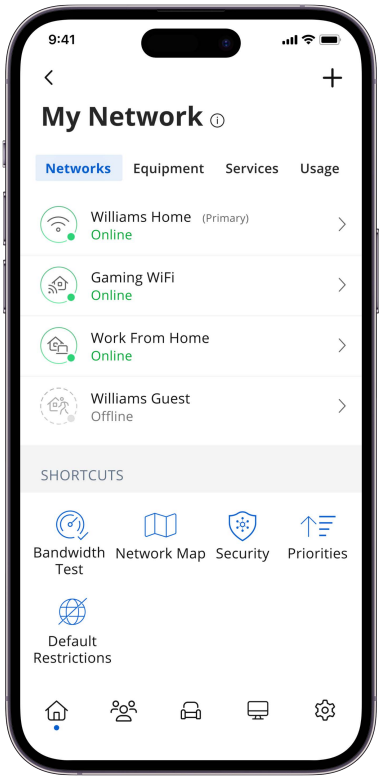
"Alexa, ask my router what device is using the most bandwidth on my network?"

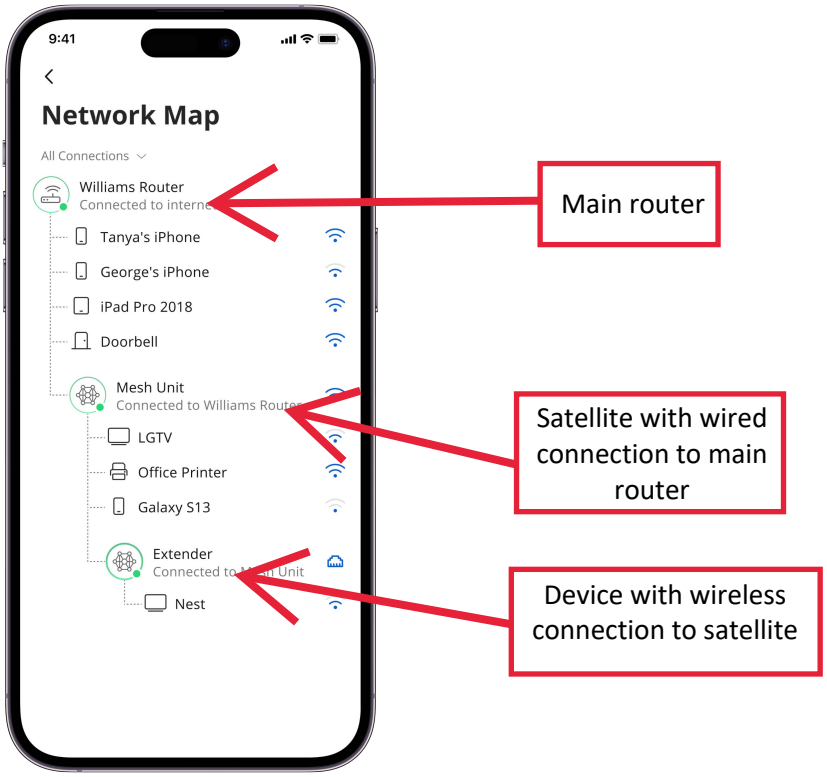
OR

"Alexa, ask my router for the results of my last speed test".

How do I view how devices are mapped in my network?

To view a map of the connected devices in your network, go to **My Network > Network Map**. A map displays showing the connected devices in your network along with the router and satellite devices (if applicable) they are currently connected to. The Map also gives insight into how your mesh satellite devices are connected within the network.





If a red indicator light appears besides a device in the Network Map, that device may have lost connection with the GigaSpire. Check the following items:

- Is the satellite powered on?
- For satellites with a wired connection to the GigaSpire, check the physical connections.
- For satellites with a wireless connection to the GigaSpire, try rebooting by removing power, waiting 10 seconds, and restoring power.
    - If a power reset did not work, go through the pairing process again.

See the Network Map Help article for more information.

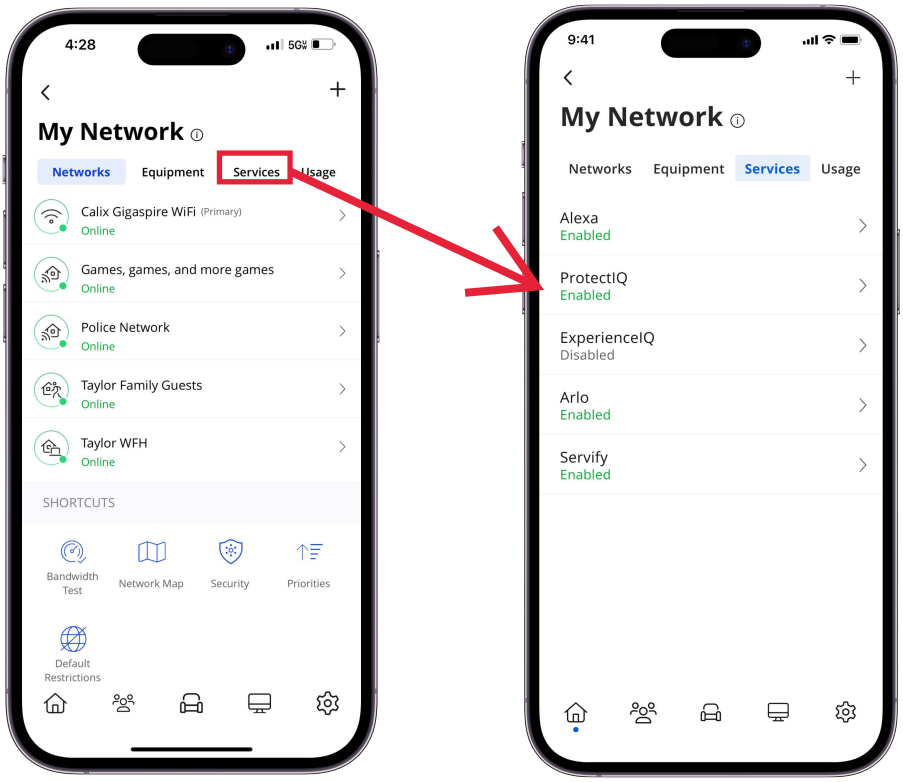
ProtectIQ

How do I get started with ProtectIQ?

ProtectIQ delivers home network protection to give you peace of mind. It detects intrusions, protects against malicious websites, monitors network traffic, and proactively blocks suspicious activity, and more.

To enable ProtectIQ:

1. Tap on **My Network** from the **Home** screen.
2. Tap on the **Services** tab, then tap on ProtectIQ.



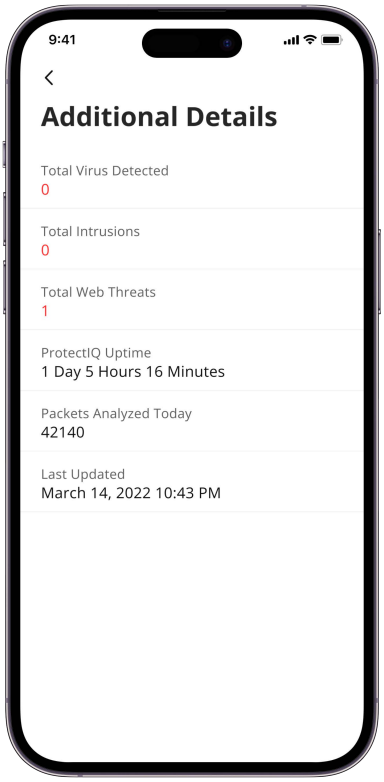
3. Tap on the toggle to turn ProtectIQ on (green toggle) or off (gray toggle).

See the ProtectIQ Help article for more information.

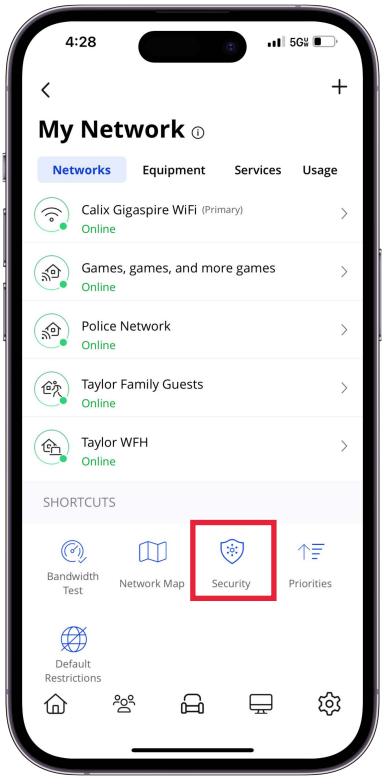
Note: You may need to verify that your service provider has enabled access to ProtectIQ. Please contact your service provider for more information.

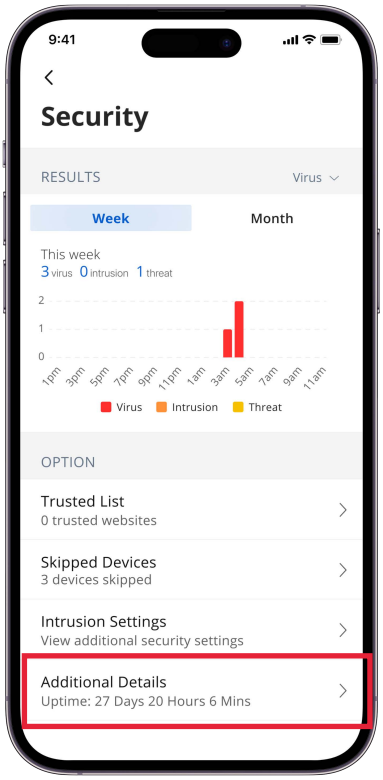
What does the Additional Details section within Security settings tell me?

The **Additional Details** section tells you how long the Protect**IQ** has been turned on (enabled in your network), when it was last updated, and how many packets of data have been scanned for the current day. You will also see the total number of viruses, intrusions, and web threats that have been blocked by Protect**IQ**.



To see Additional Details, go to **My Network > Security > Additional Details**.





See the Additional Details Help article for more information.

What happens when I get a security notification? Should I be worried?

Each time ProtectIQ detects a threat, you will receive a notification with details about the content that was blocked. All threats are automatically blocked, so you do not need to do anything. However, if you want to view more information about the specific threat, this information will include the time the threat happened, what type of threat it was, the source IP from where it came, what action was taken, which device the threat was trying to get to and the URL. You do not need to do anything; all threats are automatically blocked.

For more information, see the ProtectIQ Alerts Help article.

What does a security alert tell me?

Security alerts include the following information:

- The protocol type that was blocked
- The time the threat occurred
- The Source IP Address of the threat
- What action was taken
- The device in your home that was targeted by the threat
- The threat's source URL

It is possible for the device to appear to be working with no issues, while the threat may be running in the background of the page, or within a page ad. A blocked threat may appear as a webpage failing to load if a threat is detected on that page. All threats are blocked automatically; you do not need to take any action to remain protected.

What is the Trusted List in ProtectIQ?

When a security threat occurs, you have the option to add it to a Trusted List if you know the content is not harmful. This should not be an action taken with frequency. After you add an identified threat to the Trusted List, it no longer blocks that threat for any devices on your home network. At any time, you can enter the Trusted List to remove items from this list and revert to blocking them.

See the Trusted List Help article for more information.

In ProtectctIQ, what are Intrusion Settings?

The Intrusion Prevention System settings are editable to your preference. Select these boxes to turn on the following features:

- IPS Protocol Anomaly: Looks for unusual patterns and uses of a given data communication protocol as an indicator of potential malicious behavior and blocks that specific traffic.
- IPS Port-Scan-Defense: Senses external malicious actors scanning the system for open ports to exploit. This defense monitors for IP addresses hitting the system and scanning all ports that could be used as an exploit. When this type of activity is detected, it blocks the IP address from communicating with that IP address ever again.

See the Intrusion Prevention System (IPS) Settings Help article for more information.

There may be specific devices within your home that you do not want scanned for security threats. All devices connected to the network are scanned by default. If you want to prevent specific devices from being scanned, you can use this feature to "skip" specific devices. Please note that if you skip devices, these devices could act as a point of vulnerability and introduce security threats into your home.

My device appears to be working normally, but I keep seeing a security alert. What do I do?

First, make sure your device is updated to the latest available software. Protect**IQ** may be detecting a vulnerability in the software on your device. If you are still seeing notifications with the latest available software, report any issues to your service provider so they can escalate the issue. In the meantime, if you do not want to see the notifications, you can Skip that device.

ExperienceIQ

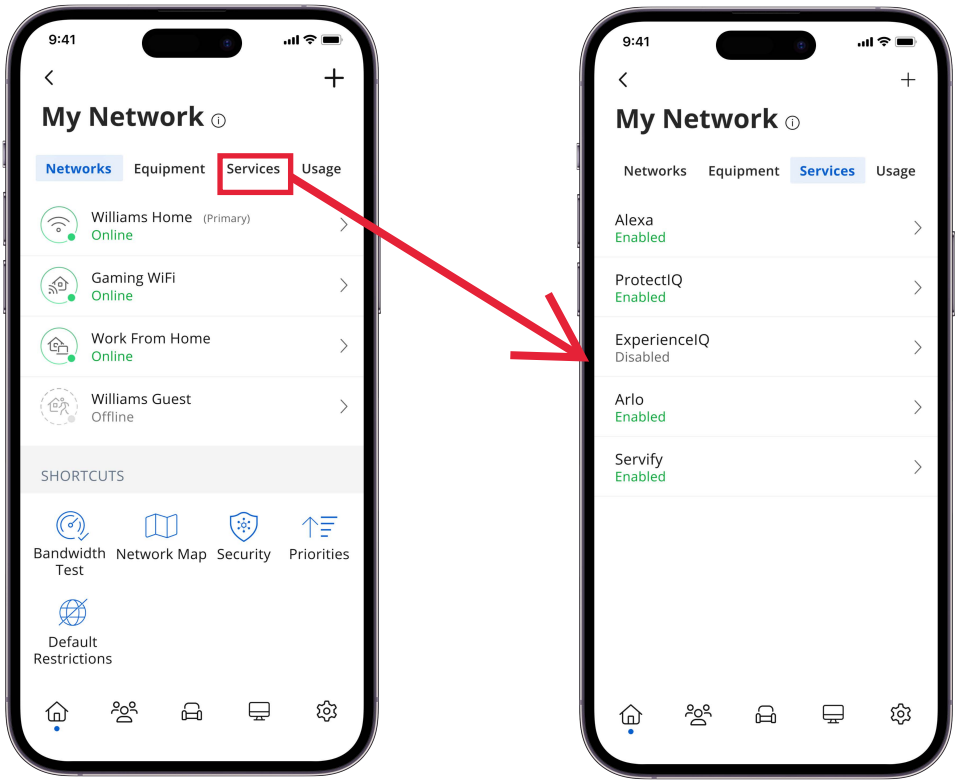
How do I get started with ExperienceIQ?

Setting up Experience**IQ** gives you the ability to monitor and establish parameters for internet access profiles and assign devices for basic on/off control. With Experience**IQ** you have access to enhanced parental controls and the ability to set additional restrictions.

Once you have created your household profiles, you can select the profile(s) that require parental controls.

To enable Protect**IQ**:

1. Tap on **My Network** from the **Home** screen.
2. Tap on the **Services** tab, then tap on Experience**IQ**.



3. Tap on the toggle to turn Experience**IQ** on (green toggle) or off (gray toggle).

See the ExperienceIQ Help topic for more information.

Note: You may need to verify that your service provider has enabled access to Experience**IQ**. Please contact your service provider for more information.

What's next after I enable ExperienceIQ?

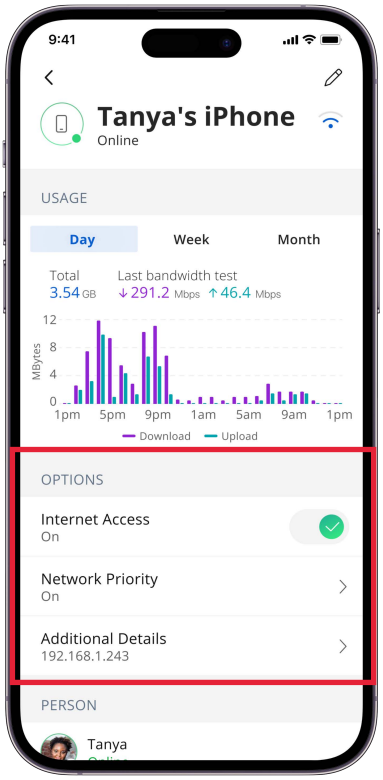
After you enable Experience**IQ**, you can set restriction for your users. For example, you can set network restrictions for your children.

1. Go the **People** screen.
2. Tap on the desired person.

From the person's profile, you can view a chart that lists the top applications accessed by that person. You can view data for the Day, Week, or Month.

Below the chart is the Options section that allows you to perform the following actions:

- Turn on/off internet access
- Set time limits
- Set more advanced content restrictions (requires access to Experience**IQ**)

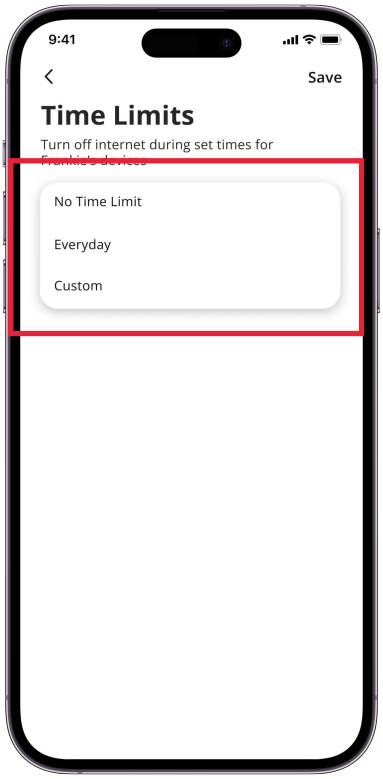


See the Parental Control Profiles and Parental Control Settings Help topics for more information.

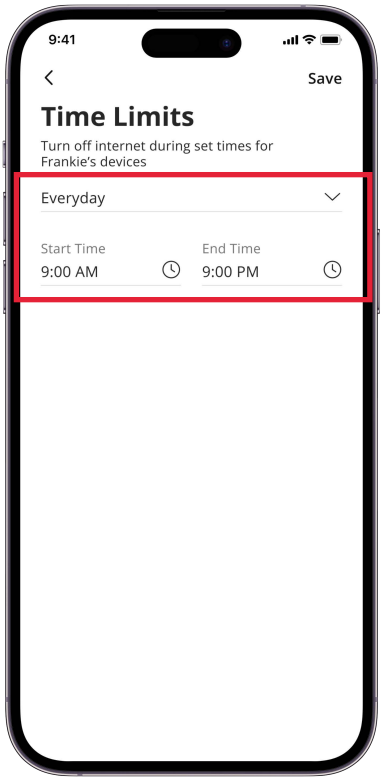
How do I set time network limits?

To set network time limits for a person:

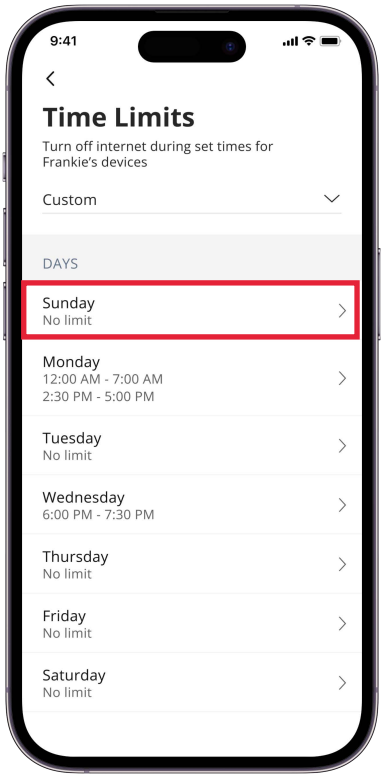
1. Go to the **People** screen.
2. Tap on the desired person.
3. Tap **Time Limits**.
4. Select a time limit option:

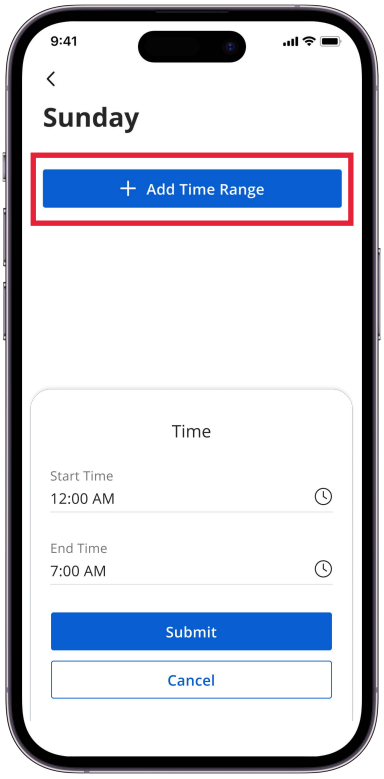


- None (Default)
- Everyday: Applies the same time limit to each day of the week (Sunday through Saturday). Set the **Start Time** and the **End Time**.



- Custom: Allows you to define a different time limit for each day of the week. Select the day(s) on which you would like to impose time limits. Tap **+ Add Time Range**. Set the **Start Time** and the **End Time**, then tap **Submit**.





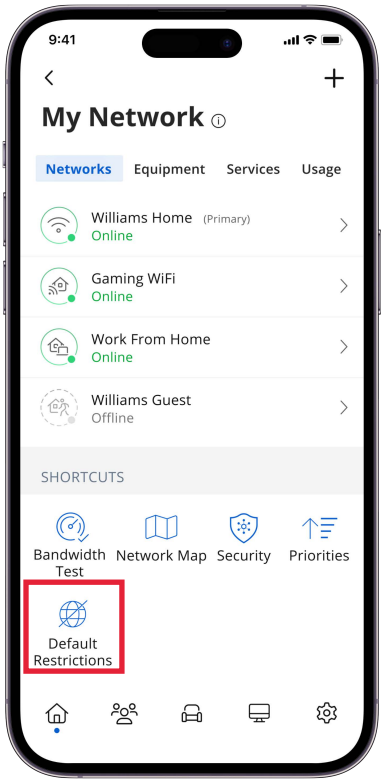
5. Tap **Save**. The person will only have network access during the set times. A device trying to connect during days/times where access is blocked may behave as if it does not have an internet connection or display an error, depending on the individual device or browser.

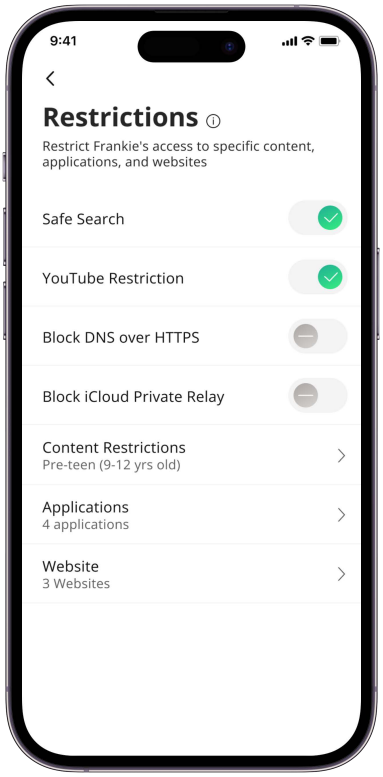
See the Parental Control Profiles Help article for more information.

Note: When setting filters and time limits, it may take a few minutes to become active and apply those settings to active device connections.

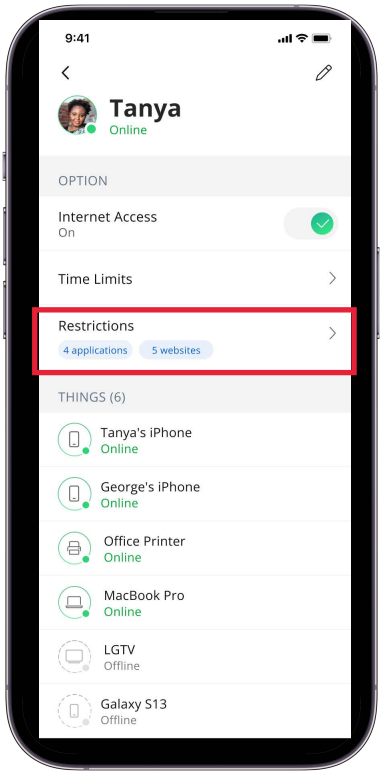
How do I restrict access to specific content, applications, and websites?

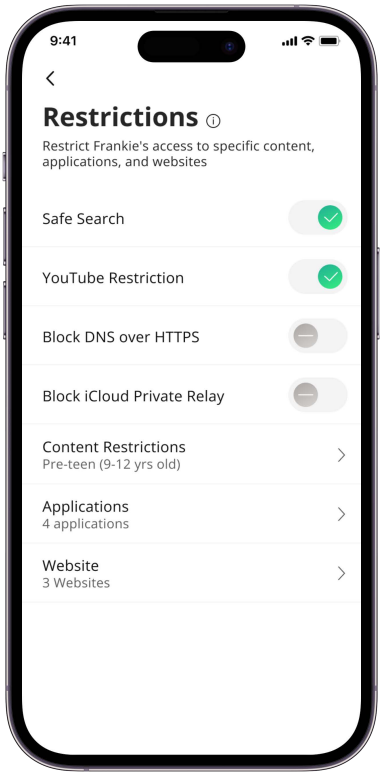
You can set restrictions globally from the **My Network > Default Restrictions** screen.





You can also set restrictions for an individual person from the person's profile. To set restrictions for a person, go to the **People** screen, tap on the person, then tap **Restrictions**.





From the **Restrictions** screen, you can configure Safe Search, content, application, and website restrictions.

See the Parental Control Settings Help article for more information.

Note: You will NOT receive a notification for every type of content that is blocked as it could result in constant notifications to your phone.

What are the options to filter content?

With Experience**IQ**, you can select content and application filters. This feature blocks devices from seeing data from specified categories, applications, and websites.

Experience**IQ** also allows you to permit specific content that might have otherwise been blocked by a category filter. For example, you could block the category Social network, then add facebook.com to the website filter and set it to allow access specifically to Facebook.

The following restriction options are available:

- Safe Search (Google and Bing)
- YouTube Restriction
- Block DNS over HTTPS
- Block iCloud Public Relay
- **Content Restrictions** prevent users from accessing entire sections of the internet, such as pornographic and gambling websites, sites featuring violent content, and P2P/File Sharing sites. Select the toggles to restrict access to a particular content type. After the item is checked, the app refreshes, and the filter is applied. You can set custom restrictions for all users, or select from a pre-defined set of restrictions by age group:
    - Child (0-8 yrs old)
    - Pre-teen (9-12 yrs old)
    - Teen (13-18 yrs old)
- The **Applications** section is where you can ban or allow profile access to specific applications. For example, if your child needs to get homework done, you can ban a gaming application from connecting to the internet for that span of time. You can do this with other applications like Instagram, Steam, Discord, Skype, and Minecraft. Simply start typing to see if the application is available to block.
- The **Websites** section allows you to ban or allow specific websites. For example, if you notice that a user is spending too much time browsing specific sites, you can add the URL to block it.

See the Parental Control Settings Help article for more information.

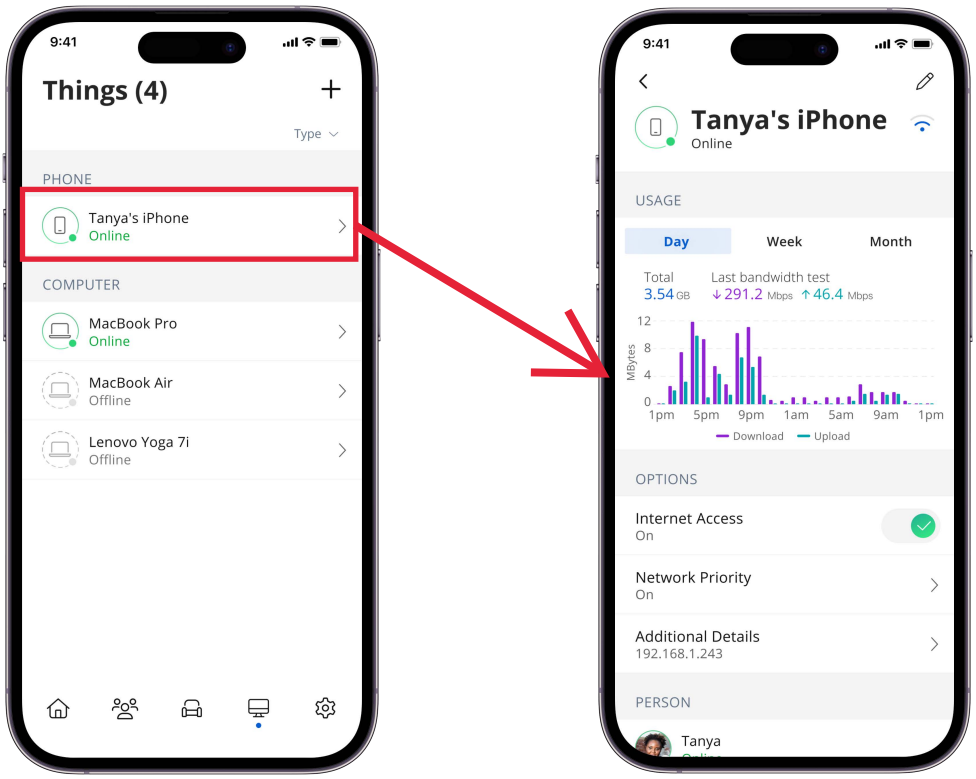
Note: Applications are not websites. Applications access data directly from servers that a web browser would never know about or be able to block by name. This is where the application filter is used. For example: you can block the website twitter.com via the website filter. If the Twitter application is installed on the device as an app, it will also need to be blocked in the application filter.

Note: Individual websites are categorized into groups for content restriction purposes. While this does not represent all categories imaginable, it is the set that represents some of the most common groups parents wish to restrict. Cloud services and automation are responsible for analyzing and categorizing websites focusing on the most-seen sites. Users can always block a specific site if it has not been categorized yet by using the website filter option.

How can I view device usage from a person's profile?

To view device usage:

1. Go to the **People** screen.
2. Tap on the desired person.
3. Scroll to the **Things** section and tap on the desired thing. You can view usage within the past few minutes or hours as well as by day and week. This capability allows you to track approximate usage over time.



You can also view device usage information by tapping on a thing from the **Things** screen.

I accidentally put my phone into a parental control profile and turned it off, now I cannot turn it back on. What should I do?

Simply turn off Wi-Fi on your phone and wait for it to connect to the cellular network. You can then enter the app and select the checkmark icon to turn your profile back on. We would recommend that you remove your phone as a Thing from the profile if you do not want to accidentally turn yourself off.

What are VPN detection alerts?

You will receive an alert if a device within your network is using or attempting to use a virtual private network (VPN) or other secured data transfer method. This can show you if a device may be attempting to bypass restrictions you have set. VPN detection alerts can help keep you informed of potentially unwanted traffic your network and helps you better manage profiles within your network (e.g., children or minors).

To disable or enable VPN detection alerts:

1. Go to **Settings > Alerts**.
2. Tap on the **VPN Detection** toggle to turn VPN detection on or off.