![Volcano Communications Group logo]

Going beyond connectivity to business productivity

CommandWorx® gives you easy access to a snapshot view of your small business network. Through the app you can manage your Wi-Fi networks, configure a backup internet connection, and more. **Command**Worx puts you in charge!
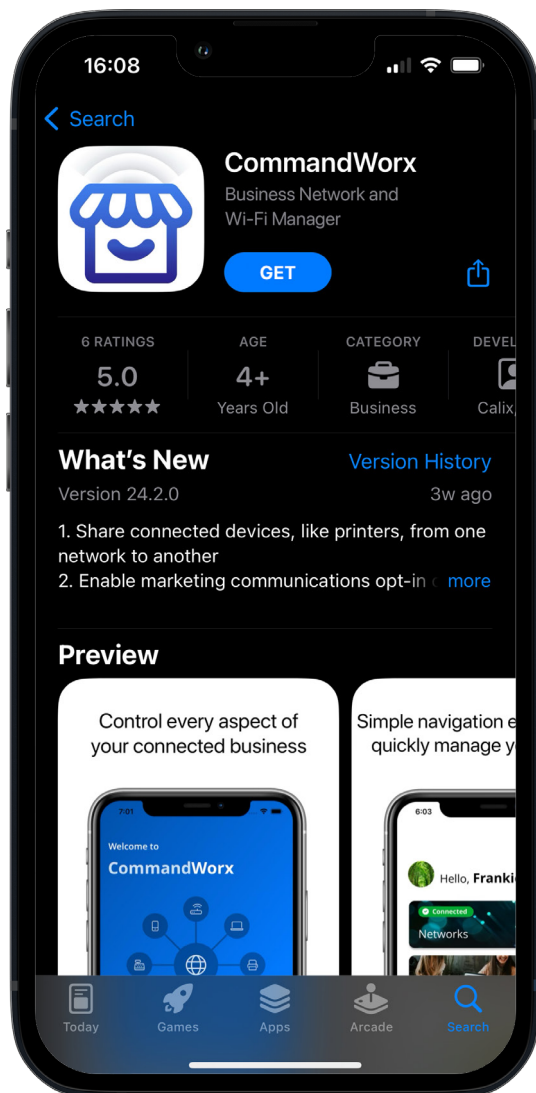
Table of contents

SET-UP GUIDE

Command*Worx*

One app to rule them all

Welcome to the future! The GigaSpire BLAST is the ultimate Wi-Fi system. To begin, download Command*Worx* from the Apple® App Store® or the Google Play™ Store and install onto your phone or tablet.
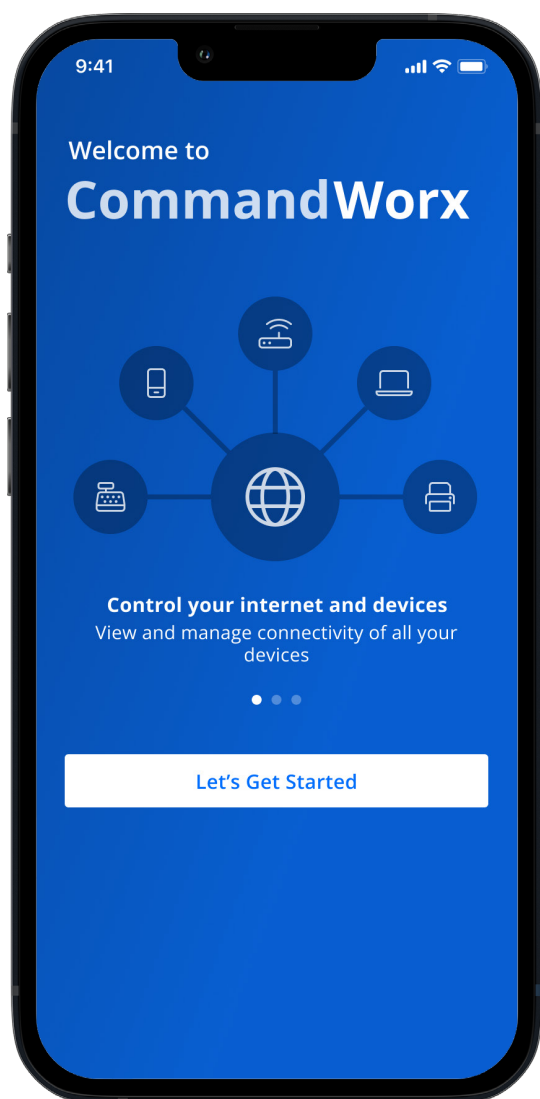
App setup

Setting up your app has never been easier!

STEP 1

Tap Let's Get Started

If you forget the password to access your CommandWorx, tap **Forgot Password?** to reset and access your account.
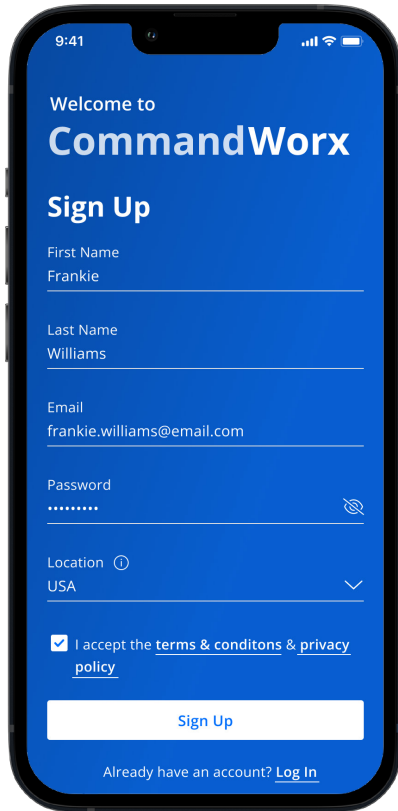
STEP 2

Enter basic personal information

The password you enter here is the password you use to log in to the app.

STEP 3

New system setup

Now plug your new system into a power outlet. It may take several minutes for the unit to be ready. You'll know once the light turns solid green.

Step 1 of 4

Scan Device

Plug in your new device and scan the QR code to continue
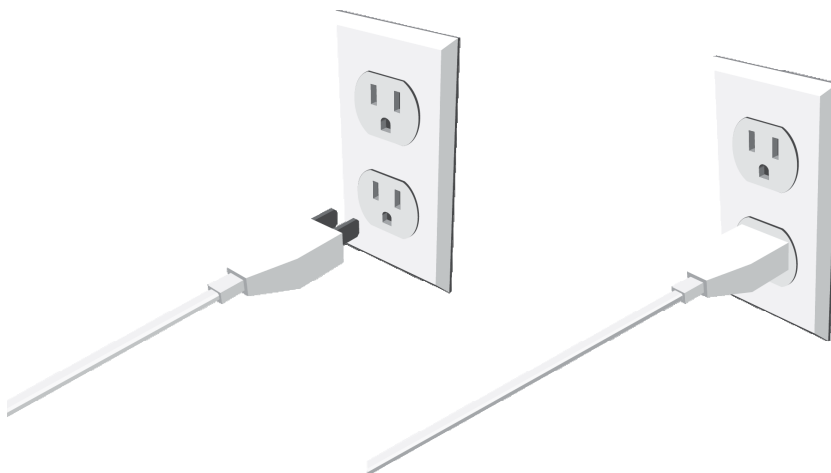
GigaSp
Jose, CA 95134
Model: u
Model No.:
300-Level N
Serial No.:
ONU MAC:
MTA MAC:
SSID:

Issues Scanning?

Router Wiring Setup

STEP 4

Scan the QR code

Your system has a QR code on the side or bottom. Simply open the app, tap OK, and scan the QR code.

Alternately, you can tap **Issues Scanning?** to manually enter the MAC Address and Serial Number.
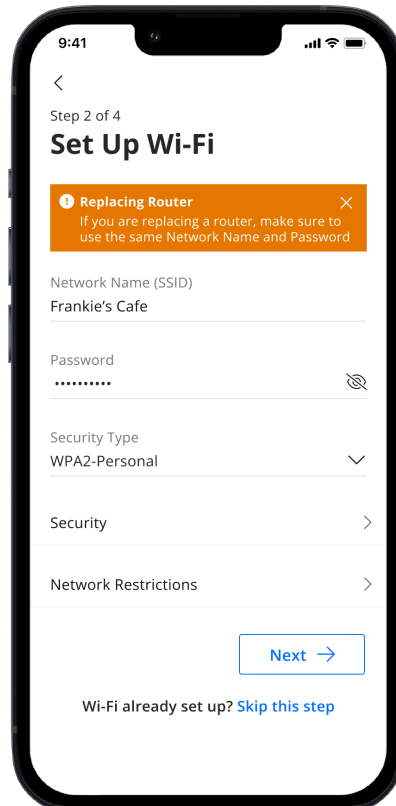
After you tap **Ok**, you may be asked to enter your account number.

STEP 5

Set up the Primary network

If you are setting up your Primary Wi-Fi network for the first time, you can assign a name and password for the network.

Optionally, configure security settings and content restrictions for the network.

Step 2 of 4

Set Up Wi-Fi

⚠ **Replacing Router** ✕
If you are replacing a router, make sure to use the same Network Name and Password

Network Name (SSID)
Frankie's Cafe

Password
....   🚫

Security Type
WPA2-Personal   ⌄

Security   ›

Network Restrictions   ›

Next →

Wi-Fi already set up? Skip this step
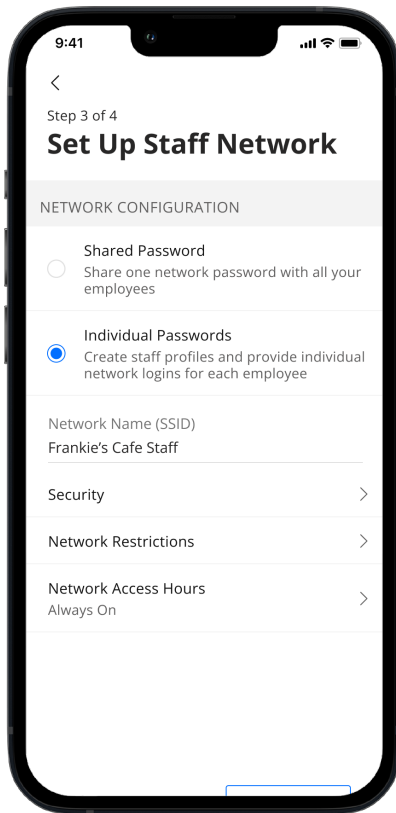
STEP 6

Set up the Staff network

You can set up a Wi-Fi network for your staff. Assign a name and select whether staff should use a shared password or individual passwords to join the network.

Optionally, configure security settings, content restrictions, and time limits for network access.

If you'd like to set up this network later, tap **Skip this step**.

STEP 7

# Set up the Point of Sale network

You can set up a Wi-Fi network specifically for point of sale devices such as card readers. Simply assign a name and a password for the network and enable access for the desired wired or wireless configuration.

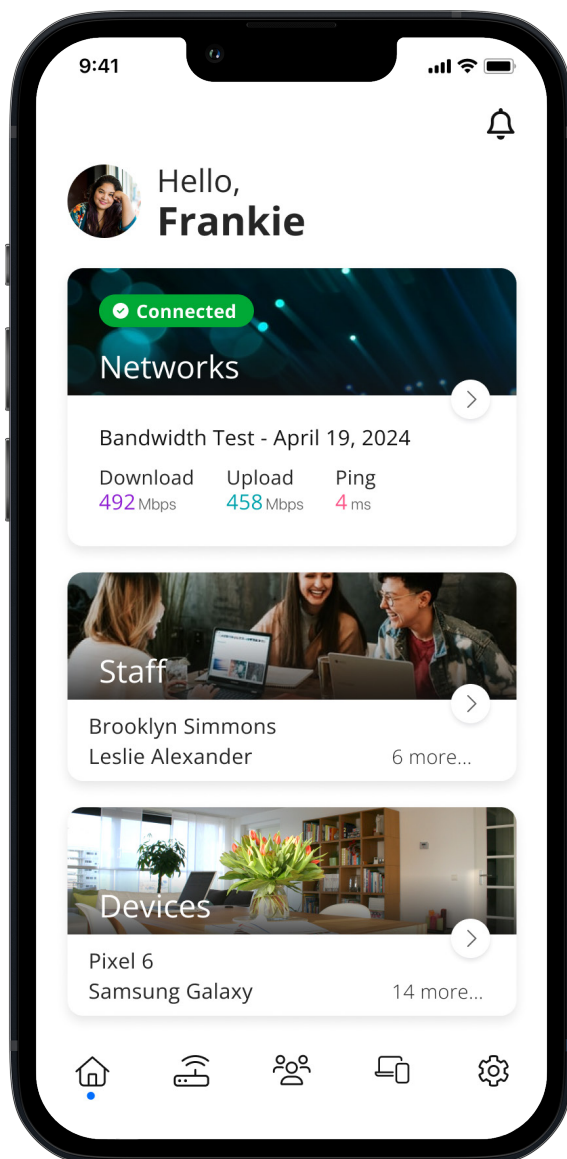Optionally, configure security settings and content restrictions for the network.

If you'd like to set up this network later, tap **Skip this step**.
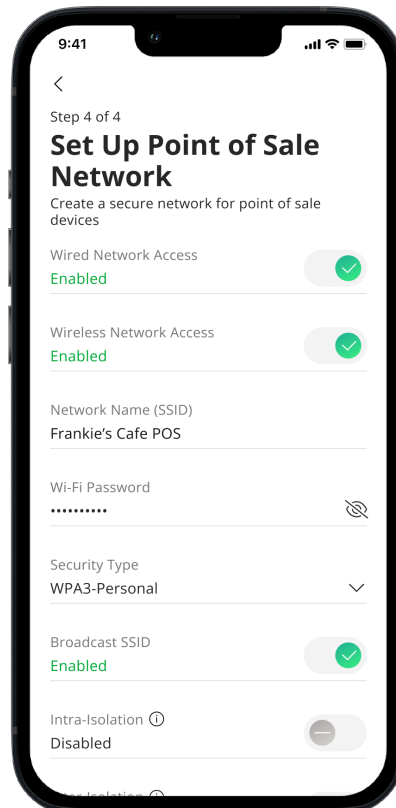
Main Dashboard

This is the home screen you'll see every time you open the app

The Dashboard gives you complete control over your networks and devices.

Tap the *bell* icon to view a list of network alerts.

Tap the **Networks** tile to:

- Access your Wi-Fi network settings
- Run a bandwidth test
- Configure the Customer Portal
- Configure Network Resilience
- View all connected devices and device usage

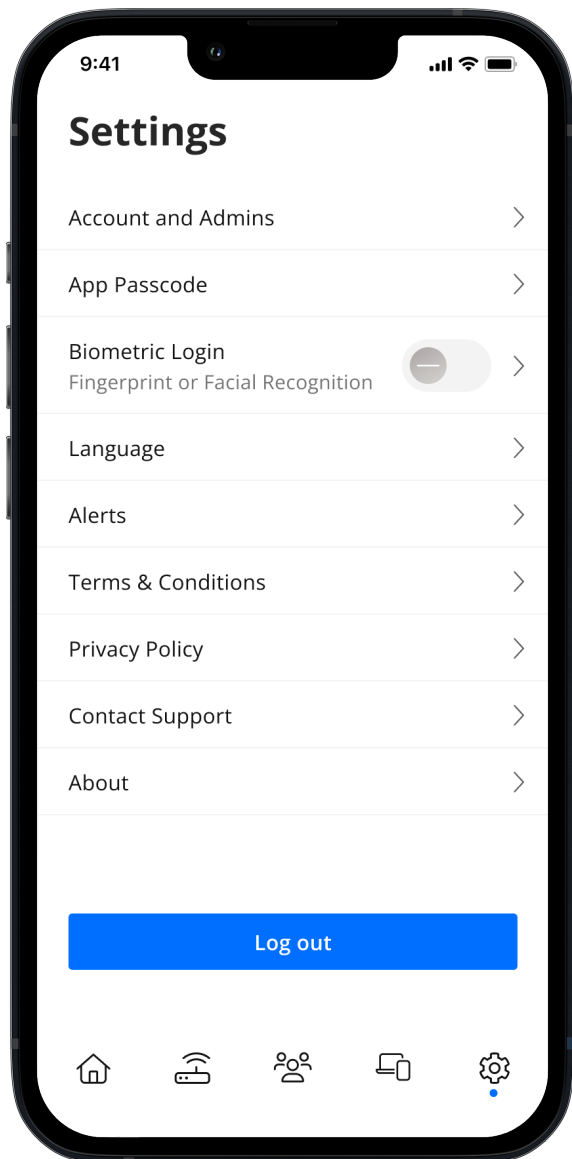Tap the **Staff** tile to view a list of staff user profiles.

Tap the **Devices** tile to acces a list of connected devices and view device details.

Use the bottom menu bar to navigate quickly throughout the app.

![Volcano Communications Group logo]

Settings

A world of customization is available to you

9:41

Settings

Account and Admins   >

App Passcode   >

Biometric Login   >
Fingerprint or Facial Recognition

Language   >

Alerts   >

Terms & Conditions   >

Privacy Policy   >

Contact Support   >

About   >

Log out

Account and Admins
Update your name, email address, and account password, or add a secondary administrator.

App Passcode
Set a PIN in lieu of an app login password.

Biometric Login
Setup biometric login in lieu of an app login password.

Language
Choose your preferred language (English, French Canadian, Spanish, German).

Alerts
Manage your alert settings.

Terms & Conditions
View the terms and conditions you acknowledge by using the app.

Privacy Policy
View the Privacy Policy of the app.

Contact Support
Access support contact details and the billing portal.

About
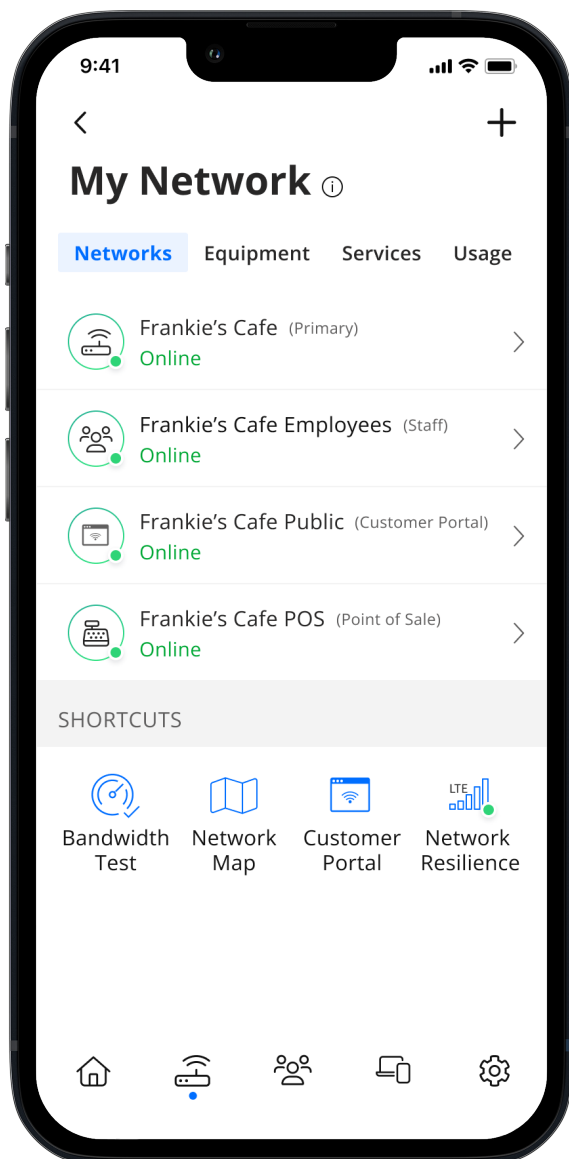View the app version and a brief summary of what the app does.

Log out
Tap to log out of the app.

Your Networks

Command**Worx** enables you to tailor your network to fit your business

Networks
Enable or disable Wi-Fi networks, add devices, and even share Wi-Fi credentials.

Customer Portal
Create a custom splash page for customers who wish to join your customer Wi-Fi network. You can configure content restrictions, login and marketing opt-in, network access hours, terms and conditions, and security settings.

Additionally, business owners can download a CSV file of visitors over a set retention period.
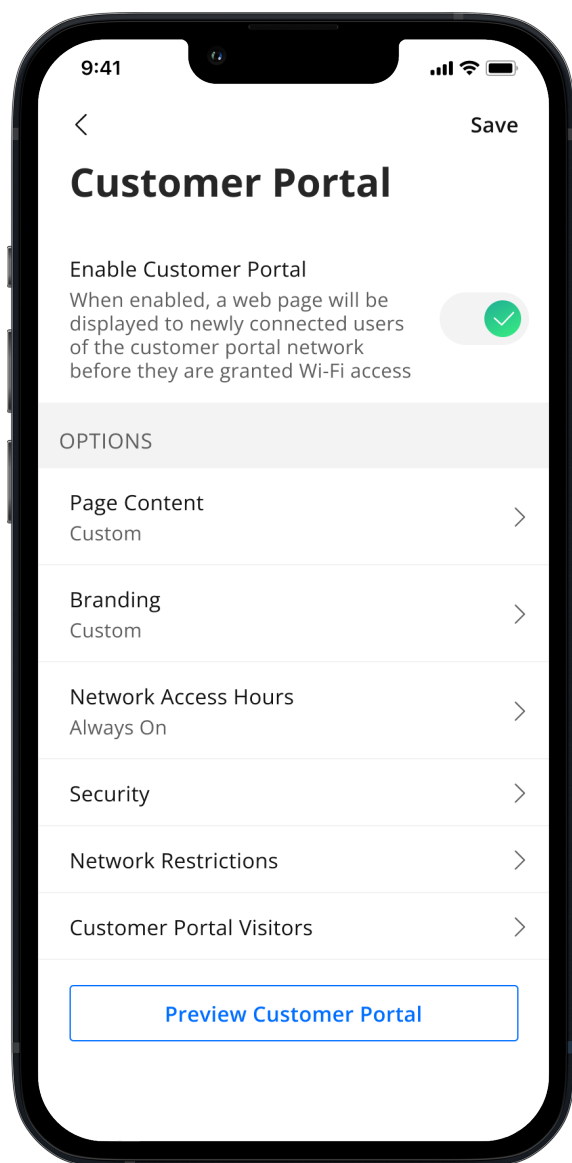
Network Resilience
Select a mobile device to provide mobile cellular/LTE service during internet service disruptions, preventing downtime and ensuring continued business operations.

Customer Portal

Providing Wi-Fi for your customers has never been easier

9:41

<   Save

Customer Portal

Enable Customer Portal
When enabled, a web page will be displayed to newly connected users of the customer portal network before they are granted Wi-Fi access

OPTIONS

Page Content
Custom   >

Branding
Custom   >

Network Access Hours
Always On   >

Security   >

Network Restrictions   >

Customer Portal Visitors   >

Preview Customer Portal

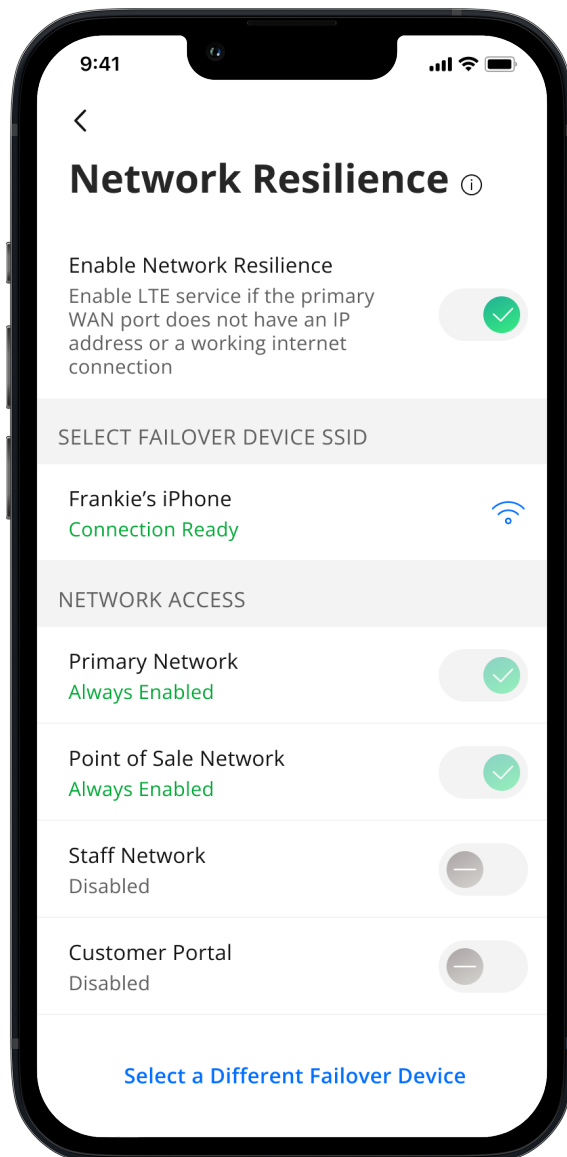From the My Network screen, tap **Customer Portal** to create a custom welcome page for your patrons.

On the Customer Portal screen, do the following:

1. Tap the **toggle** to enable the customer portal. The toggle turns green when enabled.
2. Tap **Page Content** to add a network name and page heading, add a cover photo, link your terms of service, and configure button text. You can enable marketing opt-in consent if your region contains anti-spam legislation.
3. Tap **Branding** to upload your business's logo and select the page background and font colors.
4. Tap **Network Access Hours** to set time limits for the customer network.
5. Tap **Security** to configure security settings.
6. Tap **Network Restrictions** to configure content restriction settings.
7. Tap **Customer Portal Visitors** to select how long to store visitor login information (1, 15, 30, 60, or 90 days) and retrieve a list of patrons who have accessed the network.
8. Tap **Preview Customer Portal** at any time to see how the page appears to your patrons.

Network Resilience

Keep your business running during internet outages

9:41

Network Resilience ⓘ

Enable Network Resilience
Enable LTE service if the primary WAN port does not have an IP address or a working internet connection ✓

SELECT FAILOVER DEVICE SSID

Frankie's iPhone
Connection Ready

NETWORK ACCESS

Primary Network
Always Enabled ✓

Point of Sale Network
Always Enabled ✓

Staff Network
Disabled

Customer Portal
Disabled

Select a Different Failover Device

From the My Network screen, tap **Network Resilience** to select a mobile device to provide secondary cellular/LTE service for your most critical networks during internet outages.

On the Network Resilience screen, do the following:

1. Tap the **toggle** to enable Network Resilience. The toggle turns green when enabled. Command**Worx** automatically searches for mobile hotspots.

2. Select a **hotspot** from the list.

3. Enter the **password** for the hotspot network.

4. Select which **network(s)** should use the secondary cellular/LTE service.

Network Usage

Keep track of and monitor the usage for each device
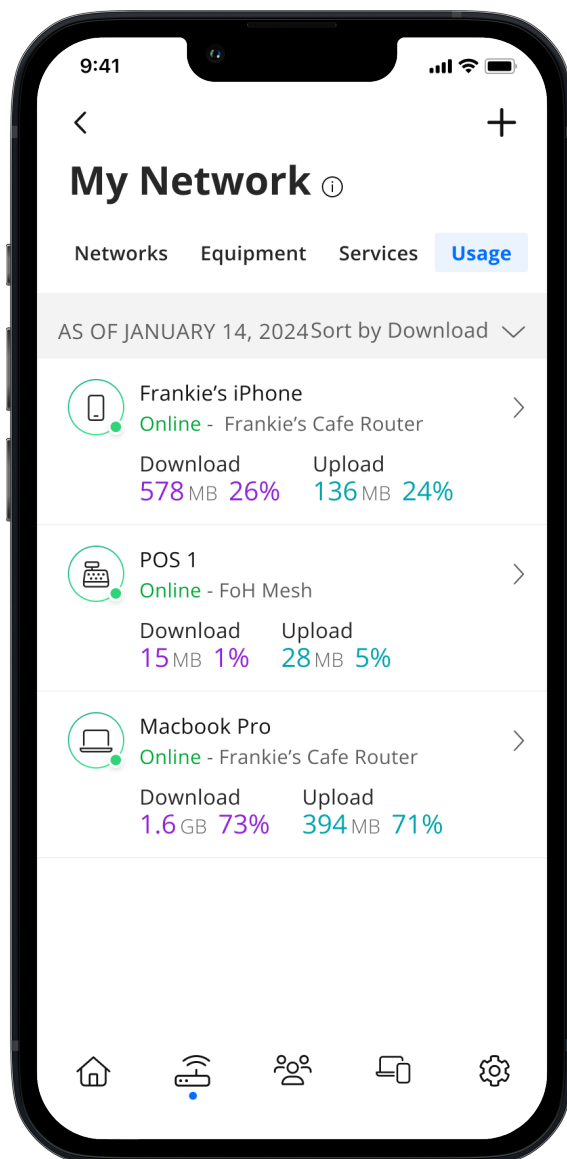
Network Usage is organized by device.

From this view, you can see basic usage information for each Wi-Fi connected device on your network, including:
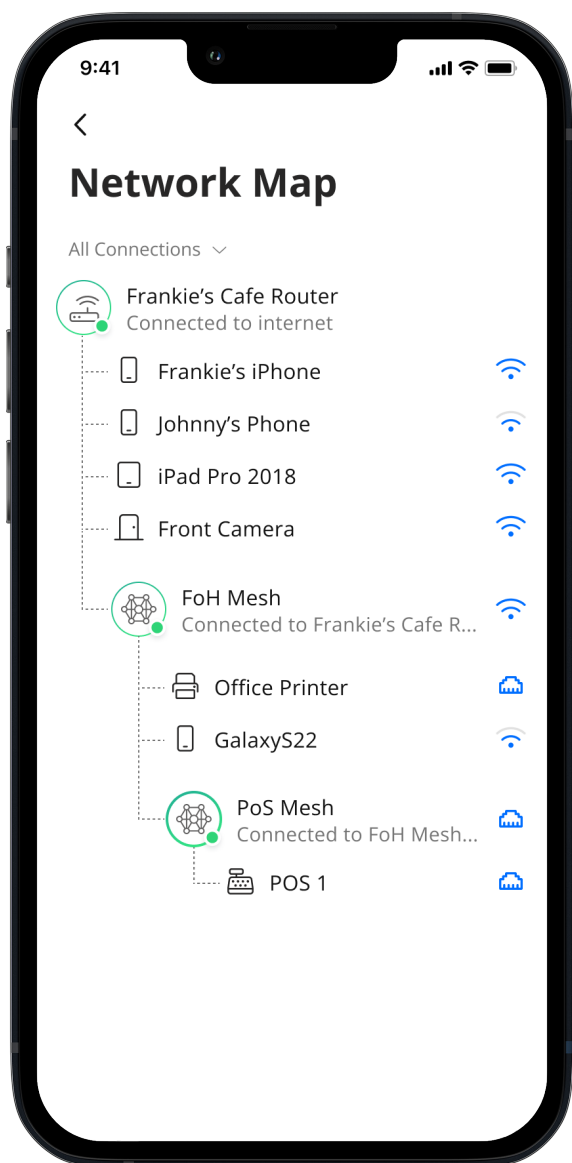
- Device identification and whether the device is connected to Wi-Fi
- What network device it is connected to
- Network usage
- The amount of data that has been used by this device

Network usage is updated each time you run a bandwidth test through the app.

Network Map

Your connected devices at a glance

9:41

‹

Network Map

All Connections ⌄

Frankie's Cafe Router
Connected to internet

📱 Frankie's iPhone 📶

📱 Johnny's Phone 📶

📱 iPad Pro 2018 📶

📷 Front Camera 📶

FoH Mesh 📶
Connected to Frankie's Cafe R…

🖨 Office Printer 🔌

📱 GalaxyS22 📶

PoS Mesh 🔌
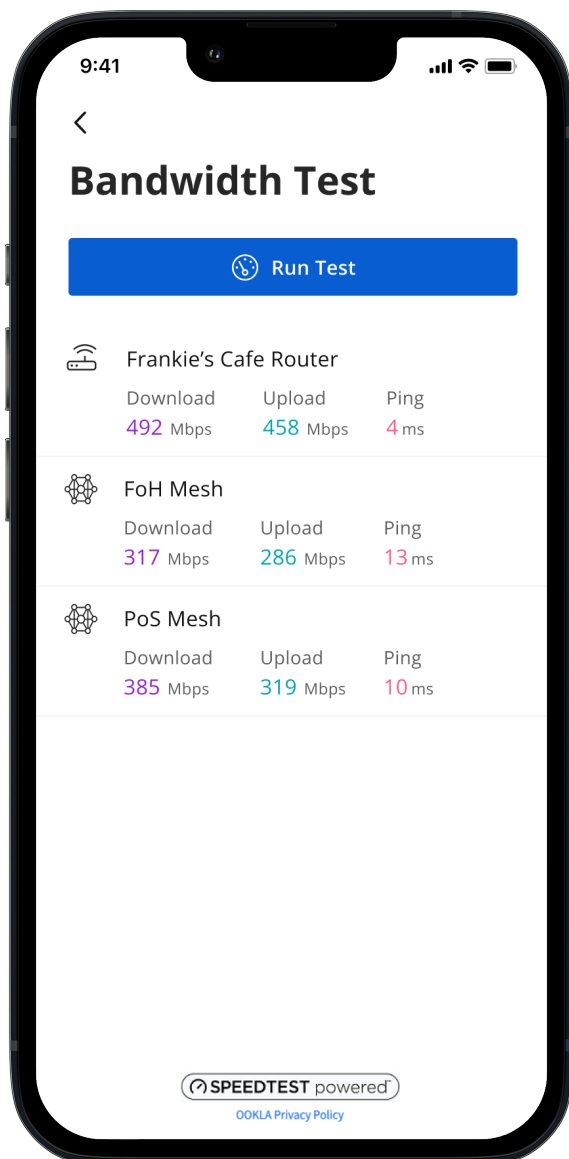Connected to FoH Mesh…

🖥 POS 1 🔌

The Network Map provides a topological view of your network. To view the Network Map, tap **Networks** on the dashboard. Next, tap **Network Map** to view devices connected to your system.

Tap on the Mesh icon to view performance information and devices connected at that Mesh unit.

Speed Test

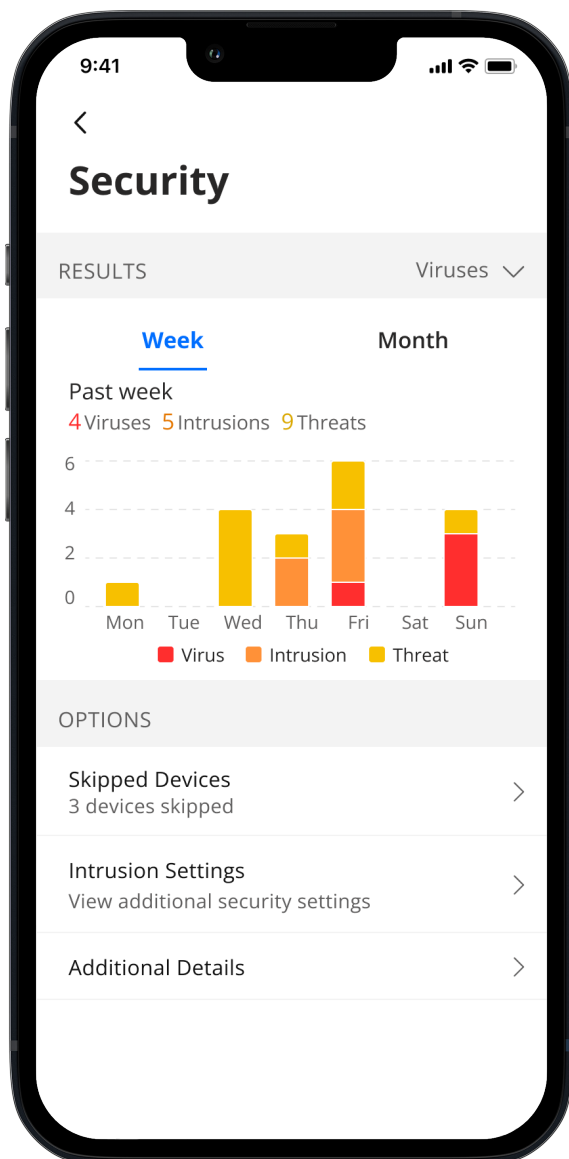## Ensure you're getting the speeds your business needs

The easiest way to run a bandwidth test is to tap **Networks** and then tap the **Bandwidth Test** icon. Then simply tap the **Run Test** button.

The speed test first runs between the router and the Internet, and then conducts a speed test between any mesh units and the router. Results display on the Networks tile on the Home dashboard.

9:41

Bandwidth Test

| Run Test |

Frankie's Cafe Router

Download	Upload	Ping
492 Mbps	458 Mbps	4 ms

FoH Mesh

Download	Upload	Ping
317 Mbps	286 Mbps	13 ms

PoS Mesh

Download	Upload	Ping
385 Mbps	319 Mbps	10 ms

SPEEDTEST powered
OOKLA Privacy Policy

Network Security

Proactive cybersecurity keeps your business safe

Your router automatically scans data coming into each network for viruses and other malicious content to provide an extra layer of protection against malicious traffic. Threats are automatically blocked from entering the network.

To view a network's security status, tap **Networks** from the home dashboard, tap on the desired network, then tap **Security**. You can track security trends over the previous week or the previous month.
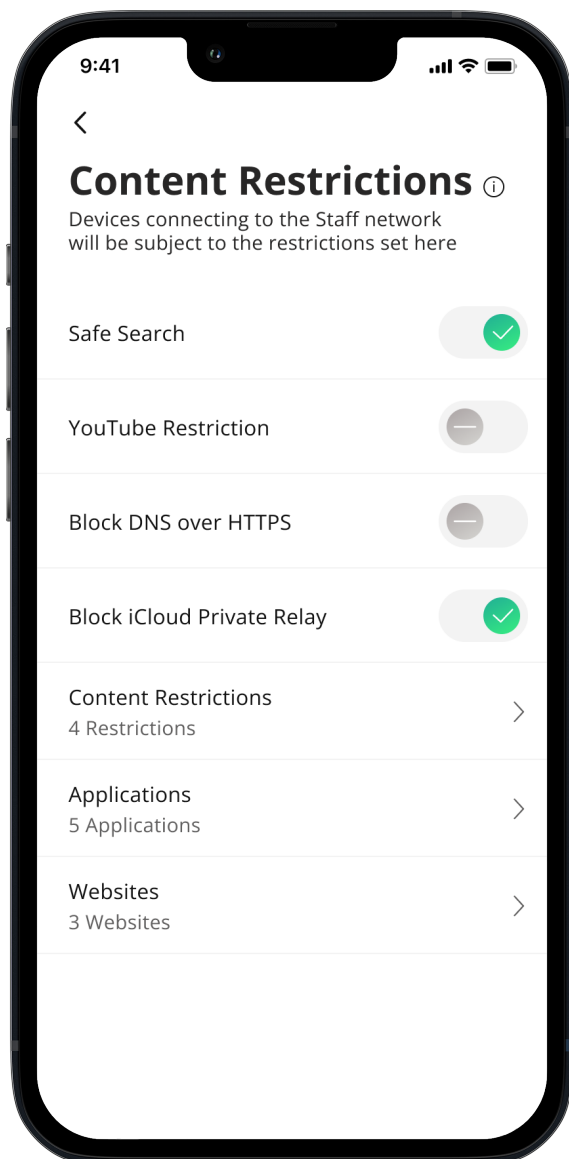
Additional Details provides additional information including packets analyzed and the total number of threats detected and blocked.

Note: Do not remove device level protection for anti-virus and malware.

Content Restrictions

Protect your business, staff, and customers from harmful content

9:41

‹

Content Restrictions ⓘ

Devices connecting to the Staff network will be subject to the restrictions set here

Safe Search ✅

YouTube Restriction ⊖

Block DNS over HTTPS ⊖

Block iCloud Private Relay ✅

Content Restrictions
4 Restrictions ›

Applications
5 Applications ›

Websites
3 Websites ›

You can configure content, application, and website restriction settings for the Primary, Customer, Staff, and Point of Sale networks.
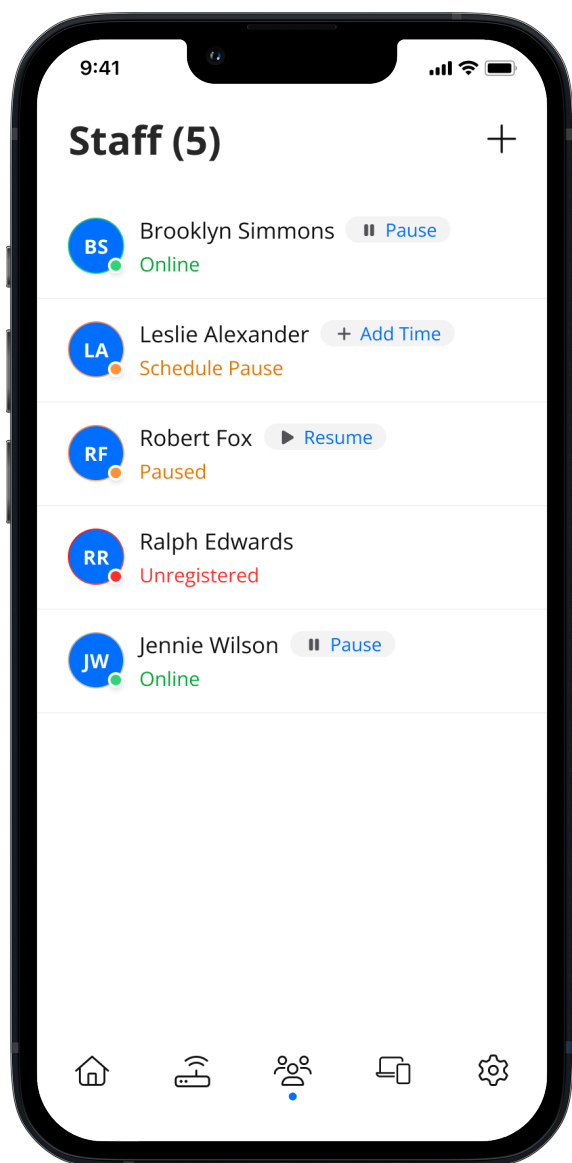
To configure restrictions:

1. Tap the **Networks** tile on the Home screen.
2. Tap on the desired network.
3. Tap **Content Restrictions**.
4. Tap the toggles to enable or disable restriction options.
5. Tap on **Content Restrictions** to configure restrictions by content category.
6. Tap on **Applications** to block access to specific applications.
7. Tap on **Websites** to block access to specific websites.

Staff List

Easily add or remove Staff and manage their device access

Staff (5) +

BS	Brooklyn Simmons ⏸ Pause Online
LA	Leslie Alexander + Add Time Schedule Pause
RF	Robert Fox ▶ Resume Paused
RR	Ralph Edwards Unregistered
JW	Jennie Wilson ⏸ Pause Online

The **Staff** screen shows a list of staff user profiles. From the Staff screen, you can:
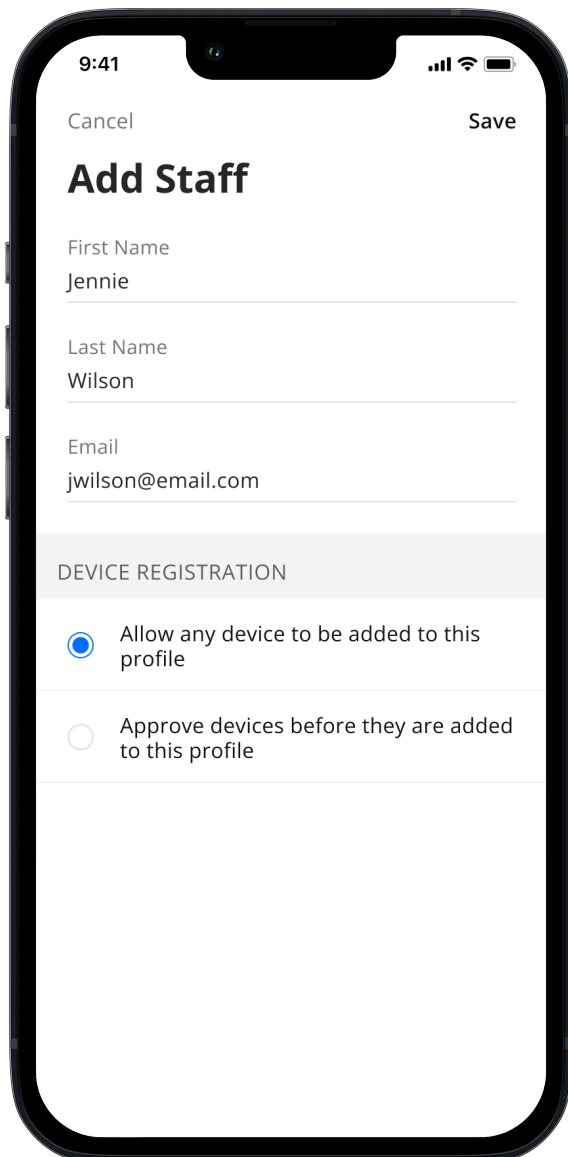
- Create staff user profiles
- View a staff user's devices
- Set network access hours
- Share network access
- Register devices

Staff Profiles

Control who has network access and how they add devices

9:41

Cancel   Save

Add Staff

First Name
Jennie

Last Name
Wilson

Email
jwilson@email.com

DEVICE REGISTRATION

● Allow any device to be added to this profile

○ Approve devices before they are added to this profile

Staff profiles allow you to control which employee devices can connect to the Staff network.

To create a staff profile:

1. From the Home screen, tap on the **Staff** tile.
2. Tap the **plus sign**.
3. Enter the user's first name, last name, and email address.
4. Select a trust level for the user's devices. You can choose automatic (high trust) or manual (low trust) device approval and registration.
5. Tap **Save**.

Device List

Managing your connected devices is as easy as 1-2-3
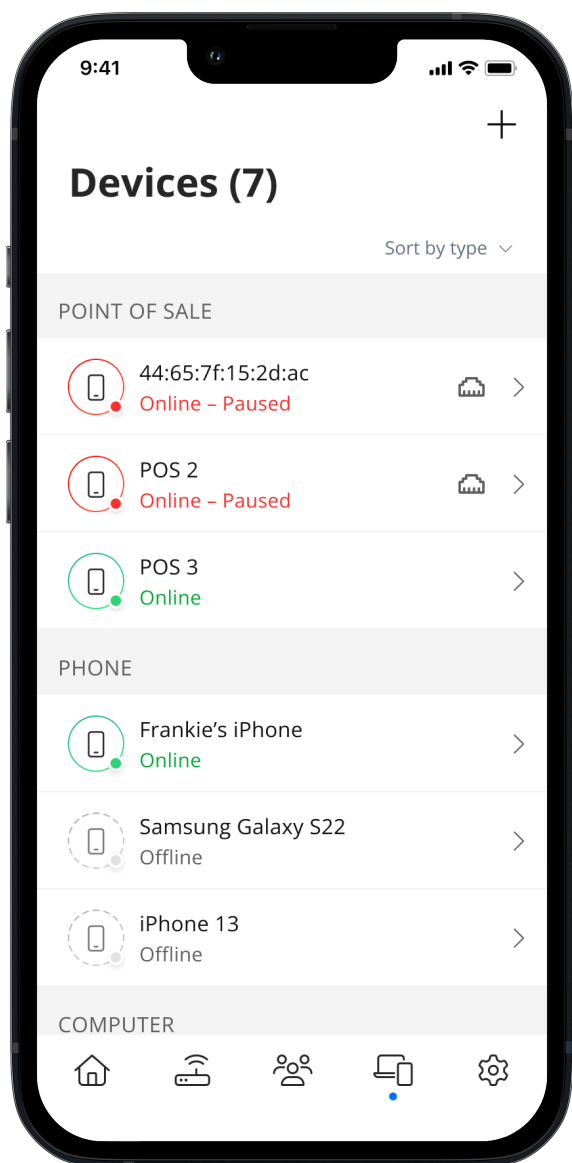
The Devices list allows you to manage the devices connected to your network. Tap on a device to enable/disable internet access or to see additional details including:

- Device name
- Signal strength
- Internet usage
- Approve connectivity*

*Only wired Primary or Point of Sale devices when first connected

Device Details

Monitor and configure a connected device
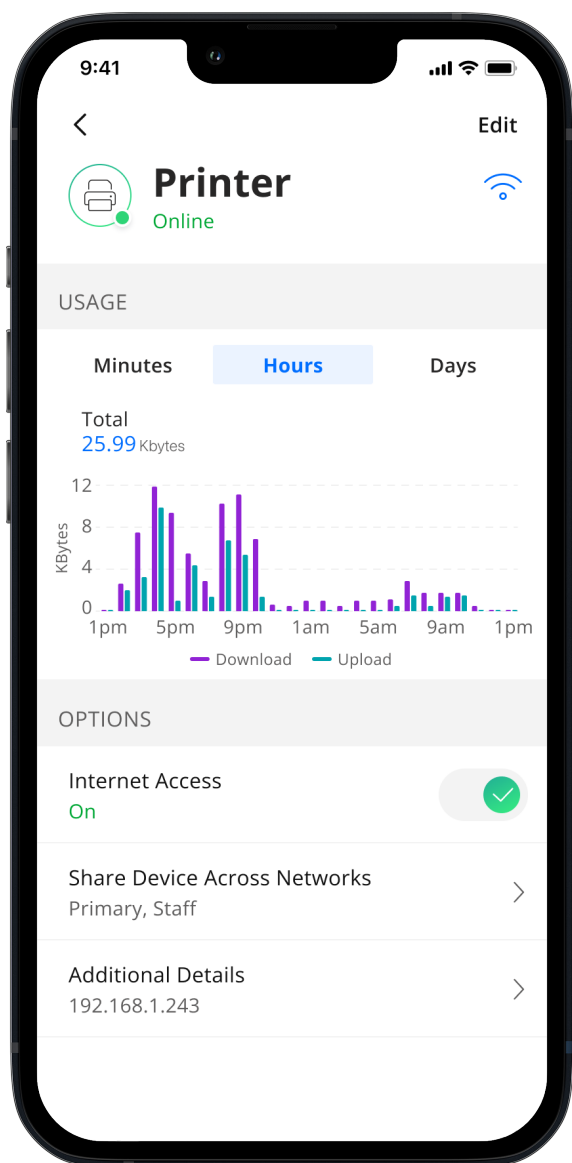
The Device details screen shows the device name at the top of the screen followed by a chart that indicates the amount of data that was used by the device over a period of time.

Tap the *pencil* icon in the upper right-hand corner to rename the device to something easier for you to identify.

Data usage shows data used by this specific device.

Toggle the **On/Off** button in the Internet Access section to enable or disable internet access for this device.

Tap **Share Device Across Networks** to select which networks you'd like this device to also be accessible from.

Tap **Additional Details** to view additional information or to change the category of the device.