Northland
COMMUNICATIONS

CommandWorx

For SmartBiz

PROGRAMMING MANUAL

March 27, 2024

TABLE OF CONTENTS

CLICK ON ANY SUBJECT BELOW TO SKIP TO THAT INFORMATION
CLICK ON ANY PAGE NUMBER TO RETURN TO THE TABLE OF CONTENTS

WHAT IS SMARTBIZ?

SmartBiz is an all-in-one managed service solution enabling small businesses to maximize their productivity, secure critical business systems and drive customer loyalty. Small business owners are connected via GigaSpire solutions and use the CommandWorx app to set up, monitor and manage each element of the SmartBiz solution.

Key CommandWorx capabilities include four business-specific networks, built-in network security, traffic and access policy for staff and customers and network resilience.

+ **Primary Network:** This primary network powers wired and wireless business devices managed by the business owner/manager such as computers, cameras, security systems, and wireless printers, keeping these business critical systems secured and separated from other networks.

+ **Staff Network:** Businesses can provide amazing bandwidth for employee activity, including office and productivity applications, without impacting primary network functions.

+ **Point of Sale Network:** Business owners that accept credit card transactions must follow specific rules to maintain Payment Card Industry Data Security Standards. SmartBiz maintains that essential compliance by providing an isolated and protected point-of-sale network that is dedicated to point-of-sale devices.

+ **Customer Portal:** Businesses can grow their brand, increase loyalty and attract new customers by providing free Wi-Fi through a customer portal with a customizable login screen the business can add their logo and colors to, right from the app! Business owners can also add their own terms of use and customize the hours the free Wi-Fi is available.

Network Resilience

Internet connectivity is essential to small businesses. You can ensure critical business systems are always operational, even if there's an internet outage, with SmartBiz Network Resilience.

In the event of an internet outage, SmartBiz will detect the outage and automatically switch to the selected backup method, ensuring connectivity to critical devices.

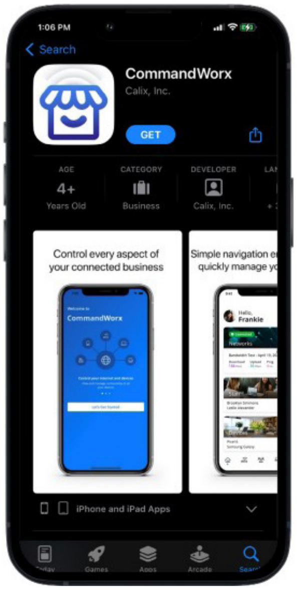
Subscribers use CommandWorx to select a dedicated hotspot (recommended) or their own LTE/5G device to provide backup. Wired (ethernet) backup may also be set up by Northland Communications via the embedded web interface (EWI). Only the 1st ethernet port (eth0) can be used for network resilience.

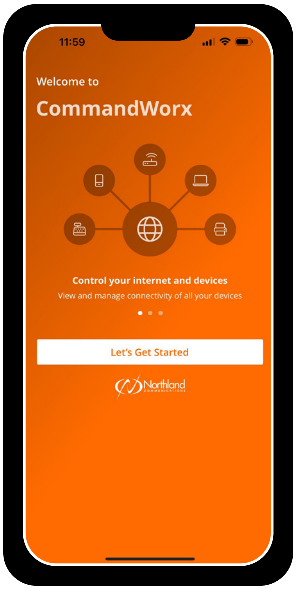
GETTING STARTED

You will need to be near the GigaSpire to complete the set steps.
NOTE: You may already have completed these initial steps with the Northland technician at the time of installation.

Download The App

To begin, download CommandWorx from the Apple® App Store® or the Google Play™ Store and install onto your Phone or tablet.

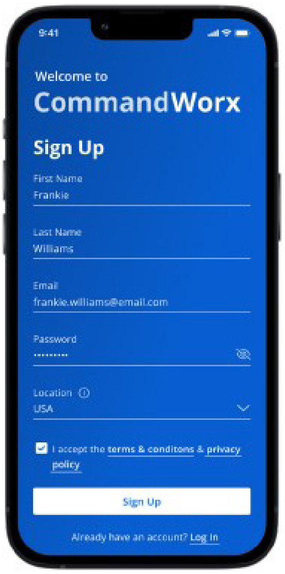



11:59

Welcome to
CommandWorx

Control your internet and devices
View and manage connectivity of all your devices

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


9:41

Welcome to
CommandWorx

Sign Up

First Name
Frankie

Last Name
Williams

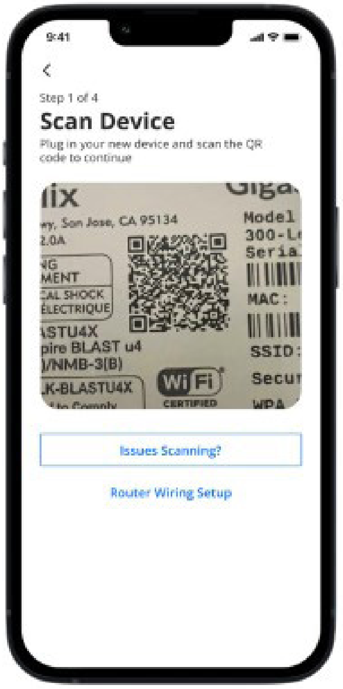
Email
frankie.williams@email.com

Password
••••••••••

Location ⓘ
USA

☑ I accept the terms & conditons & privacy policy

+ 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.
+ 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
+ Tap to select the checkbox for the I Accept the Terms & Conditions acknowledgment (required to proceed).
+ Tap the Sign Up button to save your inputs and continue to set up your router.



Step 1 of 4

Scan Device

Plug in your new device and scan the QR code to continue

- + The next step is to scan the QR Code on your GigaSpire. Your system has a metal plate with a QR code on the side or bottom. Simply open the app, tap **OK**, and scan the QR code.
- + Alternately, if your mobile device's camera cannot read the QR Code, you can tap **Issues Scanning?** to manually enter the MAC Address and Serial Number also found on that same metal plate.
- + Tap **OK**. You may be asked to enter your account number.

SET UP NETWORKS

The next step is to set up the Primary Network. This primary network powers wired and wireless business devices managed by the business owner/manager such as computers, cameras, security systems, and wireless printers, keeping these business critical systems secured and separated from other networks.

Set up the Primary Network

When you set up your Primary Network for the first time, you will assign a name and a password for the network.

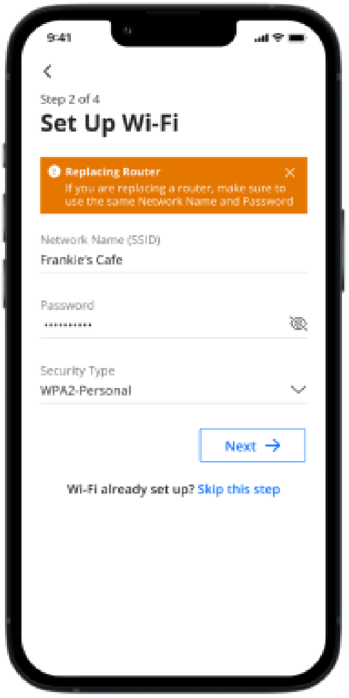
To Set Up The Primary Wi-Fi Network:

On the **Set Up 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.
+ Tap the **Password** field and enter the password for the wireless network.
+ Select the Security Type.
  Optionally, configure Security settings and Network Restrictions. These can be changed at a later time.
+ Tap **Next** to configure the Staff network

OR

+ Tap **Skip** this step to bypass this setup task (for example, if completed previously outside of CommandWorx) and proceed to set up the Staff 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

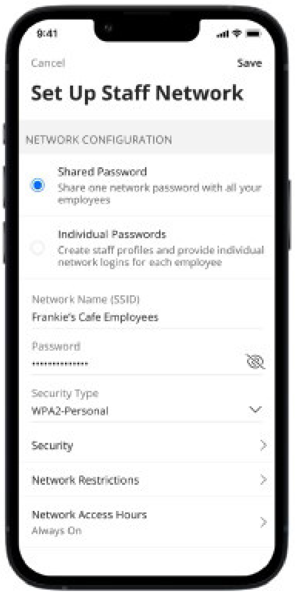
Password
••••••••••

Security Type
WPA2-Personal

Wi-Fi already set up? Skip this step

Set Up The Staff Network

The Staff Network provides Businesses with the ability to provide bandwidth for employee activity, including office and productivity applications, without impacting primary network functions.



Set Up Staff Network

NETWORK CONFIGURATION

● Shared Password
Share one network password with all your employees

○ Individual Passwords
Create staff profiles and provide individual network logins for each employee

Network Name (SSID)
Frankie's Cafe Employees

Password
••••••••••••••

Security Type
WPA2-Personal

Security

Network Restrictions

Network Access Hours
Always On

To Set Up The Staff Network:

On the **Set Up Staff Network** screen:

+ Tap the Network Name (SSID) field, then type the name for the Staff network. The default network name is SMBSTF_[router serial number].
+ You can choose a universal password for your Staff network or provide individual passwords for each employee. For the Shared Password option, tap the Password field and enter the password for the wireless network. See Individual/Shared Passwords
+ Select the Security Type.

Note: You can only select a Security Type for a Shared Password network configuration.

+ Optionally, apply Network Restrictions and Network Access Hours. These can be configured at a later time.
+ Tap **Next** to save the settings and proceed to configure the Point of Sale network.

OR

+ Tap **Skip** this step to bypass this setup task and proceed to set up the Point of Sale network.

INDIVIDUAL/SHARED PASSWORDS

CommandWorx supports two staff network configurations:

Use the Shared Password configuration to share one network password with all of your employees.
Use Individual Passwords to create staff profiles, provide individual network logins for each employee, and manage devices associated with each employee.

Set Up The Point Of Sale Network

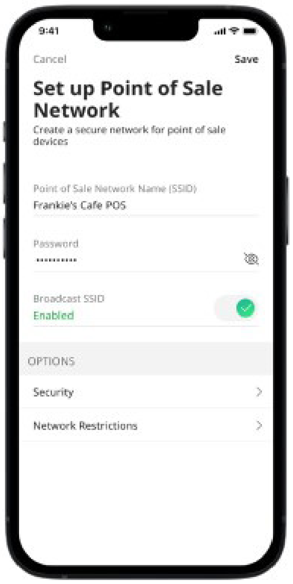
The final screen in the setup sequence allows you to configure a Wi-Fi network for wired or wireless point of sale devices.

Guidelines:

+ If Wired Network Access is disabled, wired point of sale devices join the primary LAN network.
+ If your environment contains wired and wireless devices that must communicate with one another, ensure your Inter/Intra Isolation settings are properly configured.

To Set Up Point Of Sale Network:

On the **Set Up Point of Sale Network** screen:



Set up Point of Sale Network
Create a secure network for point of sale devices

Point of Sale Network Name (SSID)
Frankie's Cafe POS

Password
••••••••••

Broadcast SSID
Enabled

+ Configure the Wired Network Access and Wireless Network Access toggles to support your preferred Point of Sale connection types.

Note: If you disable Wired Network Access, wired PoS devices will automatically join the Primary LAN network.

+ Tap the **Point of Sale Network Name** (SSID) field, then type the name for the Point of Sale network. The default SSID name is SMBPOS-[router serial number].
+ Tap the **Password** field and enter the password for the wireless network.
+ Select the Security Type.
+ Optionally, tap the Broadcast SSID toggle to allow the hotspot to broadcast the Point of Sale network SSID. This setting is disabled by default.

NOTE: You must enable Wireless Network Access to access this feature.

+ Optionally, enable the Intra Isolation toggle to prevent communication between devices on the same network. This option is disabled by default.
+ Optionally, enable the Inter Isolation toggle to prevent communication between devices on separate networks.
+ Optionally, apply Network Restrictions and Intrusion prevention settings. These can be configured at a later time.
+ Tap the **Done** button to save your inputs and complete the onboarding setup process. A confirmation displays.
+ Tap **Done** to proceed to the CommandWorx **Home** screen or select **Setup Mesh** to add a mesh satellite
+ Tap **Skip this step** at the bottom of the screen to bypass this setup task and proceed to the app dashboard (**Home** screen).

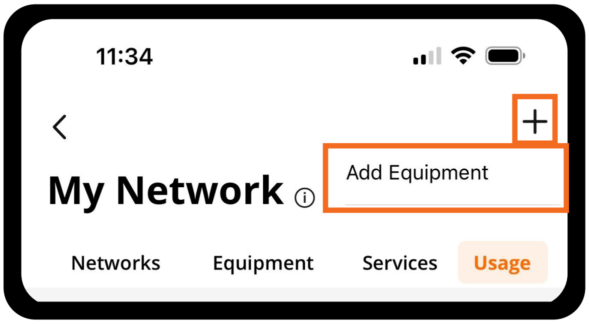
Add A Mesh (Sat) Device

After you complete the initial router onboarding and Wi-Fi setup, you have the option to onboard addition mesh (satellite) units. You can onboard up to 4 mesh units.

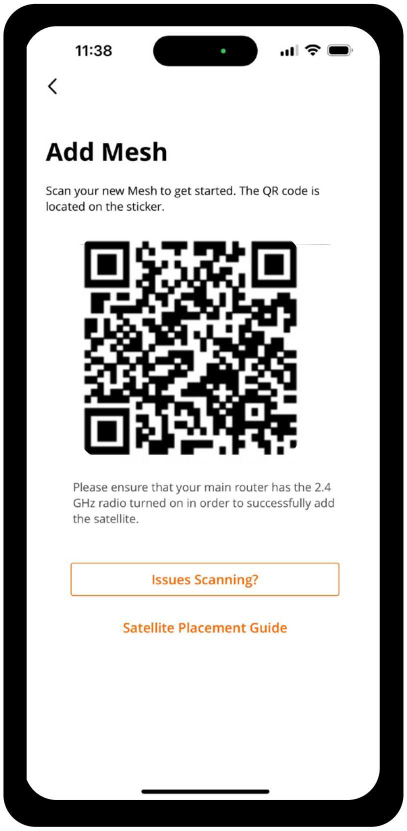
Guidelines:

- The desired mesh device must have prior RG pairing.
- If the mesh satellite has previously been paired to an RG, factory reset the mesh by holding the reset button for 30 seconds.

To Setup Mesh (SAT):



- On the My Network tab, tap the **+ (add)**.
- Tap **Add Equipment**. The **Add Message** screen is displayed.



Add Mesh

Scan your new Mesh to get started. The QR code is located on the sticker.

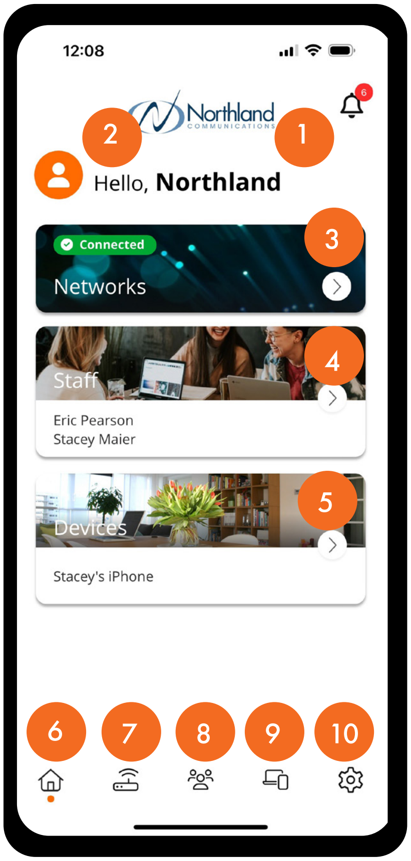
Please ensure that your main router has the 2.4 GHz radio turned on in order to successfully add the satellite.

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

DASHBOARD (HOME SCREEN)

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

Below is a screenshot of the dashboard's element map. You should familiarize yourself with the the element names.



1. Alerts: Tap to view a list of network, security, and traffic alerts on private networks. You can configure push notifications and the desired alerts from the Settings element.
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 CommandWorx is personalized for you and your business network. You can modify the account name that appears here as needed.
3. Networks: Provides the status of routers in the network as well as the last measured result of a speed test. Tap the **Networks** tile to view equipment, services, and usage statistics for devices and equipment associated with the network chosen.
4. Staff: Tap to configure and view employee profiles on the network. Tap an individual profile to view status and associated devices or edit name, email, and password information.
5. Devices: Tap to view a list of all devices on the network. Tap an individual device to view additional information, including bandwidth utilization. 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.

Bottom Menu

The bottom menu appears throughout the CommandWorx app and provides easy access to the main sections of the app:

6. **Home:** Tap to return to the **Home** screen.
7. **Networks:** Tap to access the **Networks** screen.
8. **Staff:** Tap to access the **Staff** screen.
9. **Devices:** Tap to access the **Devices** screen.
10. **Settings:** Tap to access and modify CommandWorx app settings.

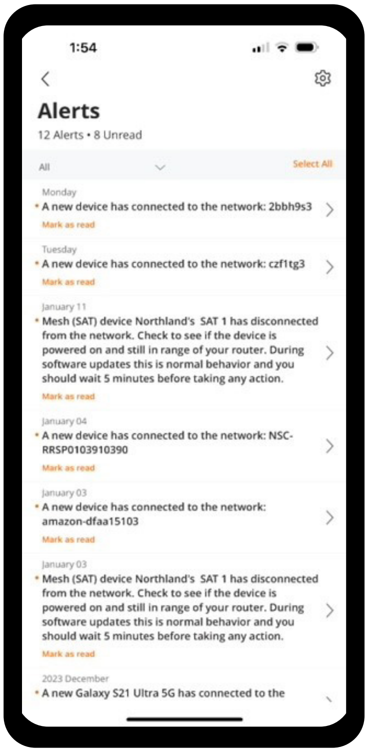
NOTE: Only Staff networks configured for individual employee passwords support the shown staff interfaces. See Individual/Shared Passwords for more information on configuring shared or individual password networks.

Alerts

Tap the ***Alerts*** icon on the **Home** screen to view a list of notifications applicable to private networks. From the

Guidelines:

- Global alerts apply to the Primary and Staff networks only.
- You can enable alerts for wired devices connecting to the Point of Sale network.
- You can configure cellular failover alerts to notify when network resilience is activated and when internet service is restored.



Alerts

12 Alerts • 8 Unread

Monday

- A new device has connected to the network: 2bbh9s3

Mark as read

Tuesday

- A new device has connected to the network: czf1tg3

Mark as read

January 11

- Mesh (SAT) device Northland's SAT 1 has disconnected from the network. Check to see if the device is powered on and still in range of your router. During software updates this is normal behavior and you should wait 5 minutes before taking any action.

Mark as read

January 04

- A new device has connected to the network: NSC-RRSP0103910390

Mark as read

January 03

- A new device has connected to the network: amazon-dfaa15103

Mark as read

January 03

- Mesh (SAT) device Northland's SAT 1 has disconnected from the network. Check to see if the device is powered on and still in range of your router. During software updates this is normal behavior and you should wait 5 minutes before taking any action.

Mark as read

2023 December

- A new Galaxy S21 Ultra 5G has connected to the

To View Alerts:

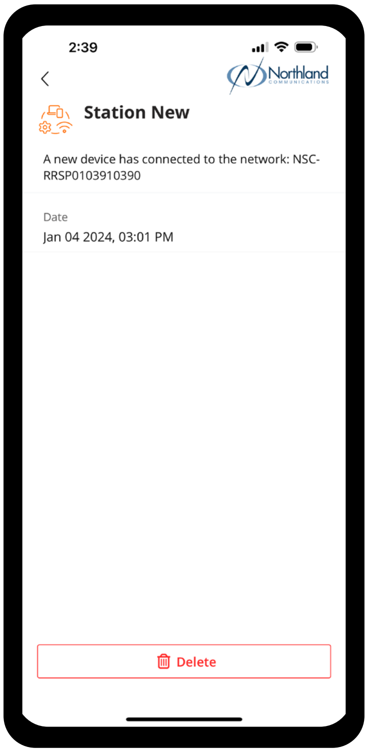
- From the **Home** screen, tap the ***Alerts*** icon.
- Tap an alert in the list to view more information.

To View Specific Alert types:

- From the **Home** screen, tap the ***Alerts*** icon.
- Tap the dropdown next to **All**.
- Tap on the alert type you want to view.

Manage Alerts you want to receive

- In the Alerts Window, tap the Settings icon.
- Toggle on/off the alerts you want to receive.
- To reset the default settings, scroll to the bottom and tap **Reset settings to default**.



2:39

Northland COMMUNICATIONS

Station New

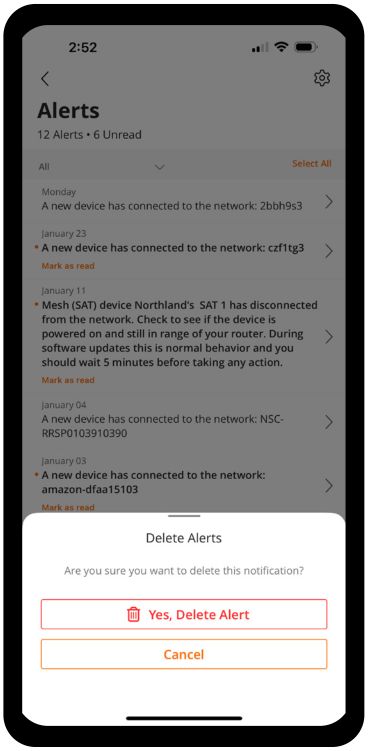
A new device has connected to the network: NSC-RRSP0103910390

Date
Jan 04 2024, 03:01 PM

To Delete An Alert:

- From the **Alert** screen, tap the desired **Alert**.
- Tap the ***Delete*** icon.

- Confirm or cancel your selection on the popup.



2:52

Alerts

12 Alerts • 6 Unread

Monday
A new device has connected to the network: 2bbh9s3

January 23
• A new device has connected to the network: czf1tg3
Mark as read

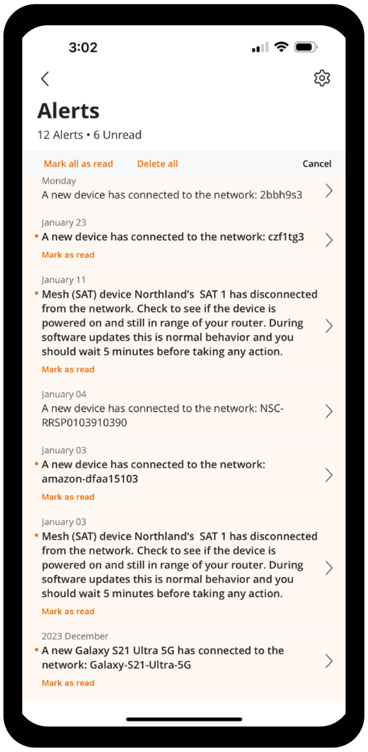
January 11
• Mesh (SAT) device Northland's SAT 1 has disconnected from the network. Check to see if the device is powered on and still in range of your router. During software updates this is normal behavior and you should wait 5 minutes before taking any action.
Mark as read

January 04
A new device has connected to the network: NSC-RRSP0103910390

January 03
• A new device has connected to the network: amazon-dfaa15103
Mark as read

Delete Alerts

Are you sure you want to delete this notification?



3:02

Alerts

12 Alerts • 6 Unread

Mark all as read · Delete all · Cancel

Monday
A new device has connected to the network: 2bbh9s3

January 23
A new device has connected to the network: czf1tg3
Mark as read

January 11
Mesh (SAT) device Northland's SAT 1 has disconnected from the network. Check to see if the device is powered on and still in range of your router. During software updates this is normal behavior and you should wait 5 minutes before taking any action.
Mark as read

January 04
A new device has connected to the network: NSC-RRSP0103910390

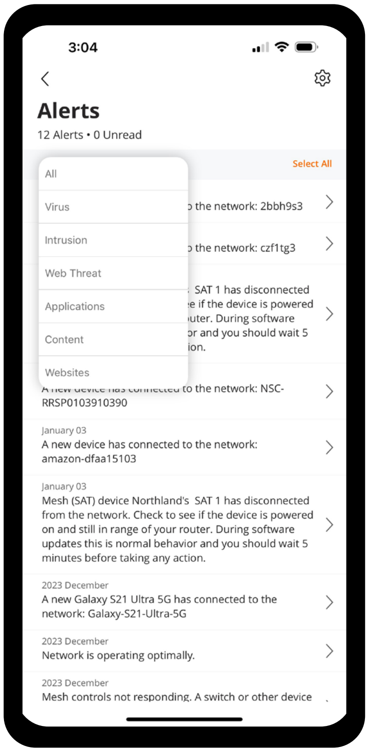
January 03
A new device has connected to the network: amazon-dfaa15103
Mark as read

January 03
Mesh (SAT) device Northland's SAT 1 has disconnected from the network. Check to see if the device is powered on and still in range of your router. During software updates this is normal behavior and you should wait 5 minutes before taking any action.
Mark as read

2023 December
A new Galaxy S21 Ultra 5G has connected to the network: Galaxy-S21-Ultra-5G
Mark as read

To Mass Edit Alerts:

+ On the **Alerts Home** screen, tap **Select All**.
+ Tap either **Mark all as read** or **Delete all**.



3:04

Alerts

12 Alerts • 0 Unread

Select All

o the network: 2bbh9s3

o the network: czf1tg3

SAT 1 has disconnected
e if the device is powered
uter. During software
or and you should wait 5
ion.

to the network: NSC-
RRSP0103910390

January 03
A new device has connected to the network: amazon-dfaa15103

January 03
Mesh (SAT) device Northland's SAT 1 has disconnected from the network. Check to see if the device is powered on and still in range of your router. During software updates this is normal behavior and you should wait 5 minutes before taking any action.

2023 December
A new Galaxy S21 Ultra 5G has connected to the network: Galaxy-S21-Ultra-5G

2023 December
Network is operating optimally.

2023 December
Mesh controls not responding. A switch or other device

To Filter Alerts By Alert Type:

+ On the **Alerts Home** screen, tap **All** to filter the alerts by alert type.

To Manage Commandworx Alert Settings:

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

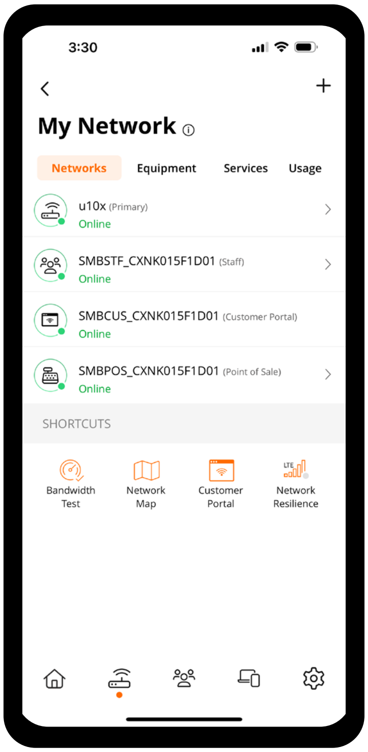
NETWORKS

The Networks section of CommandWorx allows you to view and manage your networks, run speed tests, configure the Wi-Fi Customer Portal, and more.

My Network

The **My Network>Networks** tab shows the status of each wireless network and provides acess to network tools such as Bandwidth Test and the Network Map. You can also enable or disable specific networks, personalize the Customer Portal Wi-Fi, and enable Network Resilience. CommandWorx does not allow you to to create additional networks.

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



u10x (Primary)
Online

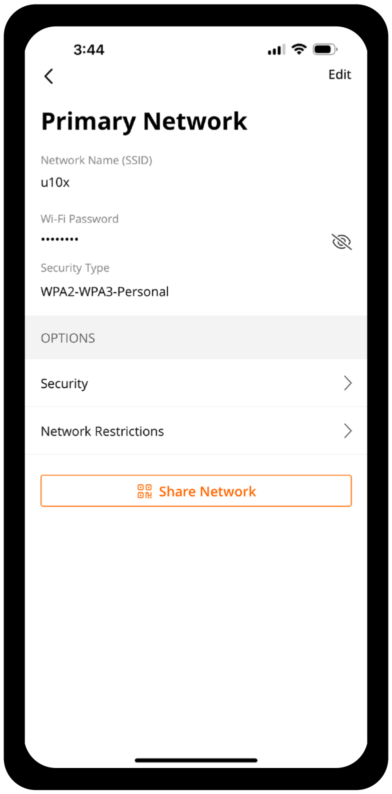
SMBSTF_CXNK015F1D01 (Staff)
Online

SMBCUS_CXNK015F1D01 (Customer Portal)
Online

SMBPOS_CXNK015F1D01 (Point of Sale)
Online

+ From the **My Network>Networks** tab, tap on the desired network.
+ View the network information, edit the network, and share network access.
+ Under the **Options** category, you can manage Security features, Network Restrictions, and Network Hours.

EXAMPLE PRIMARY NETWORK DETAILS



3:44

Edit

Primary Network

Network Name (SSID)
u10x

Wi-Fi Password
••••••••

Security Type
WPA2-WPA3-Personal

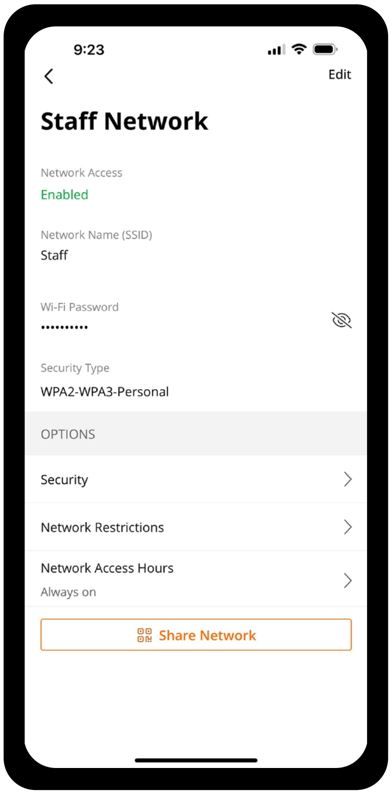
OPTIONS

Security

Network Restrictions

Share Network

EXAMPLE STAFF NETWORK DETAILS



9:23

Edit

Staff Network

Network Access
Enabled

Network Name (SSID)
Staff

Wi-Fi Password
••••••••••

Security Type
WPA2-WPA3-Personal

OPTIONS

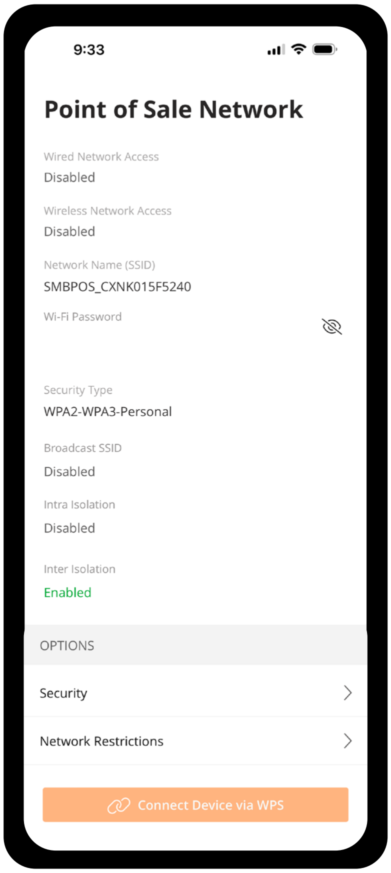
Security

Network Restrictions

Network Access Hours
Always on

Share Network

EXAMPLE POINT OF SALE NETWORK DETAILS



9:33

Point of Sale Network

Wired Network Access
Disabled

Wireless Network Access
Disabled

Network Name (SSID)
SMBPOS_CXNK015F5240

Wi-Fi Password

Security Type
WPA2-WPA3-Personal

Broadcast SSID
Disabled

Intra Isolation
Disabled

Inter Isolation
Enabled

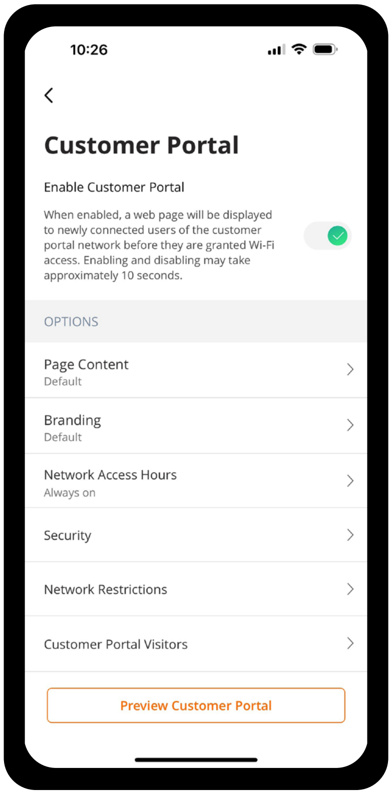
OPTIONS

Security

Network Restrictions

Connect Device via WPS

EXAMPLE CUSTOMER PORTAL DETAILS



10:26

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. Enabling and disabling may take approximately 10 seconds.

OPTIONS

Page Content
Default

Branding
Default

Network Access Hours
Always on

Security

Network Restrictions

Customer Portal Visitors

Preview Customer Portal

Edit A Network

From the **Networks** tab of the **Networks>My Network** screen, you can enable networks and edit a network's SSID and password.

Guidelines:

- The Primary network cannot be disabled.
- You cannot create custom Wi-Fi networks.

To Edit Primary Network Details:

- From the **My Network** screen, tap on the Primary network.
- Tap **Edit**.
- Edit the **Network Name (SSID), Wi-Fi Password** and **Security type** to your preferences.
- Tap **Save**.

To Edit Staff Network Details:

- From the **My Network** screen, tap on the Staff network.
- Tap **Edit**.
- Tap the toggle to enable or disable the Staff network.
- Edit the **Network Name (SSID), Wi-Fi Password**, and **Security Type** to your preferences.

NOTE: You can only change the security type and Wi-Fi password on a network configures for a Shared Password.

To Edit Point Of Sale Network Details:

- From the **My Network** screen, tap on the Point of Sale network.
- Tap **Edit**.
- Tap the toggles to enable or disable wired and wireless access to the Point of Sale network.
- Edit the **Network Name (SSID), Wi-Fi Password**, and **Security Type** to your preferences.
- Tap the Broadcast SSID toggle to enable or disable SSID broadcasting.
- Tap the toggles to enable or disable inter-isolation and intra-isolation settings.
- Tap **Save**.

To Edit Customer Portal Details:

- From the **My Network** screen, tap Customer Portal.
- Tap the toggle to enable or disable the customer network.
- Edit the **Network Name (SSID)** to your preference. You cannot change the security type for this network.
- Edit page content and branding options as desired.
- Tap **Save**.

Share Primary And Staff Network Access

You can share Primary and Staff Wi-Fi network access information with users via the following methods:

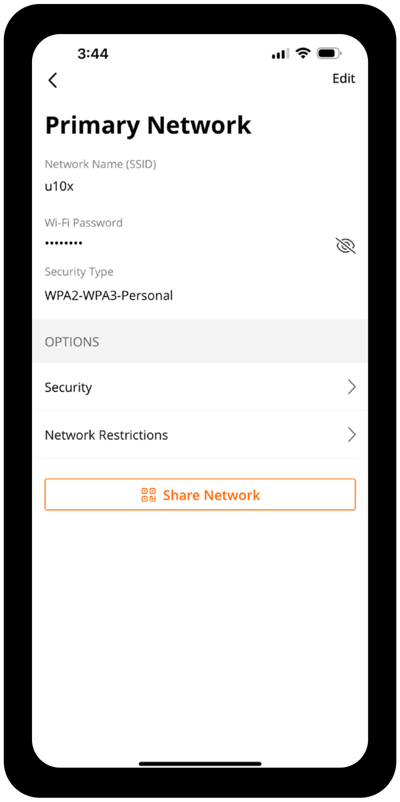
+ QR code: Presents a QR code for the user to scan with their device.
+ Text message: Sends a text message to the user's phone that includes a QR code, links to iOS and Android QR scanner applications, and the Wi-Fi network SSID and passphrase.

Guidelines:

+ The Point of Sale and Customer Wi-Fi network credentials cannot be shared.
+ Staff networks configured for Individual Passwords must be separately shared with each staff profile.

To Share Network Access Via Qr Code:

+ Tap the **Networks** tile on the **Home** screen. Alternately, tap the ***Networks*** icon in the bottom menu bar.
+ Tap on either the Primary or Staff network.
+ Tap **Share Network**.
+ A QR code displays on the screen for the user to scan with their device.



3:44

Edit

Primary Network

Network Name (SSID)
u10x

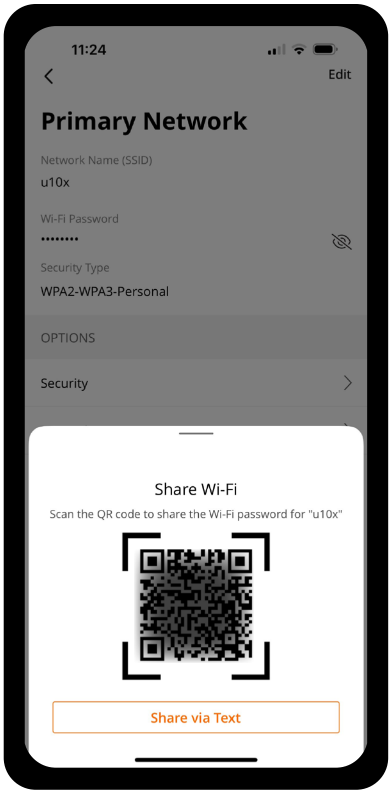
Wi-Fi Password
••••••••

Security Type
WPA2-WPA3-Personal

OPTIONS

Security

Network Restrictions



11:24

Edit

Primary Network

Network Name (SSID)
u10x

Wi-Fi Password
••••••••

Security Type
WPA2-WPA3-Personal

OPTIONS

Security

Share Wi-Fi

Scan the QR code to share the Wi-Fi password for "u10x"

To Share Network Access Via Text Message:

+ Tap the **Networks** tile on the **Home** screen. Alternately, tap the ***Networks*** icon in the bottom menu bar.
+ Tap on the network you want to share.
+ Tap **Share Network**.
+ Tap **Share via Text**.
+ Select the desired contact from your device and send the message.

To Join A Mobile Device To The Network Via Text Message:

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

Connect a Wired or Wireless Device to the Point of Sale Network

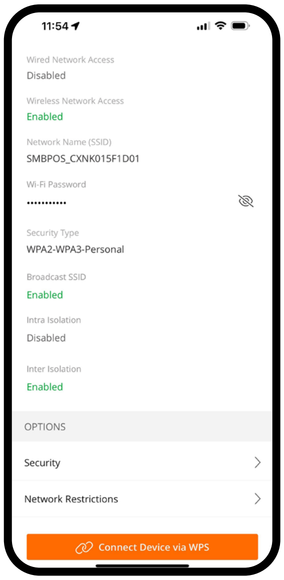
You can connect wired devices to the Point of Sale SSID or wireless devices via WPS.

Guidelines:

+ You can only initiate a WPS connection by tapping the **Connect Device via WPS** button within the app. You cannot press the physical WPS button on the device to initiate a connection.
+ If **Wired Network Access** is disabled, wired PoS devices will automatically join the Primary LAN network.
+ To connect wireless devices via WPS, **Wireless Network Access** must be enabled.
+ If your environment contains wired and wireless devices that must communicate with one another, ensure your Inter/Intra Isolation settings are properly configured.
+ To configure network access and Intra/Inter Isolation settings, see Edit a Network.

To Connect A Wireless Device To The Point Of Sale SSID:

+ From the **Home** screen, tap the **Networks** tile. Alternately, tap the ***Networks*** icon in the bottom menu bar.
+ Tap on the Point of Sale Network.
+ Tap **Connect Device via WPS** to begin a two-minute WPS session.
+ If a connection is not established after two minutes, tap the **Connect Device via WPS** button again to retry.



11:54

Wired Network Access
Disabled

Wireless Network Access
Enabled

Network Name (SSID)
SMBPOS_CXNK015F1D01

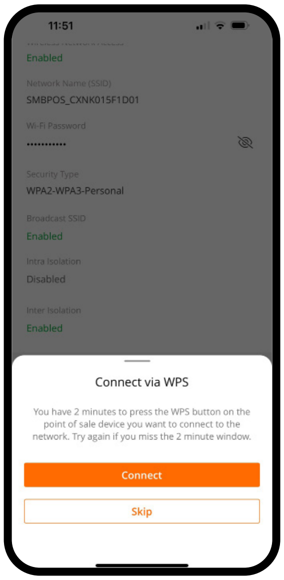
Wi-Fi Password
•••••••••••

Security Type
WPA2-WPA3-Personal

Broadcast SSID
Enabled

Intra Isolation
Disabled

Inter Isolation
Enabled



11:51

Enabled

Network Name (SSID)
SMBPOS_CXNK015F1D01

Wi-Fi Password
•••••••••••

Security Type
WPA2-WPA3-Personal

Broadcast SSID
Enabled

Intra Isolation
Disabled

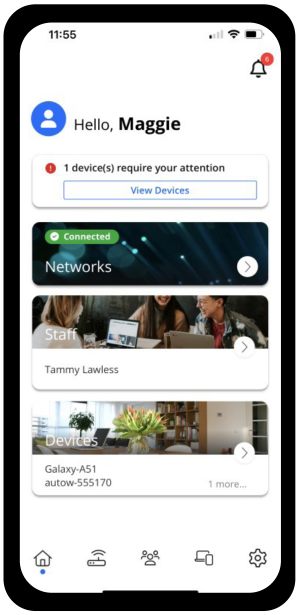
Inter Isolation
Enabled

Connect via WPS

You have 2 minutes to press the WPS button on the point of sale device you want to connect to the network. Try again if you miss the 2 minute window.

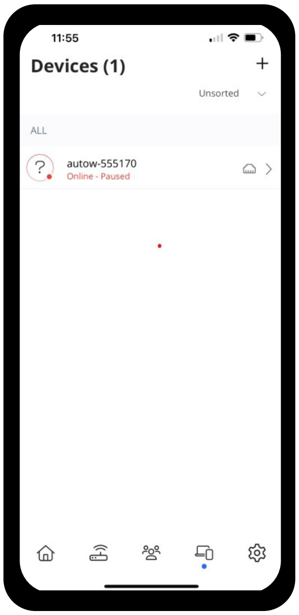
To Connect A Wired Device To The Point Of Sale Network:

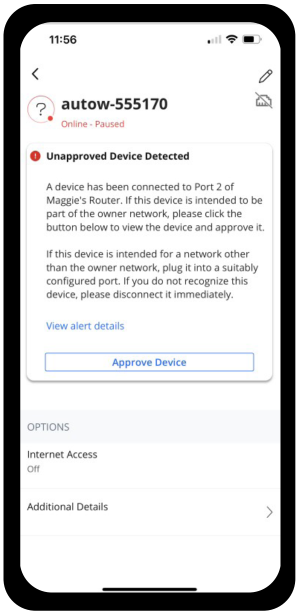
- Enable Wired Device Alerts in the Alerts settings and ensure Wired Network Access is enabled.
- Connect your PoS device to a free LAN port on your SmartBiz Gateway using an Ethernet cord.
- The new connection triggers a security event within the CommandWorx app.
- Tap **View Devices** on the security popup.



1 device(s) require your attention

- With Wired Device Alerts enabled, foreign wired devices remain in a paused state on the network until they are approved by the user. Select the PoS device you would like to connect.





Unapproved Device Detected

A device has been connected to Port 2 of Maggie's Router. If this device is intended to be part of the owner network, please click the button below to view the device and approve it.

If this device is intended for a network other than the owner network, plug it into a suitably configured port. If you do not recognize this device, please disconnect it immediately.

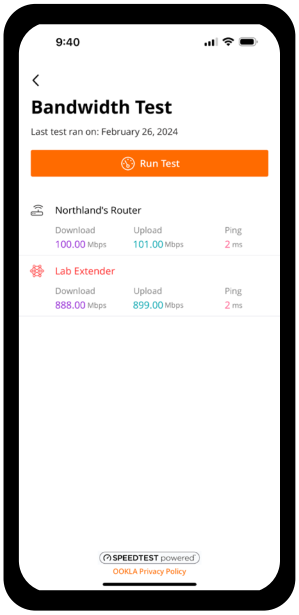
- Review device details to confirm legitimacy. Tap Approve Device and select Okay to confirm successful approval.

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:



9:40

Bandwidth Test

Last test ran on: February 26, 2024

Run Test

Northland's Router

Download	Upload	Ping
100.00 Mbps	101.00 Mbps	2 ms

Lab Extender

Download	Upload	Ping
888.00 Mbps	899.00 Mbps	2 ms

SPEEDTEST powered

OOKLA Privacy Policy

- From the **My Network** screen, tap **Bandwidth Test**.
- Tap **Run Test**.

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

- After the test completes, results for all equipment in the network are displayed.
  - Download Speed
  - Upload Speed
  - Ping Time

- The Run Test button provides visual confirmation that the bandwidth test is in progress.
- Bandwidth testing is capped at 2.5 GBps.

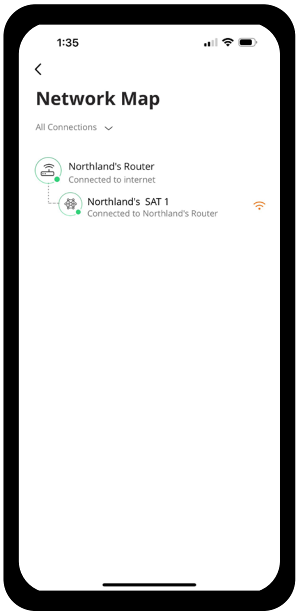
NOTE: Bandwidth testing may not be available in all countries. Check with your service provider for details

NETWORK MAP

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

To view the network map:

- From the Home screen, tap on the **Networks** tile.
- Tap **Network Map**.
- The network map displays the following information:
- The RG and its current connection strength.
- A list of devices connected to the RG.
- The connection type of the devices on the network (Wi-Fi or Ethernet).
- The relative signal strength for each device in the network.


1:35

Network Map

All Connections

Northland's Router
Connected to internet

Northland's SAT 1
Connected to Northland's Router

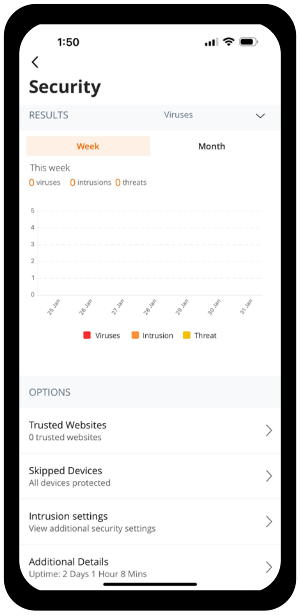
SECURITY

You can manage trusted websites, intrusion settings, and a list of skipped devices for each network.

The Primary network provides virus, intrusion, and threat data for your entire network.

To View Security Data:

- From the Home screen, tap on the **Networks** tile.
- Tap on the **Primary** network.
- Under the options heading, select **Security**.
- Select Week or Month to view historical security data for the selected time period. Filter the results to view virus, intrusion, and threat data.



1:50

Security

RESULTS Viruses

Week Month

This week
0 viruses 0 intrusions 0 threats

🟥 Viruses 🟧 Intrusion 🟨 Threat

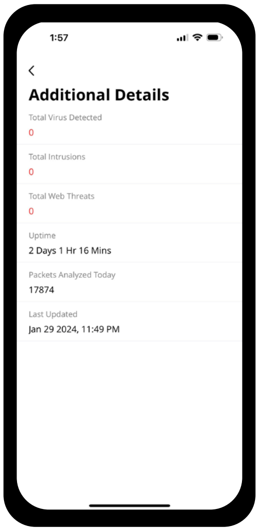
OPTIONS

Trusted Websites
0 trusted websites

Skipped Devices
All devices protected

Intrusion settings
View additional security settings

Additional Details
Uptime: 2 Days 1 Hour 8 Mins


1:57

Additional Details

Total Virus Detected
0

Total Intrusions
0

Total Web Threats
0

Uptime
2 Days 1 Hr 16 Mins

Packets Analyzed Today
17874

Last Updated
Jan 29 2024, 11:49 PM

- Tap Additional Details to view more detailed security information, including the total number of detected viruses, intrusions, and threats.

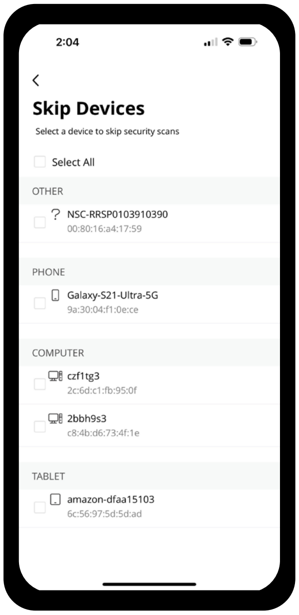
NOTE: Results do not include security events encountered on public networks.

Skipped 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 the learned device to the appropriate category so that network traffic coming to or from the device is no longer scanned again by ProtectIQ. Configure Skipped Devices on the Primary network.

To skip security scans:

+ From the Networks screen, select the **Primary** network and tap **Security**.
+ Tap **Skipped Devices**.
+ A list of network devices displays.



2:04

Skip Devices

Select a device to skip security scans

□ Select All

OTHER

□ ? NSC-RRSP0103910390 00:80:16:a4:17:59

PHONE

□ Galaxy-S21-Ultra-5G 9a:30:04:f1:0e:ce

COMPUTER

□ czf1tg3 2c:6d:c1:fb:95:0f

□ 2bbh9s3 c8:4b:d6:73:4f:1e

TABLET

□ amazon-dfaa15103 6c:56:97:5d:5d:ad

+ Tap the device of interest and select OK. You can revert this configuration at any time by tapping the device name once more.

NOTE: Intrusion settings continue to scan skipped devices.

Intrusion Settings

You can enable or disable Intrusion Prevention System (IPS) settings for each network profile.

From the Networks tab, select the network of interest and navigate to Security > Intrusion Settings.

Intrusion settings are handled by two security options in ProtectIQ:

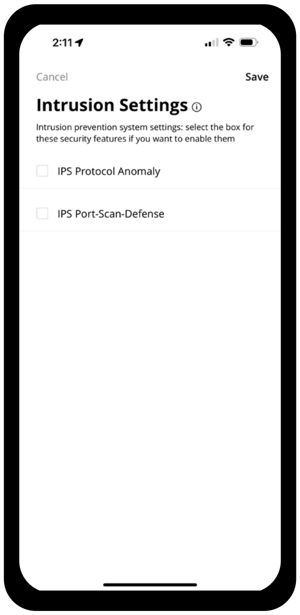
- IPS Protocol Anomaly is used for detecting both network and computer intrusions and potential misuse by monitoring system activity and classifying traffic as either normal or anomalous. To identify attacking kind of traffic, the system learns what normal traffic looks like and applies the protocol anomaly feature as needed.

  IPS 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 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.
  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



Cancel Save

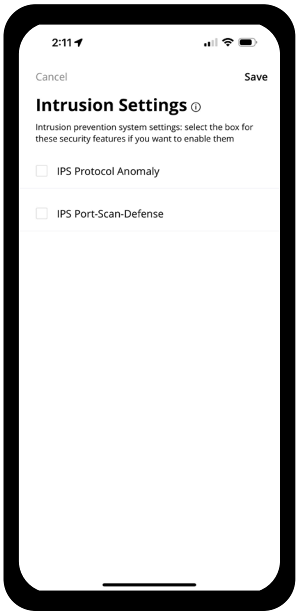
Intrusion Settings ⓘ

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 ⓘ icon.



2:11

Cancel 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

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.

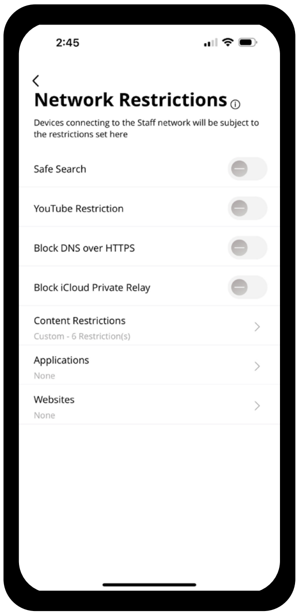
Port scans monitor the GigaSpire WAN interface, LAN ports, and Wi-Fi.

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 CommandWorx.

Network Restrictions



2:45

Network 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
Custom - 6 Restriction(s)

Applications
None

Websites
None

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 CommandWorx. 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 Google Chrome™, Microsoft Edge®, and Mozilla 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.

CommandWorx supports blocking iCloud Private Relay. This triggers the VPN notification in CommandWorx 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

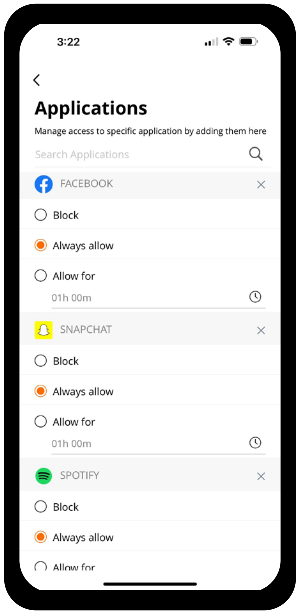
There are a couple of different ways in determining whether these filters are in effect:

Within CommandWorx, from Networks > Default Restrictions, tap the Safe Search and YouTube Restriction toggles to ensure the current algorithms are in effect.
Users can validate the settings for identified devices within a given profile by surfing to the following locations:
YouTube: https://www.youtube.com/check_content_restrictions - Tap the LEARN MORE link for instructions.
SafeSearch: https://www.google.com/preferences
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.

To Configure Content Restrictions:

+ From the **Network Restrictions** tab, select **Content Restrictions**.
+ Adjust the content sliders to customize restrictions, or select an age group filter.
  + To apply age group specific filtering, select the appropriate group from the menu:
    - No Restrictions
    - Very Restrictive
    - Moderately Restrictive
    - Mildly Restrictive
    - Custom
  + The content restrictions update based on your selection. Scroll down and check the content types are filtered.



3:22

Applications

Manage access to specific application by adding them here

Search Applications

FACEBOOK ×

○ Block

● Always allow

○ Allow for

01h 00m

SNAPCHAT ×

○ Block

● Always allow

○ Allow for

01h 00m

SPOTIFY ×

○ Block

● Always allow

○ Allow for

To Configure Application Restrictions:

+ From the **Network Restrictions** tab, select **Applications**.
+ Begin typing the name of the app. The system auto-completes the word you are typing. When a match is found, select the app.
+ After the application is displayed, choose whether you want to block the app.

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

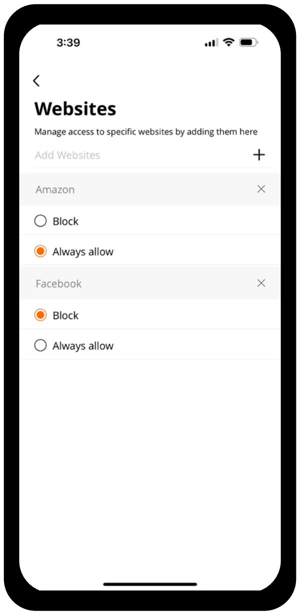
+ Continue adding applications until done.

GigaSpire BLAST safety features provide website security alerts.

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

Conversely, you can block content from any website.

CommandWorx displays sites or services based on security notifications.



3:39

Websites

Manage access to specific websites by adding them here

Add Websites +

Amazon ×

○ Block

● Always allow

Facebook ×

● Block

○ Always allow

To Configure Website Restrictions:

+ From the **Home** screen, tap on the **Networks** tile.
+ Tap on the network of interest.
+ Select **Network Restrictions > Websites**.
+ Enter the website URL and tap the ***Plus*** icon.
+ Tap **Block** or **Always allow** to filter this specific website.

Customer Portal Wi-Fi

From the **Networks > Customer Portal** screen, you can enable and personalize the web page that is presented to your customers when they access your customer wireless network. You can upload a cover photo, enter welcome text, and change the page background and font color to match your brand. When enabled, the Customer Portal prompts customers to enter their name and email address and to accept your terms of use before they can join the network.

The Customer Portal screen provides access to the following settings:

+ **Page Content:** Enter welcome text, upload a cover photo, customize button text, and link the Terms of Use.
+ **Branding:** Upload a company logo and change the page background and font colors to match your business's brand.
+ **Network Access Hours:** Specify the days and hours the customer Wi-Fi network provides internet access to customers. You can allow unrestricted access, apply the same time limit to every day of the week, disable internet for an entire day, or create a custom hourly schedule for each day. After you set a schedule, the customer network only provides internet access on the selected days and within the specified hours.
+ **Security:** View virus, intrusion, threat data, and manage intrusion settings. See Security for more information.
+ **Network Restrictions:** Configure content, application, and website restriction settings. See Network Restrictions for more information.
+ **Customer Portal Visitors:** Set a retention period (1, 15, 30, 60, or 90 days) for visitors' login information. During the retention period, returning visitors may connect to the customer SSID without re-authenticating. After the retention period expires, all visitors are required to re-enter their name and email address. The default retention period is 30 days.

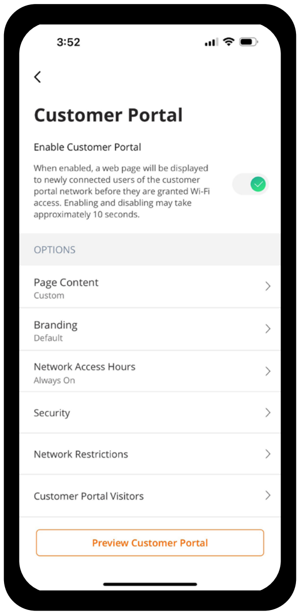
Sample custom schedule:

+ Sunday: No access
+ Saturday: 9:00am-12:00pm
+ Monday, Wednesday, Friday: 8:00am-11:30am, 1:00pm-6:00pm
+ Tuesday, Thursday: 10:00am-4:00pm.

NOTE: A customer portal visitors log in information will be stored for a designated period of time. You can receive an email containing a CSV file of the unique visitors that have connected to the captive portal network.
See [View Customer Portal Details]

To Enable the Customer Portal:

+ Go to **Networks > Customer Portal**.
+ Tap the Enable Customer Portal toggle to enable (turn the toggle green).
+ Proceed to customize page content, configure branding options, and select login retention options.



3:52

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. Enabling and disabling may take approximately 10 seconds.

OPTIONS

Page Content
Custom

Branding
Default

Network Access Hours
Always On

Security

Network Restrictions

Customer Portal Visitors

Preview Customer Portal

To Personalize Customer Portal Page Content:

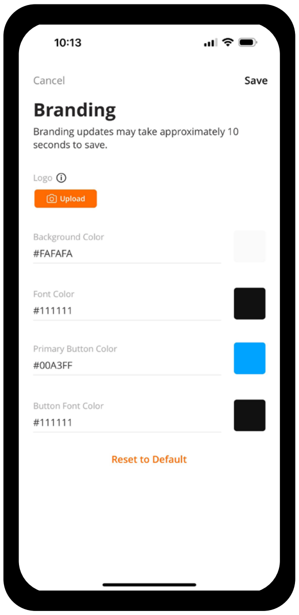
+ From the **Customer Portal** screen, tap **Page Content**.
+ Enter a **Network Name (SSID)**.
+ Enter a **Page Heading**.
+ Tap **Upload** to select a cover photo from your device.
+ **Login Requirements:** Tap Email, First Name, Last Name to require visitors to log in, or Tap none if a log in is not required.d.
+ **Terms of Service**
  Enter the URL for your terms and conditions into the **Terms of Service** text box or choose Text Only and enter the Terms of Service in the text box.

NOTE: If using a URL, your Terms of Service page should be a simple HTML page that contains only text. Pages with too much formatting or too many images do not load.

+ Enter the Button Text (e.g., Connect, Join).
+ Tap **Save**.
+ To see how the Customer Portal page appears to your customers, tap **Preview Customer Portal**.

To Configure Customer Portal Branding:

From the Customer Portal screen, tap Branding.
Tap **Upload** to select a logo image from your device.
Select the **Background Color, Font Color, Primary Button Color**, and **Button Font Color**:



Branding

Branding updates may take approximately 10 seconds to save.

Logo

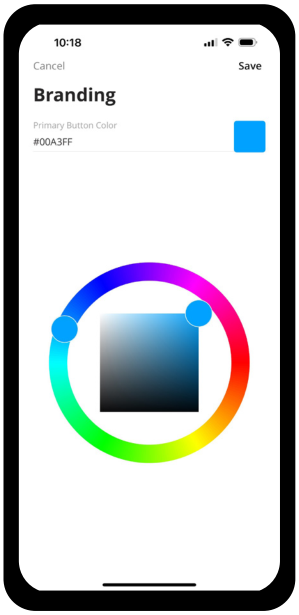
Background Color #FAFAFA

Font Color #111111

Primary Button Color #00A3FF

Button Font Color #111111

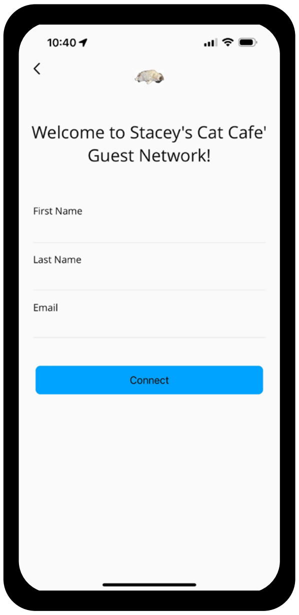
+ Tap on the color ring to select a color.
+ Tap on the square to select the color shade.
+ Tap **Save**.



Branding

Primary Button Color #00A3FF

+ Tap **Save**.
  To see how the customer portal page appears to your customers, tap **Preview Customer Portal**.



Welcome to Stacey's Cat Cafe' Guest Network!

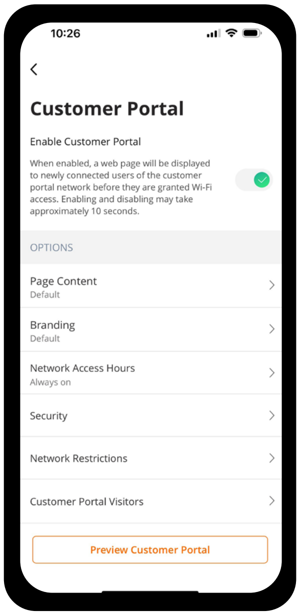
First Name

Last Name

Email

To View Customer Portal Details:

- From the **Home** screen, tap the **Networks** tile. Alternately, tap the ***Networks*** icon in the bottom menu bar.
- Tap on the **Customer Portal** in the bottom.



10:26

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. Enabling and disabling may take approximately 10 seconds.

OPTIONS

Page Content
Default

Branding
Default

Network Access Hours
Always on

Security

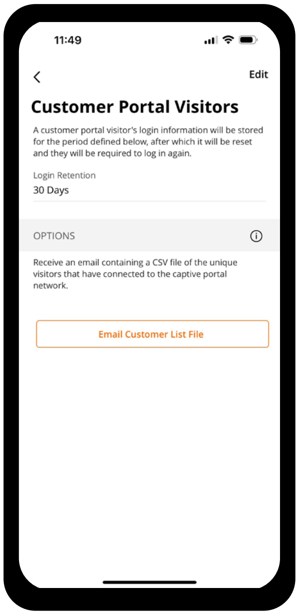
Network Restrictions

Customer Portal Visitors

Preview Customer Portal

- Tap **Customer Portal Visitors.**
- Tap **Email Customer List.**

A response shows the email has been sent to the email address associated with SmartBiz.



11:49

Edit

Customer Portal Visitors

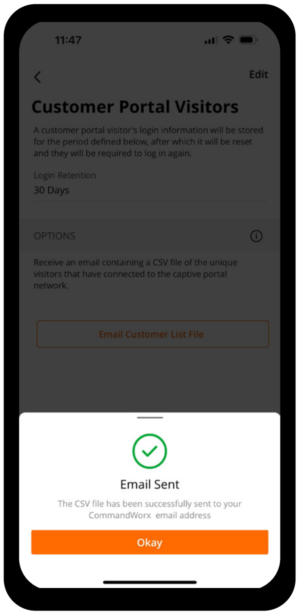
A customer portal visitor's login information will be stored for the period defined below, after which it will be reset and they will be required to log in again.

Login Retention
30 Days

OPTIONS

Receive an email containing a CSV file of the unique visitors that have connected to the captive portal network.

Email Customer List File



11:47

Edit

Customer Portal Visitors

A customer portal visitor's login information will be stored for the period defined below, after which it will be reset and they will be required to log in again.

Login Retention
30 Days

OPTIONS

Receive an email containing a CSV file of the unique visitors that have connected to the captive portal network.

Email Customer List File

Email Sent

The CSV file has been successfully sent to your CommandWorx email address

Okay

Network Access Hours

You can set time limits for the customer and staff networks. Access to these networks is confined to the configured time parameters.

To Configure Network Access Hours:

From the Networks screen, tap the Customer or Staff network and select Network Access Hours.

+ Select a schedule option from the drop-down menu:
  + **Always On** (Default)
  + **Every Day**
    - Tap on the **Start Time** and **End Time** fields to select the start and end times. (When Every Day is chosen)
  + **Custom**
    - Tap on a day. (When Customer is Chosen)
    - Tap **+ Add Time Limit**.
    - Tap on the **Start Time** and **End Time** fields to select the start and end times.
    - Tap **Submit**.
    - Add additional time limits to the day, if desired.
    - Repeat for the remaining days.
    - Tap **Save**.

To Set Login Retention Settings:

This is how long a customer's log in information remains in the system before they are asked to log in again.

+ From the Customer Portal screen, tap **Customer Portal Visitors**.
+ Tap **Edit**.
+ Select a login retention period from the drop-down menu.
+ Tap **Save**.

Network Resilience

From the **Network Resilience screen,** you can select a mobile device (phone or tablet) to provide cellular/LTE service as a backup internet connection in case of an internet service disruption. You can also select which network(s) may use the back-up connection to ensure uninterrupted flow of business-critical traffic. After Network Resilience is enabled, devices on the selected network(s) automatically use the cellular/LTE network after the primary WAN loses internet connectivity.

Guidelines:

+ The Primary and Point of Sale networks are enabled by default.
+ Only the CommandWorx System Administrator can enable and configure Network Resilience.

To Configure Network Resilience:

+ Go to **Networks > Network Resilience**.
+ Tap the **Enable Network Resilience** toggle to enable (turn the toggle green).
  Your BLAST router automatically detects nearby mobile hotspots.
+ Tap the ***Refresh*** icon if the desired hotspot does not appear.

Add Equipment

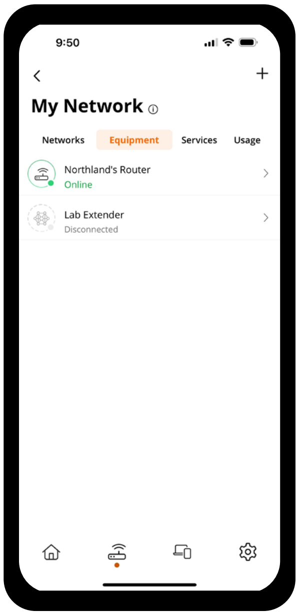
You can add up to 4 mesh satellites to your network from the My Network screen.

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:

- From the Home screen, tap on the **My Network** tile.
- Tap the plus sign and select **Add Equipment**.
- The **Add Mesh(SAT)** screen opens.
- 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.
- Tap **Next**.
- Enter a Name for the device.
- 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.



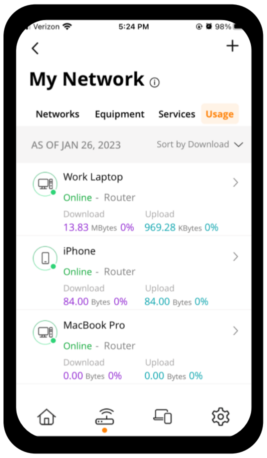
Device Usage

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

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

To View Device Usage:

+ Go to the **My Network > Usage** screen.
  The following usage statistics display for each device:
  + Device name
  + Device connection status (Online/Offline)
  + Router the device is connected to
  + Download and Upload usage
  + Download and upload percent usage for each device



Verizon 5:24 PM 98%

My Network ⓘ

Networks | Equipment | Services | Usage

AS OF JAN 26, 2023 — Sort by Download

Work Laptop
Online - Router
Download 13.83 MBytes 0% — Upload 969.28 KBytes 0%

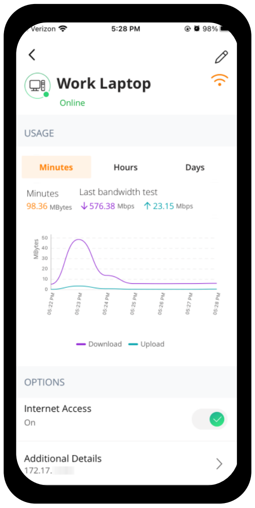
iPhone
Online - Router
Download 84.00 Bytes 0% — Upload 84.00 Bytes 0%

MacBook Pro
Online - Router
Download 0.00 Bytes 0% — Upload 0.00 Bytes 0%

+ Tap on a device to view additional details.
  + Device type (e.g., Phone, Computer)
  + Device name
  + Connection status (Online, Offline)
  + 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.



Verizon 5:28 PM 98%

Work Laptop
Online

USAGE

Minutes | Hours | Days

Minutes 98.36 MBytes — Last bandwidth test ↓576.38 Mbps ↑23.15 Mbps

OPTIONS

Internet Access
On

Additional Details
172.17.[redacted]

OPTIONS

+ Internet Access (On, Off)
NOTE: See the Manage 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

STAFF

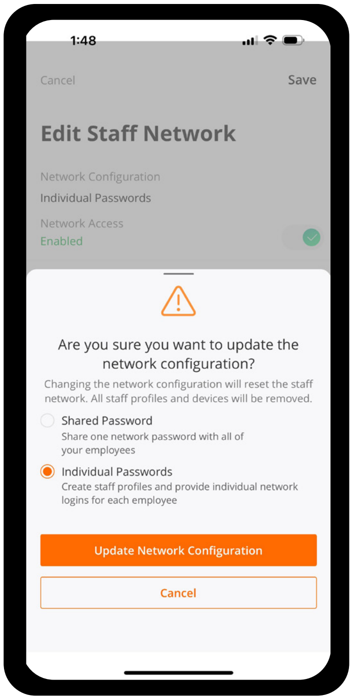
The Staff section of CommandWorx allows you to manage access to the Staff Wi-Fi. You can add, edit, or remove employees from the Staff network as well as set time and content restrictions..

To access the Staff section, tap the ***Staff*** icon in the bottom menu bar.

Individual/Shared Passwords

CommandWorx supports two staff network configurations:

Use the **Shared Password** configuration to share one network password with all of your employees.
Use **Individual Passwords** to create staff profiles, provide individual network logins for each employee, and manage devices associated with each employee.



1:48

Cancel Save

Edit Staff Network

Network Configuration
Individual Passwords

Network Access
Enabled

Are you sure you want to update the network configuration?

Changing the network configuration will reset the staff network. All staff profiles and devices will be removed.

○ Shared Password
Share one network password with all of your employees

● Individual Passwords
Create staff profiles and provide individual network logins for each employee

Update Network Configuration

Cancel

To Edit The Staff Network Configuration:

+ From the **My Network** screen, tap your Staff network.
+ Tap the ***Edit*** icon in the upper corner to enter the **Edit Staff Network** screen.
+ Select **Change Staff Network Configuration** and the desired configuration.
+ Update and save your changes.

NOTE: Updating the network configuration deletes all staff profiles and associated devices. You must recreate these profiles and reactivate your devices upon update.

Add/Remove Staff

If your Staff network supports individual passwords, you can configure staff profiles to customize access to the network.

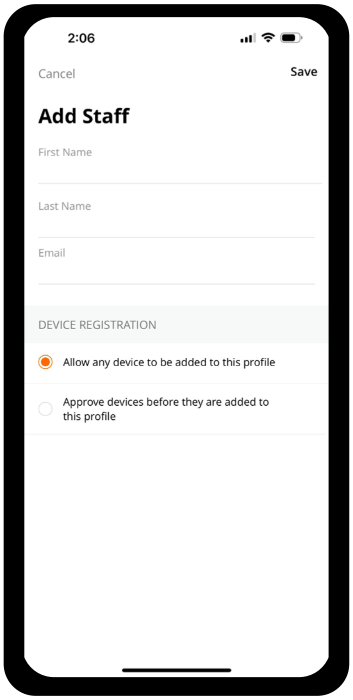
CommandWorx supports two staff profile configurations:

High-trust profile: Employee may associate any device to their profile and join the network.
Low-trust profile: New device requests must be approved in the CommandWorx app before joining the network.

To Add A Staff Profile:

+ From the Staff tab on the bottom menu, tap the ***Plus*** icon at the top of the screen.
+ Tap the profile avatar to add a profile image and enter a name and email address.
+ Choose a profile trust level to control device filtering. This can be changed at a later time.
+ Save the profile.

NOTE: CommandWorx currently supports up to 20 staff profiles.



Add Staff

First Name

Last Name

Email

DEVICE REGISTRATION

● Allow any device to be added to this profile

○ Approve devices before they are added to this profile

To Remove A Staff Profile:

+ From the Staff tab on the bottom screen, select the desired profile.
+ Tap **Edit** in the upper corner.
+ Select **Delete Staff** and confirm your selection.

NOTE: Because individual passwords are unique to each staff profile, Calix recommends you promptly delete obsolete staff profiles and create new staff profiles for incoming hires. Tap the profile avatar to add a profile image and enter a name and email address.

+ Choose a profile trust level to control device filtering. This can be changed at a later time.
+ Save the profile.

NOTE: CommandWorx currently supports up to 20 staff profiles.

To Turn Internet Access on/off:

You can temporarily turn a staff members internet access off.

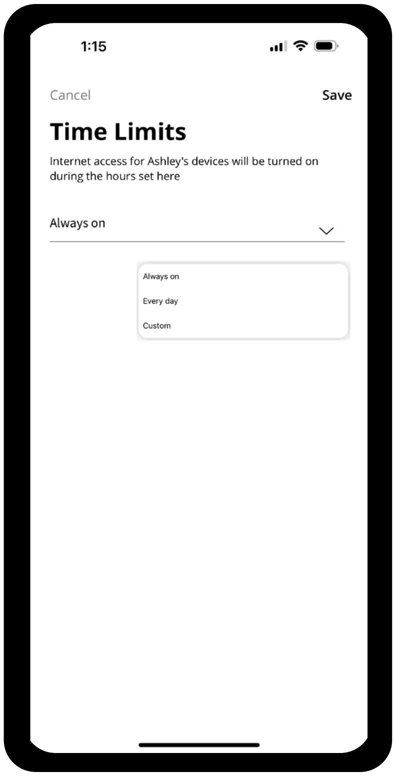
+ From the Staff tab on the bottom screen, select the desired profile.
+ Toggle Internet Access to off

NOTE: You will need to toggle internet access to on again when ready.

Create Staff Time Limits

Once you have added a staff profile, you can set up time limits based on the staff member's hours/days of the week.

+ From the Staff tab on the bottom screen, select the desired profile.
+ Select **Time Limits**
+ **Select one of the following:**
  Always on: The internet will remain accessible to that staff member 24/7.
  Every Day: The internet will be accessible 7 days and you will be prompted to enter time parameters.
  Custom: You will be prompted to select both days of the week and times of the day for the internet to be accessible for tht staff member.
+ When finished, tap **Save**.



Time Limits

Internet access for Ashley's devices will be turned on during the hours set here

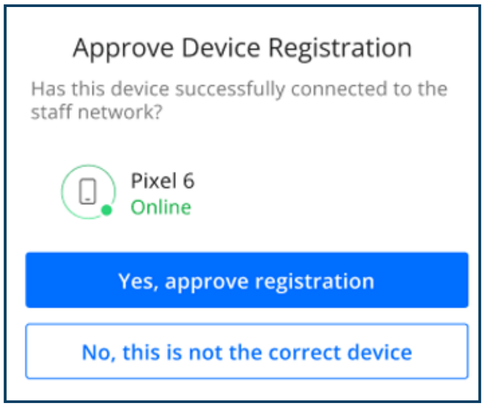
Always on

Activate/Deactivate Staff Devices

Once you have added a staff profile, you can register devices to that profile.

To Activate A Device For High-Trust Profile:

+ From the Staff tab on the bottom menu, select a staff profile.
+ Tap **Share Network** and scan or text the QR code to the appropriate device.
+ Tap **Join** on the device pop-up.
+ Confirm connection on the new device.



Approve Device Registration

Has this device successfully connected to the staff network?

Pixel 6
Online

To Activate A Device For A Low-Trust Profile:

+ From the Staff tab on the bottom menu, select a staff profile.
+ Tap **Register Device(s)** and scan or text the QR code to the appropriate device.
NOTE: This code expires after 2 minutes. If no devices are added within this time, you must select **Register Device(s)** to restart the registration process.
+ Tap **Join** on the device pop-up.
+ Respond to the alert within the CommandWorx app.
+ Confirm connection on the new device.
NOTE: You can add up to 3 devices per staff profile.

To Deactivate A Device From The Network:

+ From the Staff tab on the bottom menu, select a staff profile.
+ Select the desired device.
+ Tap **Unregister and Remove This Device.**
+ Confirm the device no longer appears in the staff profile.

Edit Staff Information

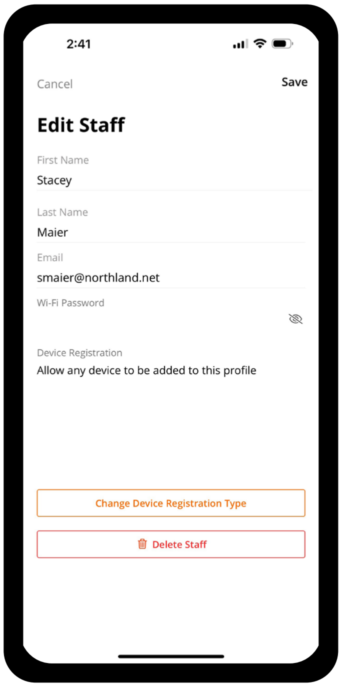
You can edit staff information, view individual network passwords, and change device registration settings from the Edit Staff page.

To Edit Employee Information:

+ From the Staff tab on the bottom menu, tap a staff profile.
+ Tap **Edit** in the upper corner of the screen.
+ Edit the desired fields or change the staff profile image by tapping the ***Blue Avatar*** icon. You can change the profile trust level by selecting **Change Device Registration Type**.

NOTE: Changing the device registration type deletes all devices associated with the staff profile. You must register all desired devices to associate them with the staff profile.

+ Save your changes.



Edit Staff

First Name
Stacey

Last Name
Maier

Email
smaier@northland.net

Wi-Fi Password

Device Registration
Allow any device to be added to this profile

Content Restrictions

You can configure content restrictions specific to your staff network. Refer to the Security page for more information on Intrusion Settings, Network Restrictions, and setting Network Access Hours.

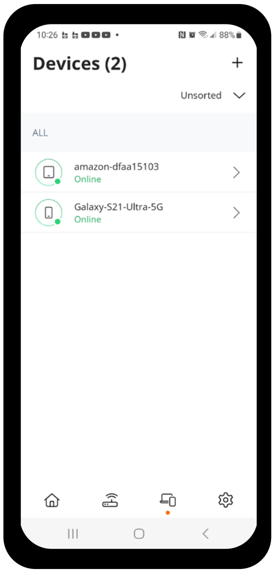
DEVICES

The **Devices** screen stores information on all components connected to the network. Each device 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. Listed devices can be sorted by Type, People, and Place.

View Devices

To View Devices:

- Tap the ***Devices*** icon in the bottom menu bar. Alternately, tap the **Devices** tile on the Home screen.
- The list of devices connected to your network displays.



10:26 88%

Devices (2) +

Unsorted

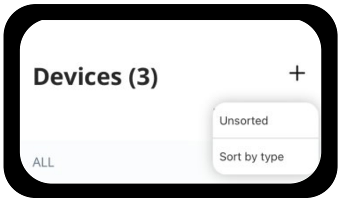
ALL

amazon-dfaa15103
Online

Galaxy-S21-Ultra-5G
Online

To View Devices by Type:

- Tap the ***plus*** sign.
- Tap **Sort by type**.



Devices (3) +

Unsorted

Sort by type

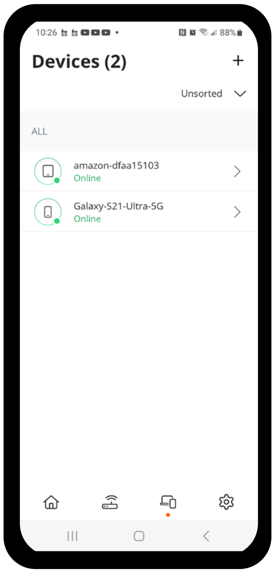
ALL

The following information displays:

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

USAGE

- Speed test results
- Total data usage
- Download speed
- Upload speed
- Select a time frame to view data for the previous three minutes, the previous six hours, or the previous seven days.



10:26 88%

Devices (2) +

Unsorted

ALL

amazon-dfaa15103
Online

Galaxy-S21-Ultra-5G
Online

CONFIGURATION

Internet Access (On, Off)
NOTE: See the Manage 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
  + Wireless protocol
  + Efficiency
  + Radio band
  + Channel
  + Device IP address
  + Device MAC address
  + Device vendor
  + Device model

Add A Device

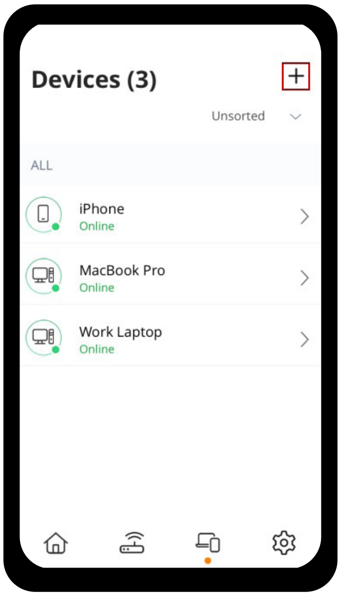
You can add devices to the Primary or Point of Sale networks by either connecting the device to the wireless SSID or connecting via WPS.

Guidelines

- To connect a wireless device to the Point of Sale network via wireless SSID, the Broadcast SSID feature must be enabled. See Edit a Network for more information.
- If you would like to add a wired point of sale device, see Connect a Wired or Wireless Point of Sale Device for more information.
- You can only add devices to the Primary or Point of Sale networks via the Devices screen. To add devices to the Staff network, see Activate/Deactivate Staff Devices

To add a device by connecting to the wireless SSID:

- Tap the ***Devices*** icon in the bottom menu bar. Alternately, tap the **Devices** tile from the **Home** Screen.
- Tap the ***plus*** sign.
- Select the desired network.
- Connect the device to the network using the provided SSID and password. After the device connects to the network, it appears in the Devices list.



Devices (3)

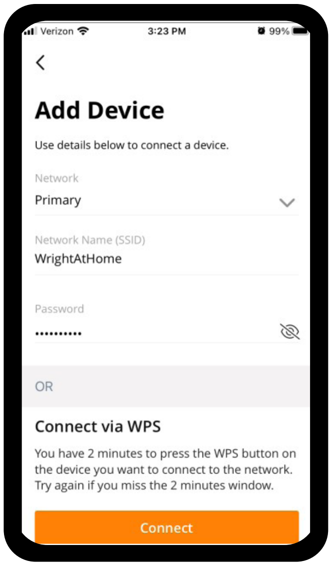
Unsorted

ALL

iPhone
Online

MacBook Pro
Online

Work Laptop
Online



Verizon 3:23 PM 99%

Add Device

Use details below to connect a device.

Network
Primary

Network Name (SSID)
WrightAtHome

Password
••••••••••

OR

Connect via WPS

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.

Connect

To add a device via WPS:

- Tap the ***Devices*** icon in the bottom menu bar. Alternately, tap the **Devices** tile from the **Home** screen.
- Tap the ***plus*** sign.
- Tap the Connect button on the bottom of the screen to begin a two-minute WPS session. The device to be connected listens for a signal from the network and continues to try to connect. If a connection is not established within two minutes, tap the Connect button again to retry.

Edit A Device

From the **Devices** screen, you can edit a device's name.

To Edit a Device:

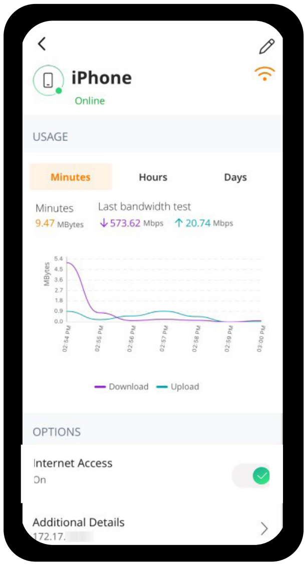
- Tap the ***Devices*** icon in the bottom menu bar. Alternately, tap the **Devices** tile from the **Home** Screen.
- Tap the desired device.
- Tap the ***Pencil*** icon to view the device details.
- Tap **Save**.
- Tap **Cancel** to return to the **Devices** Screen.

Manage Internet Access for a Device

CommandWorx allows you to prevent devices on your network from accessing the internet. After you disable internet access for a device, the device can still connect to network SSIDs but will not be able to access the internet. Internet access

To Disable Internet Access for a Device:

- Tap the Devices tile on the Home screen. Alternately, tap the Devices icon in the bottom menu bar.
- Tap on the desired device.
- Tap the Internet Access toggle to turn internet access On (green) or Off.



iPhone
Online

USAGE

Minutes | Hours | Days

Minutes 9.47 MBytes
Last bandwidth test ↓573.62 Mbps ↑20.74 Mbps

OPTIONS

Internet Access
On

Additional Details
172.17.

SETTINGS

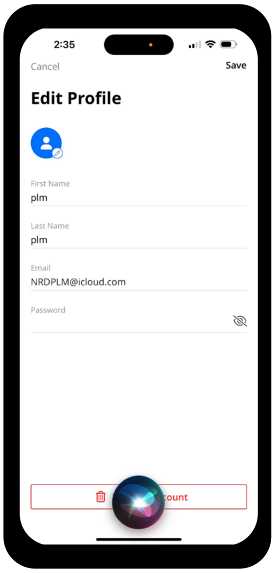
From the **Settings** menu, you can modify and personalize app settings and your home broadband Wi-Fi experience. The Settings menu is accessible directly from the bottom menu bar.

To View Selection Options on the Settings Tab:

+ From the **Home** screen, tap the ***Settings*** icon in the bottom menu bar.
+ 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:** CommandWorx 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:** CommandWorx 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 CommandWorx 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 CommandWorx app on the About screen as well as the current CommandWorx release version.
  + **Log out:** Tap the Log out button to log out from the CommandWorx app.

Accounts and Admins

From **Settings > Account and Admins**, the account admin can edit or delete their account, invite a secondary admin to the network, and delete the secondary admin account.



Edit Profile

First Name
plm

Last Name
plm

Email
NRDPLM@icloud.com

Password

To Update the Primary CommandWorx User Account:

+ Navigate to **Settings > Account and Admins.**
+ To update the profile image, tap the ***Profile*** icon to select a new image from your photo library.
+ Update the first name, last name, email address, and password fields as necessary.
  + The email address used to log into CommandWorx, established during the initial setup, can be changed at any time. Selec this item to modify the app login password.
  + The password to log into CommandWorx that you established during the 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.

To Invite A Secondary Admin:

+ Navigate to **Settings > Account and Admins**.
+ Tap **Invite Admin**.
+ 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.

+ Tap **Send Invite**. An email is sent to the secondary account with a link to create the password. After the email is sent, the secondary account status switches to Pending until the Invitee accepts.
  After the user creates their password, the account status changes to Activated in CommandWorx.

NOTE: Each network allows only a single secondary account.

To Delete The Primary Account:

On occasion, the account that manages the SmartBiz hotspot or its satellites must be reset (deleted).

+ Navigate to **Settings > Account and Admins**.
+ Tap **Edit**.
+ Tap **Remove Account**.
  A warning message displays ensuring that you do not inadvertently remove this account.
+ Tap **Yes, Remove**.

CommandWorx removes the account and deletes all account information, including routers and mesh systems, 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.

To Delete The Secondary Account As The Primary Admin:

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

To Delete The Secondary Account As The Secondary Admin:

The secondary account user may also delete their own account.

- Go to **Settings > Account and Admins**.
- Tap **Edit**.
- Tap **Delete**.
- Confirm the deletion.

Set Passcode

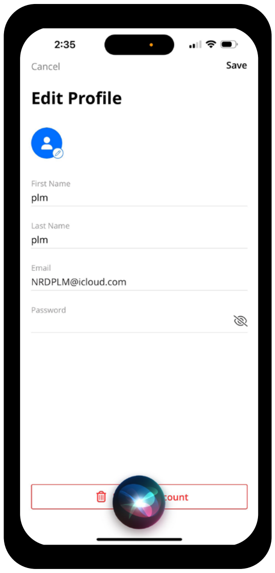
CommandWorx supports the optional use of a numeric Personal Identification Number (PIN) to log into the app, in lieu of an alphanumeric password. If you prefer to use a PIN code instead of a password for login, you can establish a PIN code from the Set Passcode screen.

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 CommandWorx app to resume use.

To Set Passcode For Login:

- Navigate to **Settings > Set Passcode**.
- Tap into the **Type New PIN** field and type to enter a PIN code (up to six digits in length).
- Tap into the **Confirm PIN** field and re-type the PIN code to confirm a match.
- 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



Edit Profile

First Name
plm

Last Name
plm

Email
NRDPLM@icloud.com

Password

Enable Biometric Login

To Enable Biometric Login:

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

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

To Reset A Passcode:

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

To Disable Passcode Login:

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

Language

To Enable Biometric Login:

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

To Change the Language:

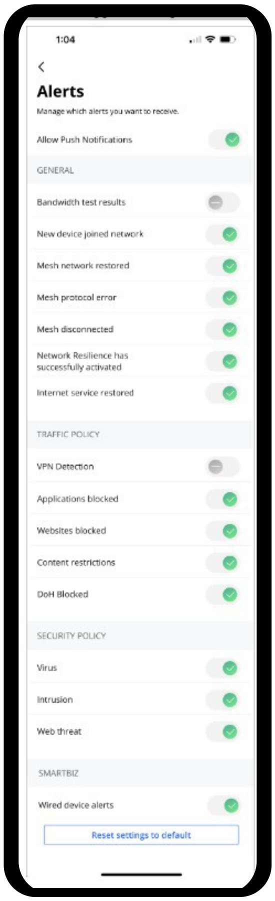
+ Navigate to **Settings > Language**.
+ Tap on your desired language:
  + English (default)
  + French Canadian
+ Tap **Save**. The screen text throughout the app changes to the selected language.

Alerts

CommandWorx can notify users for events on the Primary, Staff, and Point of Sale networks. 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 by-passing 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 CommandWorx.



1:04

Alerts

Manage which alerts you want to receive.

Allow Push Notifications	✓
GENERAL	
Bandwidth test results	○
New device joined network	✓
Mesh network restored	✓
Mesh protocol error	✓
Mesh disconnected	✓
Network Resilience has successfully activated	✓
Internet service restored	✓
TRAFFIC POLICY	
VPN Detection	○
Applications blocked	✓
Websites blocked	✓
Content restrictions	✓
DoH Blocked	✓
SECURITY POLICY	
Virus	✓
Intrusion	✓
Web threat	✓
SMARTBIZ	
Wired device alerts	✓

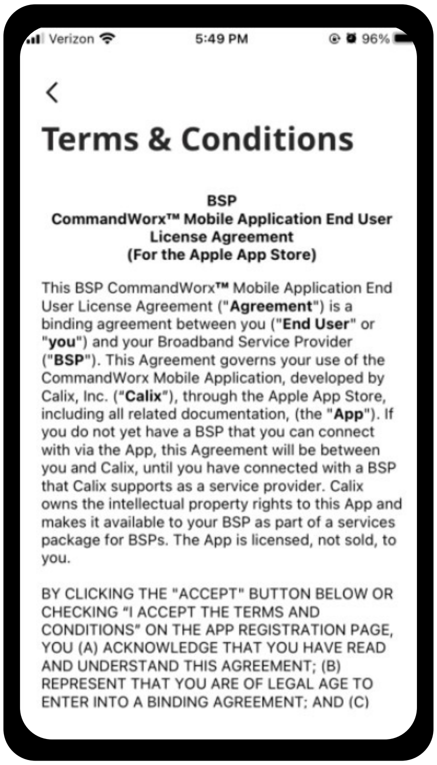
To Edit Alert Settings:

- From the **Home** screen, tap the ***Alerts*** icon.
- Tap the ***Settings*** icon. Alternately, navigate to **Settings > Alerts**.
- Select the toggle to enable or disable alert push notifications on your device.
- Select the toggle to configure alert settings for CommandWorx network activity.
- You can revert to default settings by tapping the ***Reset settings to default*** icon.

Terms & Conditions

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



Terms & Conditions

BSP
CommandWorx™ Mobile Application End User License Agreement
(For the Apple App Store)

This BSP CommandWorx™ Mobile Application End User License Agreement ("**Agreement**") is a binding agreement between you ("**End User**" or "**you**") and your Broadband Service Provider ("**BSP**"). This Agreement governs your use of the CommandWorx Mobile Application, developed by Calix, Inc. ("**Calix**"), through the Apple App Store, including all related documentation, (the "**App**"). If you do not yet have a BSP that you can connect with via the App, this Agreement will be between you and Calix, until you have connected with a BSP that Calix supports as a service provider. Calix owns the intellectual property rights to this App and makes it available to your BSP as part of a services package for BSPs. The App is licensed, not sold, to you.

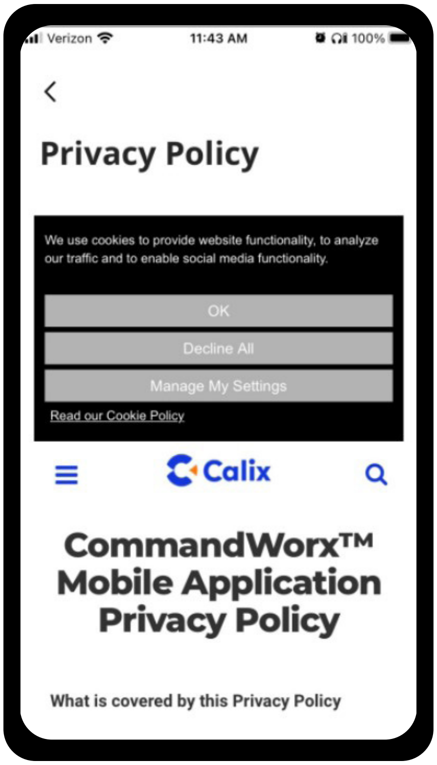
BY CLICKING THE "ACCEPT" BUTTON BELOW OR CHECKING "I ACCEPT THE TERMS AND CONDITIONS" ON THE APP REGISTRATION PAGE, YOU (A) ACKNOWLEDGE THAT YOU HAVE READ AND UNDERSTAND THIS AGREEMENT; (B) REPRESENT THAT YOU ARE OF LEGAL AGE TO ENTER INTO A BINDING AGREEMENT; AND (C)

To View the App's Terms and Conditions:

+ Navigate to Settings > Terms & Conditions.
+ 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 CommandWorx app.



Privacy Policy

We use cookies to provide website functionality, to analyze our traffic and to enable social media functionality.

OK

Decline All

Manage My Settings

Read our Cookie Policy

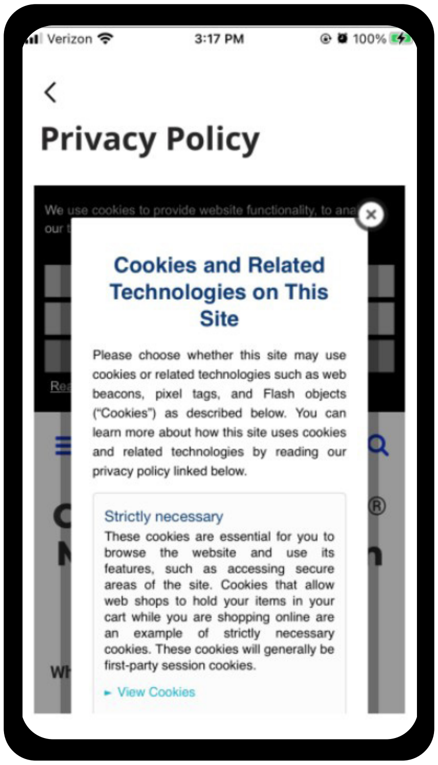
Calix

CommandWorx™ Mobile Application Privacy Policy

What is covered by this Privacy Policy

To view the Calix Privacy Policy:

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



Privacy Policy

We use cookies to provide website functionality, to ana

Cookies and Related Technologies on This Site

Please choose whether this site may use cookies or related technologies such as web beacons, pixel tags, and Flash objects ("Cookies") as described below. You can learn more about how this site uses cookies and related technologies by reading our privacy policy linked below.

Strictly necessary

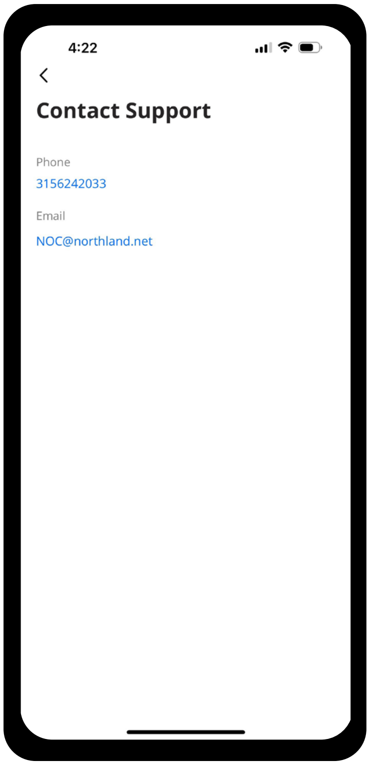
These cookies are essential for you to browse the website and use its features, such as accessing secure areas of the site. Cookies that allow web shops to hold your items in your cart while you are shopping online are an example of strictly necessary cookies. These cookies will generally be first-party session cookies.

▸ View Cookies

+ A brief summary of how cookies are handled in CommandWorx.
+ If you agree, tap **Agree and Proceed**.
+ Tap **View Cookie Settings** to make further changes.

Contact Support

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



Contact Support

Phone
3156242033

Email
NOC@northland.net

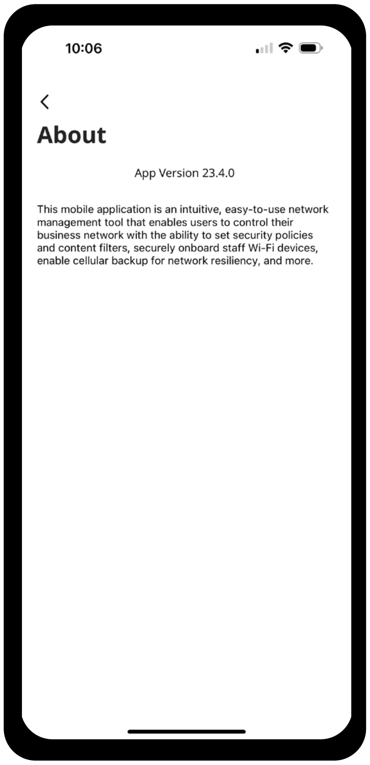
To view the Contact Support Information:

The following information is displayed.

+ Northland Communications Support Telephone Number.
+ Northland Communications Support Email Address.

Contact Support

The About screen shows the developer's description of CommandWorx.



About

App Version 23.4.0

This mobile application is an intuitive, easy-to-use network management tool that enables users to control their business network with the ability to set security policies and content filters, securely onboard staff Wi-Fi devices, enable cellular backup for network resiliency, and more.