

## NETWORK RESILIENCE

Network Resilience ensures business critical devices remain connected, even in the event of an unexpected outage.

- To enable, tap Network, then tap the Network Resilience Shortcut.
- Tap the toggle to enable Network Resilience
- Tap Select Failover Device SSID and select the hotspot name of the cellular or dedicated hotspot device. The device must be on and discoverable.
- Enter the hotspot password.
- Check the terms box.
- Tap Connect to Hotspot.
- You will be notified when the connection is successful.
- Select which business-critical networks will connect to the hotspot in the event of an outage.

## NETWORK RESTRICTIONS

Built-in content restrictions can boost staff productivity and reduce liability by restricting distracting or dangerous internet content. Create a better customer and work experience by limiting content that may be objectionable to other patrons or staff members. Restrictions are customizable for each network and for individual staff members.

- Tap Network from the Home screen.
- Select the desired network.
- Select Network Restrictions in Options.
- Select Content Restrictions to restrict access to content categories.
- Select Applications to block specific applications or add time limits on the staff network.
- Select Websites to block specific websites.

## NETWORK ACCESS HOURS

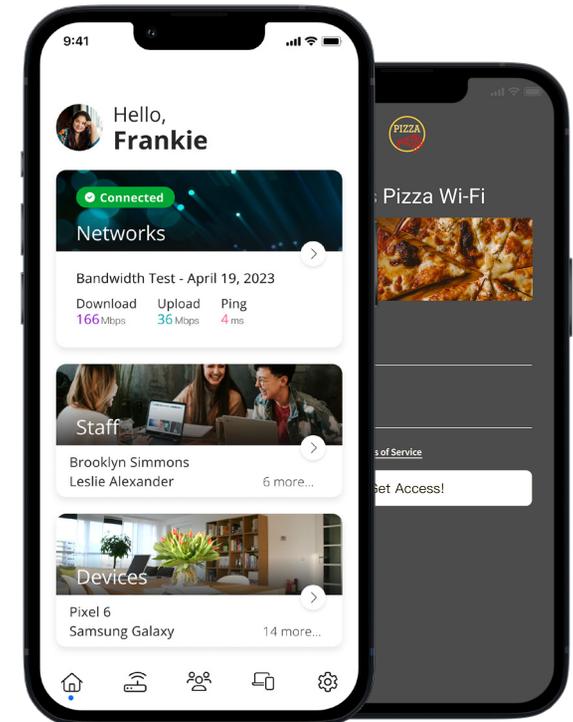
You may set hours and days that WiFi access is available for customer and staff networks.

### Customer Portal Access Hours

- Select Networks. Select Customer Portal in Shortcuts.
- Select Network Access Hours in Options.
- Select Every Day to set a start and end time for all days of the week.
- Select Custom to create custom start and end times or turn access off for specific days of the week.

### Staff Network Access Hours

- If the Staff Network is configured with a single shared password, select Network Access Hours in Options.
- Select Every Day to set a start and end time for all days of the week that apply to all staff members.
- Select Custom to create custom start and end times or turn access off for specific days of the week for all staff members.
- If Staff Network is configured with individual passwords, select the individual staff member in the Staff tile from the Home screen. Set access hours for each staff member as desired.



Visit [goctc.com/smartbiz](https://goctc.com/smartbiz) for additional information, how-to videos, and FAQs.



**CommandWorx**  
Quick Start Guide



## SMARTBIZ NETWORKS

Easily set up and manage up to four business specific networks. Each dedicated network is protected with business-class cybersecurity and may be customized with restrictions and more.

### Primary Network Set Up

- Tap Network from the Home screen.
- Tap the plus sign.
- Select the desired network.
- Enter the Network Name (SSID).
- Enter a secure WiFi password.
- Tap Options to customize and view security and Network Restriction options.
- Click Save.

### Point of Sale Network Set Up

- Tap Network from the Home screen.
- Tap the plus sign.
- Select the desired network.
- Enter the Network Name (SSID).
- Enter a secure WiFi password.
- Tap Options to customize and view security and Network Restriction options.
- Follow steps 1 through 6 above.
- To connect wireless point of sale (POS) devices, enable Wireless Network Access. To enhance business security, the POS network does not broadcast the POS SSID. Tap Edit and enable Broadcast SSID to connect a wireless POS device or tap Connect Device via WPS (WiFi Protected Setup) to connect a POS device that requires WPS connectivity.
- Contact your service provider to assist with connecting wired POS devices.

## STAFF NETWORK

Protect your business by connecting staff to an isolated and protected network. Boost productivity with network access hours and content restrictions.

- Tap Network from the Home screen.
- Tap the plus sign.
- Select Staff network.
- Select Staff Network Configuration. See details below.

### Shared Password for Staff

- Select Shared Password to create one password all staff members will share to access the Staff Network.
- Add a secure password.
- Customize Options which will apply to all staff members.

### Individual Passwords for Staff

- Select Individual Passwords to maximize efficiency with staff changes, security and customization.
- Customize Options that apply to entire staff network.
- Tap the Home icon.
- Tap the Staff tile on the Home screen.
- Tap the plus sign to add a staff member(s).
- Add the first name, last name and email address.
- Select the Device Registration Type.
- Click Save.
- Customize Options for the staff member.
- To remove a staff member, select the staff member, tap Edit and and select Delete Staff.

## CUSTOMER PORTAL

Deliver a better customer experience, capture marketing contacts and attract new customers via a brandable customer WiFi portal.

- Tap Network from the Home screen.
- Tap Customer Portal in Shortcuts.
- Tap the toggle to enable the Customer Portal
- Tap Page Content to customize the WiFi splash page.
- Enter the Network Name, Page Heading, upload a cover photo.
- Select Login Requirements. Select name and email address if you wish to be able to view a list of users of your customer portal.
- Select URL or Text, then add your terms of service for using your customer WiFi.
- Enter the Button Text, such as "Connect".
- Click Save.
- Tap Branding.
- Upload your logos or an image and add colors.
- Click Save.
- Tap Preview Customer Portal to view your Splash page. Edit as desired following the steps above.
- Set Network Access Hours (see instructions on back panel).
- Add Network Restrictions to block objectionable content or applications.
- Tap Customer Portal Visitors to select the Login Retention Period. Login Retention Period indicates how often the customer will need to re-enter their information to connect and how data will be stored.
- Tap Email Customer List File to send a list of unique visitors over the login retention period to your CommandWorx email address.