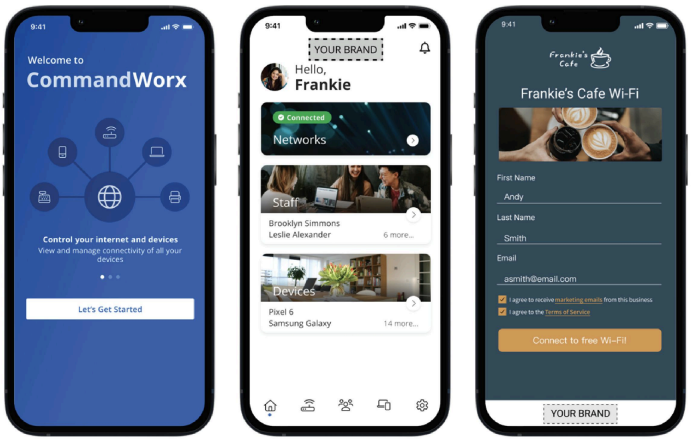
Wyverd Fiber SmartBiz Guide

CommandWorx™ Mobile Phone App

CommandWorx is a self-service mobile app that enables small business owners to monitor and manage network and device administration duties from anywhere. Business owners can easily set up and share WiFi networks, create a branded customer WiFi portal, receive security and content alerts, manage staff profiles and device access, invite a secondary admin, and more.



Dedicated Primary, Staff, Point-of-Sale, and Customer Networks

SmartBiz enables business owners to easily set up and manage up to four business persona-defined networks that are relevant for many small businesses. Business owners can configure these networks themselves using CommandWorx. Each dedicated network is isolated with customizable security and content restrictions, keeping business-critical traffic — such as point-of-sale transactions — separate from any other network traffic.

Designed for the Small Business

The Calix small business platform software — referred to as SmartBizWorx™ — transforms GigaSpire and GigaPro WiFi systems into a small business networking and business productivity solution. The integrated SmartBiz™ solution includes:

- SmartBizWorx™ software bundle
- CommandWorx™ mobile phone app
- Dedicated Primary, Point-of-Sale, Staff, and Customer networks
- Optional custom networks
- Staff management
- Mesh WiFi controller
- Network security
- Content restrictions
- Small business-branded Customer Portal
- Network resilience

Primary Network

The Primary network should be used for business devices — computers, cameras, phone systems — that are installed, secured, and maintained by the business managers.

- SSID with shared password (SPSK: single pre-shared key)
- All LAN ports on the Calix WiFi gateway system serve the Primary network by default
  - When *Wired Network Access* is enabled, both Primary and Point-of-Sale wired devices will require manual approval through CommandWorx when first connected
- All WiFi and LAN connected devices are connected to a full layer-2 bridge and able to access other devices only on the Primary network

Point-of-Sale Network

The Point-of-Sale (POS) network is available as a dedicated network for the business POS systems. Network isolation enables small businesses to maintain compliance (e.g., the Payment Card Industry Data Security Standard (PCI DSS) used to secure credit card transactions).

- Single SSID with password authentication (SPSK)
- LAN ports can be assigned to the Point-of-Sale network through Service Cloud
  - When *Wired Network Access* is enabled, both Primary and Point-of-Sale wired devices will require manual approval through CommandWorx when first connected
- All devices on the POS network are connected to a full layer-2 bridge and able to access other devices on the POS network by default
  - Optionally, all devices on the network can be isolated from each other by enabling Intra-Isolation
- Supports Soft-WPS (WiFi Protected Setup) POS device pairing using CommandWorx

Staff Network

This is a dedicated network for employees with workstations, business systems, or personal devices.

- SSID with shared password (SPSK: single pre-shared key) or unique per-employee password (MPSK: multi pre-shared key)
- LAN ports cannot be assigned to the Staff network
- All devices on the Staff network are connected to a full layer-2 bridge and able to access other devices on the Staff network
- SSID can be automatically enabled and disabled via scheduling *Network Access Hours*

Customer Portal Network

The dedicated customer network is an isolated WiFi network for customers of the small business to access the Internet while visiting the small business.

- SSID with locally hosted Customer Portal for network access
- All devices on the Customer network are connected to a full layer-2 bridge but are not able to access other devices on the Customer network
- SSID can be automatically enabled and disabled via scheduling *Network Access Hours*

Mesh WiFi Controller

WiFi is an essential service for small businesses, contributing to employee productivity and creating an enjoyable customer experience. The integrated WiFi controller provides an exceptional experience for the small business.

Controller capabilities include:

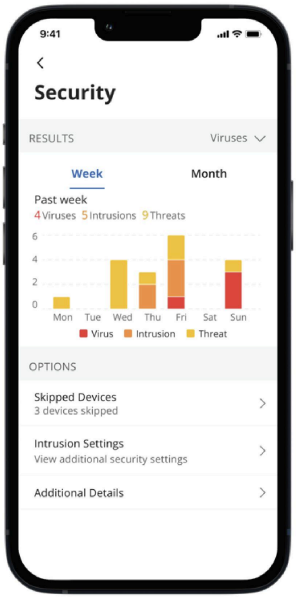
- Dynamic channel and band selection
- Client band and node steering
- Support for DFS channels
- Star topology
- Wired and wireless mesh satellite access points
- Up to 8 mesh satellites can be controlled by the gateway WiFi controller
- No more than 2-deep subtended APs (Gateway > Mesh > Mesh)

Alert Notifications

Network Security, Content Restriction, Network Resilience, and Wired Device alerts give business owners insight into various activities on their network. Alerts are sent through CommandWorx and provide detailed information about the activity. The business owner can customize which types of alerts they want to receive.

Network Security

SmartBiz Network Security protects businesses from cyberattacks and costly downtime. The integrated firewall blocks unauthorized traffic, malicious websites, and provides protection from viruses and intrusions.



Key capabilities include:

- Malicious website protection, anti-virus, and intrusion prevention
- Combines local database of signatures and cloud-based signatures
- Automatically blocks suspicious traffic
- Network Security is always enabled for the entire business and all networks
- Network Security settings can be adjusted on a per-network basis
- Owner will receive Network Security alerts through CommandWorx for devices on the Primary, Point-of-Sale, and Staff networks

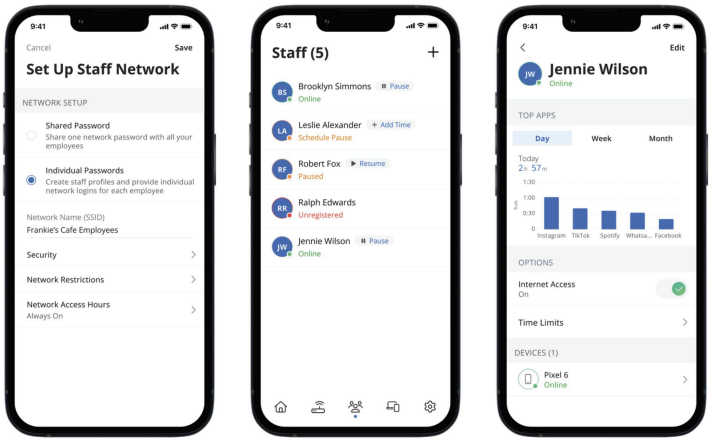
Content Restrictions

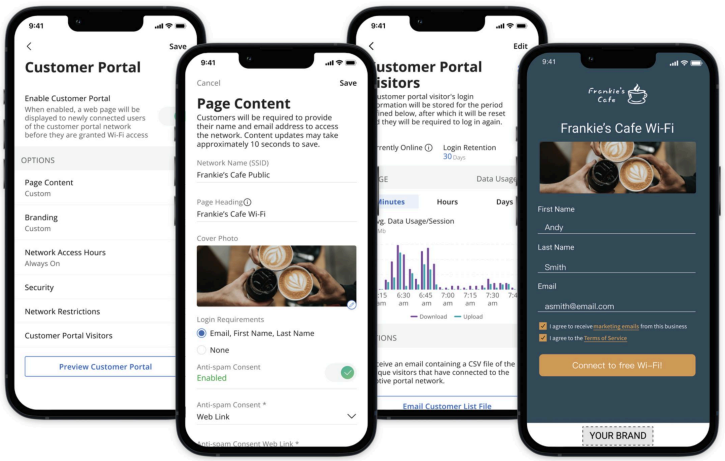
Small business owners can easily customize and apply content restrictions for each of their networks. Content restrictions provide business owners peace of mind by protecting their business, staff, and customers from inappropriate or harmful content.

Staff Onboarding and Management

Employees can be onboarded onto the Staff WiFi network using CommandWorx, enabling improved network security and productivity. When business owners choose to use individual passwords (MPSK), they have more granular control over content restrictions, Internet access, and device management.

Staff device registration can be designated as "Allow any device to be added to this profile" (high trust) or "Approve devices before they are added to this profile" (high control). Removing a staff member profile will automatically revoke network access for only their associated devices. Up to 50 staff profiles can be created, and when designated as *high control*, that employee will be limited to 3 devices.



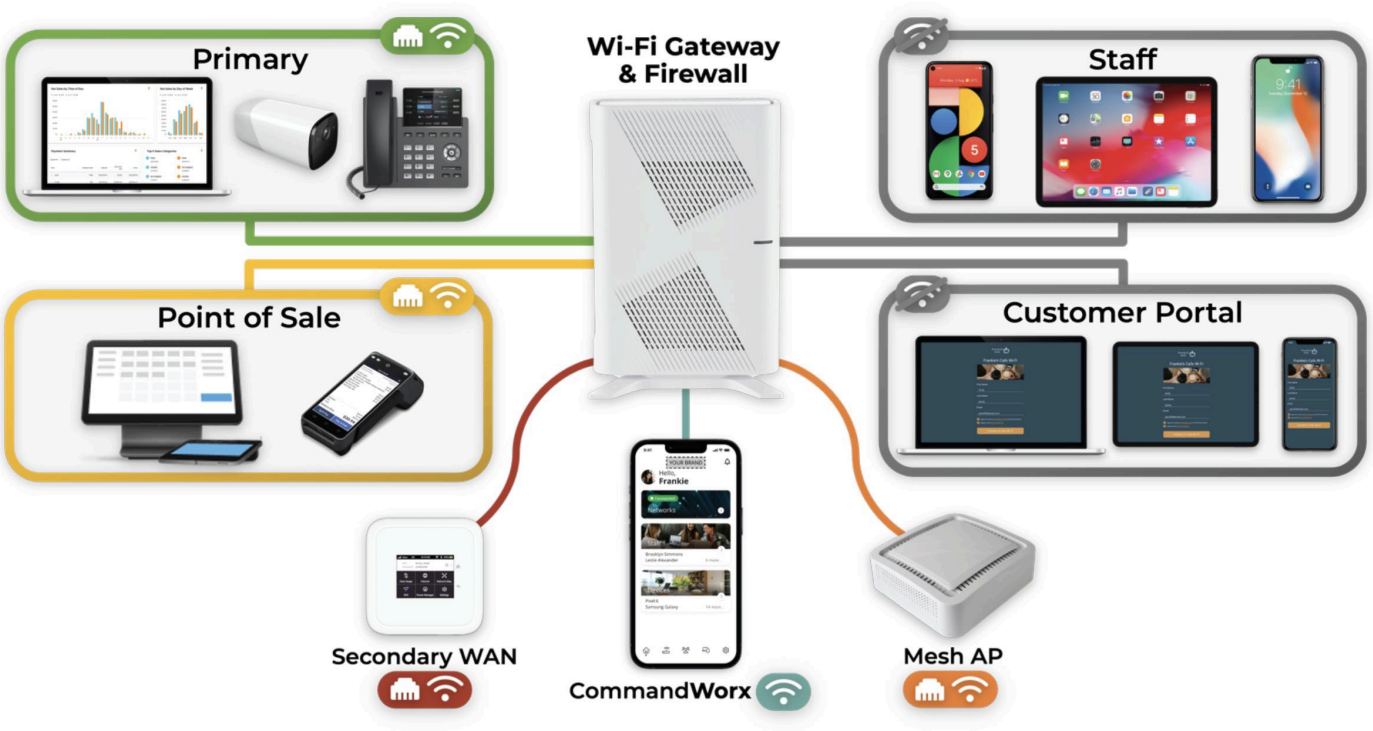


Small Business-Branded Customer Portal

Using the CommandWorx mobile app, each business owner can create and customize a splash page that will be presented when customers connect to the Customer Portal WiFi network. By default, if a customer returns to the business within 30 days, reauthentication in the Customer Portal is not required. Business owners can set security policies to block access to malicious websites, set time-based access restrictions, and access built-in analytics to review aggregate session length and network usage of their visitors. The business owner can export the guest list to their registered email, which can be used for marketing campaigns such as targeted ads.

Network Resilience

Ensuring business-critical systems stay online, such as POS systems, is critical for small business success. In the event of an outside disruption, SmartBiz offers the ability to handoff traffic to a backup device, such as the owner's mobile phone, a standalone hotspot, or a secondary wired connection. Wireless-based Network Resilience is enabled and configured by the business owner through CommandWorx.



To prevent lockout and ensure business continuity, the Primary and Point-of-Sale networks are always selected and cannot be disabled. The business owner can configure which other networks — Staff and/or Customer — will be allowed to use the backup connection. They will also receive alerts in CommandWorx when Network Resilience is activated and after the primary WAN is restored.

Wyyerd Fiber does not provide a backup solution. It is the responsibility of the business to have a backup device in place, should they wish to maintain connectivity in the event of an outside disruption.