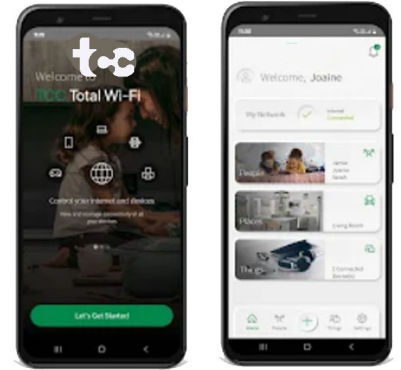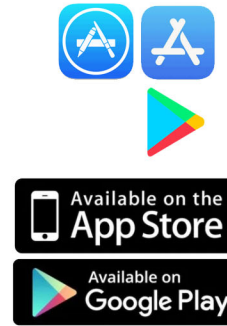# TCC Total Wi-Fi Details

DOWNLOAD TCC Total Wi-Fi:

Go into your smartphone's app store, search for "TCC Total Wi-Fi" and tap on the app icon. Download it, open it, and follow the steps to register the app and link it to your router.

https://tccpro.net/gettcc/total-wi-fi

CONTROL

- Change or reset your Wi-Fi network name or password directly from the app.
- See devices currently using your Wi-Fi.
- Categorize your devices (e.g. work, gaming,streaming, etc.).
- Pause the Internet for any device, at any time.
- Create routines for scheduled downtime (bedtime, school time, etc.).
- Create a temp/sharable guest network for guests, babysitter, kids' friends to use.
- Run a speed test to make sure you are getting the speed you are expecting.

MANAGE

- Block inappropriate categories (e.g. pornography, violence).
- Block applications that you deem inappropriate. (e.g. Grand Theft Auto, TikTok, Snapchat).
- Set time limits for specific apps like TikTok.
- Set Safe Search and YouTube Restriction to block harmful or inappropriate content through searches with searching on Google, Bing, or YouTube.
- View usage for all devices.
- Prioritize application groups or specific devices to ensure the best possible experiience for your most important needs -- including scheduled priority.

☑ **Included with FREE Version**

☐ **Included with $14.95* Version**
(*also includes router & mesh)

PROTECT

- Proactively monitors your home's incoming traffic and automatically blocks anything suspicious.
- Blocks attempted visits to known harmful websites, presenting users with a browser message indicating that the website is not available.
- Provide an active security monitoring service that uses a large and constantly growing database of threats (database is updated weekly).
- Uses Intrusion Prevention Settings (IPS) to monitor, notify, and prevent activity such as hackers trying to gain access to the local video content (Wi-Fi connected doorbell or baby monitor), virtual meetings, and other streams.
- Actively terminates data transfers before a malicious payload is delivered to any vulnerable network device.
- Notifies users whenever a security issue is triggered, with details about the device that was attacked, where the attack came from, and when it occurred.