TECH BULLETIN

TECHNICAL SUPPORT

# ClareHome and Home Network Security Best Practices

**Last modified:** 10/24/17

## Introduction

Security is a top priority at Clare Controls. This document contains a brief description of how ClareHome protects your security and some suggestions for keeping your home network secure.

## ClareHome

Clare Controls values the customer's security and has worked hard to make sure that the ClareHome App is protected.

### SmartHome system PIN (personal identification number)

ClareHome secures App access through a PIN, assigned by default and then customized by the user.

The default SmartHome PIN should be changed immediately after your first connection to the SmartHome with the App. To change the PIN, open the App and browse to **Reset PIN** (**Settings** > **Configuration** > **Reset PIN**), and then select a PIN that contains a combination of letters (upper and lowercase), numbers, and symbols. Avoid selecting an easily guessed PIN-1234.

Consider changing your PIN every 30 to 90 days, or after guests/installers access your SmartHome system. This prevents continued access from undesired users.

**Note:** For added security, first time connections to the ClareHome project with a user device (smartphone) must be made while on premises and connected to the LAN.

### Secure tokens for remote connections

ClareHome uses secure tokens for device connections. Thermostats, security devices, etc., all use tokens. These tokens are short lived and change regularly to ensure that connections are safe.

### Reverse proxy

The ClareHome App opens a secure encrypted tunnel to a cloud based system using authorized user provided credentials, to authenticate device communication in the home. The encrypted tunnel is created between the user's device and the ClareHome App, no further communication is made to other internet services.

### Homeowner notified when their system is accessed using Install Assist

The homeowner is notified when a dealer accesses their project using the Clare Controls Install Assist App. This appears as pop-up notification on all connected Android smartphones or iOS devices. This alerts the homeowner that their system is being accessed. So, no more blind updates or changes. The homeowner can contact the dealer to learn about the changes.

### Controlled incoming connections

The ClareHome controller only uses encrypted SSL (Secure Socket Layer) based protocols to communicate with client devices and the App. The controller initiates all connections and does not allow traffic over ports without valid credentials. This makes unauthorized devices unable to connect to your ClareHome system.

## Home network security

Not only do we care about ClareHome security, but also general home network security. See the security suggestions below.

### Change your default router administrator password and username

Most Wi-Fi wireless routers and access points have a manufacturer set default admin username and password. This information is often simple and documented. If unchanged, this leaves you vulnerable to cybercriminals. These settings should be changed immediately. A secure router password should be at least 20 characters long and include a combination of numbers, letters (upper and lowercase), and symbols.

### Choose a strong Wi-Fi password

Default router passwords are easy to guess when manufacturer information is known or available. A secure wireless password should be at least 20 characters long and include a combination of numbers, letters (upper and lowercase), and symbols. A complex password also discourages hackers from accessing your network to “borrow” your data.

### Use network encryption

Do not use outdated encryption technology. WEP and WPA encryption are older and susceptible to hacking. WPA2 AES is the current secure standard, compatible with most modern routers and Wi-Fi devices.

### Hide your network SSID

If you do not need to broadcast your SSID, hide it. Most routers allow an admin user to disable the network broadcast feature.

### Change your network's default SSID

Routers come with a default manufacturer Wi-Fi name (SSID), often containing the manufacturer name. Broadcasting this manufacturer name makes it easier for hackers to exploit the known vulnerabilities of the router. The SSID name should be changed immediately and not include personal information (names, address, etc.). Do not make it easy for a hacker to guess which Wi-Fi network is yours.

### Use guest networks on your router

When possible setup a guest network with an SSID, password, and IP scheme different from the home's current SSID. This allows guests to connect to your home's internet, but can be disabled or changed as desired.

For example – when changing the IP scheme from 192.18.1.0/24, set the guest account to 10.0.0.1/24. Make the scheme different. This prevents access to on premises equipment isolating the network from guest access.

**Note:** If a Guest Network will not be used, disable the guest network option so that it cannot be exploited.

### Strategically position your router

Set up your router as close to the center of your home as possible. This maximizes your signal coverage while minimizing the signal strength outside of your home. A hacker can infiltrate your wireless network if it can be accessed from a neighboring house or outside on the street.

### Disable remote access

Some routers allow remote access from the internet. Disabling this feature helps prevent hackers from connecting to your router on a device not on your wireless network.

### Keep your router's firmware/software up-to-date

Router firmware/software may contain exploitable flaws. Ensure your router is running the latest firmware/software to minimize vulnerability to router exploits. Your router may support auto-updates, check for and enable the auto-update setting.

### Use a firewall

Your router may include a network firewall. For added security, ensure that your network firewall is active and, if applicable, enable SPI (Source Packet Inspection). This option verifies that all incoming/outgoing packets are from the correct authorized senders.

## Contact information

Clare Controls, LLC.
7519 Pennsylvania Ave, Suite 104
Sarasota, FL 34243

General: 941.328.3991
Fax: 941.870.9646
www.clarecontrols.com

Integrator/Dealer Support: 941.404.1072
claresupport@clarecontrols.com

Homeowner Support (ClareCare): 941.315.2273 (CARE)
help@clarecontrols.com