



Clare Security Panel Integration

Release Notes

Content

Introduction...	1
Installation...	2
Installation with Wi-Fi in the Home...	2
Installation without Wi-Fi in a home...	3
Connecting the CLIQ.mini to Wi-Fi from AP mode...	7
Configuring with Clare Controls Install Assist...	9
Hardwired zone input module configuration...	15
Clare Security Panel user management...	22
Configuring in Fusion...	26
User interface example...	35
Silence Beeping...	36
Troubled states...	37
Configuring the ClareNet Activation portal...	39
Contact information...	42

Last modified: 08/28/19

Introduction

The Clare Security panel is an IP security panel and alarm system created for residential use. It has been tested and certified for integration with ClareHome.

The instructions in this document help you quickly integrate the panel into the ClareHome system and configure ClareNet Activation. This document is not intended to be a complete installation guide.

Notes

- The security panel supports one partition.
- Only 1 panel can be integrated with a ClareHome project.
- The security panel's initial configuration must be done with the Clare Controls Install Assist App.

Supported models

CS-SEC-10

Clare Security Panel supported properties in ClareHome

The following panel features are supported in ClareHome.

- **Arm and disarm:** Arm and disarm are options in the user interface. Swipe the screen to arm or disarm the system.
- **Armed stay:** The panel arms in stay mode, bypassing zones that are not included in arm stay (motion detectors) by default, each zone is configurable.
- **Armed away:** The panel arms in away mode, activating the entire security system (internal and external).
- **Zone status:** The user can see the status of all zones in the system.
- **Zone bypass:** Bypasses a zone the next time it is armed. Zone bypassing is only available when the panel is unarmed.
- **Zone configuration:** Configure zone properties.
- **Zone pair/remove:** Pair and remove zones through the Install Assist App.
- **Security settings:** Configure all settings through the Install Assist App.
- **User PINs:** Configure user PIN numbers through Fusion.

Installation

A qualified technician should install the security panel. Refer to the installation instructions that came with your device. Clare Controls does not assume any responsibility for damages caused by improper installation or connection to the network.

Note: You need 2 Ethernet cables and an Ethernet switch.

Installation with Wi-Fi in the Home

The CLIQ.mini and panel can be configured with the home's existing Wi-Fi.

To connect the panel to the CLIQ:

Note: This scenario requires the CLIQ device to use the home's existing Wi-Fi network.

1. Connect the panel's power supply to the power port on the panel.
2. Connect an Ethernet cable to the CLIQ, and then connect the other end of the cable to an Ethernet switch.
3. Connect a second Ethernet cable to the switch, and then connect the other end of the cable to the security panel.
4. Connect your iOS device or Android smartphone to the home's Wi-Fi network.

Note: This requires the home's Wi-Fi SSID and password.

5. Configure and setup the panel using the Clare Controls Install Assist App.

Note: When setting up the panel, use Install Assist to configure the panel and devices. If the panel and devices are not configured through Install Assist, the devices do not integrate correctly.

Installation without Wi-Fi in a home

To connect and configure the panel in a home with no Wi-Fi, the CLIQ.mini must be in AP mode with no router attachment.

Notes

- You will need 2 Ethernet cables and an Ethernet switch.
- PoE switches are not supported for this installation method. The PoE injector, included with the CLIQ.mini, can be used. Do not use the LAN port until the device is ready to connect to the internet.
- A router is not used in this setup, you must use an Ethernet switch.

To connect the panel to a CLIQ.mini using AP mode:

1. Attach the power supply to the power port on the panel.
2. Connect an Ethernet cable to the panel, and then connect the other end of the cable to an Ethernet switch.
3. Attach the CLIQ.mini to its power supply, and then wait for the mini to power on.
4. Verify that the CLIQ.mini is in AP mode, the LED flashes red in .5 second intervals. If it is not, see “To reboot the CLIQ.mini and enter AP mode,” on page 4.
5. Attach a separate Ethernet cable to the CLIQ.mini, and then plug the other end of the cable into Ethernet switch. Wait for the CLIQ.mini to broadcast its Wi-Fi, and then connect your iOS device or Android smartphone to the mini’s Wi-Fi.

See “To connect to the CLIQ.mini’s Wi-Fi using an iOS device,” on page 5.

– or –

See “To connect to the CLIQ.mini’s Wi-Fi using an Android device,” on page 6.

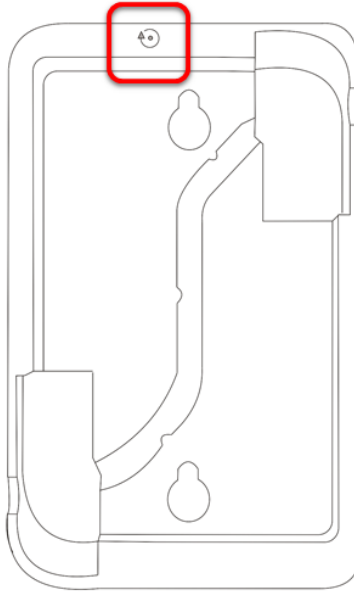
6. Use the Install Assist App to configure the panel and devices, see “Configuring with Clare Controls Install Assist,” on page 9.

Note: If the panel and devices are not configured through Install Assist, the devices do not integrate correctly.

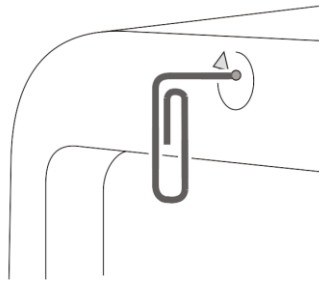
7. After Configuring the panel using the Install Assist App, remove the Ethernet switch, and when available, connect the CLIQ.mini to the home's Wi-Fi. See "Connecting the CLIQ.mini to Wi-Fi from AP mode," on page 7.

To reboot the CLIQ.mini and enter AP mode:

1. Locate the recessed push button on the CLIQ.mini.



2. Insert the paper clip (provided), pressing the button down and holding for 20 seconds.



3. Remove the paper clip and observe the LED behavior.
The CLIQ.mini's LED indicators alternate red and blue signifying it has entered the reboot state.
4. Once the CLIQ.mini boots and the LED flashes red in .5 second intervals, it is in AP mode. Connect your Android or iOS device to the mini's Wi-Fi and continue using the Install Assist App.

To connect your CLIQ.mini with LAN from AP mode:

1. Verify that your mini is in AP mode (LED flashes red in .5 second intervals.)
2. Connect the Ethernet cable to the Ethernet port on the CLIQ.mini.
See Figure 1, item 6.
3. Locate the recessed push button on the CLIQ.mini. See Figure 1, item 1.
4. Insert the paper clip (provided) pressing the button down and holding for 5 seconds.
5. Remove the paper clip and observe the LED behavior. The CLIQ.mini's LED indicators alternate red and blue signifying it has started shutting down.
6. After the CLIQ.mini shuts down, disconnect the CLIQ.mini's power supply.
7. Reconnect the power supply and verify that the CLIQ.mini restarts. Continue with installation and setup.

Figure 1: CLIQ.mini rear connections

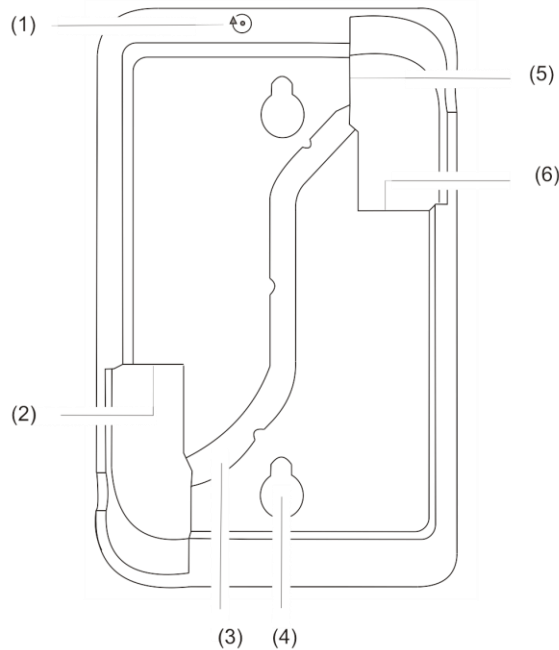


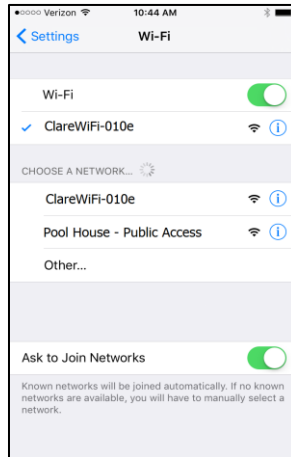
Figure 1


- | | |
|--------------------------|----------------------|
| (1) Recessed push button | (4) Wall mount slots |
| (2) 2 USB ports | (5) Micros USB port |
| (3) Wire routing channel | (6) Ethernet port |

To connect to the CLIQ.mini's Wi-Fi using an iOS device:

Note: To use this App successfully you must be connected to the CLIQ.mini's Wi-Fi. This Wi-Fi network displays as ClareWifi-xxxx. The xxxx is replaced with the last 4 digits of your CLIQ.mini's MAC address.

1. Tap **Settings**.
2. Tap **Wi-Fi**, and then select the CLIQ.mini's broadcasted Wi-Fi.




3. Return to the home screen and tap  to access your App.

To connect to the CLIQ.mini's Wi-Fi using an Android device:

1. Access the device's settings.
2. Tap Wi-Fi, and then select the CLIQ.mini's broadcasted Wi-Fi.



3. Return to the home screen and tap  to access your App.

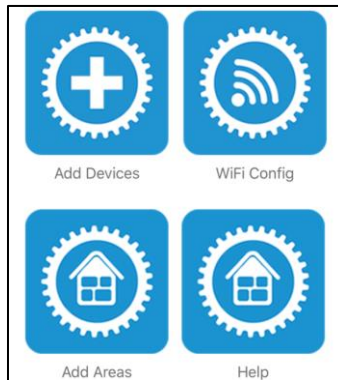
Note: Some Android phones require Wi-Fi verification if there is no internet access. Opt to allow the Android device to stay connected to the CLIQ.mini's Wi-Fi. For more information and detailed instructions, see [CLIQ.mini and Android Nougat: AP Mode Wi-Fi Error \(DOC ID 1459\)](#).

Connecting the CLIQ.mini to Wi-Fi from AP mode

After using the Install Assist App in AP mode, the CLIQ.mini remains in AP mode. Leave the mini in this state until internet is available to the home. Once Wi-Fi is available, use the Install Assist App to configure the CLIQ.mini to the home's Wi-Fi network.

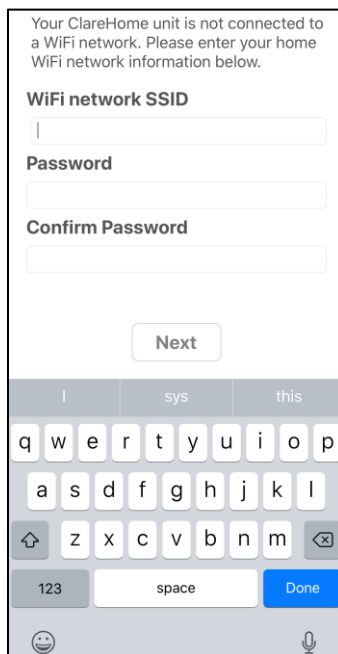
To connect the CLIQ.mini to the home's Wi-Fi network using Install Assist:

1. Launch the Install Assist App.

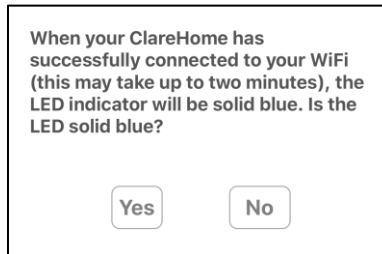


2. Tap **WiFi Config**.

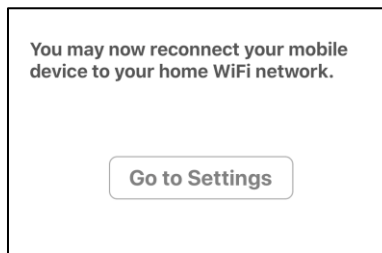
Note: If you are using an Android smartphone, tapping in the **WiFi network SSID** field presents the user with a Wi-Fi drop-down menu. Select the appropriate network.

A screenshot of the WiFi configuration screen in the Install Assist App. At the top, a message states: 'Your ClareHome unit is not connected to a WiFi network. Please enter your home WiFi network information below.' Below this, there are three input fields: 'WiFi network SSID', 'Password', and 'Confirm Password'. A 'Next' button is positioned below the 'Confirm Password' field. At the bottom of the screen, a QWERTY keyboard is visible, with a 'Done' button on the right.

3. Enter or select (if using an Android smartphone) the Wi-Fi network SSID, the password, confirm the password, and then tap **Next**.

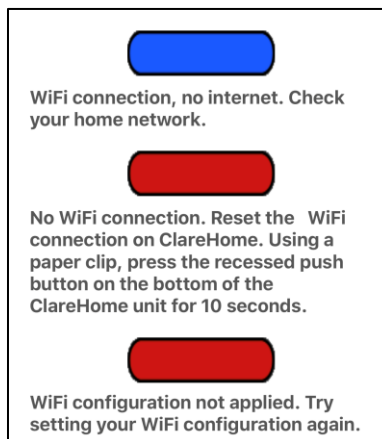


4. Read the displayed information and then tap **Yes** or **No** accordingly.
If tapping **Yes**, continue the configuration steps.



— or —

If you tapped **No**, onscreen status LEDs and instructions display. You must verify the network is available and the CLIQ.mini is set in AP mode, and then return to step 1.



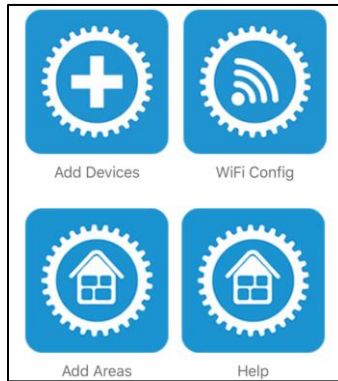
5. Tap **Go to Settings**, and then verify that your iOS device or Android smartphone is connected to the correct Wi-Fi network.


Configuring with Clare Controls Install Assist

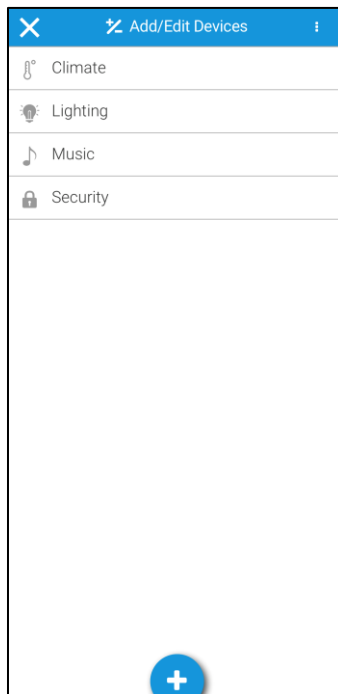
After the panel is successfully installed, add and configure it with the Install Assist App.

To add devices with the App:

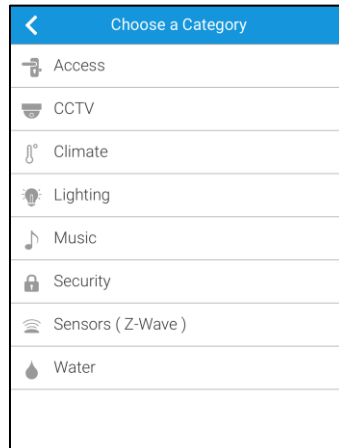
1. Tap **Add Devices**.



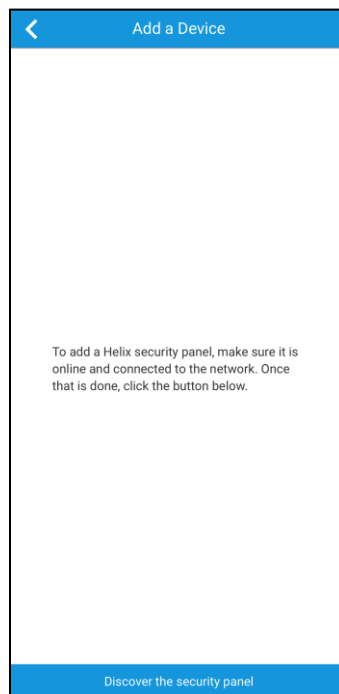
2. At the bottom of the screen, tap the plus icon .



3. Tap **Security**.



4. Read the displayed information, and then tap **Discover the security panel**.



5. The panel is discovered. Enter a name for the panel, and then customize the panel settings as desired.

Notes

- Discovery can take up to a minute.
- The panel's defaults are recommended for standard use.

The screenshot shows the 'Edit Device' settings screen. At the top is a blue header with a back arrow and the title 'Edit Device'. Below this, the 'Device Name' is set to 'Security'. The 'Type' is 'Security Device'. The 'Status' is 'Device is online' with a green checkmark. A blue button labeled 'Configure Security Users' is present. Under 'Device Settings', there are three toggle switches: 'Audible Alarm' (disabled), 'Global Auto Bypass' (enabled), and 'Global Chime' (enabled). At the bottom, there are two sliders for entry delays: 'Long Entry Delay' is set to 60 seconds (range 30-240) and 'Standard Entry Delay' is set to 30 seconds (range 30-240).

System Settings

Audible Alarm: This feature allows audible alarms. If disabled all audible alarms, except chimes, are silenced.

Global Auto Bypass: This allows a zone(s) to be bypassed when the alarm is set. It must be enabled for the auto bypass to function.

Global Chime: This allows the panel to use chimes. If this is not enabled, all chimes are silenced.

Delay options

Note: There are 2 delay options, allowing zones to use different set delays.

Long Entry Delay: The time in seconds between a zone fault (door opening) and triggering the alarm. This is set to a longer amount of time than the Standard Entry Delay.

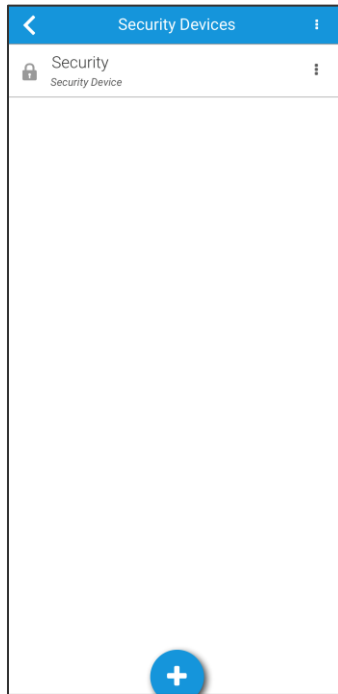
Standard Entry Delay: The time in seconds between a zone fault (door opening) and triggering the alarm. This is set to a shorter amount of time than the Long Entry Delay.


Status (Chime/Arm/Disarm) Volume: This determines the volume of chimes and entry/exit delays sounds.

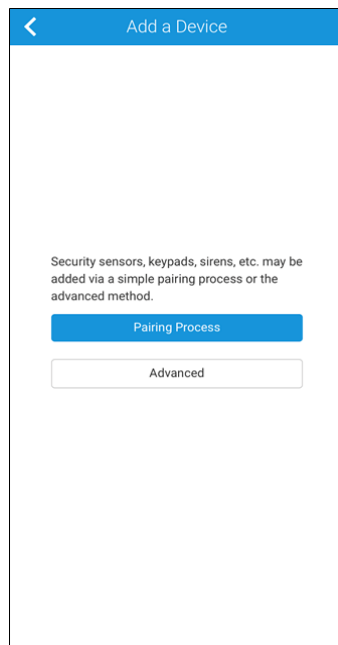
Wireless Siren Status Volume: This determines the volume for any wireless sirens used with panel.

6. Tap < **Edit Device** to save the panel settings.

The security devices page displays.



7. Tap the plus icon  to add a new security zone (sensors, keypads, and sirens).



8. Tap **Pairing Process**, and then follow the on-screen instructions regarding device tab removal.

Note: The Advanced option is only used for the hardwired zone input module.

9. The security zone is discovered, name the zone and custom the desired fields.

The screenshot shows the 'Edit Device' interface. At the top is a blue header with a back arrow and the title 'Edit Device'. Below the header, the 'Device Name' field contains the text 'Window'. The 'Serial Number' field displays '00 00 00 00'. The 'Type' field shows a lock icon followed by 'Window/Door Sensor'. The 'Status' section indicates 'Device is online' with a green checkmark icon. A section titled 'Device Settings' contains five toggle switches, all of which are turned on (blue): 'Active in Arm Away', 'Active in Arm Stay', 'Allow Bypass', 'Auto Bypass', and 'Close Chime'. Each toggle switch has a small 'i' icon to its right.

Device Settings

Clare Controls currently supports Clare Security peripherals and sensors. Each sensor has configurable settings. See below for a list of supported peripherals/sensors and the configurable sensor settings.

Note: Peripheral devices, such as the sirens, keypads, and key fob do not have configurable settings are not displayed in the ClareHome or Install Assist App.

Supported sensors and peripherals

CS-DWS-10 Window/Door Sensor	CS-360-10 360 Degree Ceiling Mount Indoor Motion Detector
CS-PNC-10 Panic Pendant	CS-KFB-10 5-Button Security Keyfob
CS-GBS-10 Glass Break Sensor	CS-WTR-10 Water/Temp Sensor
CS-SMK-10 Smoke Detector	CS-PIR-10 PET Immune PIR Motion Sensor
CS-CMD-10 Carbon Monoxide Detector	CS-NDWS-10 Micro Window/Door Sensor
CS-SRN-10 Siren with Battery Backup	CS-MMA-10 Micro Mounting Accessory
CS-WRP-10 Wireless Range Extender	CS-HWT-10 Hardwired Zone Input Module
CS-PIN-10 Wireless Pinpad	
CS-OMS-10 Outdoor Motion Sensor	

Configurable sensor settings

Active in Arm Away: This enables/disables the zone generation of an alarm event while in Arm Away mode.

Active in Arm Stay: This enables/disables the zone generation of an alarm event while in Arm Stay mode.

Allow Bypass: This enables/disables the ability to bypass the zone.

Auto Bypass: This enables/disables the zone to be automatically bypassed if it is open when arming the panel.

Close Chime: This turns on/off the audible chime when the zone is closed.

Entry/Exit Delay: The entry/exit delay setting for arming and disarming, select Long, Short, and Standard. Exact values are configured in partition.

Follow Zone: This enables/disables the application of the entry/exit delay.

Open Chime: This turns on/off the audible chime when a zone is opened.

Report Code: The intrusion perimeter set for an input.

Sensor Input Name: The configured external input number.

10. Repeat steps 6 through 9 for each zone.

11. Connect the CLIQ.mini to the home's network.

Hardwired zone input module configuration


use

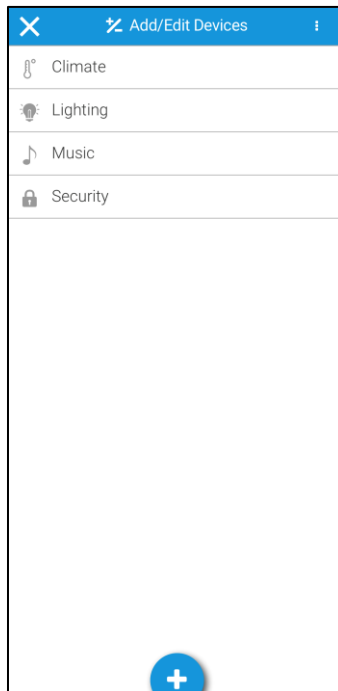
To configure the module in Install Assist:

Note: Configuration of the wired zones requires that the installer records which sensors are connected to which physical connectors on the module.

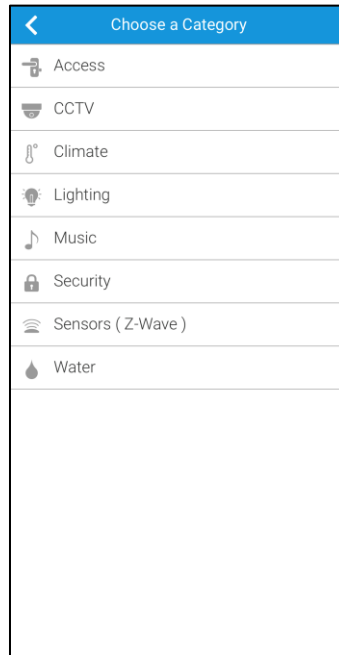
1. Tap **Add Devices**.



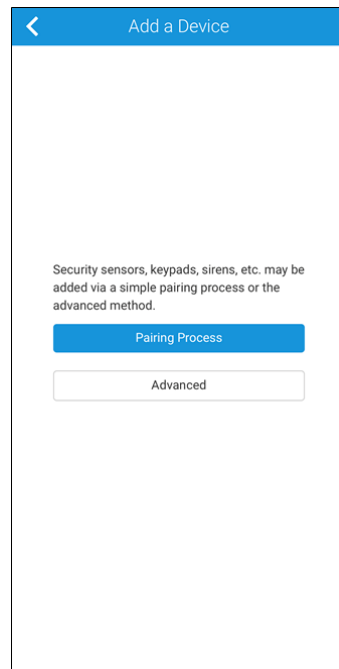
2. At the bottom of the screen, tap the plus icon .



3. Tap **Security**.



4. Tap **Advanced**.



5. Enter your zone input module's serial number, and then tap **Get Zone Inputs**.

The screenshot shows a mobile application interface titled "Add a Device". At the top, there is a blue header bar with a back arrow and the text "Add a Device". Below the header, the "Sensor" section is visible, with the instruction "Enter the sensor's serial number or select an existing sensor". Underneath, there is a "Serial Number" label followed by a text input field containing "20909090". Below the input field is a section titled "Existing Sensors" with a dropdown menu. At the bottom of the screen is a blue button labeled "Get Zone Inputs".

The zone inputs display.

The screenshot shows the same "Add a Device" screen, but now the "Zone Inputs" section is expanded. It contains the instruction "Select a zone profile for each input to be used. Used inputs will appear as individual devices. To make a used input available again, remove the zone input's device." Below this instruction are six rows, each labeled "External Input 1" through "External Input 6". Each row has a dropdown menu showing "Perimeter (Default)" and a blue "Save" button. At the bottom of the screen, there is a small, partially visible section labeled "External Input 7".

- Using the first configured input on the module, select the zone's profile.

Note: Configure the zone inputs in order to avoid confusion. There are no names displayed, only zone numbers (zone names can be changed later in the process). The configured inputs may not start with Zone 1 in the security device list. For example, the security panel has 2 motion sensors (zone 1 and 2), the first configured input will be automatically assigned to zone 3, or the next available zone in the configuration. If there is a gap in the zone number, i.e. there are 6 zones and zone 4 is removed, the next zone to be added is zone 4.

Sensor
20 90 90 90 - [Change](#)

Zone Inputs
Select a zone profile for each input to be used. Used inputs will appear as individual devices. To make a used input available again, remove the zone input's device.

External Input 1
Perimeter (Default) [Save](#)

External Input 2
Perimeter (Default) [Save](#)

External Input 3
Perimeter (Default) [Save](#)

External Input 4
Perimeter (Default) [Save](#)

[Done](#)

Motion Night
Motion Outdoor
Panic
Perimeter (Default)
Special
Supervised Only
Tripwire

7. Once the input is selected, tap **Save**.

Note: You must tap Save after selecting each input.

Sensor
20 90 90 90 - [Change](#)

Zone Inputs
Select a zone profile for each input to be used. Used inputs will appear as individual devices. To make a used input available again, remove the zone input's device.

External Input 1
Auxiliary **Save**

External Input 2
Perimeter (Default) **Save**

External Input 3
Perimeter (Default) **Save**

External Input 4
Perimeter (Default) **Save**

External Input 5
Perimeter (Default) **Save**

External Input 6
Perimeter (Default) **Save**

8. Repeat steps 6 through 7 for each additional input.

Note: Once an input is saved, it is no longer available to select/edit. To reuse or reconfigure an input, the zone must be deleted and then re-added.

Sensor
20 90 90 90 - [Change](#)

Zone Inputs
Select a zone profile for each input to be used. Used inputs will appear as individual devices. To make a used input available again, remove the zone input's device.

External Input 1 - In Use

External Input 2
Perimeter (Default) **Save**

External Input 3
Perimeter (Default) **Save**

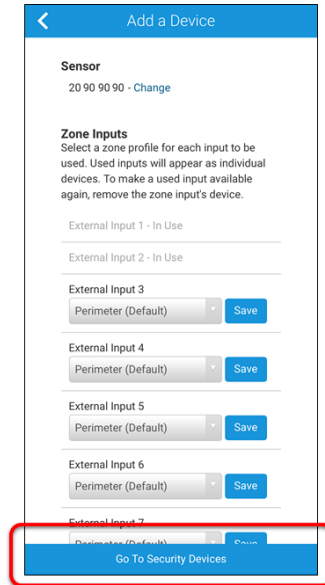
External Input 4
Perimeter (Default) **Save**

External Input 5
Perimeter (Default) **Save**

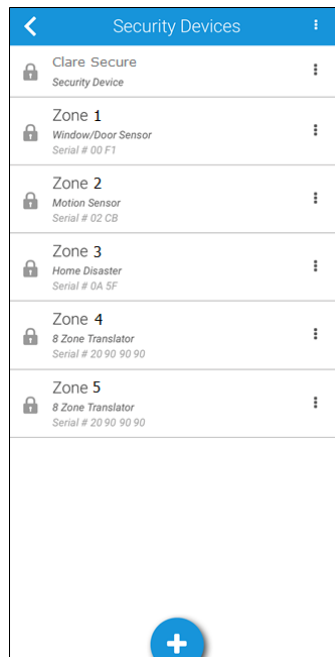
External Input 6
Perimeter (Default) **Save**

[Go To Security Devices](#)

9. After module configuration, tap **Go To Security Devices**.



All configured security devices display.



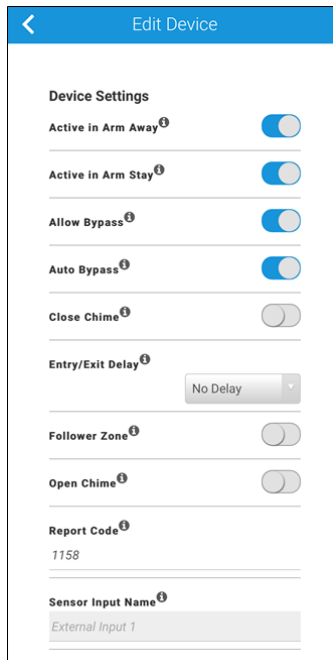
Zones created using the hardwired zone input module can be modified or deleted like other security devices.

To check a zone's input:

1. Tap the desired zone.

2. Scroll down to view the report code and input field.

For report code meaning, see Table 1: Input report codes, profiles, and alarm type.



Edit Device

Device Settings

Active in Arm Away ☒

Active in Arm Stay ☒

Allow Bypass ☒

Auto Bypass ☒

Close Chime ☐

Entry/Exit Delay

Follower Zone ☐

Open Chime ☐

Report Code

Sensor Input Name

Table 1: Input report codes, profiles, and alarm type

Report code	Profile	Alarm type
1150	Auxiliary	Auxiliary
1162	CO	Carbon monoxide
1134	Entry/Exist Standard	Intrusion, perimeter with a standard delay
1134	Entry/Exit Long	Intrusion, perimeter with a long delay
1110	Fire	Fire, smoke, heat
1154	Flood	High water level
1131	Glassbreak	Intrusion, glass break
1114	Heat	Fire, heat sensor
1158	High Temperature	High temperature
1132	Interior	Intrusion, interior, no delay
1132	Interior Follower	Intrusion, interior follower
1159	Low Temperature	Low temperature
1132	Motion	Motion, no delay
1132	Motion Follower	Intrusion, interior, follower
1132	Motion Night	Intrusion, interior, no delay


1136	Motion Outdoor	Intrusion, perimeter, long delay
1120	Panic	Panic, police
1131	Perimeter	Intrusion
1133	Special	Special, only disarmed using special disarm
0	Supervised Only	Monitored for trouble conditions
0	Trigger	Trigger zone

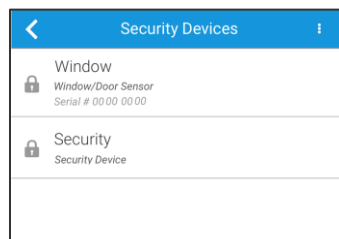
Clare Security Panel user management

User management allows the homeowner to change their security system's PIN, create new users, remove users, and reset existing PINs.

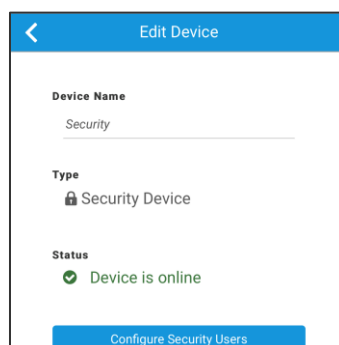
Note: For security, no one can see another user's PIN. This information is private. If a user forgets their PIN, the homeowner/master user can reset the PIN. If the master user forgets their PIN, the security panel must be factory defaulted and requires configuration assistance from the installer.

To access user management:

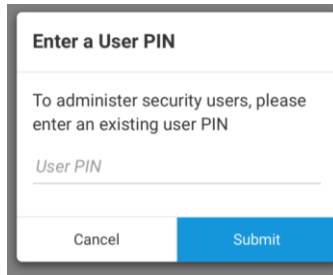
1. Launch the ClareHome app, and then tap the **Menu** icon .
2. Tap **Devices**.
3. Tap **Security**, select the security panel.



4. Tap **Configure Security Users**.



5. Enter the User PIN, and then tap **Submit**.

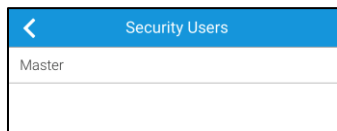


The screenshot shows a dialog box titled "Enter a User PIN". Below the title, it says "To administer security users, please enter an existing user PIN". There is a text input field labeled "User PIN". At the bottom, there are two buttons: "Cancel" and "Submit".

Notes

- The Master User PIN is set by the security dealer when the security system is installed. This PIN should be changed by the homeowner once they are in possession of the security system. This PIN gives the user the ability to manage other users and change their PIN.
- Any user PIN that has access to manage users can be used.
- If you enter the PIN of a user that does not have permission to manage users, you are unable to proceed.

6. A list of the panel's users displays.

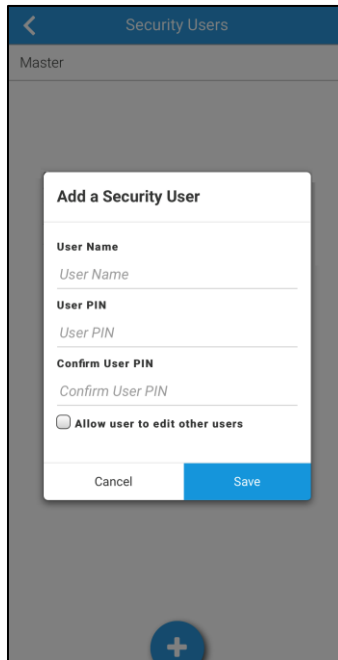


The screenshot shows a list titled "Security Users". The list contains one entry, "Master".

To add a new user:

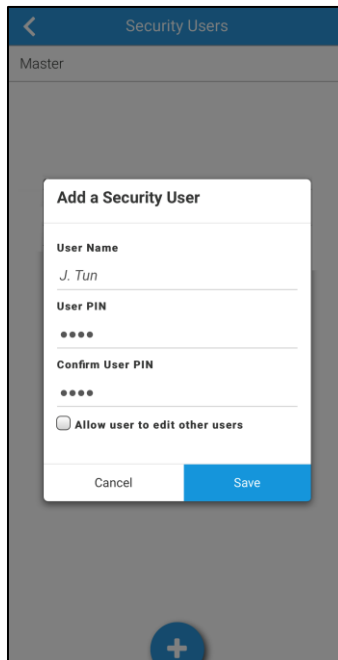
1. Tap the blue **Plus**  icon at the bottom.

The New User dialog displays.



2. Enter the **User Name**, **User PIN**, and confirm the PIN.

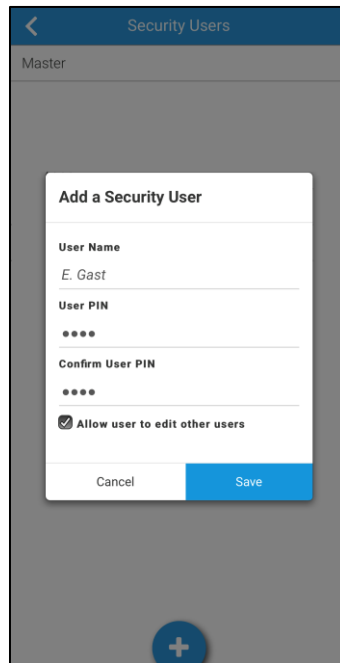
Note: Only select the checkbox if you want the new user to be able to view and modify existing users.



3. Tap **Save**.

To modify an existing user:

1. Tap the desired user's name.

A screenshot of a mobile application interface titled "Security Users". At the top, there is a blue header bar with a back arrow and the text "Security Users". Below the header, the word "Master" is displayed. The main content area is a light gray background. Overlaid on this is a white dialog box titled "Add a Security User". The dialog box contains three input fields: "User Name" with the text "E. Gast", "User PIN" with four dots, and "Confirm User PIN" with four dots. Below these fields is a checkbox labeled "Allow user to edit other users" which is checked. At the bottom of the dialog box are two buttons: "Cancel" and "Save". A blue circular button with a white plus sign is visible at the bottom center of the screen, below the dialog box.

2. Modify the user as desired, and then tap **Save**.

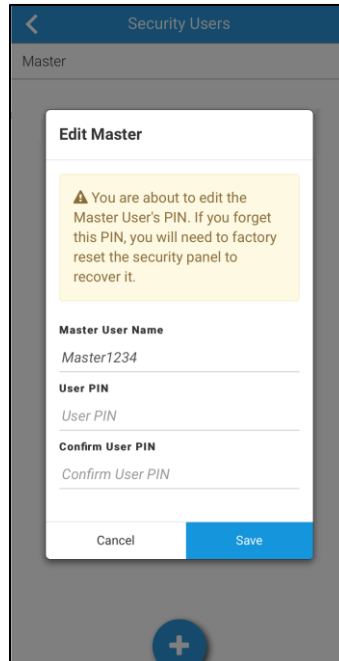
To remove a user:

1. Tap the dots next to the desired user's name.
2. Tap **Remove**, and then confirm user's removal.

To modify the Master PIN:

1. Tap the master user's name.

Note: If you change the master user's PIN, note it. If this PIN is forgotten the security panel must be factory reset.



2. Modify the user as desired, and then tap **Save**.

Configuring in Fusion

After installation and panel configuration, the device is automatically added to Fusion. Access the partition in Fusion to manage users and configure rules if desired.

Note: The panel supports one partition.

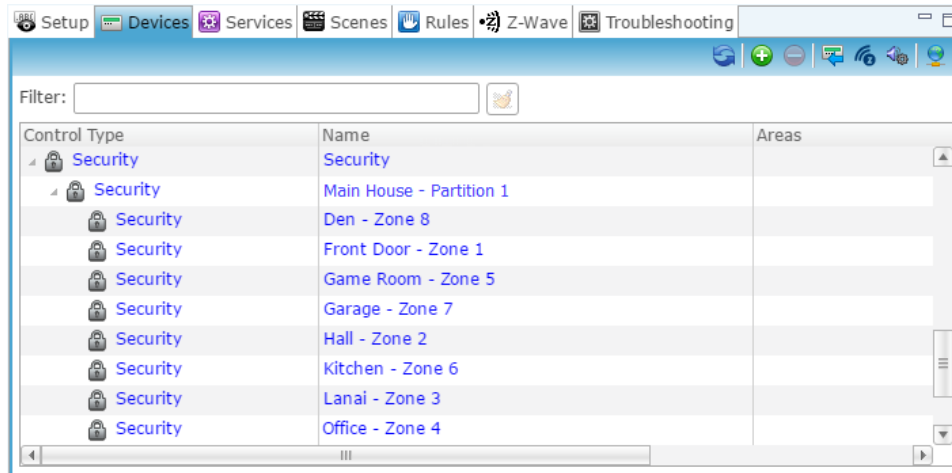
Managing users

Once you have added the panel, add and manage the users.

To access the Intrusion User Admin Menu:

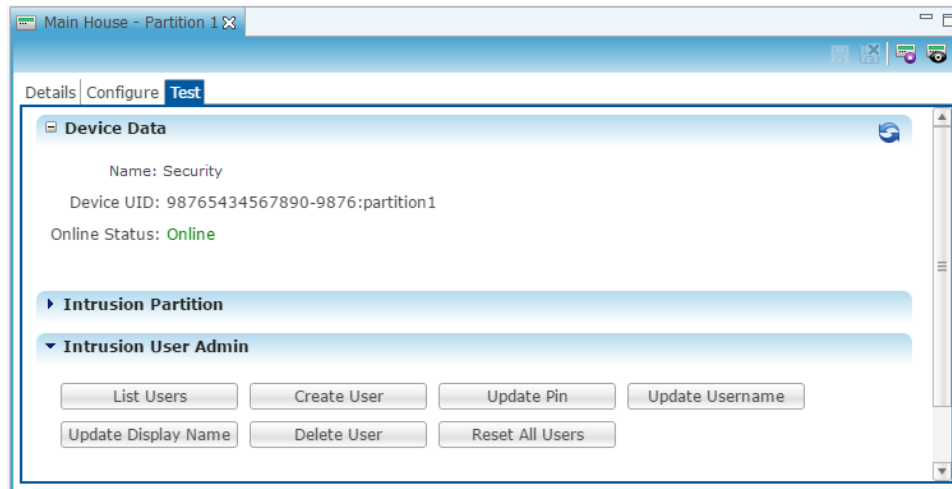
1. Access the desired Fusion project and view the devices.

2. Expand the security panel to view the partition.

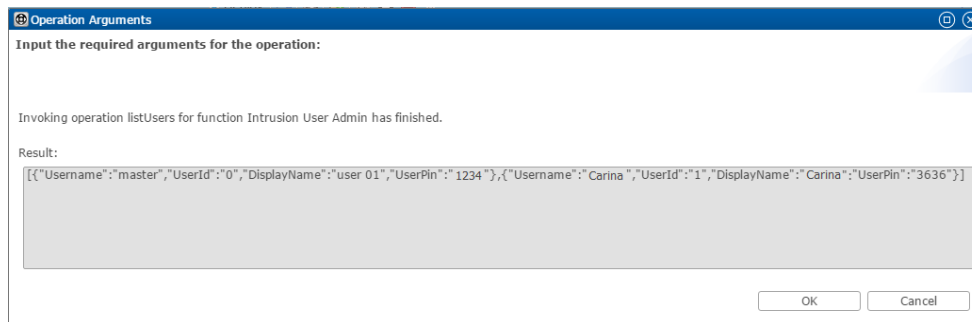


3. Double click the partition, the partition's **Details** tab displays.

4. Click the **Test** tab, and then expand **Intrusion User Admin**.



List Users: This button displays a list of all current users and their configured information including PIN, Username, Displays name, and User ID.



Note: The user id's start at 0. The default master user id is 0. The first user manually added is user 1.

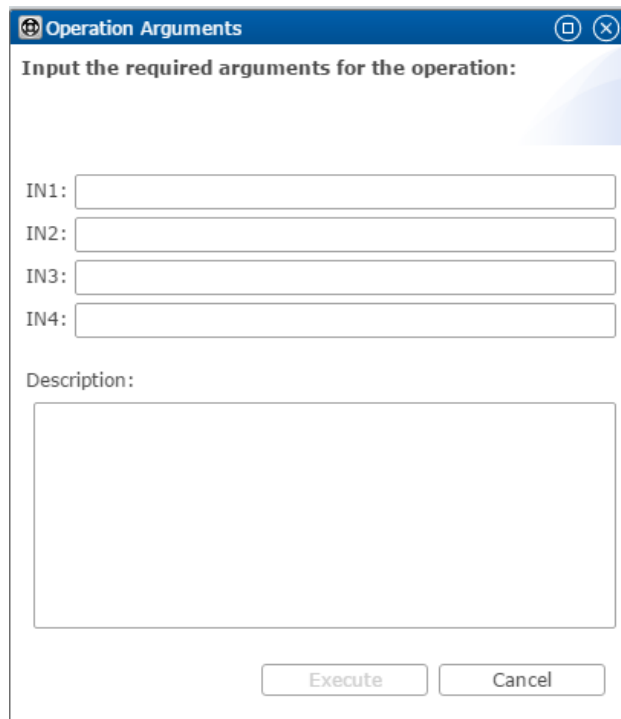
Create User: This button allows you to create a new user for the security panel.

1. Configure the boxes as follows.

IN1: The user's desired PIN.

IN2: The user's User Name.

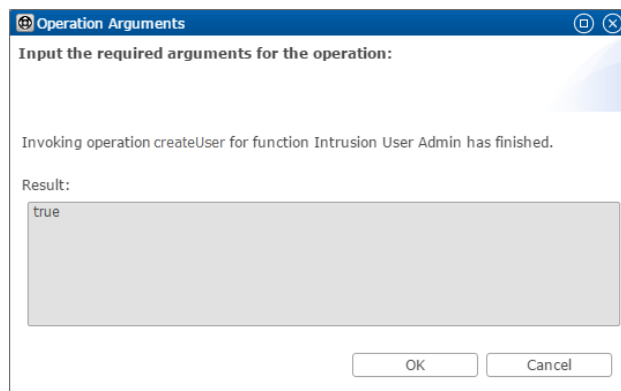
Note: Leave IN3 and IN4 blank. Information entered in these fields is not used.



The dialog box titled "Operation Arguments" has a blue header bar with a close button. Below the header, it says "Input the required arguments for the operation:". There are four input fields labeled IN1, IN2, IN3, and IN4. Below these is a larger text area labeled "Description:". At the bottom right, there are two buttons: "Execute" and "Cancel".

2. Click **Execute**.

The results box displays. If the operation was successful, the box displays true.



The dialog box titled "Operation Arguments" shows the results of the operation. It says "Invoking operation createUser for function Intrusion User Admin has finished." Below this, it says "Result:" and displays "true" in a text area. At the bottom right, there are two buttons: "OK" and "Cancel".

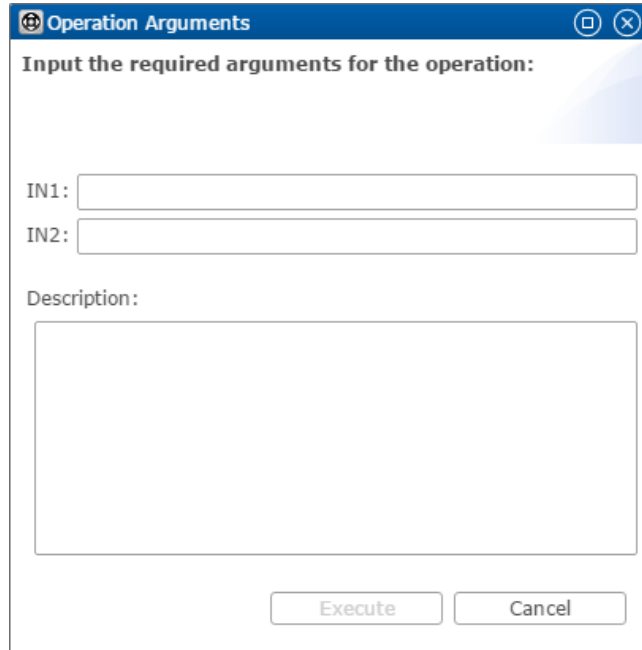
3. Click **OK**.
4. Click **List Users** to verify the new user was created.

Update Pin: This changes the user's PIN.

1. Configure the boxes as follows.

IN1: The user ID.

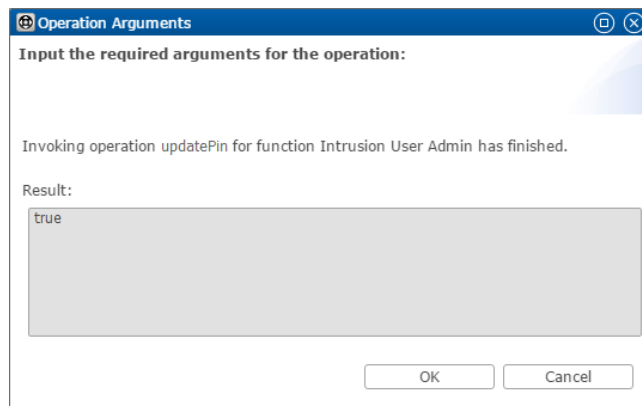
IN2: The new Pin.



The dialog box titled "Operation Arguments" has a blue header bar with a gear icon and window controls. Below the header, it says "Input the required arguments for the operation:". There are two input fields: "IN1:" followed by a text box, and "IN2:" followed by a text box. Below these is a "Description:" label followed by a large text area. At the bottom right are "Execute" and "Cancel" buttons.

2. Click **Execute**.

The results box displays. If the operation was successful, the box displays true.



The dialog box titled "Operation Arguments" shows the results of the operation. It says "Invoking operation updatePin for function Intrusion User Admin has finished." Below that is a "Result:" label followed by a text box containing the word "true". At the bottom right are "OK" and "Cancel" buttons.

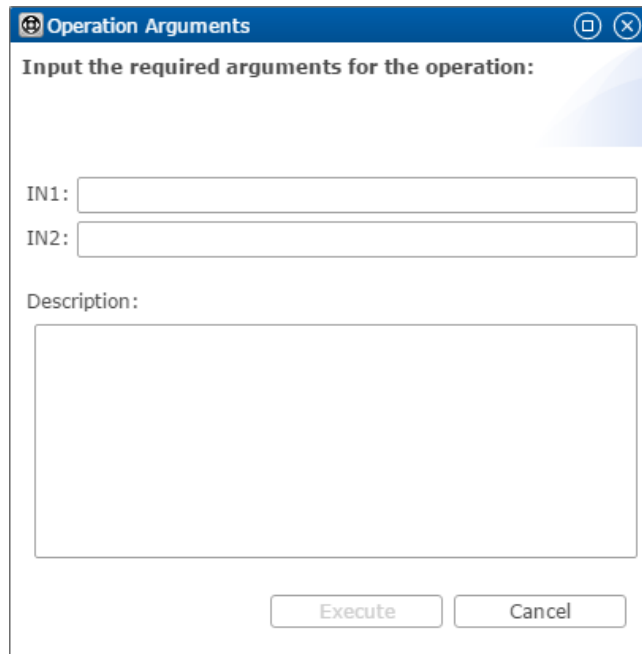
3. Click **OK**.
4. Click **List Users** to verify the new PIN was saved.

Update Username: This changes the username associated with an existing user ID.

1. Configure the boxes as follows.

IN1: The user ID.

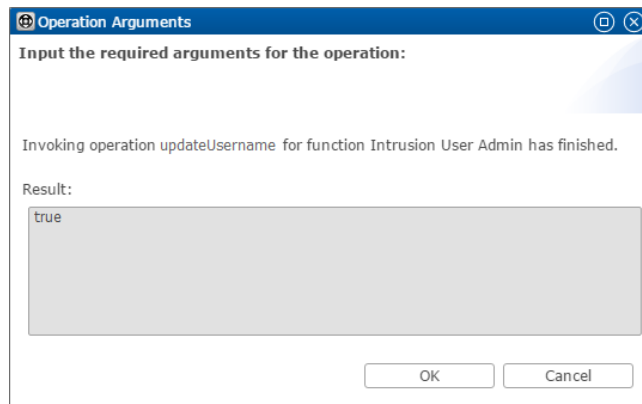
IN2: The new username.



The image shows a dialog box titled "Operation Arguments". It has a blue header bar with a gear icon on the left and minimize, maximize, and close buttons on the right. The main area is white and contains the text "Input the required arguments for the operation:". Below this text are two input fields: "IN1:" followed by a text box, and "IN2:" followed by another text box. Below these fields is a larger text area labeled "Description:". At the bottom of the dialog are two buttons: "Execute" and "Cancel".

2. Click **Execute**.

The results box displays. If the operation was successful, the box displays true.



The image shows the same "Operation Arguments" dialog box, but now it displays the results of the operation. The text "Invoking operation updateUsername for function Intrusion User Admin has finished." is shown above a "Result:" label. Below the label is a text box containing the word "true". At the bottom of the dialog are two buttons: "OK" and "Cancel".

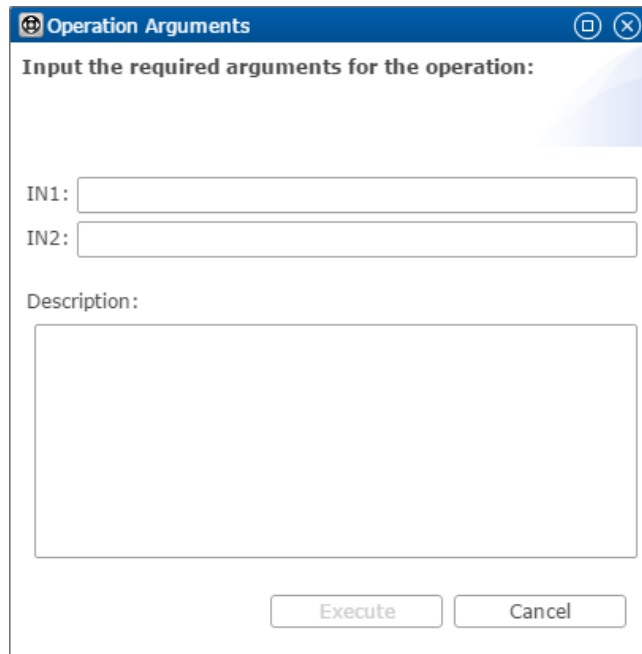
3. Click **OK**.
4. Click **List Users** to verify the new username was saved.

Update Display Name: This changes the display name associated with an existing user ID.

1. Configure the boxes as follows.

IN1: The user ID.

IN2: The new update display name.

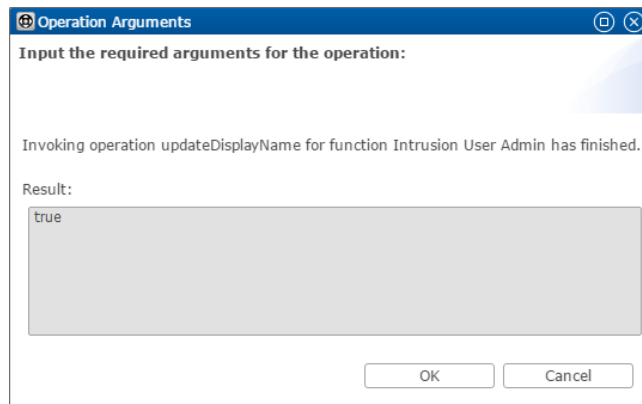


The dialog box is titled "Operation Arguments" and contains the following elements:

- A title bar with a maximize button and a close button.
- A label "Input the required arguments for the operation:".
- Two input fields labeled "IN1:" and "IN2:".
- A label "Description:" followed by a large text area.
- Two buttons at the bottom: "Execute" and "Cancel".

2. Click **Execute**.

The results box displays. If the operation was successful, the box displays true.



The dialog box is titled "Operation Arguments" and contains the following elements:

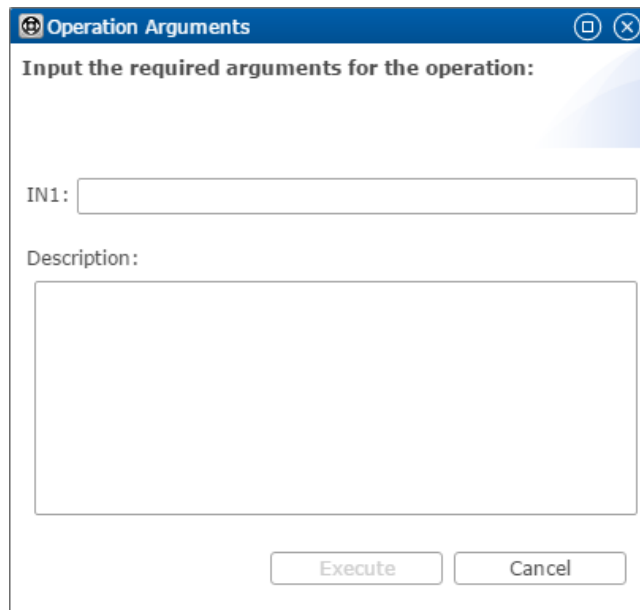
- A title bar with a maximize button and a close button.
- A label "Input the required arguments for the operation:".
- A message: "Invoking operation updateDisplayName for function Intrusion User Admin has finished."
- A label "Result:" followed by a text area displaying the word "true".
- Two buttons at the bottom: "OK" and "Cancel".

3. Click **OK**.
4. Click **List Users** to verify the new display name was saved.

Delete User: This removes an existing user.

1. Configure the boxes as follows.

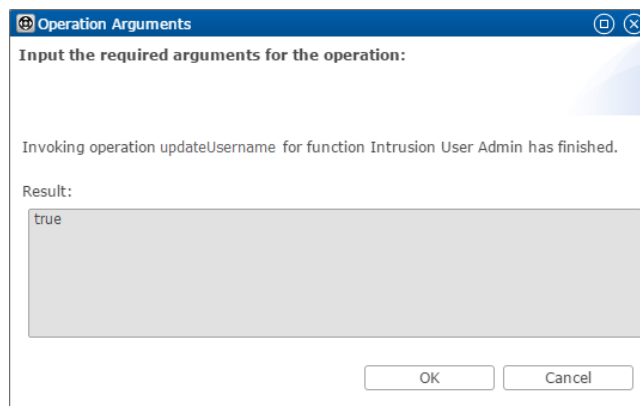
IN1: The user ID.



The image shows a dialog box titled "Operation Arguments". It has a blue header bar with a gear icon on the left and standard window controls (minimize, maximize, close) on the right. The main area is white and contains the text "Input the required arguments for the operation:". Below this text, there is a label "IN1:" followed by a single-line text input field. Underneath the input field is a label "Description:" followed by a larger, empty text area. At the bottom of the dialog, there are two buttons: "Execute" and "Cancel".

2. Click **Execute**.

The results box displays. If the operation was successful, the box displays true.



The image shows the same "Operation Arguments" dialog box, but now it displays the results of the operation. The text "Invoking operation updateUsername for function Intrusion User Admin has finished." is shown above a "Result:" label. Below the label, a text area displays the word "true". At the bottom, the buttons are now "OK" and "Cancel".

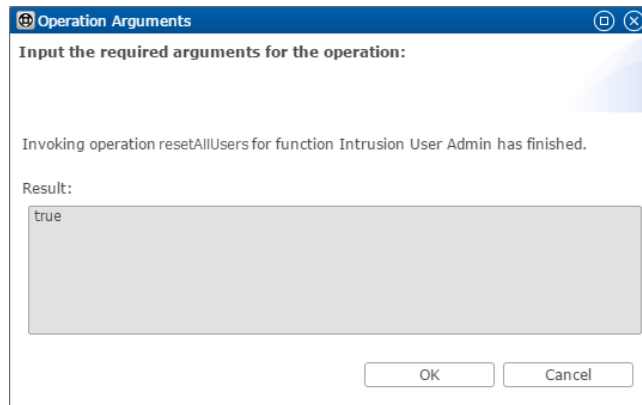
3. Click **OK**.
4. Click **List Users** to verify the user was deleted.

Reset All Users: This removes all existing user and defaults the master user's settings.

Note: Resetting the users reboots the panel, making it appear offline for several seconds.

1. Click **Reset All Users**.

The results box displays. If the operation was successful, the box displays true.



2. Click **OK**.
3. Click **List Users** to verify that only the defaulted master user remains.

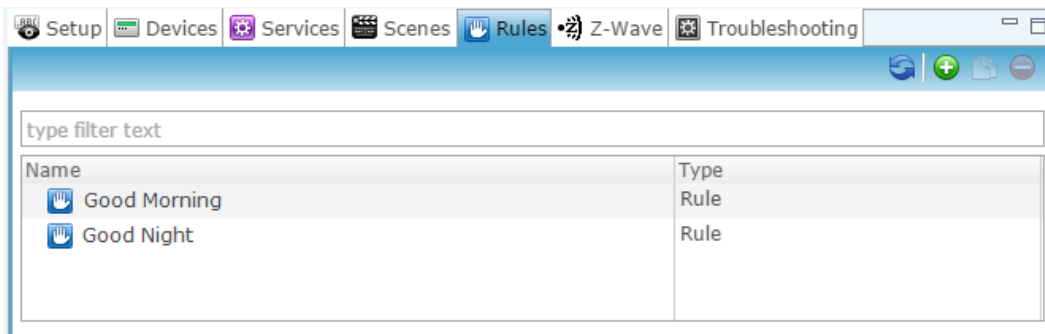
(Optional) Configuring rules with Clare Security

Configure a rule for Clare Security.

The following example sets an Armed Away rule. When the panel is set to Arm Away, all lights are turned off.

To create an Armed Away rule in Fusion:

1. Access your project, and then click the **Rules** tab.



2. Click the **New Rule** button .

3. Enter a name for the rule, and then select the Enable Rule checkbox.

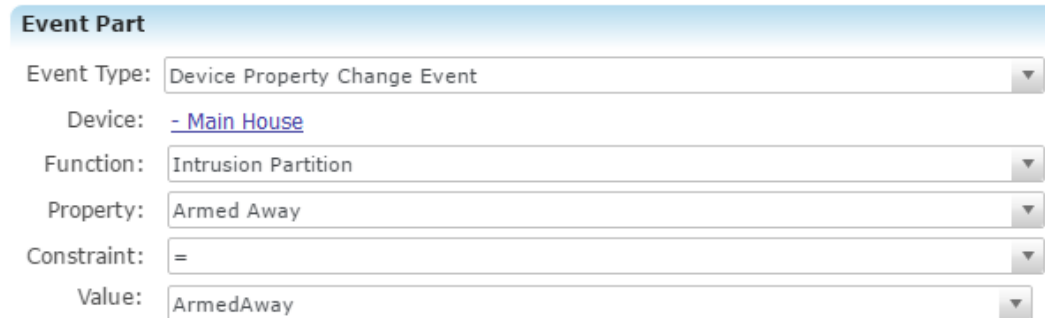


Rule Info

Name: ☒ Enabled

4. Configure the Event Part as below.

- **Event Type:** Device Property Change Event
- **Device:** Security partition device
- **Function:** Intrusion Partition
- **Property:** Armed Away
- **Constraint:** =
- **Value:** ArmedAway



Event Part

Event Type:

Device:

Function:

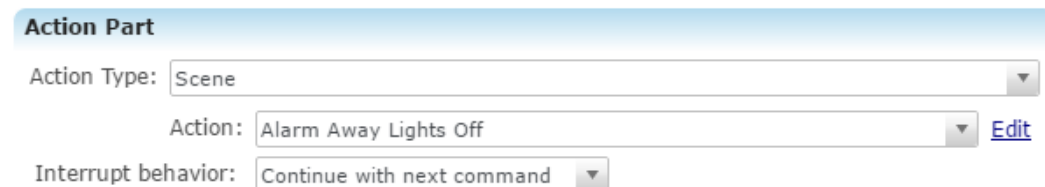
Property:

Constraint:

Value:

5. Configure the Action part as below.

- **Action Type:** Scene
- **Action:** Alarm Away Lights Off
- **Interrupt behavior:** Continue with next command




Action Part

Action Type:

Action: [Edit](#)

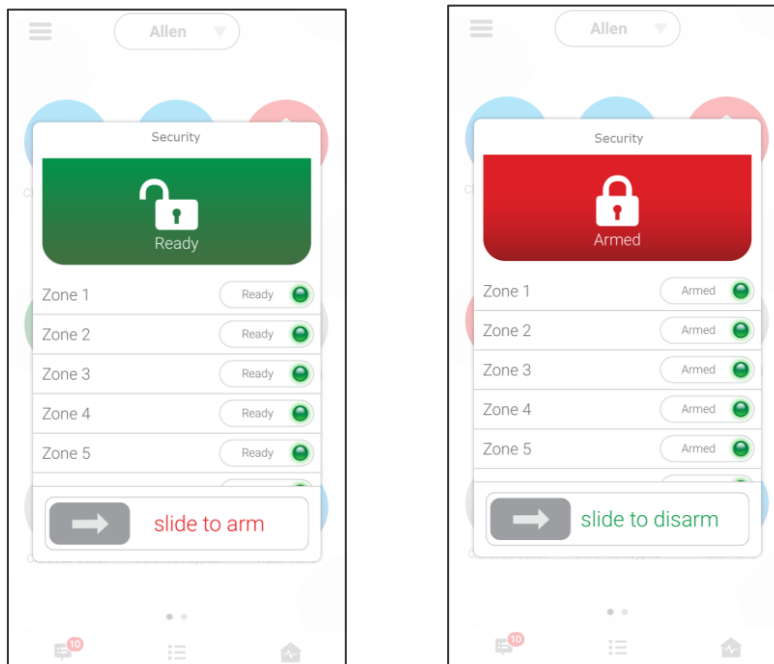
Interrupt behavior:

6. Click **Save** , and then deploy the project.

User interface example

The following figures show the panel controls in the ClareHome App.

Figure 2: Clare Security in the Ready and Armed state



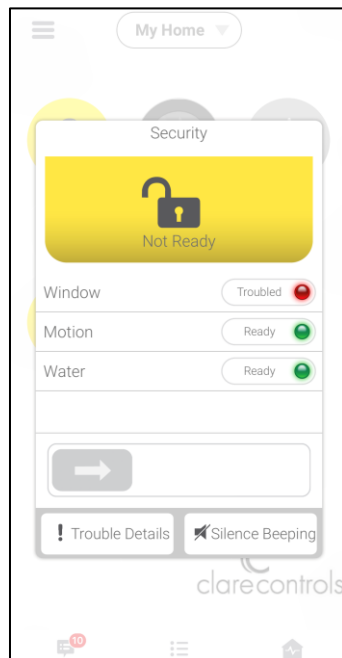
Silence Beeping

The panel supports the Silence Beeping feature. This feature allows the user to silence/stop the panel's beeping due to a troubled state in a panel or zone.

Notes

- Silence Beeping does not stop the Clare Security Alarm from going off.
- Each new troubled state will require the user to silence beeping. For example, if there is currently a troubled water sensor that is silenced, and then the low battery state occurs in the panel, a new set of beeps starts. You must silence them, and each new troubled occurrence.
- Silence beeping last for 24 hours. After 24 hours, if the troubled state is not resolved, the panel resumes the beeping alert.
- Not all trouble conditions cause the panel to beep.

Figure 3: Silence Beeping option



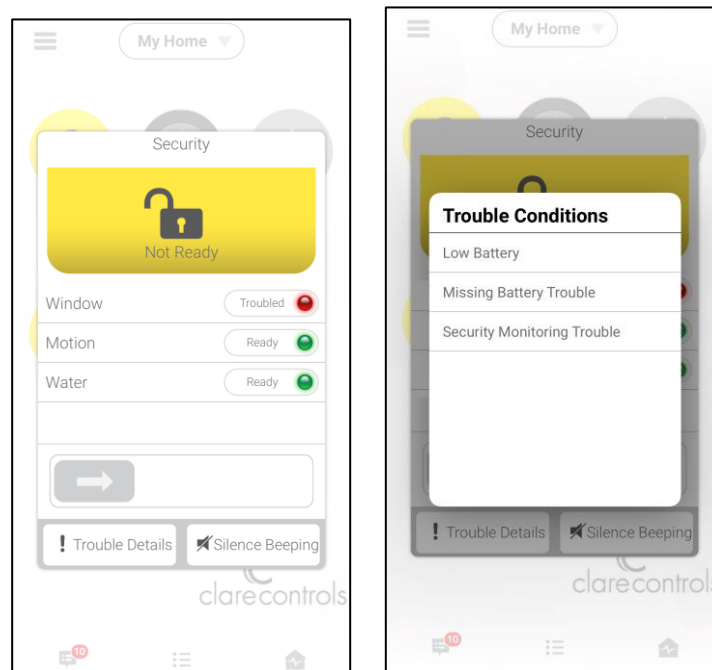
Troubled states

When the panel is troubled, you can view a list of what is causing the troubled state. The panel supports the following troubled states.

Notes

- These are panel states, not zone states.
- These panel states do not prevent the arming/disarming of the panel but alert the user that something may affect their security.

Figure 4: ClareHome App troubled Clare Security panel and trouble conditions



Troubled states

Missing Battery: No battery source is detected in the panel.

Low Battery: The battery in the panel needs to be replaced soon because the battery is low. This may indicate that the panel's battery is failing and not recharging as it should.

Wireless Siren Trouble: The wireless siren has a low battery or is unplugged.

Receiver Jam: The receiver signal is being jammed.

Keypad Trouble: The keypad has a low battery or out of range.

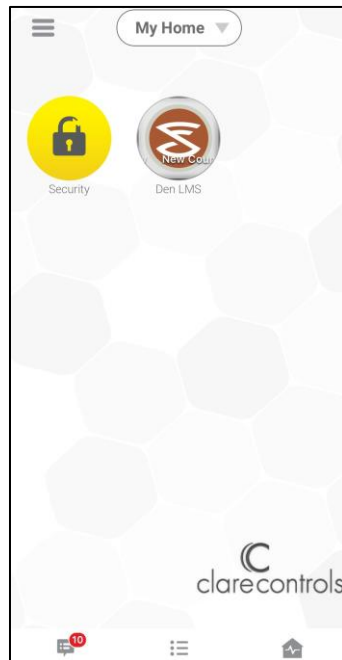
Keyfob Trouble: The keyfob has a low battery.

Power Failure: A power failure in the home faulted the panel, the home may have experienced a power outage, or the panel was unplugged.

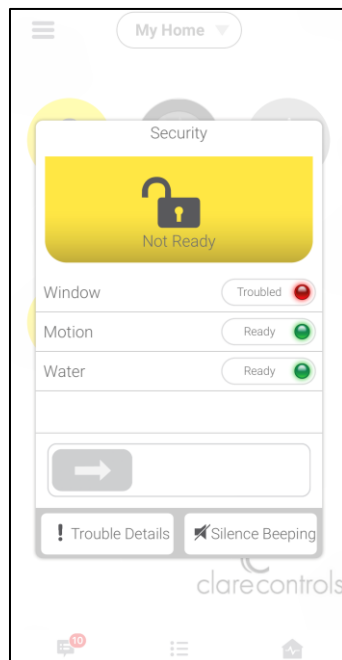
Security Monitoring Trouble: The panel lost connection to ClareNet.

To view the troubled state:

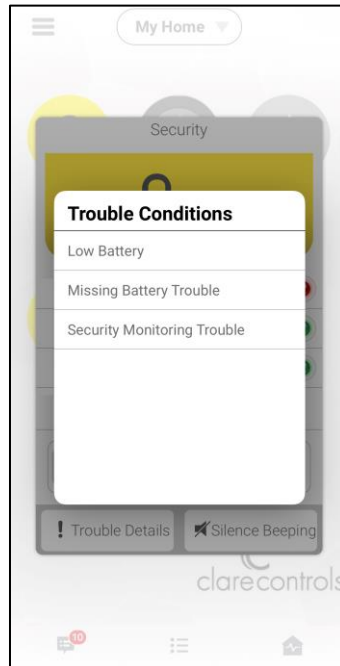
1. Launch ClareHome, and then tap the security UI.



2. Tap **Troubled Details**.



A list of the troubled states displays.



Configuring the ClareNet Activation portal

Once you have successfully added and configured your security panel in Fusion and created your Central Station account, configure the security system in the ClareNet Activation portal.

Notes

- You must be a Clare Controls authorized security dealer to access the ClareNet Portal. To become an authorized dealer, contact Tech Support.
- The Central Station is selected and created outside of Clare Controls. This is an individual company decision, see your security experts for information on the central station services and configuration.
- Verify that the myClareHome form is configured in Fusion. This form contains information vital in making sure that the customer contact information (phone number, address, etc...) is accurate for updates and security alerts.

To configure the ClareNet Activation portal:

1. Browse to the Clare Controls Dealer Dashboard.

2. Click **ClareNet**.

Note: ClareNet is only available when the user is signed in as an authorized Clare Controls security dealer.

A list of projects with security options displays.

The screenshot shows the ClareNet Activation page. At the top, there is a navigation bar with links: Welcome, My Account / Logout, Google Custom Search, and a CART icon showing 0 items for \$0.00. Below the navigation bar is a blue header with the text "ClareNet Activation". Underneath the header is a section titled "Available Projects". It includes a search bar for "Search homeowner, project name, status..." and a filter section showing "6 items" and "Filter: All | Active | Disabled | Not registered". A table lists the available projects:

Project Name	Customer Name	Email	Phone	Street	City	State	Cellular Backup	Central Station
T- House	Smith, J	bb.call@gmail.com	9415555555	1 Toucan Way	Sarasota	Florida		
Taneleer - 7519 Pennsylvania Ave	Taneleer, Tivan	user.email@gmail.com	9415555555	7519 Pennsylvania Ave	Sarasota	Florida		

3. Click on the desired project.

The ClareNet Activation page displays.

The screenshot shows the ClareNet Activation page for the project "Taneleer - 7519 Pennsylvania Ave". The page has a blue header with the text "ClareNet Activation". Below the header is a navigation bar with links: Back to Projects and Taneleer - 7519 Pennsylvania Ave. The main content area is divided into three sections: Security Device, ClareNet, and Cellular Backup. The Security Device section shows the CLIQ Status as Online, Panel Status as Online, Added On as Apr 17 2017, MAC Address as 54:21:60:10:49:35, and Firmware Version as 0.5.7.5. The ClareNet section shows the Status as unavailable and a message that ClareNet could not be reached. The Cellular Backup section shows the Provider as Verizon, Status as Activated, and buttons for Deactivate and Activate. Below these sections are two steps: Step 1: Confirm Information and Step 2: ClareNet Activation. Step 1 includes fields for Email, First Name, Last Name, Street Address, Street Address 2, City, State/Province, ZIP Code, Phone, and Country. Step 2 includes fields for CS Receiver Phone #, Your unique receiver # for the Central Station, CS Account Number, Your account number with the Central Station, CS Auxiliary Number, and CRC Code. There is also a checkbox for Block Open/Close Sending to CS? and a button for Activate Monitoring.

Security Device

- CLIQ Status: Online
- Panel Status: Online
- Added On: Apr 17 2017
- MAC Address: 54:21:60:10:49:35
- Firmware Version: 0.5.7.5

ClareNet

- Status: unavailable
- ClareNet could not be reached.

Cellular Backup

- Provider: Verizon
- Status: Activated
- MEID: [Redacted]
- Buttons: Deactivate, Activate

Step 1: Confirm Information

CLIQ Secure

Email *
users.email@gmail.com

First Name *
Taneleer

Last Name *
Tivan

Street Address *
7519 Pennsylvania Ave

Street Address 2
[Redacted]

City *
Sarasota

State/Province *
Florida

ZIP Code *
34243

Phone *
9415555555

Country
United States

Save

Step 2: ClareNet Activation

CS Receiver Phone #
[Redacted]

Your unique receiver # for the Central Station
[Redacted]

CS Account Number
[Redacted]

Your account number with the Central Station
[Redacted]

CS Auxiliary Number
[Redacted]

CRC Code
[Redacted]

☒ Block Open/Close Sending to CS?
Turning off this feature may generate higher costs with CS

Activate Monitoring

4. Configure **Step 1: Confirm Information.**

Verify and edit the **Confirm Information** fields as necessary.

Step 1: Confirm Information

CLIQ Secure

Email *

users.email@gmail.com

First Name *

Taneleer

Last Name *

Tivan

Street Address *

7519 Pennsylvania Ave

Street Address 2

City *

Sarasota

State/Province *

Florida

ZIP Code *

34243

Phone *

9415555555

Country

United States

Save

5. Click **Save.**

6. Configure **Step 2: ClareNet Activation.**

Step 2: ClareNet Activation

CS Receiver Phone #

Your unique receiver # for the Central Station

CS Account Number

Your account number with the Central Station

CS Auxiliary Number

CRC Code

☒ Block Open/Close Sending to CS?
Turning off this feature may generate higher costs with CS

[Activate Monitoring](#)

CS Receiver Phone #: The central station's receiver phone number.

CS Account Number: The central station account number.

CS Auxiliary Number: This is only required for some central stations.

CRC Code: The code provided on the security panel's box. If the box is not available, please contact the installer.

7. Click **Activate Monitoring**.
8. (Optional) Select weather that Cellular Backup is activated or deactivated.

Note: This is a paid service.

9. Test the alarm functions and verify that the ClareNet Activation portal is connected to the central station.

Note: If any information entered incorrectly the alarm updates and alerts may not function as desired. Clare Controls accepts no responsibility for any security configurations or setup.

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