HSGW-Gen2-V1
IP Alarm System
User Manual

Certified by Telefication BV
Manufacturer: Climax Technology, Taiwan
Type: HSGW-Gen2-V1
Compliance with Standard:
EN50131-3:2009 / EN50131-6:2017 /
EN50131-5-3:2017 / EN50130-4:2011+A1:2014 /
EN50131-10:2014 / EN50136-2:2013 /
EN 50130-5:2011, Security Grade 2
Environmental Class II
CIE Type A

August 19, 2022

Table of Contents

1. INTRODUCTION **1**

1.1. SYSTEM SPECIFICATION 1

1.2. PACKAGE CONTENT 3

2. PANEL INFORMATION **4**

2.1. IDENTIFYING THE PARTS: 4

2.2. THE POWER SUPPLY: 5

2.3. SYSTEM REQUIREMENTS: 5

3. GETTING STARTED **6**

3.1. HARDWARE INSTALLATION 6

3.2. CONNECT TO PANEL 8

4. DEVICE MANAGEMENT **12**

4.1. LEARNING 12

4.2. SENSOR MANAGEMENT 14

5. PANEL MANAGEMENT **17**

5.1. ARMING SETTING 18

5.2. SOUND SETTING 19

5.3. MONITORING STATION SETTINGS 20

5.4. TIMER 21

5.5. TROUBLE CONDITION SETTING 21

5.6. USER CODES 22

5.7. WI-FI SETTING 23

5.8. MISCELLANEOUS SETTING 23

6. SYSTEM SETTINGS **24**

6.1 CENTRAL STATION REPORTING 24

5.2. ENABLING EN GRADE 2/INCERT MONITORING 25

5.3. DATE AND TIME 26

6.4. CHANGE PASSWORD 28

7. NETWORK **31**

7.1. CELL AND IP COMMUNICATION 31

8. SYSTEM OPERATION **33**

8.1 FAULTS AND TAMPERS 33

8.2 VIEW HISTORY 35
8.3 HISTORY 36
8.4. REQUESTING A FIRMWARE UPGRADE 37
8.5 SYSTEM OPERATION AND MAINTENANCE 37
8.5.1 Device Test *37*
8.5.2 IP/GSM reporting *37*
9. AUTOMATION DEVICES 40
9.1. DEVICE LEARNING AND OPERATION 40
10. APPENDIX 41
APPENDIX A: SENSOR GROUPS 41
APPENDIX B: FAULTS 43

1. Introduction

HSGW-Gen2-V1 is a fixed wall mounting wireless alarm system control panel. It is designed to protect your home by forming an alarm system with various wireless sensors. When an intruder is detected, the wireless sensor will transmit signal to the control panel to raise an alarm and report to the Central Monitoring Station.

HSGW-Gen2-V1 features RF and Z-Wave wireless protocol for communication with accessory devices. The RF devices are simple and easy to use while the Z-Wave devices, using corresponding network, is capable of performing more advanced function and add flexibility to alarm system such as using Remote Keypad to control system mode, view alarm memory and event log, or capturing alarm pictures using PIR Camera to send to panel wirelessly for alarm visual verification.

Integrating IP, GSM, Z-Wave and RF for multi-path reporting, HSGW-Gen2-V1 features a user-friendly webpage for the user to connect via Local Area Network for easy programming and control.

1.1. System Specification

Function	
Zone Number	160 Wireless Zones
Area Number	2
Zone Types	Start Entry Delay, Burglar Follow, Burglar Instant, Burglar Outdoor, 24 Hours, Fire, Medical, Emergency, Emergency (Quiet), Water, Set/Unset, Silent Panic, CO, Gas, Heat For information on configuring Zone Groups, please see Appendix A
User PIN Codes	6 Users, 1 PIN Code each user (6-digits, number 0~9), available combination from 000002~999999 (999998 different combinations, 000000 and 000001 are disallowed). Note: Input of 5 invalid User PIN codes at the remote keypad will lock the remote keypad for 15 minutes.
Control Facilities	Remote Keypad & Remote Controller Alarm.com Server Webpages
Report Destinations	20 Monitoring Stations or mobile number
Reporting Format	Contact ID, SIA, SMS Text,
Arming Modes	Away, Home 1, Home 2, Home 3
Alarm Type	Burglar, Panic, Fire, Medical, Emergency, Water, Silent
Siren Timeout	Programmable (3 min. by default), For Remote Keypad use only

Supervision	Programmable time frame for inactivity alert	
Special Function	Tamper Protection	
GSM Standards	Compiles with CE standards	
EN Classification	EN Grade 2 Class II	
Alarm Transmission Path	Dual Path: DP1 (EN50136-1:2012)	
Supported RCT	Alarm Report Server (ARS), Fibro, OH200, MasterMind, Manitou, MicroKey and SIA DC 09	
Mode of Acknowledgement Operation.	Pass-through (EN50136-2:2013, Clause 6.1.3)	
Memory	DDR3L SDRAM: 512Mbyte eMMC : 4GByte	
Electrical		
Power Source	Built-in switching power supply, 100-240V, 50/60Hz input, 12V 1.5A output	
Power Supply Type	PS Type A, not suitable for use external to supervised premises.	
Backup Battery	7.2V, NiMH 600mAh AAA rechargeable battery pack (built-in)	
APS fault Low Voltage SD signal threshold	7.3 V ± 3%	
Battery Duration	14 hours	
Battery Recharge Time to 80% of 600mAH	72 hours	
Minimum Energy Level of Backup Battery	86%	
Current Drain	AC Powered	Average. 126mA/12V standby 839mA/12V full load
	Battery Powered	Average. 42mA/7.2V standby 876mA/7.2V full load
Wireless		
WCDMA Frequency	B1/B2/B5/B8	
LTE Frequency	B1/B2/B3/B4/B5/B7/B8/B28/B40	
RF Frequency	433.82MHz	

Z-Wave Frequency	908.4/916/919.8/921.4M
Antenna Type	GSM: Main – PIFA; AUX – Dipole ZW: Monople RF: Monople
Encryption	Private Encryption Method
Protocol	Climax
Physical Properties	
Operating Temperature	-10°C to 45°C (14°F to 113°F)
Humidity	50 ~ 85% relative humidity @23°C, non-condensing
Size	185mm x 185mm x 50mm
Weight	580g (Includes backup battery)

1.2. Package Content

1 x HSGW-Gen2-V1 Control Panel

1 x AC Power Cord for Built-in S.P.S (12V 1.5A)

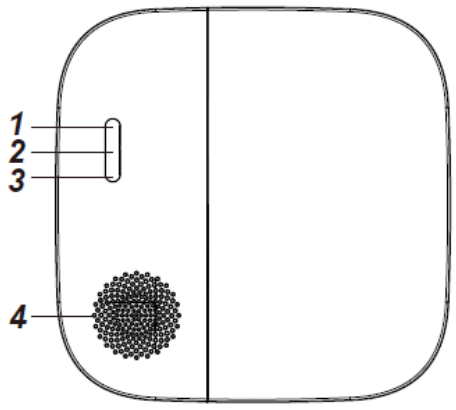
1 x Installation and Instruction Manual

4 x Screws and Wall Plug for wall mounting

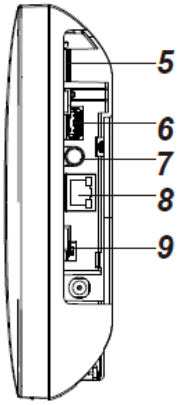
2. Panel Information

2.1. Identifying the parts:

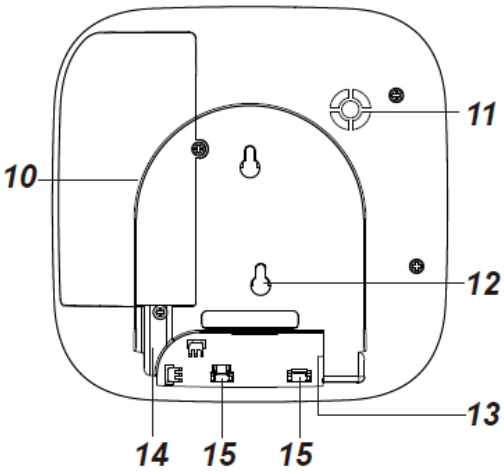
Front Cover view



Side View



Back View



1 LED 1 - Area 1 (Green/Red)

Full Arm mode - Red lighting up

Home/1/2/3 mode - Red flashing

Disarm mode - Green lighting up

Walk Test or Learning mode - Green flashing

2 LED 2 - Area 2 (Green/Red)

Full Arm mode - Red lighting up

Home/1/2/3 mode - Red flashing

Disarm mode - Green lighting up

Walk Test or Learning mode - Green flashing

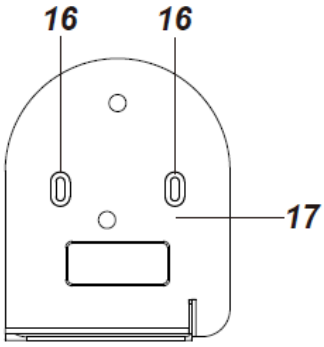
3 LED 3 - Status (Orange/Red)

System Fault - Orange lighting up

Alarm Trigger – Red flashing

Alarm in Memory – Red lighting up

Mounting Bracket



4 Speaker

5 Micro SIM Card Compartment

6 USB Port

7 Learn/Reset Button

8 Ethernet Port

9 Battery Switch (slide to "ON" to meet requirements of the applicable EN standard.)

10 Internal Cover

11 Buzzer

12 Tamper Switch

The panel is protected by an internal tamper switch which is compressed when the panel is

hooked onto the mounting bracket. When the panel is removed from the mounting bracket, the tamper switch will be activated and the panel will send a tamper open signal to remind the user of this condition.

13 **Power Cord Inlet**

14 **Wiring Hole**

15 **Fixing Screws x 2**

16 **Wall Mounting Holes x 2**

17 **Mounting Bracket**

2.2. The Power Supply:

Built-in Power Supply

- Built-in Switching Power Supply (S.P.S) is installed in the Control Panel. You can use the AC Power Cord for Built-in S.P.S to connect to the mains power.

Please note:

☞ ***Ensure to turn off all power supplies including the built-in power supply and battery before connecting or removing cables or wires.***

Rechargeable Battery

- There is a rechargeable battery inside the Control Panel, which serves as a backup in case of a power failure.
- The battery switch for the rechargeable battery must be switched **ON** for the Control Panel to meet requirements of the applicable EN standard.
- During normal operation, the built-in switching power supply is used to supply power to the Control Panel and at the same time recharge the battery.

<NOTE>

☞ If the AC power is missing and the battery is near exhaustion, a low battery message will be displayed and the internal siren will be disabled to conserve power.

☞ When the AC power is restored, the low battery message will be dismissed.

2.3. System Requirements:

The Control Panel requires a TCP/IP network environment to access its webpage for programming and control. To view the Control Panel webpage, your computer must have:

- Microsoft Windows 8 or Windows 10 operating system, or later
- Google Chrome 104 or Mozilla Firefox 103, or later.
- CPU: Intel Pentium II 266MHz or above
- Memory: 32MB (64MB recommended)
- VGA resolution: 800x600 or above

3. Getting Started

Read this section of the manual to learn how to set up your HSGW-Gen2-V1 Panel and program System Settings over the Web page.

3.1. Hardware Installation

The panel can be either fixed on the wall or placed on deskop. **For the panel to meet requirements of the applicable EN standard, wall mounting installation must be used.**

1 Remove the 2 screws that secured the panel casing to the mounting bracket. (Figure 1)

2 Remove the mounting bracket to reveal the back cover fixing screw. (Figure 2)

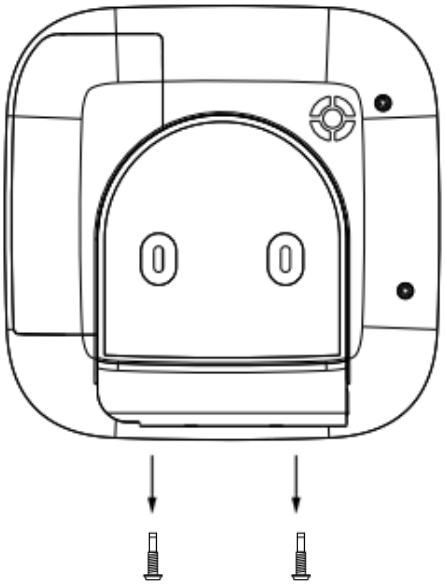


Figure 1

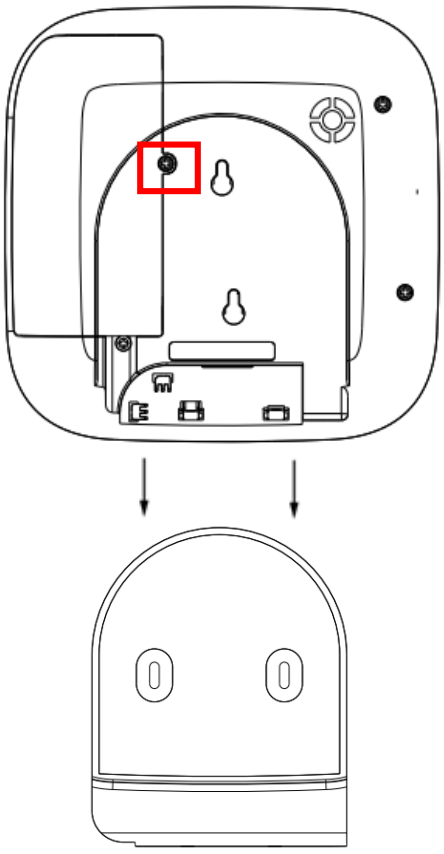


Figure 2

3 Remove the screw securing the back cover (as circled in Figure 2).

4 Set up the Control Panel though the following steps:

I. Connect Ethernet cable to panel Ethernet port.

II. Insert a functional micro SIM Card into Micro SIM Card Compartment, the SIM Card PIN Code must be disabled first.

III. Slide Battery Switch to ON position.

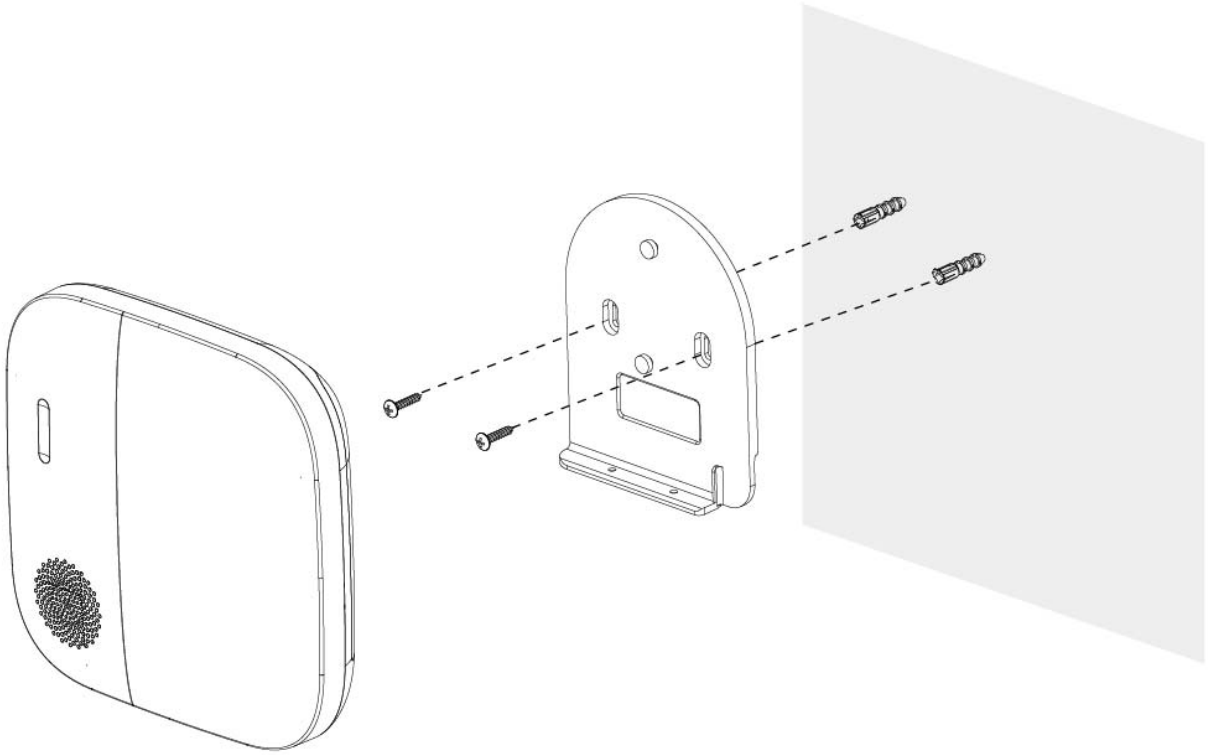
IV. Use the AC Power Cord for Built-in S.P.S to to connect to the mains power.

5 Wire the cable, close the back cover and secure it by fastening the screw. Proceed to mount the panel onto the wall.

Wall Mounting: (EN Compliance)

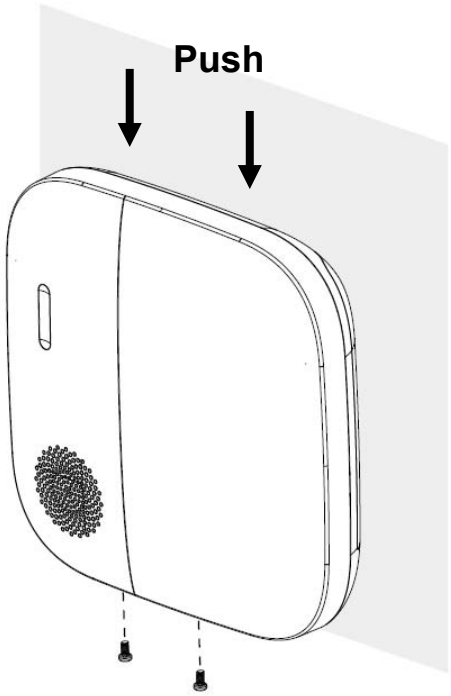
I. Use the mounting holes as template, mark mounting locations on the wall.

II. Secure the mounting bracket onto the wall by tightening the 2 screws through the wall mounting holes.



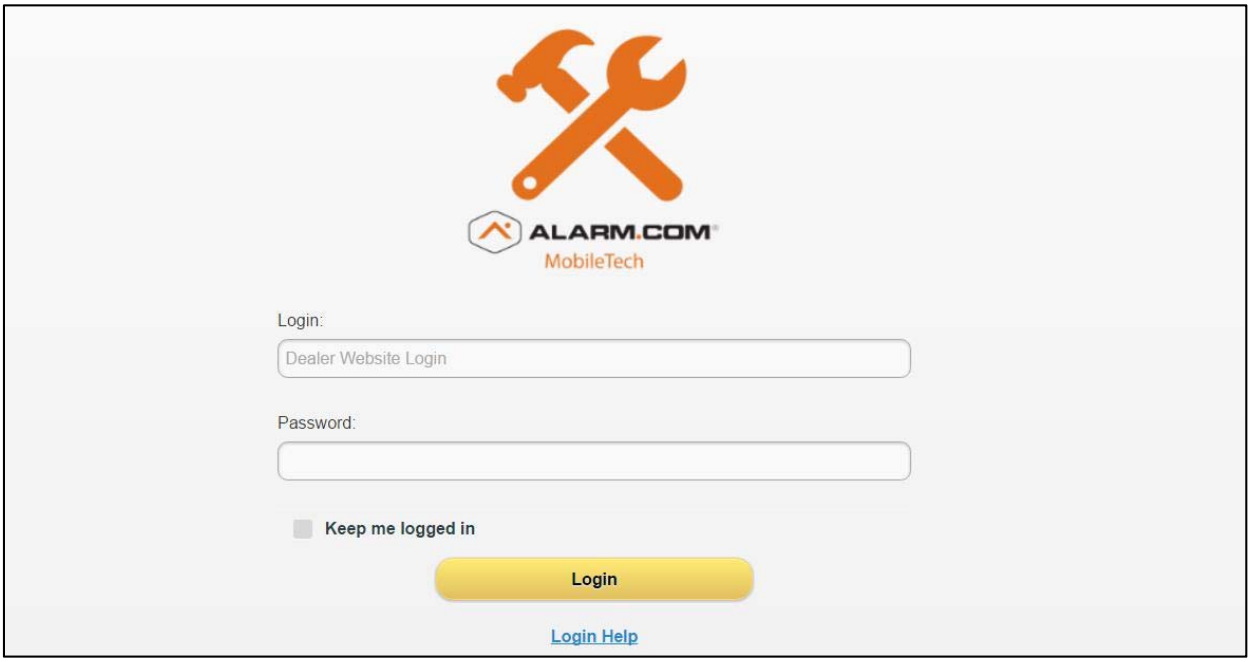
III. Mount the Control Panel with the hooks of the mounting bracket latched onto the back cover of the the panel, and push it downward until you hear a clicking sound.

Make sure the tamper switch is properly compressed against the hook of the mounting bracket. Then fasten the 2 bottom fixing screws to complete the installation.

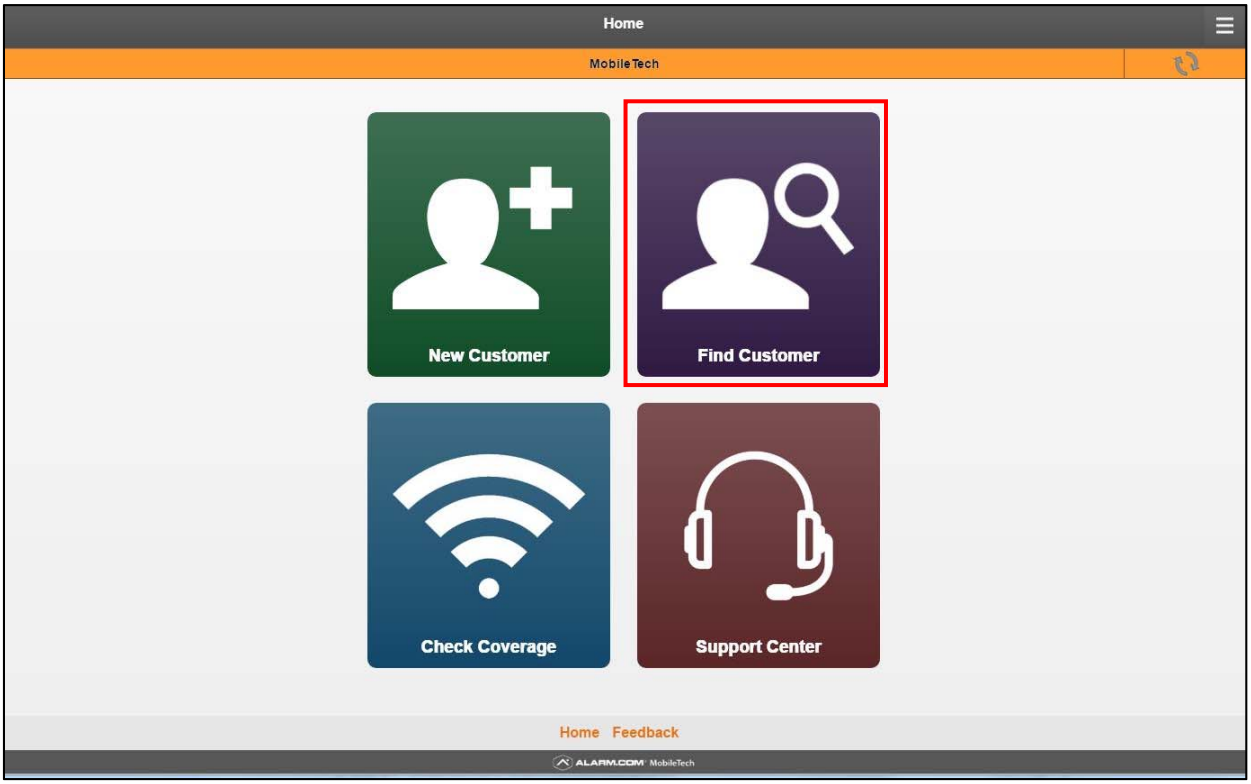


3.2. Connect to Panel

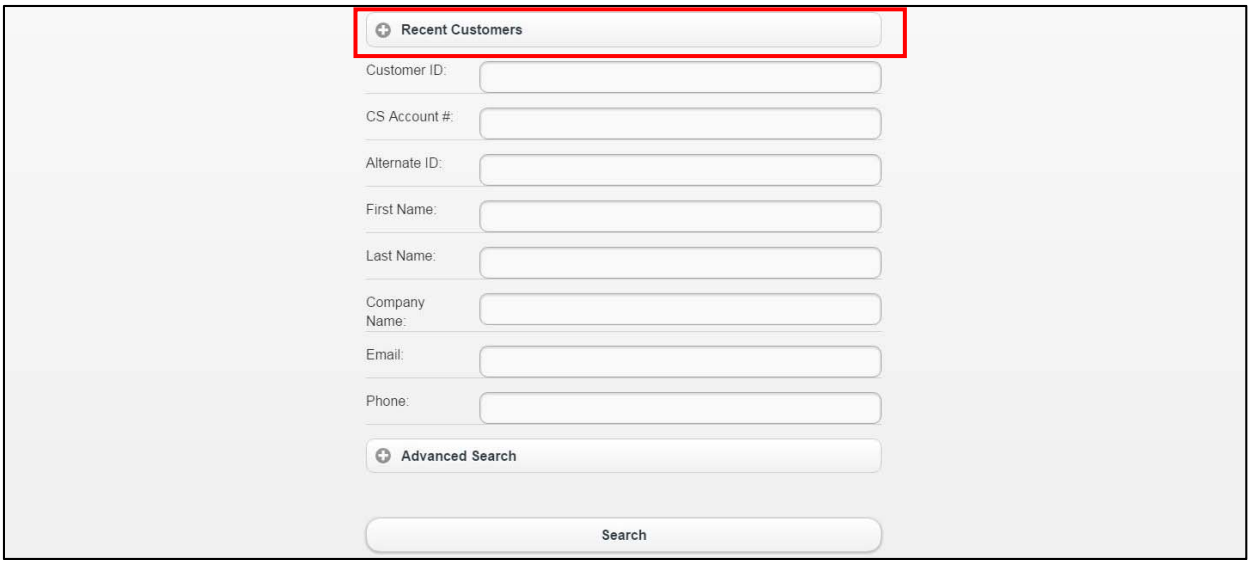
Step 1. Connect to https://alarmadmin.alarm.com/mobile/Default.aspx and log in with provided username and password



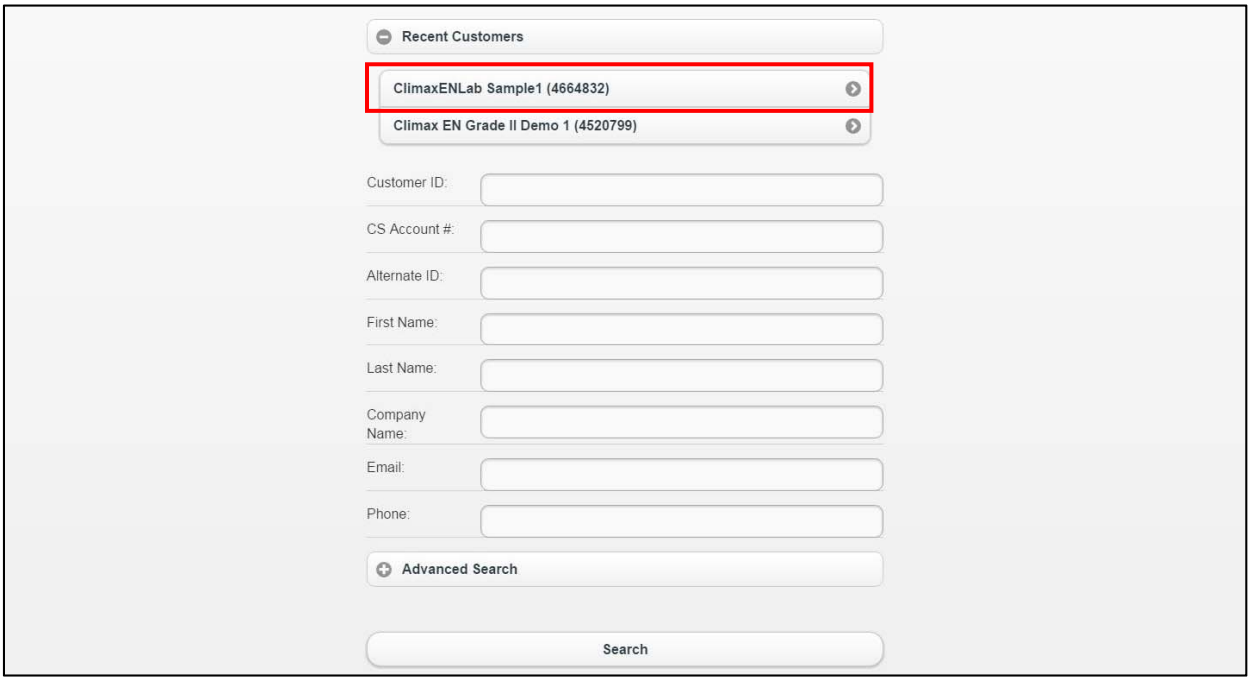
Step 2. In the main page, select “Find Customer”.



Step 3. Select “Recent Customers” to expand.



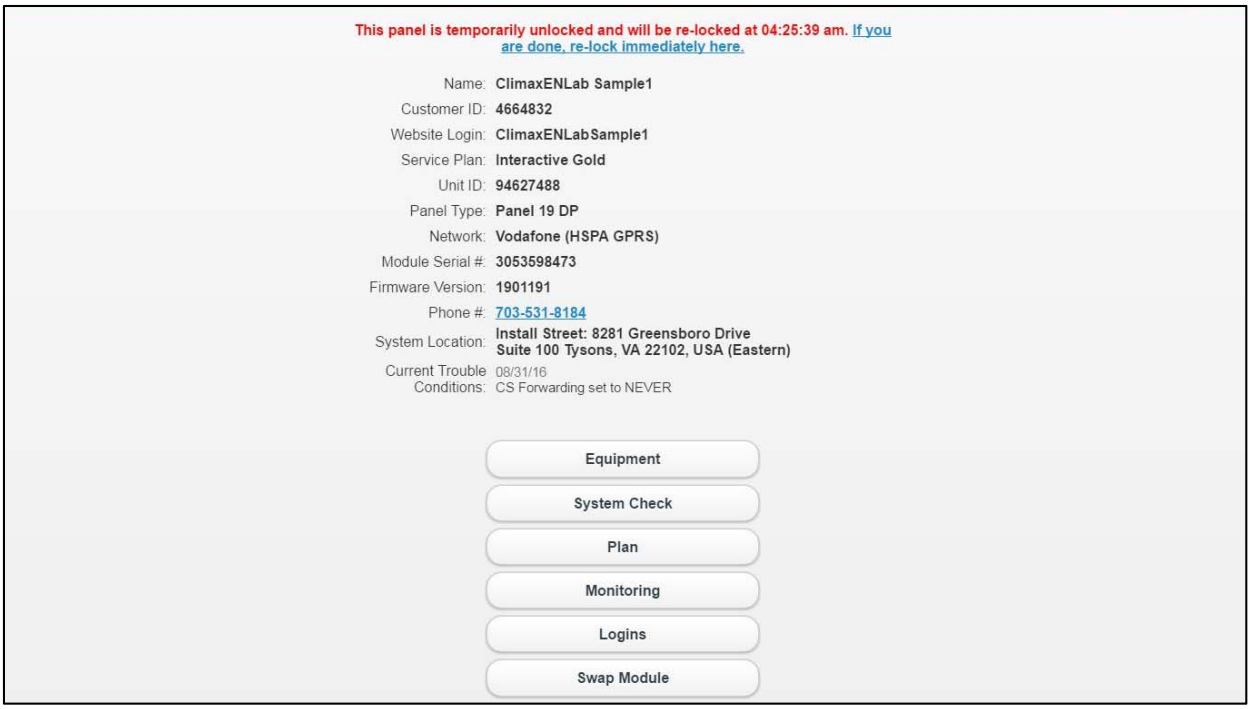
Step 4. Select the panel account you with to access.



<IMPORTANT NOTE>

- ☞ The Installer Access function must be granted by user first to enable installer functions. By default, Installer Access is granted for 6 hours per session.
- ☞ After logging into the Installer App, if there is no activity for 10 minutes, the installers session will timeout and the rep will be logged out of the application.

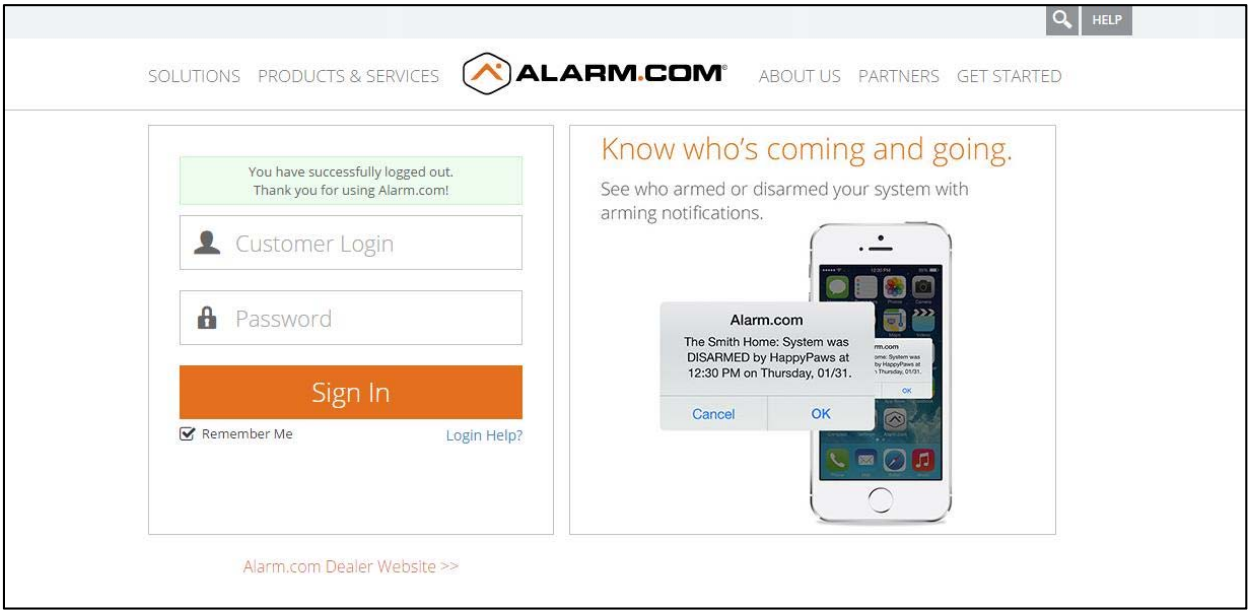
Step 5. You will access the panel user's customer information.



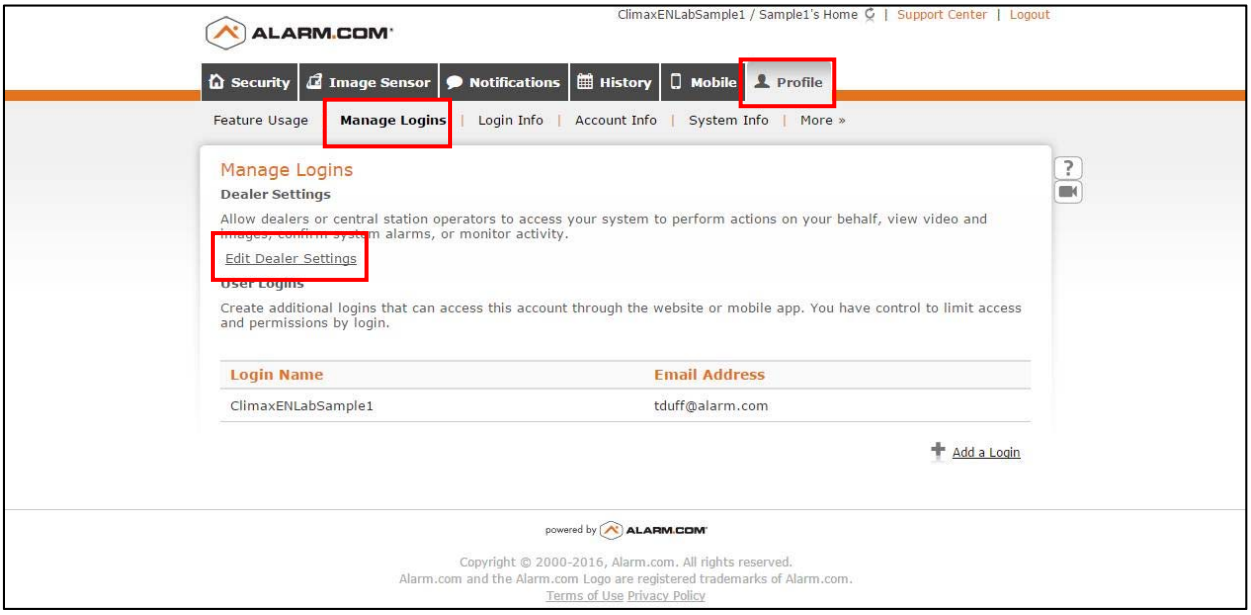
<IMPORTANT NOTE>

- ☞ The Installer Access function must be enabled by user first, otherwise login attempt will fail.
- ☞ To enable user access, ask the user to follow steps below:

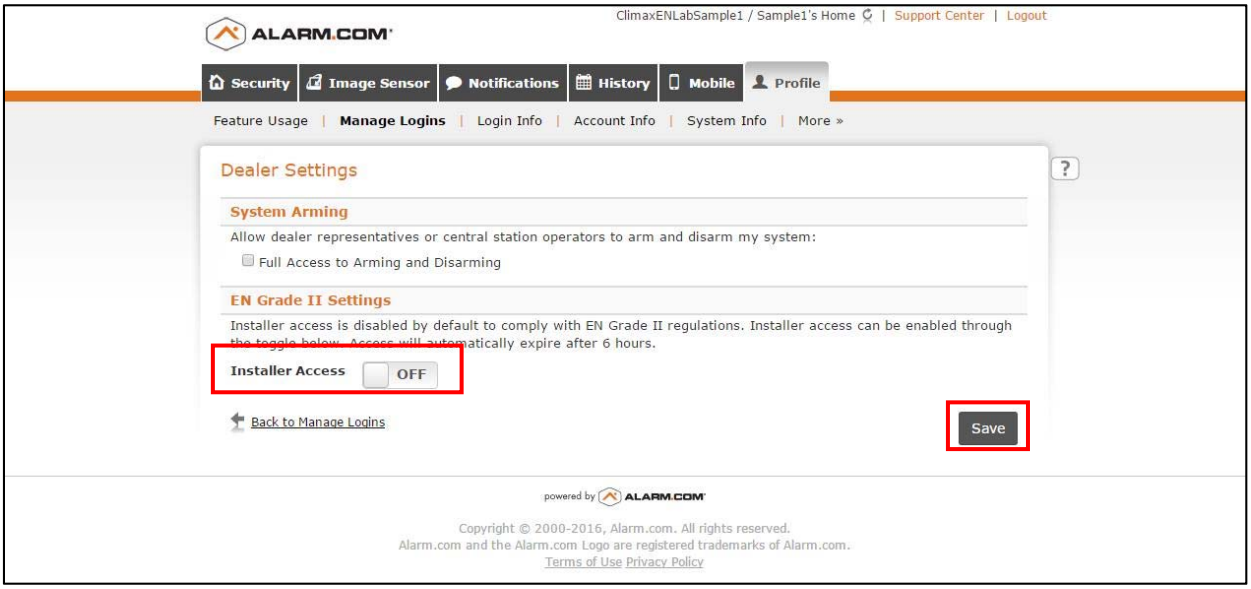
I. Go to https://www.alarm.com/login.aspx and login with the user account information.



II. Select “Profile” – “Manage Logins” – “Edit Dealer Setting”.



III. Set “Installer Access” to “”On” then save the setting.

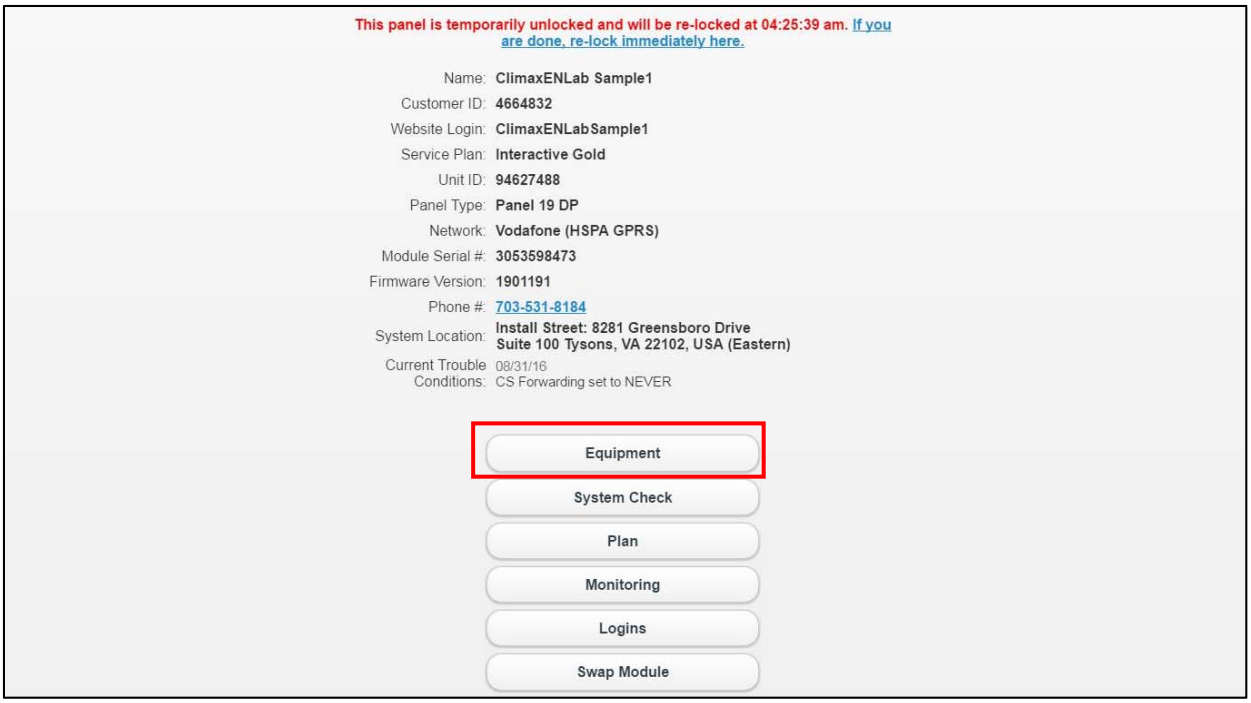


<IMPORTANT NOTE>

☞ After 20 minutes of inactivity on the Customer App, the user’s session will timeout and the user will need to log in again to use any functions.

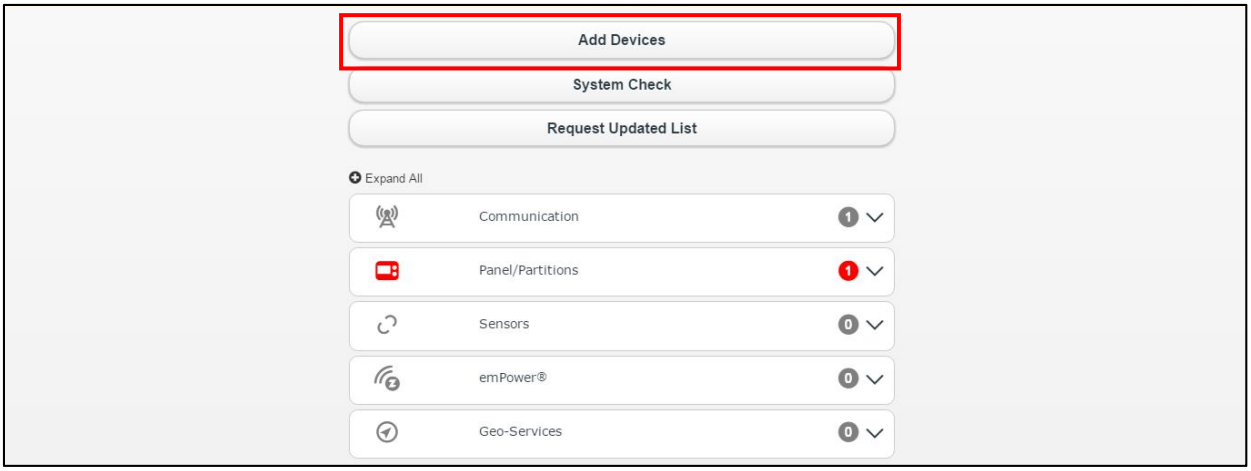
4. Device Management

Under Customer Info page, select “Equipment” to for device management.

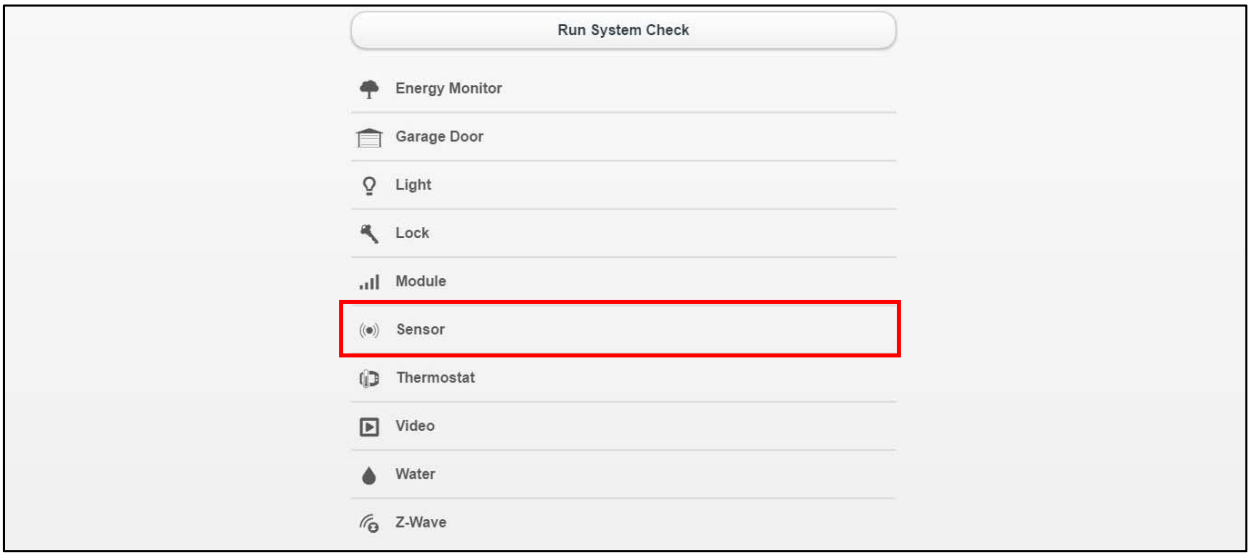


4.1. Learning

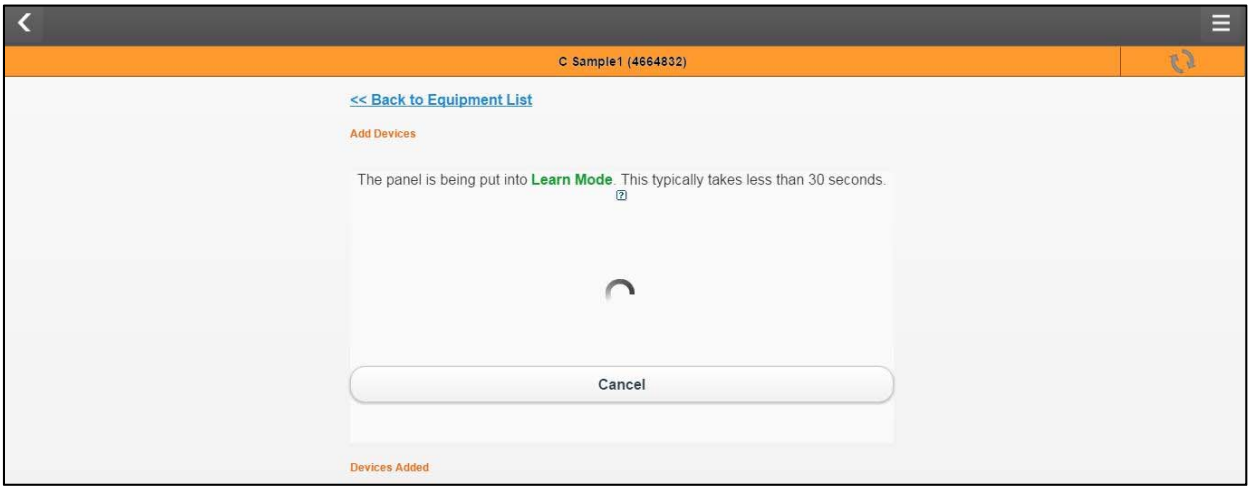
Step 1. Under Equipment page, select “Add Devices”.



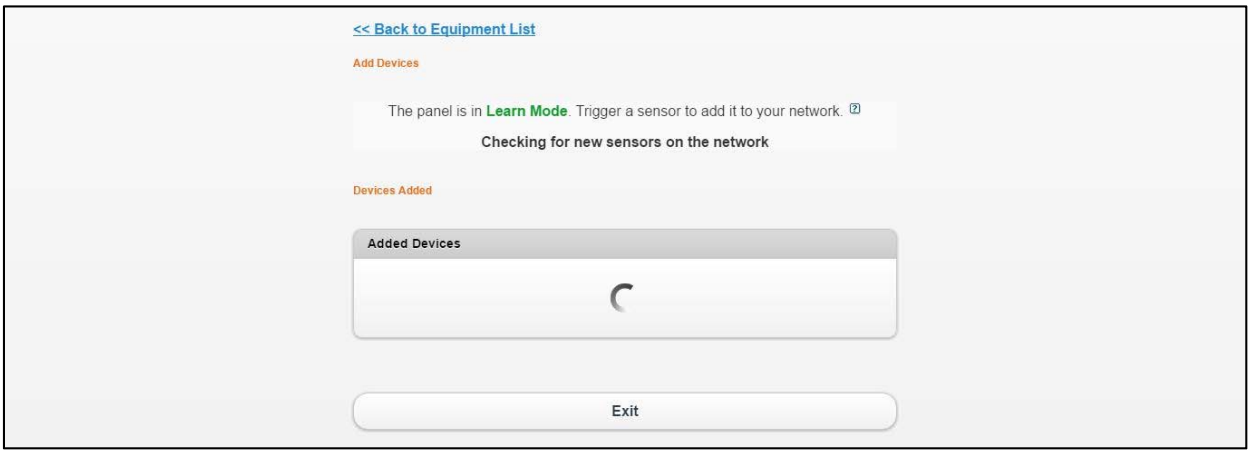
Step 2. Select the device type from the menu. For example, select “Sensor”



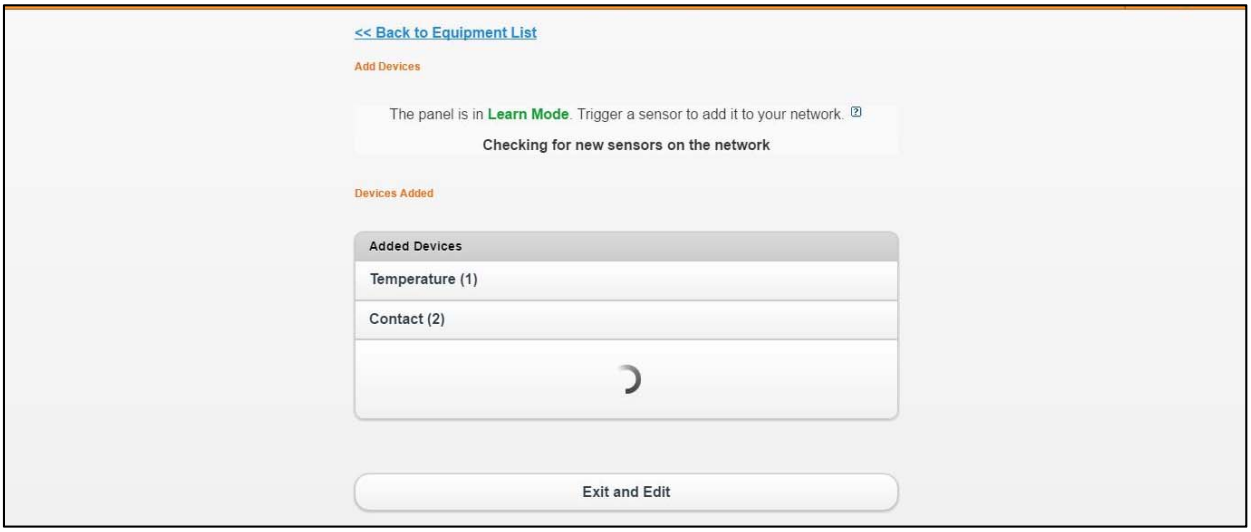
Step 3. The Panel will begin to enter learning mode.



Step 4. After the panel has entered learning mode, activate the device to send signal to panel.

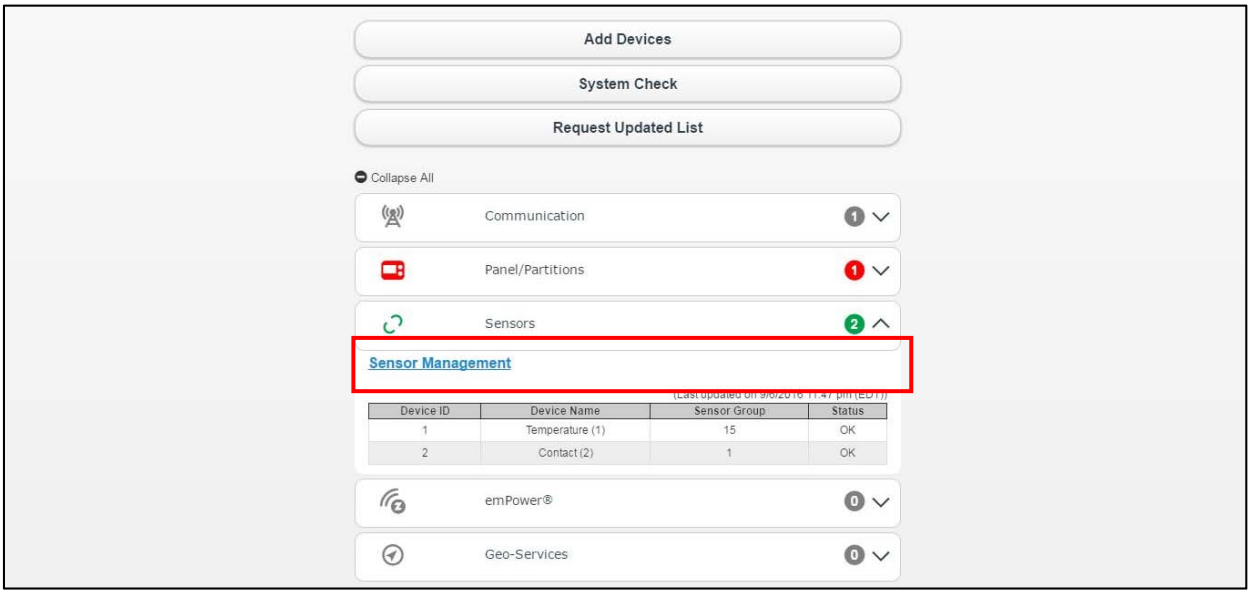


Step 5. When the panel receives sensor signal, the sensor info will be displayed on webpage. Add any additional devices and click “Exit and Edit” to proceed to next step.



4.2. Sensor Management

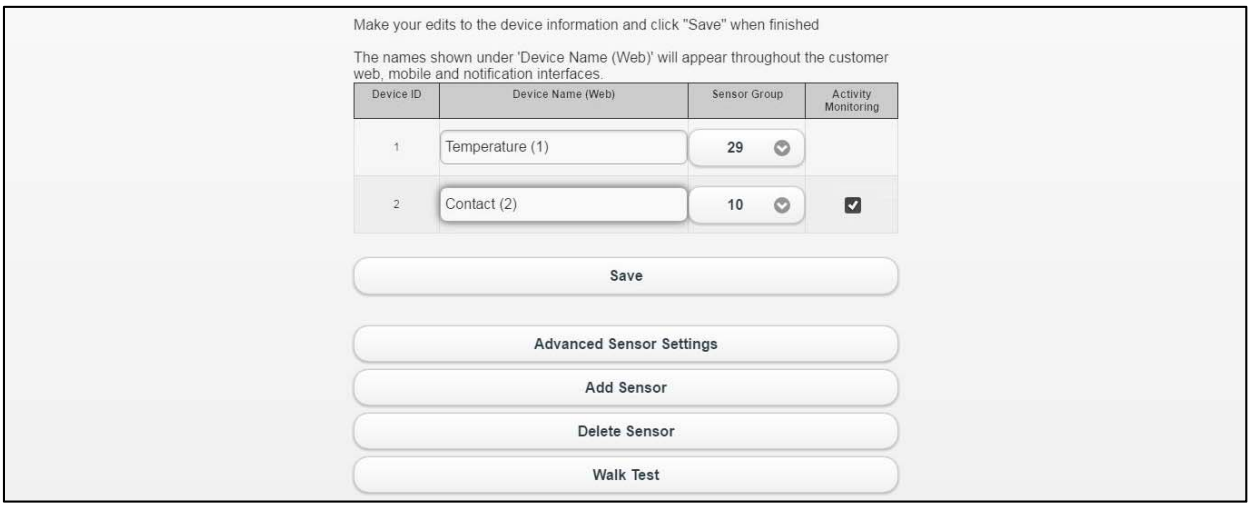
The Sensor Management page can be accessed either after finish adding new device, or by selecting “Sensor” – “Sensor Management” under Equipment page.



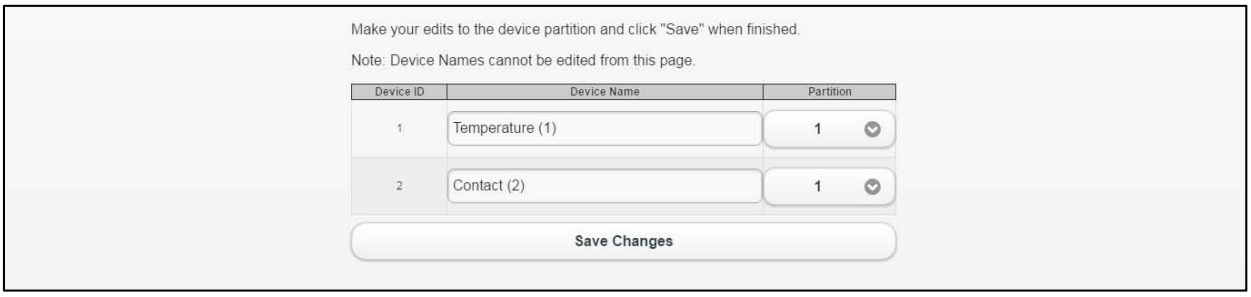
- Under the Sensor Management page, choose to edit device name, sensor group and activity monitoring, the click Save to confirm. Sensor Group allows the configuration of the sensors as different Zone types. Please see Appendix A for descriptions of Sensor Groups.

<NOTE>

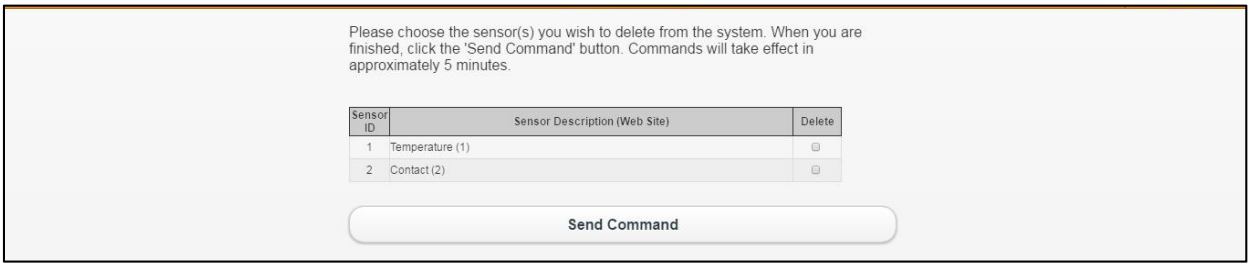
☞ For EN Grade 2 Compliance, the Activity Monitoring box may NOT be checked. Without Sensor Activity Monitoring, Automation rules will still function, however sensor based Notifications from Alarm.com will not work.



- The sensor partition can be edited by selecting “Advanced Sensor Settings”. Choose new partition for the device and click “Save Changes” to confirm.

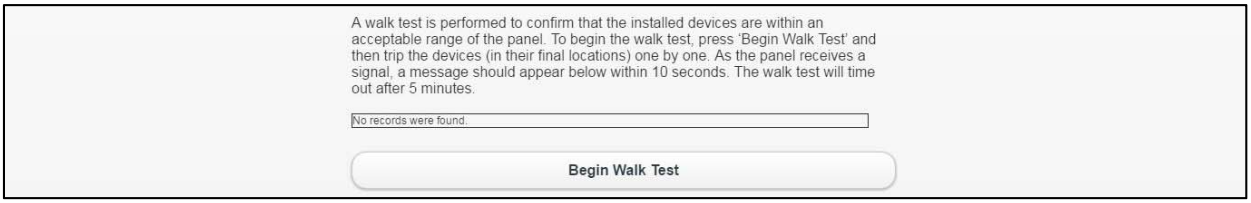


- Click “Add Sensor” to learn new sensors, see *4.1. Learning* for detail.
- Click “Delete Sensor” to remove device, you will enter device removal page. Select the device to be removed and click “Send Command” to confirm.

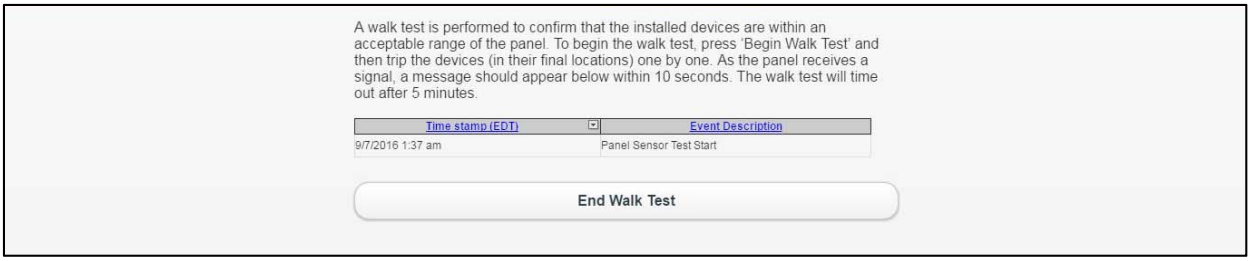


- Click “Walk Test” to access Walk Test function. The Walk Test function allows you to test signal strength of the device.

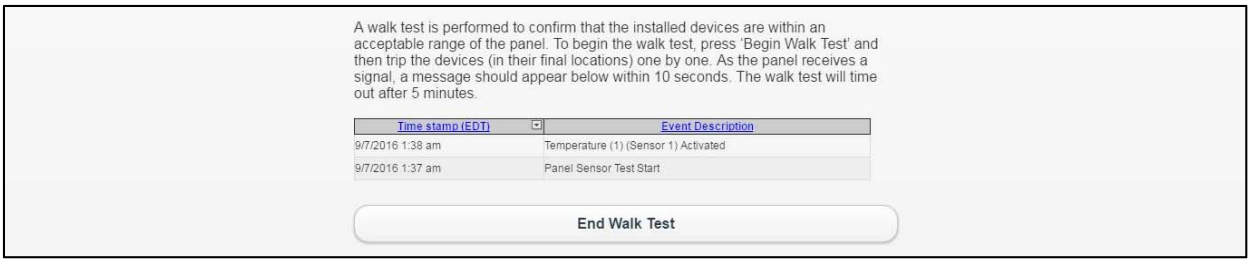
  I. Click “Begin Walk Test” to put panel into Walk Test Mode.



  II. When the panel is under Walk Test mode, activate a learnt in device to send signal to Panel.

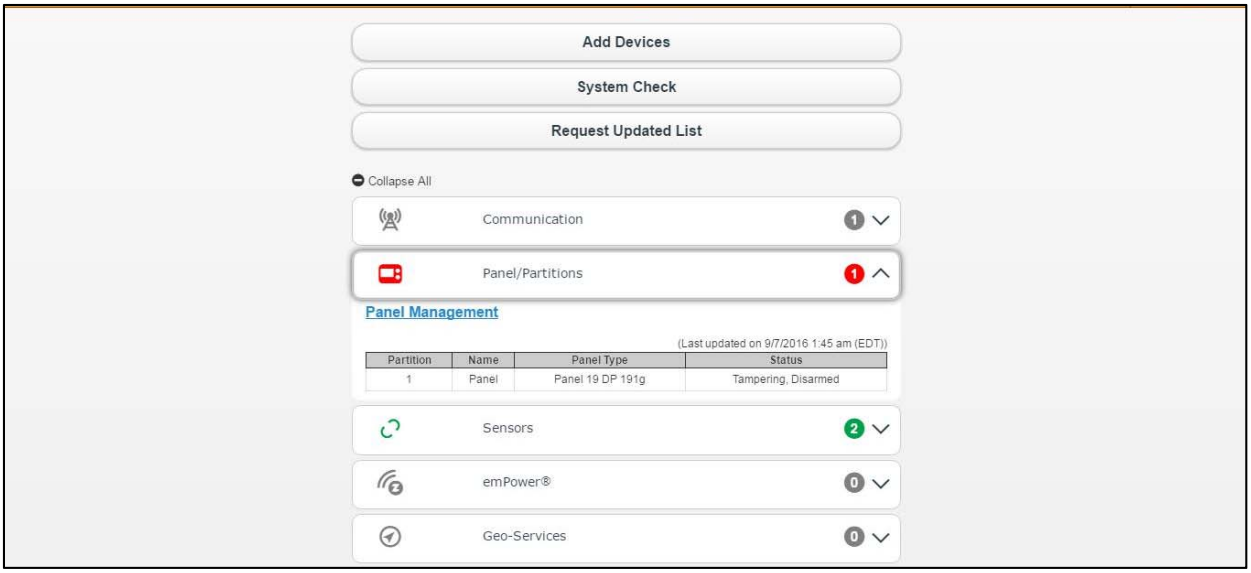


III. When the panel receives signal from panel, the webpage info will be updated with sensor info. After finish testing all sensor, click End Walk Test to exit Walk Test Mode.

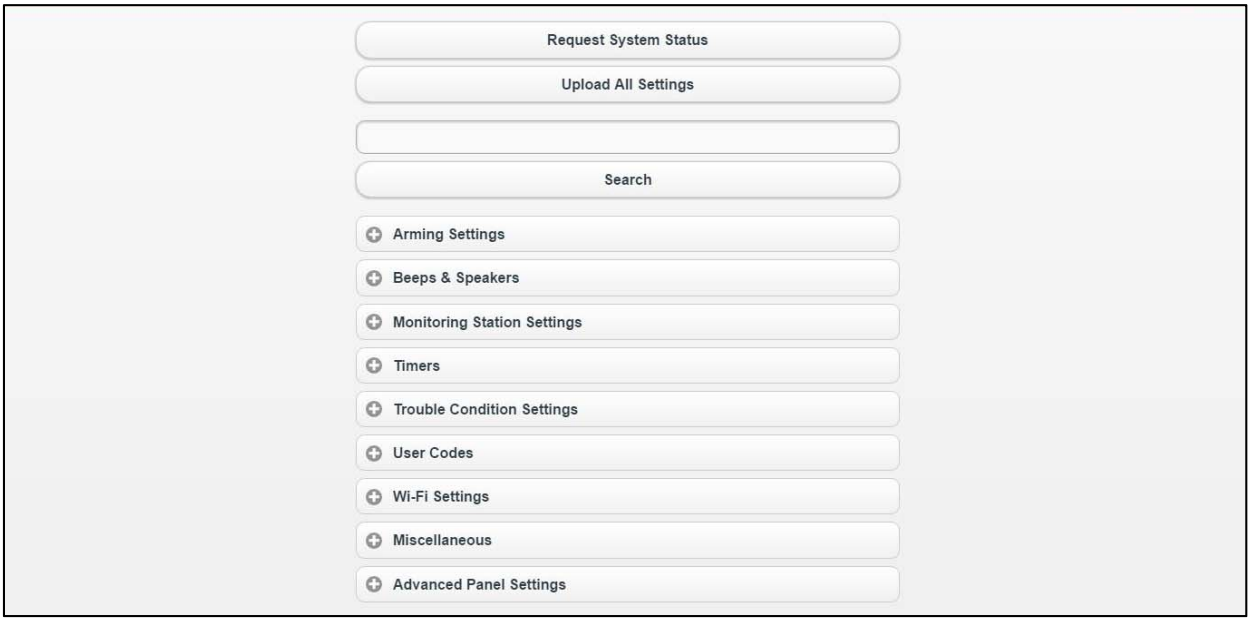


5. Panel Management

Under Customer Info page, select “Panel/Partitions” – “Panel Management” to access panel management page.



Click each option to expand the setting for configuration



<NOTE>

☞ For EN Grade 2 Compliance, the following Panel Management Settings must be configured:

- Auto-Phone Test: 6 hrs.
- Supervision Timer: 2 hrs.
- Swinger Shutdown: 3
- Ethernet Bypass: Disabled
- AC Fail Report Timer: 5 minutes
- Dialer Delay: 0

5.1. Arming Setting

The Arming Setting includes parameters which affects system mode change function. Click “Edit” to modify each setting.

- **Arm Fault Type**: Select how the system should respond when it is being armed under fault condition.
  - ✓ Confirm: The panel will first display a “Mode Change Fault” message and emit 2 beeps. Arming again within 10 seconds will force arm the system.
  - ✓ Direct Confirm: The system will be force armed directly without displaying fault message and report an event.
- **Final Door**: If set to **On**: When the system is Away Armed and under exit timer countdown, if an opened Door Contact is closed, the system will automatically arm the system even if the exit delay timer has not expired yet.
- **Entry Delay 1 for Arm Away**: Set Entry Delay Timer 1 for Away Arm mode. When a sensor set to Start Entry Delay 1 is triggered under Away Arm mode, the control panel will begin Entry Delay Timer countdown according to duration set with this option

  If the Control Panel is disarmed before the Entry Delay Timer expires, the panel returns to Disarm mode and no alarm is activated. If the Control Panel is not disarmed before the Entry Delay Timer expires, the alarm will be activated and the panel will send report.
- **Entry Delay 1 for Arm Stay**: Set Entry Delay Timer 1 for Arm Stay mode. When a sensor set to Start Entry Delay 1 is triggered under Arm Stay mode, the control panel will begin Entry Delay Timer countdown according to duration set with this option

  If the Control Panel is disarmed before the Entry Delay Timer expires, the panel returns to Disarm mode and no alarm is activated. If the Control Panel is not disarmed before the Entry Delay Timer expires, the alarm will be activated and the panel will send report.
- **Entry Delay 2 for Arm Stay**: Set Entry Delay Timer 2 for Arm Stay mode. When a sensor set to Start Entry Delay 2 is triggered under Arm Stay mode, the control panel will begin Entry Delay Timer countdown according to duration set with this option

  If the Control Panel is disarmed before the Entry Delay Timer expires, the panel returns

to Disarm mode and no alarm is activated. If the Control Panel is not disarmed before the Entry Delay Timer expires, the alarm will be activated and the panel will send report.

- **Entry Delay 2 for Arm Away**: Set Entry Delay Timer 2 for Away Arm mode. When a sensor set to Start Entry Delay 2 is triggered under Away Arm mode, the control panel will begin Entry Delay Timer countdown according to duration set with this option

  If the Control Panel is disarmed before the Entry Delay Timer expires, the panel returns to Disarm mode and no alarm is activated. If the Control Panel is not disarmed before the Entry Delay Timer expires, the alarm will be activated and the panel will send report.

- **Exit Delay for Arm Away**: Set the Exit Delay Timer when entering Arm Away mode. When the user changes system mode to Away Arm, the panel will begin Exit Delay Timer Countdown and enter Away Arm mode when the timer expires. The user must leave area protected by sensors before the timer expires, otherwise an alarm will be activated with the sensor is triggered.
- **Exit Delay for Arm Stay**: Set the Exit Delay Timer when entering Arm Stay mode. When the user changes system mode to Arm Stay, the panel will begin Exit Delay Timer Countdown and enter Arm Stay mode when the timer expires. The user must leave area protected by sensors before the timer expires, otherwise an alarm will be activated with the sensor is triggered.
- **Alarm Length**: Set the duration the external siren should sound when an alarm is activated. For EN Grade 2 Compliance, this should be set to a minimum of 1 minute.
- **Swinger Shutdown**: This indicates the maximum number of Events that will be recorded by an individual device per Set/Unset period. *For EN Grade 2 Compliance, this must be set between 3 and 10.*

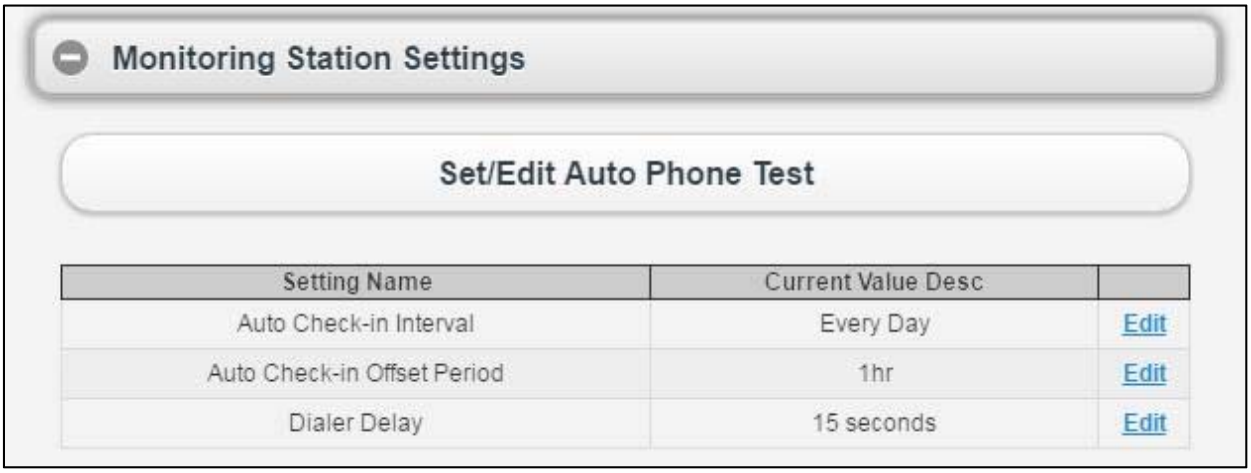
5.2. Sound Setting

The sound setting determines panel indication sound configuration. To change existing setting, click “Edit”.

- **Entry Delay Sound for Arm Away**: this is for you to decide whether the Control Panel sounds count-down beeps and volume of beep during the entry delay time in Away Arm mode.
- **Exit Delay Sound for Arm Away**: this is for you to decide whether the Control Panel sounds count-down beeps and volume of beep during the exit delay timer in the Away Arm mode.

- **Entry Delay Sound for Arm Stay**: this is for you to decide whether the Control Panel sounds count-down beeps and volume of beep during the entry delay time in Arm Stay mode.
- **Exit Delay Sound for Arm Stay**: this is for you to decide whether the Control Panel sounds count-down beeps and volume of beep during the exit delay timer in Arm Stay mode.
- **Entry/ Exit Only Final Beeps:** This is for you to determine when the Control Panel should start warning beep during Entry or Exit countdown timer. For example, if the setting is set to 5 seconds, the Control Panel will only stat warning beep during the last 5 seconds of Entry or Exit countdown timer. When set to Disable, the Control Panel will sound warning beep during the entire Entry or Exit countdown timer.
- **Door Chime Setting**: Select the volume for door chime notification sound.

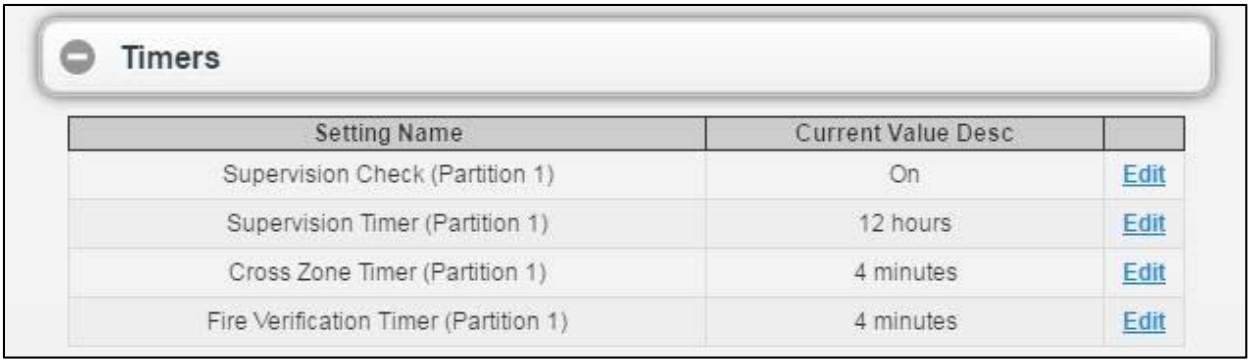
5.3. Monitoring Station Settings



The Monitoring Station setting allows monitoring station reporting configuration.

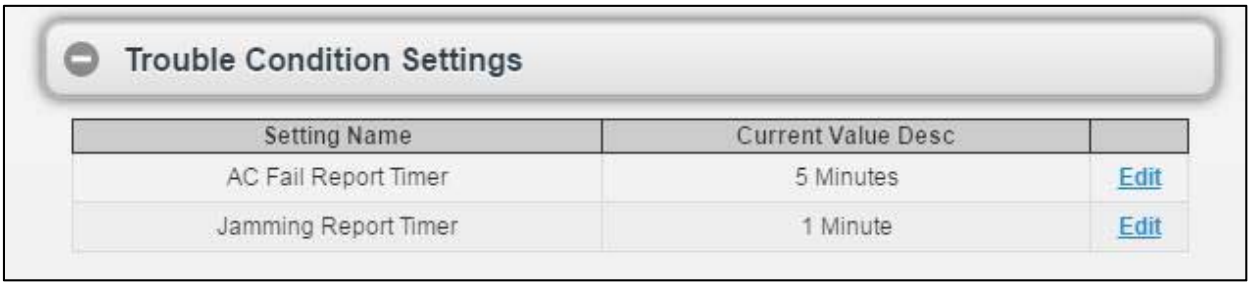
- **Set/Edit Auto Phone Test**: Set to turn ON or Off the auto phone test function. This function must be set to ON for the other functions in this menu to be used.
- **Auto Check-in Interval**: Set the waiting interval between each auto check-in report. *Note: This must be set to 6 hrs or smaller to meet the requirements of EN Grade 2.*
- **Auto Check-in Offset Period**: This is to set the time delay before the first **Auto Check-In** report is made. After power is supplied or re-supplied to the Control Panel, a test report will be sent to the Monitoring Station based on the Offset Period. This is used to test whether the Monitoring Station is able to receive the report from the Panel accurately.
- **Dialer Delay**: Set the waiting time before dialing for report.

5.4. Timer



- **Supervision Check**: Select to enable or disable system supervision function. When **ON** is selected, the Control Panel will monitor the accessory devices according to the supervision signal received.
- **Supervision Timer**: The Control Panel monitors accessory devices according to the supervision signal transmitted regularly from the device. User this option to set a time period for receiving supervision signals. If the Control Panel fails to receive supervision signal from a device within this duration, it will consider the device out of order and report the event accordingly. NOTE: This must be set to 2 hours or less to meet the requirementes of EN Grade 2.
- **Cross Zone Timer**: When a Sensor configured for Cross Zone Monitoring is tripped, this timer begins to count down. If a different zone is tripped in this time period the control panel will report a Burglar Alarm, otherwise the panel will report a Cross Zone Trouble event. Repeatedly tripping the zone configured for cross zone monitoring will reset the Cross Zone Timer.
- **Fire Verification Timer**: When a Smoke Detector set to Fire Verification attribute is triggered, the panel begins to sound alarm, counts down Fire Verification Timer and reports a Near Alarm event (CID 118). Triggering a regular Smoke Detector with Smoke attribute during the Fire Verification Timer will prompt panel to report Smoke Alarm event (CID 111), the timer will not be reset. When the Fire Verification Timer expires, the panel reports Fire Verification Timeout event (CID 695).

5.5. Trouble Condition Setting



The Trouble Condition Setting determines panel report time when AC failure or RF jamming is detected.

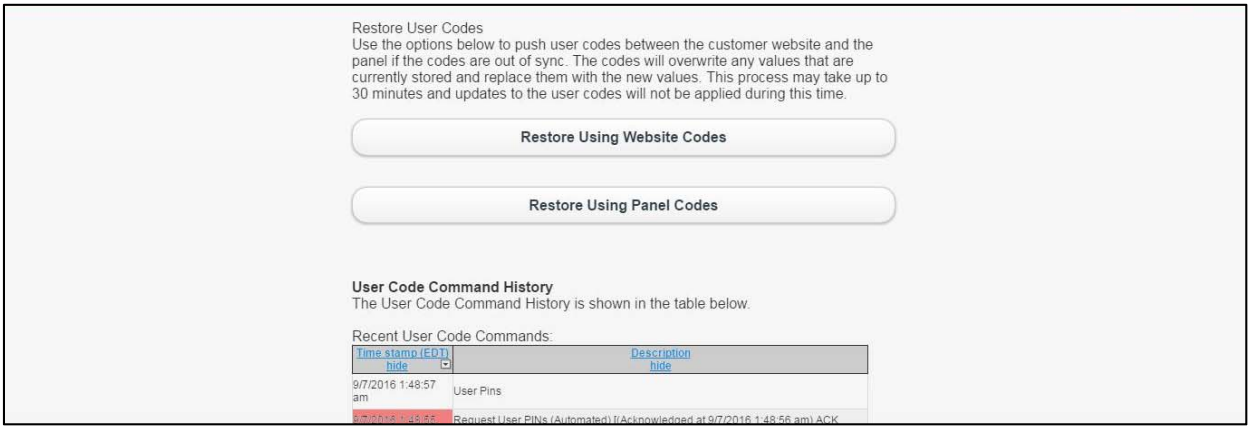
- **AC Fail Report Timer**: Set the waiting time before Control Panel report to Monitoring Station when AC failure is detected.
- **Jamming Report Timer**: Set the waiting time before the panel report to Monitoring Station when radio inteference is detected.

5.6. User Codes

The User Codes setting allows configuration of access codes stored in the panel.

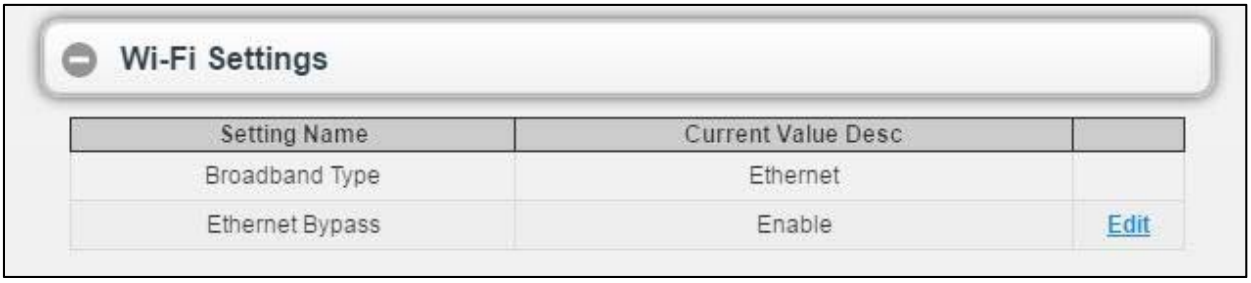
- **Edit Panel User Codes**: Select to edit the panel user code, then click “Manage User Code” to access the panel user interface and program User setting. **NOTE:** Only 6 six user codes are available on EN Grade 2 Compliant panels

- **Restore User Code**: If the panel and the web server User Code setting is out of synchronization, use this function to retore the User Code Setting. Choose to either synchornize using the codes stored n the website, or with the codes stored inside the panel.



- **Dealer Code:** Set the Dealer code use to resolve panel faults for INCERT.

5.7. Wi-Fi Setting

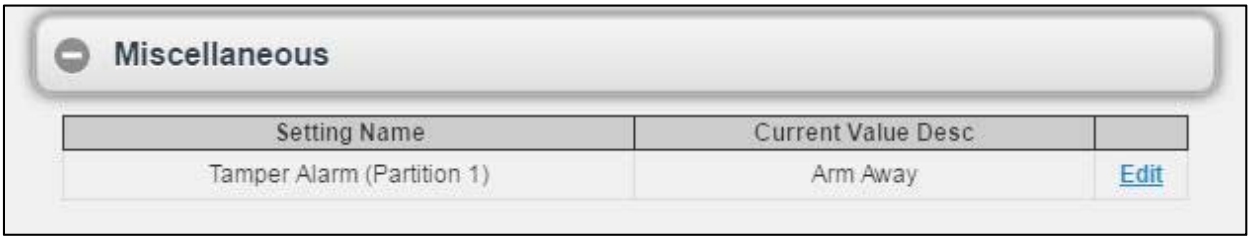


The Wi-Fi setting allows you to check panel broadband setting, and determine whether Ethernet connection should be bypassed.

<NOTE>

- ☞ For EN Grade 2 Compliance, Ethernet Bypass must be set to “Disable”:

5.8. Miscellaneous Setting



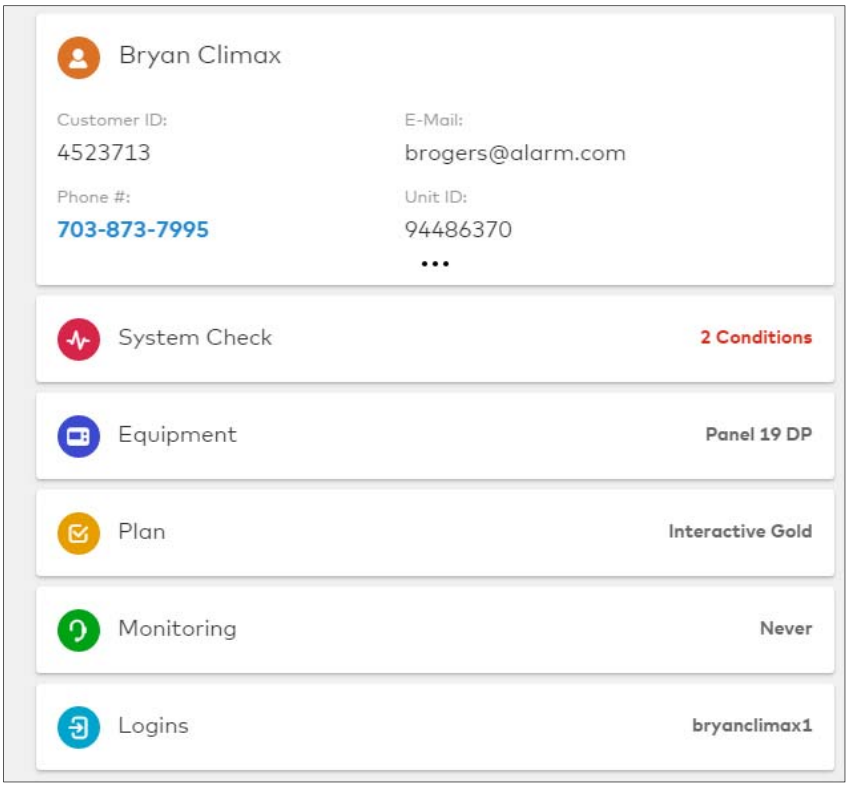
The Miscellaneous Setting includes following setting option:

- **Tamper Alarm**: Select when the panel should activate alarm if tamper switch is triggered.
  - ✓ Arm Away: when tamper is triggered under Away Arm mode, Control Panel raises a local alarm and sends report to the monitoring center. While under Arm Stay or Disarm modes no alarm will be activated, nor report sent.
  - ✓ Always: Control Panel raises a local alarm and send report for tamper-trigger in all modes.

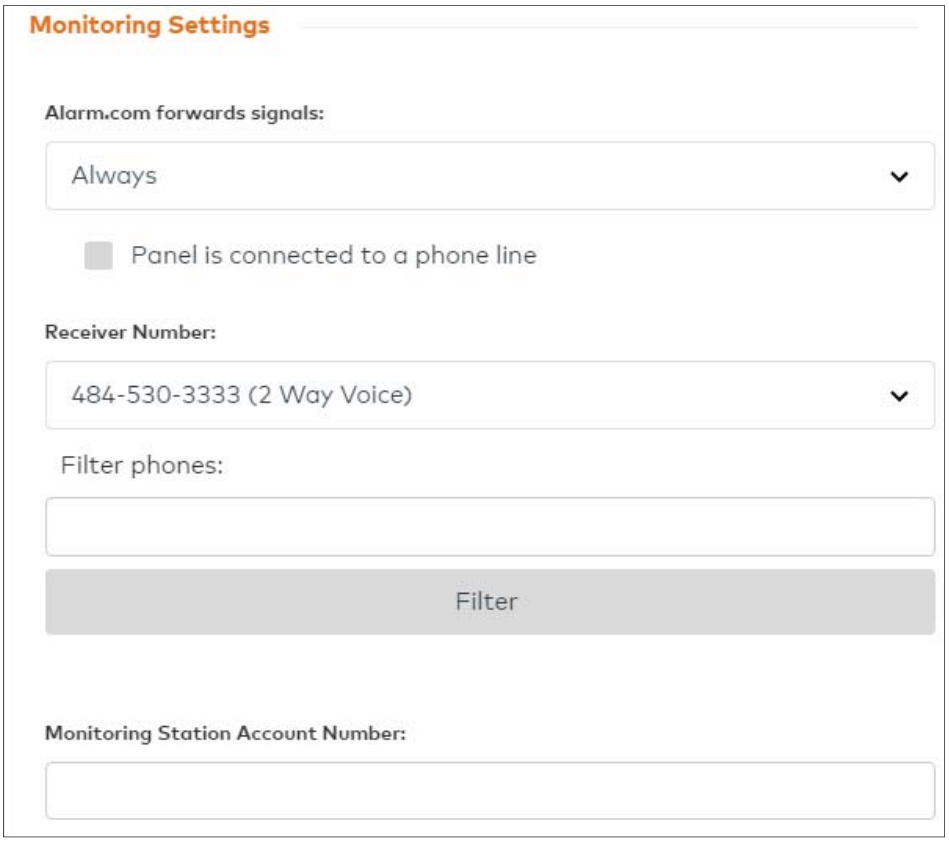
6. System Settings

6.1 Central Station Reporting

Please follow the steps below to enable Central Station reporting and choose which events are reported to a central station.



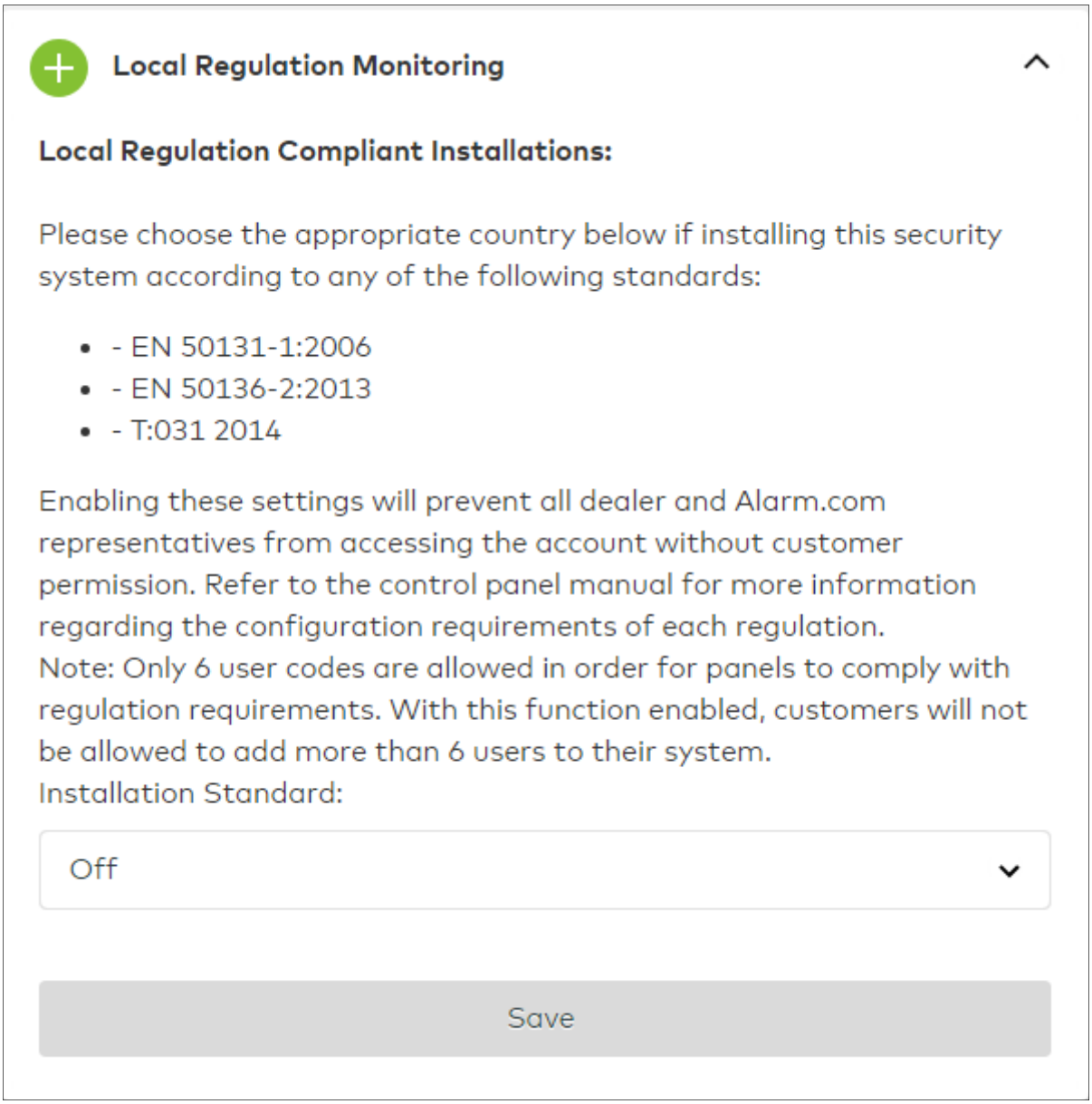
From the “Customer Info” page, select “Monitoring.



Under Monitoring Settings, set the “Alarm.com forwards signals” option to “Always.” Choose the Receiver Number, Monitoring Station Account Number, and which events to forward to the Central Station.

5.2. Enabling EN Grade 2/INCERT Monitoring

To comply with the EN Grade 2/INCERT security regulations, Local Regulation settings must be enabled. This setting will enable Level 3 user lockout and reset the panel settings to the minimum default values required by the regulation. To enable Local Regulation monitoring, go to **Monitoring > Local Regulation Monitoring** and select the certification standard the system is being installed to from the dropdown menu and click **Submit.**

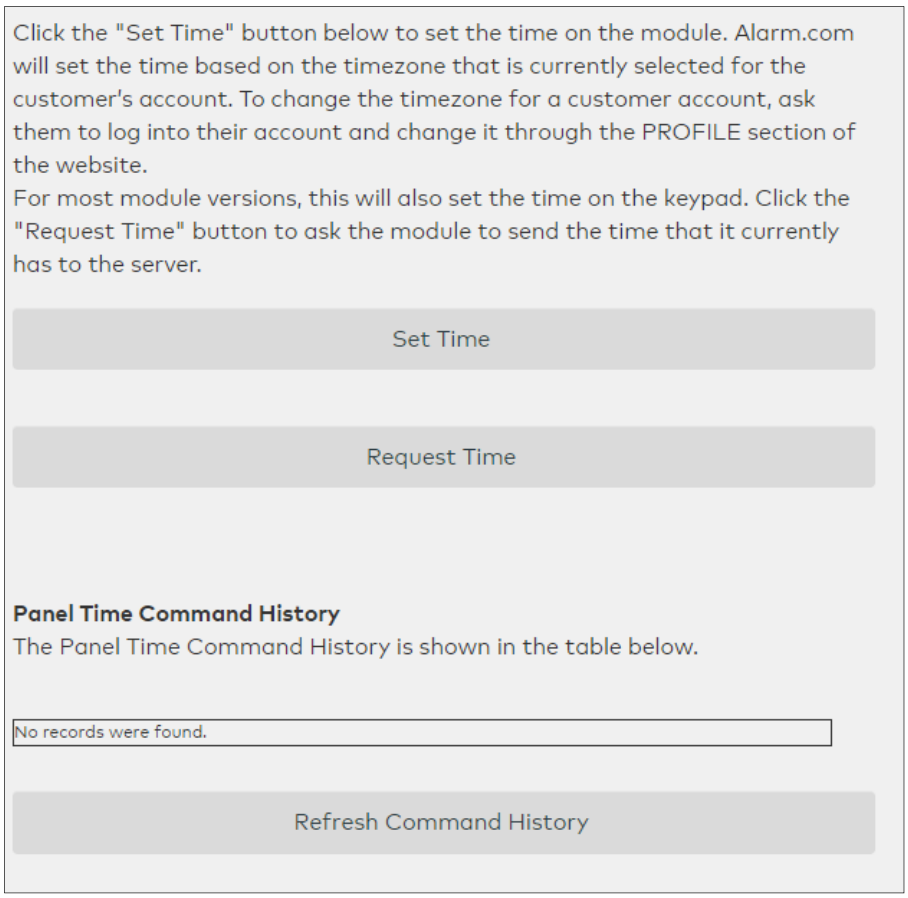


5.3. Date and Time

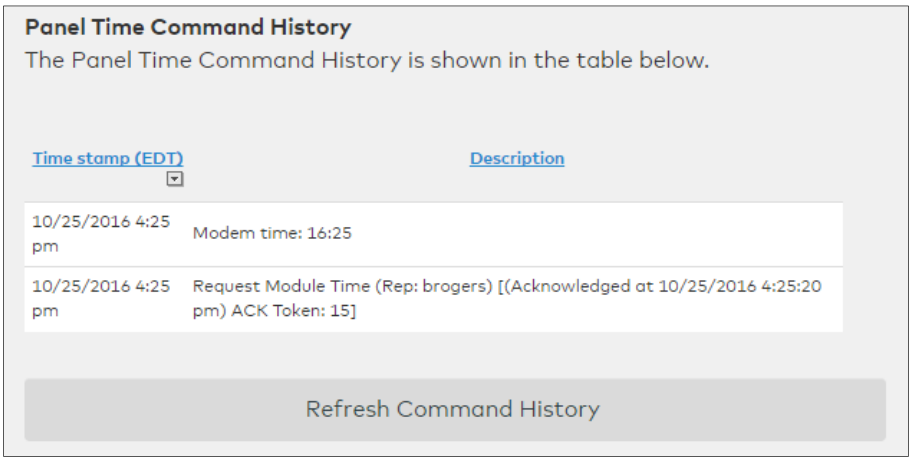
6.3.1 Check Date and Time

To edit the panel date and time, go to **Equipment > Panel Management > Advanced Panel Settings > Panel Time > Request Time.**

The time request will populate in the **Panel Time Command History** section, as well as the panel event history.



The time request will populate in the **Panel Time Command History** section, as well as the panel event history. You may need to **Refresh Command History** to populate the panel time.

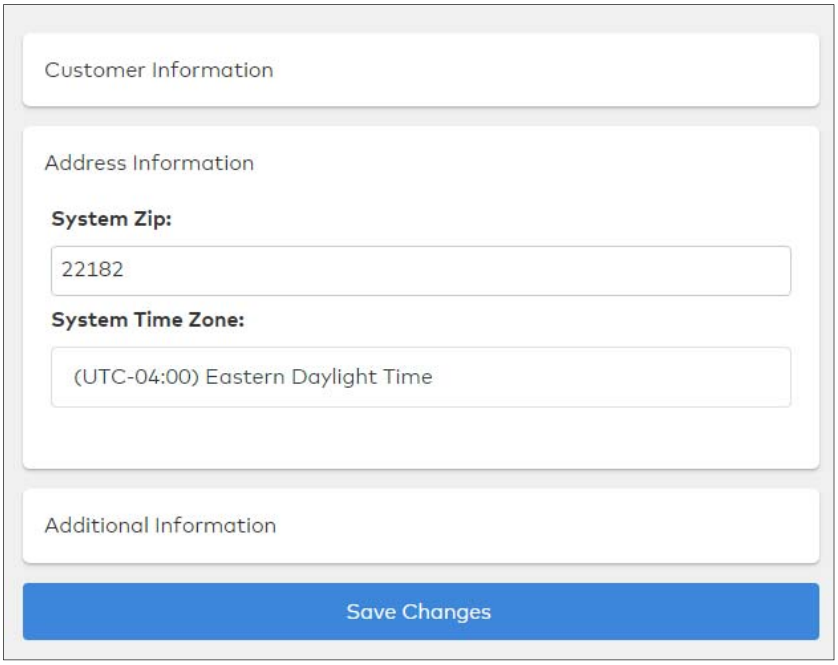


6.3.2. Set Time

To set the panel time, go to **Equipment > Panel Management > Advanced Panel Settings > Panel Time > Set Time.** The panel time will be set according to the current time zone based on the Customer Profile.

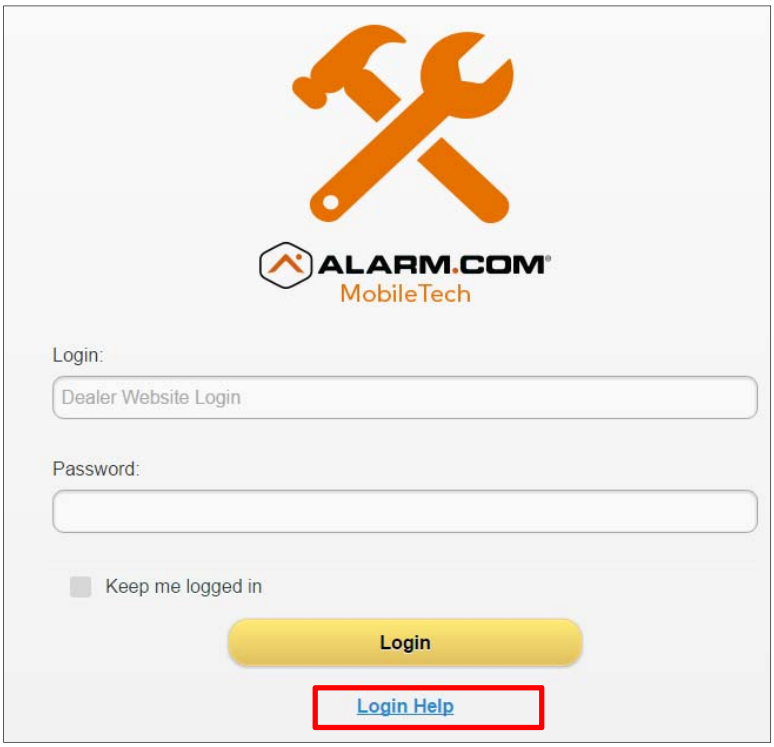
6.3.3. Setting the Customer Time Zone

To set the customer Time zone, find a customer, and select **Edit** from the customer info box. Select **Address Information > System Time Zone** and set the customer time zone to the appropriate value. Make sure to Set the panel time after adjusting the time zone.

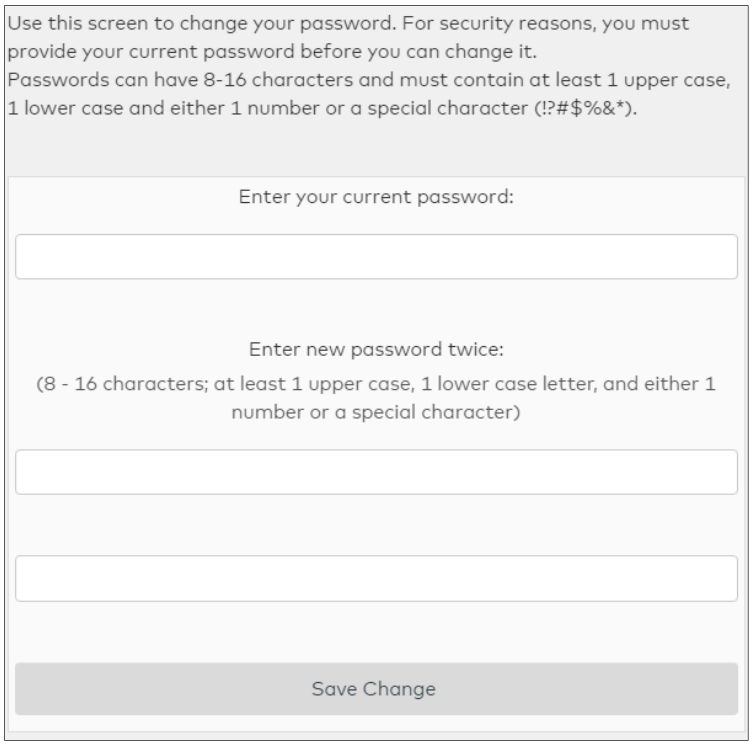


6.4. Change Password

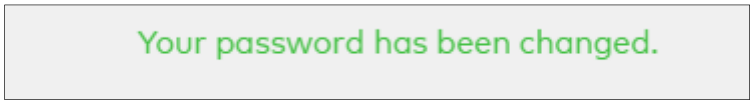
6.4.1 Installer Password

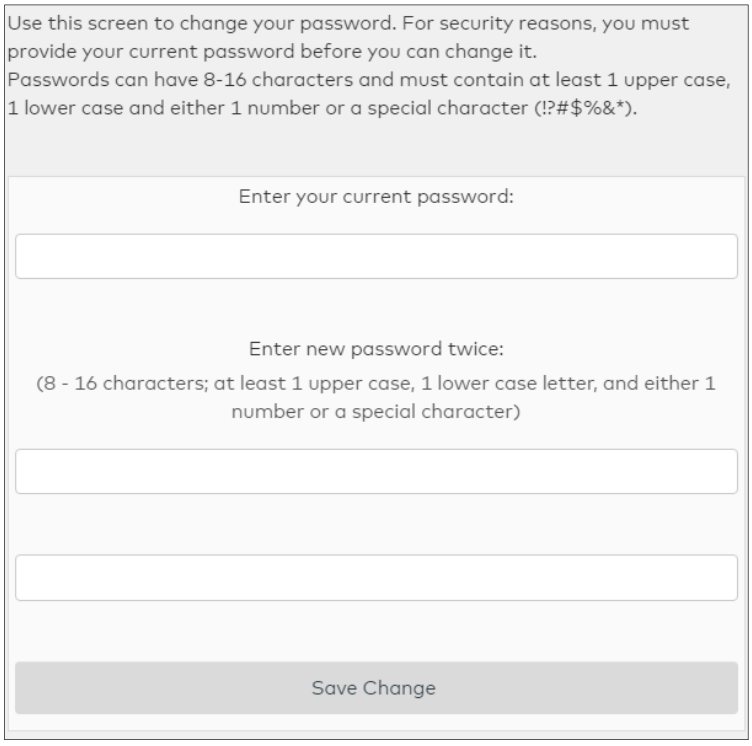


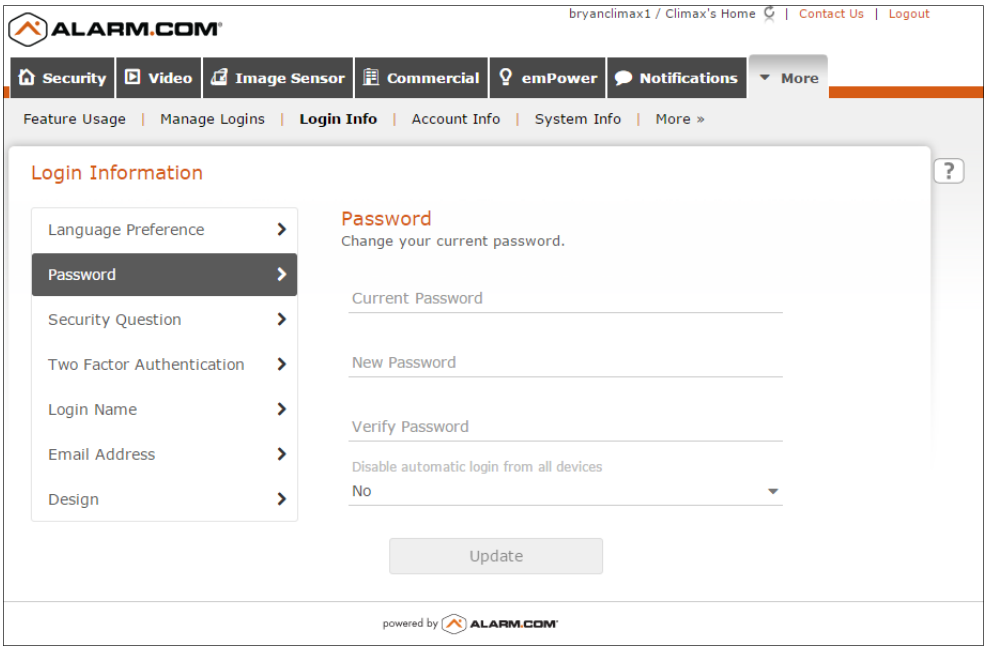
To change your password, login to the Installer app, and go to https://alarmadmin.alarm.com/mobile/ManageDealer/ChangeRepPassword.aspx



You will be prompted to enter your current password once, and your new password twice. After clicking **Save Change**, you will receive confirmation that your password has been updated.







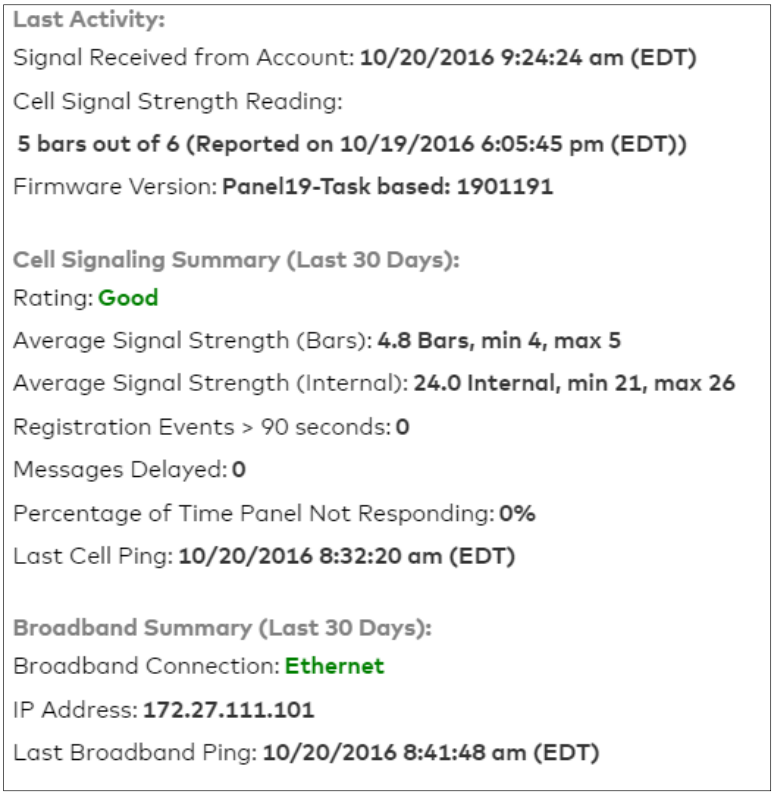
To change a user's password, go to **More > Profile > Login Info > Password**. Enter the current password and the new password twice and select **Update.**

7. Network

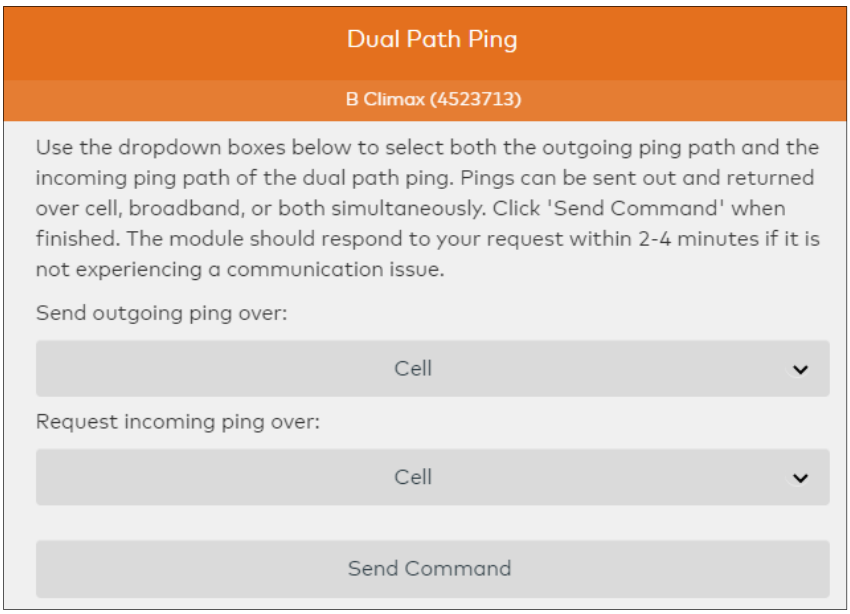
7.1. Cell and IP Communication

The Communication Management page allows the configuration and troubleshooting of Cell and IP Network Settings.

Step 1. Navigate to **Equipment** > **Communication Management**



The Signaling Section will alert you to the current status of GSM and IP Communication. The **Cell Signal Strength Reading** should be strong and recent, additionally the **Last Cell Ping** and **Last Broadband Ping** fields should contain recent timestamps.



If the ping timestamps are not recent, ping the panel using **Dual Path Ping**. Configure a ping to send both the outgoing and incoming ping over cell and click **Send Command.** Next, configure an outgoing and incoming ping over broadband and select **Send Command**. The signaling page will update to a current timestamp when the pings go through.

8. System Operation

8.1 Faults and Tampers

8.1.1 Fault and Tamper Status:

The Control Panel is capable of monitoring the system for any faulty conditions. When any fault event is detected, the amber Fault LED on the Control Panel and Remote Keypad (KP-35) will light up to indicate the situation. The fault event will be logged and reported to destinations programmed under Report setting accordingly. The remote keypad as well as the Customer and Installer webpages will also display fault event information. Refer to table below to solve the faults and pictures below to view the fault history.

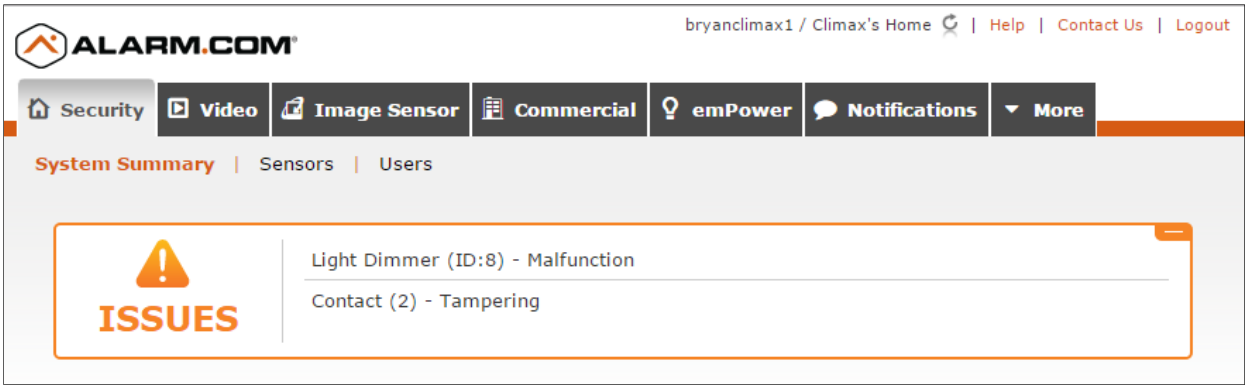
<NOTE>

- ☞ After solving the fault events, use the Remote Keypad to clear the fault events to remove the fault event display on the Control Panel webpage, or the fault event will remain even after they have been solved.

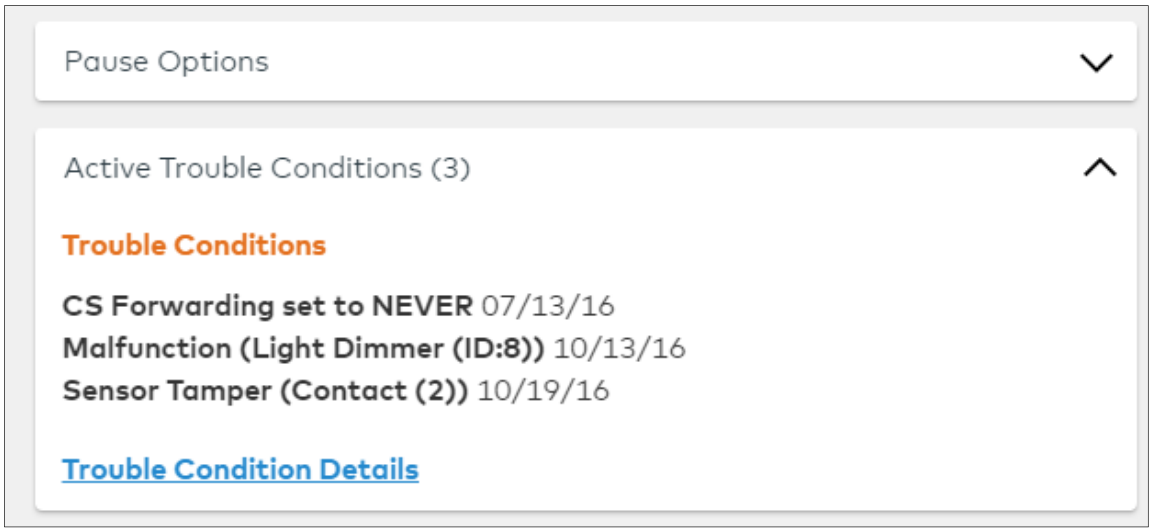
For a list of all Panel Faults, please see Appendix B.

8.1.2 Viewing Faults on webpages:

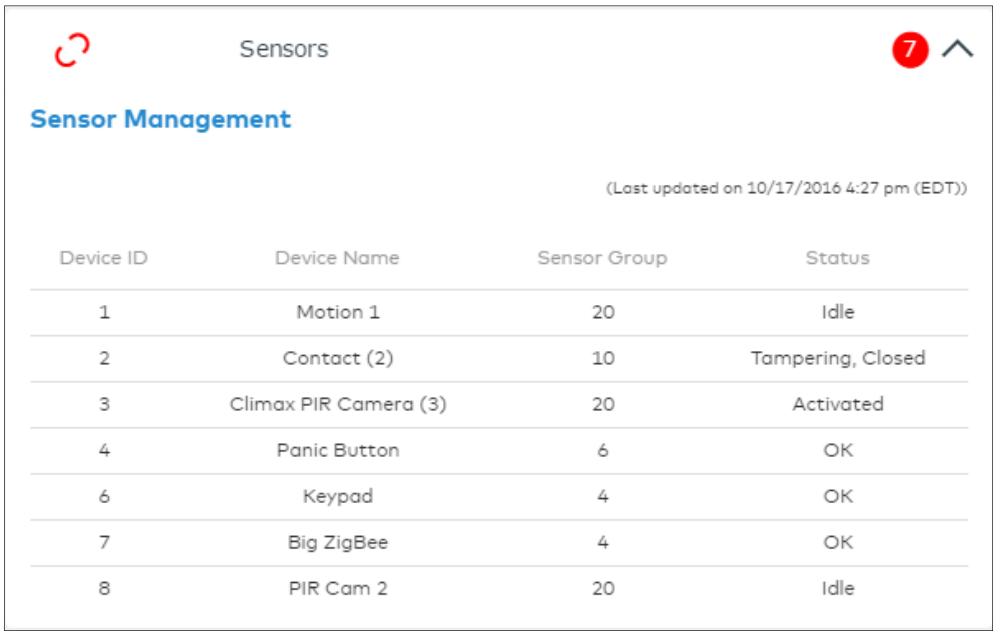
Customer Interface: Issues Box on the “System Summary” page:



Installer Interface: “Active Trouble Conditions” on the “System Check” tab:



Device List and Status: This is found on the “Equipment Section” of the Installer Page, you can find the list by expanding the relevant Section. Sensor Management will allow configuration of sensors and peripherals

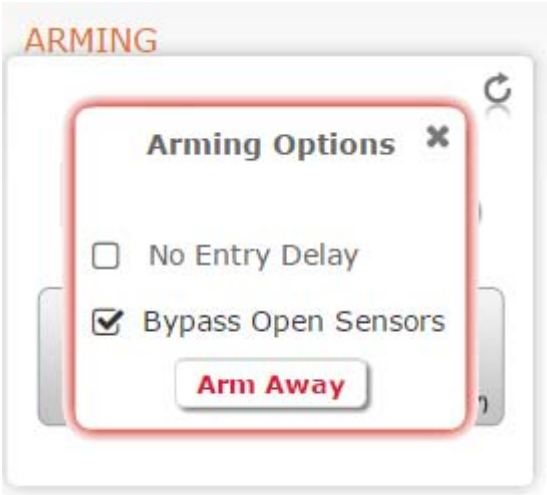


8.1.3 Restoring Faults

In order to Restore a Fault and remove the Fault Indication, the Fault condition must be physically resolved and the fault notice must be acknowledged by the Level 2 user at the remote keypad.

8.1.4 Force Arming the Control Panel

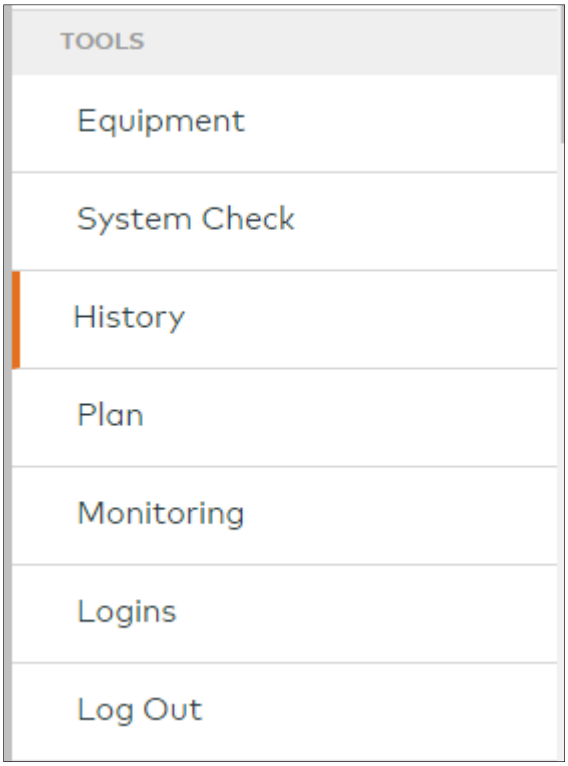
When there is a Tamper or Fault that has not been restored, or a Zone is open/activated the control panel will give an “Arming Failed” indication. This can be overridden at the remote keypad by choosing to arm a second time, and on the Alarm.com Webpage by choosing the “Bypass Open Sensor” option. Please note, any open zones that have been bypassed will remain bypassed until they are closed.



8.2 View History

History and Event Logs can be accessed either through the ZigBee keypad, or through the installer and customer tools.

Installer App: Select “History” from the Sidebar option menu:



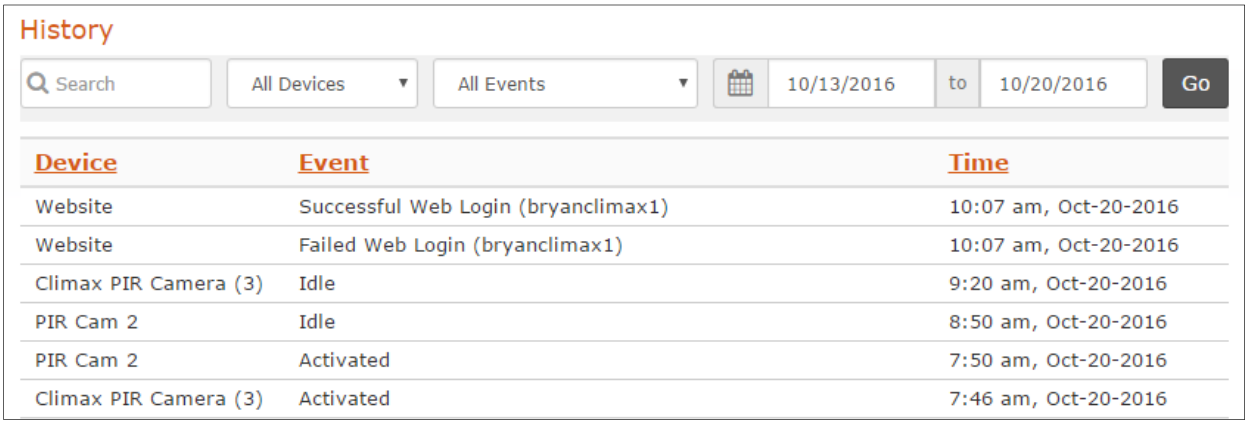
Customer App: Select “History” from the “More” dropdown menu:

8.3 History

The history pages contain events, timestamps, and acknowledgement information. The History pages contain all history records for the past 90 days. The Acknowledgement timestamp indicates what time the event was received by the Monitoring station and whether the event went through. If the event does not report within 2 minutes, faults and logs will be taken.

Type	Description	Time (EDT)
Monitor	Successful Web Login (bryanclimax1)	10/20/2016 10:07:12 am
Monitor	Failed Web Login (bryanclimax1)	10/20/2016 10:07:05 am
Message	Panel Auto-phone test	10/20/2016 10:05:43 am

Type: Message Type
Description: Detailed description of the event including: Zone, Status, Reporting Status (Acknowledgement)
Time: Timestamp for when the event occurred



Device: A description of which device the event happened on, including whether it was remote

of local to the system.

Event: Detailed description of the event and activity

Time: Timestamp for when the event occurred

8.4. Requesting a Firmware Upgrade

To request a firmware upgrade, please contact your Alarm.com Support Representative. To request an upgrade, you will need to provide the unique Customer ID of the panel to be upgraded. To perform the upgrade, the customer must enable EN Grade 2 installer access from the Customer Site as described in section 3.2.

8.5 System Operation and Maintenance

For system regular operation, refer to this section for operation mechanics and various issues or problems which may arise during operation.

8.5.1 Device Test

You should test the accessory devices included in the alarm system regularly to ensure that they are functioning properly.

Option 1:

Step1. Enter a valid PIN code into the local keypad and scroll down to the Option for “Walk Test”

Step2. Trip the security devices to transmit a signal to the control panel.

Step3. If the control panel receives the signal successfully, it will emit 1 long beep.

Option 2:

See section 4.2 Sensor Management for how to perform a Walk Test remotely from the Alarm.com Installer Application.

8.5.2 IP/GSM reporting

The Control Panel utilize “Pass-through” operation mode as specified in EN50136-2, clause 6.1.3. When an event is triggered, the panel will not consider the event reporting complete without receiving acknowledgement from the report recipient.

The HSGW-Gen2-V1 utilizes IP and GSM reporting methods. The panel will still be able to report events normally even when it loses connection to one of the reporting paths, by using the remaining reporting path as alternative to ensure the alarm system does not become unavailable.

For example, when the Control Panel loses Ethernet connection, the events will be reported via GSM network; if the GSM network loses connection, the events will be reported via Ethernet. The Alarm.com backend will notify a failure to communicate over broadband within 30 minutes,

and a failure to communicate over cell within 24 hours. If both paths are down, a fault for the failed report message will be logged and reported within 2 minutes. Additionally, if both paths are down the Receiving Centre Transceiver (RCT) will recognize the fault after 25 hours of not receiving any reports from panel and inform the Monitoring Center of the fault event.
After finish programming all settings for operation, you should follow instruction below to test your alarm system to make sure it can report to your programmed reporting destination successfully.

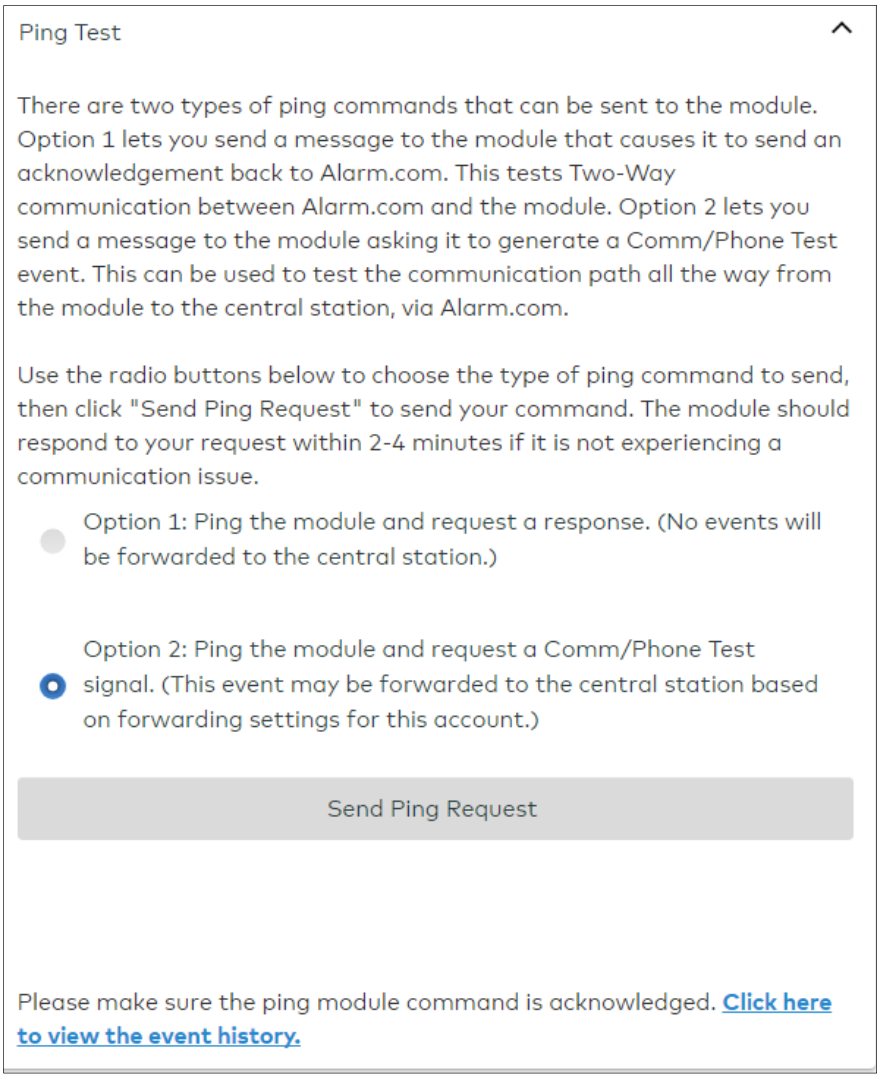
Cell and IP Communications Test

The control panel has the ability to test communication along the individual reporting paths through the “Dual Path Ping” page (Section 7.1 Cell and IP communication).
Step 1: Send an incoming and outgoing ping over the Broadband path.
Step 2: Send an incoming and outgoing ping over the Cell path.
Step 3: Navigate to the History Page. This page will show a record of both commands, and if Communication is successful along the individual paths, the commands will show an Acknowledgement Time Stamp

Type	Description	Time (EDT)
Command	Dual Path Ping (Incoming Broadband) (Rep: 1115rogers) [(Acknowledged at 5/2/2017 10:00:18 am) ACK Token: 29]	5/2/2017 10:00:18 am
Command	Dual Path Ping (Incoming Cell) (Rep: 1115rogers) [(Acknowledged at 5/2/2017 10:00:27 am) ACK Token: 59]	5/2/2017 10:00:12 am

Round Trip Reporting Test

It is also possible to test a round trip reporting test to the Central Monitoring Station. This test is helpful to ensure that the correct information has been configured for the Central Monitoring Station, and that communication with the Central Monitoring Station has been successfully established.
Step 1: Ensure that the correct Monitoring Station settings have been configured on the **Monitoring** page.
Step 2: Navigate to **Equipment > Communication > Ping Test**
Step 3: Select Option 2: “Ping the module and request a Comm/Phone Test signal” and click **Send Ping Request.** Provided the **Monitoring** settings have been configured to forward Phone Test events to the Central Monitoring Station, the Central Station should receive and acknowledge this signal.


Ping Test
There are two types of ping commands that can be sent to the module. Option 1 lets you send a message to the module that causes it to send an acknowledgement back to Alarm.com. This tests Two-Way communication between Alarm.com and the module. Option 2 lets you send a message to the module asking it to generate a Comm/Phone Test event. This can be used to test the communication path all the way from the module to the central station, via Alarm.com.
Use the radio buttons below to choose the type of ping command to send, then click "Send Ping Request" to send your command. The module should respond to your request within 2-4 minutes if it is not experiencing a communication issue.
Option 1: Ping the module and request a response. (No events will be forwarded to the central station.)
Option 2: Ping the module and request a Comm/Phone Test signal. (This event may be forwarded to the central station based on forwarding settings for this account.)
Send Ping Request
Please make sure the ping module command is acknowledged. Click here to view the event history.

9. Automation Devices

9.1. Device Learning and Operation

The HSGW-Gen2-V1 allows for interaction with Home Automation devices using the Z-Wave protocol. These home automation devices can be learned in using the same steps described in section 4.1. The operating instructions for these devices are contained in the device installation manual.

10. Appendix

Appendix A: Sensor Groups

Sensor Group	Physical Type	Short Description	Description	Other Allowed Groups
0	Keypad/Pull Station	Fixed Panic	24-hour audible fixed emergency buttons, instant alarm, always armed	2, 4
1	Keyfob/Panic Button	Portable Panic	24-hour audible portable emergency buttons, instant alarm, always armed	3, 6
2	Keypad/Pull Station	Silent Fixed Panic	24-hour silent fixed emergency buttons, instant alarm, no siren, always armed	0, 4
3	Keyfob/Panic Button	Silent Portable Panic	24-hour silent portable emergency buttons, instant alarm, no siren, always armed	1, 6
4	Keypad	Fixed Auxiliary	24-hour auxiliary sensor, instant alarm, always armed	0, 2
6	Keyfob/Panic Button	Portable Auxiliary	24-hour portable auxiliary alert button, instant alarm, always armed	1, 3
8	Contact	Cabinet/Safe	Special belongings, such as gun cabinets and wall safes, instant alarm, always armed	8, 10, 11, 13, 14, 16, 19, 31, 36
10	Contact	Door/Window	Entry and exit doors, standard delay alarm, armed in Stay and Away modes	8, 11, 13, 14, 16, 19, 31, 36
11	Contact	Extended Delay/Door	Garage doors and entrances, extended delay alarm, armed in Stay and Away modes	8, 10, 13, 14, 16, 19, 31, 36
13	Contact	Door/Window or Glassbreak	Exterior doors and windows, instant alarm, armed in Stay and Away modes	8, 10, 11, 14, 16, 19, 31, 36
14	Contact	Door/Window	Interior doors, instant alarm, armed in Stay and Away modes	8, 10, 11, 13, 16, 19, 31, 36
15	Motion	Motion	Motion Sensors, follower, armed in Stay and Away modes	17, 18, 20, 25, 50
16	Contact	Door/Window	Interior Doors, instant alarm, armed in Away mode Only	8, 10, 11, 13, 14, 19, 31, 36

17	Motion	Motion	Motion Sensors, follower, armed in Away mode only	15, 18, 20, 25, 50
18	Motion	Motion Sensor with Cross Zone Verification	Motion sensors subject to false alarms, instant alarm, armed in Away mode only	15, 17, 20, 25, 50
19	Contact	Door/Window	Interior doors, standard delay alarm, armed in Away mode only	8, 10, 11, 13, 14, 16, 31, 36
20	Motion	Motion	Motion sensors, standard delay alarm, armed in Away mode only	15, 17, 18, 25, 50
25	Motion	Motion-Chime Only	Chime notifies a user when a door is opened, no alarm, three beeps, no CS report	15, 17, 18, 20, 50
26	Smoke/Heat	Smoke/Heat	24-hour fire, rate-of-rise heat, and smoke sensors, instant alarm, always armed	61
29	Temperature	Freeze/Water Sensor	Auxiliary freeze or water sensors, instant alarm, no siren, trouble beeps when tripped, always armed	
31	Contact	Door/Window-Chime Only	Chime notifies a user when a door is opened, no alarm, three beeps, no CS report	8, 10, 11, 13, 14, 16, 19, 36
33	Siren	Siren	Wireless Siren Supervision	
34	CO	Carbon Monoxide	Carbon Monoxide gas detectors, instant alarm, always armed	
36	Contact	Cabinet/Safe	Special intrusion such as gun cabinets and wall safes, reports as tamper if tripped, instant alarm, always armed	8, 10, 11, 13, 14, 16, 19, 31
38	Water	Water Sensor	Auxiliary: Water Sensors, instant alarm, no siren, trouble beeps when tripped, always armed	
50	Motion	Motion	Motion sensors, standard delay alarm, armed in Stay and Away modes	15, 17, 18, 20, 25
61	Smoke/Heat	Smoke Detector with Fire Verification	24-hour fire with verification, smoke or heat rise sensor, instant alarm, always armed	26

Appendix B: Faults

Fault Message Displayed	Fault Situation	Solution
Panel Low Battery	Control Panel backup battery voltage is low.	Connect AC power to the panel and turn on the battery switch. The battery will be charged automatically.
Panel AC Fault	Control Panel AC Power is disconnected.	Check AC power cord connection to power socket and panel AC input.
Panel Battery Missing/Dead	Control Panel backup battery is under one of the following faults: 1. Disconnected from panel. 2. Battery switch turned off. 3. Battery out of order.	1. Open panel battery compartment cover, reconnect the battery to panel board. 2. Turn on battery switch with a sharp object. 3. If the problem is not solved, the battery is out of order, please change battery.
Panel Tamper	Control Panel is removed from the mounting bracket and its tamper switch is open.	Hook the panel on the mounting bracket, make sure the tamper switch is depressed against the bracket.
GSM No Signal	Control Panel cannot connect to GSM network.	1. SIM card not inserted, insert a SIM card. 2. Allow panel to reset cell radio and register to GSM network 3. Move the panel to another location for better GSM signal strength.
Jam Detect	Control Panel is experiencing radio signal interference that prevents devices from communicating with panel.	Locate the interference source by turning off all wireless devices in your home, wait for 3 minutes to clear the fault event, then turn on the devices one by one to check which device triggers the jamming fault.
Supervision Failure (Zone#)	The device at specified zone has not reported to Control Panel within a supervision period.	1. Check if device is on low battery by checking the fault event display. 2. If device is on low battery, change battery. 3. If device battery is normal, change device location for better signal strength. Use Walk Test to find the new location. 4. If the battery is normal and the device signal cannot be received by panel at all using Walk Test, replace the device.
Low Battery (Zone#)	The device at specified zone is low on battery	Change device battery.

Tamper (Zone#)	The tamper switch of the device at specified zone is open. The device is either removed from mounted location, or cover opened.	1. Check device mounted location, make sure device is properly mounted 2. Check if device cover is opened, close the cover..
Door Opened (Zone#)	The Door contact at specified zone is opened (Door Contact not aligned with its magnet) **Note: This event will only appear when you try to arm the system with the Door Contact opened.**	Close the door the Door Contact is mounted on.
Out of Order (Zone#)	The device at specified zone is out of order (supervision failure) **Note: This event will appear when:** **1. If the device has failed supervision, the event will be displayed on webpage.** **2. If the device has not yet failed supervision, but did not report to Control Panel for over 20 minutes, the event will be displayed on webpage when you try to arm the system**	1. Check if device is on low battery by checking the fault event display. 2. If device is on low battery, change battery. 3. If device battery is normal, change device location for better signal strength. Use Walk Test to find the new location. 4. If the battery is normal and the device signal cannot be received by panel at all using Walk Test, replace the device.
Triggered (Zone#)	This event only applies to following devices: PIR Sensor, PIR Camera, and Remote Controller Panic Button. The event will appear only when you attempt to arm the system within 5 seconds after the device is triggered or pressed.	1. Check your PIR Sensor and PIR Camera detection area and make sure your home perimeter is safe before arming the system. 2. After triggering a Panic alarm with your Remote Controller, wait for at least 5 seconds before arming the system.
Report Fail	The Control Panel has not been able to send a report for over 2 minutes.	1. Check and make sure your report setting is programmed correctly 2. Check Ethernet connection 3. Check GSM/GPRS connection
Network Cable Unplugged	The Control Panel has lost its Ethernet cable connection	Restore Ethernet cable connection to the Control Panel.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15, Part 22, Part 24, and Part 27 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

. Reorient or relocate the receiving antenna.
. Increase the separation between the equipment and receiver.
. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
. Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

FCC Radiation Exposure Statement

This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

This device complies with Part 15, Part 22, Part 24, and Part 27 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.