

Hybrid Panel Lite

User Manual

Certified by Kiwa Nederland, B.V.
Manufacturer: Climax Technology, Taiwan
Type: Hybrid Panel Lite
Compliance with Standard:
EN50131-3:2009 / EN50130-4:2011
EN50130:2011 / EN50130-5-3:2017
EN50131-6:2017 +A1:2021 / EN50131-10
Security Grade 2
ATS Category: DP2, CIE Type A
Environmental Class II
Version 1, 2024/02/29

August 12, 2024

Table of Contents

1.	INTRODUCTION	1
1.1.	SYSTEM SPECIFICATIONS	1
1.2.	WHAT'S IN THE BOX	4
2.	PANEL INFORMATION	5
2.1.	IDENTIFYING THE PARTS	5
2.2.	POWER SUPPLY	9
3.	GETTING STARTED	10
3.1.	SELECTING MOUNTING LOCATION	10
3.2.	MOUNTING	11
3.3.	HARDWARE INSTALLATION	13
3.4.	CONNECT TO HYBRID PANEL LITE HOME PORTAL SERVER	24
4.	LEVEL 2 ACCESS	25
4.1.	LOG IN	25
4.2.	SECURITY	27
4.2.1.	System Area	27
4.2.2.	Dashboard	29
4.2.3.	Sensors	30
4.2.4.	IP Cam List	30
4.3.	AUTOMATION	31
4.4.	IP CAMERA	32
4.5.	EVENT	33
4.6.	SETTING	34
4.6.1.	Device	35
4.6.2.	Geofencing	37
4.6.3.	Panel	38
4.6.4.	User PIN	39
4.6.5.	Network	40
5.	LEVEL 3 ACCESS	41
5.1.	SETTING	42
5.1.1.	Device	43
5.1.2.	Geofencing	48
5.1.3.	Panel	49
5.1.4.	Wired Device	53
5.1.5.	Network	54
5.1.6.	Report	55

6. *IP/GSM REPORTING* _____ 58

7. *APPENDIX* _____ 60

APPENDIX A: EVENT CODE _____ 60

APPENDIX B: FAULTS _____ 62

1. Introduction

The Hybrid Panel Lite is an IP-based multi-functional RF gateway with 4G/LTE capability, plus flexible hardwired and wireless sensor zone options, providing comprehensive solutions, including remote management, home security, live visual monitoring, home automation, environmental emergency monitoring, and energy management and being designed to bring all-round convenience, comfort and safety.

System Feature

- Ethernet / Cellular connection
- Communication Path: the Hybrid Panel Lite has built-in RF module.

1.1. System Specifications

Functions	
Number of areas and zones (wired & wireless)	2 areas, 80 zones per area, 160 zones in total
Number of on-board wired zones	8 on-board zones
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
Zone expansion module	8 wired zone expansion module (WEZC-8) available
Wired input	NO/NC Single end-of-line (SEOL), Double end-of-line (DEOL) loop configuration, with selectable resistor values of 1K Ω , 2.2K Ω , 3.74K Ω , 4.7K Ω , 5.6K Ω , 6.8K Ω , 8.2K Ω , 10K Ω Triple end-of-line (TEOL) loop (Non-compliant to EN regulation) can be configured in different combinations: 4.7K Ω , 6.8K Ω , 12K Ω (resistor value selection: 6.8K), 4.7K Ω /5.6K Ω , 4.7K Ω , 2.2K Ω /3K Ω (resistor value selection: 4.7K), or 4.7K Ω /5.6K Ω , 5.6K Ω , 2.2K Ω /3K Ω (resistor value selection: 5.6K)
Number of BUS terminal	1 pluggable BUS terminal
Number of connected BUS devices	Up to 128 BUS devices (a max. of 4 KPT-35-COMBOs allowable)
Number of users / PIN codes	6 users per area, 12 users in total, 1 PIN Code each user (6-digits, number 0~9), available combination from 000000 to 999999 (1000000 different combinations). Note: Input of 5 invalid User PIN codes at the remote keypad will lock the remote keypad for 15 minutes.
Number of PGM output port	1

Total NOR flash size	32MB
Total DRAM size	512MB
Number of event logs can be stored on panel	250 <i>Note: The contents of the event log will not be lost or corrupted when the panel is powered off.</i>
Cable Type	Unshielded
Tamper protection	Dual wall mount & front cover tampers
Ethernet interface	RJ-45 connection
Control Facilities	Remote Keypad & Remote Controller Home Portal Server
Report Destinations	20 Monitoring Stations or mobile number
Reporting Format	Contact ID, SIA, CSV_IP, Email, SMS Text
Arming Modes	Away Arm, Home Arm
Alarm Type	Burglar, Panic, Fire, Medical, Emergency, Water, CO, Gas, Heat, Silent
Siren Timeout	Programmable (3 minutes by default) (for Remote Keypad only)
Supervision	Programmable time frame for inactivity alert
Special Function	Tamper Protection
Cellular Standard	Complies with CE standards, EN301 511, EN301908-1.
Real Time Clock (RTC)	The Control Panel keeps and displays time and date. This feature is also used for the log file by providing the date and time of each event.
GSM Standards	Compliant with CE standards 4GPP TS 51.010-1, EN301 511, EN301489-7
EN Classification	EN Grade 2 Class II
Alarm Transmission Path	Dual Path: DP2 (EN50136-1:2012)
Supported RCT	Alarm Report Server (ARS), Fibro, OH200, MasterMind, Manitou, MicroKey and SIA DC09s
Modes of acknowledgement operation	Pass-through (EN50136-2:2013, Clause 6.1.3)
Electrical	
Power supply	100 – 240VAC, 50/60Hz

Backup battery	12V 4Ah Sealed Lead Acid Battery	
Battery duration	21 hours *Note: Actual battery life may vary with product settings, operating environment, and usage patterns.	
APS fault Low Voltage SD signal threshold	11.5 V \pm 3%	
Total output for hardwired zones, auxiliary output, BUS devices, expansion modules and PGM port	13.5V/1.5A (max.)	
Ripple of Output (from AC/DC adapter to Hybrid Panel Lite)	+/-0.6V	
Current Drain	AC Powered	Avg. 230VAC/50HZ 17mA @no loading (BUS device & wired device & SLA Battery)
	Battery Powered	Avg. 21mA @no loading (BUS device & wired device)
Wireless		
LTE Frequency	B1 (2100 MHz) / B3 (1800 MHz) / B5 (850 MHz) / B7 (2600 MHz) / B8 (900 MHz) / B20 (800 MHz)	
3G Frequency	B1 (2100 MHz) / B5 (850 MHz) / B8 (900 MHz)	
RF Frequency	F1 868 MHz	
RF encryption	Private Encryption Method	
RF protocol	Climax	
Antenna Type	External: Dipole, Internal: On-board, Monopole	
Physical Properties		
Operating temperature	-10°C to 45°C (14°F to 113°F)	
Operating humidity	85% relative humidity @23°C (non-condensing)	
Dimensions	320 mm x 250 mm x 93 mm	
Weight	1450 g (without battery)	

1.2. What's in the Box

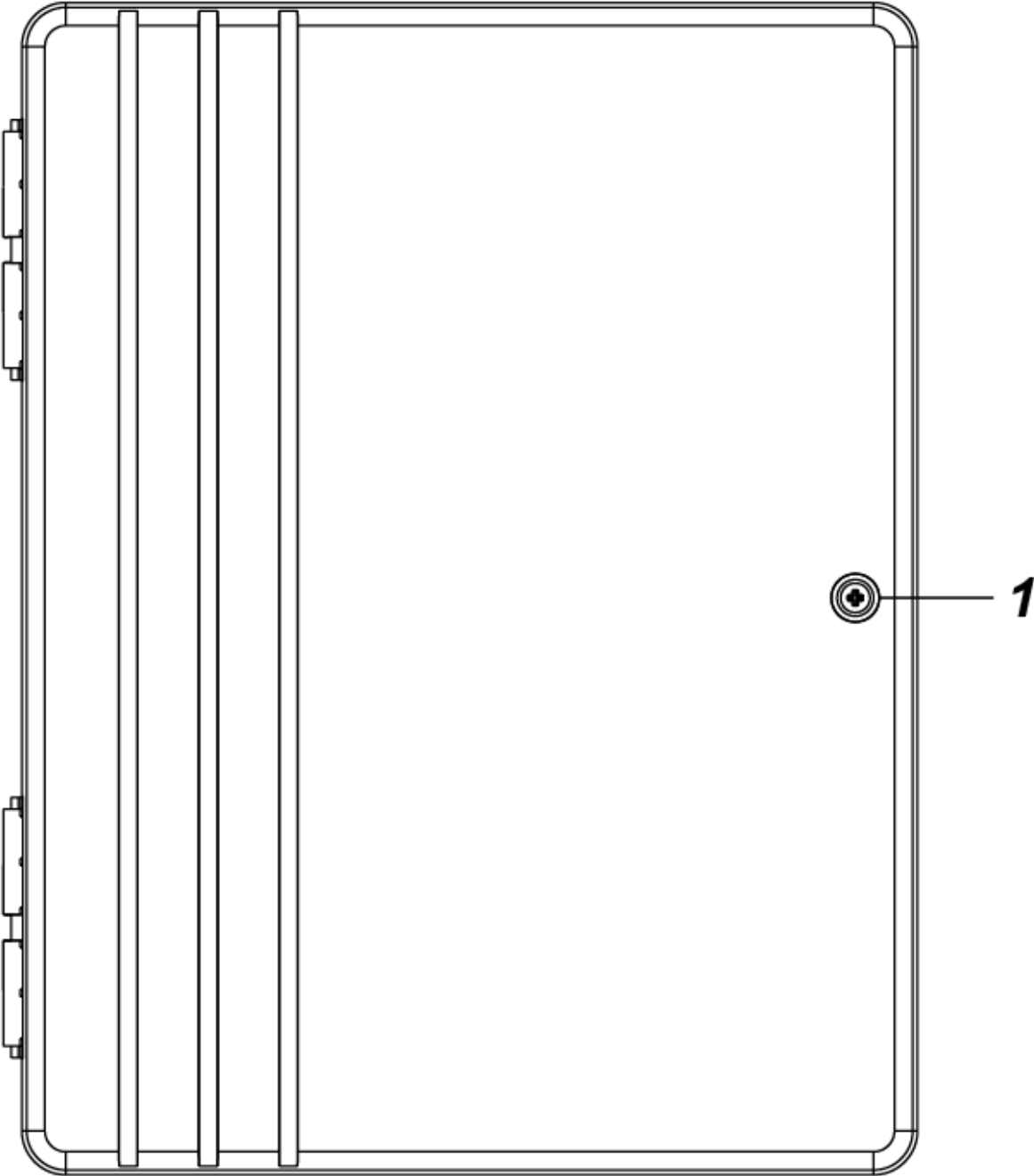
Your package includes the following items:

- Control Panel *1
- Open Frame Power Cord *1
- Ethernet Cable *1
- Accessories:
 - Jumper Connector * 2
 - U-shaped Grommet * 2
 - 5.6K Resistor * 16 (2 resistors for each zone, 16 resistors for 8 zones in total)
 - Mounting Screw * 4
 - Wall Plug * 4

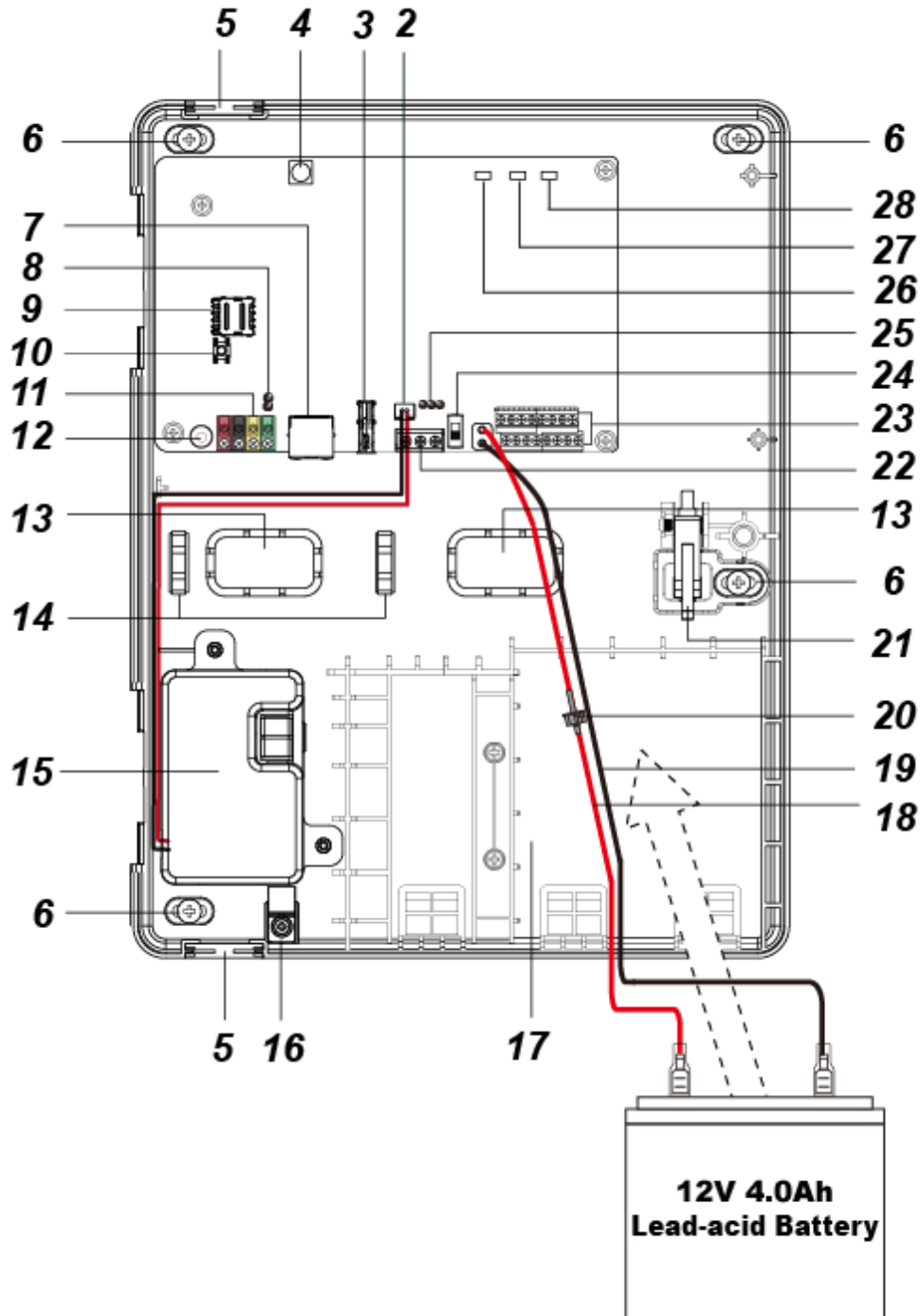
2. Panel Information

2.1. Identifying the parts

Top Cover (front view)



Back Cover (internal view)



1 Cover Fixing Screw

2 Built-in Power Unit Connector

3 USB Port

When connecting a USB dongle into the port, it is suggested to use a USB extension cable.

4 4G LTE External Antenna Terminal (SMA Plug)

5 Removable Protective Cover * 2 (at the top and bottom of the back cover)

Reveal or hide the wiring hole

6 Mounting Holes * 4

7 Ethernet Port

8 J53 Jumper Switch

J53 Jumper Switch can be served as a terminating resistor, which can be turned to ON when wiring different BUS devices to the panel to enhance connection.

9 Micro SIM Card Socket (not hot swappable)

10 Learn Button

For local learning or local reset

11 Pluggable Bus Terminal

Connect to wired BUS devices.

12 EGND Terminal

Please refer to **3.3 Hardware Installation** for detail.

13 Alternative Hole for Wiring Management * 2

14 Wiring Clip * 2

For securing power cables

15 Built-in Power Unit

Input: 100-240VAC

Open Frame built-in power unit is installed. Use the built-in power unit to connect to the mains power.

☞ Ensure to turn off all power supplies including Built-in Power Unit and SLA Battery before connecting or removing cables or wires.

16 Wire Saddle

17 Room for SLA Battery

Room for installing 12V 4Ah Sealed Lead Acid rechargeable battery

18 Embedded Battery Cable (Power) (Red)

19 Embedded Battery Cable (GND) (Black)

20 Tube Fuse Holder

Please note:

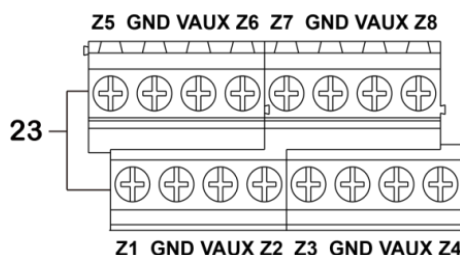
☞ The tube fuse is pre-installed onto the battery cable; it is recommended not to change or replace the cable on your own to avoid possible hazards.

21 Dual Wall-mount & Front Cover Tamper

22 PGM Port

To be used as a voltage output port or a dry contact relay output depending on J24 jumper settings.

23 Zone Terminal & Auxiliary Voltage Output Terminal & GND Terminal



24 Battery Switch

Switch to “ON” for the battery to be charged when AC power is connected and serve as a backup power source when AC power is missing.

25 J24 Jumper Switch

The jumper is used for PGM Port setting. Please refer to **3.3 Hardware Installation** for details.

26 LED 1 - Area 1 (Green/Red)

- ☞ Full Arm mode - Red lighting up
- ☞ Home/1/2/3 mode - Red flashing
- ☞ Learning mode - Green lighting up
- ☞ Walk Test mode - Green flashing

27 LED 2 - Area 2 (Green/Red)

- ☞ Full Arm mode - Red lighting up
- ☞ Home/1/2/3 mode - Red flashing
- ☞ Learning mode - Green lighting up
- ☞ Walk Test mode - Green flashing

28 LED 3 - Status (Orange/Red)

- ☞ System Fault - Orange lighting up
- ☞ Alarm Trigger – Red flashing
- ☞ Aarm in Memory – Red lighting up

2.2. Power Supply

Built-in Power Unit

- You can use the built-in power unit to connect to the mains power. AC module built-in power unit or Open Frame built-in power unit is installed. Please refer to ***Using the built-in Power Unit*** in **3.3 Hardware Installation** for more details.

Please note:

- ☞ **Ensure to turn off all power supplies including Built-in Power Unit and SLA Battery before connecting or removing cables or wires.**

Rechargeable Battery

- A rechargeable battery (12V 4Ah SLA battery) can be installed inside the Control Panel to serve as a backup in case of a power failure.
- During normal operation, AC power is used to supply power to the Control Panel and at the same time recharge the battery.
- If the battery switch is set as **OFF**, the battery will not be charged when AC power is connected and nor will it serve as a backup power source when AC power is missing. You need to switch the battery to **ON** for it to be charged when AC power is connected and serve as a backup power source when AC power is missing.

Power Output

- The panel supports up to a maximum total of 13.5V/1.5A (typical) for the current derived from VDD auxiliary voltage output terminals.
- The total current provided by Hybrid Panel Lite for hardwired devices, BUS devices, wired keypad and expansion modules should not exceed 1.5A. Otherwise, additional power is required.

Please note:

- ☞ **If the total current exceeds 1.5A, components of Hybrid Panel Lite could be damaged.**

3. Getting Started

Read this section of the manual to learn how to set up your Control Panel.

3.1. Selecting Mounting Location

The Control Panel is designed to be wall mounted and protected against unauthorized case opening or removal from its mounting surface, follow guidelines below when planning installation location:

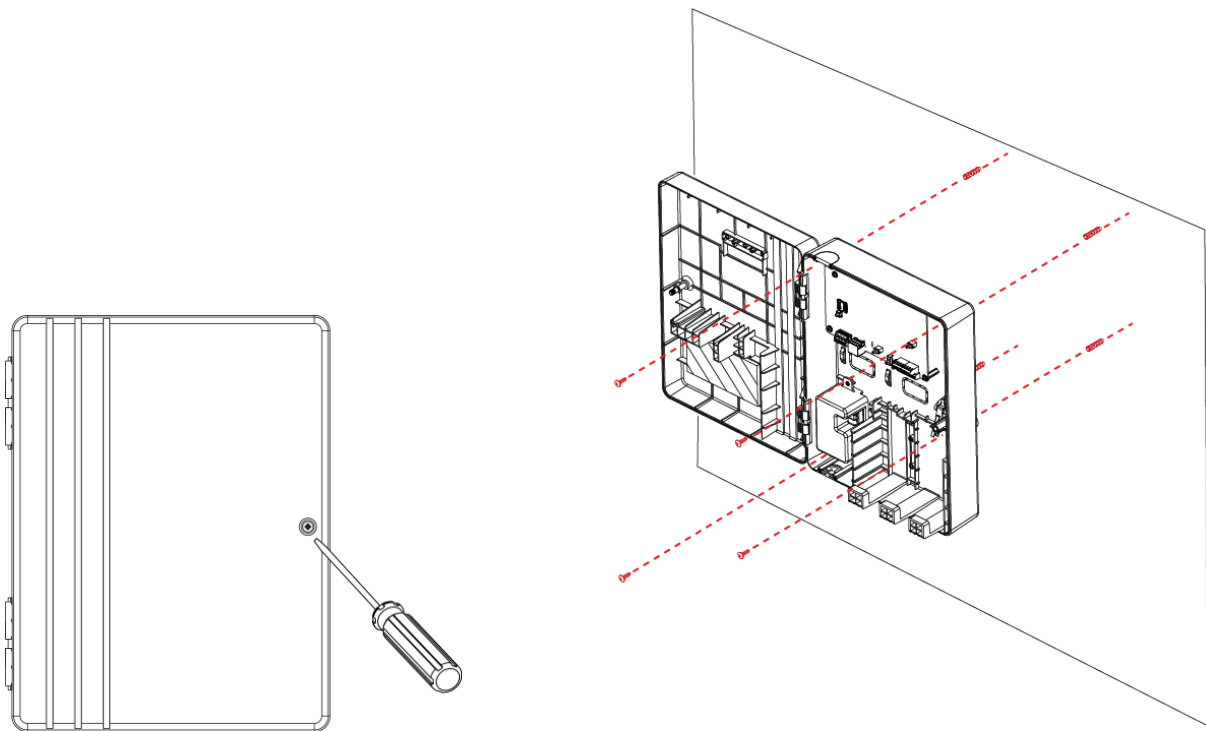
- The Control Panel requires the mains power and Ethernet connection.
- If a Cellular Module is used, ensure that there is good cellular coverage (Advisable to have a level of at least 4 out of 5).
- The Control Panel needs to have access to the routing of cables for the system to connect with wired devices.
- A central location between all the devices is often the best place, making wiring to expanders or devices easier, and preferably a place that is hidden from outside view.
- Avoid mounting the Control Panel in a damp location, close to a heat source, or near large metal objects, which may affect wireless radio strength.
- The Control Panel should be protected by sensors so that no intruder can reach the Control Panel without first activating a sensor.

3.2. Mounting

Before installation or any maintenance work, make sure the power supply has been disconnected, and the battery switch has been slid to OFF position.

Step 1. Use a flat-head screwdriver to loosen the cover fixing screw to open the top cover.

Step 2. Use the 4 mounting holes as a template to mark and drill holes appropriately.



Step 3. Use the provided wall plugs for plaster/brick installation. Make sure the wall plugs are flush with the wall.

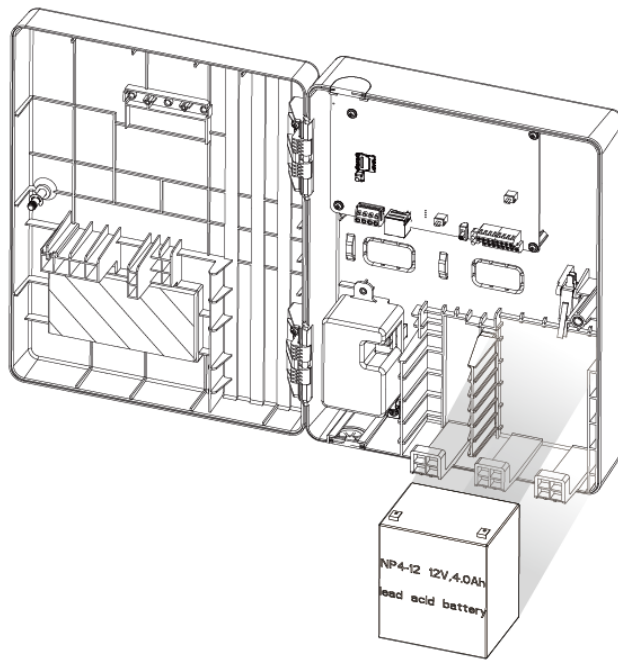
Step 4. Screw the Control Panel onto the wall. Make sure the Tamper Switch is fully depressed against the wall

Step 5. Complete wiring following the instructions in later section **3.3. Hardware Installation.**

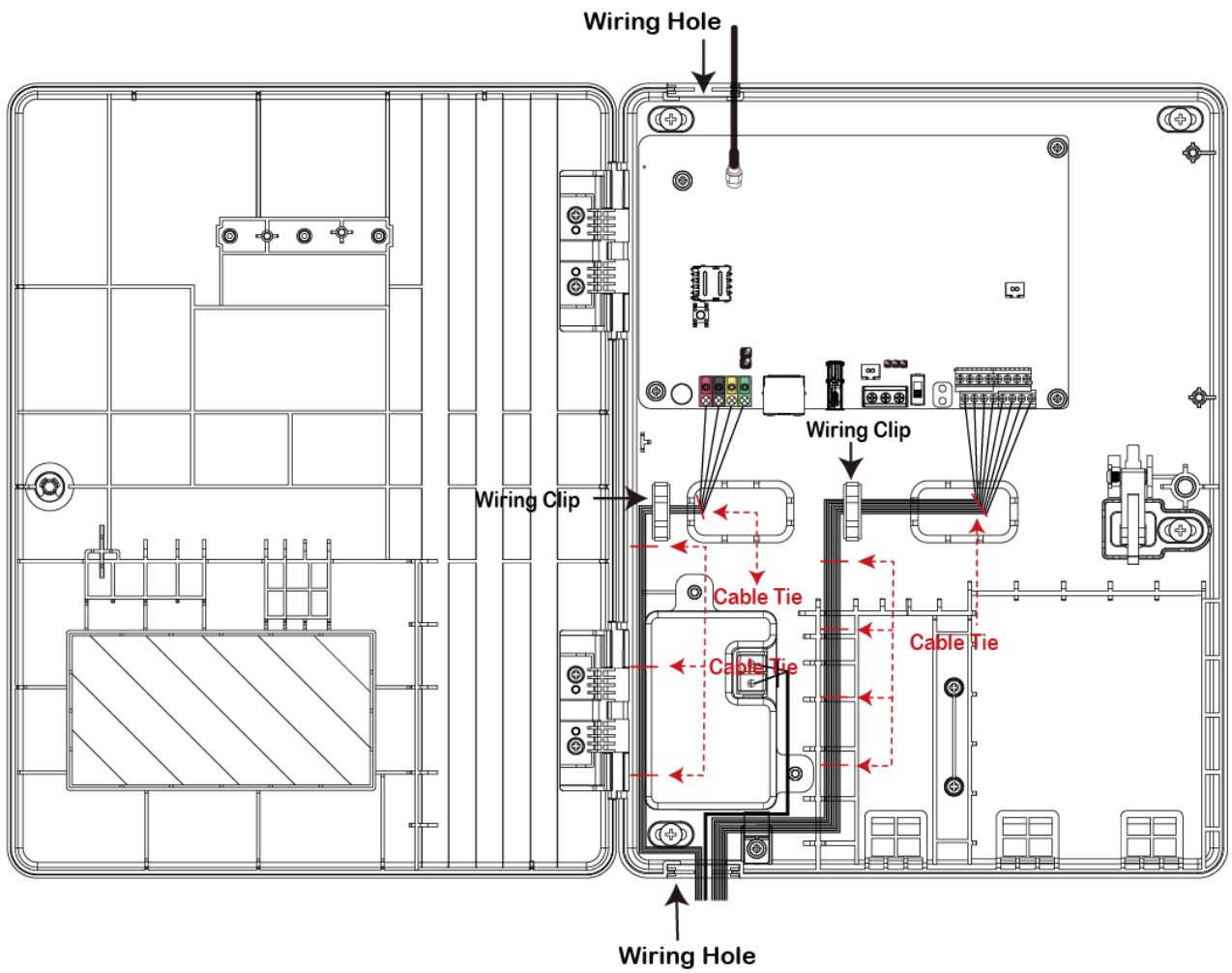
Step 6. Arrange all wires along the wire clips and then route the wires to the wiring hole on bottom. For external antenna, route the wire to the wiring hole on top.

Use cable ties (not included) to thread through the wire clips and secure the wires. Use the U-shaped grommets around the cable holes to manage wires.

Step 7. Attach the battery to Hybrid Panel Lite.



Step 8. Close the cover and tighten the cover fixing screw.



3.3. Hardware Installation

CAUTION: Before servicing, make sure the AC power has been disconnected, and the battery switch has been slid to OFF position.

- Wiring of the Hybrid Panel Lite should only be performed by certified technician with proper knowledge and training in electric equipment.
- Before installation or any maintenance work, make sure the power supply has been disconnected, and the battery switch has been slid to OFF position.
- Do not connect the devices to loads exceeding supported load current.
- Do not connect the battery or the built-in power unit until all wiring is complete.
- The control panel enclosure must be secured to the wall before operation.
- Internal wiring must be routed in a manner that **prevents**:
 - Wiring over circuit boards
 - Excessive strain on wire and on terminal connections
 - Loosening of terminal connections
 - Damage of conductor insulation
- Incorrect connections will result in failure or improper operation. Inspect wiring and ensure proper connections before applying power.

Step 1. For configuration and operation of the Control Panel via Ethernet, connect an Ethernet cable to RJ-45 port.

Step 2. Insert SIM card (Optional): Slide the metal frame of the SIM card socket leftwards (**FIG. 1**) and flip it over (**FIG. 2**); then put a SIM card onto the socket (**FIG. 3**).

When putting the SIM card, make sure the metal side of the card faces DOWN. After the SIM card is put in place, flip the metal frame back and slide it rightwards to lock it. Note that the notch of the SIM card should be in the lower left corner as in FIG. 3.

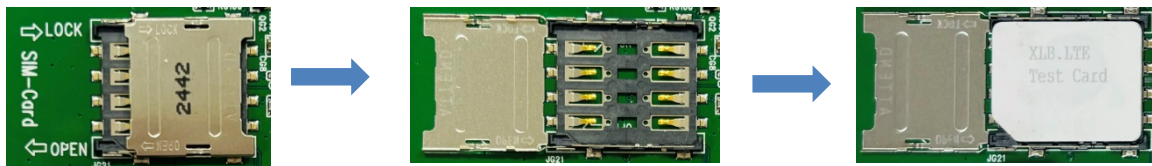


FIG. 1

FIG. 2

FIG. 3

<NOTE>

- ☞ Before inserting the SIM card, please make sure the pin code is deactivated and SMS messages are removed first.
- ☞ Inserting or Remove the SIM Card when the Panel is powered off.
- ☞ Make sure to insert a SIM card with a data plan.

Step 3. Complete wiring for Zone 1-8 terminals, GND terminals, AUX power terminals, and BUS terminal. (Please see the following sections for details.)

Step 4. Connect the external antenna to the antenna terminal on the panel.

<NOTE>

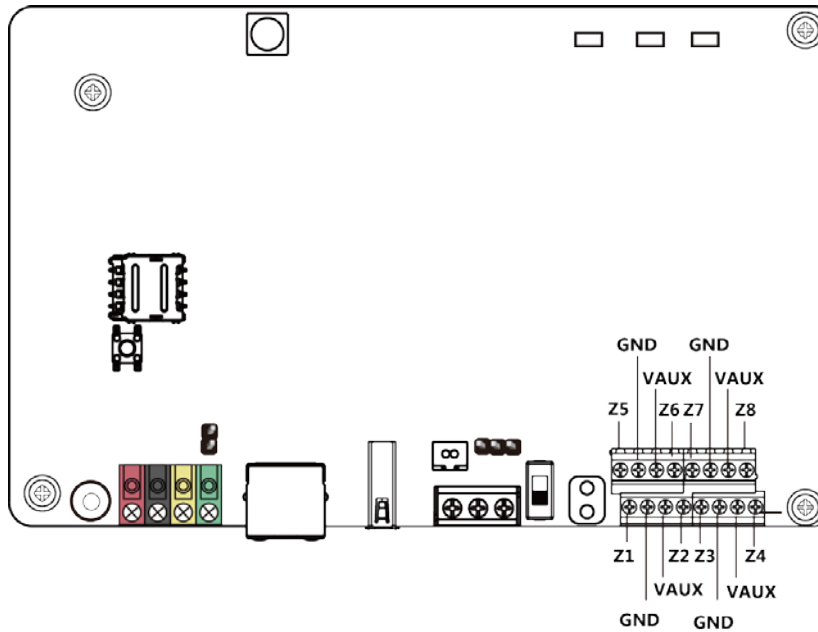
- ☞ Make sure to connect or remove the antenna when the Panel is powered off.
- ☞ Do not place the antenna close to metallic materials.

Step 5. Connect the battery to the PCB board. See **Battery Installation** in the following section for more details.

Step 6. Connect to the mains power using the built-in power unit.

Step 7. Slide the battery switch to ON position.

Zone Wiring (Zone 1 - 8)



- The 8 zones can be wired by supervising NC (normally close) or NO (normally open) devices, e.g. PIR sensor, door contact, smoke detector, water sensor, fire sensor, CO sensor, gas detector, heat detector, and glass break detector, etc.
- Wire gauge: Minimum 22 AWG, maximum 19 AWG. Do not use shielded wire.
- Total wiring length limit for connected NO/NC devices:
 - Max. 3000 ft / 914 m @ AWG-22
 - Max. 4900 ft / 1493 m @ AWG-20
 - Max. 6200 ft / 1889 m @ AWG-19

<NOTE> The wiring length is calculated based on maximum wiring resistance of 100Ω(50Ω multiplied by 2 because the wire is round-tripped).

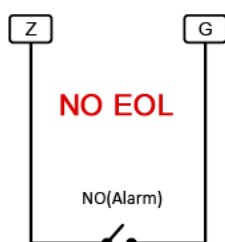
- The hardwired zones support Single-End-of-Line (SEOL), Double-End-of-Line (DEOL) loop configuration, with selectable resistor values of 1KΩ, 2.2KΩ, 3.74KΩ, 4.7KΩ, 5.6KΩ, 6.8KΩ, 8.2KΩ, 10KΩ.
- Triple end-of-line (TEOL) loop (**Non-compliant to EN regulation**) can be configured in different combinations: 4.7KΩ, 6.8KΩ, 12KΩ (resistor value selection: 6.8K), 4.7KΩ/5.6KΩ, 4.7KΩ, 2.2KΩ/3KΩ (resistor value selection: 4.7K), or 4.7KΩ/5.6KΩ, 5.6KΩ, 2.2KΩ/3KΩ (resistor value selection: 5.6K).
- For an NO loop, please have an EOL resistor in parallel (across) the loop.
- For an NC loop, please have an EOL resistor in series with the loop.
- If a zone wiring method is changed, be sure to turn the system power off and back on again to avoid triggering the alarm.

Please refer to the following diagrams of loop 1 to 10 for wiring examples.

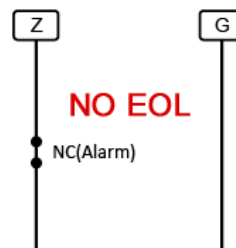
NO/NC Wiring

The panel can detect alarm for corresponding NO or NC devices via the open, secure or shorted circuits. <Note> There is no EOL resistor in loop 1 and loop 2

1.



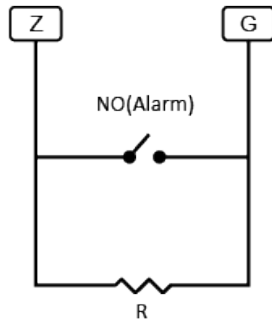
2.



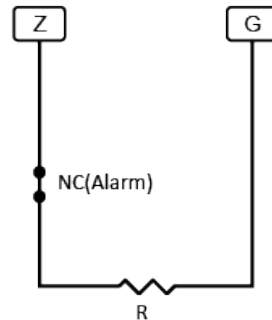
Single-End-of-Line (SEOL) Resistor Wiring

The single-end-of-line (SEOL) resistor shall be installed near the wired device at the end of a zone loop to supervise the wiring conditions for NO and NC devices, so the panel can detect alarm and tamper for corresponding devices via the open, secure or shorted circuits.

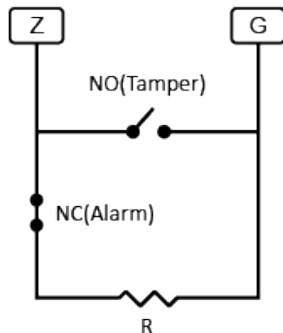
3.



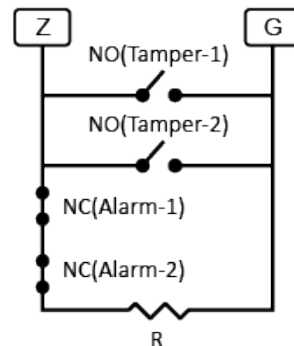
4.



5.



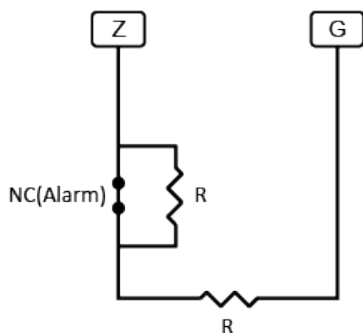
6.



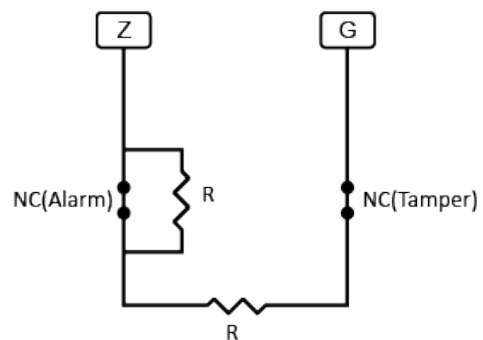
Double-End-of-Line (DEOL) Resistor Wiring

The double-end-of-line (DEOL) resistor shall be installed near the wired device at the end of a zone loop to supervise the wiring conditions for NC devices, so the panel can detect alarm and tamper for corresponding devices via the open, secure or shorted circuits.

7.



8.

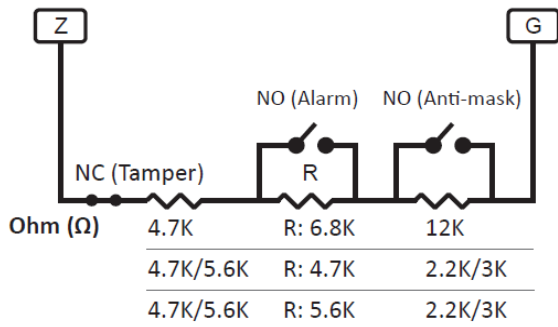


Triple-End-of-Line (TEOL) Resistor Wiring (Non-compliant to EN regulation)

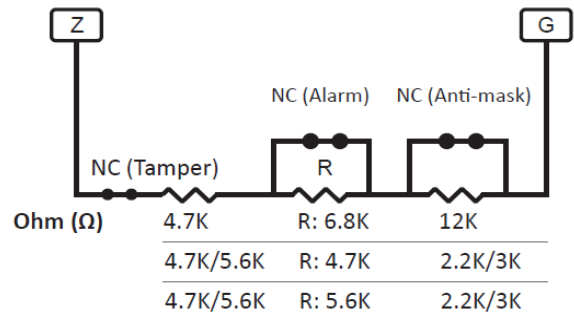
The triple-end-of-line (TEOL) resistor shall be installed near the wired device at the end of a zone loop to supervise the wiring conditions for NC or NO devices, so the panel can detect alarm, tamper and anti-masking for corresponding devices via the open, secure or shorted circuits.

☞ The unit for values in the following is in ohms (Ω).

9.



10.



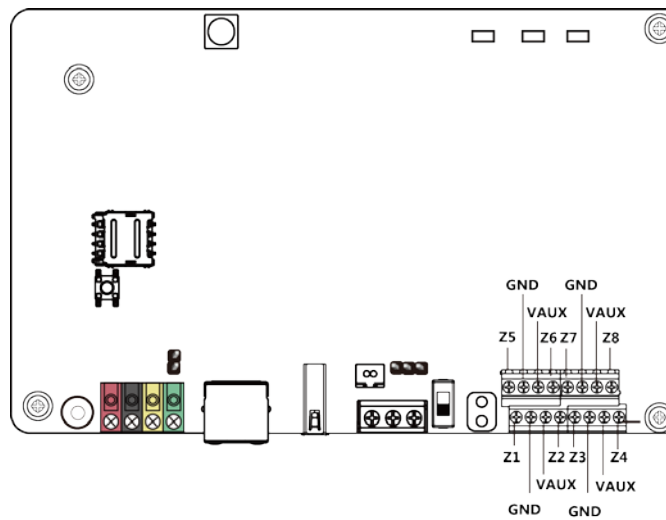
Z: Wired Zone Input

G: GND

NO: Normal Open Contact

NC: Normal Close Contact

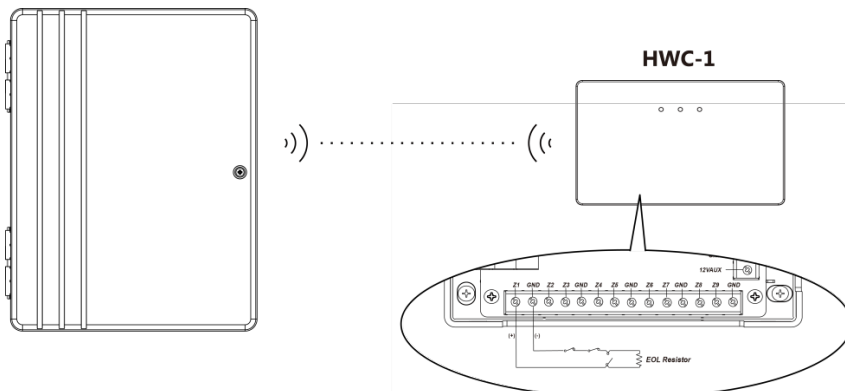
AUX Power Wiring



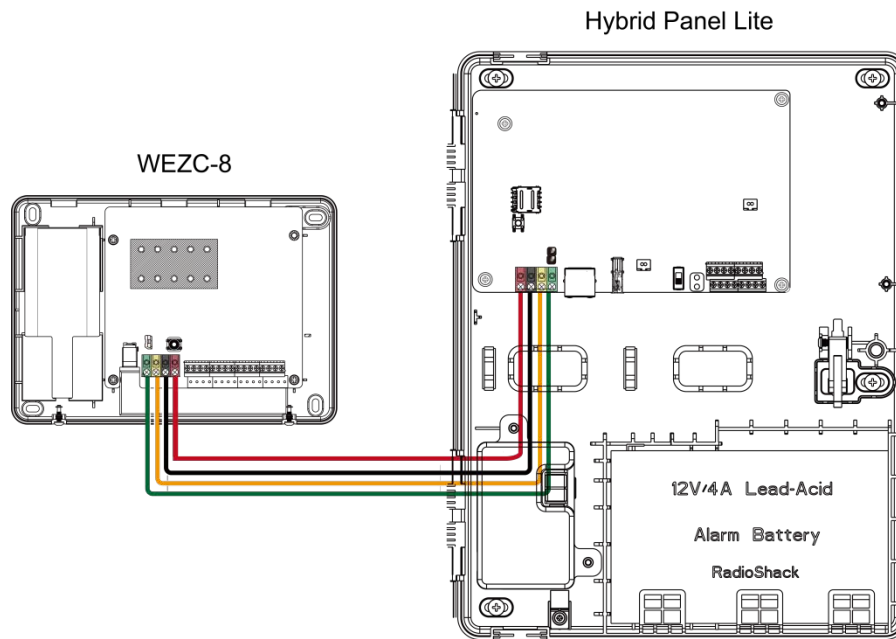
- The Control Panel can provide a total of **1.5A** current for hardwired zones, auxiliary output, BUS devices, wired keypad, expansion modules, and PGM port.
- Min/Max operating voltages for devices/detectors is 10 VDC -14VDC.
- Please note that the total current should **not exceed 1.5A**; otherwise, an additional power supply is required.

Wired Zone Expansion

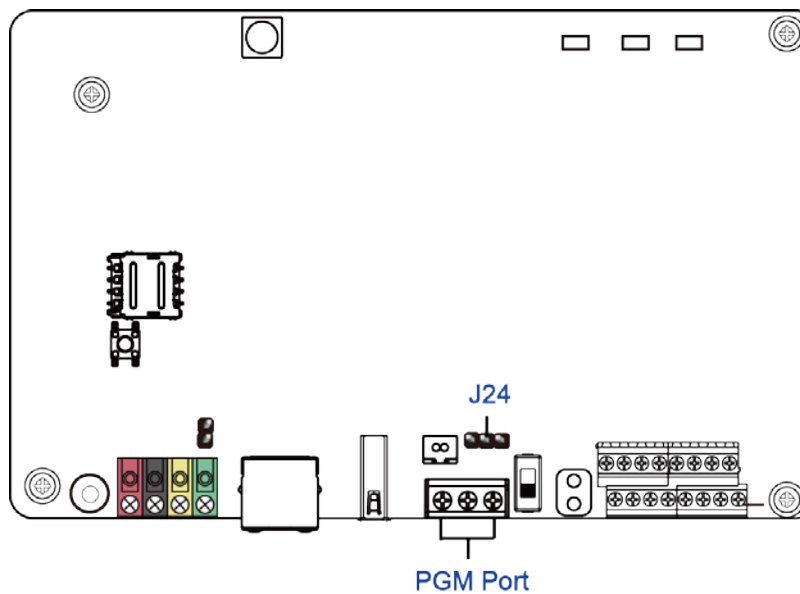
- Hybrid Panel Lite is compatible with HWC-1 Wireless Converter. One HWC-1 can add 9 wired zones to the Control Panel.



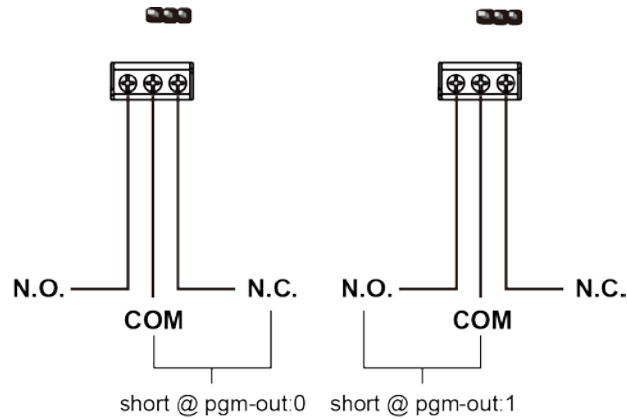
- The WEZC-8 Expansion Module can be connected to the Hybrid Panel Lite via BUS, enabling the expansion of 8 wired zones.



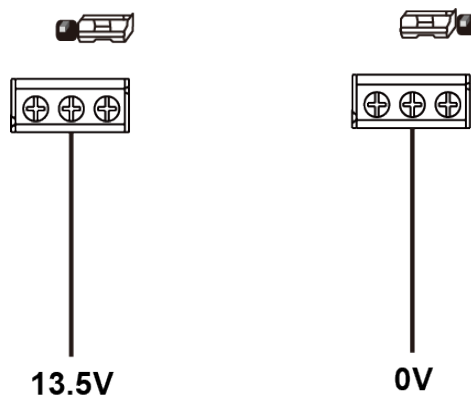
PGM Wiring



- The output of PGM is 13.5V with a maximum current of 500mA. The total current drawn from all sources—hardwired zones, auxiliary output, BUS devices, wired keypad, expansion modules, and the PGM port—should not exceed **1.5A**.
- The PGM port function either as a voltage output port (specifically for connecting to a siren) or as a dry contact relay output, depending on the J24 jumper settings:
- When J24 Jumper Switch is disconnected, PGM port will operate as a dry contact relay output.



- When the J24 jumper link is inserted connecting the 1st and 2nd pins (from the right), the PGM port will provide 13.5V output for a connected siren.
- When the J24 jumper link is inserted connecting the 2nd and 3rd pins (from the right), the PGM port will provide 0V output.



Connecting Keypads / Wired Security Devices / Expansion Modules via the data BUS

The keypads, security devices, and expansion modules compatible with Hybrid Panel can be connected in series via the data BUS.

To assist with cable connections, the terminal blocks on each system module are color-coded for easy identification.

Terminal block color codes:

Red	VDD
Black	GND
Yellow	485A
Green	485B



Note:

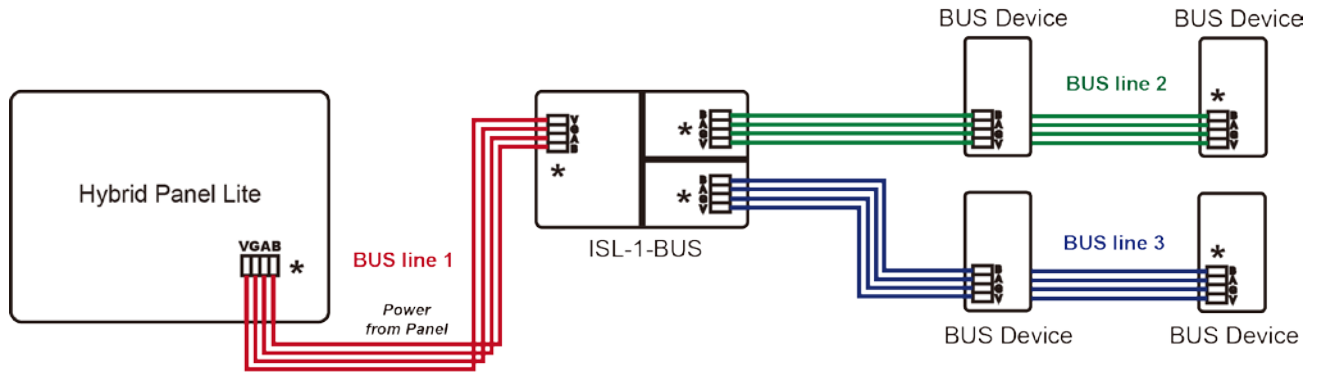
☞ For KPT-35-COMBO and KPT-35(N)-BUS, the terminal blocks are marked as V, G, A, B instead of color-coded.

Wiring Guideline

- The Hybrid Panel Lite is the first device on the data BUS. Ensure the Control Panel's J53 Jumper Switch and the furthest BUS device's Jumper Switch are set to ON to serve as a terminating resistor.
 - ☞ Be sure to only enable the aforementioned 2 jumper switches and do not set the jumper switches to ON for any other BUS devices in between.
- The total wiring length limit is a maximum of 3000 ft / 914 m.
 - ☞ Depending on wired device's power consumption, PWB-1-BUS (auxiliary power supply

module), or AMP-1-BUS (Range Extender), or ISL-1-BUS (Isolated Range Extender) might be needed.

- The total number of BUS devices (refer to as “nodes”; the Hybrid Panel is counted as one node) on each BUS line must be within 32 or less. Otherwise, BUS signal abnormalities may occur. Be noted that a maximum of 128 BUS devices (including Hybrid Panel Lite and other nodes) can be connected to the panel.
- In the example below, there are a total of 3 BUS lines/segment: **BUS line 1** contains 2 nodes (Hybrid Panel Lite and ISL-1-BUS), **BUS line 2** contains 3 nodes (ISL-1-BUS and 2 BUS devices), **BUS line 3** has 3 nodes (ISL-1-BUS and 2 BUS devices).



* : Terminal Resistor Jumper (switch to ON)

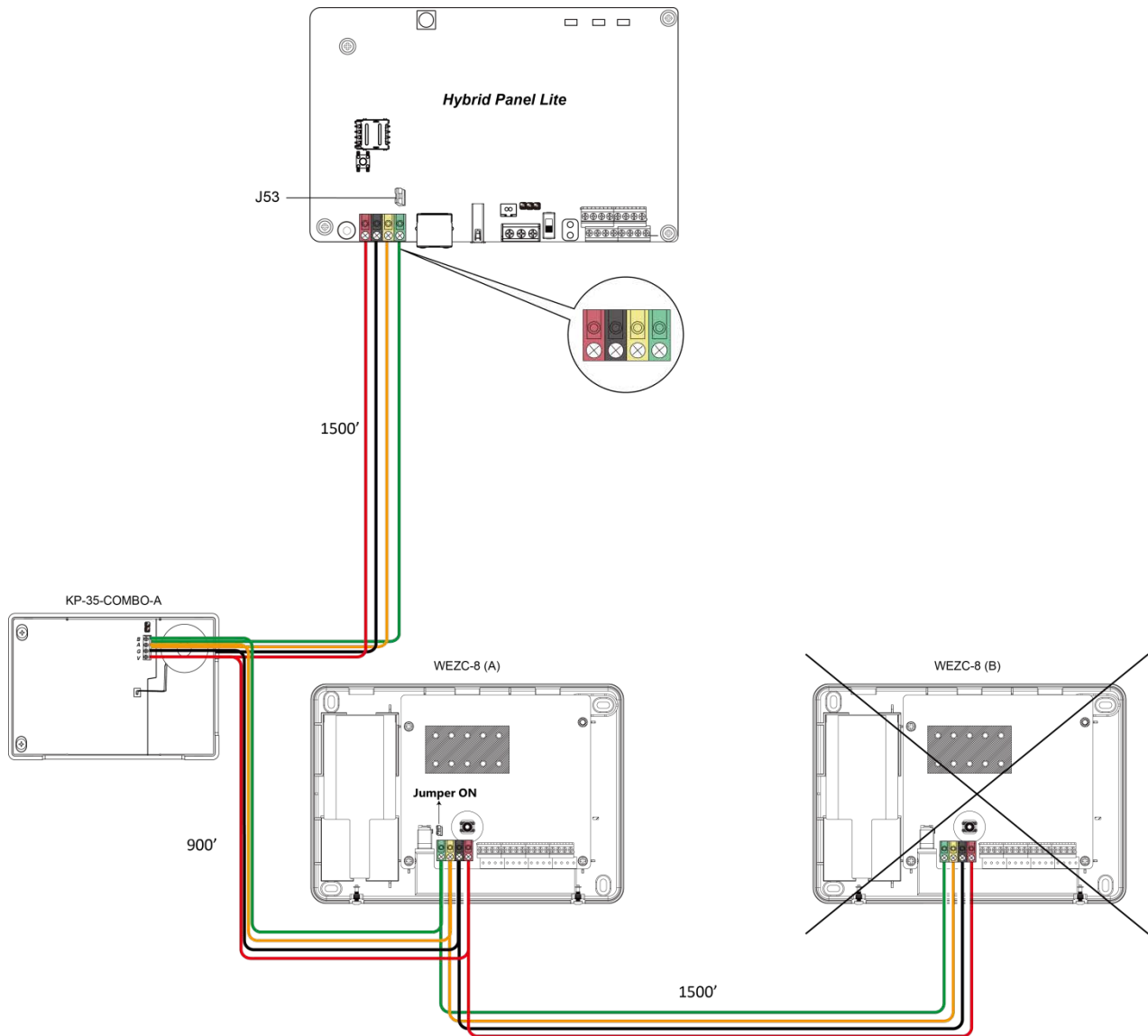
- Out of the 128 BUS devices mentioned above, a maximum of 4 keypads can be connected.
- The total number of zone expansion modules, relay expansion modules, wired keypads, and other BUS devices depends on wired device's power consumption. PWB-1-BUS (power bank) may be needed.

NOTE:

- ☞ **Please note that if you connect all the BUS devices first, then connect them all to the Control Panel to start the learning process, the maximum number of connected BUS devices should not exceed 20.**
- ☞ **If you connect more than 20 devices, the system may not operate smoothly and could cause errors on the panel programming webpage. It is recommended to connect and learn the devices one by one to ensure optimal system operation.**

Wiring Example

- **KPT-35-COMBO-A** and **WEZC-8 (A)** are wired correctly in series, as the total wire distance of the two devices from the Control Panel are within 3000 feet. **WEZC-8 (B)** is NOT wired correctly as it is 3900' / 1185m from the panel, which makes it exceed the total length of wiring of 3000 feet.
- For optimal communication in the wired connection between the Control Panel and the connected BUS devices, ensure the Communication Jumper Switch of the furthest BUS device and the J53 Jumper Switch of the Control Panel are set to ON to serve as terminating resistors. Only enable these 2 jumper switches and do not set the jumper switches to ON for any other BUS devices in between. For example, for the **WEZC-8 (A)** in the picture below, ensure its jumper switch is set to ON to serve as a terminating resistor since it has the furthest distance from the Control Panel.



BUS Power Supply Management

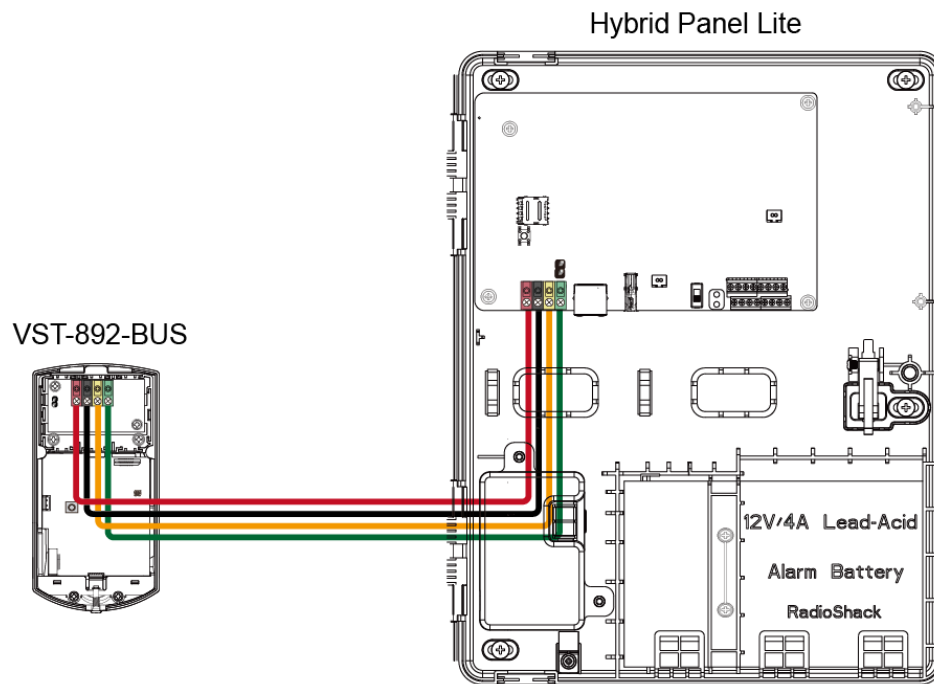
- When using the Hybrid Panel Lite to connect multiple external devices, it is important to ensure that the power supply is adequate for connected devices.
- Hybrid Panel Lite can provide a maximum of 13.5V/1.5A power supply to the connected BUS devices or expansion modules.
- Expansion boards WEZC-8B and WEPC-1B support backup battery, and they can be employed to use external power supply if power supply from the Panel is not enough.

When connecting an expansion board with external power supply to BUS, please bypass the red VDD terminal. Use the provided Wago 221 Splicing Connector to connect the VDD terminal on the Control Panel to the next BUS device that is powered by Hybrid Panel Lite.

Bus Power Supply Connection Examples

BUS devices can be connected in different combinations of devices, and be powered by different power sources. Here are three of the two possible connection methods with different device combination.

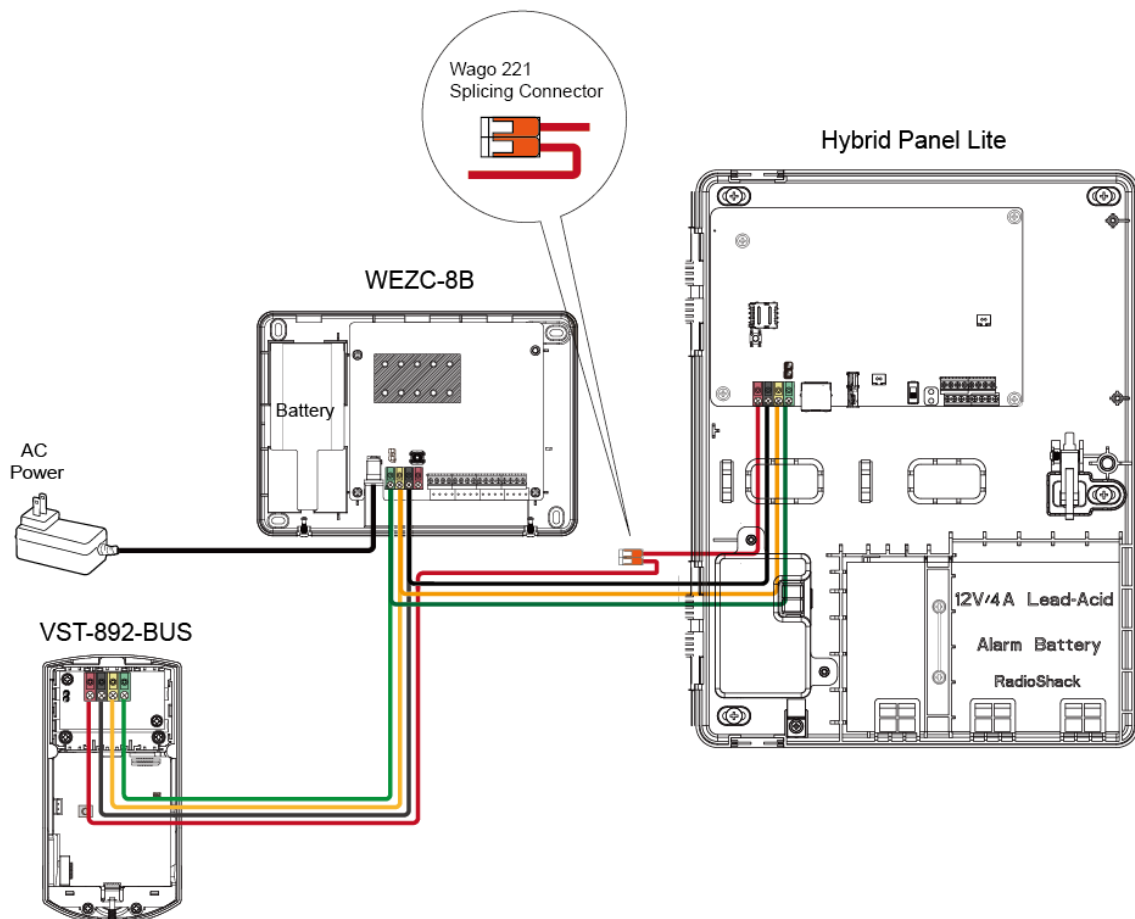
- **Example 1:** Power supply from the Control Panel to a BUS device (VST-892-BUS):



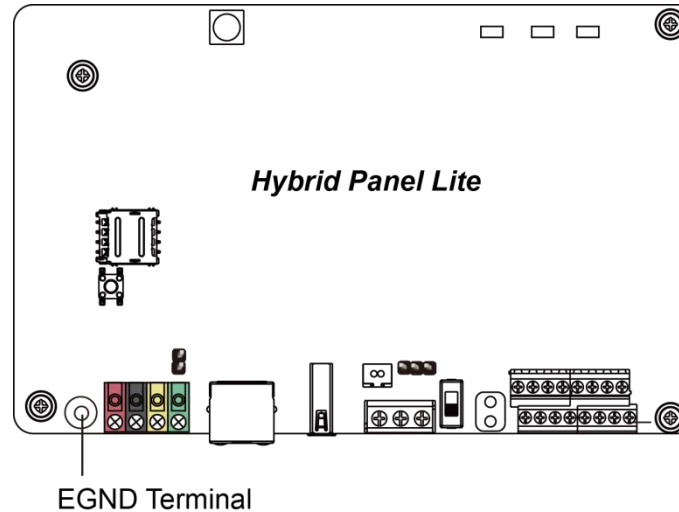
- **Example 2:** Power supply from the Control Panel to BUS device (VST-892-BUS), and Expansion Board (WEZC-8B) receives power from external power source:

Note:

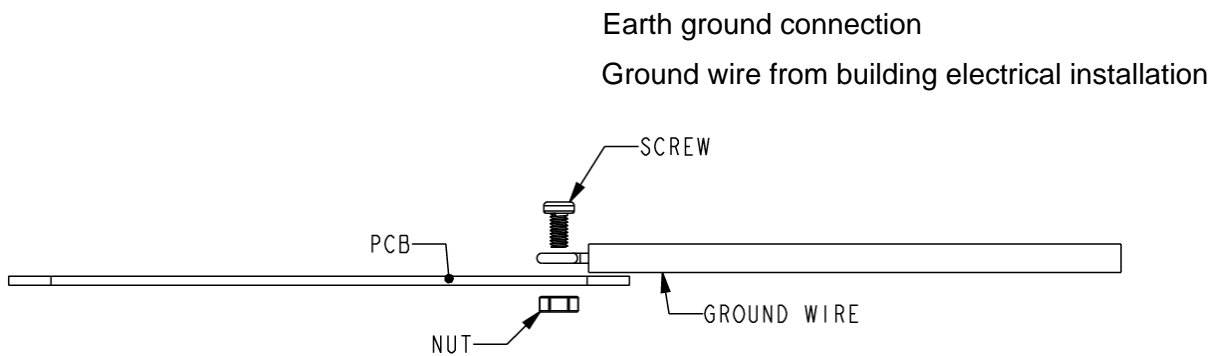
Be sure to bypass the red VDD terminal on the Control Panel using the provided Wago 221 Splicing Connector. Connect the VDD terminal to the next BUS device (VST-892-BUS as example) that is powered by Hybrid Panel Lite.



Ground Wiring



- EGND ground wiring is implemented to protect the panel from electricity leakage.
- Prepare grounding wire (insulated green wire, minimum 22 AWG), and connect it to the building's electrical outlet. Then, secure the grounding wire onto Hybrid Panel Lite's EGND Terminal using a ground screw and nut.

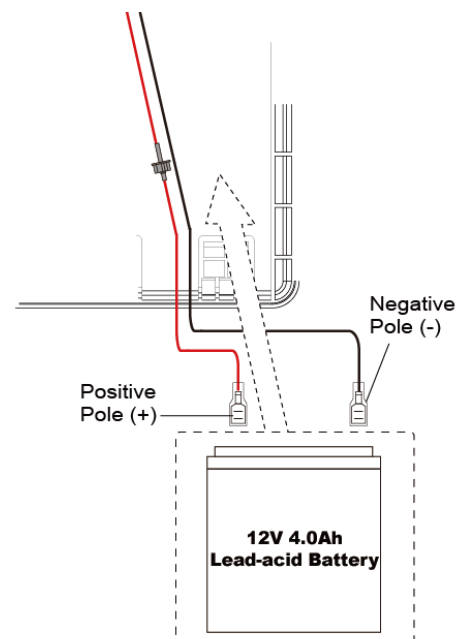


NOTE:

The ground wire, nut and screw are not included in the product's package.

Battery Installation

- The Control Panel can support a rechargeable battery to serve as a backup power source.
- Battery:
12V/4Ah SLA battery (see **3.2. Mounting** for details).
- To Install the battery, follow the steps below:
 - 1) Connect the GND cable (Black) to the negative pole (-) of battery.
 - 2) Connect the power cable (Red) to the positive pole (+) of battery
 - 3) Attach the battery to the Hybrid Panel Lite.



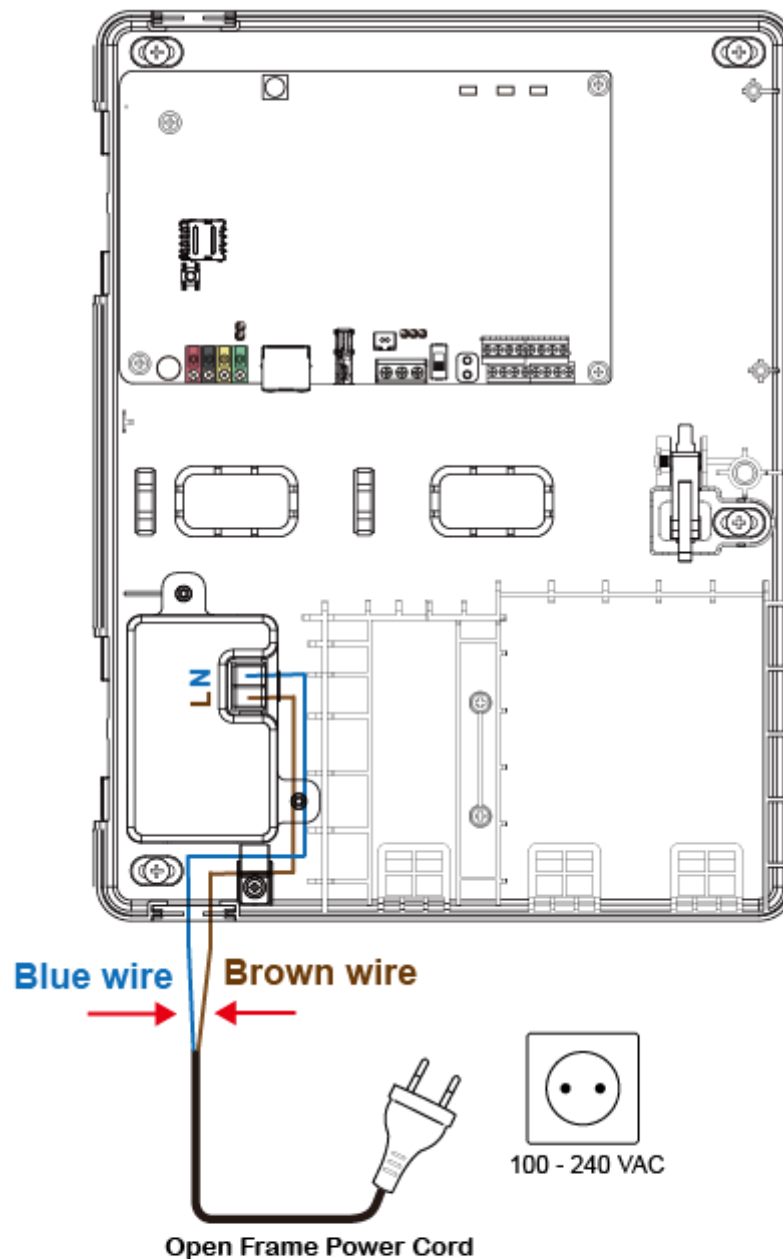
Using the built-in Power Unit

- **Open Frame** built-in Power Unit is installed. For Open Frame, connect **BROWN** wire of the power cord to Terminal **L** of the built-in Power Unit, and connect **BLUE** wire to Terminal **N**. Please refer to the figure below.

NOTE:

- ☞ Ensure to turn off all power supplies including Built-in Power Unit and Battery before connecting or removing cables or wires.

- **Open Frame built-in Power Unit:**

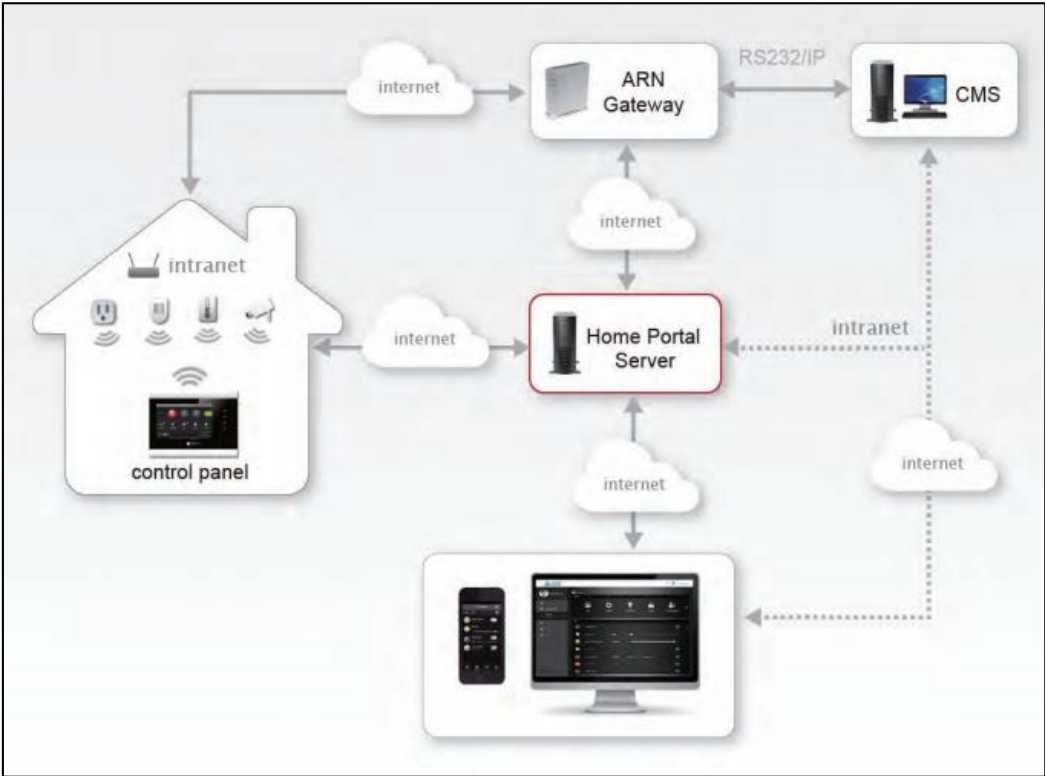


Open Frame Built-in Power Unit:
Connecting **BROWN** wire to Terminal **L**
Connecting **BLUE** wire to Terminal **N**

3.4 Connect to Hybrid Panel Lite Home Portal Server

Home Portal™ Sever is a smart home platform that allows user to connect to the Hybrid Panel Lite via PC or smart phones over internet, delivering smart home services for users to control home devices and security remotely.

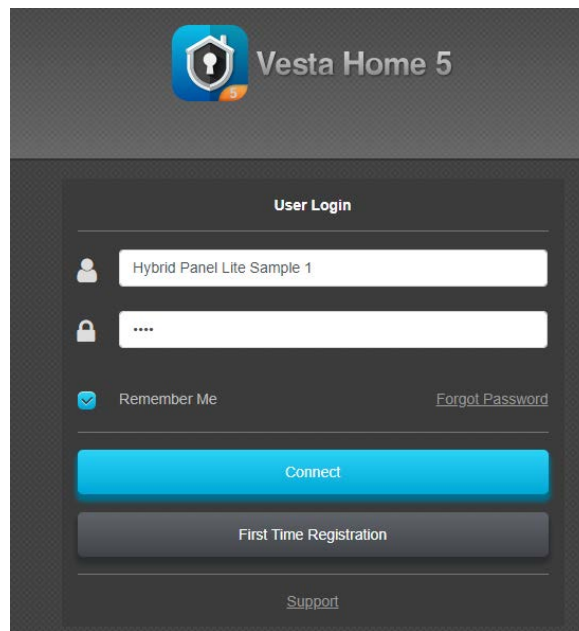
Home Portal™ Sever can provide level 2 and level 3 access of the Hybrid Panel Lite once the panel is registered and connected to server. Level 2 users are masters, who can operate the alarm system. Level 3 users are installers, who are authorized to program system configurations and more advanced settings.



4. Level 2 Access

4.1. Log In

Step 1. Connect to <https://eu.vestasmarthome.com> and log in with provided username and password as below.



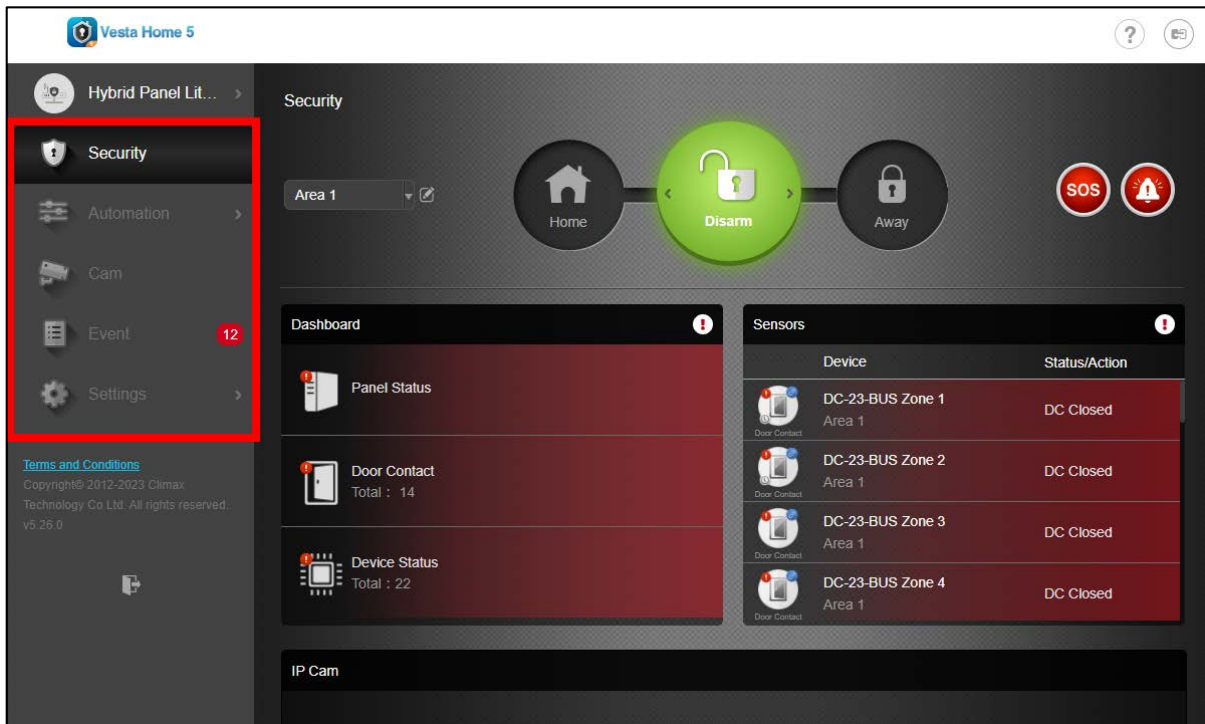
1. Functional Test	MAC Address	Username	Password
Hybrid Panel Lite Sample 1	00:1D:94:1B:24:B3	Hybrid Panel Lite Sample 1	1234
2. EMC Test	MAC Address	Username	Password
Hybrid Panel Lite Sample 2	00:1D:94:1B:58:17	Hybrid Panel Lite Sample 2	1234
3. Climatical Test	MAC Address	Username	Password
Hybrid Panel Lite Sample 3	00:1D:94:1B:24:B7	Hybrid Panel Lite Sample 3	1234
4. Power Supply Test	MAC Address	Username	Password
Hybrid Panel Lite Sample 4	00:1D:94:1B:58:D5	Hybrid Panel Lite Sample 4	1234
5. Communication Test	MAC Address	Username	Password
Hybrid Panel Lite Sample 5	00:1D:94:1B:24:A5	Hybrid Panel Lite Sample 5	1234

6. RF Alarm Transmission Test	MAC Address	Username	Password
Hybrid Panel Lite Sample 6	00:1D:94:1B:24:A2	—	—
7. RF Functional Test	MAC Address	Username	Password
Hybrid Panel Lite Sample 7	00:1D:94:1B:58:3F	Hybrid Panel Lite Sample 7	1234

Step 2. You will log in as a **master user (Level 2 access)** and enter the main page of your account.

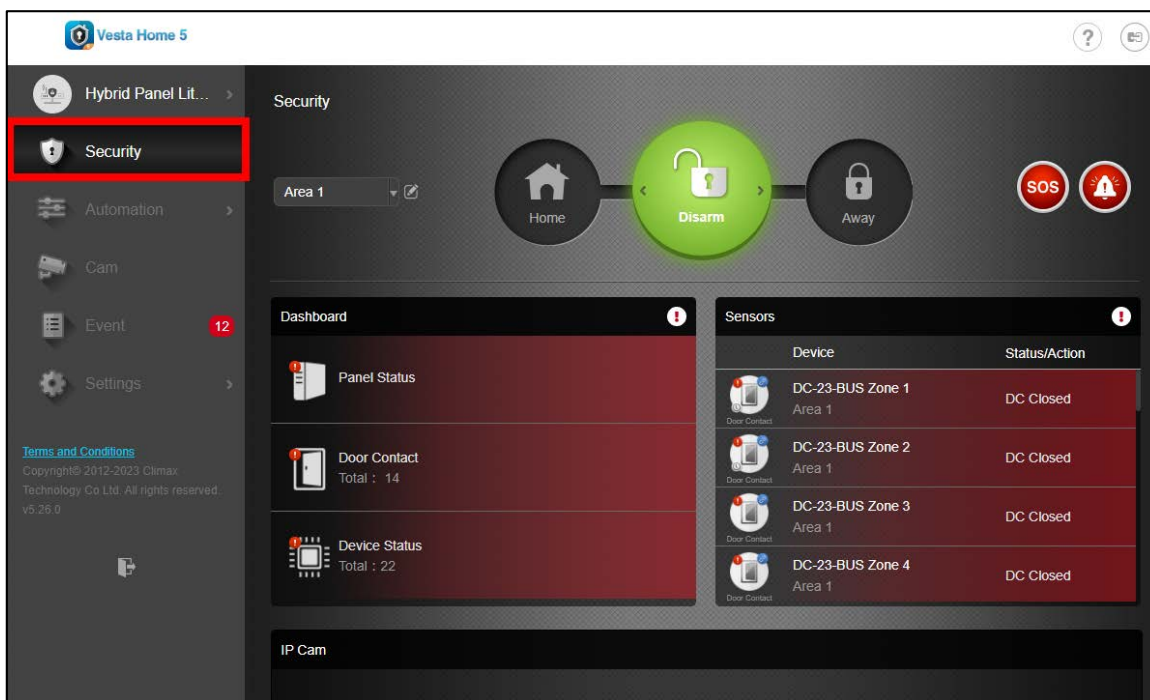
As a master user, you will be able to operate the alarm system with access to the following functions:

- **View current system mode and a list of security sensors/devices**
- **Arm/Disarm/Home arm**
- **Fault display**
- **Home Automation Setting**
- **Camera Viewing/Setting**
- **Event log**
- **Partial Setting Functions**



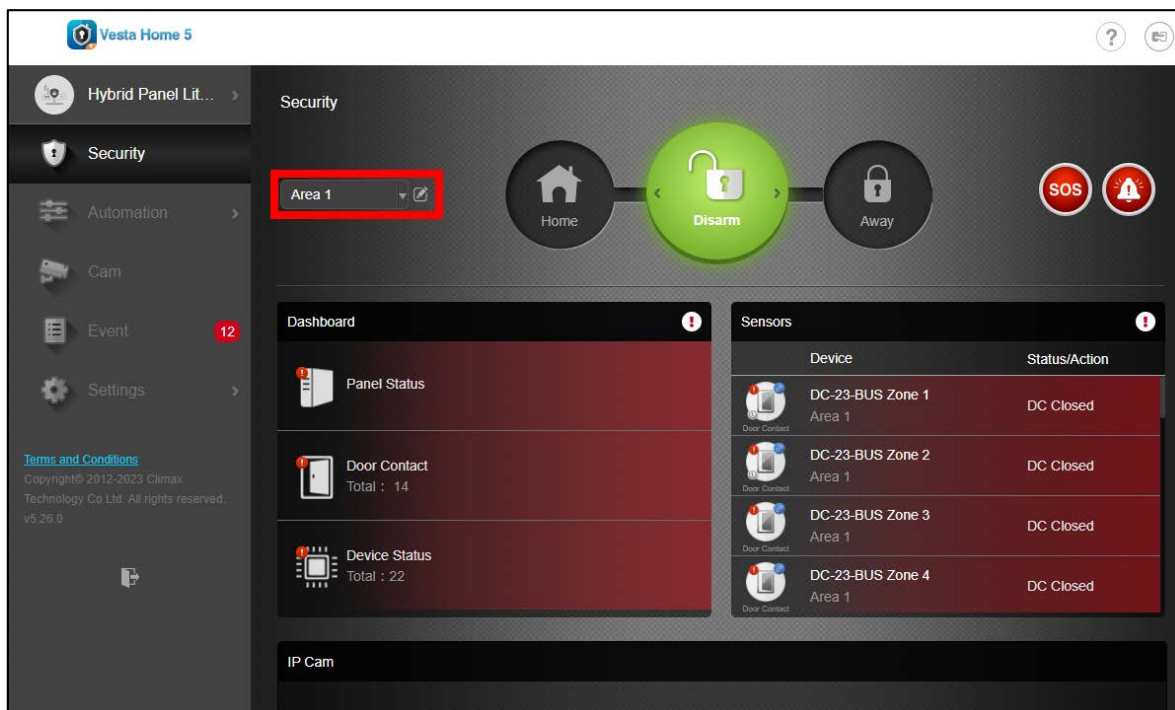
4.2. Security

The Security page displays current system mode and security sensors/devices learnt in the Control panel for quick access.



4.2.1. System Area

The Security webpage displays the security sensors, and security cameras for the selected area.



System Mode: The system mode is indicated by the 3 buttons at top of the webpage. The current system mode will light up.



To change system mode:

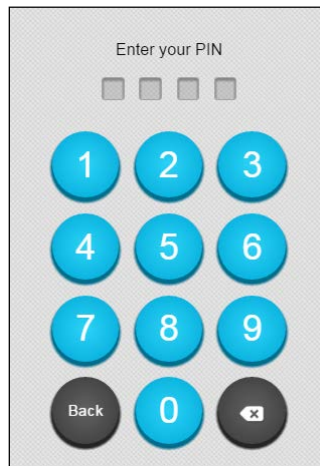
Step 1. Click on the desired mode button. You will be required to enter one of the Control Panel User PIN Code for the area to confirm action.

User PIN #1 in Area 1

User PIN #1 in Area 2

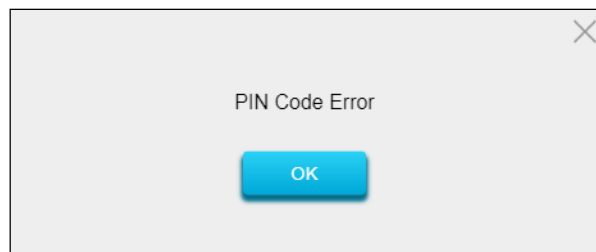
Password: **123456**

Password: **654321**



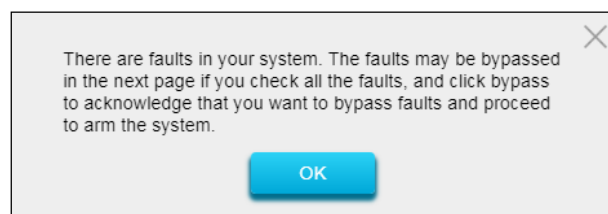
Step 2. Enter the User PIN Code, if the PIN Code is correct for arming action, the Control Panel will begin Exit Time countdown.

If incorrect PIN Code is entered, the webpage will display error message and arming will be aborted.



(Compliant with EN 50131-3 (2009) Clause 11.7.2 Prevention of setting and overriding of prevention of setting procedures)

If the system has existing fault events when arming, the webpage will display fault message and arming will be aborted. If you still want to arm the system, repeat the arming action within 30 seconds to Force Arm.



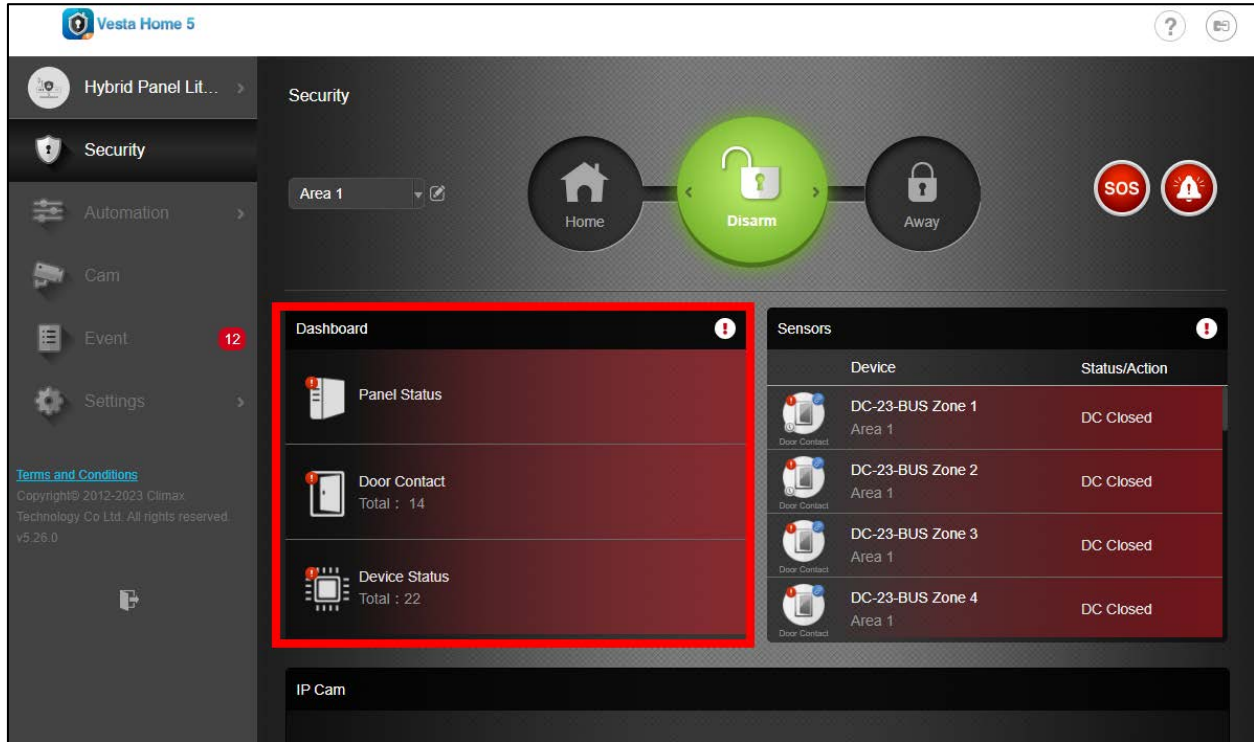
<NOTE>

☞ Force Arm is not allowed if there is device tamper fault. Device tamper fault can only be cleared by level 3 user. (Please refer to **5.1.1 Device** for details.)

Step 3. When arming/disarming is complete, the mode button will change accordingly.

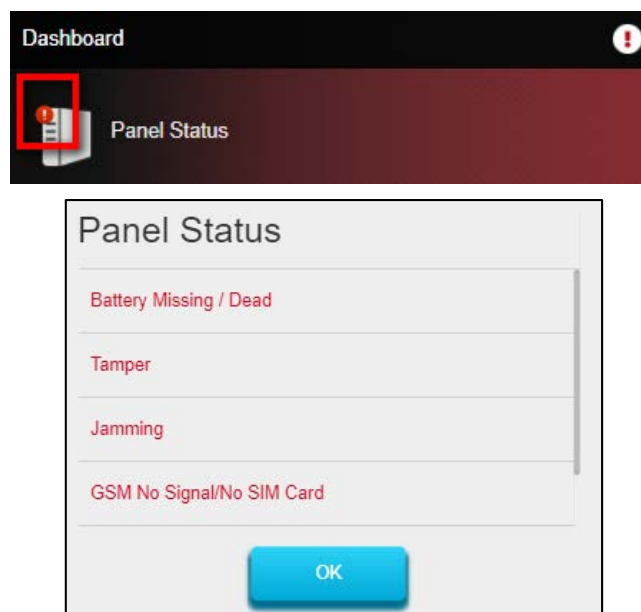
4.2.2. Dashboard

At-a-Glance Dashboard (Panel Status / Door Contact Status / Device Status) has been added to Security page.



The control panel constantly checks the system for any faults. When fault event exists in the system, the panel Orange LED 3 will turn on. The Panel Status column in Dashboard will change to red, the fault icon will appear on top left corner of the Panel icon to alert the user.

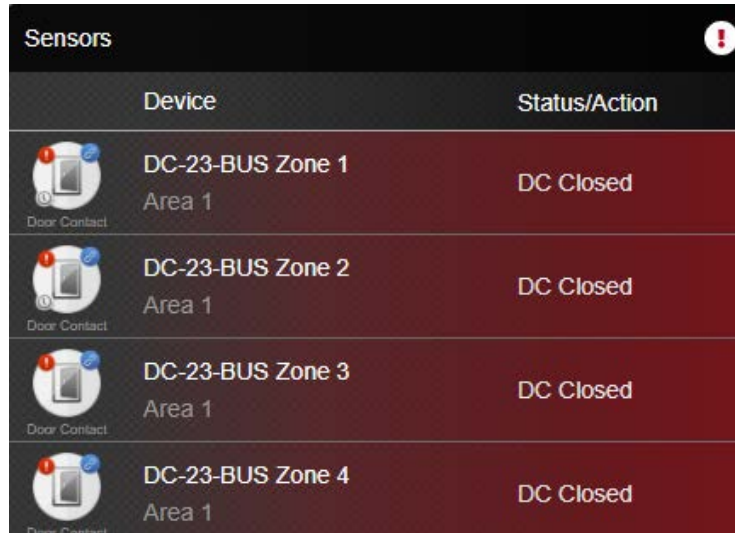
Click the panel icon to check the detailed fault information.



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

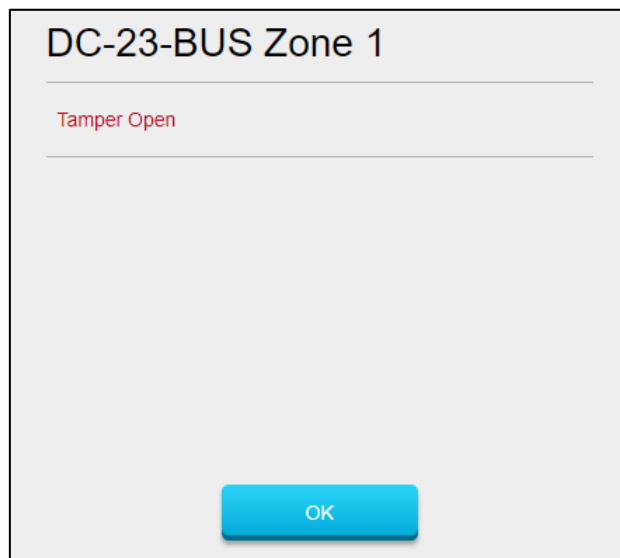
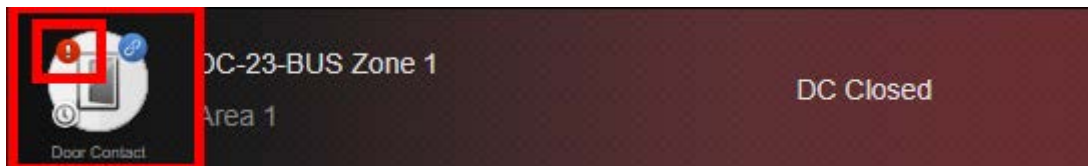
4.2.3. Sensors

The sensor section lists all security function related accessory device in the system.



Device	Status/Action
DC-23-BUS Zone 1 Area 1 Door Contact	DC Closed
DC-23-BUS Zone 2 Area 1 Door Contact	DC Closed
DC-23-BUS Zone 3 Area 1 Door Contact	DC Closed
DC-23-BUS Zone 4 Area 1 Door Contact	DC Closed

If a particular sensor has fault, the sensor's column will change to red, the fault icon will appear on top left corner of the device icon to alert the user. Click the sensor fault icon to check the detailed fault information.



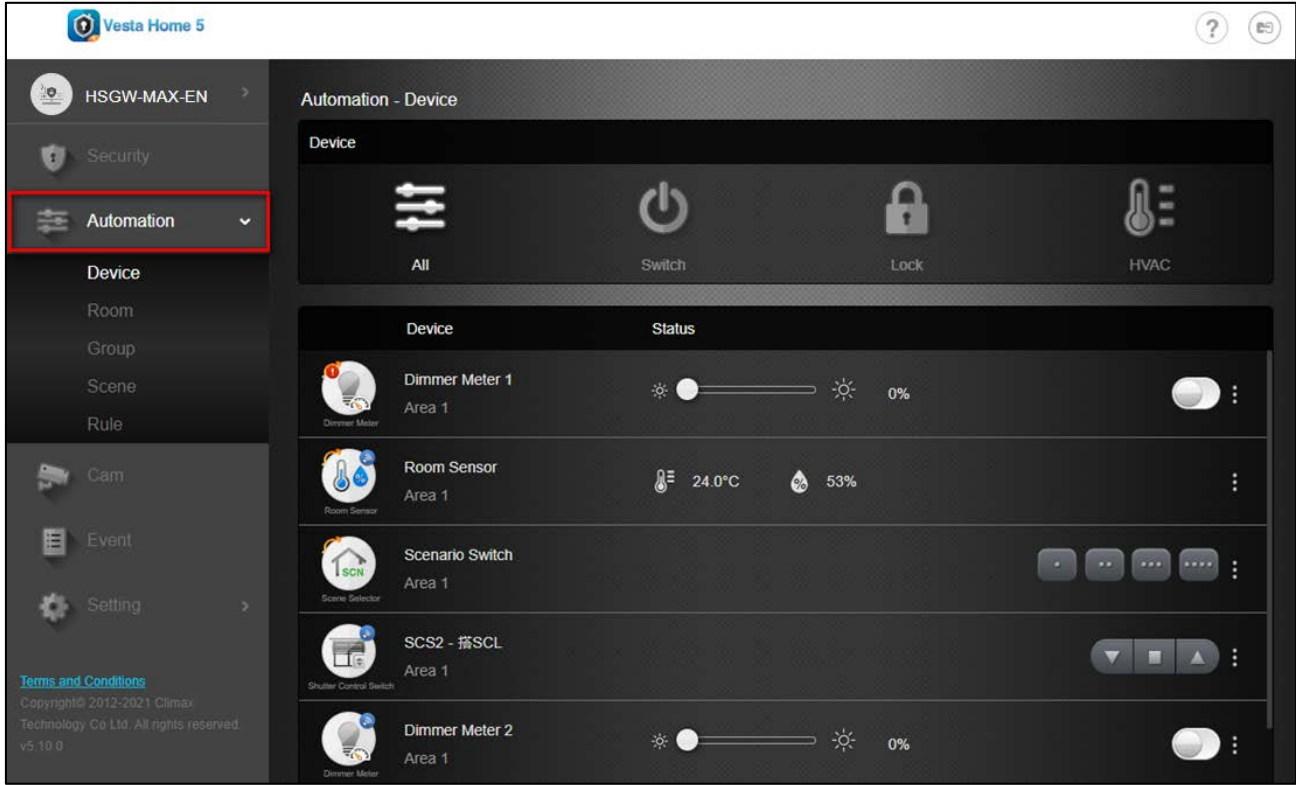
4.2.4. IP Cam List

The IP Cam List shows the IP Cameras currently learnt in the Control Panel. Click on the IP Camera Image to go to IP Cam page and view streaming video



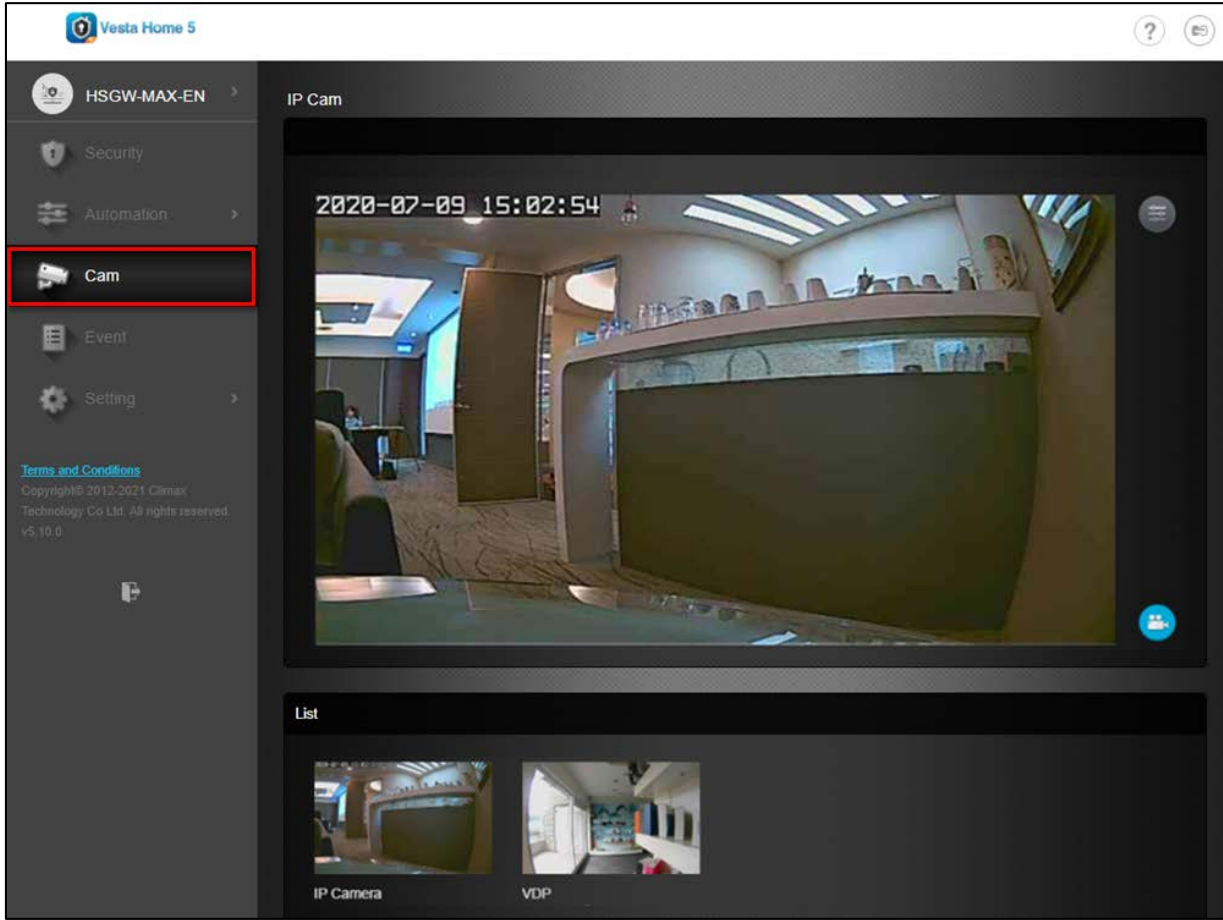
4.3. Automation

The Automation page provides access to home automation functions in the Control Panel.



4.4. IP Camera

The IP Camera page provides real time video streaming from your IP Cameras and Video setting functions.



4.5. Event

The Event page records all alarm/status event transmitted from the Control Panel.

2024/02/21	Event Type	Area	Time	Source
	Tamper	Area 1	09:26:47	DC-23 Zone 16
	Remote Disarm	Area 1	09:11:02	user
	Tamper	Area 1	09:10:52	DC-23 Zone 19
	Burglar	Area 1	09:10:52	DC-23 Zone 19
	Tamper	Area 1	09:09:33	DC-23 Zone 20
	Burglar	Area 1	09:09:33	DC-23 Zone 20
	Tamper	Area 1	09:04:32	DC-23 Zone 17
	Burglar	Area 1	09:04:32	DC-23 Zone 17

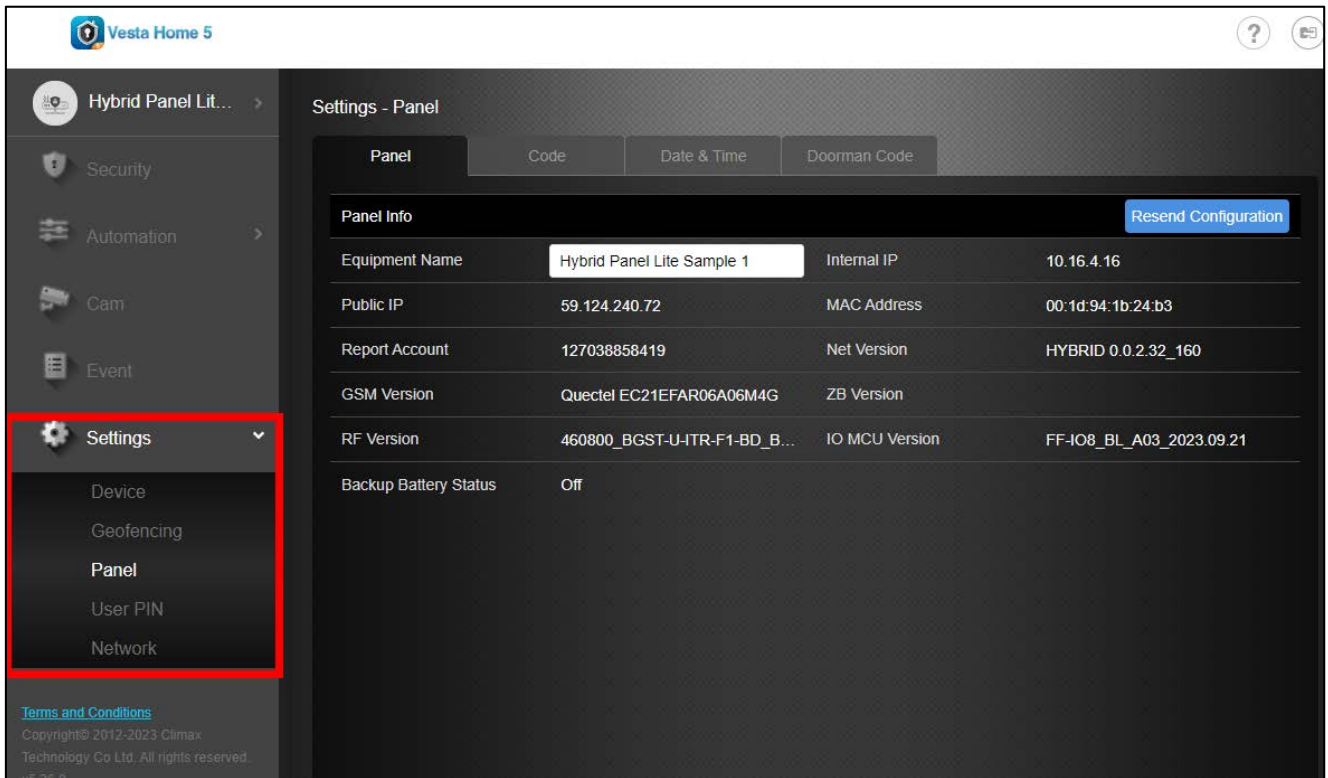
Select the event category to determine what events are displayed



4.6. Setting

The master user (**Level 2 access**) can access partial Setting page functions, including:

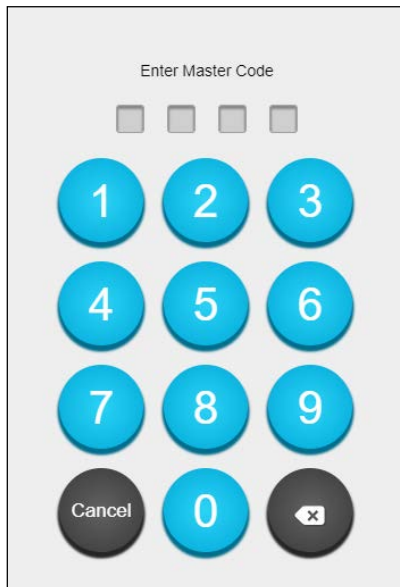
- **Device**
 - Device Search
 - Walk Test
 - Partial Device Configuration
- **Geofencing Setting**
- **Code setting**
 - Individual Master Code
 - Temporary Code
- **Date and Time setting**
- **User PIN**
- **Network Setting**



The screenshot displays the Vesta Home 5 web interface. The top navigation bar includes the Vesta Home 5 logo and a help icon. The left sidebar contains a menu with items: Hybrid Panel Lit..., Security, Automation, Cam, Event, and Settings. The Settings menu is highlighted with a red box and expanded to show sub-items: Device, Geofencing, Panel, User PIN, and Network. The main content area is titled 'Settings - Panel' and features a tabbed interface with 'Panel', 'Code', 'Date & Time', and 'Doorman Code'. The 'Panel' tab is active, showing a table of panel information. A 'Resend Configuration' button is located in the top right corner of the panel info section.

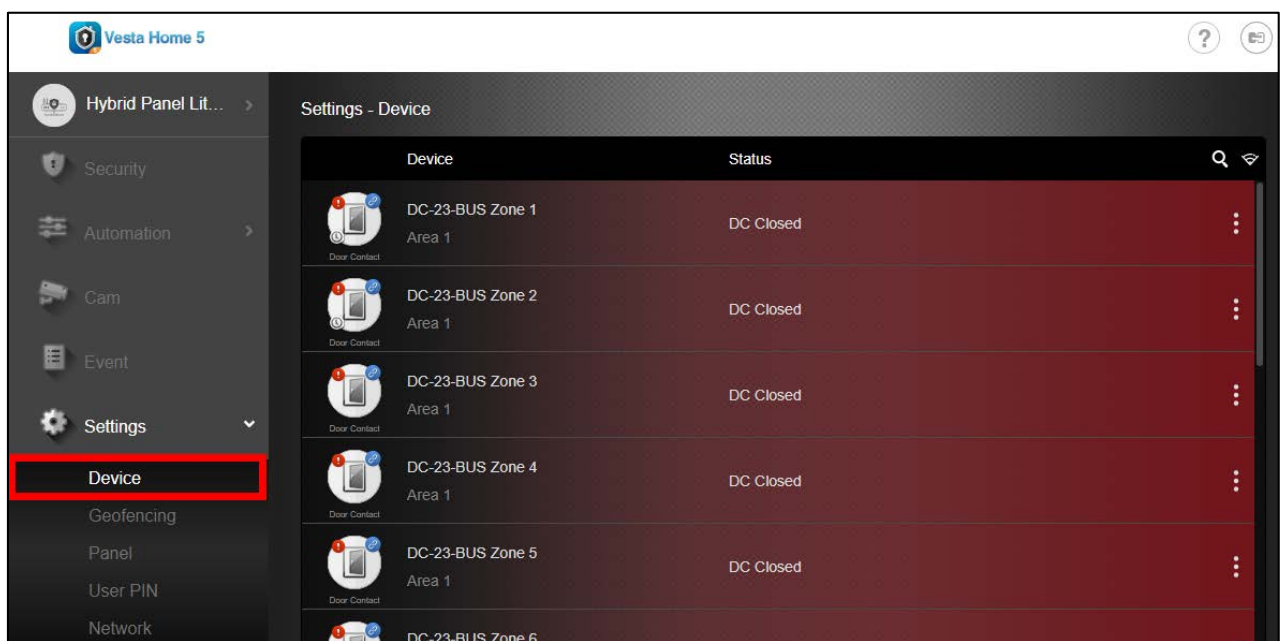
Panel Info			
Equipment Name	Hybrid Panel Lite Sample 1	Internal IP	10.16.4.16
Public IP	59.124.240.72	MAC Address	00:1d:94:1b:24:b3
Report Account	127038858419	Net Version	HYBRID 0.0.2.32_160
GSM Version	Quectel EC21EFAR06A06M4G	ZB Version	
RF Version	460800_BGST-U+TR-F1-BD_B...	IO MCU Version	FF-IO8_BL_A03_2023.09.21
Backup Battery Status	Off		

- 1 Click "Setting" to access Setting page, you will be prompted to enter code.
- 2 Enter the Control Panel's **Master Code** (Default: 1111), please check your panel's setting to acquire correct code.





4.6.1. Device


The Device setting subpage includes the following functions:

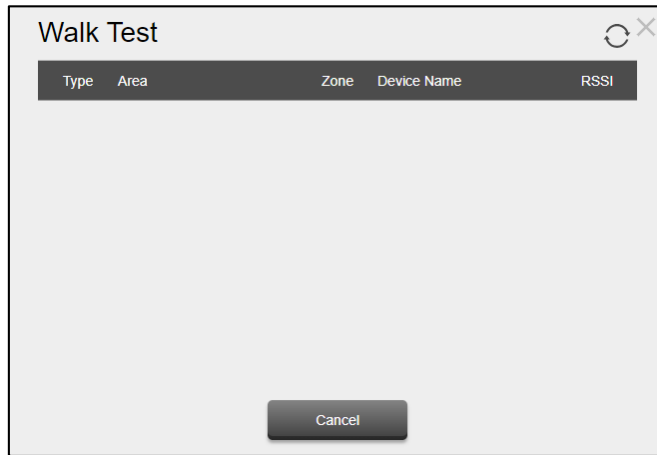


Click the corresponding icon to access different functions for level 2 user:

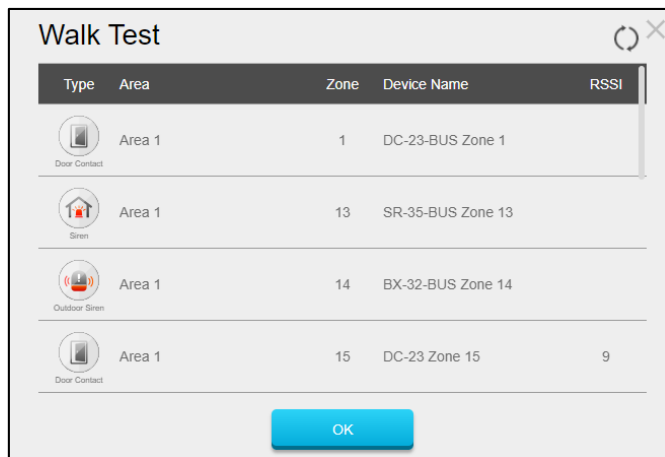


- Device Search  Users can directly search for the device they are seeking without scrolling through the entire list of devices.
- Walk Test 


Step 1. Click  icon to enter Walk Test mode.



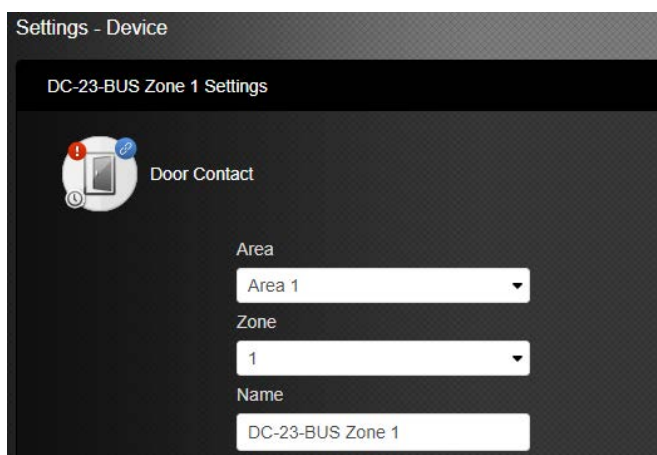
Step 2. Refer to device menu and press the test button to transmit a test signal for signal range test. When the signal is received, the webpage will be updated to show device info d. For wireless device, the signal strength in RSSI value will be displayed.



To Edit Device:

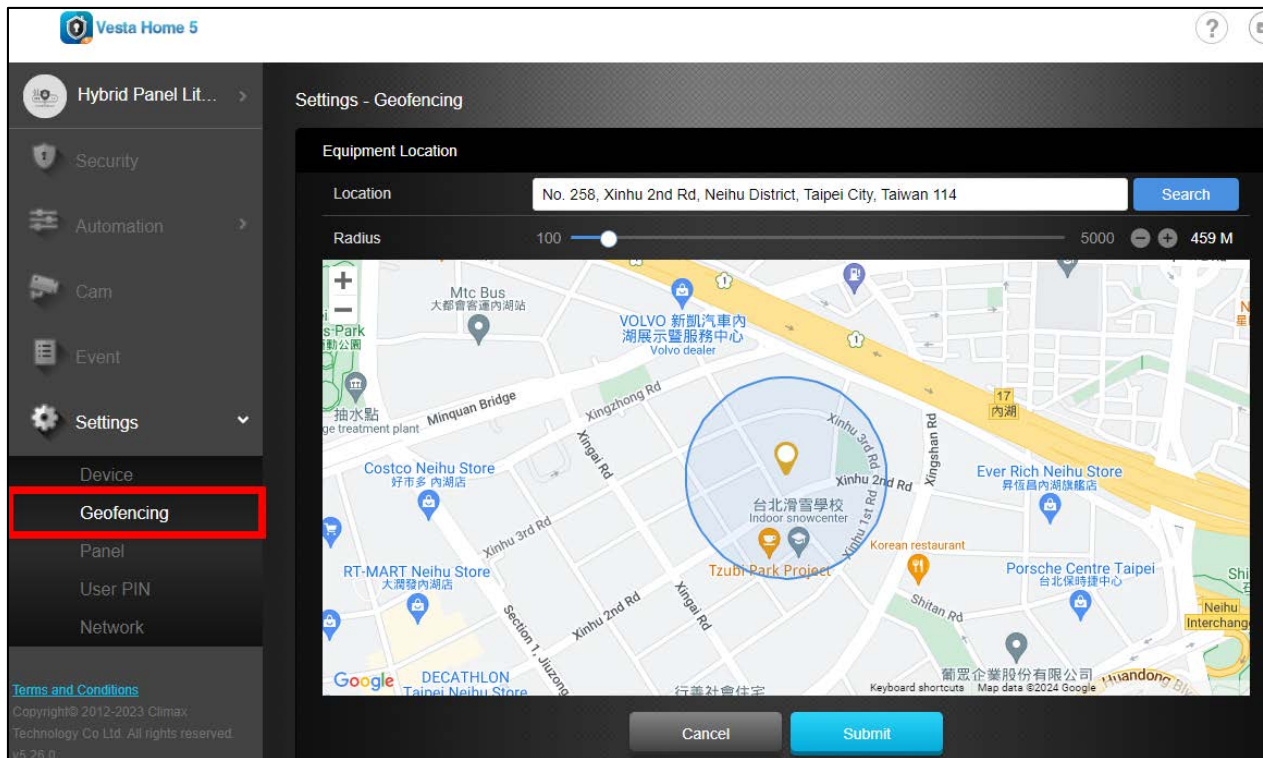
To edit the device, click the  icon at end of each device info column to enter Edit Device Page.

The master user (**Level 2 access**) can edit the Device Name, Area, and Zone number.



4.6.2. Geofencing

The Geofencing setting page allows users to set up a Geofence area. After Geofencing setup is complete, you can log in your smartphone application to enable the Smart Alert function.



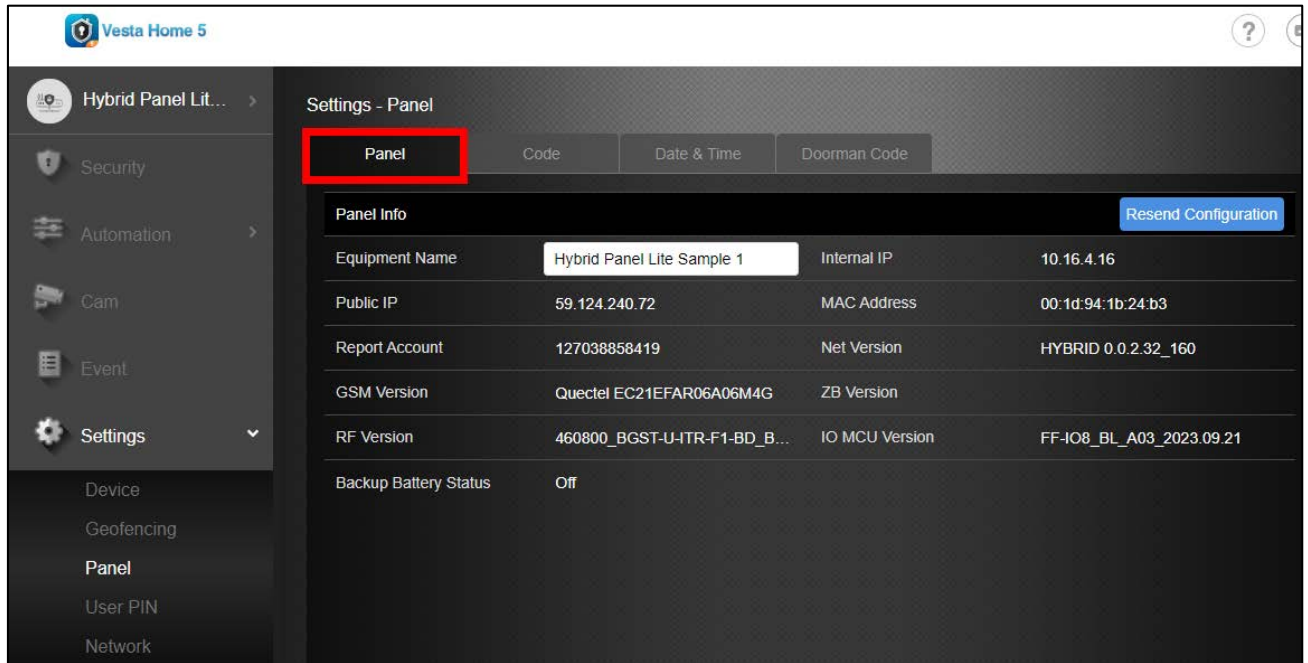
- **Equipment Location:** Enter the address of where the Control Panel is located and click the search icon.
- **Radius:** Users can slide the radius adjustment bar to adjust radius range between 100M to 5000M.
- Click **Submit** to complete the setup process. Users will need to re-log in for the new settings to take effect. After setup, users can log in their smartphone application to enable the Smart Alert function. When enabled, users can determine when to receive a push notification when the Geofence condition is met.

4.6.3. Panel

The Panel setting page provides access to Control Panel operation settings. In the **Panel** Section, level 2 user can program **Panel, Code, and Date and Time** settings.

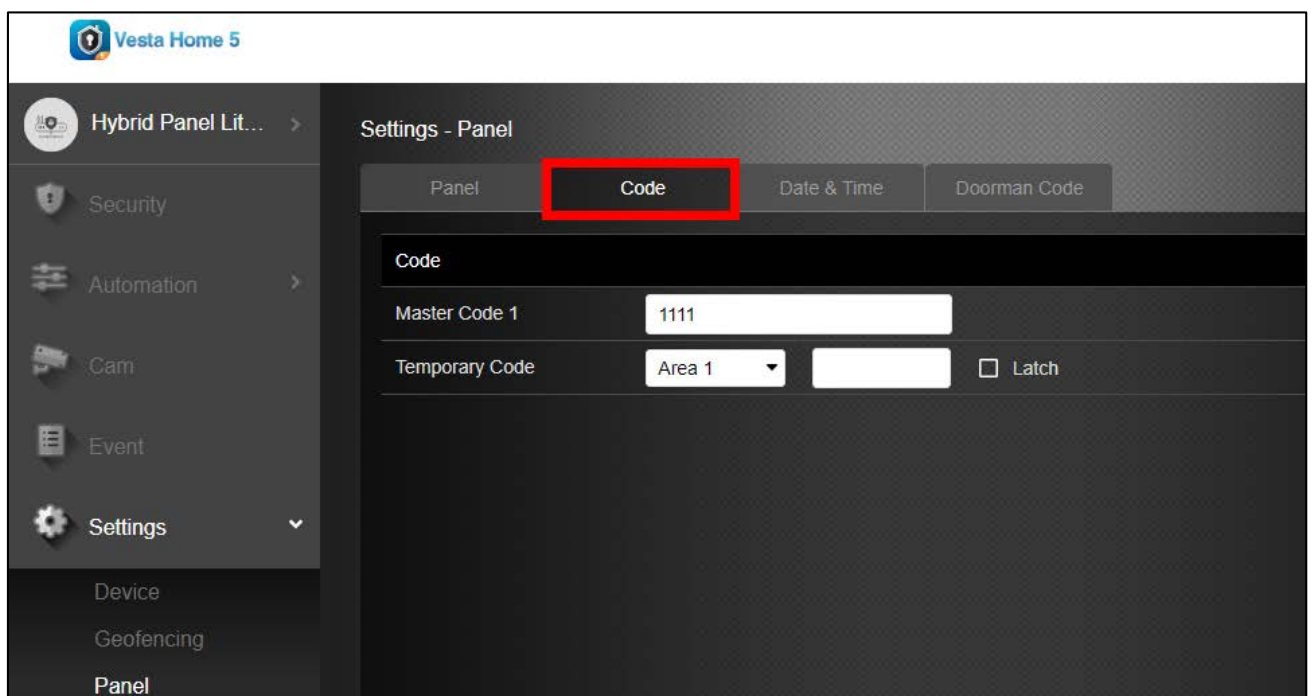
4.6.3.1 Panel

In the panel info page, the **level 2 user** is only allowed to edit the panel name.



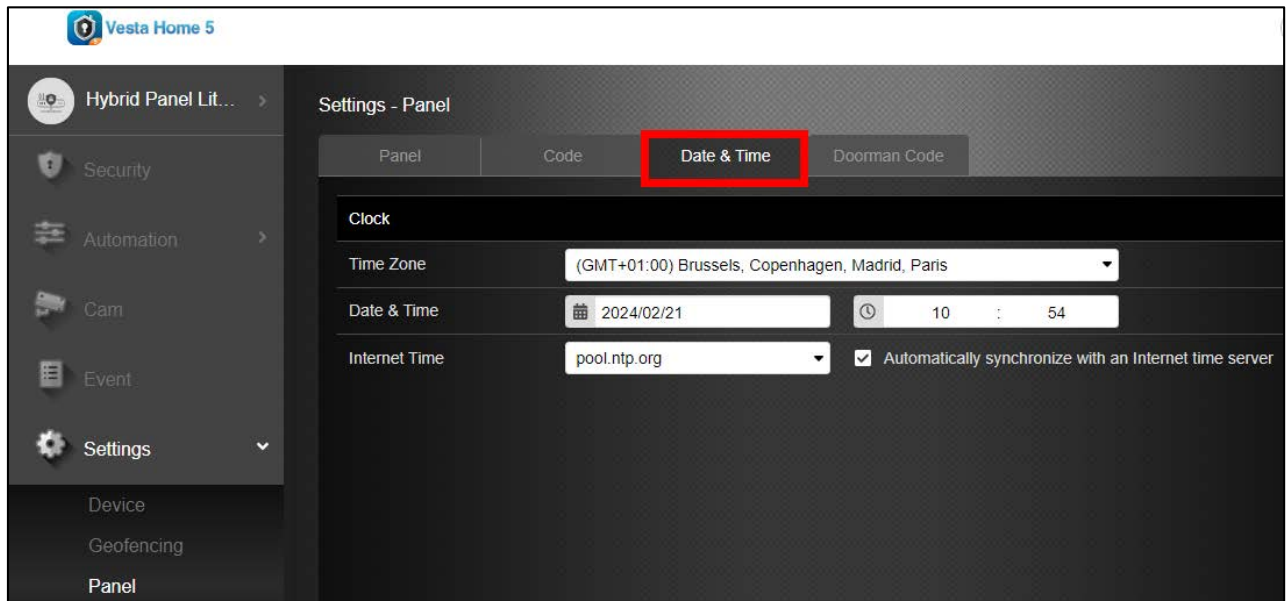
4.6.3.2 Code

The **Master User (Level 2 access)** is able to change his/her own Master Code, and set a Temporary Code for a temporary user.



4.6.3.3 Date and Time

Program the current **Date & Time** and set automatic synchronization with internet time server.



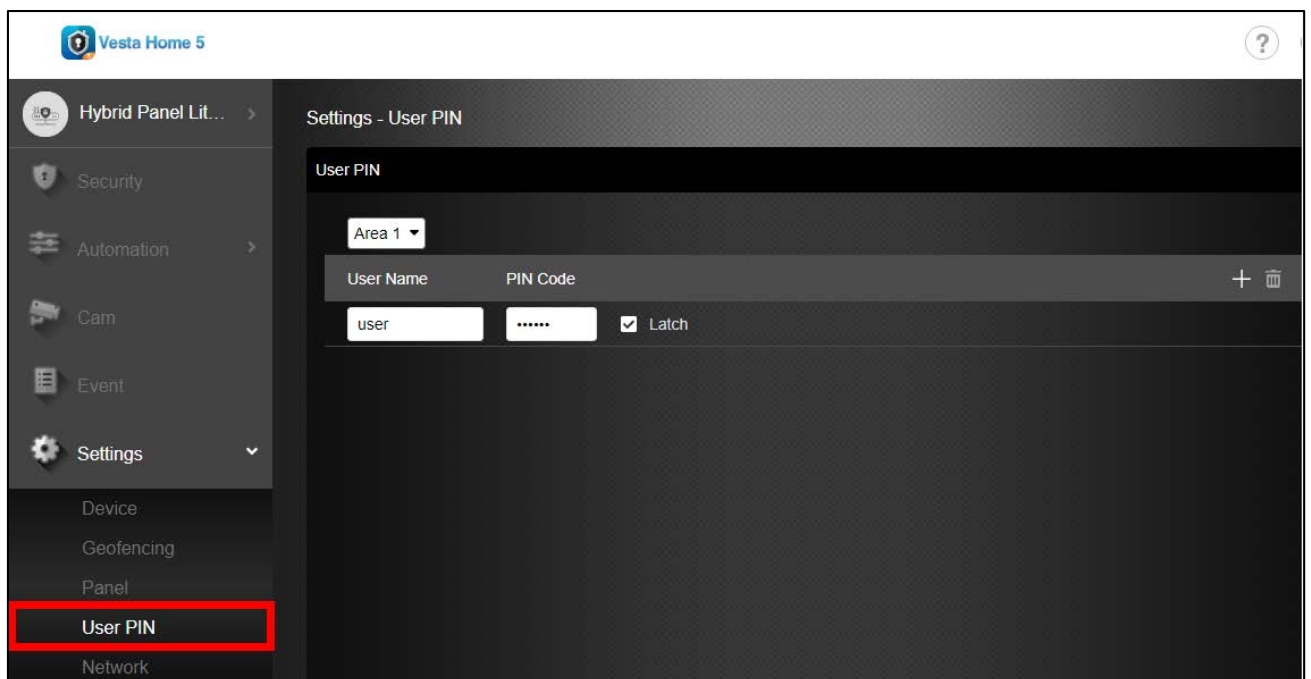
4.6.4. User PIN

The **Master User (Level 2 access)** is able to add User Codes for users to access the alarm system.

For **Area 1**, User PIN code #1 is activated with “**123456**” as factory default.

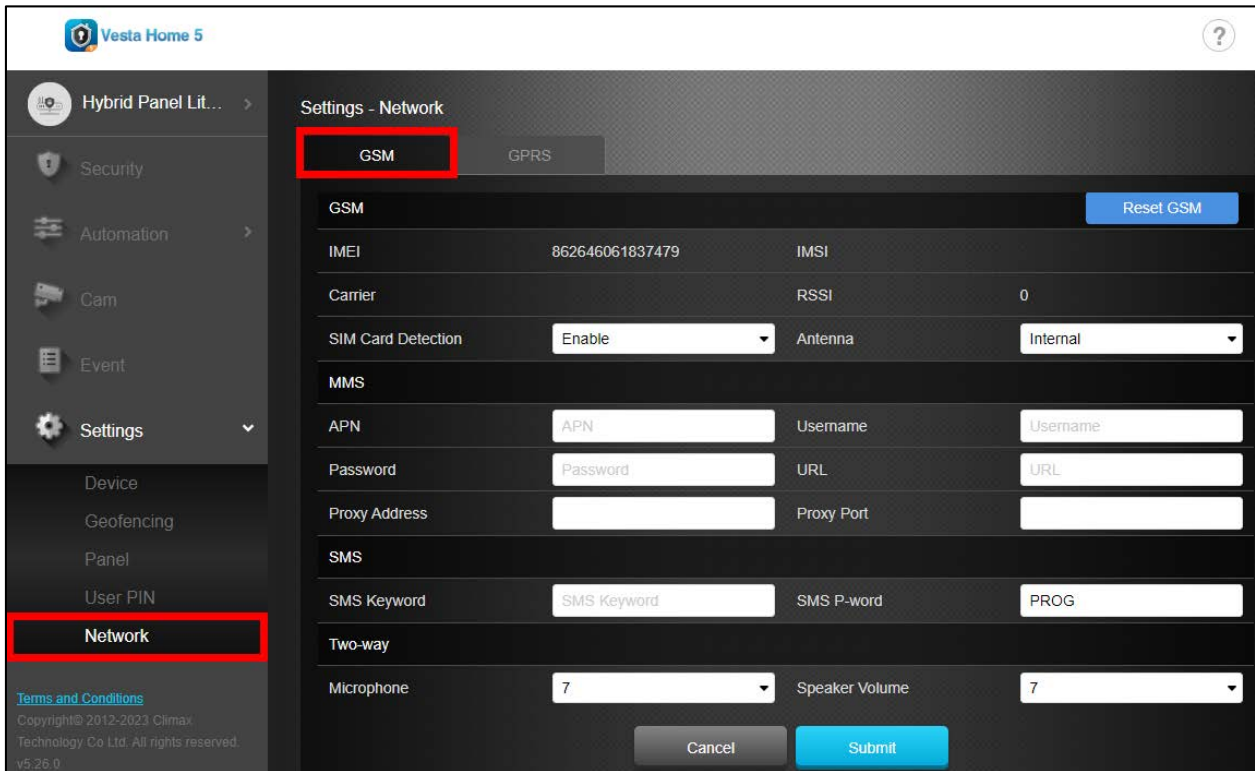
User PIN code #2 is activated with “**111111**” as factory default.

For **Area 2**, User PIN code #1 is activated with “**654321**” as factory default.

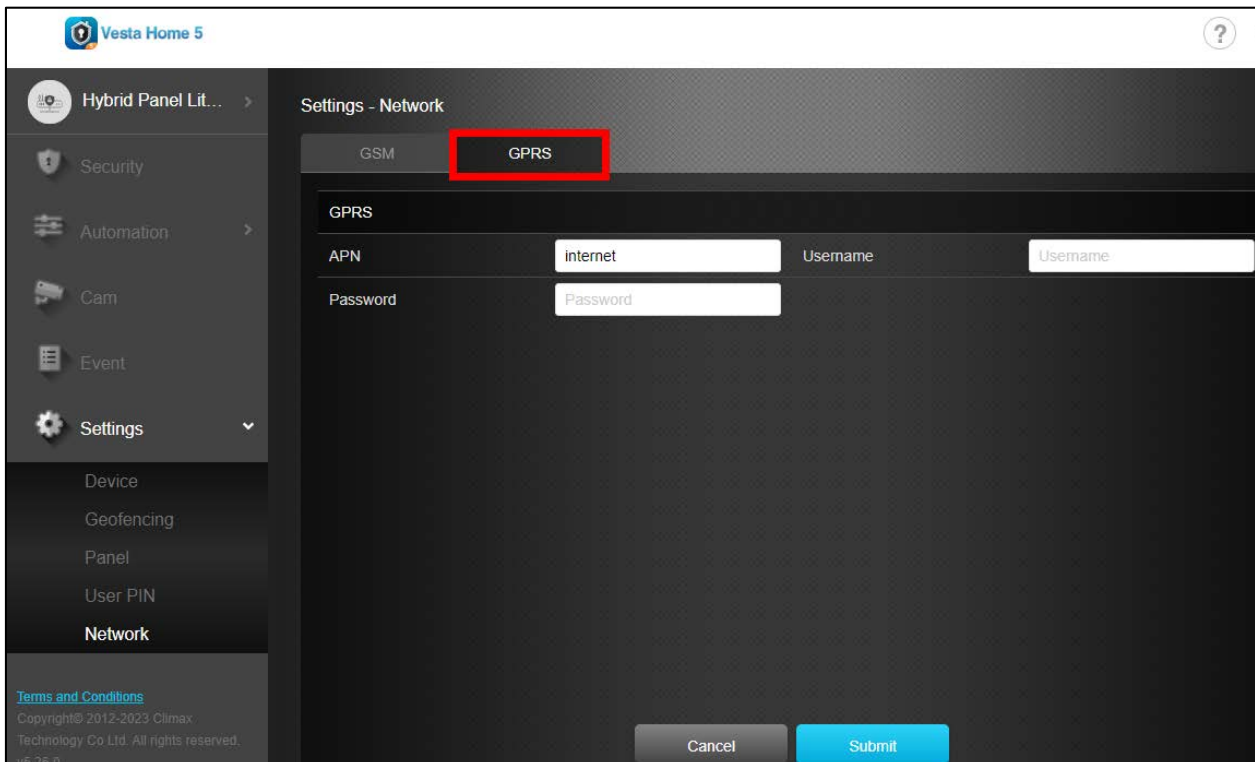


4.6.5. Network

The Network function allows **Master User** to program GSM and GRPS network.



The screenshot shows the 'Settings - Network' interface with the 'GSM' tab selected. The left sidebar contains a menu with 'Network' highlighted. The main content area displays GSM configuration fields: IMEI (862646061837479), Carrier, SIM Card Detection (Enable), APN, Password, Proxy Address, SMS Keyword, Two-way, Microphone (7), and a 'Reset GSM' button. There are also fields for IMSI, RSSI (0), Antenna (Internal), Username, URL, Proxy Port, and SMS P-word (PROG). 'Cancel' and 'Submit' buttons are at the bottom.



The screenshot shows the 'Settings - Network' interface with the 'GPRS' tab selected. The left sidebar contains a menu with 'Network' highlighted. The main content area displays GPRS configuration fields: APN (internet), Password, Username, and a 'Submit' button. There are also 'Cancel' and 'Submit' buttons at the bottom.

5. Level 3 Access

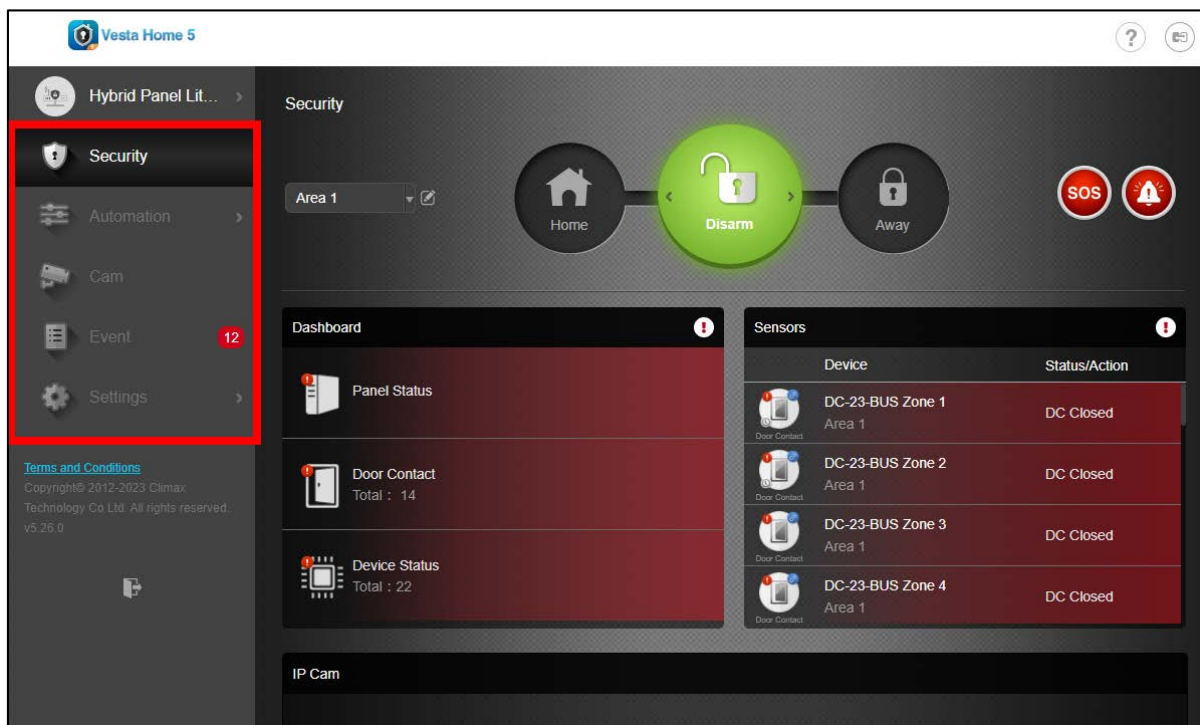
The **Installer Access (Level 3 access)** must be granted by level 2 user first to enable installer functions.

Connect to <https://eu.vestasmarthome.com> and log in with your registered username and password. Refer to the list of usernames and passwords provided in **4.1. Log In.**

Enter the **Installer Code** (default: **7982**) to access full programming functions.

As an Installer, you will be able to operate the alarm system and program panel settings for the user. Level 3 access includes the following functions:

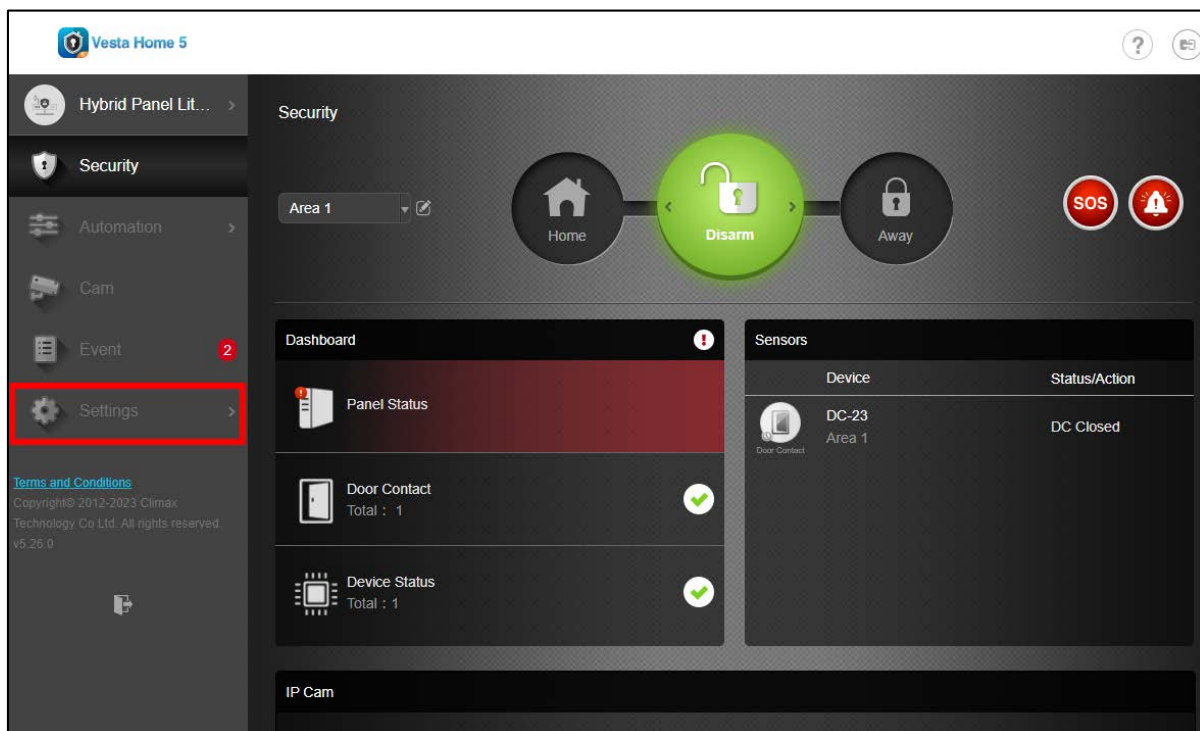
- **View current system mode and a list of security sensors/devices**
- **Arm/Disarm/Home arm**
- **Fault display**
- **Home Automation Setting**
- **Camera Viewing/Setting**
- **Event log**
- **Full Programming Functions**



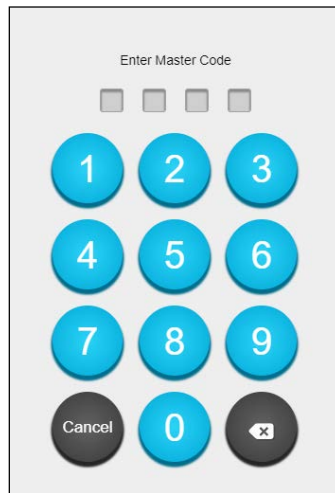
5.1 Setting

The **Installer user (Level 3 access)** can access full Setting page functions, including:

- **Device**
 - Clear Faults
 - Device Search
 - Device Learning
 - Device Exclusion
 - Walk Test
 - Refresh Device List
 - Delete Device
 - Full Device Configuration
- **Geofencing Setting**
- **System configurations**
- **PIN code setting:**
 - All Master Codes
 - Duress Code
 - Guard Code
 - Temporary Code
 - Individual Installer Code
- **Date and Time setting**
- **Factory Reset**
- **Wired Sensor Setting**
- **Network Setting**
- **Report Setting**

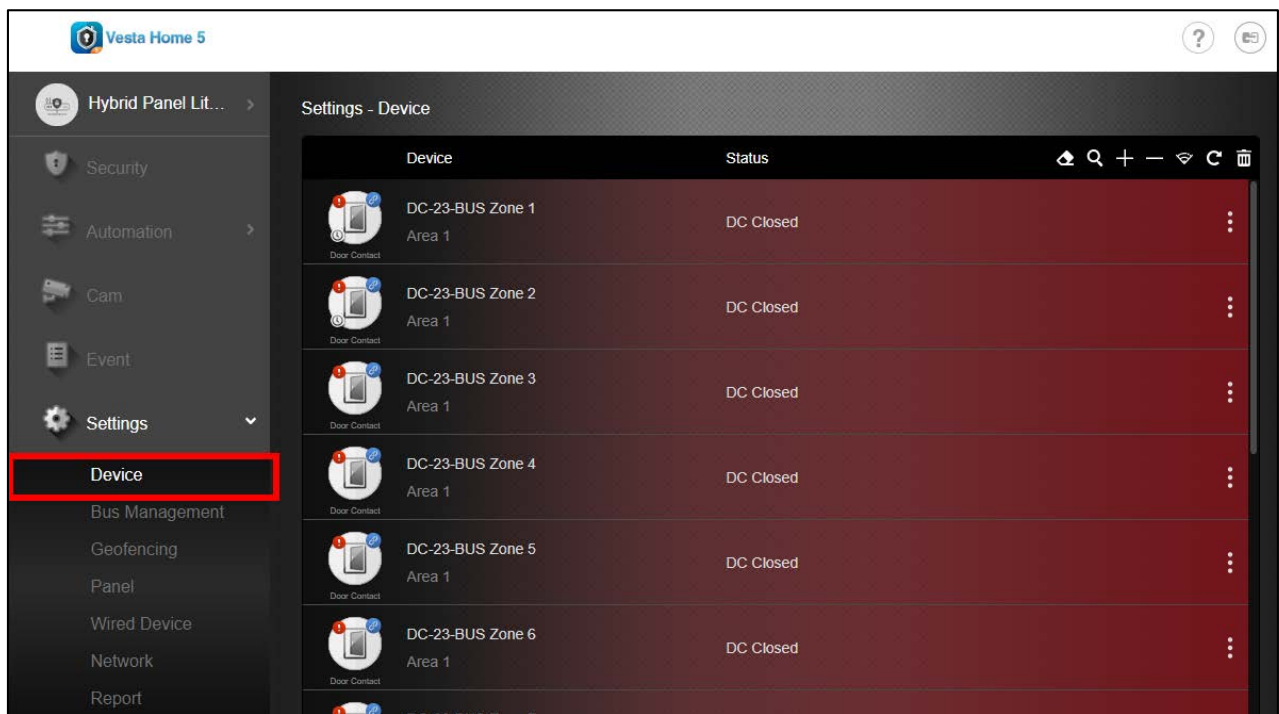


- 1 Click "Setting" to access Setting page, you will be prompted to enter code.
- 2 Entering the **Installer Code** (Default: **7982**) grants access to full setting functions.

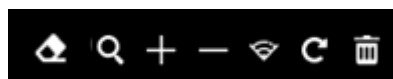


5.1.1 Device

The Device setting subpage includes the following functions:




Click the respective icon for different function setting (from left to right):




- Clear Faults 


Level 3 user (Installer) can click  icon to clear all device faults.


<NOTE>

 Force Arm is not allowed if there is device tamper fault. Device tamper fault can only be cleared by level 3 user in this page.

- Device Search 

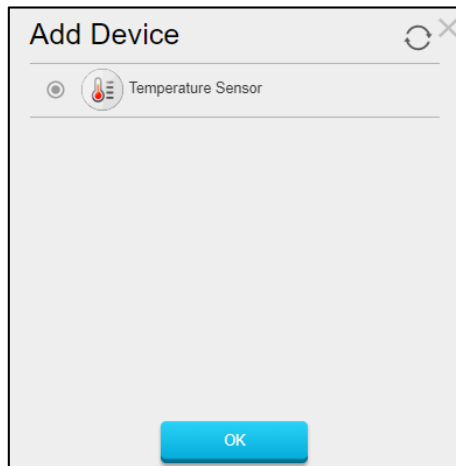
Users can directly search for the device they are seeking without scrolling through the entire list of devices.

- Device Learning 

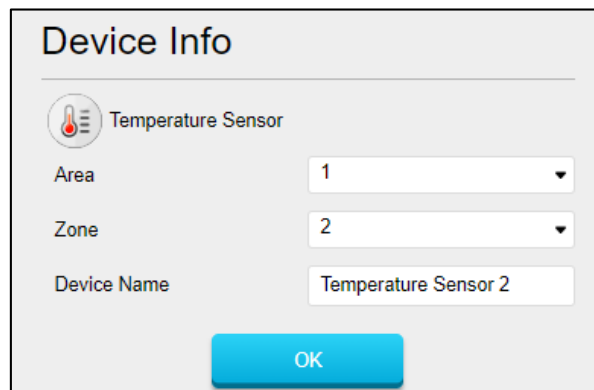
Step 1. Level 3 user (Installer) can click  icon to enter learning mode.


Step 2. Refer to accessory device manual to transmit learn signal from the device. When the panel receives learn signal, the webpage will display device info.

Step 3. Check the box in front of device info, then click OK to add the device into Control Panel.

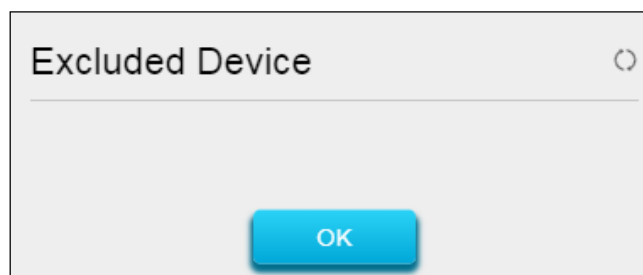


Step 4. After a new device has been learnt into the Control Panel, a Device Wizard will pop up, allowing users to edit area, zone, and device name.

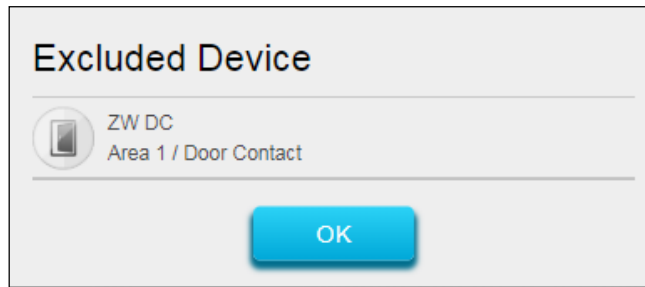


- Device Exclusion  (This function is NOT supported by Hybrid Panel Lite.)


Step 1. Level 3 user (Installer) can click  icon to enter removing Z-Wave device mode.




Step 2. Refer to the Z-Wave device manual to transmit signal. When the panel receives exclusion signal, the webpage will display device info.

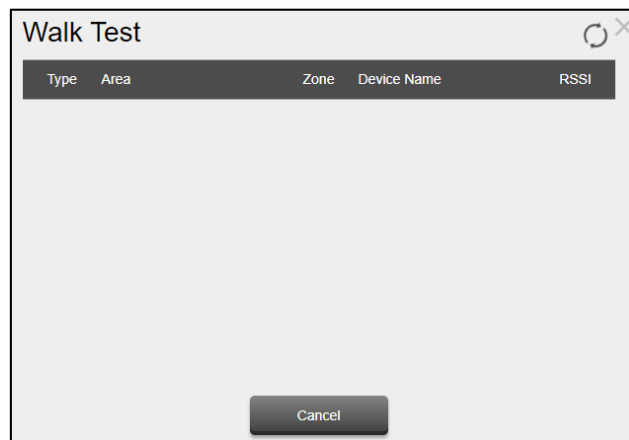


Step 3. Click OK to remove the Z-Wave device.

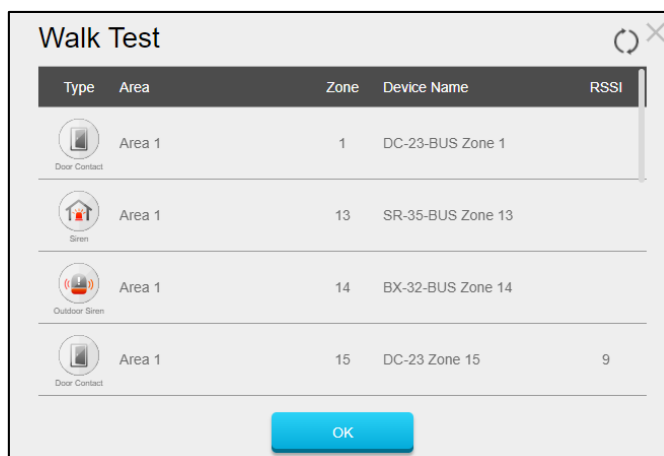
Step 4. Click  icon to refresh device list info. The Z-wave device is removed from the panel.

● Walk Test 

Step 1. Click  icon to enter Walk Test mode.



Step 2. Refer to device menu and press the test button to transmit a test signal for signal range test. When the signal is received, the webpage will be updated to show device info. For wireless device, the signal strength in RSSI value will be displayed.

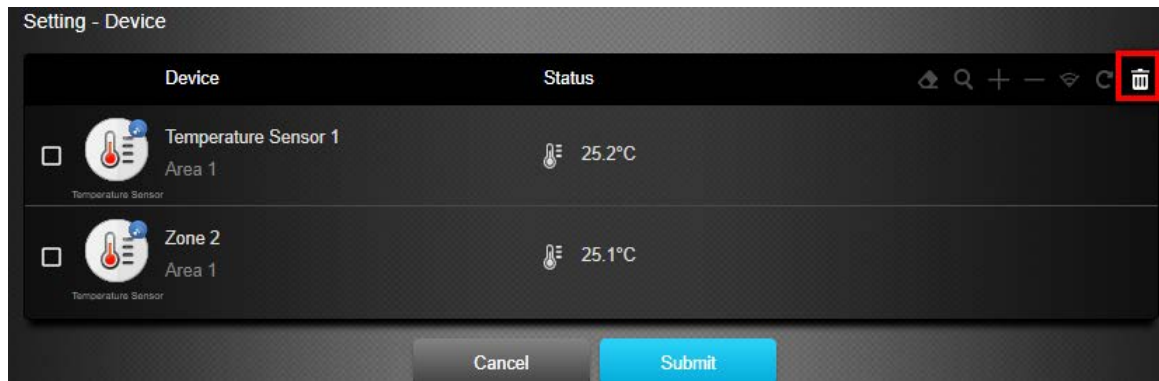


● Refresh Device List 

Level 3 user (Installer) can click  icon to refresh device list info.


● Delete Device

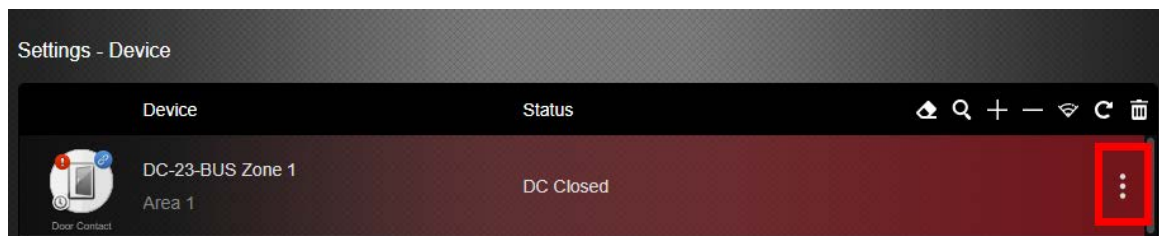
Step 1. Level 3 user (Installer) can click  icon to access delete device menu.



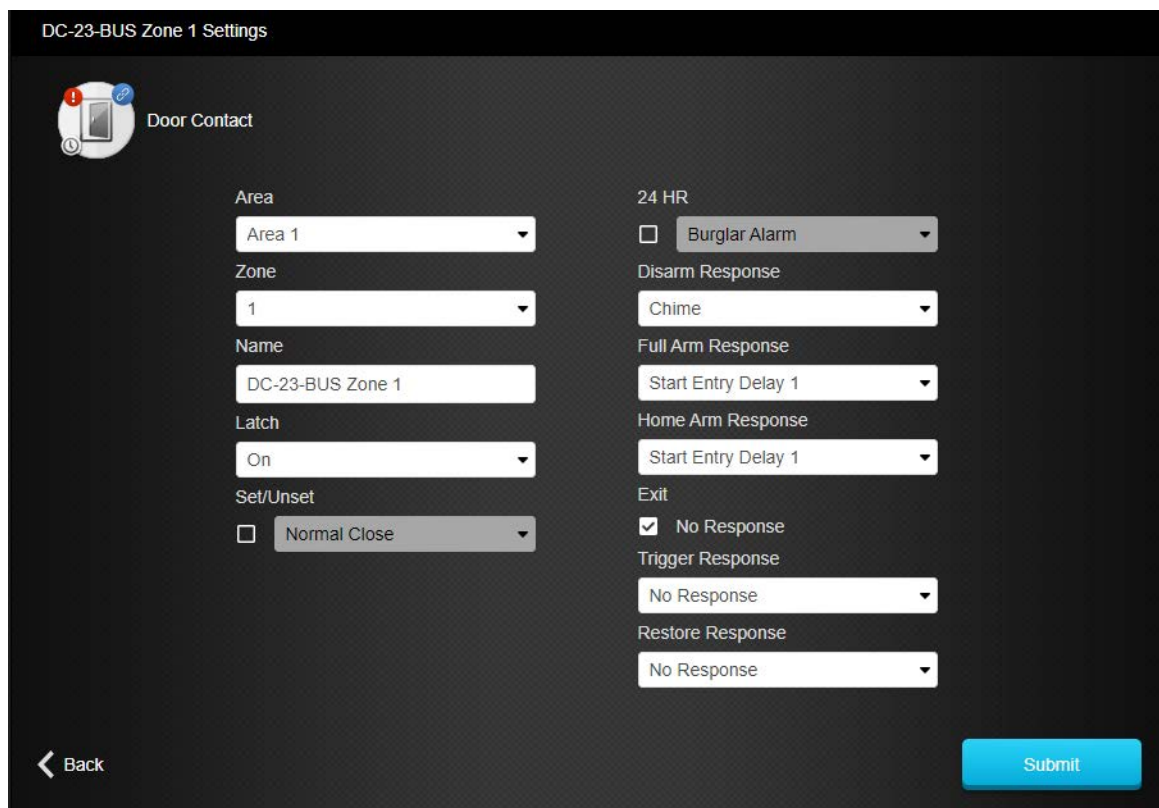
Step 2. Check the box at end of device column and click OK to remove selected devices from panel.

To Edit Device:

To edit the device, click the  icon at end of each device info column to enter Edit Device Page.



Level 3 user (Installer) can access full programming functions of each device.



- **Area:** Select Area.
- **Zone:** Select the Device zone number.
- **Name:** Enter a name for easy device recognition.

- **Latch Report** (Only for Remote Controller or Door Contact for use of Set/Unset attribute):

Latch Report ON = Whenever the system is armed, home armed or disarmed, the Control Panel will report the arm/disarm event by the particular device.

Latch Report OFF = Whenever the system is armed, home armed or disarmed, the Control Panel will NOT report the event. (**Selecting this option will make the Control Panel non-compliant to EN regulation**)
- **Set/Unset:** For Door Contact only. This function allows Door Contact to control system mode. (**Enabling this function will make the Control Panel non-compliant to EN regulation**)

Normal Close = The system will be armed when the Door Contact is opened, and disarmed when Door Contact is closed.

Normal Open = The system will be armed when the Door Contact is closed, and disarmed when Door Contact is open.
- **24H:** This function enables the sensor to activate selected alarm event whenever it is triggered regardless of system mode..

(**Enabling this function and selecting Burglar Alarm will make the Control Panel non-compliant to EN regulation**)

System Mode Attributes:

The System Mode Attributes determines system behavior under particular arming mode when the sensor is triggered.

No Response

- When a sensor with **No Response** is triggered, the Control Panel will not respond. (**Setting a sensor to No Response under any arm mode will make the Control Panel non-compliant to EN regulation**)

Start Entry Delay 1/ Start Entry Delay 2

- When the system is under Full Arm or Home Arm mode, if a sensor with **Start Entry Delay 1/2** attribute is triggered, Control Panel will start an entry countdown period to give enough time to disarm the system.
- When the Control Panel is in the Disarm mode, if a sensor with **Start Entry Delay 1/2** attribute is triggered, the Control Panel will immediately report a burglar interior alarm (**CID code: 132**).
- When the Control Panel is in the Full Arm mode, if a sensor with **Start Entry Delay 1/2** attribute is triggered, the Entry Delay 1/2 timer starts counting down. If no correct pin code is entered during the entry delay timer to disarm the system, the Control Panel will report a burglar perimeter alarm (**CID code:131**) immediately after entry delay timer 1/2 expires.
- When the Control Panel is in the Home Arm mode, if a sensor with **Start Entry Delay 1/2** attribute is triggered, the Entry Delay 1/2 timer starts counting down. If no correct pin code is entered during the entry delay period to disarm the system, the Control Panel will report a burglar interior alarm (**CID code: 132**) immediately after entry delay timer 1/2 expires.

Chime

- When the system is in Arm / Disarm / Home Arm mode, if a sensor set to Chime is triggered, the Control Panel will sound a Door Chime (Ding-Dong Sound).

Burglar Follow

- When the system is in Full Arm or Home Arm mode, if a sensor set to **Burglar Follow** is triggered, the Control Panel will report a burglar alarm immediately.
- When a Start Entry sensor is triggered and the system is under Entry Delay Timer countdown, if a sensor set to **Burglar Follow** is triggered, the Control Panel will wait until the Entry Delay Timer expires before activating a burglar alarm. If the system is disarmed before the timer expires, the Control Panel will not activate alarm.

☞ **Burglar Instant**

- When the system is under Full arm or Home Arm / Disarm / Entry Time mode, if a sensor set to **Burglar Instant** is triggered, the Control Panel will report a burglar alarm immediately.

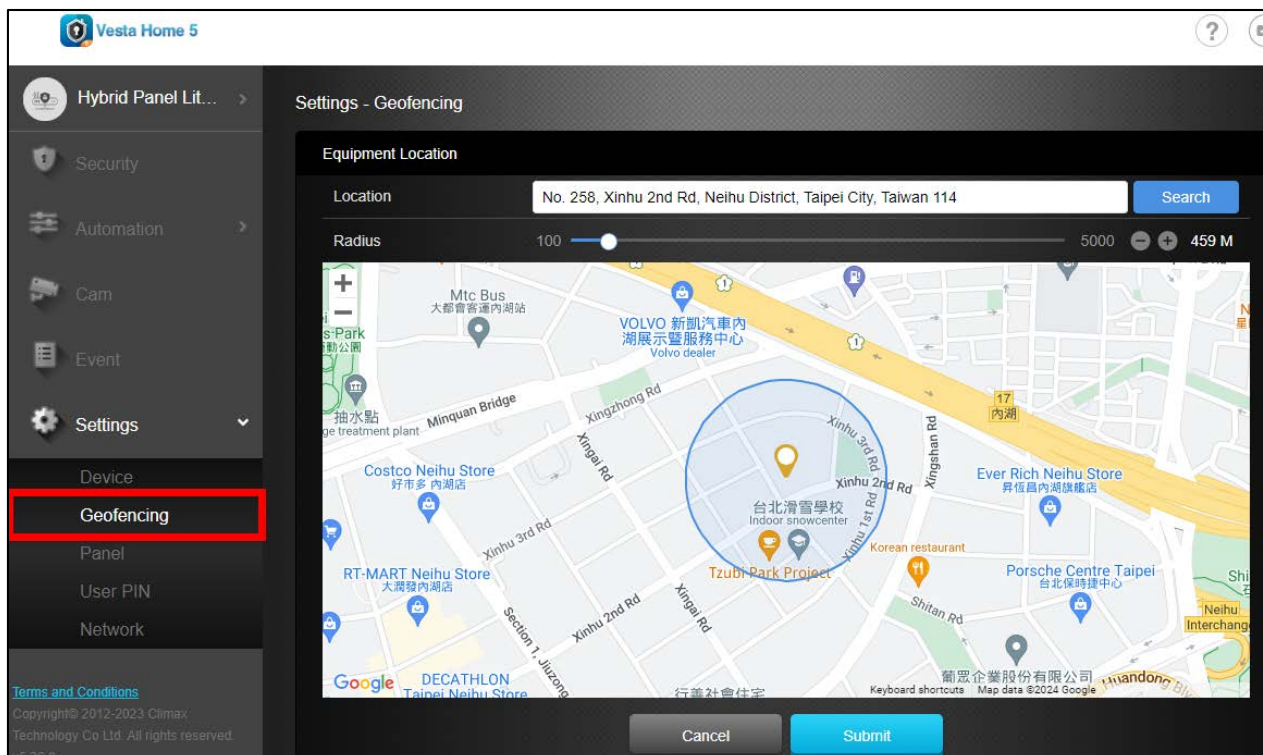
☞ **Burglar Outdoor**

- When the system is in Full Arm or Home Arm / Disarm // Entry Time mode, if a sensor set to **Burglar Outdoor** is triggered, the Control Panel will report a burglar outdoor event immediately.

- **Exit (No Response):** If checked, the panel will ignore trigger signal from this sensor during Exit Time countdown. If deselected, the panel will activate burglar alarm and report immediately when the sensor triggered during Exit Delay Timer.

5.1.2. Geofencing

The Geofencing setting page allows users to set up a Geofence area. After Geofencing setup is complete, you can log in your smartphone application to enable the Smart Alert function.



- **Equipment Location:** Enter the address of where the Control Panel is located and click the search icon.
- **Radius:** Users can slide the radius adjustment bar to adjust radius range between

100M to 5000M.

- Click **Submit** to complete the setup process. Users will need to re-log in for the new settings to take effect. After setup, users can log in their smartphone application to enable the Smart Alert function. When enabled, users can determine when to receive a push notification when the Geofence condition is met.

5.1.3. Panel

The Panel setting page provides access to Control Panel operation settings. In the **Panel** Section, the **level 3 user (Installer)** can program **Security, Panel, Code, Date and Time, and Factory Reset** settings.

5.1.3.1. Security

Program the Panel, Time and Sound Settings in this page.

The screenshot shows the 'Settings - Panel' page in the Vesta Home 5 application. The 'Security' tab is selected and highlighted with a red box. The 'Panel' option in the left sidebar is also highlighted with a red box. The main content area shows settings for Area 1, categorized into All Mode, Away, and Home. Each category has a table of settings with dropdown menus for values like Off, Full Arm, 2 hr(s), Disable, Low, High, Confirm, On, 3 min(s), and Disable. At the bottom, there are 'Cancel' and 'Submit' buttons.

All Mode

- **Area:** Select operation area to apply setting.
- **Final Door:** If set to **On**: When the system is Away Armed and under exit timer countdown, if an opened Door Contact set to Entry attribute is closed, the system will automatically arm the system even if the exit delay timer has not expired yet.
- **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.

<NOTE>

- ☞ Force Arm is not allowed if there is device tamper fault. Device tamper fault can only be cleared by level 3 user. (Please refer to **5.1.1 Device** for details.)
 - ✓ Direct Confirm: The system will be force armed directly without displaying fault message and report an event.
- **Tamper Alarm:** Select whether the siren should sound alarm when the tamper is triggered.
 - ✓ Full Arm: when tamper is triggered under Full arm mode, Control Panel raises a local alarm and sends report to the monitoring center. While under Home Arm 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.
- **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 for Fixed Device:** 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.
- **Alarm Length:** Set the duration the external siren should sound when an alarm is activated.
 - Available Options: 90 seconds, 2~15 minutes
 - Factory default is set to **3 minutes**.
- **Entry Delay 1/2 for Full Arm:** When a device set to “Start Entry Delay 1” or Start Entry “Delay 2” for Full Arm mode is triggered, The Control Panel will begin to countdown Entry Delay Timer according to duration programmed with this option. The system must be disarmed before the timer expires or an alarm will be activated.
 - Available Options: Disabled, 10, 20, 30, 45 seconds
 - Factory default is set to **10 seconds**.
- **Exit Delay for Full Arm:** When you change Control Panel mode to Full Arm, the Control Panel will begin to countdown Exit Delay Timer according to duration programmed with this option The system will enter your selected arm mode after the Exit Delay Timer expires, you need to leave the protected perimeter before the timer expires or you will activate an alarm by triggering sensors.
 - Available Options: Disabled, 10, 20, 30, 45 seconds
 - Factory default is set to **10 seconds**.
- **Entry Delay 1/2 for Home Arm:** When a device set to “Start Entry Delay 1” or Start Entry “Delay 2” for Home Arm 1/2/3 mode is triggered, The Control Panel will begin to countdown Entry Delay Timer according to duration programmed with this option. The system must be disarmed before the timer expires or an alarm will be activated.
 - Available Options: Disabled, 10, 20, 30, 45 seconds
 - Factory default is set to **10 seconds**.
- **Exit Delay for Home Arm:** When you change Control Panel mode to Home Arm 1/2/3, The Control Panel will begin to countdown Exit Delay Timer according to duration programmed with this option. The system will enter your selected arm mode after the Exit Delay Timer expires, you need to leave the protected perimeter before the timer expires or you will activate an alarm by triggering sensors.
 - Available Options: Disabled, 10, 20, 30, 45 seconds
 - Factory default is set to **10 seconds**.

5.1.3.2. Panel

Program the Panel Settings in this page.

The screenshot shows the 'Settings - Panel' page in the Vesta Home 5 interface. The 'Panel' tab is highlighted with a red box. The settings are organized into sections: Panel Settings, Program RF Siren, and Panel Info. The Panel Settings section includes dropdown menus for AC Fail Report (1 min), Jamming Report (1 min), Auto Check-in Interval (1 day), Auto Check-in Offset Period (1 hr), Outdoor IR Camera in Grayscale (Disable), and Power Supply Overcurrent Restart Time (3 min). The Program RF Siren section has two buttons: 'Siren Tamper On' and 'Siren Tamper Off'. The Panel Info section includes a 'Resend Configuration' button and a table of system information.

Equipment Name	Hybrid Panel Lite Sample 1	Internal IP	10.16.4.16
Public IP	59.124.240.72	MAC Address	00:1d:94:1b:24:b3
Report Account	127038858419	Net Version	HYBRID 0.0.2.32_160
GSM Version	Quectel EC21EFAR06A06M4G	ZB Version	
RF Version	460800_BGST-U-TR-F1-BD_B...	IO MCU Version	FF-IO8_BL_A03_2023.09.21
Backup Battery Status	Off		

Panel Setting

- **AC Fail Report:** Set the waiting time before Control Panel report to Central Monitoring Station when AC failure is detected.
 - Available Options: 1,3,5,10,15,20,30 minutes, 1 hour.
 - Factory default is set to **1 min**.
- **Auto Check-in Interval:** Set the interval waiting time between each report.
 - Available Options: 2,3,4,5,10,15,20,30 minutes, 1,2,3,4,6,8,12 hours, and 1 day.
 - Factory default is set to **1 day**.
- **Auto Check-in Offset Period:** This is to set the time delay before the first “Auto Check-in Report” report is made. For example, if “Offset” time period is set to 2 Hours, then the Control Panel will make the first “Auto Check-in Report” report after 2 hours.
 - Available Options: 2,3,4,5,10,15,20,30 minutes, 1,2,3,4,6,8,12 hours
 - Factory default is set to **1 hour**.
- **Bypass Ethernet Fault:** When **ON** is selected, the Control Panel will bypass connection fault when Ethernet cable unplugged status is detected.
 - Factory default is set to **OFF** .

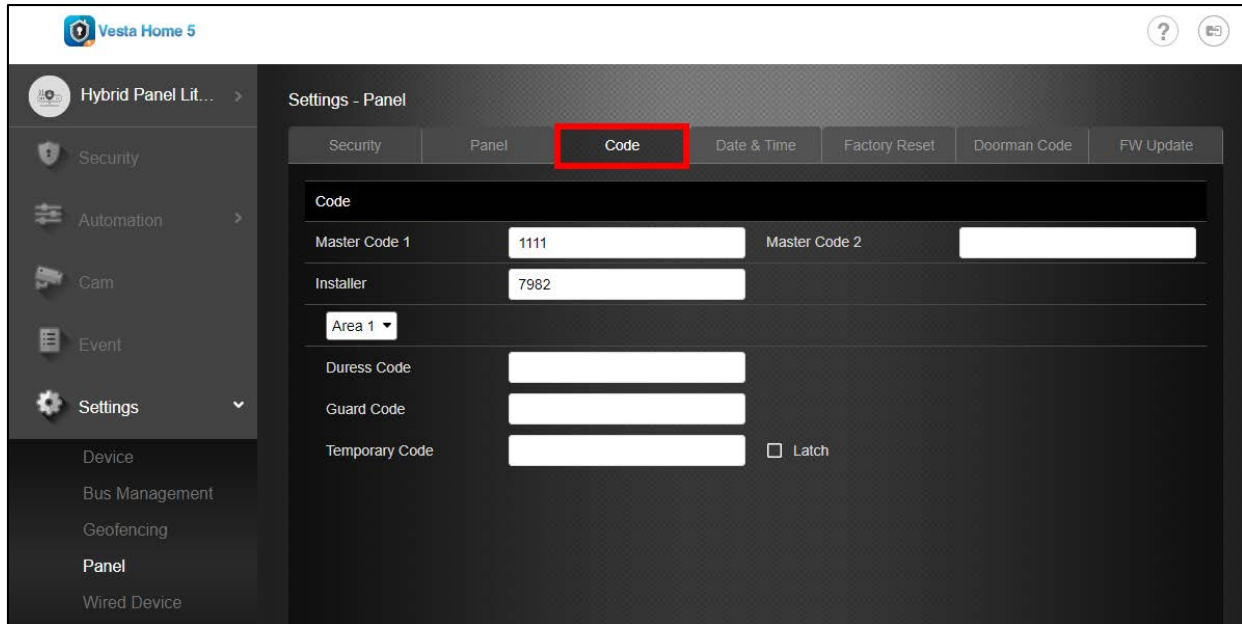
(This feature is not EN compliant)

Panel Setting

- The panel name can be edited in this page.

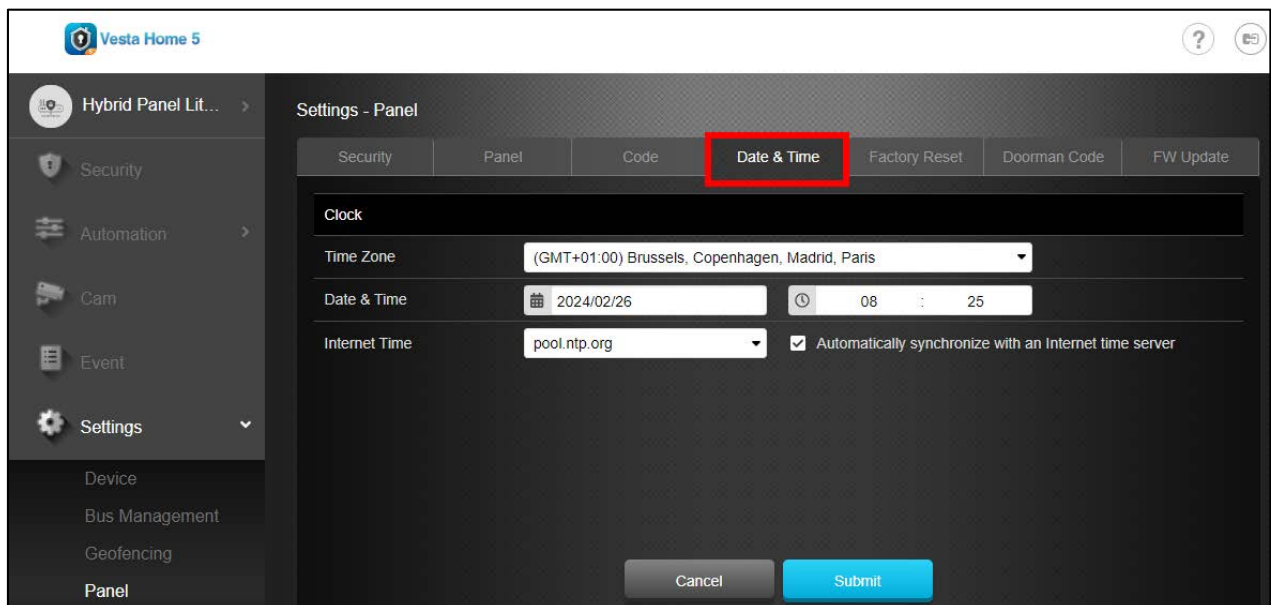
5.1.3.3. Code

The **Installer User (Level 3 access)** is able to program the Master Codes for all areas, change his/her own Installer Code, set a Duress Code for transmitting a secret & silence alarm, a Guard Code for security patrol personnel to arm/disarm the system, or a Temporary Code for a temporary user.



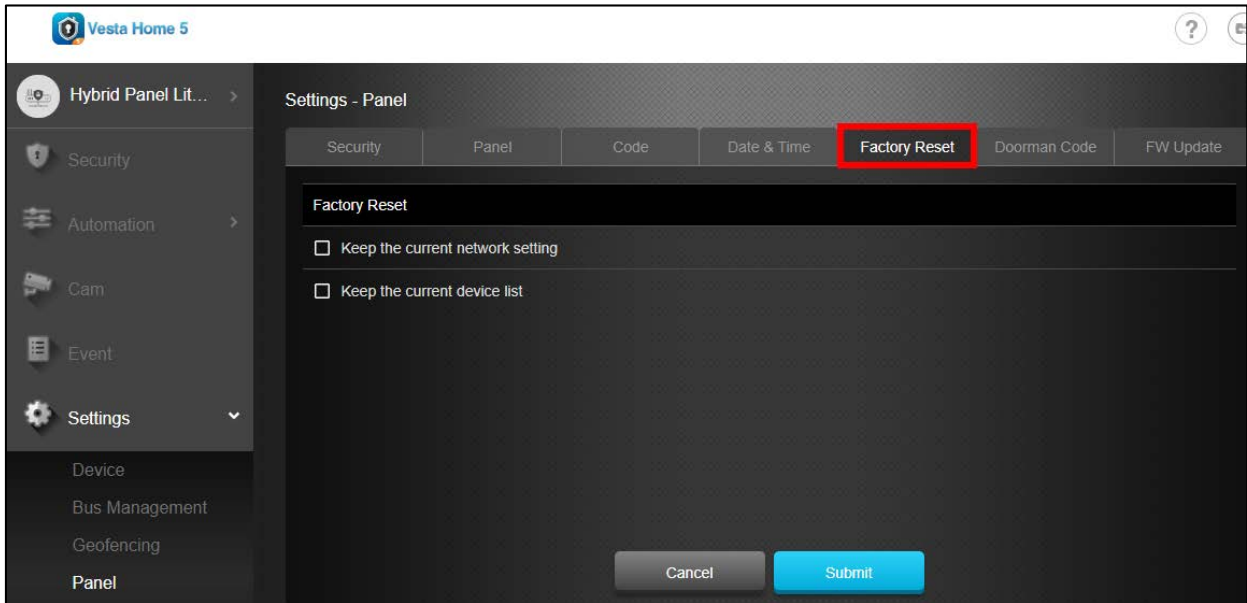
5.1.3.4. Date and Time

Program the current **Date & Time** and set automatic synchronization with internet time server.



5.1.3.5. Factory Reset

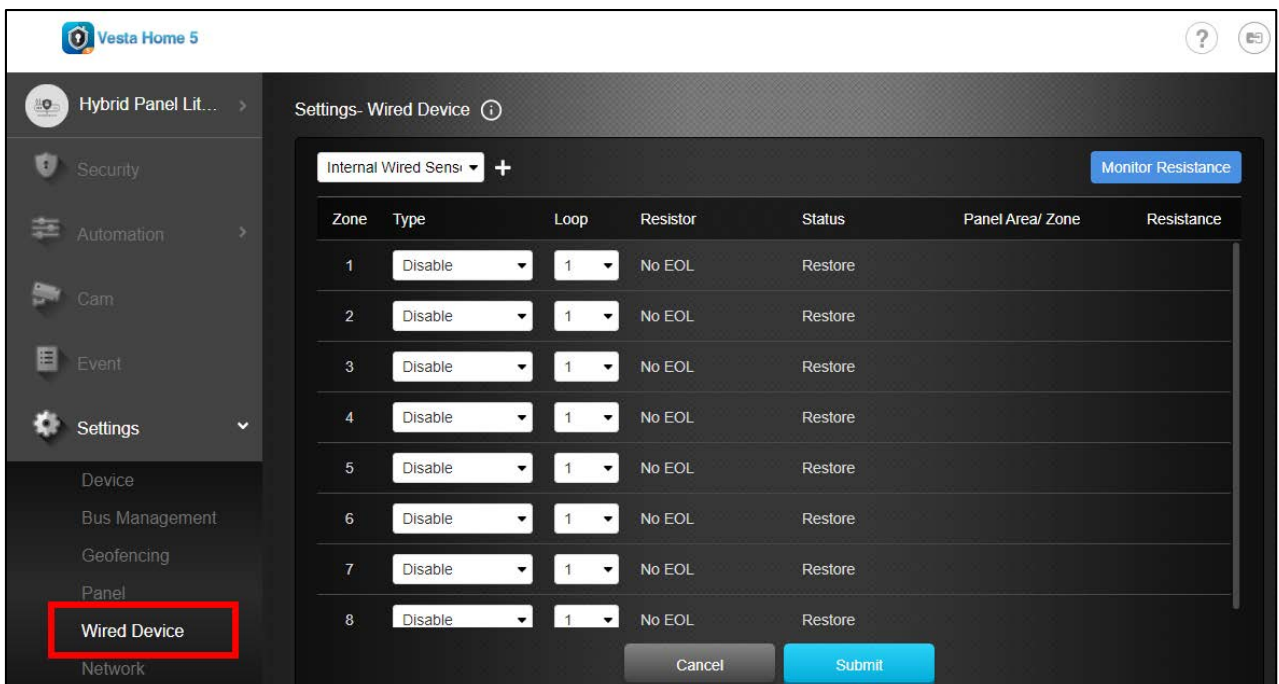
The **Installer User (Level 3 access)** is able to factory reset the Panel.



5.1.4. Wired Device

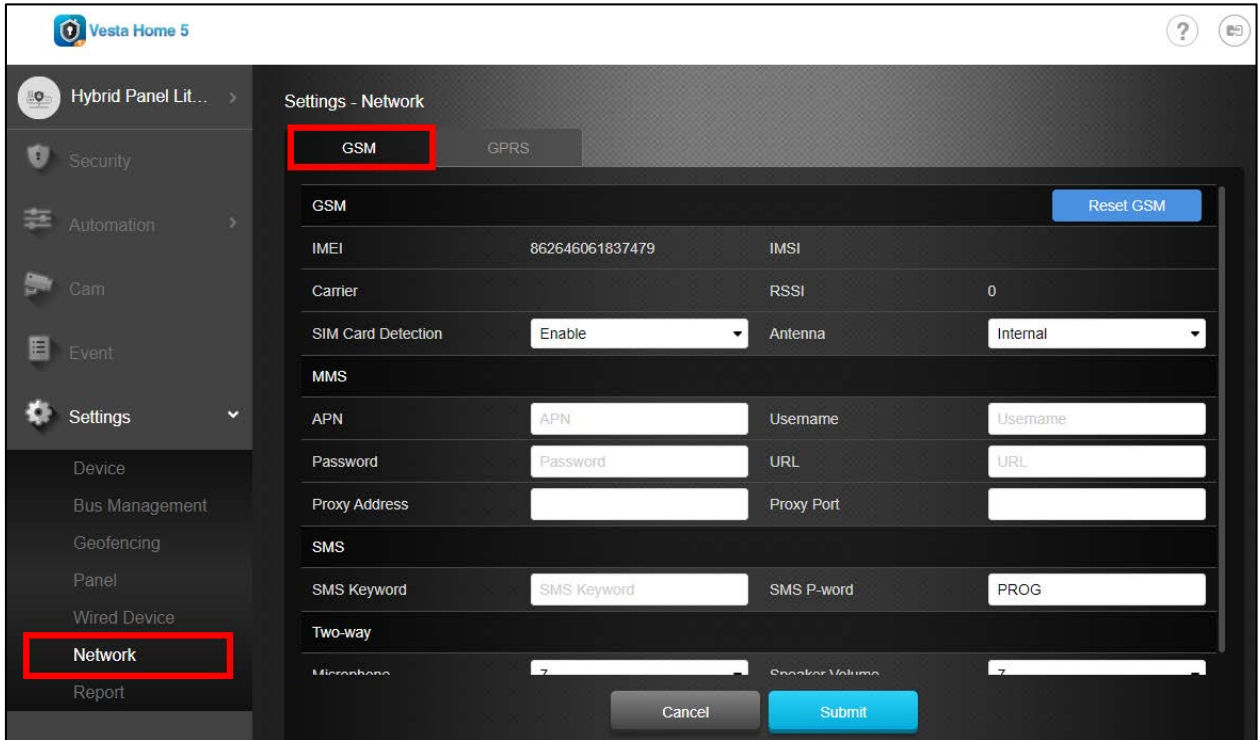
This page provides setting of wired sensor type, loop, and resistor to bind the sensor into hybrid panel. Once the binding is established, the corresponding panel area zone info will show up to the right of the sensor row.

You can also click “Monitor Resistance” to read the resistor value of each zone.

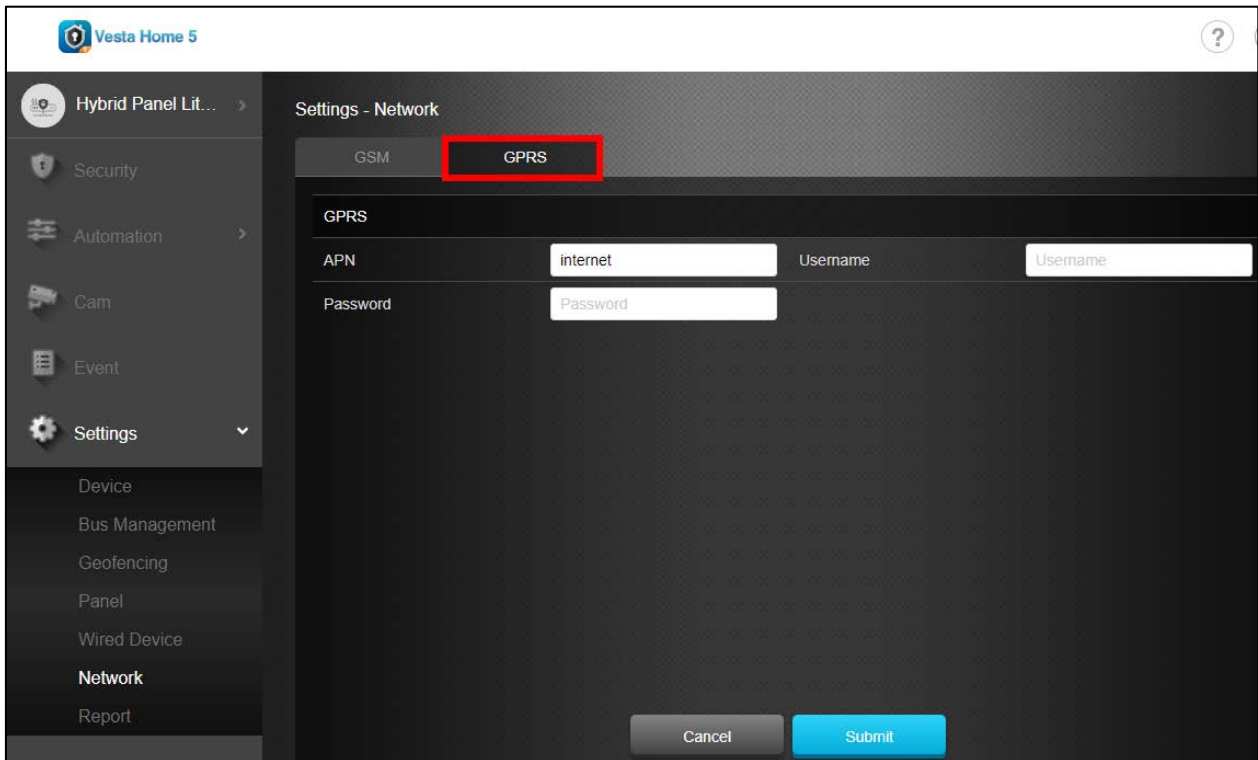


5.1.5. Network

The Network function allows **Installer User** to program GSM and GRPS network.



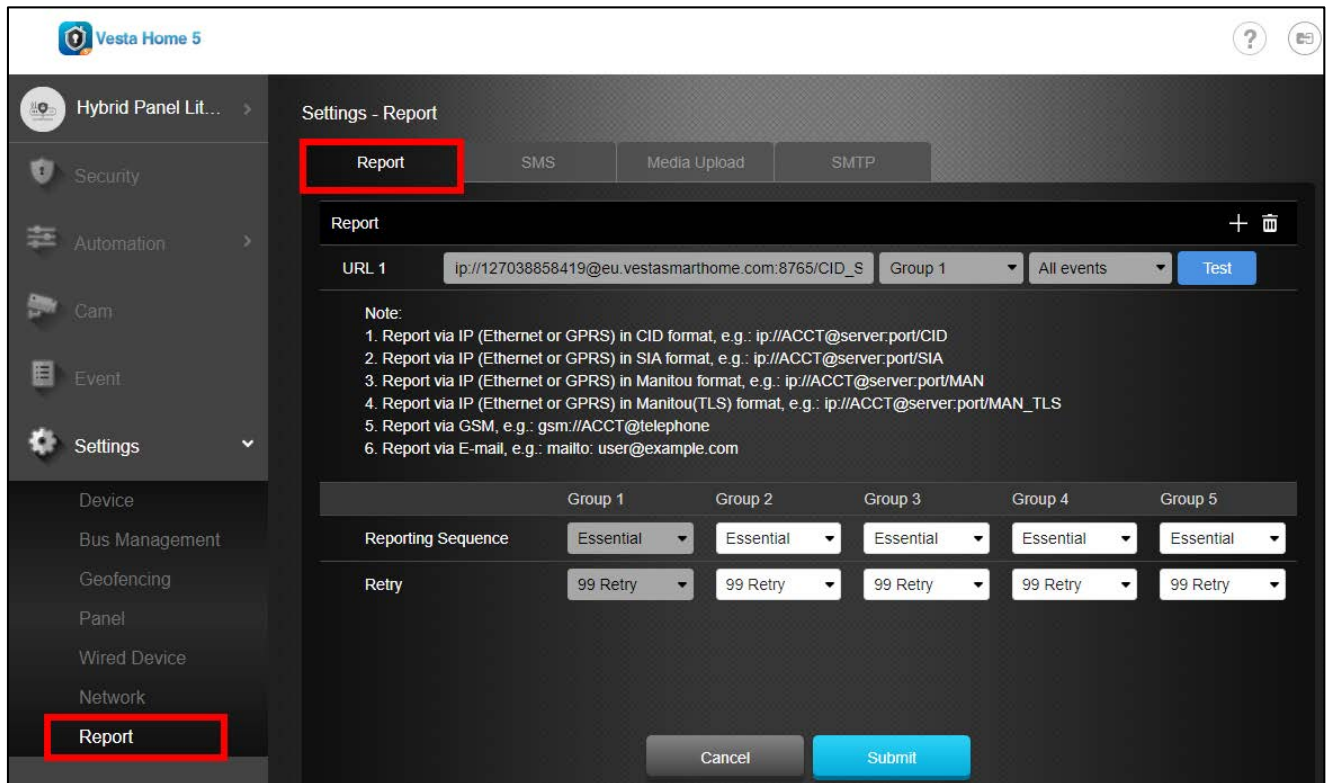
The screenshot shows the 'Settings - Network' interface with the 'GSM' tab selected. The left sidebar contains a menu with 'Network' highlighted. The main content area displays GSM settings including IMEI (862646061837479), Carrier, SIM Card Detection (Enable), Antenna (Internal), MMS (APN, Password, Username, URL, Proxy Address, Proxy Port), SMS (SMS Keyword, SMS P-word, PROG), and Two-way settings. A 'Reset GSM' button is visible in the top right of the GSM section. 'Cancel' and 'Submit' buttons are at the bottom.



The screenshot shows the 'Settings - Network' interface with the 'GPRS' tab selected. The left sidebar contains a menu with 'Network' highlighted. The main content area displays GPRS settings including APN (internet), Password, and Username. 'Cancel' and 'Submit' buttons are at the bottom.

5.1.6. Report

This is used for **Installer User (Level 3 access)** is to program / set all requirements for reporting purposes.



Report

- URL: This is used for installer to program report destinations.
- Climax CID protocol via IP
Format: ip://(Account Number)@(server ip):(port)/CID
Example: ip://1234@54.183.182.247:8080/CID
- SIA DC-09 protocol via IP
Format: ip://(Account Number)@(server ip):(port)/SIA
Example: ip://1234@54.183.182.247:8080/SIA
- SIA DC-09 protocol via IP with AES encryption
Format: ip://(Account Number)@(server ip):(port)/SIA/KEY/(128,196 or 256 bits Key)
Example:
ip://1234@54.183.182.247:8080/SIA/KEY/ 4A46321737F890F654D632103F86B4F3
- SIA DC-09 protocol using CID event code via IP
Format: ip://(Account Number)@(server ip):(port)/CID_SIA
Example: ip://1234@54.183.182.247:8080/CID_SIA
- SIA DC-09 protocol using CID event code via IP, with HEX encryption.
Format: ip://(Account Number)@(server ip):(port)/CID_SIA/KEY/(HEX)
Example:

ip://1234@54.183.182.247:8080/CID_SIA/KEY/4A46321737F890F654D632103F86B4
F3

- CSV protocol via IP

Format: ip//(Account Number)@(server ip):(port)/CSV

Example: ip://1234@54.183.182.247:8080/CSV

- CSV protocol via IP including username and password

Format: ip//(Account Number)@(server ip):(port)/CSV/User/Password

Example: ip://1234@54.183.182.247:8080/CSV/abcd/1357

- CID protocol via GSM

Format: gsm://(Account Number)@(telephone number)

Example: gsm://1234@0987654321

- Email

Format: mailto:user@example.com

Example: <mailto:john@gmail.com>

<NOTE>

- When the panel is registered into Climax's Home Portal Server, URL1 will be filled in with Home Portal Server report information. Do not change the information once registration is complete or reporting to Home Portal Server may encounter error.
- After registering the panel in Home Portal Server, if you wish to set more reporting destination, the new report destination should be set to different group than URL1 otherwise it may not be able to receive report successfully.

To add a reporting destination, click .

- **Reporting Sequence:** Select a group for your report destination The system will make report according to the following principle:

- ☞ Group with higher priority will be reported first: Ex: Group 1 → Group 2 → Group 3....
- ☞ If reporting to the first destination in a group fails, the system will move on to the next report destination in the group.
- ☞ If reporting to one of the report destinations in a group is successful, the system will consider reporting to this group successful and stop reporting to rest of the destinations in the group. It will then move on to report to the next group.
- ☞ If reporting to all destinations in a group fails, the system will retry report to group according to retry times set below. If reporting is still unsuccessful after retries, the system will move on to report the the next group according to Essential/Optional setting below.
- ☞ After completing a round of reporting (From Group 1 → Group 2 →Group5), If there is any group set as Essential which has not received report successfully, the system will restart the reporting cycle to retry reporting until every group set as Essential is reported successfully.
- ☞ Essential/Optional

Essential: the system will report to all groups set as **Essential**. The system will never give up trying to report to any group set as Essential until at least one of the destinations in every Essential group successfully receives the report. Group 1

is always set as **Essential** and cannot be changed.

Optional: The system will only report to group set as **Optional** when reporting to its previous group fails. For example: if Group 3 is set is optional, the Control Panel will only report to Group 3 if reporting to Group 2 fails.

- **Retry:** If reporting to all destinations in a group fails, the system will retry reporting to the group according to the retries times set here.

6. IP/GSM reporting

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

Depend on different models; the Control Panel is capable of reporting events to multiple report destinations via either or both Ethernet and GSM/GPRS network. 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/GPRS network; if the GSM/GPRS network loses connection, the events will be reported via Ethernet. Fault event for unavailable reporting path will be logged and reported within 3 minutes, if both Ethernet and GSM/GPRS network are unavailable, the Home Portal Server 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 instructions below to test your alarm system to make sure it can report to your programmed reporting destination successfully.

● IP Reporting Test

- Step 1.** Make sure the Control Panel has programmed an IP reporting destination (Please refer to **5.1.6 Report**)
- Step 2.** Make sure the Control Panel has a valid internet connection, and does not have a SIM card inserted, so that the only reporting route is through IP.
- Step 3.** Learn-in a Remote Controller into the Control Panel.
- Step 4.** Trigger a Panic Alarm with the Remote Controller. (Please refer to Remote Controller manual for detail)
- Step 5.** Do not disarm the system to stop the alarm event, and wait for 2~3 minutes.
- Step 6.** Check Reported Event page to see whether the triggered alarm is reported successfully. (see **4.5. Event** for detail)

If reporting is unsuccessful, please check the following:

- ✓ Check your report destination setting under Report Setting page, make sure the report destination format and information is correct.
- ✓ Check your internet connection to make sure the panel internet connection is normal.

● GSM/GPRS Reporting Test

- Step 1.** Make sure the Control Panel has programmed a GSM/GPRS reporting destination (Please refer to **5.1.6 Report** for detail)
- Step 2.** Make sure the Control Panel has a working SIM Card inserted, and does not have an Ethernet connection, so that the only reporting route is through GSM/GPRS.
- Step 3.** Learn-in a Remote Controller into the Control Panel.
- Step 4.** Trigger a Panic Alarm with the Remote Controller. (Please refer to Remote Controller manual for detail)

Step 5. Do not disarm the system to stop the alarm event, and wait for 2~3 minutes.

Step 6. Check Reported Event page to see whether the triggered alarm is reported successfully. (See **4.5. Event** for detail)

If reporting is unsuccessful, please check the following:

- ✓ Check your report destination setting under Report Setting page, make sure the report destination format and information is correct.
- ✓ Check your SIM card status under the GSM page.
 1. Make sure SIM card PIN code is already disabled.
 2. For GPRS reporting, Confirm with your SIM card provider that the GPRS APN settings are correct.
 3. If GSM signal is low, change panel mounted location, or SIM card provider.

7. Appendix

Appendix A: Event Code

- **100 – Medical**
- **101 – Emergency**
 - ◆ When device set to Emergency Alarm is activated.
- **102 – Inactive**
- **110 – Fire**
 - ◆ When device set to Fire Alarm is activated.
- **111 – Smoke**
 - ◆ When device set to Smoke Alarm is activated
- **114 – Heat**
 - ◆ When device set to Heat Alarm is activated.
- **120 – Panic**
 - ◆ When device set to Panic Alarm is activated.
- **121 – Duress**
 - ◆ When the Duress Code is entered to disarm or arm the system.
- **122 – Silent Panic**
 - ◆ When a device set as Silent Panic is pressed.
- **130 – Burglar**
 - ◆ When a device is set as **Burglar** alarm or **Burglar Instant** is triggered.
 - ◆ When a device set as **Burglar Follow** is triggered.
- **131 – Burglar Perimeter**
 - ◆ When a device set as **Start Entry Delay** is triggered in Full Arm mode and Entry Delay Timer expires without disarming the system.
- **132 – Burglar Interior**
 - ◆ When a device set at **Start Entry Delay** is triggered in Home Arm mode and Entry Delay Timer expires without disarming the system.
- **136 – Burglar Outdoor**
 - ◆ When any device set at **Burglar Outdoor** is triggered.
- **137 – Panel Tamper/ Panel Tamper Restore**
 - ◆ When the panel's tamper protection is triggered.
 - ◆ When the panel's tamper protection is restored.
- **147 – Sensor Supervision Failure/ Sensor Supervision Restore**
 - ◆ When the control panel can't receive the signal transmitted from any one of the devices individually for a preset time.
 - ◆ When the supervision function of sensor is restored.
- **151 – Gas**

- ◆ When device set to Gas Alarm is activated.
- **154 – Water leakage**
 - ◆ When device set to Water Alarm is activated.
- **158 – High Temperature Alarm**
 - ◆ When high temperature alarm is triggered.
- **159 – Low Temperature Alarm**
 - ◆ When low temperature alarm is triggered.
- **162 – CO detector**
 - ◆ When device set to CO Alarm is activated.
- **170 – High Power Consumption**
 - ◆ When high power consumption alarm is triggered.
- **171 – High Humidity Alarm**
 - ◆ When high humidity alarm is triggered.
- **172 – Low Humidity Alarm**
 - ◆ When low humidity alarm is triggered.
- **301 – AC Failure/ AC Power Restore**
 - ◆ When the AC power failure is detected.
 - ◆ Restore from AC power failure
- **302 – Low battery/ Battery Normal**
 - ◆ When the battery voltage of the Panel is low
 - ◆ When the panel battery restores voltage.
- **311 – Battery Disconnection/ Battery Reconnected**
- **344 – Interference/ Interference restore**
- **358 – Network Cable Unplugged**
 - ◆ When the Ethernet cable is disconnected from the Control Panel.
- **359 – GSM No Signal**
 - ◆ When the Control Panel fails to connect to GSM network.
- **380 – Device AC Failure**
 - ◆ When an AC power device loses AC power connection.
- **383 – Sensor Tamper/ Sensor Tamper Restore**
 - ◆ When any sensor's tamper protection is triggered.
 - ◆ When the sensor's tamper function is restored.
- **384 – Sensor Low battery/ Sensor Battery Normal**
 - ◆ When the battery voltage of any one of the devices is low.
 - ◆ When any device's battery restores voltage.
- **389 – Self Test Failure**
- **400 – Arm/Disarm (by Remote Controller)**
 - ◆ When the system is armed or disarmed by using the Remote Controller.
- **401 – Remote Arm/Disarm**
 - ◆ When the system is armed or disarmed by web access

- **407 – Disarm/Away Arm/Home Arm by Remote Keypad**
- **408 – Set/Unset Arm/Disarm**
 - ◆ When the DC set at Set\Unset is triggered.
- **456 - Partial Arm**
 - ◆ When partially arm the system from Disarm to Home arm
- **465 – Alarm Reset**
- **570 – Device out of order/ Door Contact Not Closed**
 - ◆ When arm fault type is set as Direct Arm, any device is out of order after the preset exit delay time is reached
 - ◆ When arm fault type is set as Direct Arm, Door Contact is not closed after the preset exit delay time is reached.
- **602 – Periodic test report**
 - ◆ When the control panel makes periodic Check-in reporting.

Appendix B: Faults

During operation, when the panel detects faulty events, the panel will log the event and make reports. When fault events exist in the system, the panel Fault LED will light up.

Fault Message Displayed	Fault Situation	Solution
Panel AC Fault	Control Panel AC Power is disconnected.	Check AC power adaptor connection to power socket and panel AC input.
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 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. Reconnect the battery to panel board. 2. Turn on battery switch. 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.	Check if the Control Panel is properly mounted with the tamper switch depressed, and the cover is closed
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.	<p>(For Wireless Device)</p> <ol style="list-style-type: none"> 1. Check if device is low on battery by checking the fault event display. If device is on low battery, change battery. 2. If device battery is normal, change device location for better signal strength. Use Walk Test to find the new location. 3. If the battery is normal and the device signal cannot be received by panel at all using Walk Test, replace the device. <p>(For Wired Device)</p> <ol style="list-style-type: none"> 1. Check if the device is wired to the Panel properly. 2. Use walk test to check if the device is connected properly to the Panel within appropriate wiring distance. 3. If the device is connected properly to the Panel within appropriate wiring distance, but 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.	<ol style="list-style-type: none"> 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.

<p>Out of Order (Zone#)</p>	<p>The device at specified zone is out of order (supervision failure) Note: This event will appear when:</p> <p>1. If the device has failed supervision, the event will be displayed on webpage.</p> <p>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</p>	<p>(For Wireless Device)</p> <p>4. Check if device is low on battery by checking the fault event display. If device is on low battery, change battery.</p> <p>5. If device battery is normal, change device location for better signal strength. Use Walk Test to find the new location.</p> <p>6. If the battery is normal and the device signal cannot be received by panel at all using Walk Test, replace the device.</p> <p>(For Wireless Device)</p> <p>4. Check if the device is wired to the Panel properly.</p> <p>5. Use walk test to check if the device is connected properly to the Panel within appropriate wiring distance.</p> <p>1. If the device is connected properly to the Panel within appropriate wiring distance, but the device signal cannot be received by panel at all using Walk Test, replace the device.</p>
<p>Triggered (Zone#)</p>	<p>This event only applies to following devices: PIR Sensor, PIR Camera, and Remote Controller Panic Button.</p> <p>The event will appear only when you attempt to arm the system within 5 seconds after the device is triggered or pressed.</p>	<p>1. Check your PIR Sensor and PIR Camera detection area and make sure your home perimeter is safe before arming the system.</p> <p>2. After triggering a Panic alarm with your Remote Controller, wait for at least 5 seconds before arming the system.</p>
<p>Report Fail</p>	<p>The Control Panel has not been able to send a report for over 2 minutes.</p>	<p>1. Check and make sure your report setting is programmed correctly</p> <p>2. Check Ethernet connection</p> <p>3. Check GSM/GPRS connection</p>
<p>Network Cable Unplugged</p>	<p>The Control Panel has lost its Ethernet cable connection</p>	<p>Restore Ethernet cable connection to the Control Panel.</p>

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 22/24/27 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 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.