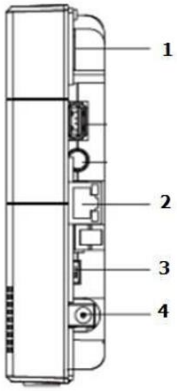
INSTALLER MANUAL

1. VESTA HSGW panel features

Commissioning

1. SIM insert (2G, 3G or 4G) "Optional"
2. Connect Ethernet
3. Set the battery switch to the position: ON
4. Connect the DC adapter
5. All LEDs will light up and after 10-15 seconds the gateway will be ready.



Vista Lateral

Panel Features:

- IP (Ethernet) y 2G o 4G
- 640 Zones - 8 Areas - 240 Users/Partition
- RF 868 MHz (2 km range) and Z-Wave (100-200 m)
- 100 Automation Rules
- 50 Scenes
- Ranura de expansión USB: Zig-Bee, Wi-Fi, 3G / LTE, LoraWAN
- Built-in siren and battery backup
- EN-50131 Grade 2
- Operational: -10°C to 45°C (14°F to 113°F) Up to 85% non-condensing

2. VESTA HYBRID panel features

Panel Features:

- IP (Ethernet) y 2G o 4G
- 640 Zones - 8 Areas - 240 Users/Partition
- RF 868 MHz (rango de 2 km) y Z-Wave/ZigBee (100- 200 m)
- 100 Automation Rules
- 50 Scenes
- Ranura de expansión USB: Z-Wave, Zig-Bee, Wi-Fi, LoraWAN
- Terminal de BUS RS485
    - Keyboard connection (touch and/or LCD)
    - Conventional zone expanders EOL, DEOL, 3EOL
    - PIR BUS V-Max
    - PIR CAM BUS V-Max
    - Sirens on V-Max BUS
    - Relay modules on V-Max BUS
    - V-Max BUS Isolators
    - V-Max BUS Amplifiers
    - Etc...
- Lema for SIRENA Output and PG Output
- Battery Backup
- EN-50131 Grade 3

3. Register an installer account

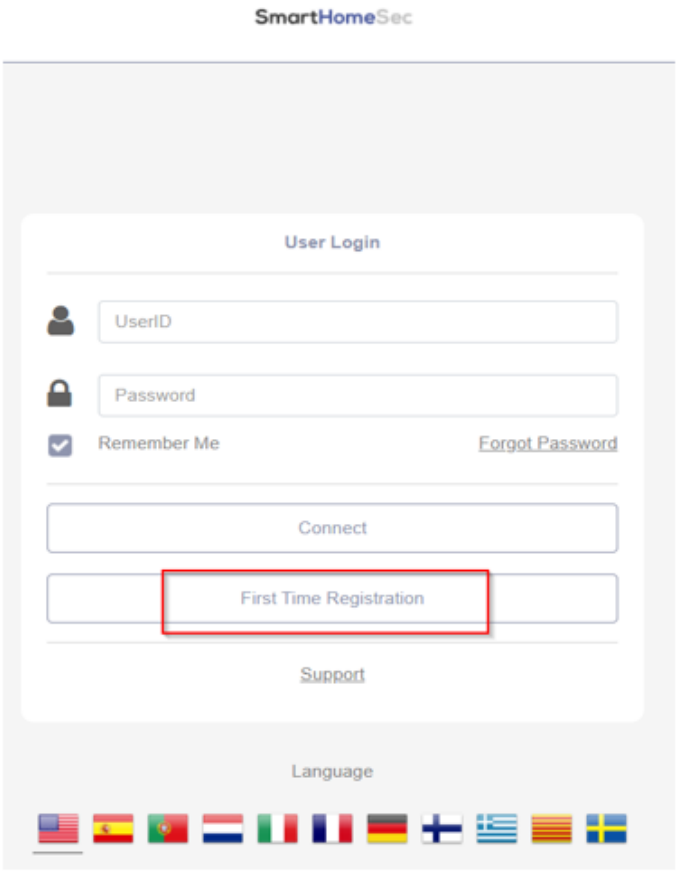
NOTE!: If you already have an installer account you can jump directly to point nº4 "Register panels under the installer account. Register Panel"

This step nº3 will only be performed once.

Activate installer account:

3.1 Login to the SmartHomeSec platform via:
3.1.1 WEB https://portal.vestasecurity.eu/Vesta/
3.1.2 o APP SHS

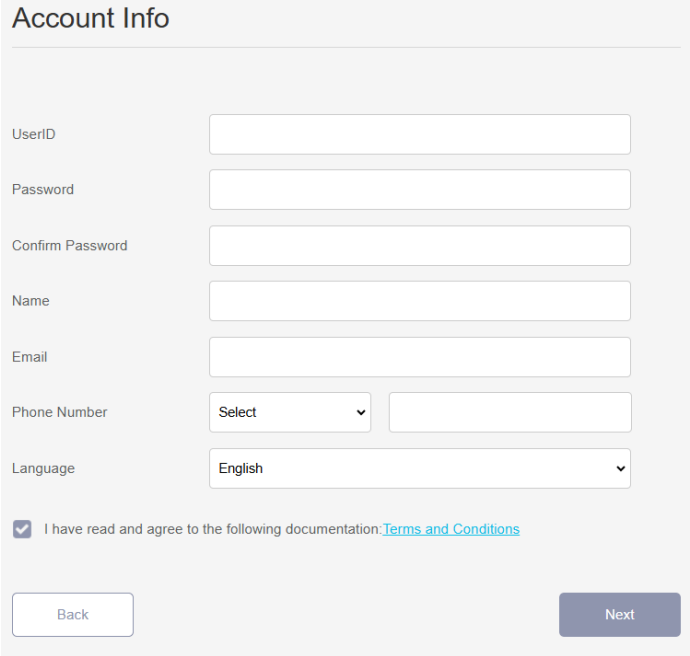
3.2 Click on Installer Registration



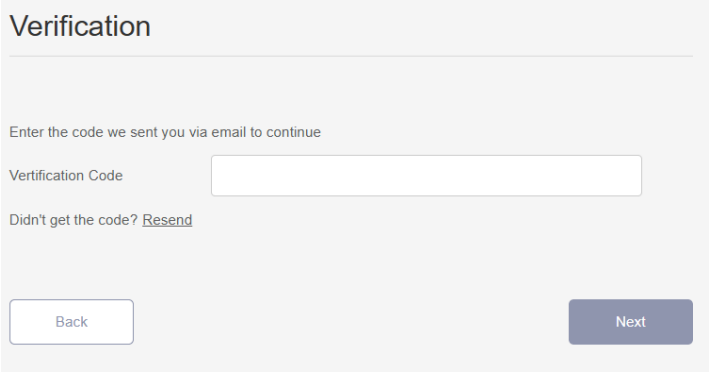
Vista WEB

Vista APP

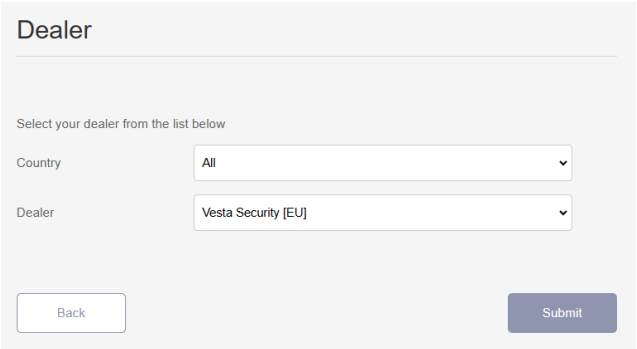
3.3 Fill in the form and click on next



3.4 Verify with the code received in the email



3.5 Dealer set Country all and choose Vesta Security [EU]



Now you have an installer account from which you can manage all your VESTA control panels!

4. Registration of panels under the installer account

Register Panel

Accessing the SmartHomeSec Platform from an Installer Account

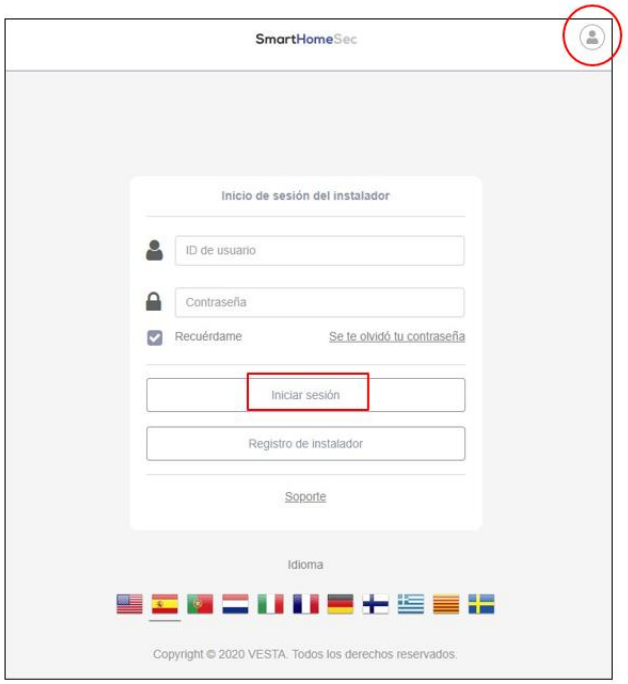
https://portal.vestasecurity.eu/Vesta/

4.1 Register panel from the SmartHomeSec WEB

To register control panels in the installer account:

Enter the SmartHomeSec WEBSITE: https://portal.vestasecurity.eu/Vesta/

- Log in with your registered username and password

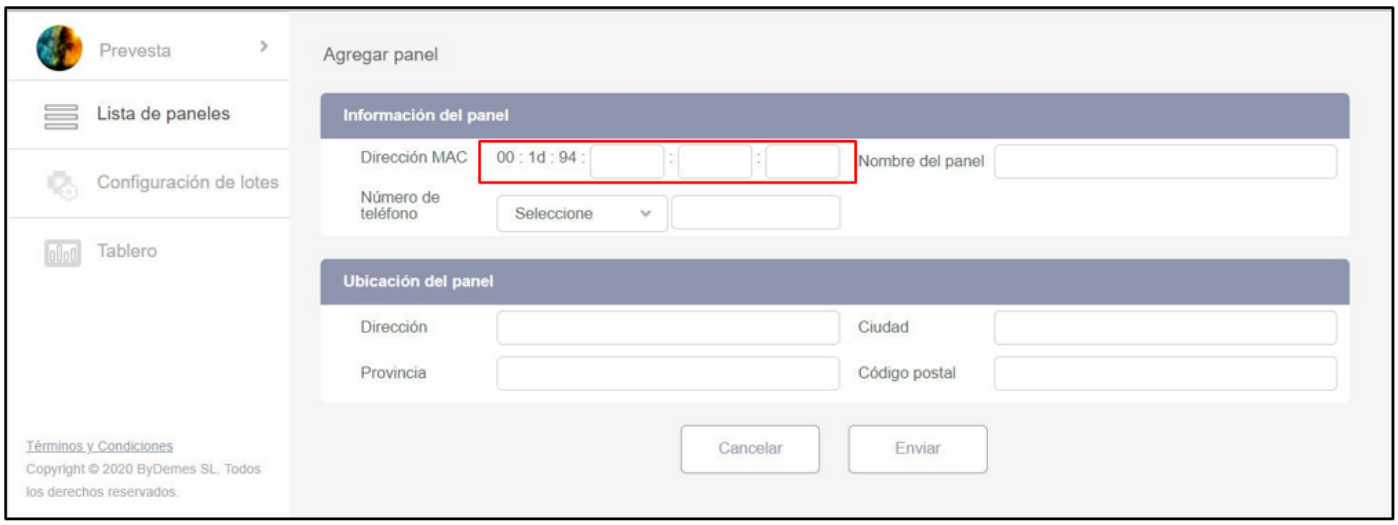


NOTE! The switch between viewing in installer or user mode is done by clicking on the icon:

- Click on the "+" button to add a new panel

Info! The panel must be turned on and connected to the internet. We will have 15 minutes after feeding to register the panel!

- Click on the "+" button to add a new panel

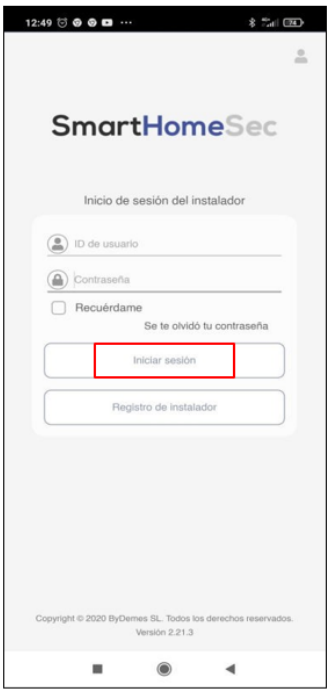


- The **MAC** is located on the side of the panels
- **Panel name with** which you will register in the system
- Telephone number, Address, City, Province and Postal Code is not mandatory, but interesting to have a small database with information on each central
- **Once the process is complete, we receive a confirmation email. Our panel is registered**

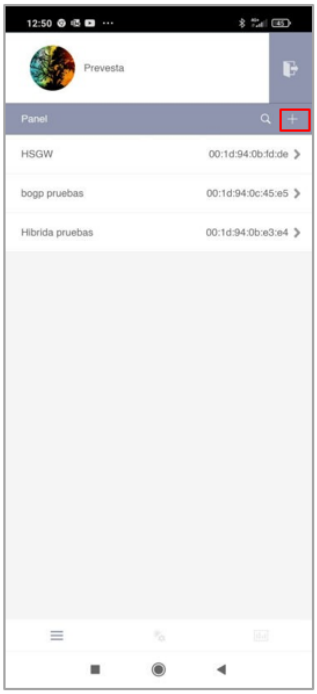
4.2 Register panel from the SmartHomeSec APP

To register control panels in the installer account

Entrar con el usuario y contraseña registrado



Seleccionar: Añadir nuevo panel



Rellenar con la dirección MAC se encuentra en el lateral de su panel

Note! The switch between viewing in installer or user mode is done by clicking on the icon:


Instalador


Usuario

Info! The panel must be turned on and connected to the internet. We will have 15 minutes after feeding to register the panel!

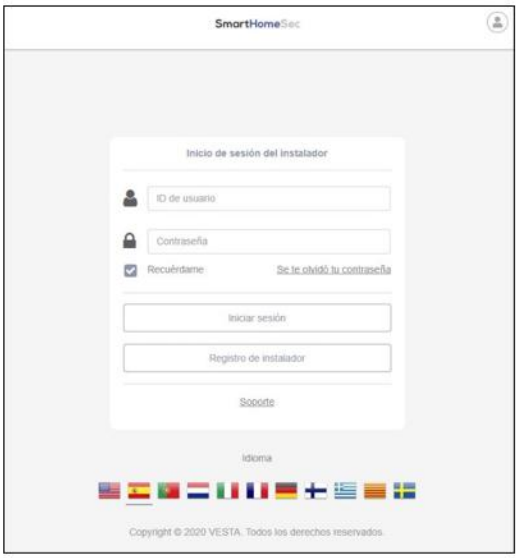
- The **MAC** is located on the side of the panels
- **Panel name with** which you will register in the system
- Telephone number, Address, City, Province and Postal Code is not mandatory, but it is interesting to have a small database with information on each central
- **Once the process is complete, we receive a confirmation email. Our panel is registered**

5. Panel Programming

To simplify this manual, from this point on all the information and figures shown will be referenced to the WEB platform! Due to the great similarity between the APP and WEB platforms, it is understood that it is not necessary to insist on the same thing and duplicate the information.

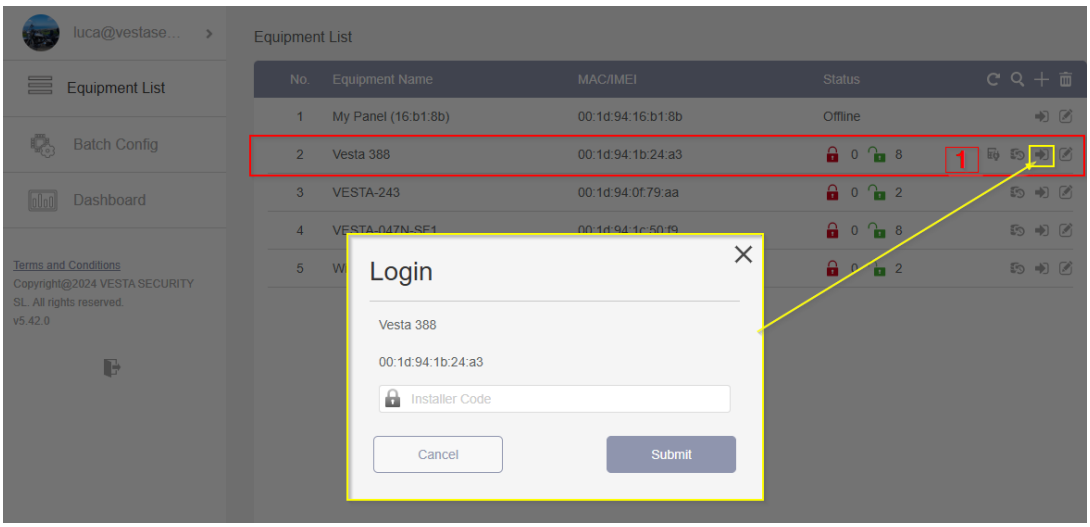
1. Enter the SmartHomeSec WEBSITE: https://portal.vestasecurity.eu/Vesta/

2. Access the installer account with the registered username and password



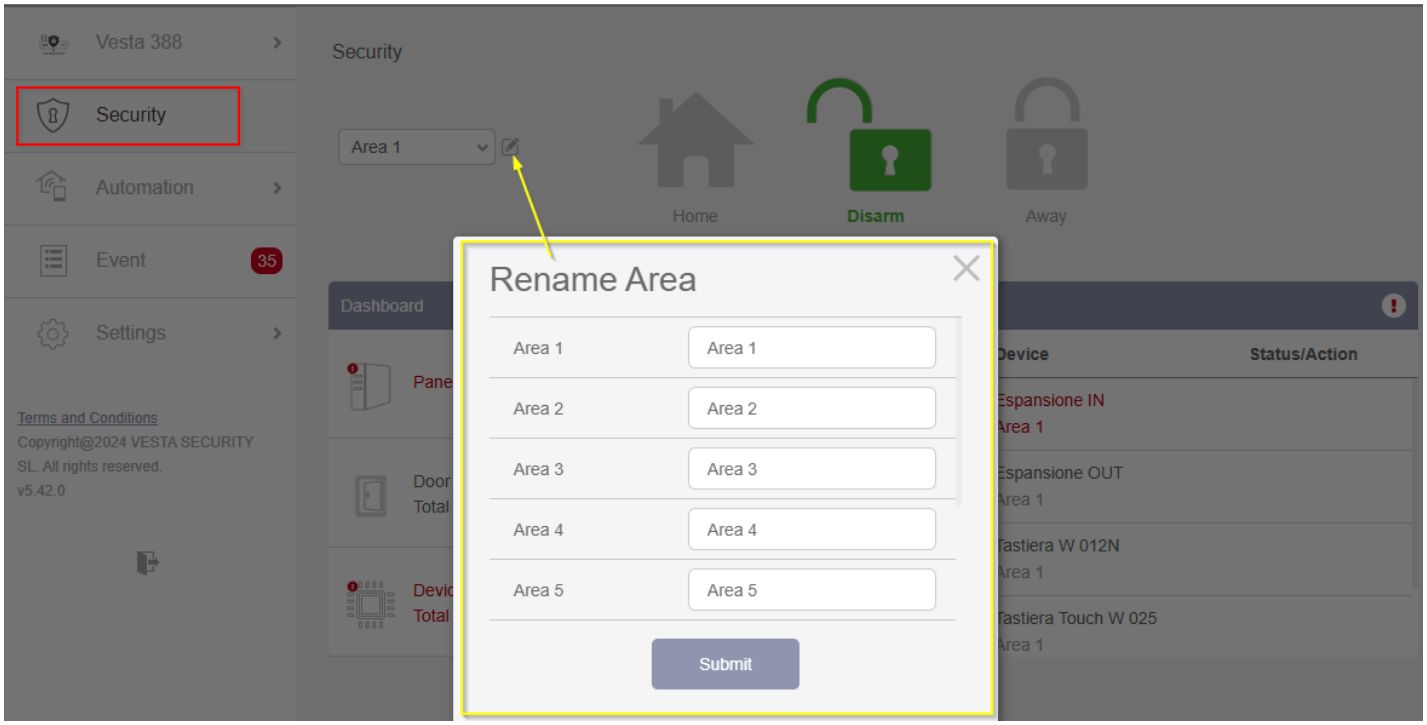
3. Select from the list [1] the target panel of

4. Insert Installer Code, Factory **7982**



6. Home screen: Security section

From here the user installer will have a general idea of the current state of the system at a technical level (technical failures of the panel or devices) that will be highlighted in red. Also, you can check if the partitions in the panel are armed or disarmed.

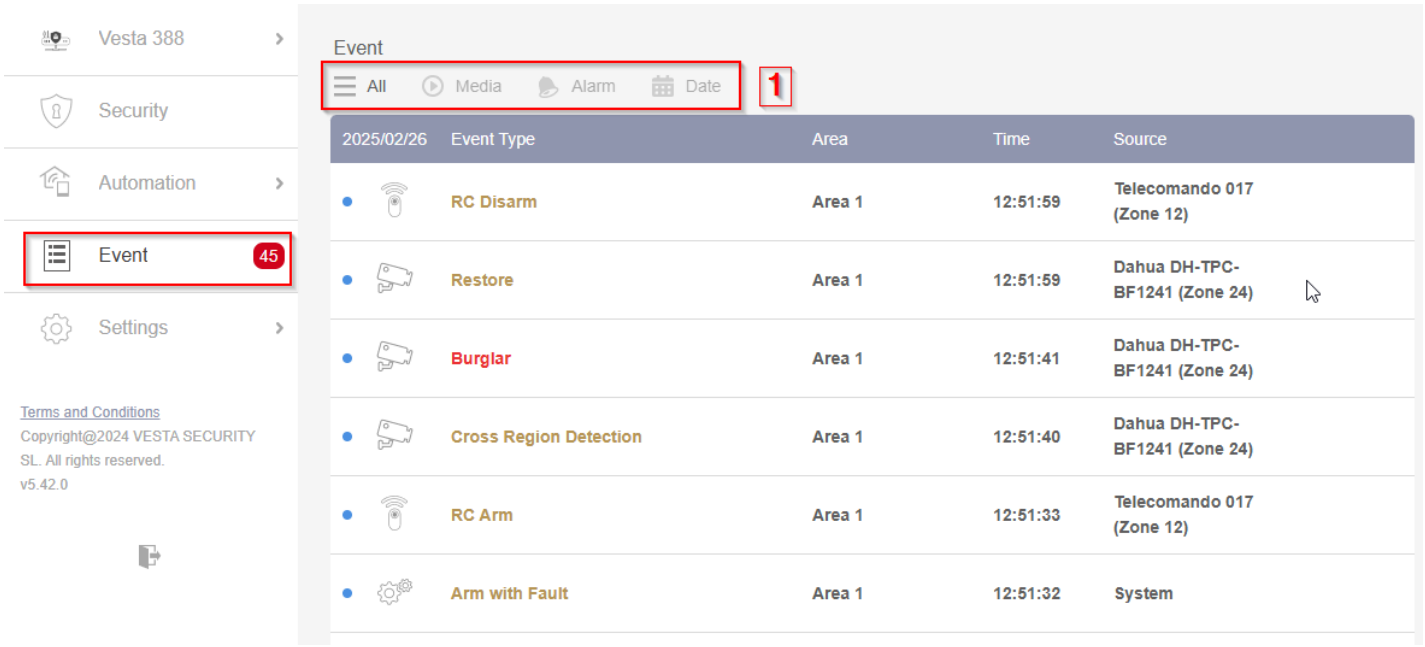


Note! By law, it is not possible to control partitions from the installer account

7. Event History

In the events section, all the events generated by the panel are saved and displayed for an approximate period of 1 month, including: armed, disarmed, technical failures, technical alarms, intrusion alarms.

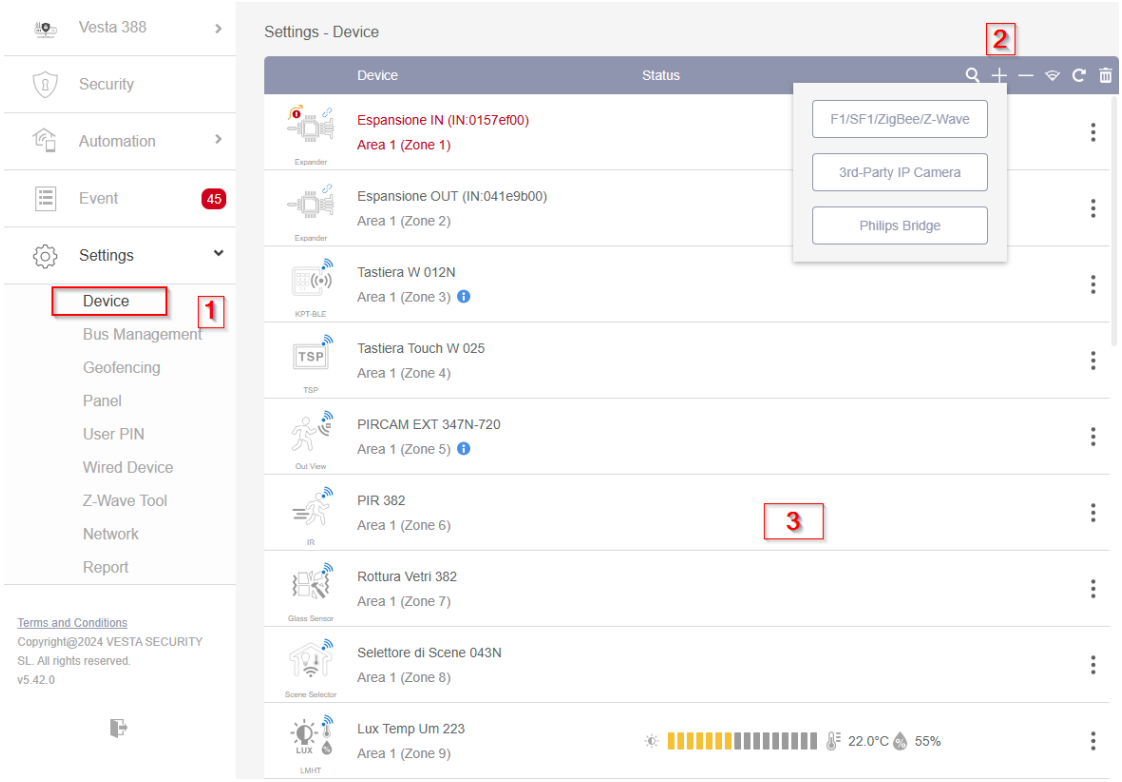
A search engine **[1]** is available from which you can apply search filters by alarm images, alarm events or search by date



8. Settings: Add Devices

Setting → Device [1] → Add Device [2] → F1/SF1/Zigbee/Z-wave [3] .

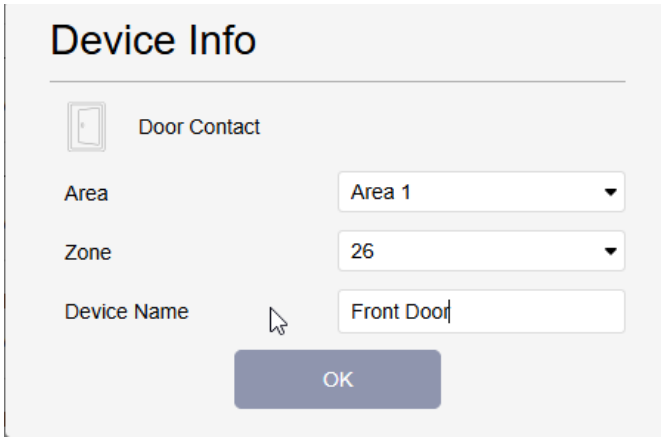
The panel switches to learning mode and waits to receive mapping signals

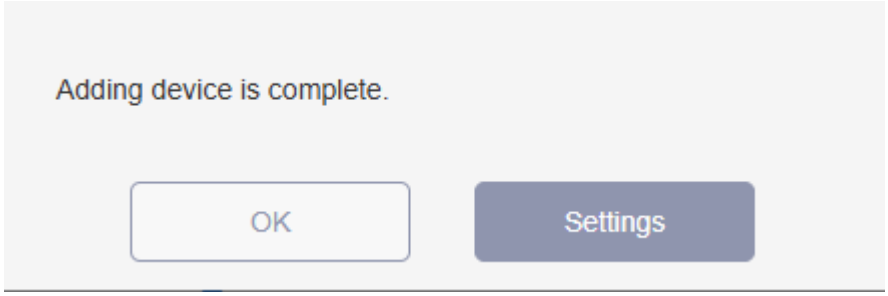


1. Press the enroll button on the device you want to add. Example: magnetic contact. Once detected in the panel, select the device and OK.

Note! Each detector has a specific button to enroll the equipment. Check your specific manual to ensure you are pressing the correct button in mode and form

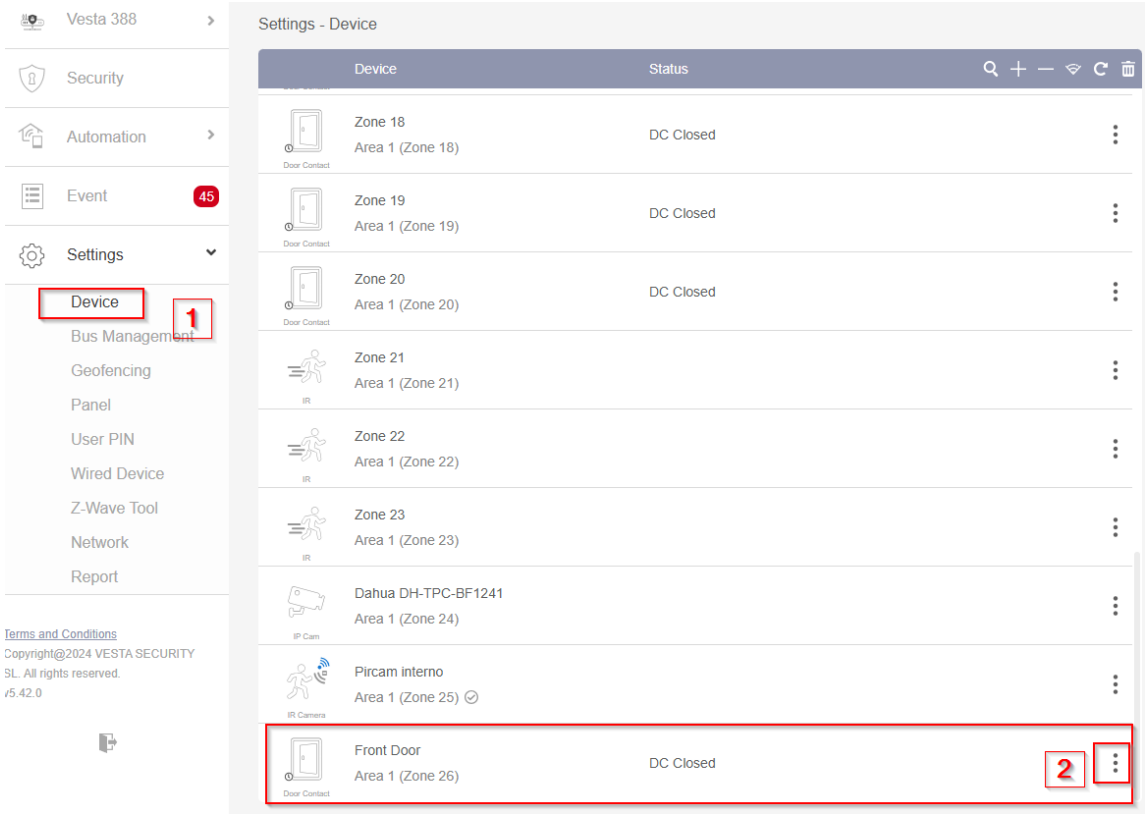
2. Select Area, Zone and give the zone a name and press OK. If can press Settings to configure the device options. The device is now successfully added to the panel





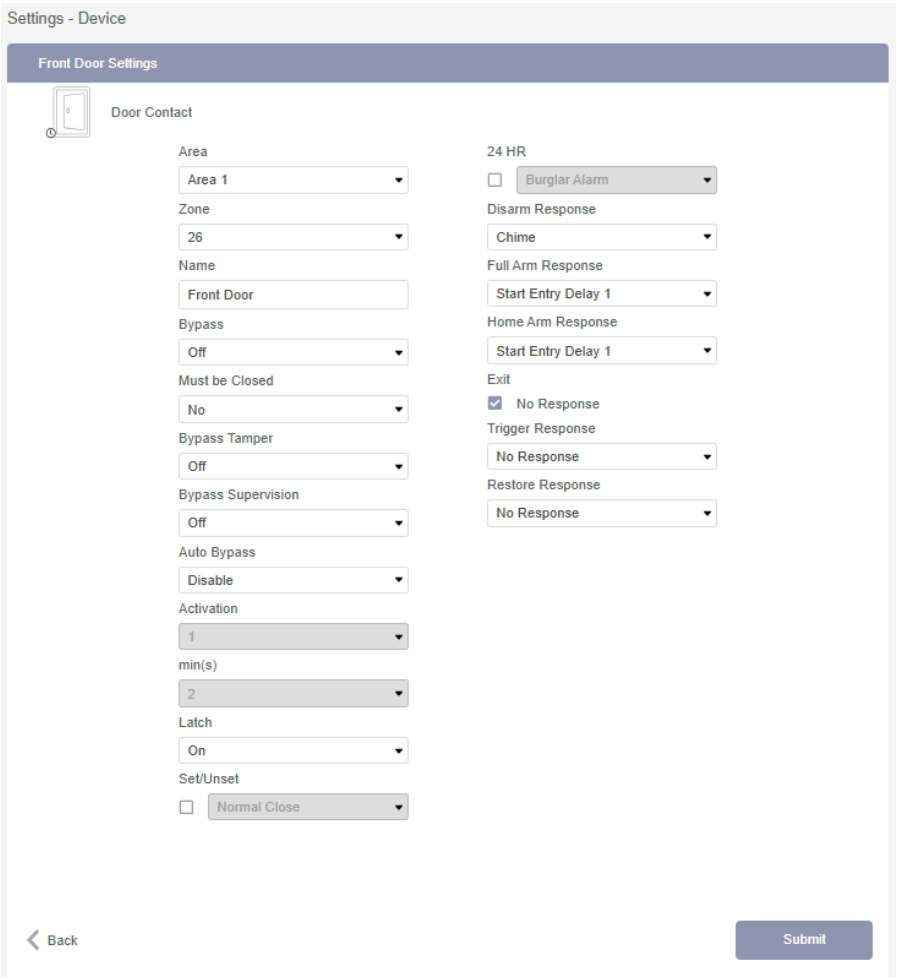
8.1 Zone Configuration

To set up a device: go to Devices [1] and tap on the device settings [2]



Note! Each detector will have different settings depending on its nature. Below is a summary of the overall adjustments based on a PIR

8.2Zone Configuration. Internal adjustments



Area -> Select Area (Partition) [1/2/3/4/5/6/7/8]

Zone -> Select Zone Number of [1-80] (the panel show you the number of the first zone free)

Name -> Zone Name: ["Front Door"]

Bypass -> Bypass Zone ON/OFF

Must be Closed -> Yes/No

Bypass Tamper -> ON/OFF

Bypass Supervision -> ON/OFF

Auto Bypass -> Enable/Disable

24 HR -> 24h zone setting

Disarm Response -> Zone Reaction when the panel is disarmed

Full Arm Response -> Zone Reaction when the Panel is armed away

Home armed Response -> Zone reaction when the panel is armed stay

Zone reaction options when the system is armed stay, away or disarmed

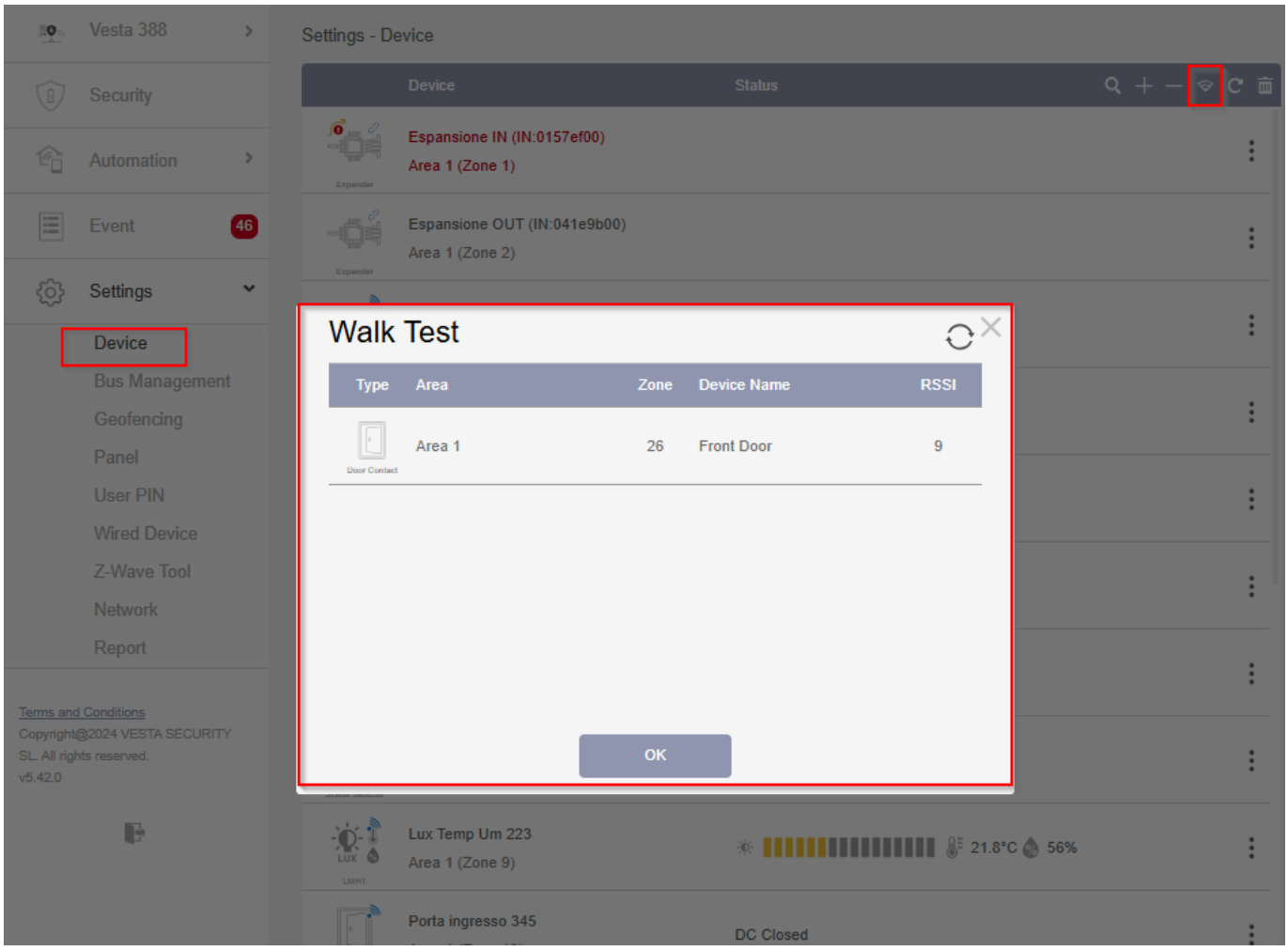
a. No Response
b. Start enrtry Delay 1
c. Start enrtry Delay 2
d. Chime
e. Burglar Follow
f. Burglar Instant
g. Burglar Outdoor
h. Burglar Silent
i. Cross zone
j. Trigger Notification

Trigger Response -> Apply Scene on open zone

Restore Response -> Apply Scene on restored zone

8.3 Walking test

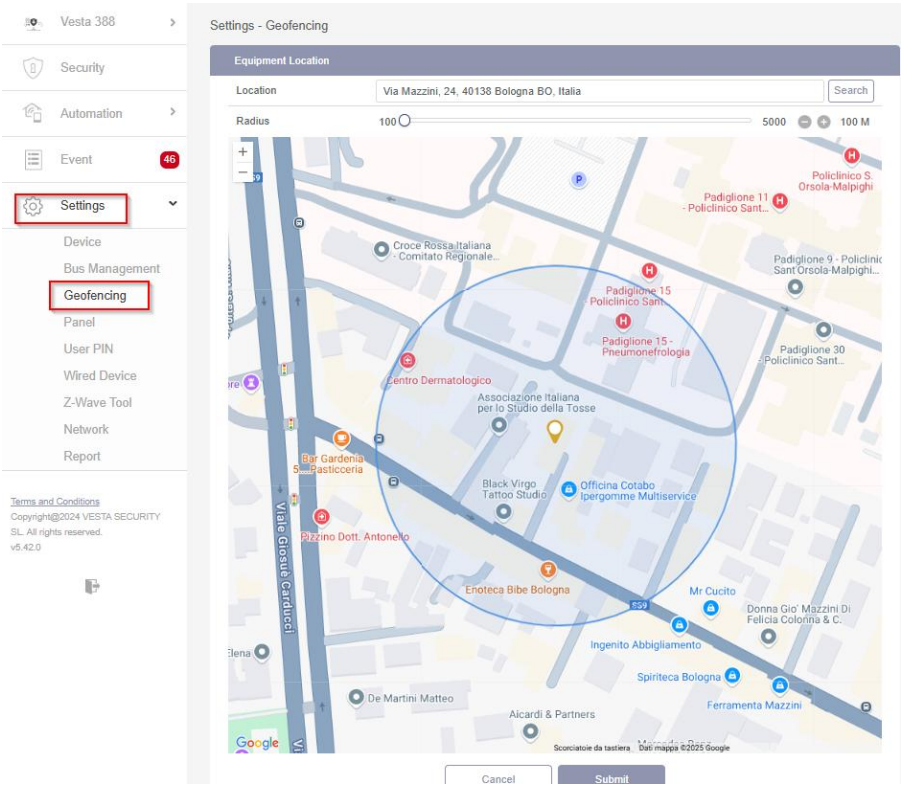
By launching a walk test, the signal strength with which the zones transmit via radio is checked



Note! Press the learn button in the same way as to assign the device. The signal strength in a range from 0 to 9 will then be displayed. Powers => 4 or less are recommended if a stable signal is maintained over time

9. Set GEOFENCING

From this section, Setting [1] →Geofencing [2] you can configure the virtual geofence



Note! Now you can use the Geofence from the SmartHomeSec APP.

Scenes can be activated by the entrance/exit of the marked virtual perimeter

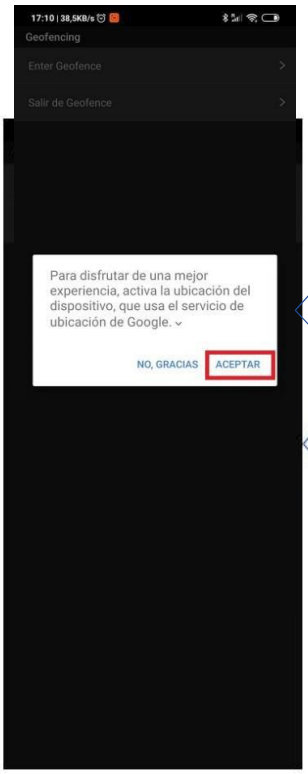
9.1 Geofence Configuration in SmartHomeSec APP

To configure geolocation on your mobile phone, you have to enter the **SmartHomeSec App**:

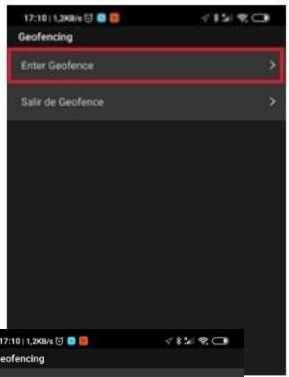
Entrar con el **usuario** y **contraseña** registrado

Entrar en **Ajustes**

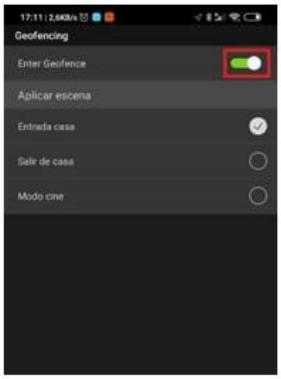
Seleccionar **Alertas Inteligentes**



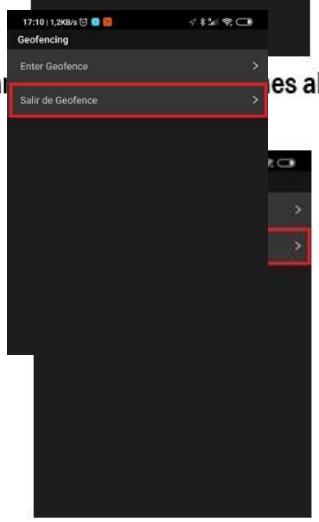
Para configurar las acciones al **Entrar en Geofence:**



Habilitar la **entrada y seleccionar Escena a aplicar**



Pa es al

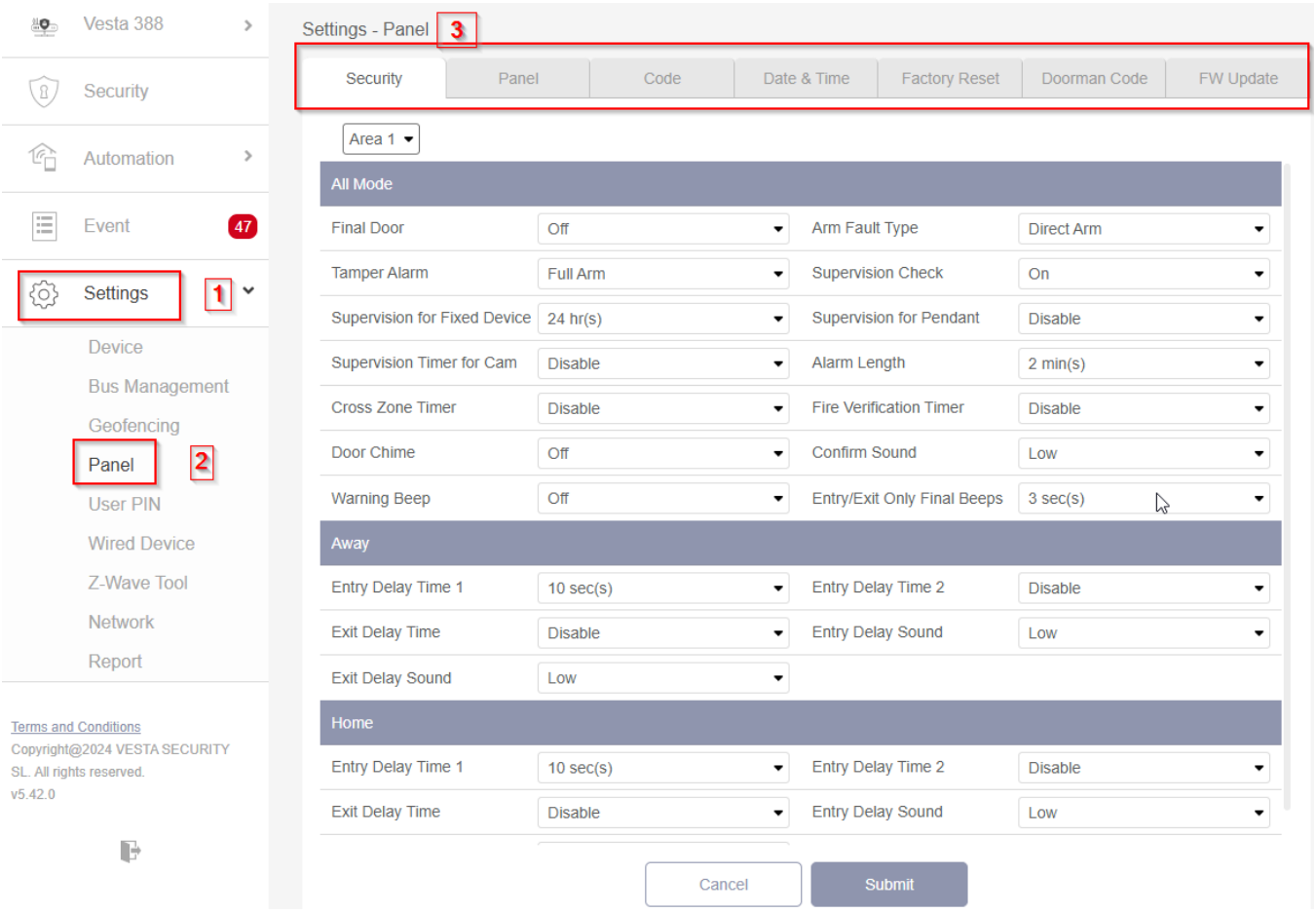


Habilitar la **Salida y seleccionar Escena a aplicar**

Note! When entering or exiting the Geofence zone, you can apply preconfigured scenarios on the dashboard, like arming or disarming the panel, turning on/off lights... (For more information on **Scenes: Sections 12.1 and 12.2)**

10. Panel Settings

To access the general panel settings: Adjustment [1] →Panel [2] →Settings- Panel [3]

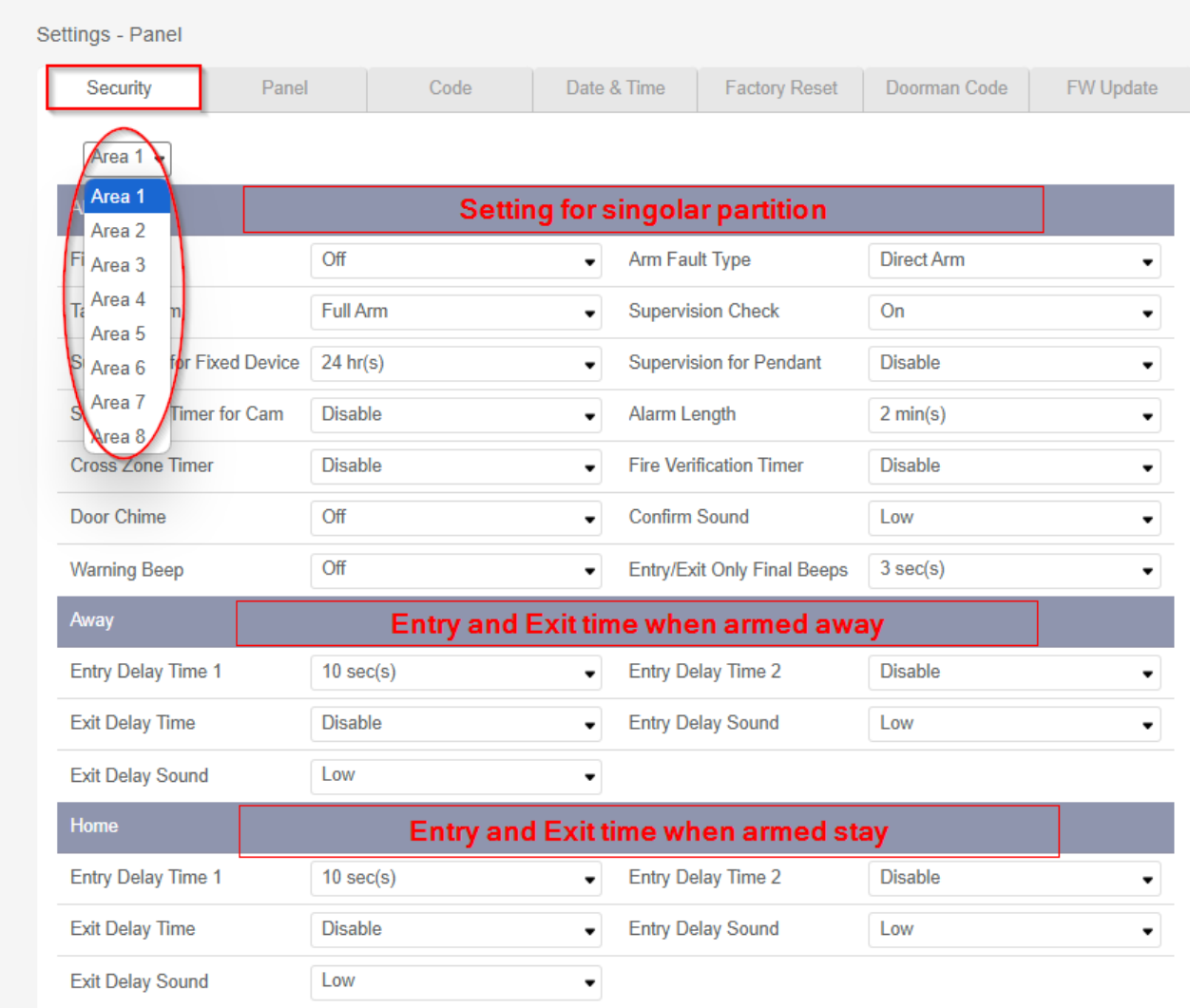


Subsections:

1. Security
2. Panel
3. Code
4. Date and time
5. Factory Reset
6. Doorman Code
7. FW Update

10.1 Security

To access the Security subsection: Setting →Panel →Settings- Security

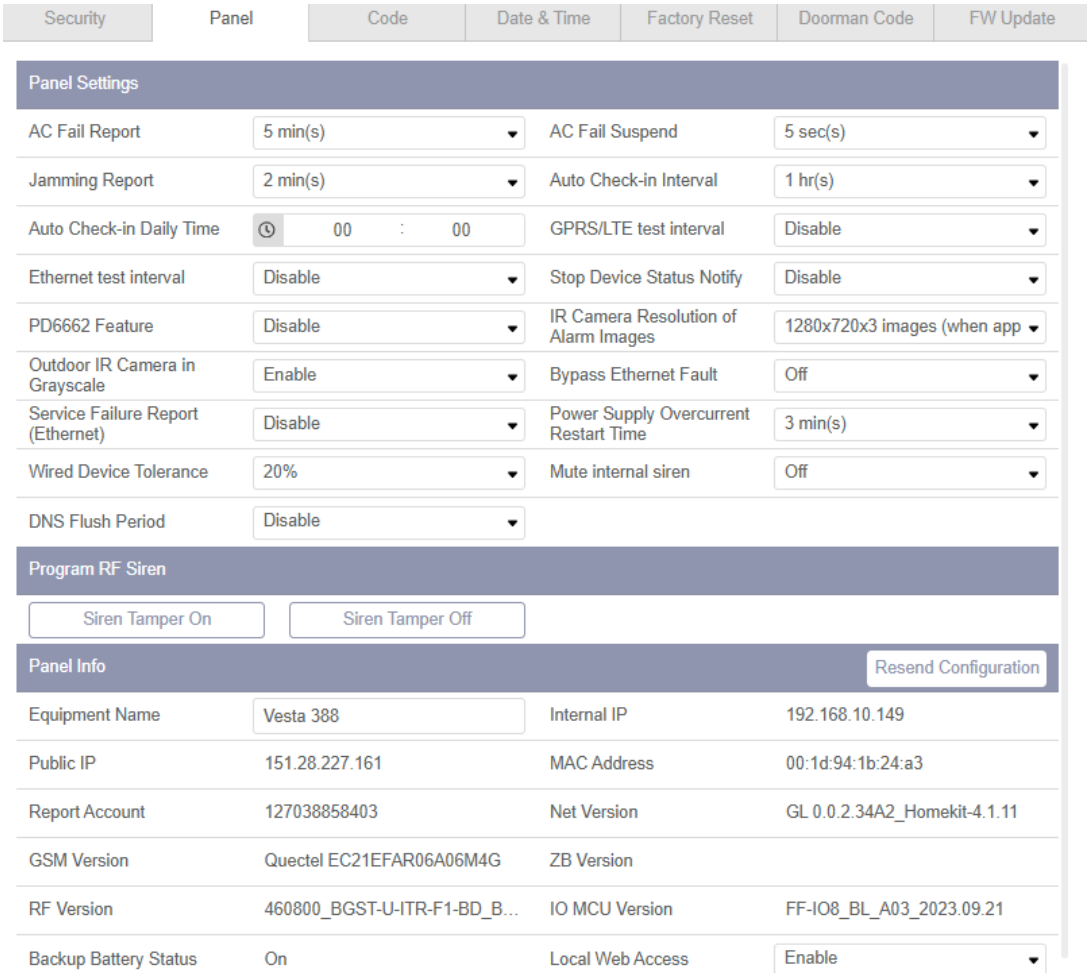


Within the Security subsection, the generic security parameters can be modified for each of the partitions. Among them:

1. Entry Time 1
2. Entry Time 2
3. Exit Delay Time
4. Alarm Length -> "Siren Activation Time in Case of Alarm"
5. Warnings Beep
6. … For more details see the full manual

10.2 Panel

To access the panel subsection : Setting →Panel

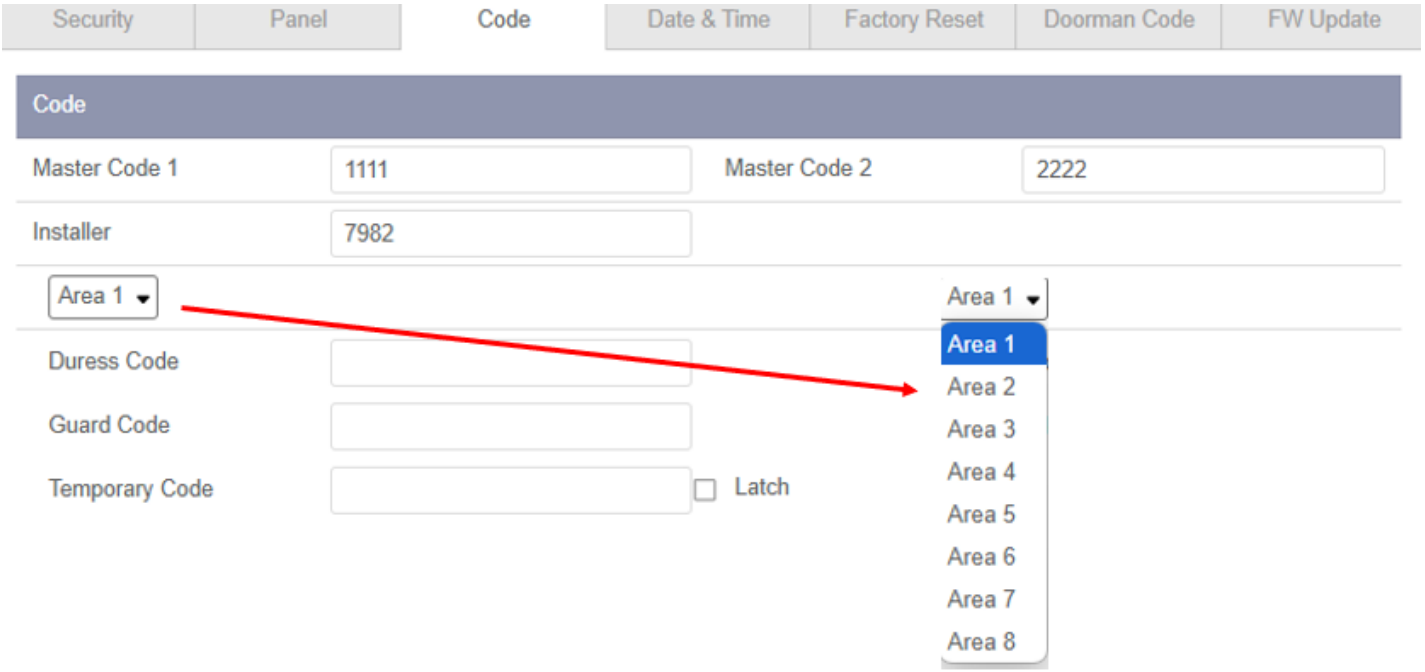


Within the Panel subsection, the panel parameters can be modified:

1. Time to notify: AC Power Failure
2. Sensitivity: RF interference
3. Supervision Time
4. Polling CRA
5. Resolution of PIRCAM photos
6. Enable/disable Tamper siren
7. Rename the Equipment
8. Panel info: Local IP, public, current FW, etc...

10.3 Codes

To access the Code subsection: Setting →Panel →Code

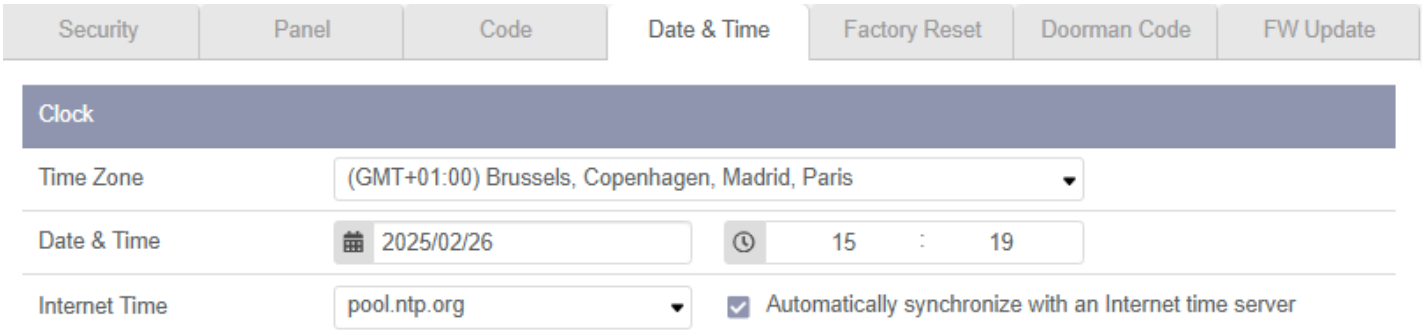


Within the Code subsection, the access parameters may be modified. That is, programming the codes that will authenticate the different types of users from any keyboard

- Master Code 1 and 2: enables a user to permanently override zones, manage codes, etc... from an App/WEB account with administrator profile
- Installer Code: allows you to program the panel completely
- Duress Code: system control with silent alarm
- Guard Code: for security personnel
- Temporary Code: Only disarm and arm 1 time

10.4 Date and Time

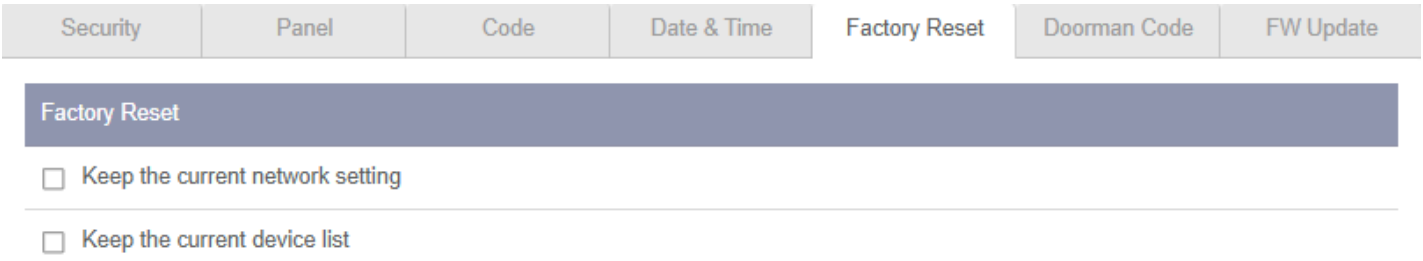
To access the Date & Time subsection: Settings →Panel →Settings- Date & Time



Note! It is recommended to leave this section from the factory, as long as the date and time coincide with the correct time zone.

10.5 Factory Reset

To access the Reset subsection: Setting →Panel →Settings- Factory Reset

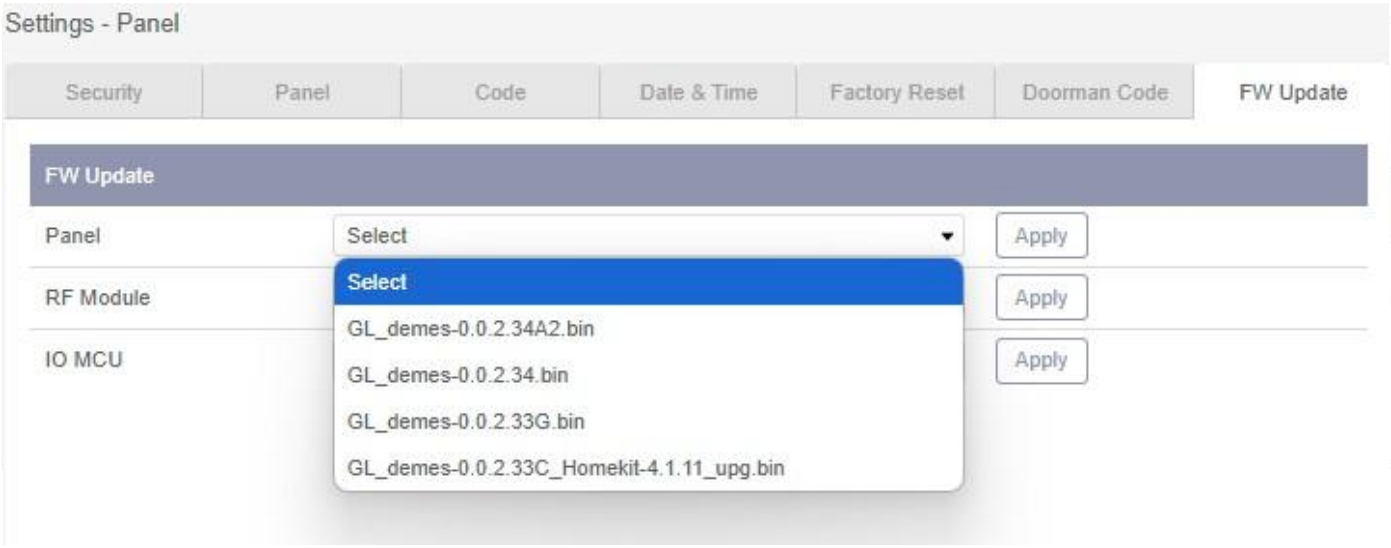


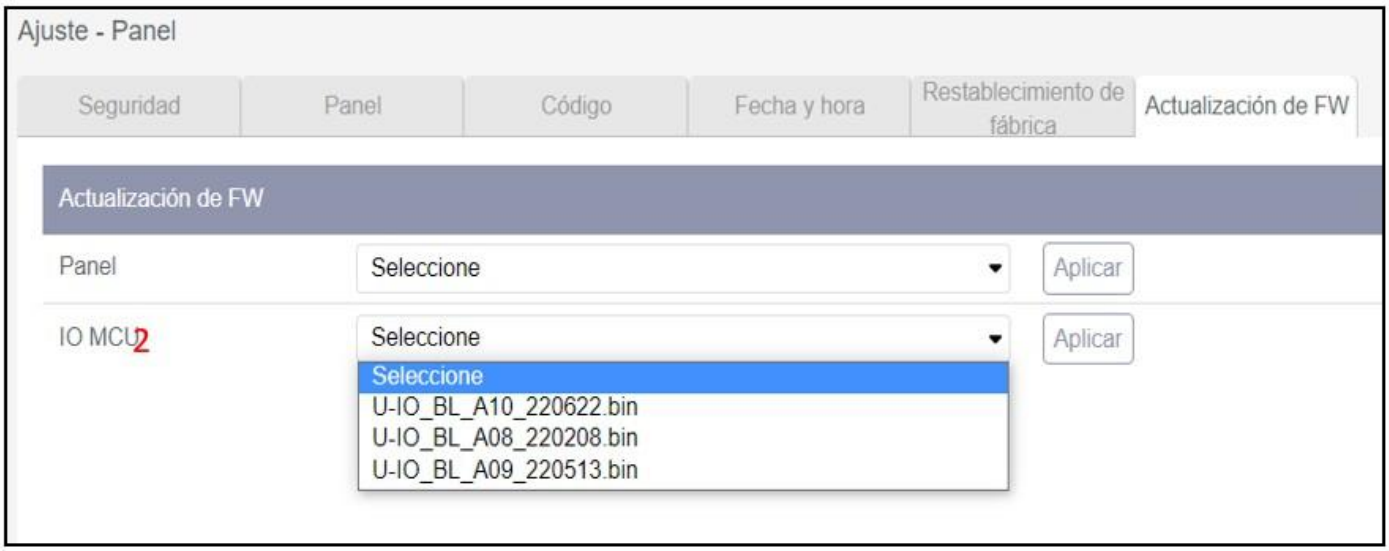
Note! A factory reset is also allowed manually. But this software-based feature gives us the possibility to keep the network configuration as well as the assigned devices after launching the reset

10.6 FW Update

Before abandoning the installation, it is recommended to leave the panel updated to the latest version of FW available.

If for some reason you are NOT, you will be able to update this FW remotely whenever you want. This is a very secure process that takes < of 3 min. and after which the panel will restart.

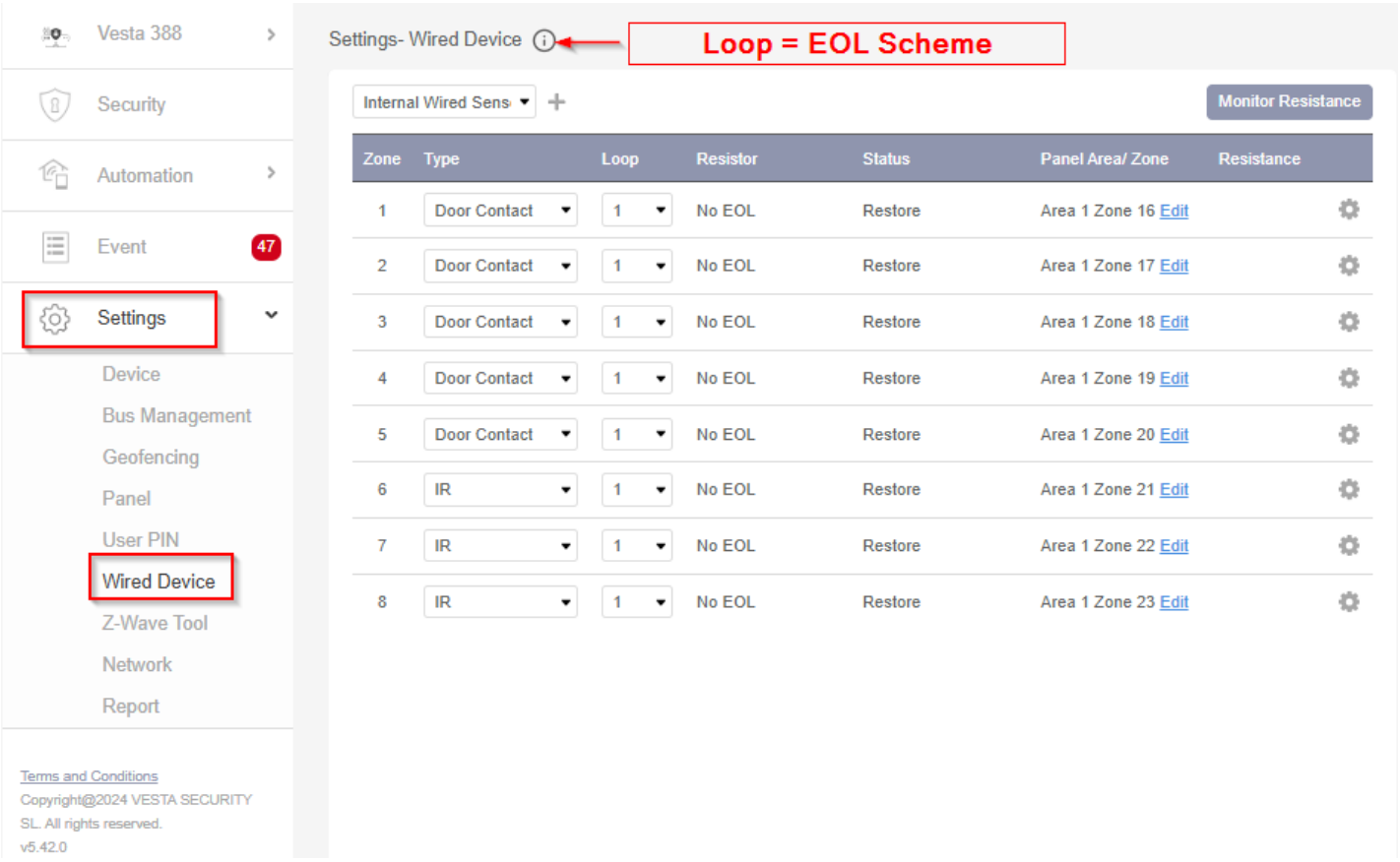




Note! The panel model with which the captures are being taken is the Hybrid, and therefore in addition to being able to update the FW of the panel [1], it will also be possible to update the FW of the IO MCU controller [2], responsible for managing the wired expanders and BUS

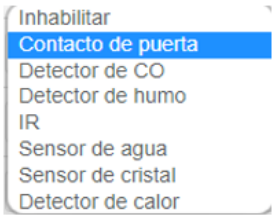
Note 2! It is recommended to always choose the latest version of FW, which usually occupies the 1st position

10.7 Conventional wired areas



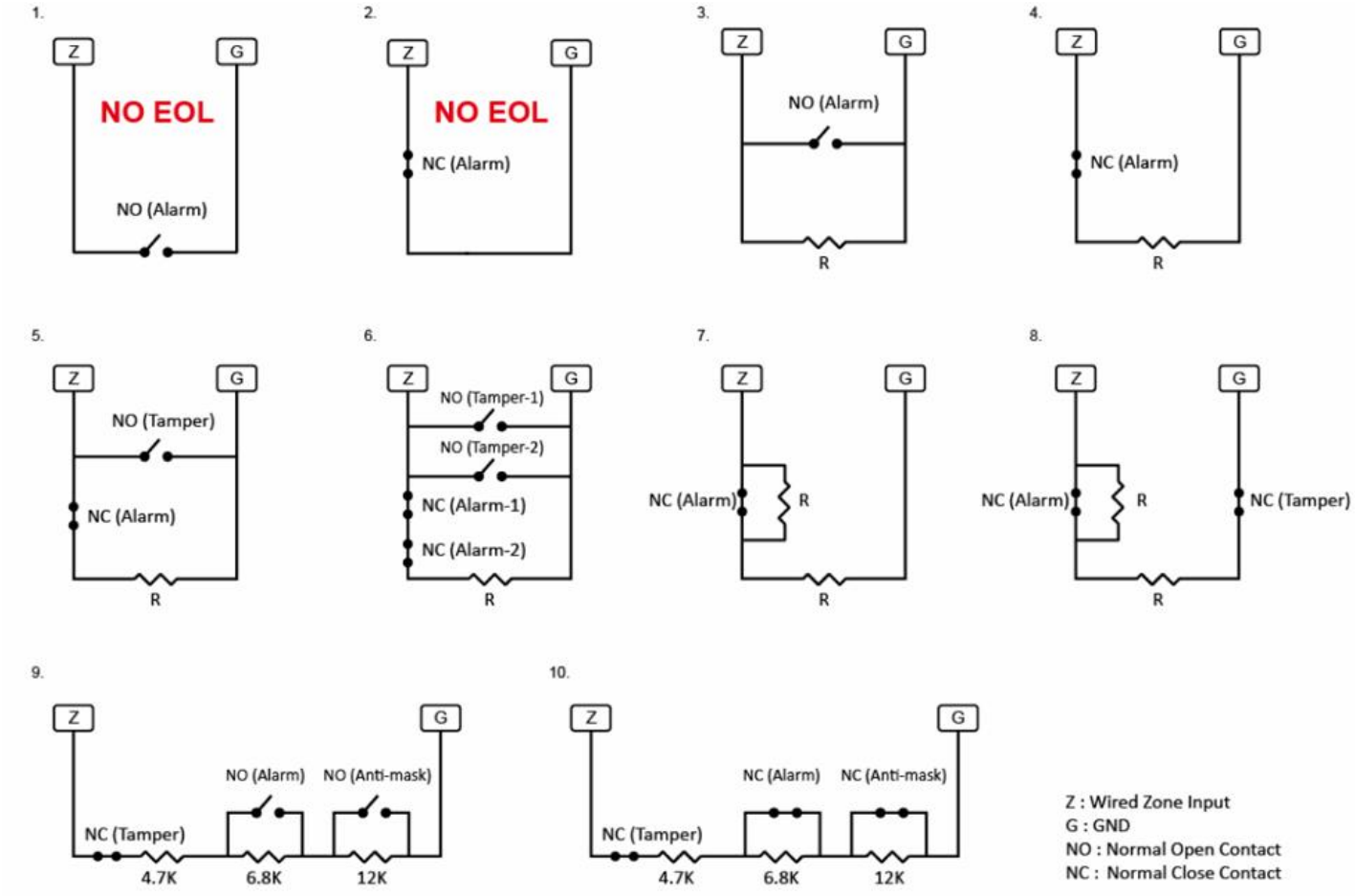
Exclusively in the HYBRID control panel, 8/16 wired zone are available on board with the capacity to protect the loop with EOL, DEOL, and 3EOL resistors or implement simple NC / NO loops. To enable the zone it is simply necessary to indicate:

- Zone Type



- Loop type, click on or view the next slide
- EOL or DEOL resistance, selectable for each of the 16 inputs

By default, the system associates the detector with a free virtual area and zone. By clicking on the button it is possible to edit these values

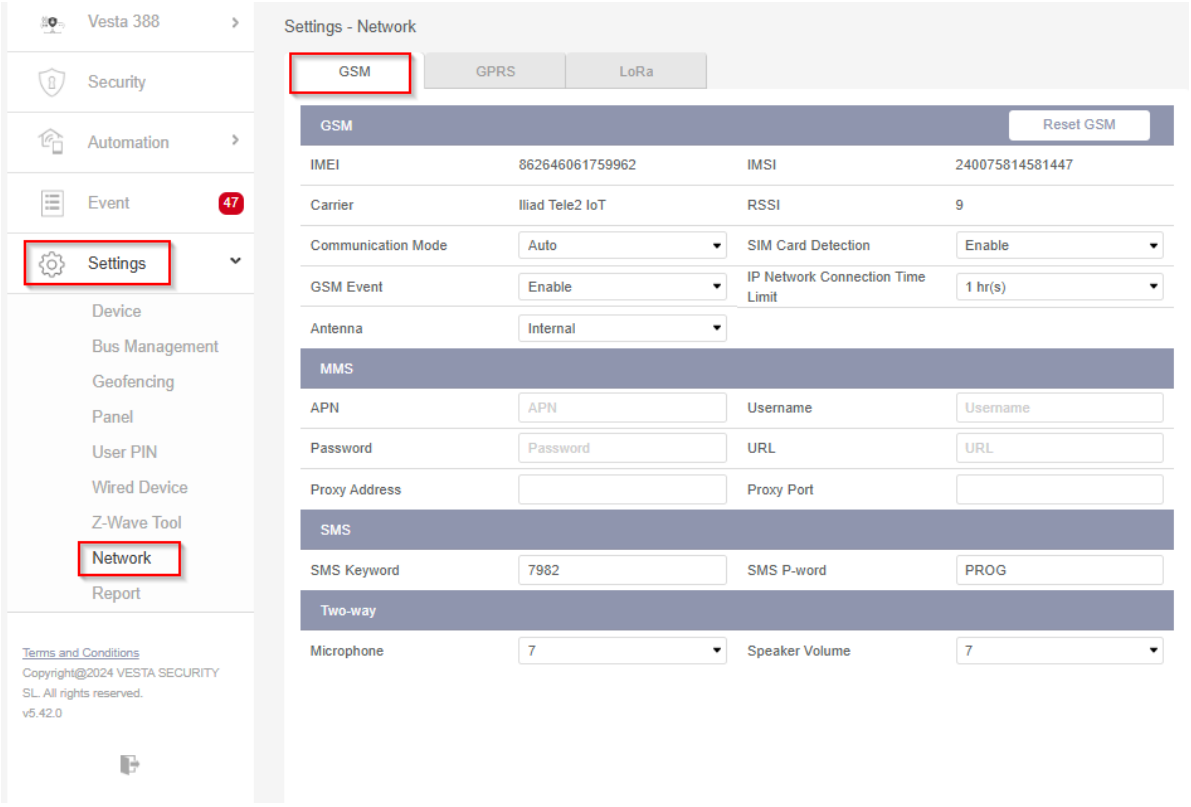


Zone Connection

Note! The resistive values within the same loop can be chosen [1k, 2.2K, 3.74K, 4.7K, 5.6K, 6.8K, 8.2k, 10K] but it must be the same for the 2 resistors except for loop 9 and 10 which is intended for 3xEOL detectors that have antimasking, alarm contact and tamper. In this case, the resistance values marked in the scheme must be respected

10.8 Network Settings: GSM

GSM/GPRS/LORA

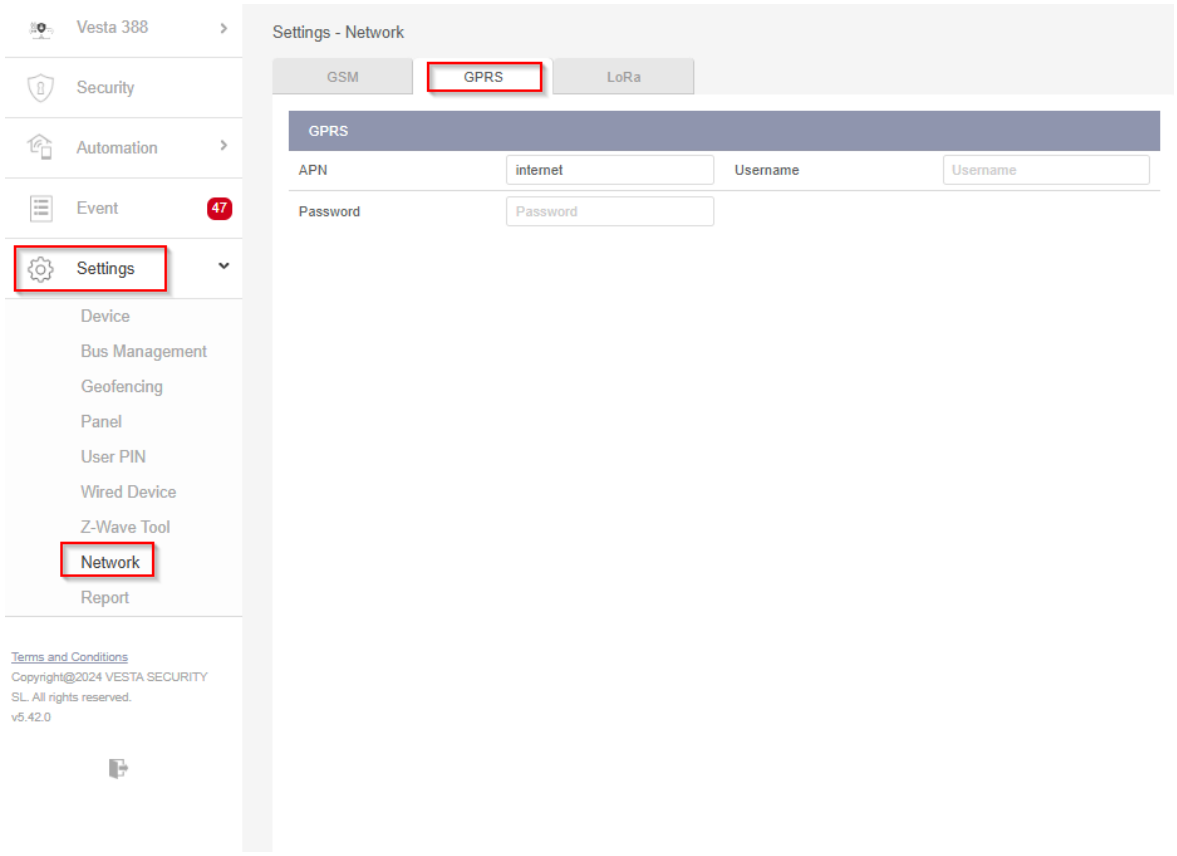


By accessing the GSM subsection, the following info is displayed:

1. GSM operator: with which panel it is connected
2. GSM signal level [0-9] where 0 implies no GSM coverage and 9 excellent signal
3. SIM Card Detection. It is possible to enable/disable the GSM communicator.
4. GSM Event: In case of recurring failures due to lack of coverage, this event can be disabled.
5. IP Network connection time limit:
   a. Facilities with dual communication track, recommended to select 1h.
   b. For Installations with only GPRS/LTE communication, select disable.
6. Antenna: if you connect a GSM amplifier antenna to the external connector, you must enable it using this parameter

10.9 Network Setting: GPRS

GSM/GPRS/LORA



Access the GPRS subsection to configure the APN and be able to go out to the internet and communicate the panel via GPRS/LTE communicator.

You can ask your operator about the SIM APN and if you do not know it you can write to

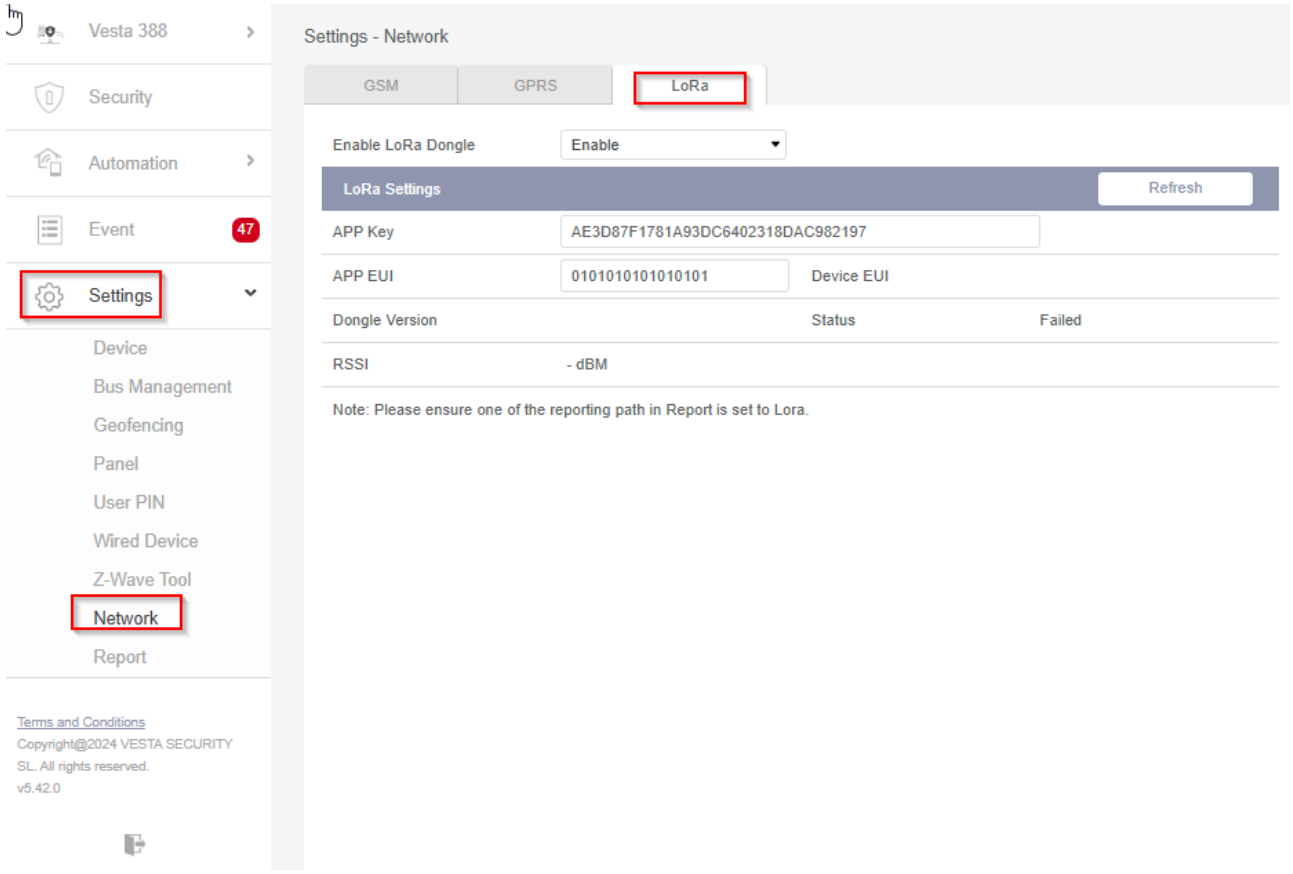
APN: internet

User: [Leave blank]

Password: [Leave blank]

10.10 Settings: LORA

GSM/GPRS/LORA



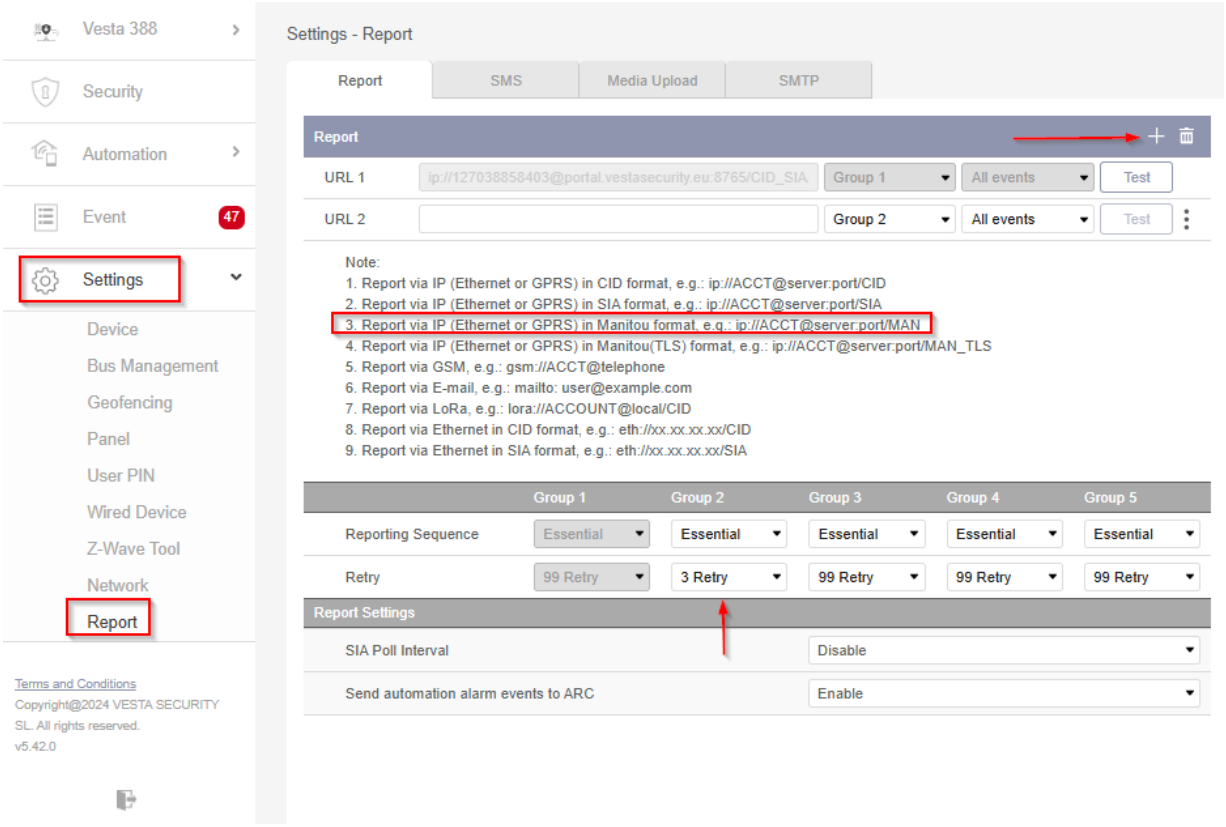
By accessing the LORA subsection, this 3rd communication route can be enabled.

In this way, in the event of an IP drop via ethernet (main path) or IP via GPRS/LTE (2nd backup path) we will be able to transmit the panel events via LORAWAN (3rd backup way) and keep the panel connected with CRA while the other ways are not available

For more information, please contact your Sales Agent or Tech Support Vesta. Specific manual available for LORA communication configuration

10.11 CRA Connection Settings: Events

Setting →Report →Report / Captured File



Within the REPORT subsection, you can configure the data of your event receiver. Simply clicking on the "+" button opens another field to connect to the CRA.

In the Note section, you will find all the supported formats, as well as examples of the URL string to be configured. The standard format with which you must connect is the one shown in example nº3 [MANITOU]

- Subscriber: subscriber number agreed with CRA
- Server: CRA public IP
- Port: CRA Public Port

/MAN, refers to the transmission of events in manitou format. Our CRA gateway, ALARMSPACE, will be responsible for converting events into a language suitable for existing receiver software.

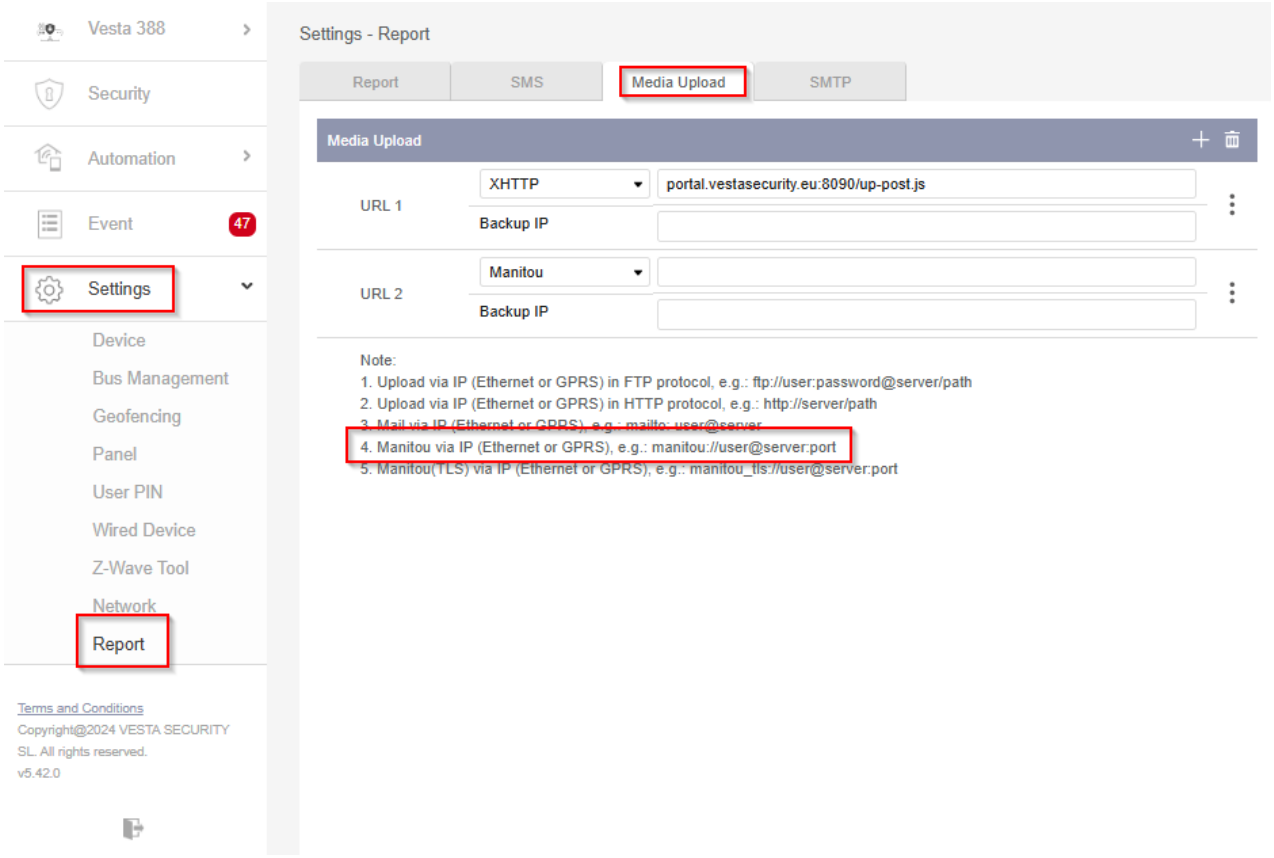
Group: Events will be streamed to all URLs that belong to different groups. URLs within the same group will act as a backup and the event will only be transmitted to one of them starting in list order (URL1,2,3...).

Note! To connect to a CRA direct the URL to group 2 since group 1 is predefined for the VESTA cloud.

Process again: 3/5 retries recommended for all groups

10.12 CRA Connection Settings: Images

Setting →Report →Report / Captured File



Within the Captured File subsection, you can configure your receiver's data to receive photo frames generated by existing CAM PIRs or IP cameras.

Simply clicking on the "+" button opens another field

to connect with the CRA.

In the Note section, you will find all the supported formats, as well as examples of the URL string to be configured. The standard format with which you must connect is the one shown in example nº4

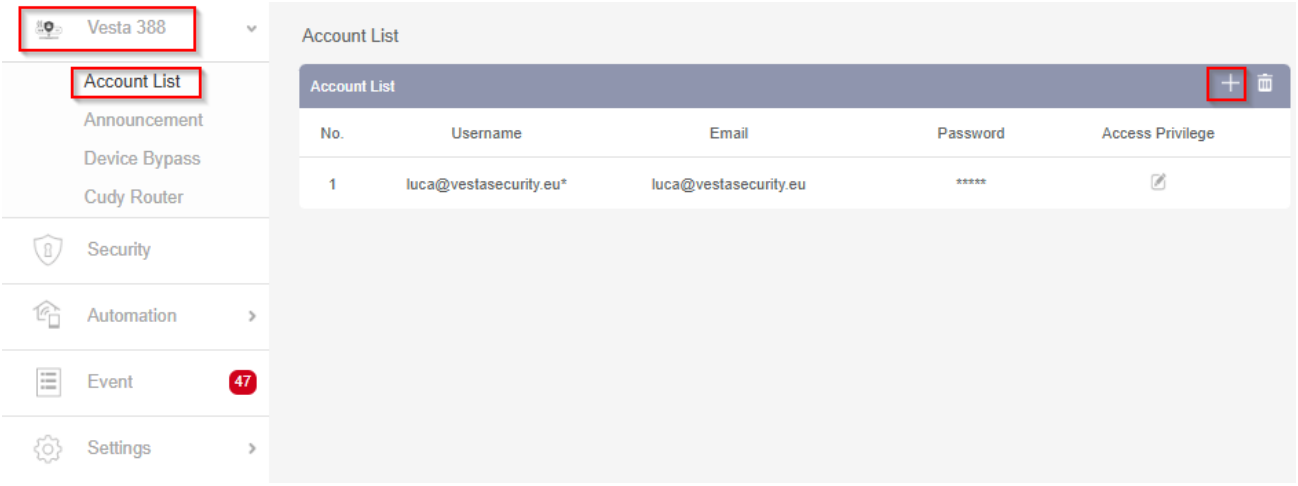
- User: subscriber number agreed with CRA
- Server: CRA public IP
- Port: CRA Public Port

From the drop-down menu, select MANITOU protocol. Our CRA gateway, ALARMSPACE, will be responsible for receiving the photos and transmitting them to the CRA software

11. Share the dashboard with the client

The installer will be in charge of creating an account (sharing the App with the client) so that the end user can control their system remotely from the App or platform WEB SmartHomeSec

[1] Enter Panel name → [2] Enter Account List → [3] Select **Add**



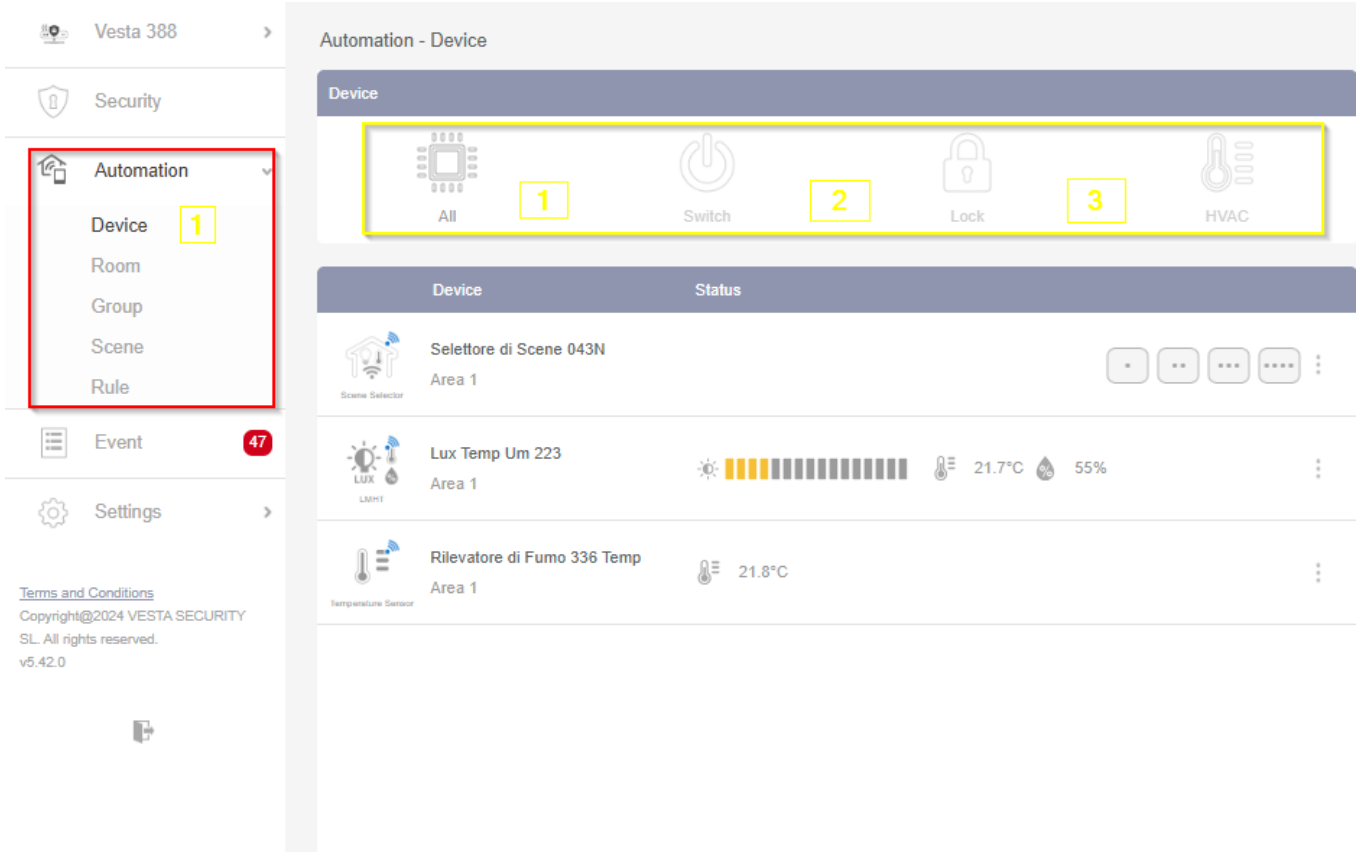
Note! As a security measure, the installer has 15 min. after feeding the panel to share with the 1st user on the list. In case of exceeding this time, simply restart the panel by disconnecting the main power + battery. That is why it is recommended to perform this step immediately after the registration of the panel. For the following shared users there is no time limit

If it's a **new customer**, select **Create an account**, and if the customer already has other panels, select

Link to an existing account or create a new one

12. Share the dashboard with the client

[1] Device



There are 3 subsections: [1] Devices, [2] Room [3] Scene, [4] Rule

[1] Device: All automation-related equipment is listed and displayed. From here, each of the home automation modules can be controlled (activated/deactivated) individually and at any time.

A filter is available at the top that organizes each of the modules by families, very useful in case of a large home automation installation.

Filter by family:

[1] All equipment

[2] Switches (on/off)

[3] Electronic locks

[4] Thermometers/thermostats

12.1 Sharing the Dashboard with the Client

Scenes allows you to set a group of actions that the Control Panel can perform with your home automation devices. The user can program the scene to manually activate a set of devices, or activate them automatically using a pre-programmed rule (See the Rules section for more details on smart actions.)

Example Scene:

SCENE: LEAVING HOME

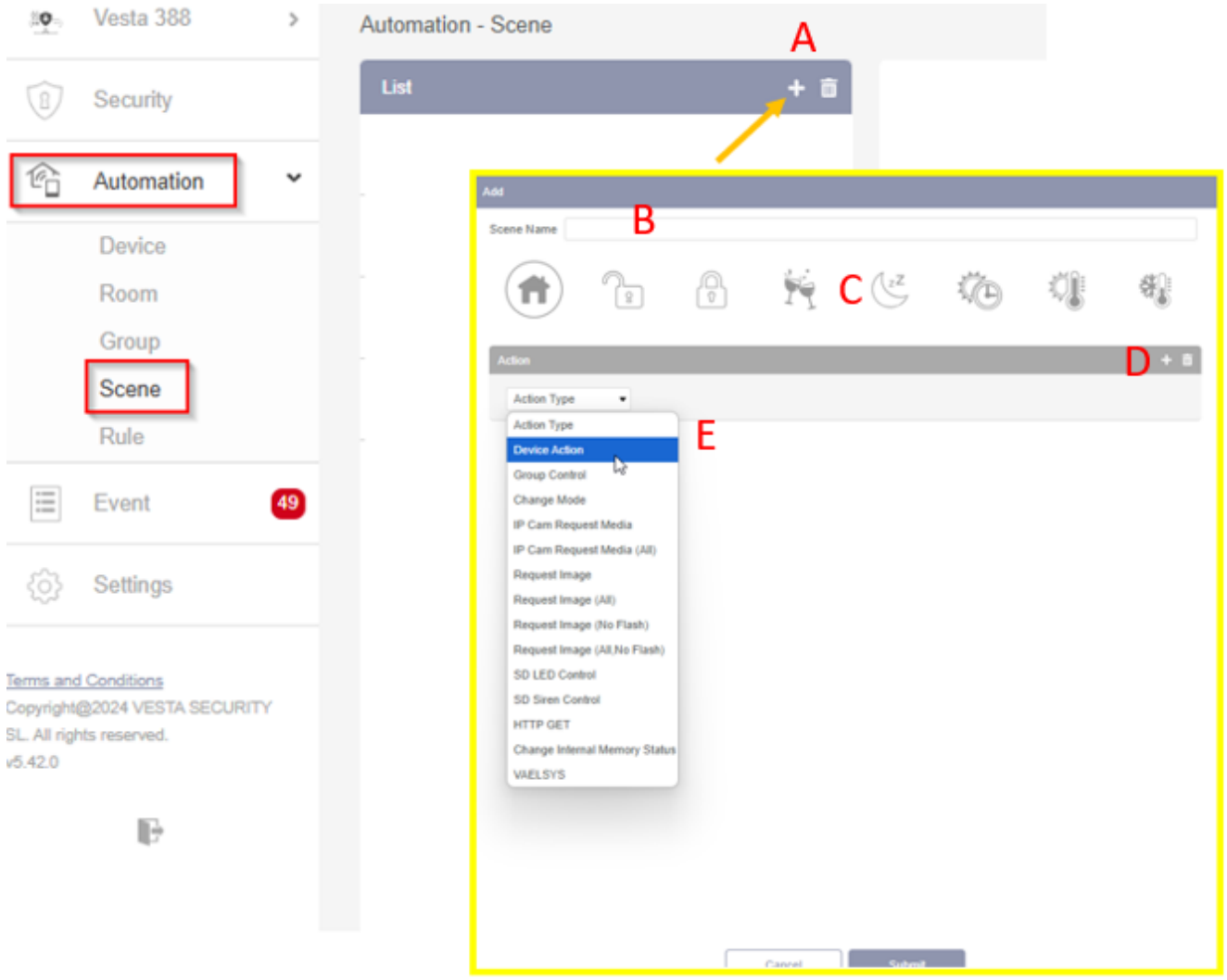
ACTIVACIÓN DE LA ESCENA	DISPOSITIVOS IMPLICADOS	ACCIÓN DEL DISPOSITIVO
La activación de las escenas puede ser de varias maneras como por ejemplo: Un selector de escenas, Geofence, con un dispositivo como un detector/contacto magnético ...etc o con Reglas	Enchufe del Salón	APAGAR
	Luces de la casa	APAGAR
	Calefacción	AJUSTAR TEMPERATURA A 22ºC
	Televisor	APAGAR
	Panel: Cambiar modo	ARMADO

As can be seen in the Example, this scene can be activated with a device such as a detector, magnetic contact, Geofence, scene selector, APP/WEB or rulers... When you activate the scene in the example, the living room socket will be turned off, the lights will be adjusted, the temperature will be set to 22ºC, the TV will be turned off and finally the panel will be switched to ARMED mode. Therefore, with just one scene action we control the status of all the desired devices and adjust them to the desired needs.

Summary: *Rule Activation*Conditions=Actions to Be Performed*

12.2 Sharing the Dashboard with the Client

[2] Scene



Note! A maximum of 10 different Scenes can be created and each with a maximum of 5 different Actions.

A. **Add Scene**
B. Name the Scene
C. Select an "Optional" Icon
D. **Add/Delete** Action.
E. Configuration of the actions to be performed:

In the photo Ex:

- Action 1: Turn Off Light Device
- Action 2: Activate Device

12.3 Sharing the Dashboard with the Client

To save the settings, select Send

The Rule subpage allows you to set a list of rules under certain conditions. For example, you can determine which device will wake up in a pre-programmed lux level range, temperature range, or calendar. You can also select the type of action to perform, or simply apply the previously created scene under the Scene subpage (Section - Scene).

Example Scene:

RULE: AUTOMATIC WATERING

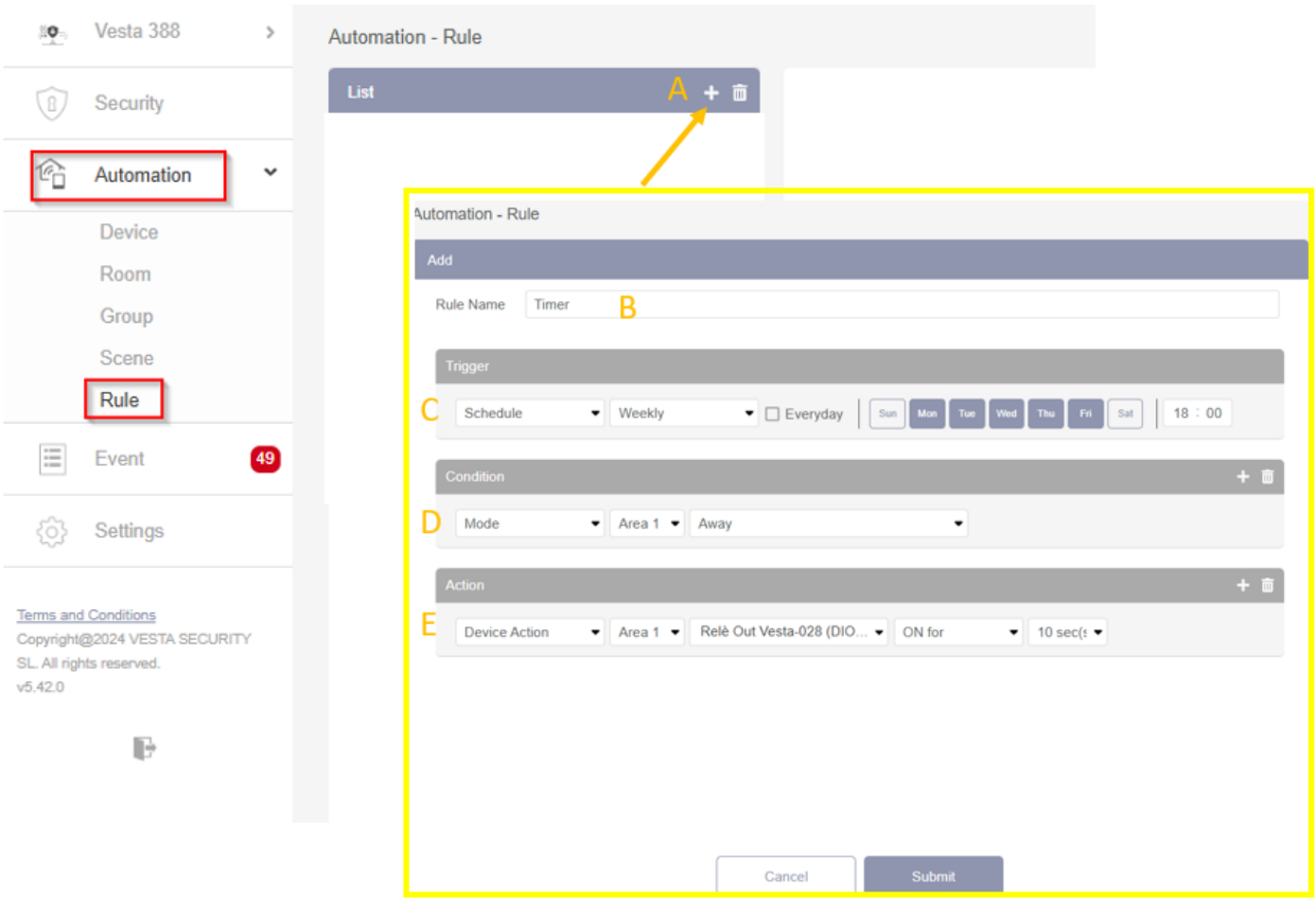
ACTIVACIÓN DE LA	DISPOSITIVOS	ACCIÓN DEL DISPOSITIVO
La activación de la regla, puede ser mediante calendario, sensores, cambio de modos (Armad/desarmado...), Detección por de movimiento por un tiempo... En este ejemplo: **Calendario – De lunes a Viernes a las 18:00h**	Sistema: Armado	Activar Relé de la Electoválvula durante 10 minutos

As can be seen in the Example, this Rule triggers from Monday to Friday at 6:00 p.m., In conditions* is optional, in this case the IF rule will always be fulfilled: it is a day from Monday to Friday at 6:00 p.m. AND the system or panel is armed, Then the solenoid valve relay will be activated for 10 minutes or the desired time.

Summary: *Rule Activation*Conditions=Actions to Be Performed*

12.4 Home automation: Rule

[3] Rule



Note! A maximum of 100 different Rules can be created

A. **Add** Rule
B. **Name** the Rule
C. Select how this rule is to be triggered.
   E.g.:
   Calendar
D. Conditions "Optional"
E. **Configuration** of the **actions** to be carried out once the above conditions have been met.
   Ex:
   *Action 1: Activate the solenoid valve relay for 10 minutes. (e.g. automatic irrigation)

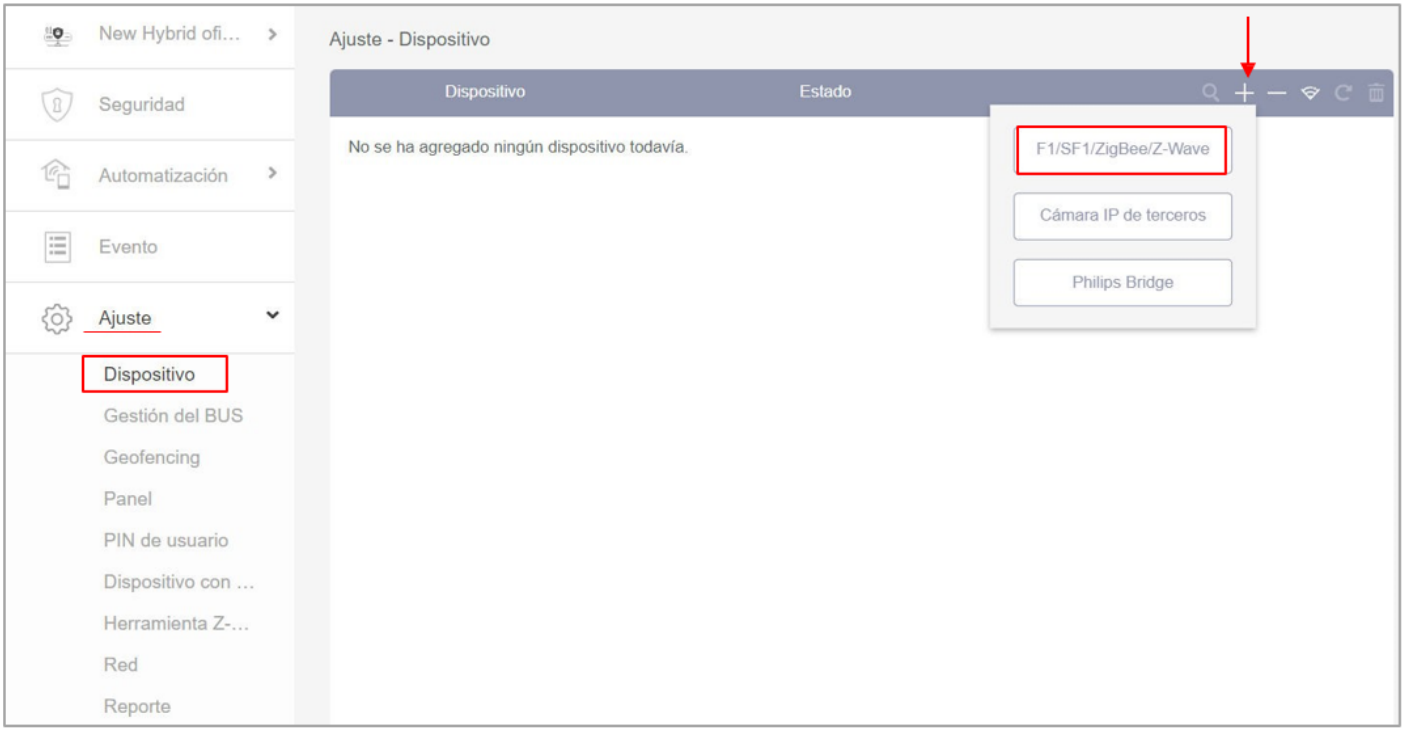
To save the settings, select **Submit**.

Addendum: V-MAX BUS Management and Configuration

This addendum specifically discusses the software and hardware options available for system configuration and management using the proprietary V-MAX BUS technology. V-MAX devices are compatible with HYBRID-IMAX panel models only. In addition, the document will specify connection topologies, current V-MAX BUS devices, and various recommendations to maximize the communication quality of the system

INDEX

Device: Add Device



Simplified process for the registration of

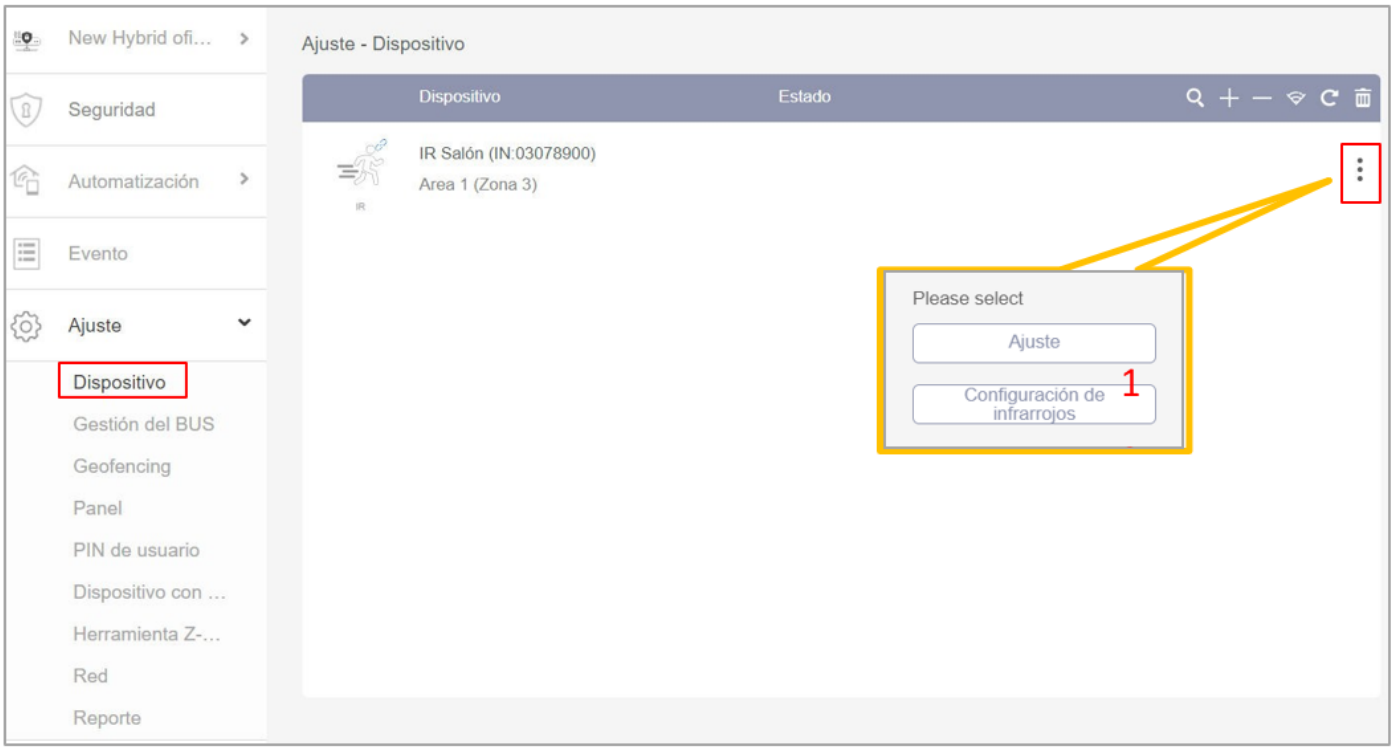
BUS devices

1. Adjustment
2. Device
3. Click on "+"
4. Devices

At this point the system enters BUS recognition mode and will display all connected devices in a list [next page]

¡Dispositivo agregado con éxito!

Device: Internal device settings

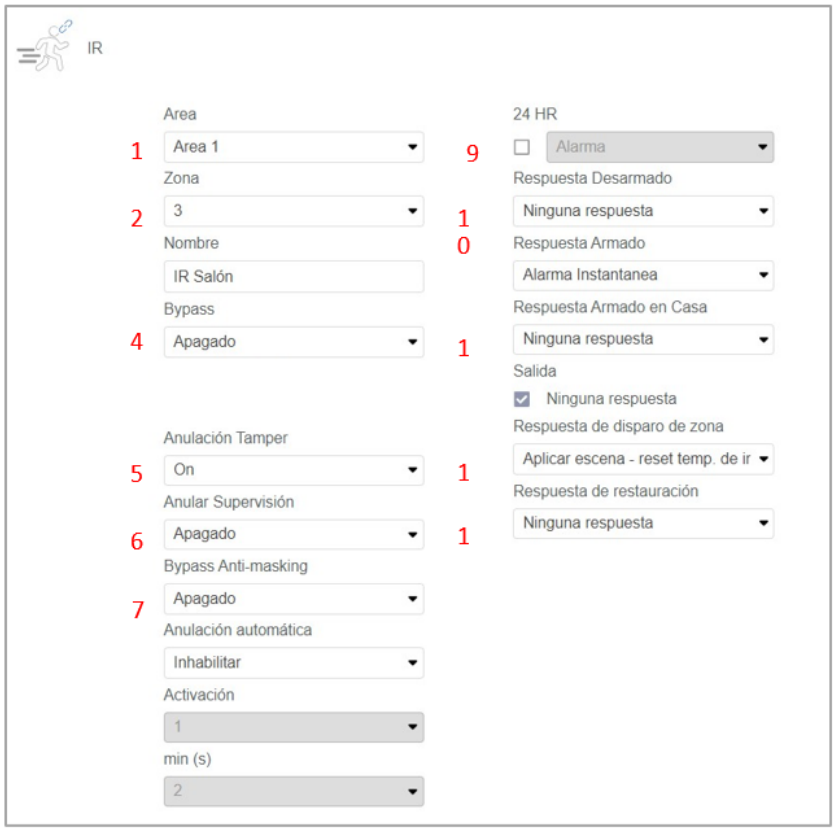


Note! Each detector will have different settings depending on its nature. Below is a summary of the overall settings based on a PIR V-MAX

1. Zone Settings
2. Infrared settings

Device: Zone and sensitivity adjustment

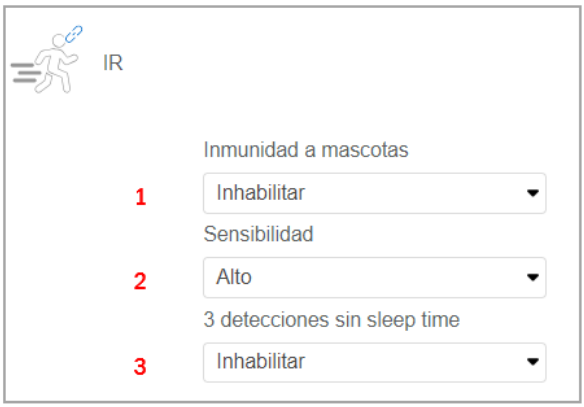
AJUSTE DE ZONA



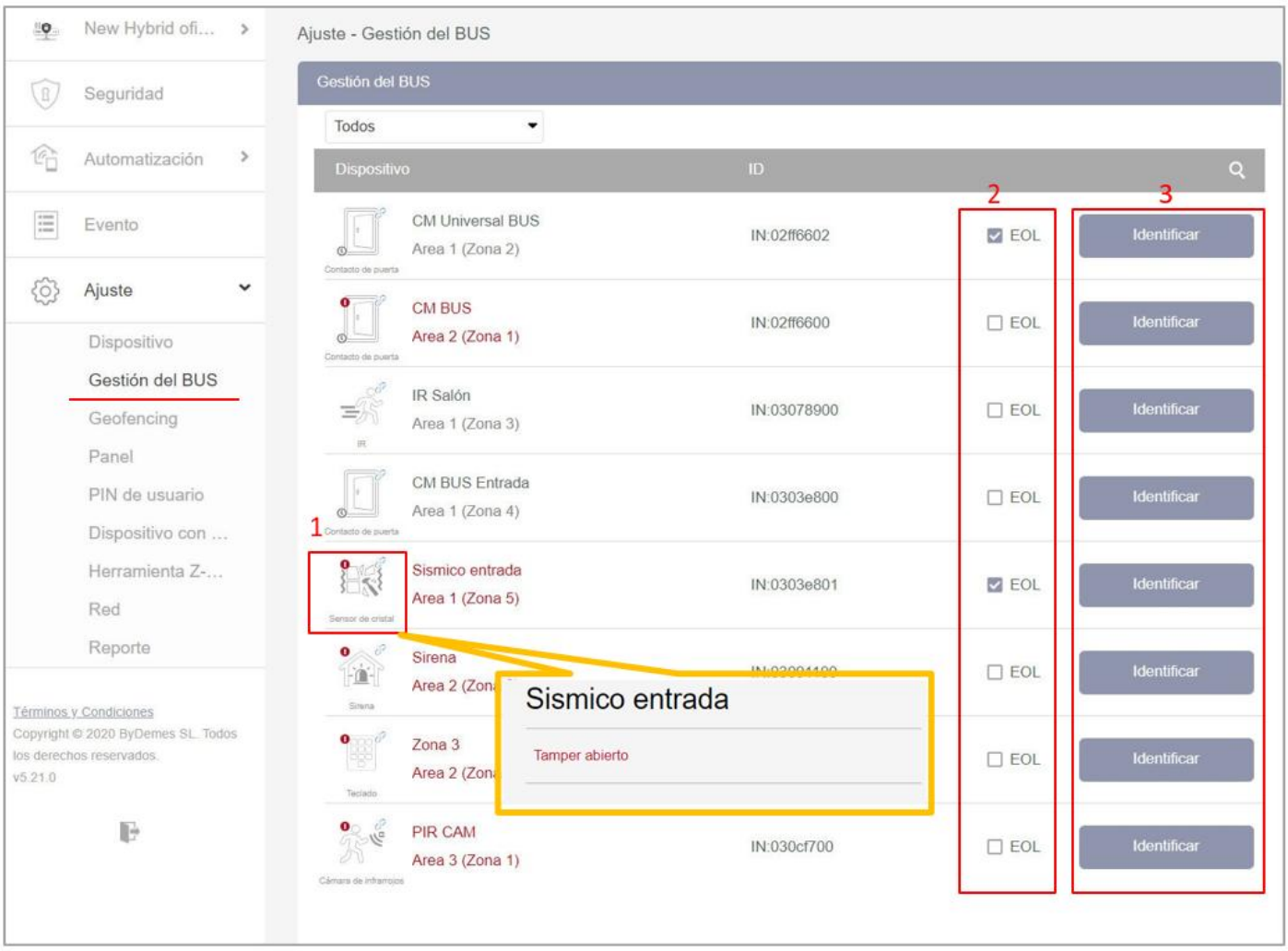
1. Seleccionar Área [1/2/3/4/5/6/7/8]
2. Seleccionar Número de zona de [1-80]
3. Asignar un Nombre de zona [“IR Salón”]
4. **Bypass ON** → Anular zona
   Bypass OFF → Habilitar zona
5. Anular tamper → ON/OFF
6. Anular supervisión de zona
7. Anular anti-masking
8. Auto anulación tras x activaciones en y minutos
9. Zona 24h
10. Reacción de zona con el panel **Desarmado**
11. Reacción de zona con el panel **Armado**
12. Reacción de zona en **Armado en Casa**
13. Aplicar Escena al detectar
14. Aplicar Escena al restaurarse

SENSIBILIDAD

1. Inmunidad mascotas: **ON /OFF**
2. Sensibilidad
   - Alto
   - Bajo
3. Activaciones consecutivas antes de entrar en modo sleep:
   - Inhabilitar = 1 activación → Sleep time 1 min.
   - Habilitar = 3 activaciones → Sleep time 1 min.



No actuar
Retardo de entrada 1
Retardo de entrada 2
Timbre
Alarma de seguimiento Alarma instantánea Alarma Exterior
Alarma silenciosa Zona cruzada



This section filters only the elements that make up the BUS, reflecting the area and zone that each element occupies.

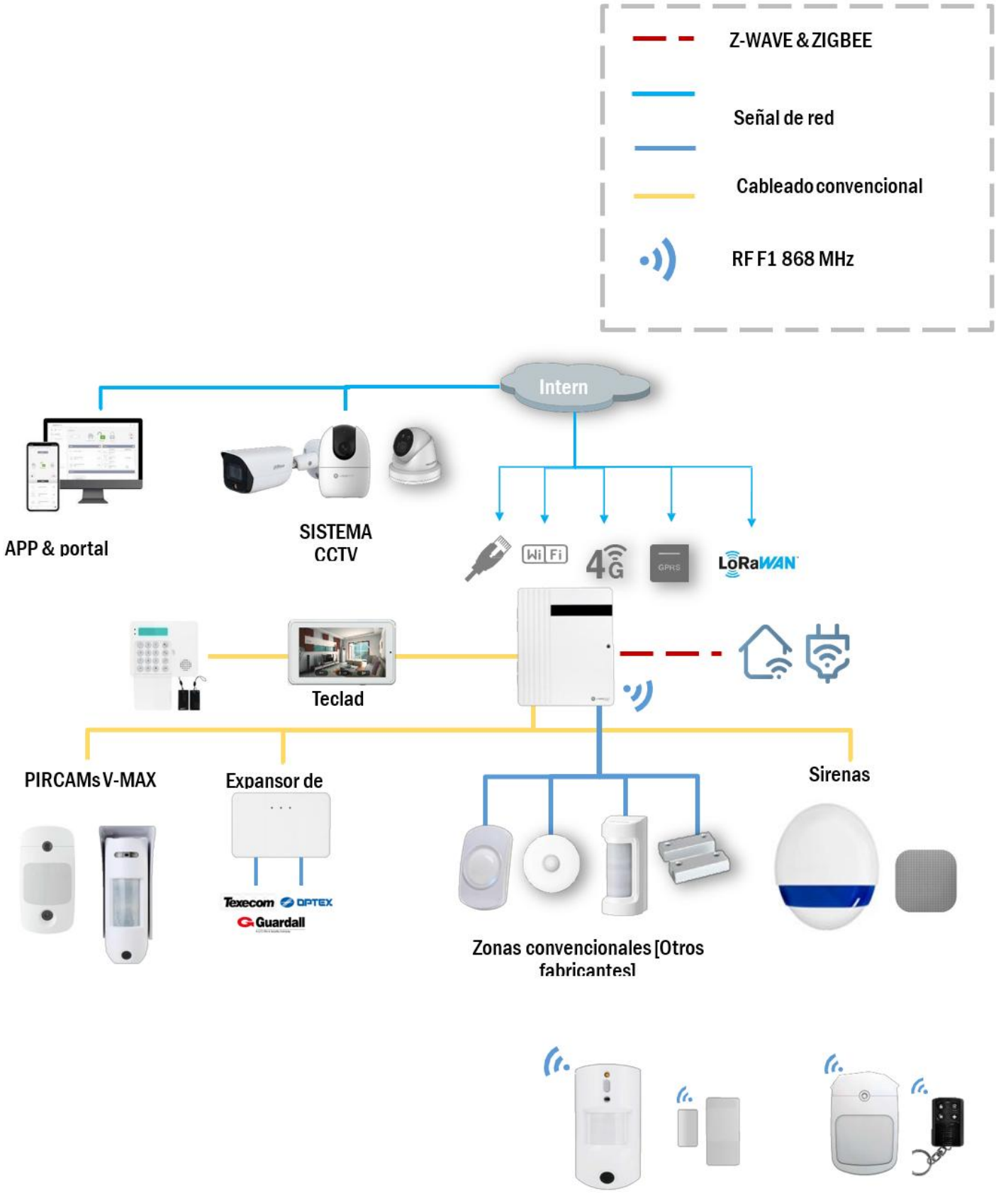
1. If an area suffers a technical breakdown, it will be reflected in red with the warning symbol. Clicking on it will display the type of fault

2. EOL The technician will manually mark those BUS elements that are line ends. It serves only as information so that at a glance you can identify them.

   Note! Those final elements of the line will be placed on the bridge intended for this purpose. See manual attached to each equipment.

3. Very useful tool to physically identify each element. By clicking on the button, the corresponding element will respond by illuminating or flashing the relevant LED.

Annex: VESTA hybrid panel architecture



Appendix: V-MAX BUS Topologies

Case 1a: An interior BUS line

*Max. 128 BUS devices

Flexible Cabling

Some of the features to highlight of the V-MAX BUS system are:

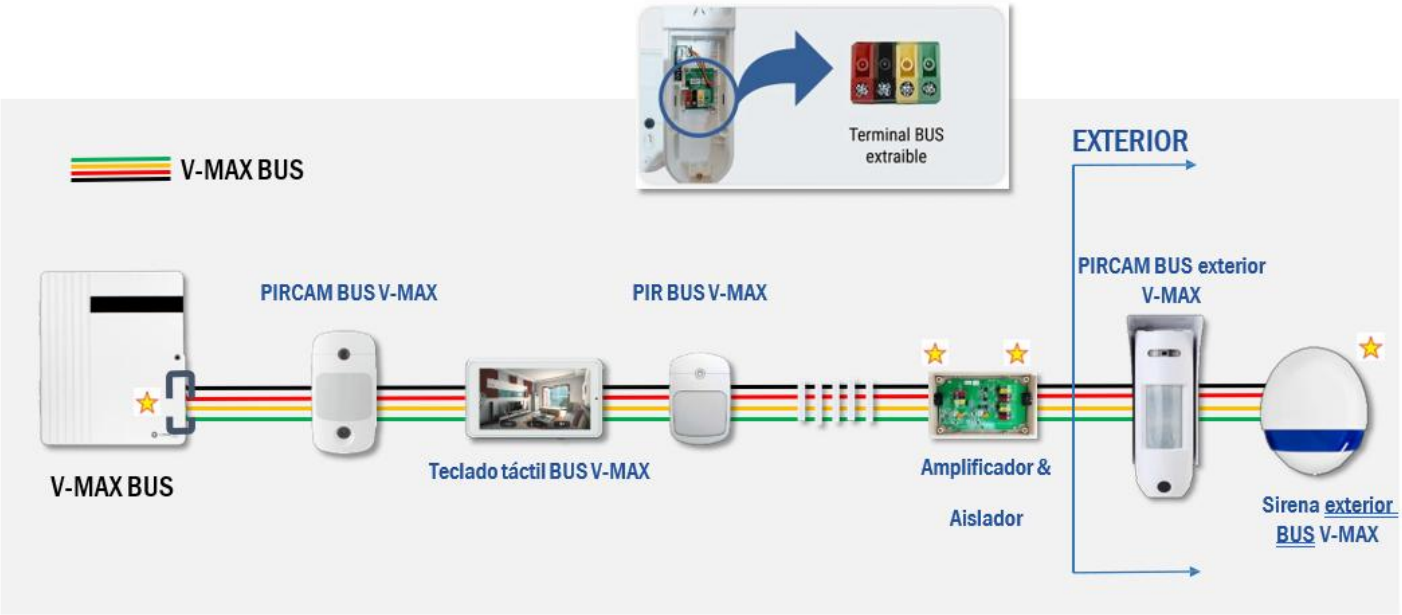
- Bi-directional adjustments for any team
- Instant monitoring
- Ease of installation and configuration
- PIR CAM BUS in GRADE 3
- PIR CAM BUS exterior
- Alarm photos of CAM PIRs in HD (720p) almost instantaneously
- Instant, high-quality photos on demand
- Great flexibility being able to opt for proprietary BUS elements or by interposing conventional detectors with a simple integration "pickup" (vesta-399)
- Supervised sources with real-time monitoring of the current and voltage supplied
- Galvanically isolated I/O amplifiers
- and much more....

Schematic: jumper configuration (end of line resistance)

The use of the jumper is recommended to improve BUS communications in terms of reliability and speed. In this case, the jumper will carry the ends of the branch: panel and last element.

Case 1b: An Inside and Outside BUS Line

*Max. 128 BUS devices

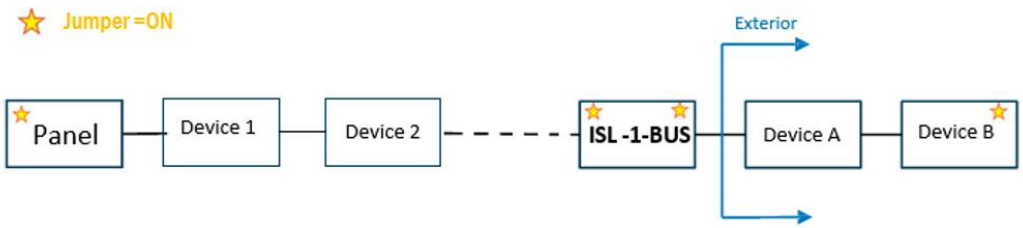


Flexible Cabling

When we go outside with the BUS, it is highly recommended, although not mandatory, to use the isolator. Galvanically insulated, it will protect the interior from any sabotage attempts from the outside.

Outline: jumper configuration (End of Line Resistance)

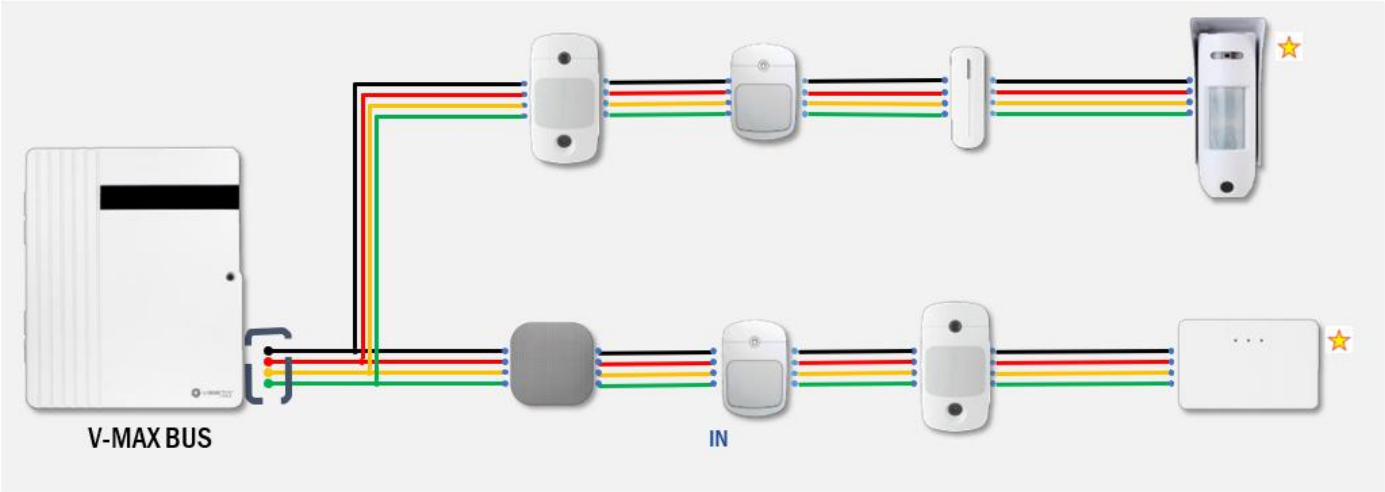
The use of the jumper is recommended to improve BUS communications in terms of reliability and speed. In this case, **the amplifier & isolator behaves as the end and start of a new independent branch** and therefore the jumpers are placed as follows the scheme.



Case 2a: Two (inside) star bus lines

*Max. 128 BUS devices

Flexible Cabling



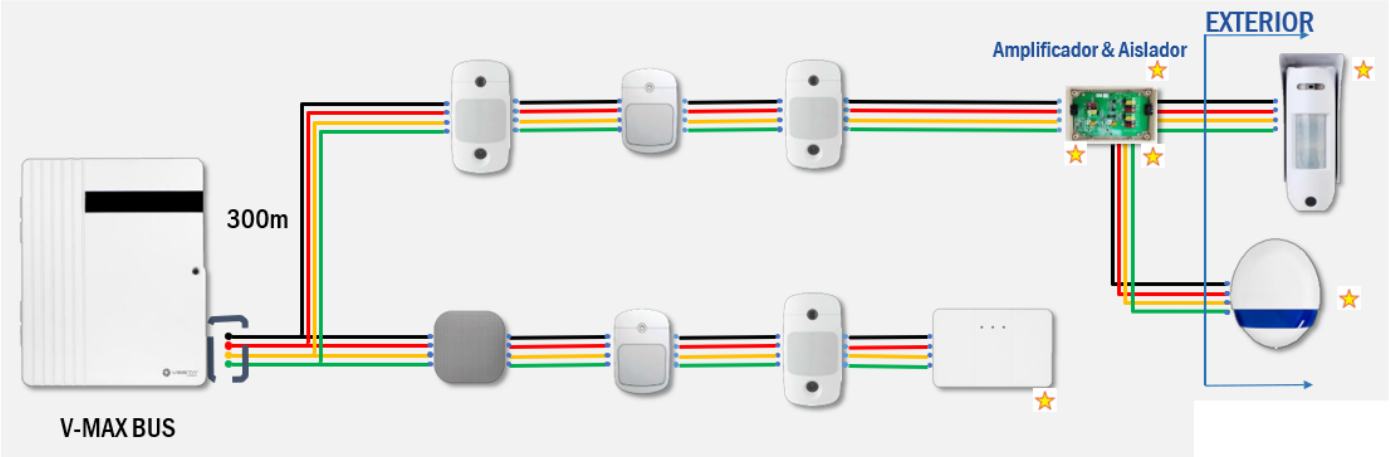
Outline: jumper configuration (End of Line Resistance)

Jumper =ON

The use of the jumper is recommended to improve BUS communications in terms of reliability and speed. In this case, **they will carry the jumper the last element of each branch**.

Case 2b: Two BUS lines (indoor & outdoor) in star

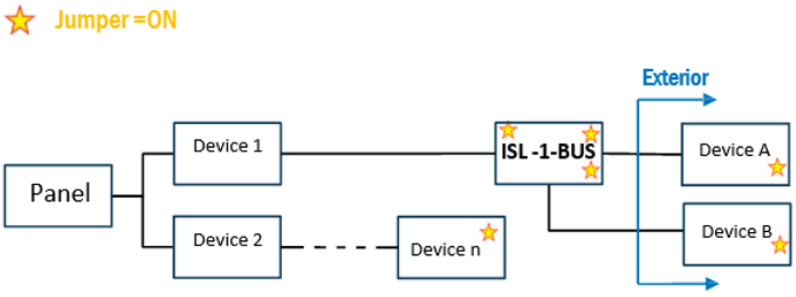
*Max. 128 BUS devices



In this case, the use of an amplifier & insulator is recommended in order to protect the installation against sabotage from the outside: short circuits, cable cutting, etc...

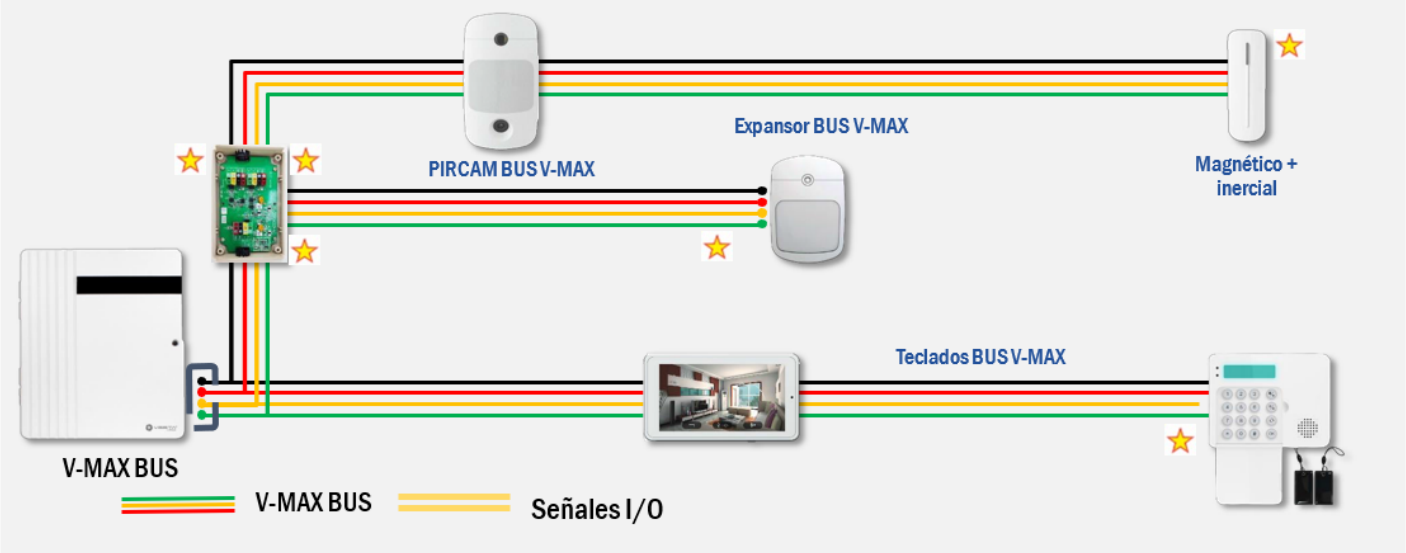
Schematic: jumper configuration (end of line resistance)

The use of the jumper is recommended to improve BUS communications in terms of reliability and speed. In this case, **the amplifier & isolator behaves as the end and the beginning of 2 new independent branches** and therefore the jumpers are placed as follows the scheme.



Case 3a: Three Star BUS Lines WITH Amplifier & Isolator

*Max. 128 BUS devices

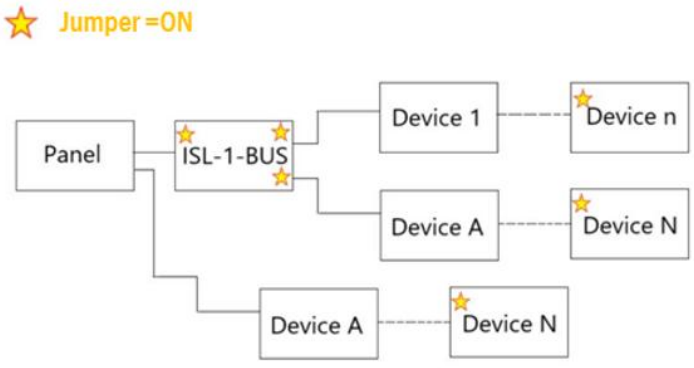


Flexible Cabling

In this case, the use of an amplifier & isolator is recommended with the sole objective of branching the BUS by 2 stars or higher (total of 3 or higher). The use of this device allows filtering, amplifying and stabilizing communications, so that the technician's only concern is the load applied to the BUS (detector consumption) and not the distances measured in accumulated cable

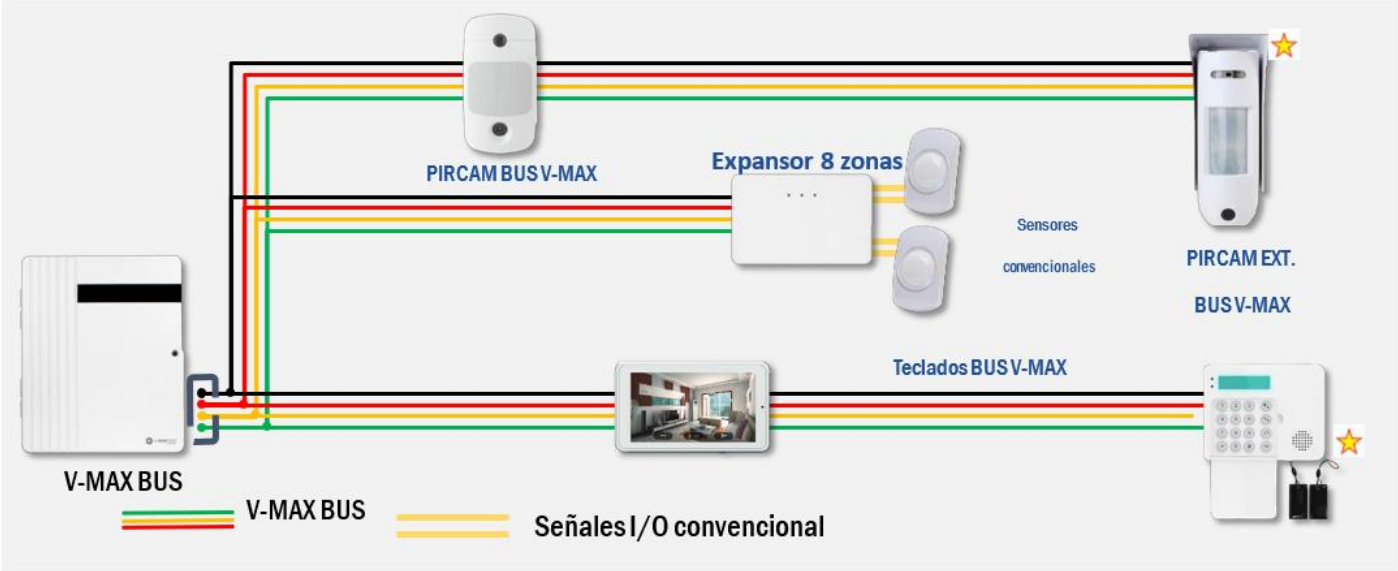
Schematic: jumper configuration (end-of-line resistance)

The use of the jumper is recommended to improve BUS communications in terms of reliability and speed. In this case, the amplifier & isolator behaves as the end and the beginning of 2 new independent branches and therefore the jumpers are placed as follows the scheme



Case 3b: Three Star BUS Lines WITHOUT Amplifier & Isolator

*Max. 128 BUS devices

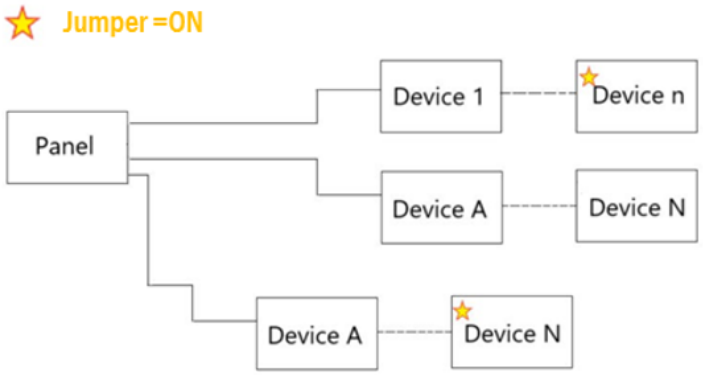


Flexible Cabling

Among the many advantages of using the VESTA hybrid panel for wired installations, is not only the possibility of wiring up to 16 conventional zones directly on the panel board, but it is also possible to expand as many conventional zones as we need by means of expanders connected to any point of the BUS. This example is used and shows how to connect the 8-zone expander, encapsulated, tamper-protected and with built-in battery backup.

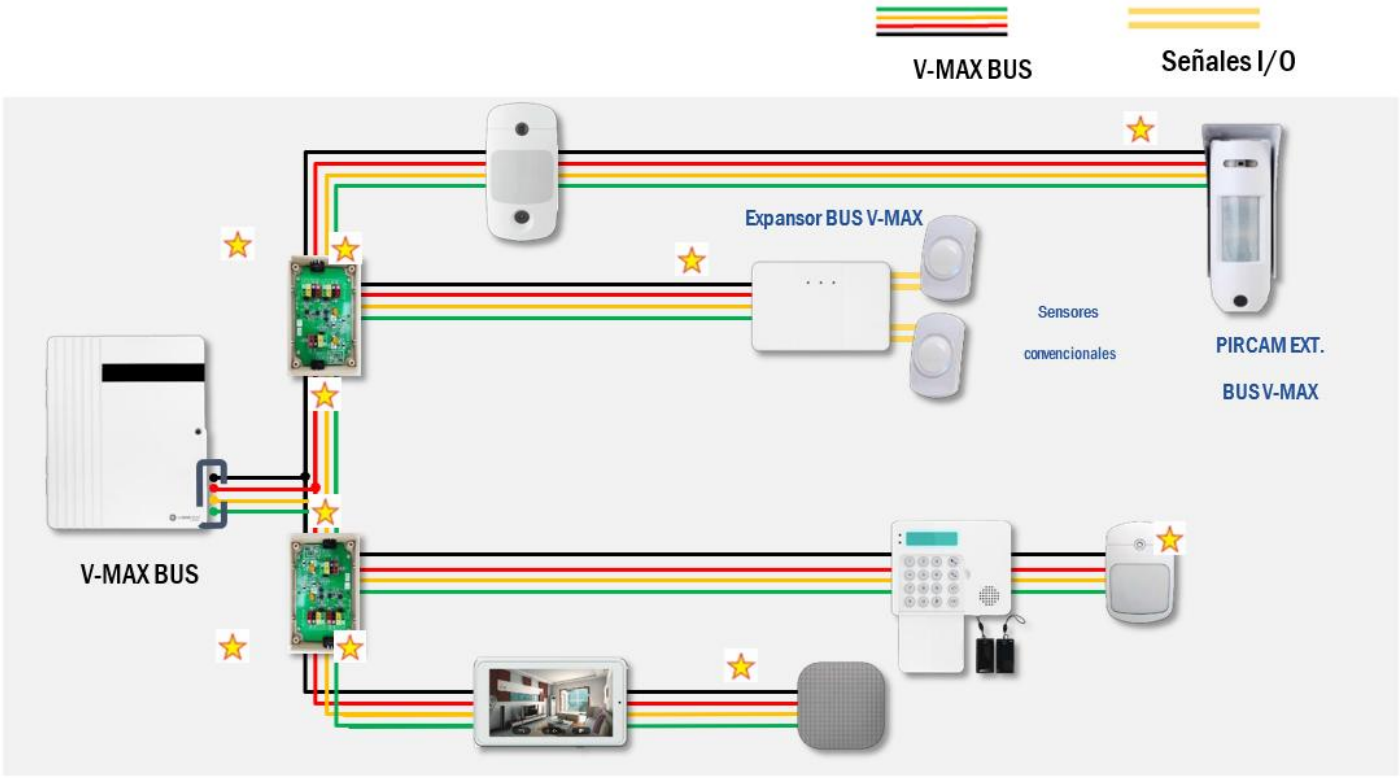
Schematic: jumper configuration (end-of-line resistance)

The use of the jumper is recommended to improve BUS communications in terms of reliability and speed. In this case, it is recommended **to place the jumper on the longest branch(es) in accumulated cable distance**



Case 4: four BUS lines in Estrella

*Max. 128 BUS devices

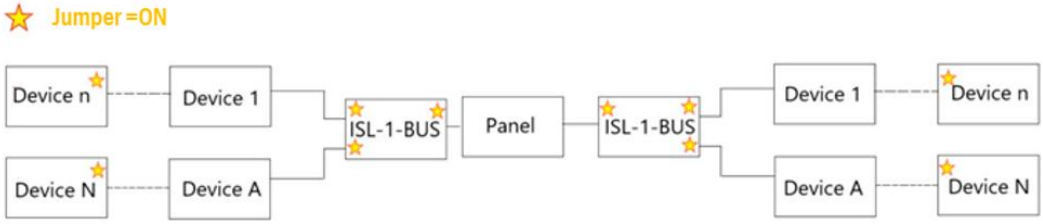


Flexible Cabling

Among the many advantages of using the VESTA hybrid panel for wired installations, is not only the possibility of wiring up to 16 conventional zones directly on the panel board, but it is also possible to expand as many conventional zones as we need by means of expanders connected to any point of the BUS. This example is used and shows how to connect the 8-zone expander, encapsulated, tamper-protected and with built-in battery with backup function

Schematic: jumper configuration (end of line resistance)

The use of the jumper is recommended to improve BUS communications in terms of reliability and speed. In this case, **the jumper will be placed at the start and end of each of the independent branches that are generated in each amp & isolator module.**



Appendix: BUS Calculator

- The maximum distance of 300m between elements must not be exceeded. For example, between the panel and the keyboard or between the keyboard and the expander, it should not exceed the indicated distance

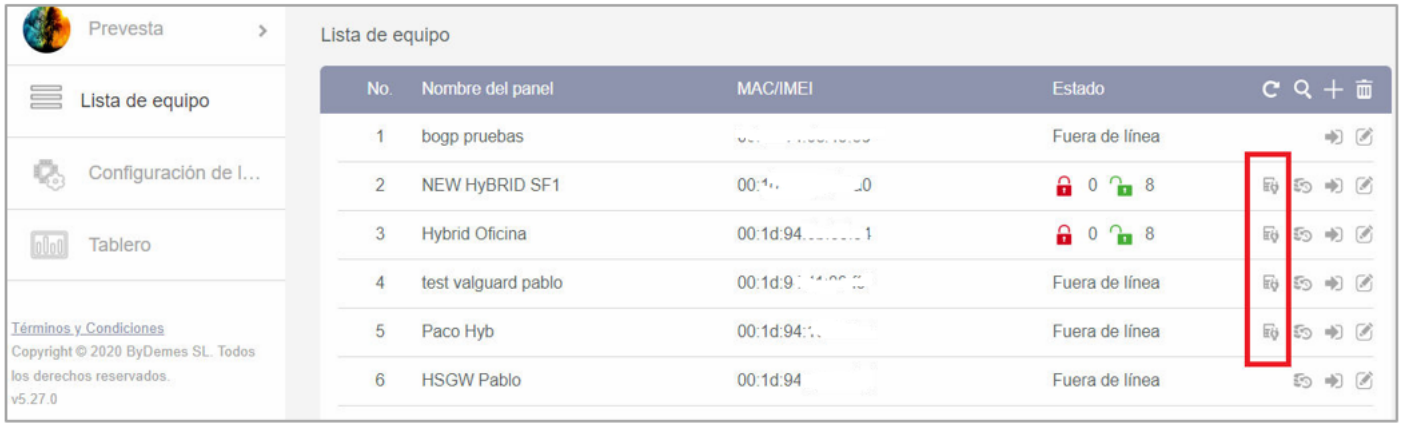
- The maximum achievable distance (in accumulated cable) will depend on the consumption and voltage at each point. If sufficient current and voltage is guaranteed in each device, the system will function properly

- It is very important to know the current required by the system (use the calculator or the consumption table of each device for this)

- Take into account the voltage drop due to losses in the cable (use calculator). If voltage drops are observed in the design or during commissioning, it will be necessary to install a supervised source or an amplifier & isolator according to the specific needs of each case.

- To implement star topologies, it is recommended to build on the 3 previous cases and make use of the amplifier & isolator

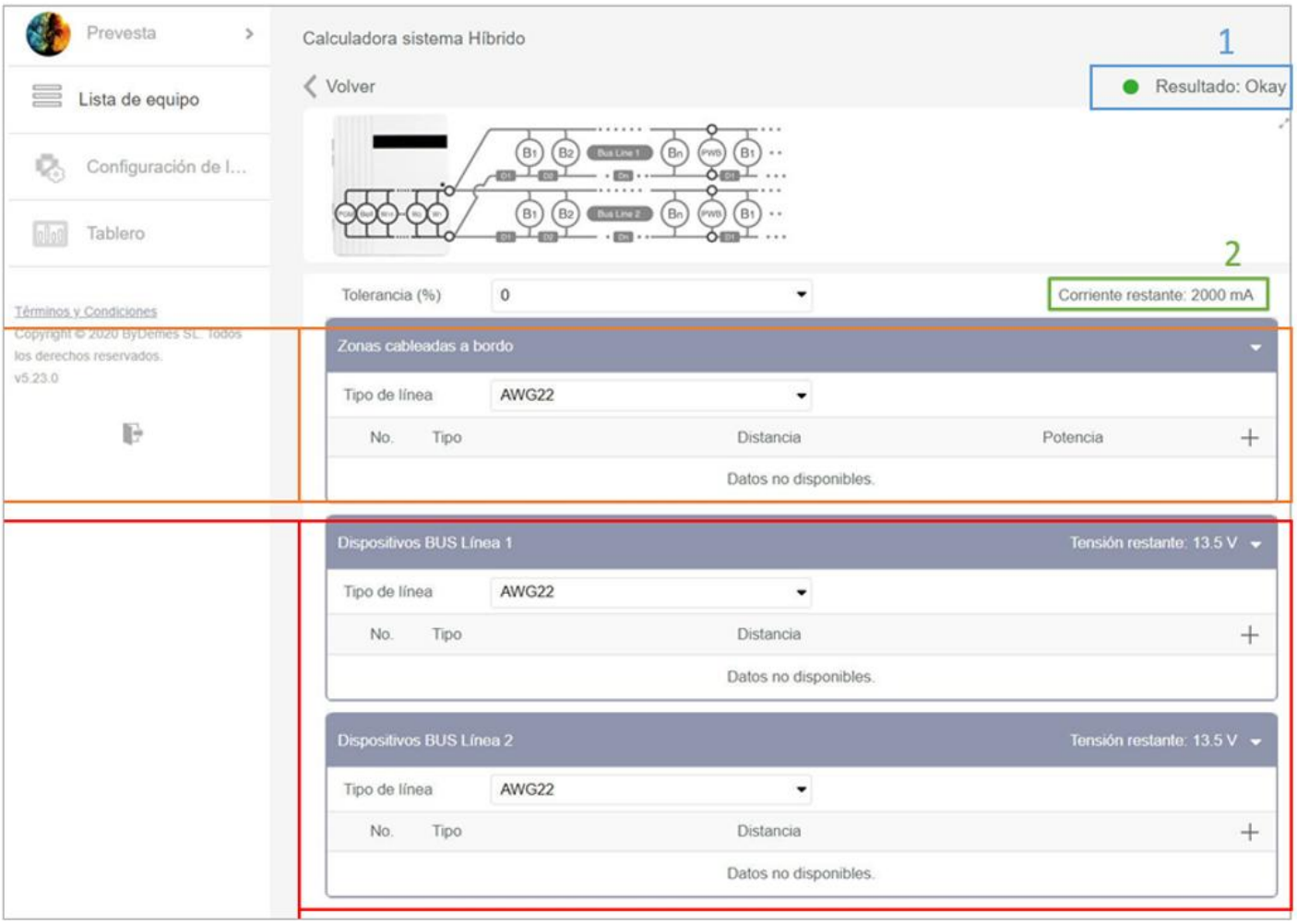
- End-of-line resistors are a key tool for improving and stabilizing communications over long distances (see topologies cases above)



The technician has access from the APP or SHS WEB to the BUS calculator. This tool allows the system to be sized correctly prior to installation. This will reduce the operating costs involved in last-minute incidents such as not enough voltage reaching the elements due to the poor choice of a cable, the need to add a backup power supply, type of cable, etc.

The only data to be provided on the platform are:

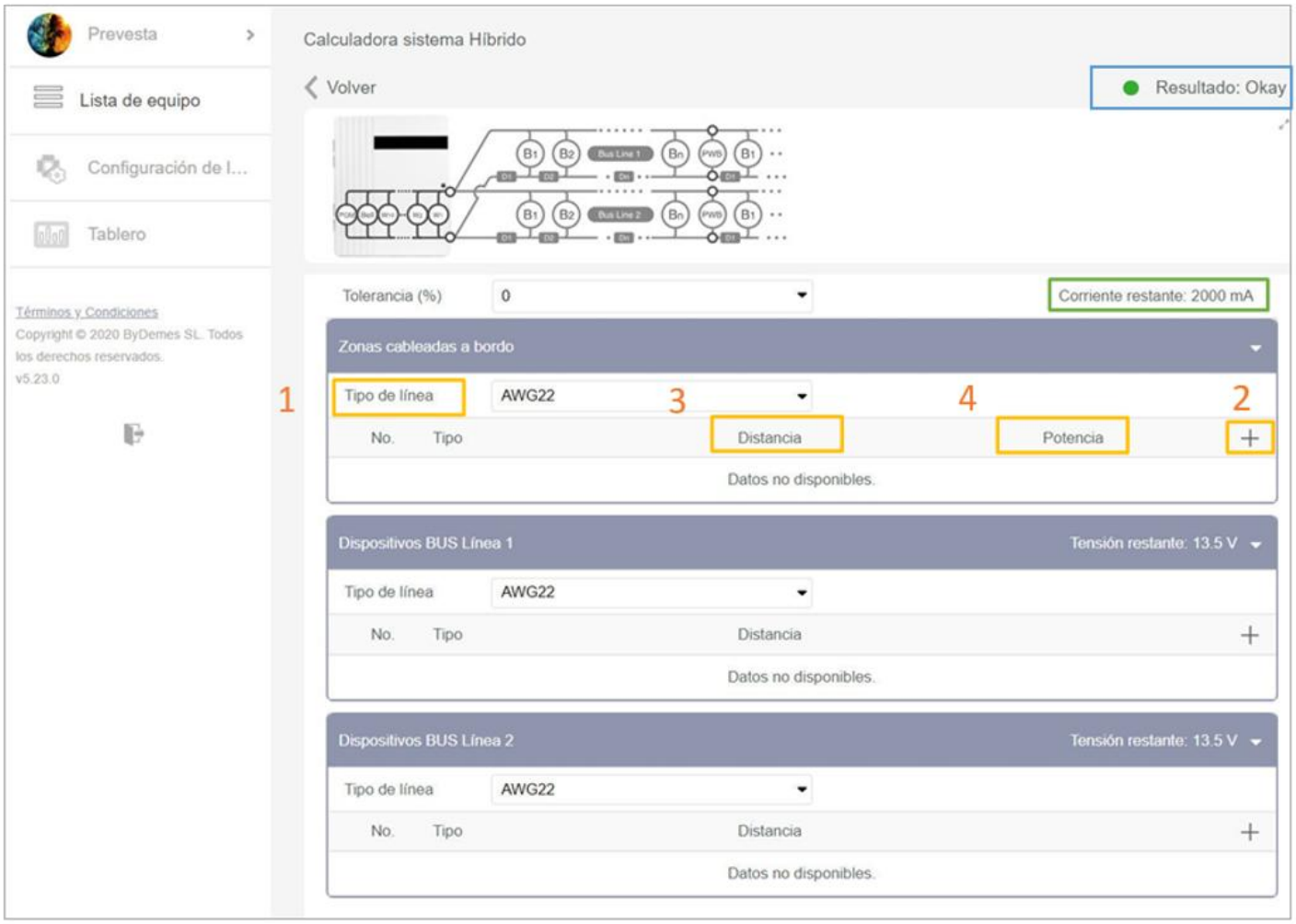
- Item Type:
    a. Conventional technology
    b. V-MAX BUS Technology
- Power consumed
- Accumulated cable distance
- Cable section



It is taken into account as a reference that the maximum current load that can be supplied by the panel source is 2A [2] and that a minimum supply voltage for detectors of approx. 10 VDC must be guaranteed.

Crossing the requested data for the zone expander [on-board wired zones] and for the BUS lines [BUS devices line 1, 2...] The system is capable of deciding whether this combination of elements, type of cable and accumulated distances is viable or not.

Result OK o No OK [1]



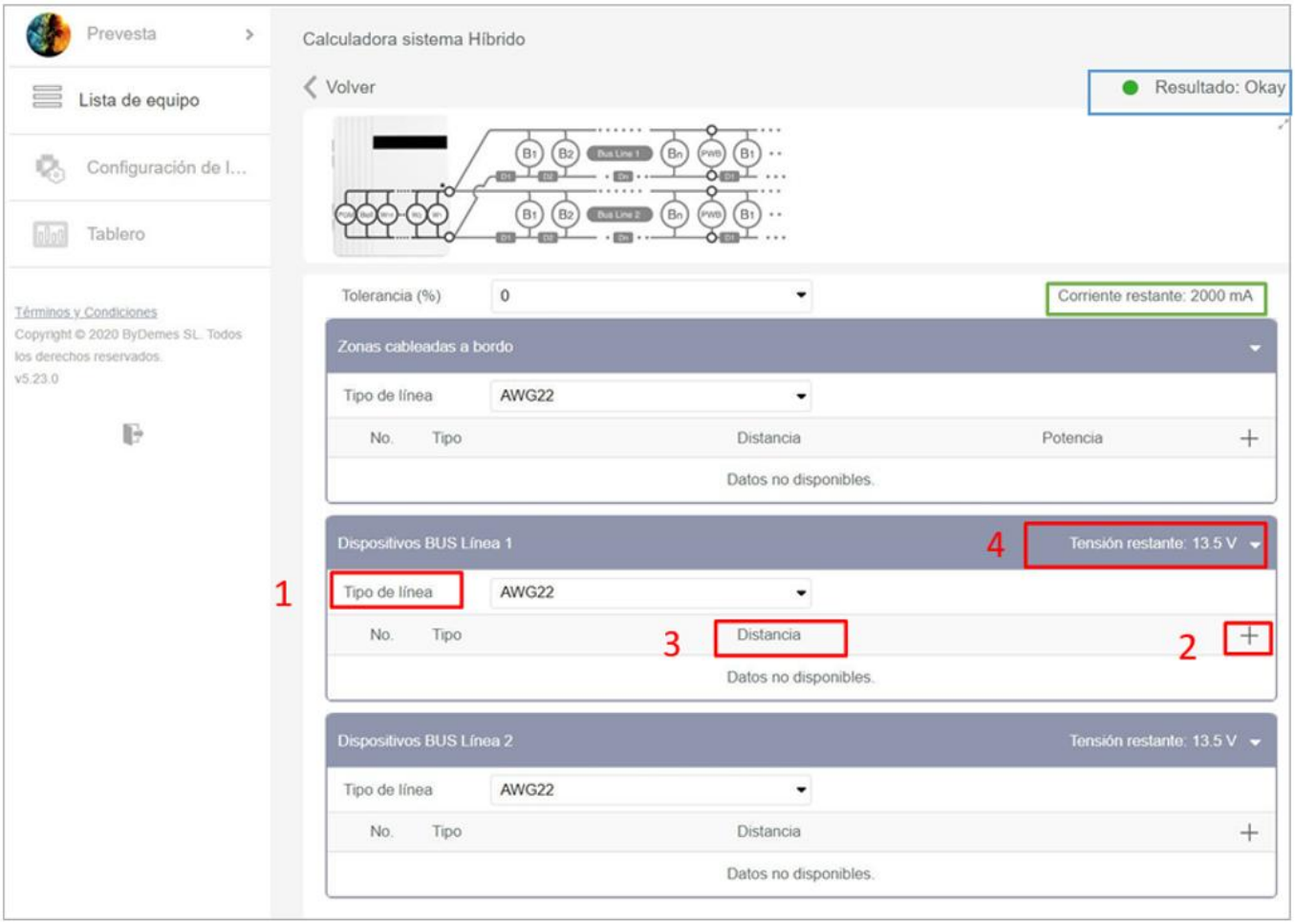
[1] Cable type: identifies the cable section used for conventional zones using Star topology

[2] Add conventional detector: a maximum of 16 zones can be added on the board

[3] Distance: Distance between conventional detector and panel

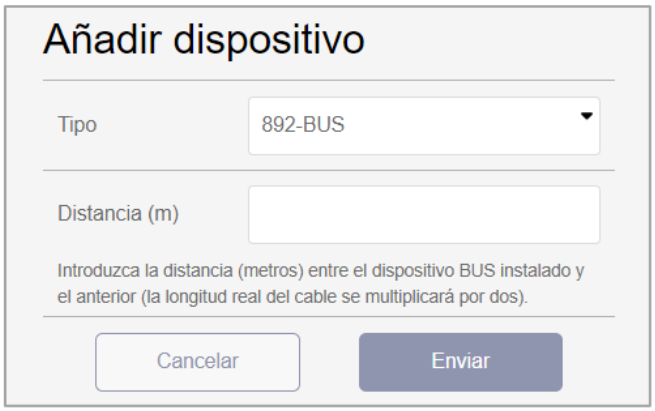
[4] Power: Maximum detector consumption

Addendum: V-MAX BUS SUPERVISED SOURCE [GRADE 3]



[1]Cable Type: Cable Section for BUS Lines

[2] Add BUS Device



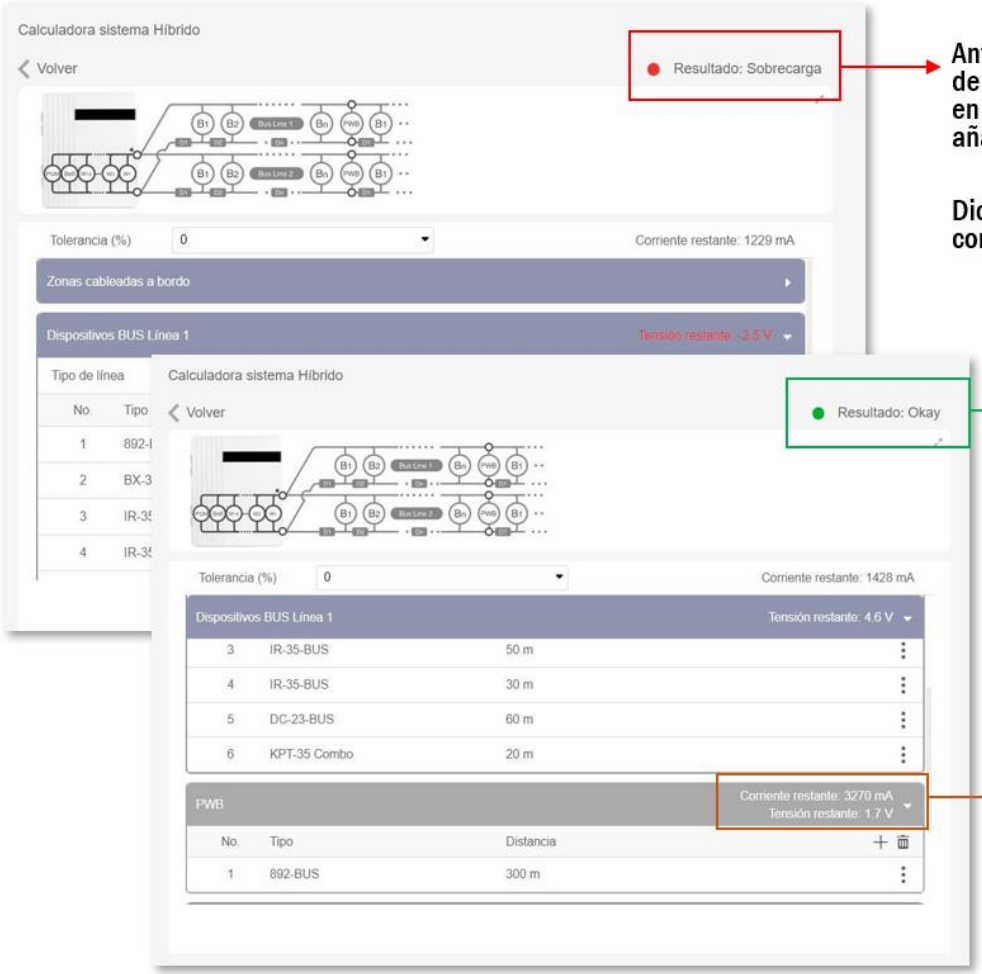
[3] Distance: accumulated cable distance from the immediately preceding BUS element

[4] Remaining Voltage: Reference voltage to measure losses in the cable. If the value reaches 0, to continue adding elements you must add the supervised power supply referenced as a PCB [see its corresponding section of the manual]

FUENTE DE HASTA 3,5A DE CORRIENTE Y 13.56V DE SALIDA CON MONITORIZACION A TIEMPO REAL DE:

- ESTADO DE BATERIA BACKUP
- TENSION DE SALIDA
- CONSUMO DE CORRIENTE

CALCULADORA



Ante un resultado fallido por exceso de consumo o perdidas de tensión en el cable el sistema te solicita añadir una fuente.

Dicho elemento está referenciado como PWB

Al añadirlo el sistema restaura volviendo su resultado a OK, conforme se puede seguir introduciendo nuevas referencias de elementos conectados desde la fuente

Las nuevas limitaciones en cuanto a carga y pérdidas vendrán dadas por la capacidad de la fuente y las distancias de cable desde este punto

Annex: V-MAX BUS Devices

Teclados BUS

CAMBIO DE MODO POR **CÓDIGO** / BLUETOOTH

CAMBIO DE MODO POR **NFC**

GESTIÓN COMPLETA INSTALACIÓN

Pircams

SEÑALES DE **ALARMA**

SUPERVISIÓN Y DETECCIÓN DE MANIPULACIONES Y **ANTI-MASKING**

CONFIGURACIÓN **REMOTA** DESDE APP

SOLICITUD DE **FOTOS** Y FOTOS DE ALARMA

Detectores y magneticos

SEÑALES DE **ALARMA**

SUPERVISIÓN Y DETECCIÓN DE MANIPULACIONES

CONFIGURACIÓN **REMOTA** DESDE APP

VINCULACIÓN CON **AUTOMATIZACIONES**

Expansores

EXPANSOR DE 8/12 Y 24 ZONAS (1EOL, 2 EOL HASTA 3EOL)

EXPANSOR 1 ZONA (1EOL, 2 EOL HASTA 3EOL)

Fuentes y Amplificadores

SUPERVISIÓN **CONSUMO** Y **TENSIÓN** DE SALIDA

SUPERVISIÓN NIVELS DE **BATERÍA**

CONFIGURACIÓN **REMOTA** DESDE APP

AMPLIFICADOR Y AISLADOR DE SEÑAL

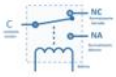
Sirenas

SIRENA DE HASTA 110 dB

SUPERVISIÓN Y DETECCIÓN DE MANIPULACIONES

CONFIGURACIÓN **REMOTA** DESDE APP

Salidas de relé



SALIDA DE **RÉLE**
CONTACTO SECO HASTA **10A**

Encapsulado, TMP , batería Backup, conector DC 12VCD

SALIDA DE **RÉLE**
CONTACTO SECO HASTA **10A**

Detector de incendio

3 EN 1

- Detector de humo

- PIR 360º

- Sirena

SIRENA DE HASTA 85 dB

SEÑALES DE **ALARMA**

CONFIG. **REMOTA** DESDE APP

AUTOMATIZ ACIONES

Doble tecnología

DETECCION PIR

MICROFONICA rotura de cristales

SUPERVISIÓN Y DETECCIÓN

DE MANIPULACIONES
CONFIGURACIÓN **REMOTA**
DESDE APP

Integración Wiegand 26

COMBO: V-MAX & F1

Integra cualquier lector de accesos WIEGAND 26

VINCULACIÓN CON **AUTOMATIZACIONES**

CONFIG. **REMOTA** DESDE APP

VR F1

DIGITAL BUS

Integración OPTEX

INTEGRACIÓN PLUG & PLAY CON **OPTEX**

CONFIGURACIÓN **REMOTA** DESDE APP

TODAS LAS SEÑALES: ALARMA, SABOTAJE, ANTIMASKING

Lector NFC

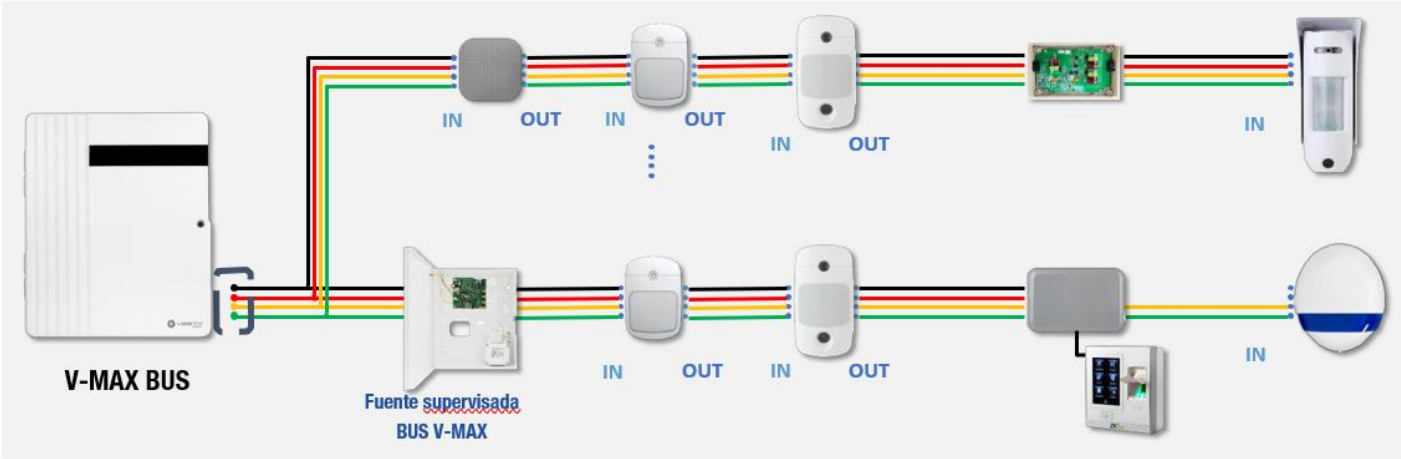
CAMBIO DE MODO POR **NFC**

CONFIGURACIÓN **REMOTA** DESDE APP

SUPERVISIÓN Y DETECCIÓN DE MANIPULACIONES

VINCULACIÓN CON **AUTOMATIZACIONES**

Annex: V-MAX BUS integration of wiegand 26 third-party readers

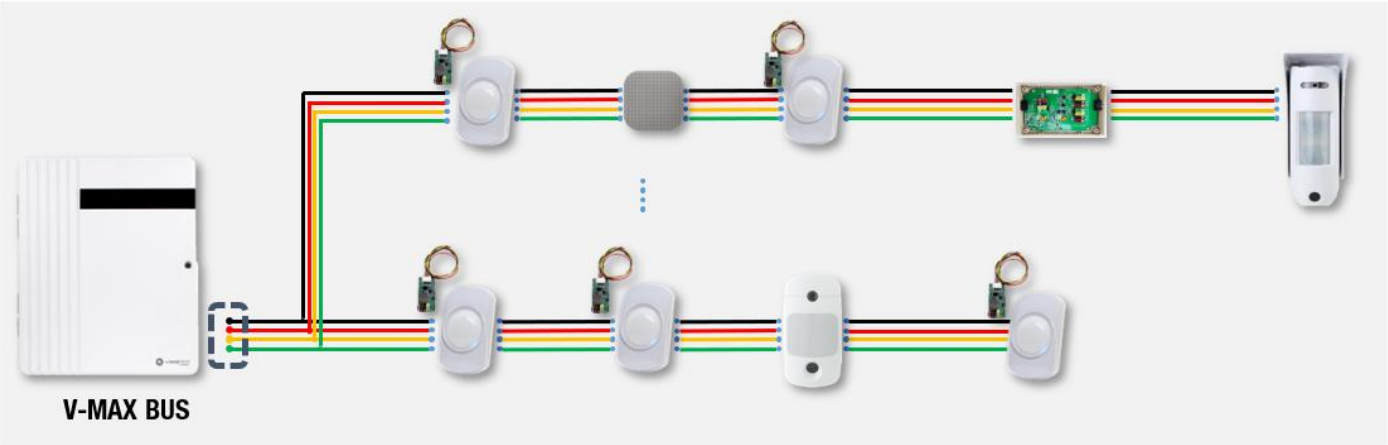


Wiegand 26 controller, vesta-344.

Flexible Cabling

The wiegand 26 integrator module, vesta-344, allows any access reader on the market compatible with this technology to be used within the VESTA system to control connections and disconnections. It is a combo device, compatible with both V-max BUS and Vesta's VR F1 technology, allowing it to be adapted to any solution. The example shows a simple integration with a third-party biometric reader.

Appendix: V-MAX BUS integration of any conventional detector



Conventional detector with dry contact outputs

1-Zone Expander (vesta-399)

Flexible Cabling

Any conventional detector on the market can be integrated and converted to VESTA BUS with the vesta-399 module. This gives the technician great flexibility when it comes to rehabilitating an obsolete intrusion system while maintaining the detectors of the old system.