

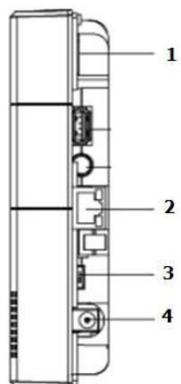
INSTALLER MANUAL



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.

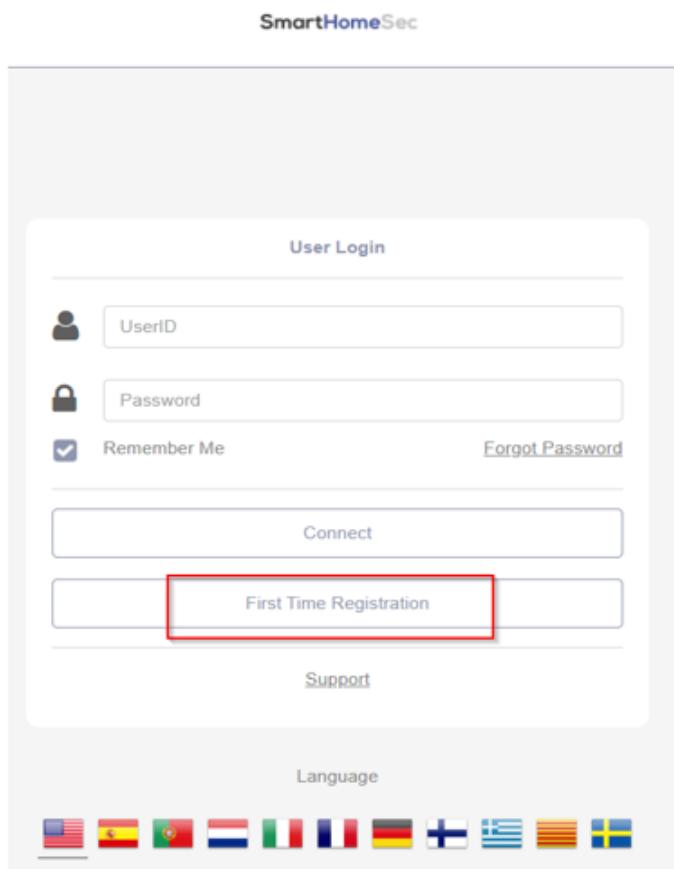
Activate installer account:

3.1 Login to the SmartHomeSec platform via:

3.1.1 WEB <https://portal.vestasecurity.eu/Vesta/>

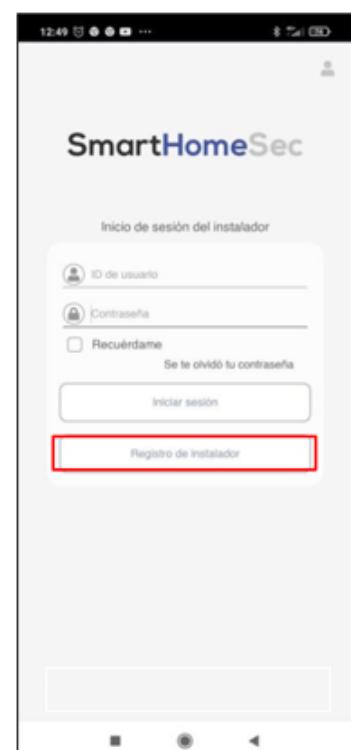
3.1.2 o APP SHS

3.2 Click on Installer Registration



The screenshot shows the SmartHomeSec User Login page. At the top, it says "User Login". Below that are fields for "UserID" (with a user icon) and "Password" (with a lock icon). There is a "Remember Me" checkbox and a "Forgot Password" link. A large blue "Connect" button is at the bottom. To the right of the "Connect" button is a red-bordered box containing the text "First Time Registration". At the very bottom, there is a "Support" link and a "Language" section with several flag icons.

Vista WEB



Vista APP

3.3 Fill in the form and click on next

Account Info

User ID

Password

Confirm Password

Name

Email

Phone Number Select

Language English

I have read and agree to the following documentation: [Terms and Conditions](#)

[Back](#) [Next](#)

3.4 Verify with the code received in the email

Verification

Enter the code we sent you via email to continue

Verification Code

Didn't get the code? [Resend](#)

[Back](#) [Next](#)

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

Dealer

Select your dealer from the list below

Country All

Dealer Vesta Security [EU]

[Back](#) [Submit](#)

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/>

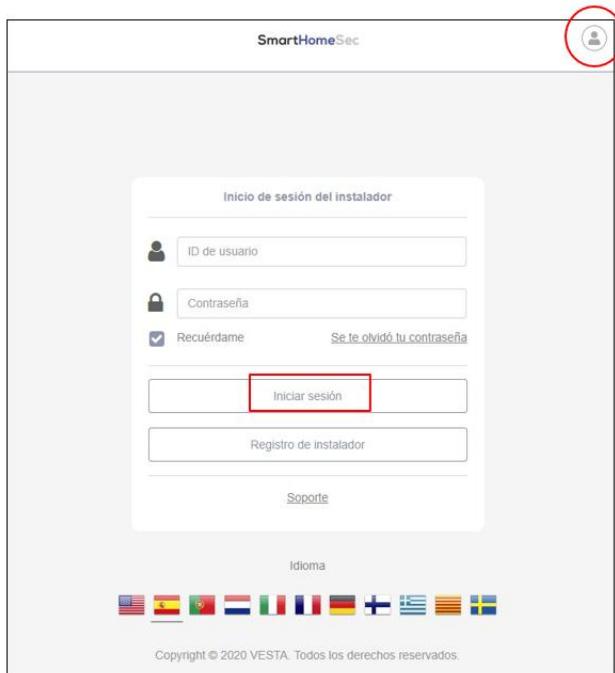


4.1 Register panel from the SmartHomeSec WEB

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

SmartHomeSec			
Prevesta	Lista de paneles		
Lista de paneles	No.	Nombre del panel	Dirección MAC
	1	HSGW	00:1d:94:0b:fd:de
	2	bogp pruebas	00:1d:94:0c:45:e5
	3	Hibrida pruebas	00:1d:94:0b:e3:e4

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

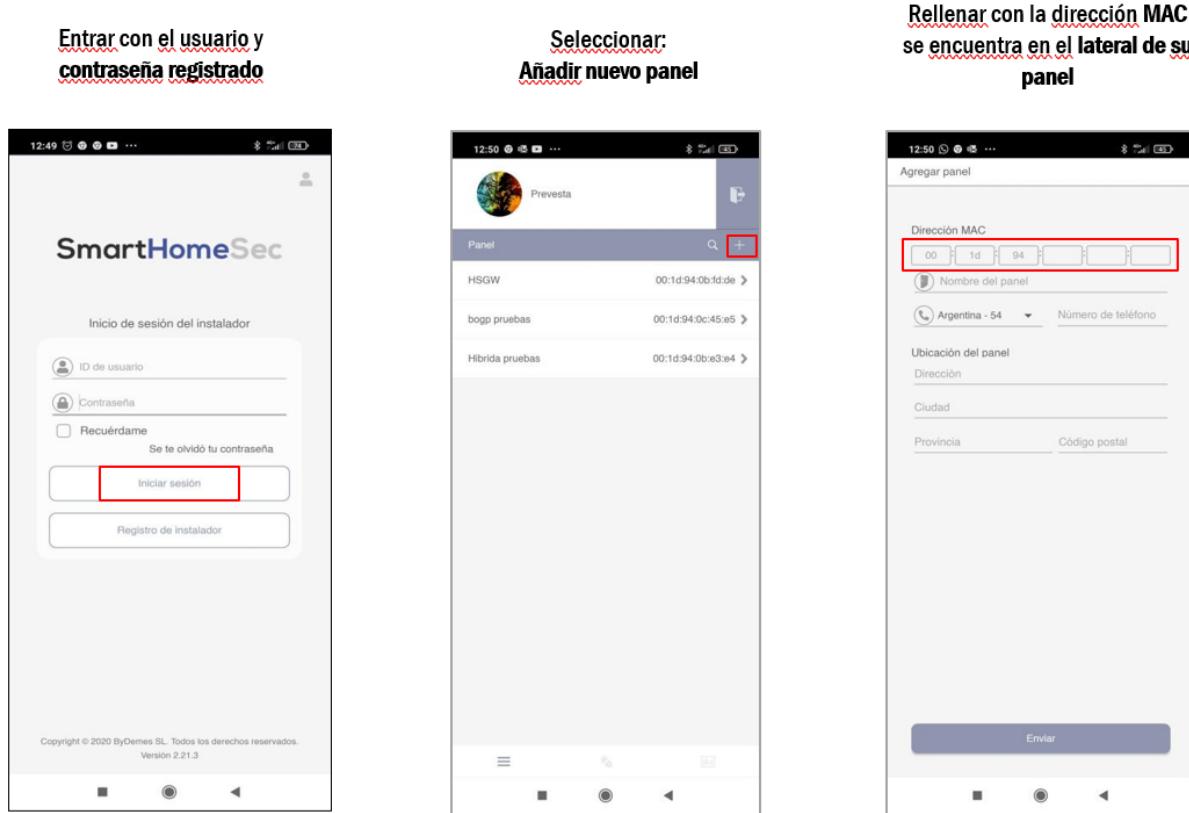
- Click on the "+" button to add a new panel

The screenshot shows the 'Agregar panel' (Add panel) form in the Prevesta software. The left sidebar has icons for 'Prevesta', 'Lista de paneles' (Panels list), 'Configuración de lotes' (Batch configuration), and 'Tablero'. The main area has two sections: 'Información del panel' (Panel information) and 'Ubicación del panel' (Panel location). In the 'Información del panel' section, there are fields for 'Dirección MAC' (MAC address) containing '00:1d:94:', 'Número de teléfono' (Phone number) with a dropdown menu 'Seleccione', and 'Nombre del panel' (Panel name). The 'Ubicación del panel' section contains fields for 'Dirección' (Address), 'Ciudad' (City), 'Provincia' (Province), and 'Código postal' (Postal code). At the bottom are 'Cancelar' (Cancel) and 'Enviar' (Send) buttons. A red box highlights the MAC address field.

- 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



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!

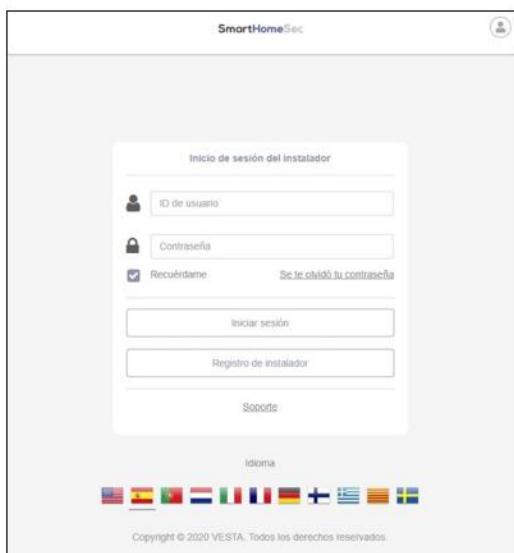
- The **MAC** is located on the side of the panels
- **Panel name** with which you will register in the system
- Telephone number, Address, City, Province and Postal Code is not mandatory, but it is interesting to have a small database with information on each central
- **Once the process is complete,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



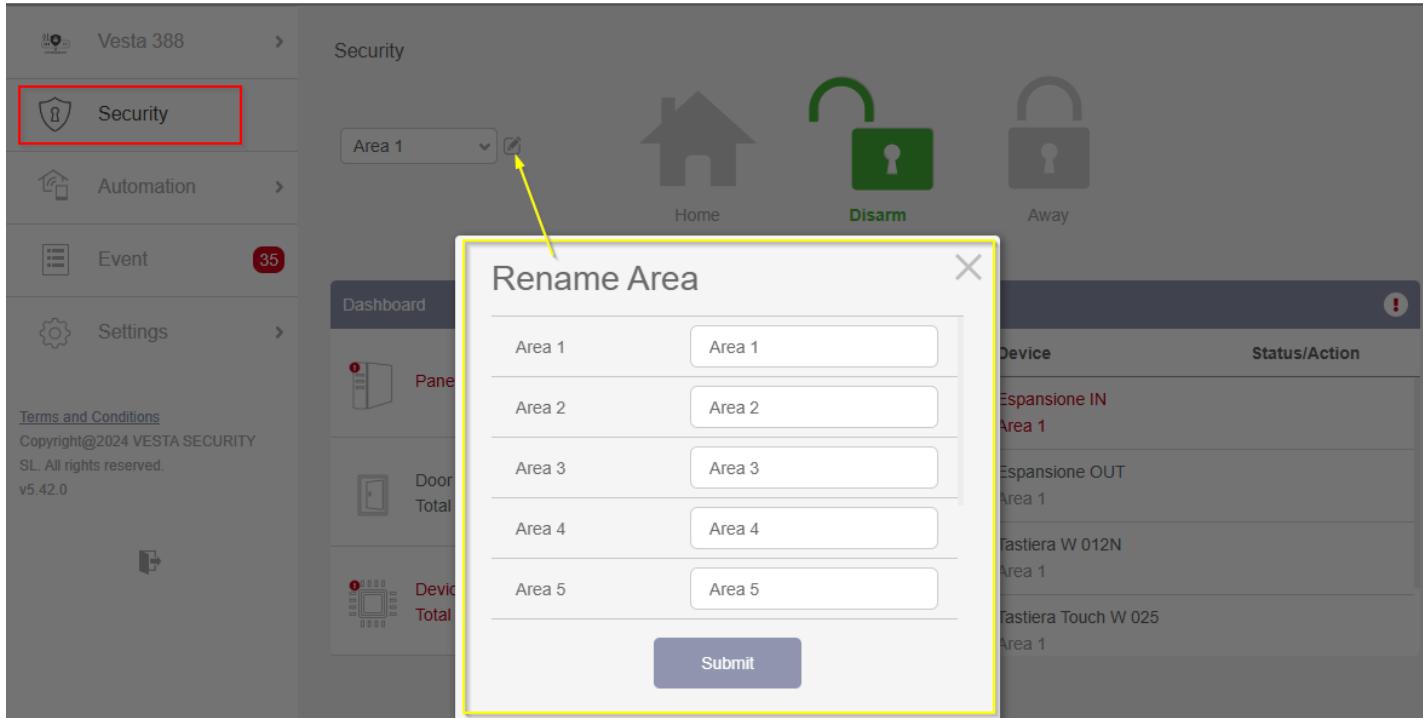
3. Select from the list [1] the target panel of

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

A screenshot of the SmartHomeSec Equipment List interface. On the left is a sidebar with "Equipment List", "Batch Config", and "Dashboard" buttons, and a "Terms and Conditions" section. The main area shows a table with columns: No., Equipment Name, MAC/IMEI, and Status. A row for "Vesta 388" is highlighted with a red border and a yellow box labeled "1" pointing to its status column. A modal dialog titled "Login" is overlaid on the table, containing fields for "Vesta 388" and "00:1d:94:1b:24:a3", and an "Installer Code" input field. A yellow box surrounds the entire "Login" dialog.

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

Date	Event Type	Area	Time	Source
2025/02/26	RC Disarm	Area 1	12:51:59	Telecomando 017 (Zone 12)
	Restore	Area 1	12:51:59	Dahua DH-TPC-BF1241 (Zone 24)
	Burglar	Area 1	12:51:41	Dahua DH-TPC-BF1241 (Zone 24)
	Cross Region Detection	Area 1	12:51:40	Dahua DH-TPC-BF1241 (Zone 24)
	RC Arm	Area 1	12:51:33	Telecomando 017 (Zone 12)
	Arm with Fault	Area 1	12:51:32	System

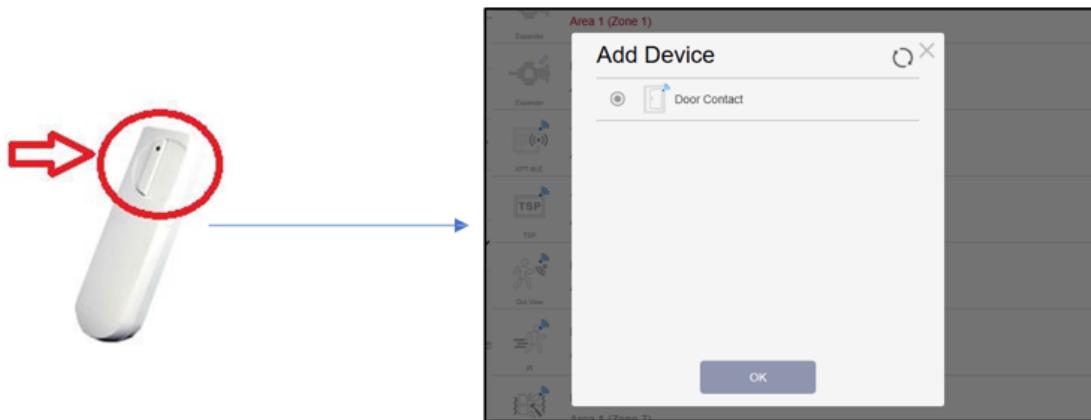
8. Settings: Add Devices

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

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

Device	Status
Espansione IN (IN:0157ef00) Area 1 (Zone 1)	
Espansione OUT (IN:041e9b00) Area 1 (Zone 2)	
Tastiera W 012N Area 1 (Zone 3)	
Tastiera Touch W 025 Area 1 (Zone 4)	
PIRCAM EXT 347N-720 Area 1 (Zone 5)	
PIR 382 Area 1 (Zone 6)	
Rottura Vetri 382 Area 1 (Zone 7)	
Selettore di Scene 043N Area 1 (Zone 8)	
Lux Temp Um 223 Area 1 (Zone 9)	

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

Device Info

Door Contact

Area: Area 1

Zone: 26

Device Name: Front Door

OK

Adding device is complete.

OK Settings

8.1 Zone Configuration

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

The screenshot shows the 'Settings - Device' screen in the Vesta 388 app. On the left, a sidebar lists categories: Security, Automation, Event (with 45 notifications), Settings (selected), Device (highlighted with a red box and a red '1'), Bus Management, Geofencing, Panel, User PIN, Wired Device, Z-Wave Tool, Network, and Report. The main area displays a table of devices:

Device	Status
Zone 18 Area 1 (Zone 18) Door Contact	DC Closed
Zone 19 Area 1 (Zone 19) Door Contact	DC Closed
Zone 20 Area 1 (Zone 20) Door Contact	DC Closed
Zone 21 Area 1 (Zone 21) IR	
Zone 22 Area 1 (Zone 22) IR	
Zone 23 Area 1 (Zone 23) IR	
Dahua DH-TPC-BF1241 Area 1 (Zone 24) IP Cam	
Pircam interno Area 1 (Zone 25)	
Front Door Area 1 (Zone 26) Door Contact	DC Closed

A red box highlights the 'Device' category in the sidebar, and another red box highlights the 'Front Door' row in the table. A red number '1' is in a red box above the 'Device' category, and a red number '2' is in a red box below the 'Front Door' row.

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

Settings - Device

Front Door Settings

Door Contact

Area	24 HR
Zone	<input type="checkbox"/> Burglar Alarm
Name	Disarm Response
Front Door	Chime
Bypass	Full Arm Response
Off	Start Entry Delay 1
Must be Closed	Home Arm Response
No	Start Entry Delay 1
Bypass Tamper	Exit
Off	<input checked="" type="checkbox"/> No Response
Bypass Supervision	Trigger Response
Off	No Response
Auto Bypass	Restore Response
Disable	No Response
Activation	
1	
min(s)	
2	
Latch	
On	
Set/Unset	
<input type="checkbox"/> Normal Close	

Back Submit

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 entry Delay 1
- c. Start entry 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

The screenshot shows the Vesta 388 mobile application interface. On the left, there is a sidebar with various menu items: Vesta 388, Security, Automation, Event (with a red notification badge '46'), Settings, and a 'Device' item which is currently selected and highlighted with a red box. The main content area is titled 'Settings - Device'. It shows a table of devices:

Device	Status	⋮
Espansione IN (IN:0157ef00) Area 1 (Zone 1)		⋮
Espansione OUT (IN:041e9b00) Area 1 (Zone 2)		⋮

In the center, a modal dialog box is displayed with a red border, titled 'Walk Test'. It contains a table with the following data:

Type	Area	Zone	Device Name	RSSI
Door Contact	Area 1	26	Front Door	9

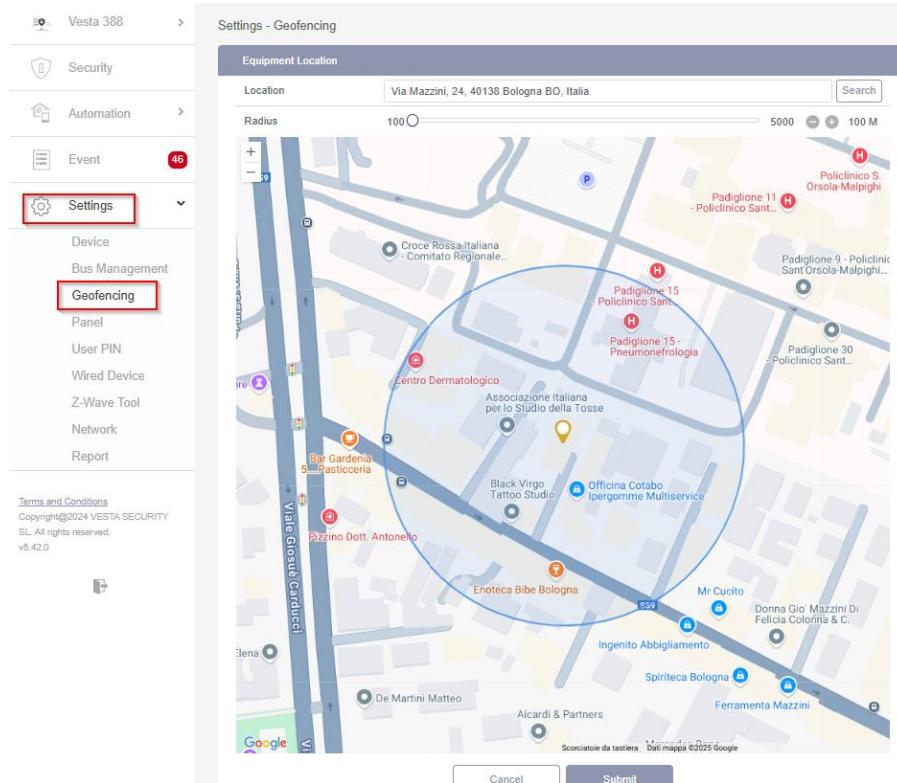
At the bottom of the dialog box is an 'OK' button.

At the very bottom of the screen, there is a footer bar with icons for Lux Temp Um 223 (Area 1 (Zone 9)), Porta ingresso 345 (DC Closed), and a battery level indicator showing 21.8°C and 56%.

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



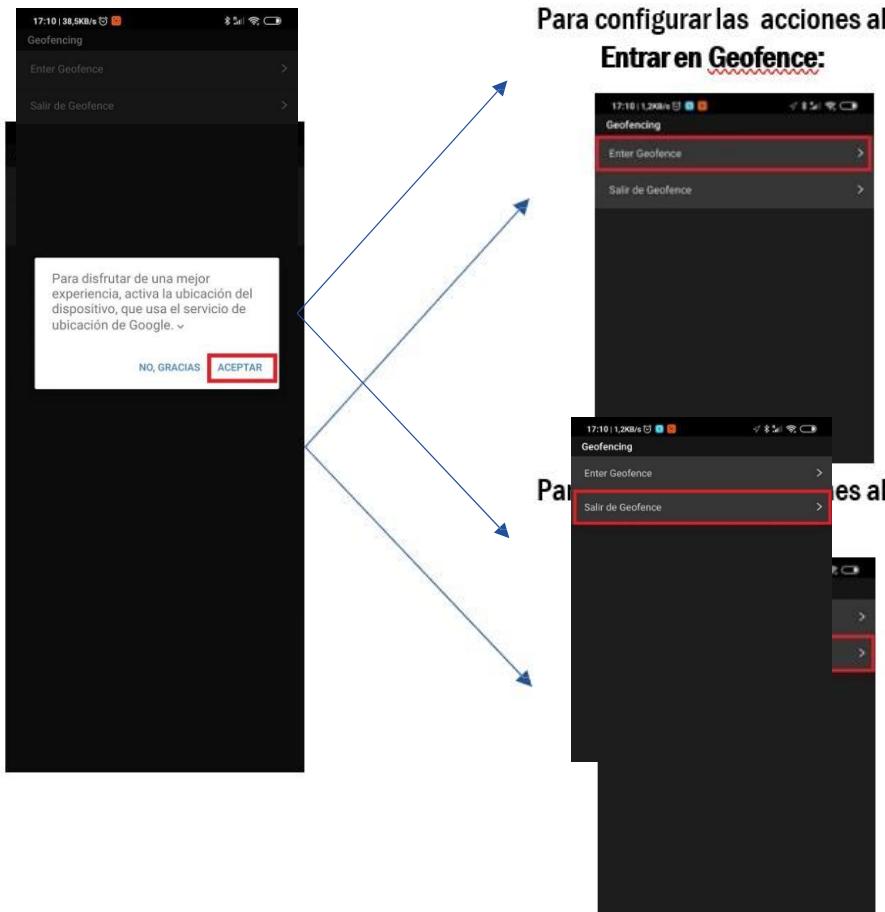
Entrar en Ajustes



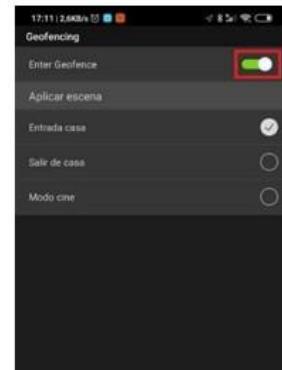
Seleccionar Alertas Inteligentes



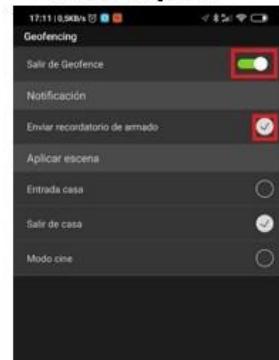
Para configurar las acciones al Entrar en Geofence:



Habilitar la entrada y seleccionar Escena a aplicar



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]

The screenshot shows the Vesta 388 software interface. The left sidebar includes sections for Vesta 388, Security, Automation, Event (with 47 notifications), Settings (highlighted with a red box and red number 1), Device, Bus Management, Geofencing, Panel (highlighted with a red box and red number 2), User PIN, Wired Device, Z-Wave Tool, Network, and Report. The bottom left of the sidebar displays Terms and Conditions, Copyright@2024 VESTA SECURITY SL. All rights reserved., and v5.42.0. The main content area is titled "Settings - Panel" (highlighted with a red box and red number 3). It features a navigation bar with tabs: Security, Panel (selected), Code, Date & Time, Factory Reset, Doorman Code, and FW Update. Below the tabs are three mode sections: "All Mode", "Away", and "Home". Each mode section contains several configuration fields, such as "Final Door" (Off), "Tamper Alarm" (Full Arm), "Supervision for Fixed Device" (24 hr(s)), "Supervision Timer for Cam" (Disable), "Cross Zone Timer" (Disable), "Door Chime" (Off), "Warning Beep" (Off), "Arm Fault Type" (Direct Arm), "Supervision Check" (On), "Supervision for Pendant" (Disable), "Alarm Length" (2 min(s)), "Fire Verification Timer" (Disable), "Confirm Sound" (Low), and "Entry/Exit Only Final Beeps" (3 sec(s)). At the bottom right are "Cancel" and "Submit" buttons.

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

Settings - Panel

Security Panel Code Date & Time Factory Reset Doorman Code FW Update

Area 1 **Setting for singolar partition**

Area 1	Off	Arm Fault Type	Direct Arm
Area 2	Full Arm	Supervision Check	On
Area 3	24 hr(s)	Supervision for Pendant	Disable
Area 4	Disable	Alarm Length	2 min(s)
Area 5	Disable	Fire Verification Timer	Disable
Area 6	Disable	Confirm Sound	Low
Area 7	Disable	Entry/Exit Only Final Beeps	3 sec(s)
Area 8			
Cross Zone Timer			
Door Chime			
Warning Beep			

Away **Entry and Exit time when armed away**

Entry Delay Time 1	10 sec(s)	Entry Delay Time 2	Disable
Exit Delay Time	Disable	Entry Delay Sound	Low
Exit Delay Sound	Low		

Home **Entry and Exit time when armed stay**

Entry Delay Time 1	10 sec(s)	Entry Delay Time 2	Disable
Exit Delay Time	Disable	Entry Delay Sound	Low
Exit Delay Sound	Low		

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

Security	Panel	Code	Date & Time	Factory Reset	Doorman Code	FW Update
Panel Settings						
AC Fail Report	5 min(s)	▼	AC Fail Suspend	5 sec(s)	▼	
Jamming Report	2 min(s)	▼	Auto Check-in Interval	1 hr(s)	▼	
Auto Check-in Daily Time	⌚ 00 : 00		GPRS/LTE test interval	Disable	▼	
Ethernet test interval	Disable	▼	Stop Device Status Notify	Disable	▼	
PD6662 Feature	Disable	▼	IR Camera Resolution of Alarm Images	1280x720x3 images (when app ▼		
Outdoor IR Camera in Grayscale	Enable	▼	Bypass Ethernet Fault	Off	▼	
Service Failure Report (Ethernet)	Disable	▼	Power Supply Overcurrent Restart Time	3 min(s)	▼	
Wired Device Tolerance	20%	▼	Mute internal siren	Off	▼	
DNS Flush Period	Disable	▼				
Program RF Siren						
Siren Tamper On		Siren Tamper Off				
Panel Info				Resend Configuration		
Equipment Name	Vesta 388		Internal IP	192.168.10.149		
Public IP	151.28.227.161		MAC Address	00:1d:94:1b:24:a3		
Report Account	127038858403		Net Version	GL 0.0.2.34A2_Homekit-4.1.11		
GSM Version	Quectel EC21EFAR06A06M4G		ZB Version			
RF Version	460800_BGST-U-ITR-F1-BD_B...		IO MCU Version	FF-IO8_BL_A03_2023.09.21		
Backup Battery Status	On		Local Web Access	Enable		

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

The screenshot shows the 'Code' subsection of a control panel's configuration menu. At the top, there are tabs for Security, Panel, Code (which is selected), Date & Time, Factory Reset, Doorman Code, and FW Update. Below the tabs, the title 'Code' is displayed in a dark blue header bar. The main area contains several input fields and dropdown menus:

- Master Code 1: Input field containing '1111'.
- Master Code 2: Input field containing '2222'.
- Installer: Input field containing '7982'.
- Duress Code: Input field.
- Guard Code: Input field.
- Temporary Code: Input field.
- Latch: A checkbox labeled 'Latch'.

Two dropdown menus are present, each with a red arrow pointing to it from the left side of the screen:

- A dropdown menu labeled 'Area 1 ▾' on the left side of the screen.
- A dropdown menu labeled 'Area 1 ▾' on the right side of the screen, which is currently open, showing options: Area 1 (selected), Area 2, Area 3, Area 4, Area 5, Area 6, Area 7, and Area 8.

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

The screenshot shows a navigation bar with tabs: Security, Panel, Code, Date & Time (which is highlighted in blue), Factory Reset, Doorman Code, and FW Update. Below the navigation bar is a section titled "Clock". It contains three input fields: "Time Zone" set to "(GMT+01:00) Brussels, Copenhagen, Madrid, Paris"; "Date & Time" set to "2025/02/26 15 : 19"; and "Internet Time" set to "pool.ntp.org". A checked checkbox "Automatically synchronize with an Internet time server" is also present.

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

The screenshot shows a navigation bar with tabs: Security, Panel, Code, Date & Time, Factory Reset (which is highlighted in blue), Doorman Code, and FW Update. Below the navigation bar is a section titled "Factory Reset". It contains two unchecked checkboxes: "Keep the current network setting" and "Keep the current device list".

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.

Settings - Panel

Security	Panel	Code	Date & Time	Factory Reset	Doorman Code	FW Update
FW Update						
Panel	Select					Apply
RF Module	Select					Apply
IO MCU	Select					Apply
	GL_demes-0.0.2.34A2.bin					
	GL_demes-0.0.2.34.bin					
	GL_demes-0.0.2.33G.bin					
	GL_demes-0.0.2.33C_Homekit-4.1.11_upg.bin					

Ajuste - Panel

Seguridad	Panel	Código	Fecha y hora	Restablecimiento de fábrica	Actualización de FW	
Actualización de FW						
Panel	Seleccione					Aplicar
IO MCU ²	Seleccione					Aplicar
	Seleccione					
	U-IO_BL_A10_220622.bin					
	U-IO_BL_A08_220208.bin					
	U-IO_BL_A09_220513.bin					

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

Settings- Wired Device Loop = EOL Scheme

Internal Wired Sens + Monitor Resistance

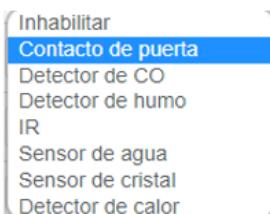
Zone	Type	Loop	Resistor	Status	Panel Area/ Zone	Resistance
1	Door Contact	1	No EOL	Restore	Area 1 Zone 16 Edit	
2	Door Contact	1	No EOL	Restore	Area 1 Zone 17 Edit	
3	Door Contact	1	No EOL	Restore	Area 1 Zone 18 Edit	
4	Door Contact	1	No EOL	Restore	Area 1 Zone 19 Edit	
5	Door Contact	1	No EOL	Restore	Area 1 Zone 20 Edit	
6	IR	1	No EOL	Restore	Area 1 Zone 21 Edit	
7	IR	1	No EOL	Restore	Area 1 Zone 22 Edit	
8	IR	1	No EOL	Restore	Area 1 Zone 23 Edit	

Device
Bus Management
Geofencing
Panel
User PIN
Wired Device
Z-Wave Tool
Network
Report

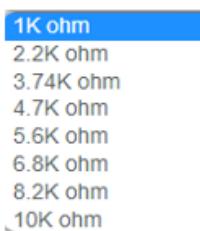
Terms and Conditions
Copyright@2024 VESTA SECURITY
SL. All rights reserved.
v5.42.0

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:

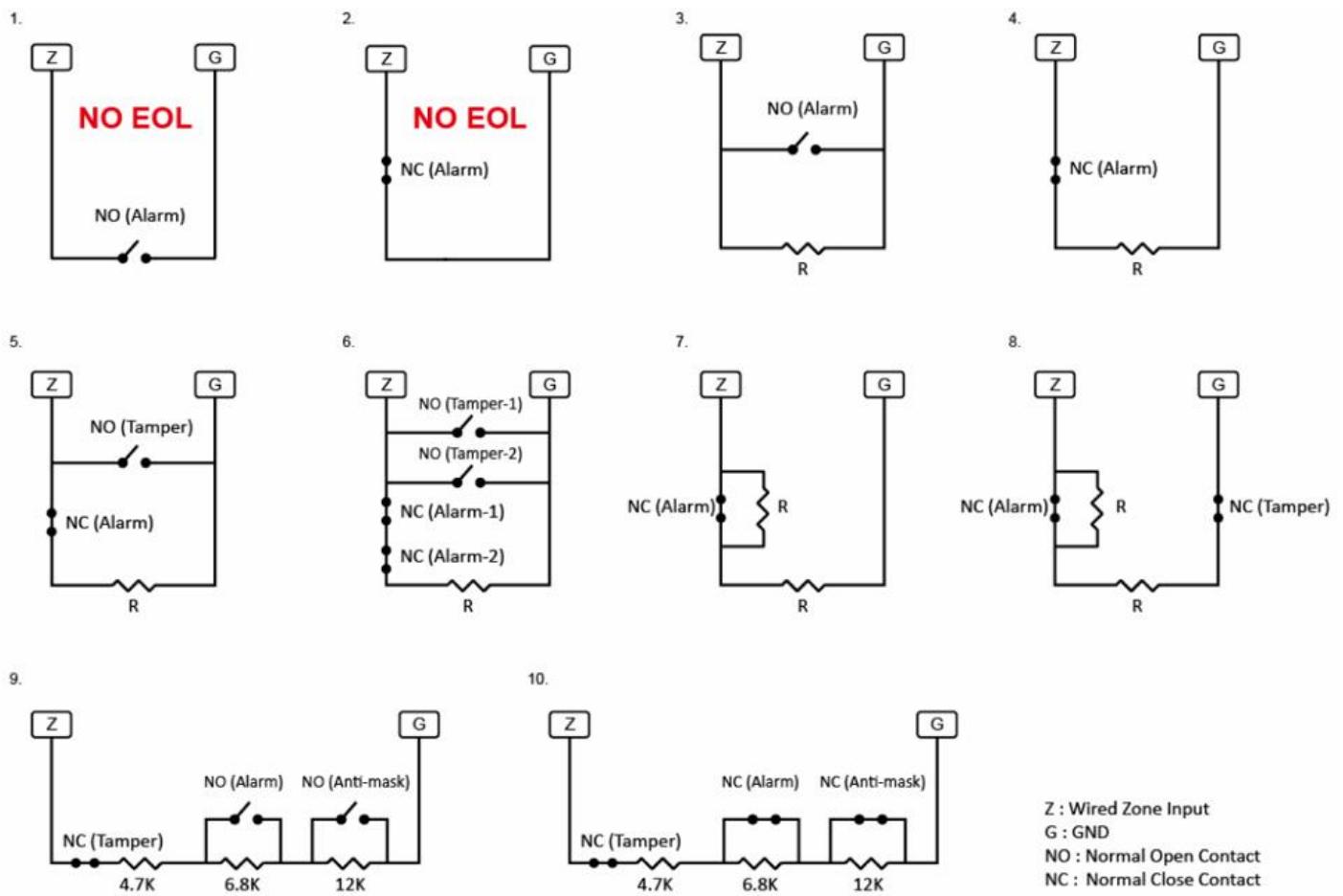
- Zone Type



- 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

The screenshot shows the 'Settings - Network' page of the Vesta 388 web interface. The left sidebar has a 'Settings' section with 'Network' highlighted. The main area has tabs for 'GSM', 'GPRS', and 'LoRa', with 'GSM' selected. The 'GSM' section displays the following information:

Parameter	Value	Parameter	Value
IMEI	862646061759962	IMSI	240075814581447
Carrier	Iliad Tele2 IoT	RSSI	9
Communication Mode	Auto	SIM Card Detection	Enable
GSM Event	Enable	IP Network Connection Time Limit	1 hr(s)
Antenna	Internal		

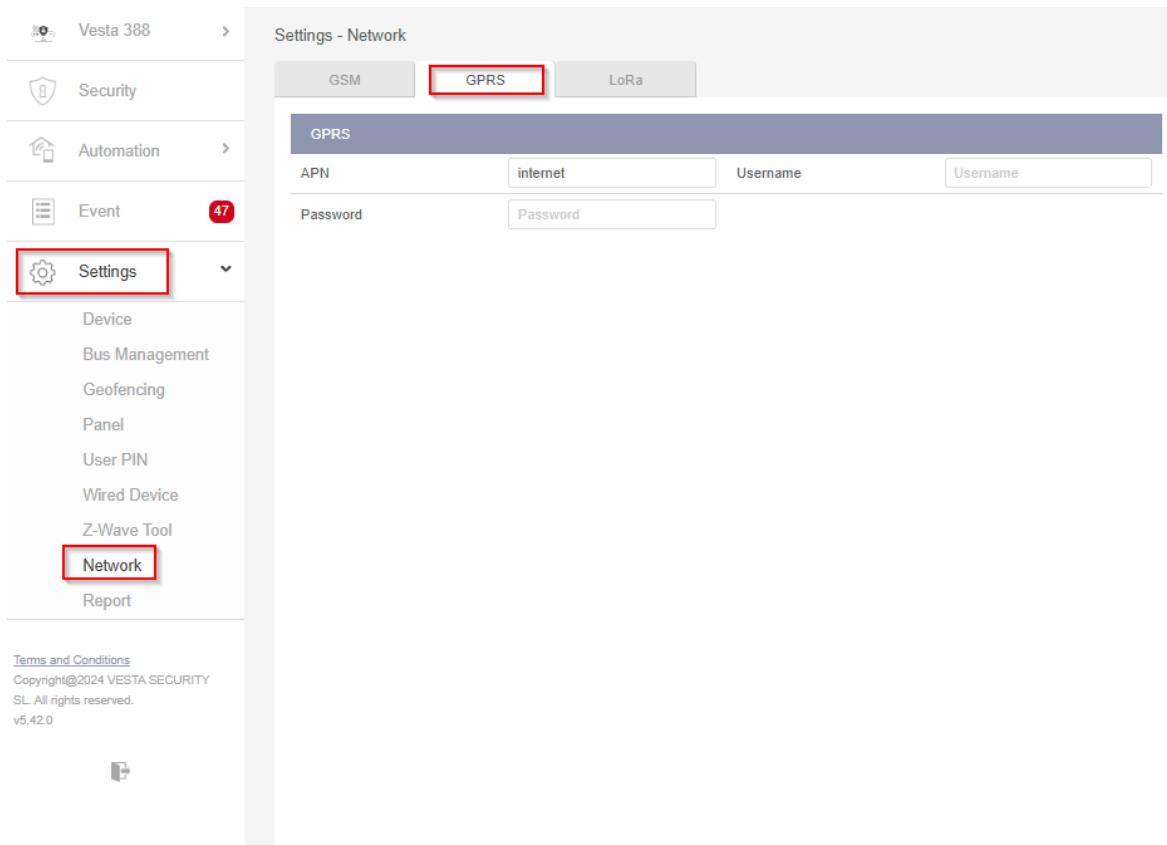
Below the GSM section are sections for MMS, SMS, and Two-way communication, each with their own sets of parameters.

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

The screenshot shows the Vesta 388 software interface. On the left, there is a navigation sidebar with the following items:

- Security
- Automation
- Event (with a red notification badge showing 47)
- Settings
 - Device
 - Bus Management
 - Geofencing
 - Panel
 - User PIN
 - Wired Device
 - Z-Wave Tool
 - Network** (highlighted with a red box)
 - Report

Below the sidebar, there is a note about terms and conditions and copyright information:

Terms and Conditions
Copyright©2024 VESTA SECURITY
SL. All rights reserved.
v5.42.0

The main content area is titled "Settings - Network". It has tabs for GSM, GPRS, and LoRa, with LoRa selected (highlighted with a red box). Below the tabs, there is a dropdown menu labeled "Enable LoRa Dongle" set to "Enable". The "LoRa Settings" section contains the following fields:

APP Key	AE3D87F1781A93DC6402318DAC982197		
APP EUI	0101010101010101	Device EUI	
Dongle Version		Status	Failed
RSSI	- dBm		

A note at the bottom of the settings section says: "Note: Please ensure one of the reporting path in Report is set to 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

The screenshot shows the Vesta 388 web interface. The left sidebar has a red box around the 'Settings' section, and the 'Report' subsection is also highlighted with a red box. The main content area shows the 'Report' tab selected. It includes fields for URLs (URL 1: ip://127.0.0.1:8080/CID_SIA, URL 2: empty), reporting groups (Group 1, Group 2), and event filtering (All events). A note section lists various reporting formats, with item 3 (Manitou format) highlighted with a red box. Below this is a table for reporting sequences across five groups, and finally report settings for SIA Poll Interval and automation alarm events.

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 n°3 [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

The screenshot shows the Vesta 388 software interface. On the left, there's a sidebar with various settings like Security, Automation, Event (with 47 notifications), Settings (selected and highlighted with a red box), Device, Bus Management, Geofencing, Panel, User PIN, Wired Device, Z-Wave Tool, Network (selected and highlighted with a red box), and Report (selected and highlighted with a red box). At the bottom of the sidebar, there are terms and conditions and a copyright notice for Vesta Security SL. The main area is titled 'Settings - Report' and has tabs for Report, SMS, Media Upload (selected and highlighted with a red box), and SMTP. Under the Media Upload tab, there's a 'Media Upload' section with two entries: URL 1 (XHTTP, portal.vestasecurity.eu:8090/up-post.js, Backup IP) and URL 2 (Manitou, Backup IP). Below this, there's a 'Note' section with instructions:

- Upload via IP (Ethernet or GPRS) in FTP protocol, e.g.: `ftp://user:password@server/path`
- Upload via IP (Ethernet or GPRS) in HTTP protocol, e.g.: `http://server/path`
- Mail via IP (Ethernet or GPRS), e.g.: `mailto: user@server`
- Manitou via IP (Ethernet or GPRS), e.g.: `manitou:/user@server:port`**
- Manitou(TLS) via IP (Ethernet or GPRS), e.g.: `manitou_tls:/user@server:port`

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 n°4

- **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**

The screenshot shows the Vesta 388 panel interface. On the left, there is a sidebar with the following items:

- Vesta 388 (highlighted with a red box)
- Account List (highlighted with a red box)
- Announcement
- Device Bypass
- Cudy Router
- Security
- Automation
- Event (with a red notification badge showing 47)
- Settings

The main area is titled "Account List". It contains a table with one row:

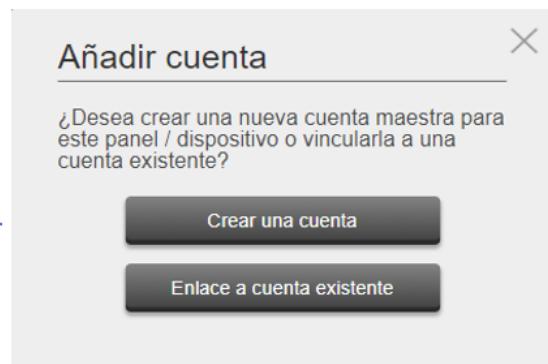
No.	Username	Email	Password	Access Privilege
1	luca@vestasecurity.eu*	luca@vestasecurity.eu	*****	

At the top right of the "Account List" table, there are two buttons: a red-bordered "+" button and a trash can icon.

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



Habilitar para restringir derechos de acceso para las cuentas de clientes compartidas.

Acceso a:

- Peticiones de foto bajo demanda [SI/NO]
- Notificaciones móviles [SI/NO]
- Icono de domótica [SI/NO]
- Icono de histórico de eventos [SI/NO]
- Icono de Cámaras IP/PIR CAM [SI/NO]

- [1] Nombre de usuario deseado
[2] Contraseña para el usuario
[3] Confirmar contraseña
[4] Correo electrónico del usuario

- [1] Nombre de usuario deseado
[2] Contraseña para el usuario
[3] Confirmar contraseña
[4] Correo electrónico del usuario

Crear una cuenta

ID de usuario	<input type="text"/> ID de usuario
Contraseña	<input type="password"/> Contraseña
Confirmar contraseña	<input type="password"/> Confirmar contraseña
Email	<input type="text"/> Email
Derecho de acceso	<input checked="" type="checkbox"/> Petición multimedia <input checked="" type="checkbox"/> Notificación <input checked="" type="checkbox"/> Automatización <input checked="" type="checkbox"/> Cámaras <input checked="" type="checkbox"/> Evento

Cancelar Enviar

Enlace a cuenta existente

Si desea otorgar acceso para este usuario a su panel, ingrese la contraseña de este usuario.

ID de usuario	<input type="text"/> ID de usuario 1
Contraseña	<input type="password"/> Contraseña 2
Derecho de acceso	<input checked="" type="checkbox"/> Petición multimedia <input checked="" type="checkbox"/> Notificación <input checked="" type="checkbox"/> Automatización <input checked="" type="checkbox"/> Cámaras <input checked="" type="checkbox"/> Evento

Cancelar Enviar

12. Share the dashboard with the client

[1] Device

The screenshot shows the Vesta 388 software interface. On the left, there's a sidebar with icons for Automation, Security, Event (with 47 notifications), and Settings. The Automation section is highlighted with a red box and has a yellow box around the 'Device' option. Below the sidebar, the main area is titled 'Automation - Device'. It features a 'Device' filter bar with four categories: All (yellow box), Switch (yellow box), Lock (yellow box), and HVAC. Underneath is a table with columns 'Device' and 'Status'. It lists three devices: 'Selettore di Scene 043N' (Area 1, Scene Selector), 'Lux Temp Um 223' (Area 1, LMHT), and 'Rilevatore di Fumo 336 Temp' (Area 1, Temperature Sensor). Each device row includes a delete icon and a more options icon.

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

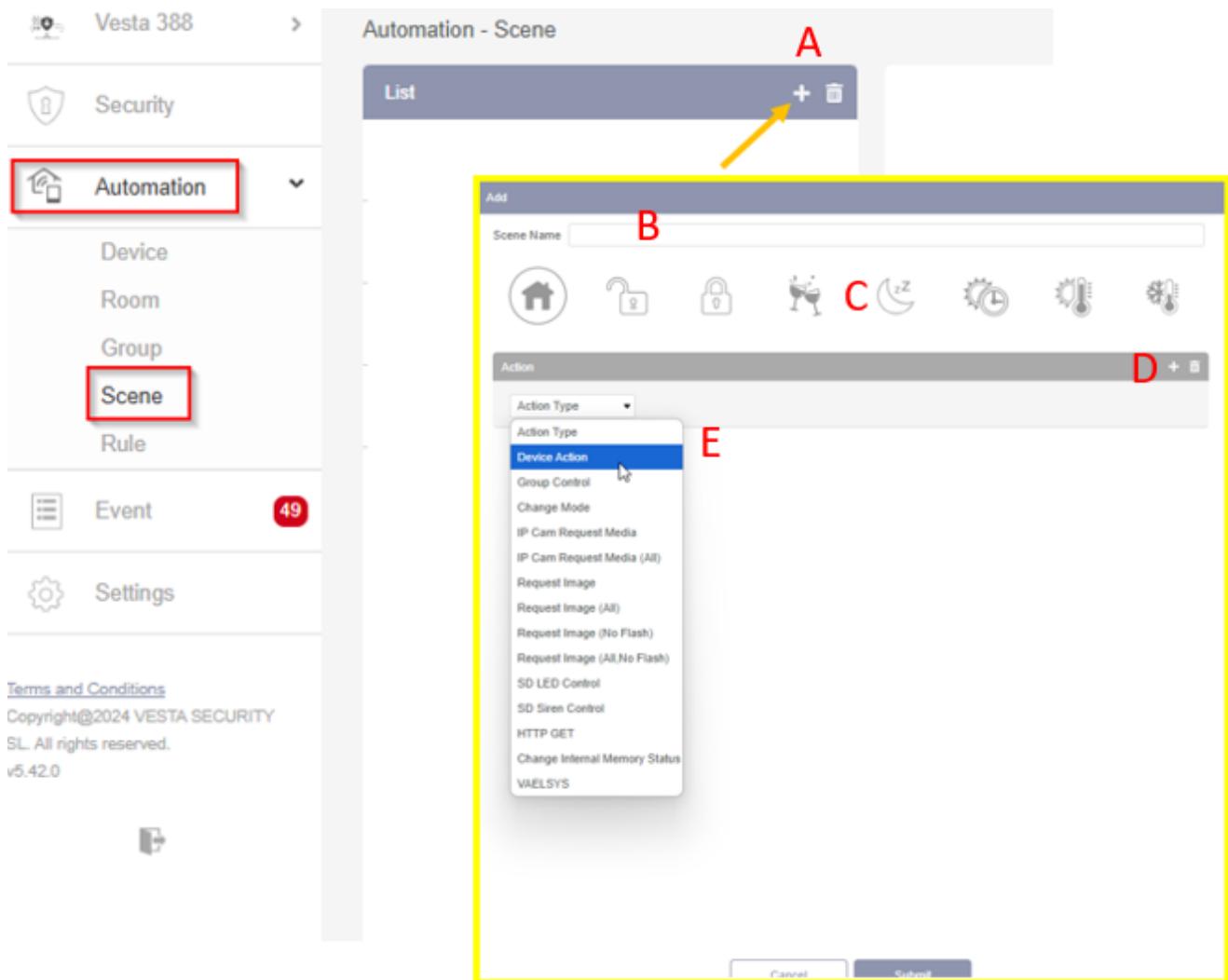
ACTIVACIÓN DE LA ESCENA	DISPOSITIVOS IMPLICADOS	ACCIÓN DEL DISPOSITIVO
La activación de las escenas puede ser de varias maneras como por ejemplo: Un selector de escenas, Geofence, con un dispositivo como un detector/contacto magnético ...etc o con Reglas	Enchufe del Salón	APAGAR
	Luces de la casa	APAGAR
	Calefacción	AJUSTAR TEMPERATURA A 22°C
	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 22°C, 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
<p>La activación de la regla, puede ser mediante calendario, sensores, cambio de modos (Armad/desarmado...), Detección por de movimiento por un tiempo...</p> <p>En este ejemplo: Calendario – De lunes a Viernes a las 18:00h</p>	Sistema: Armado	Activar Relé de la Electroválvula 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

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

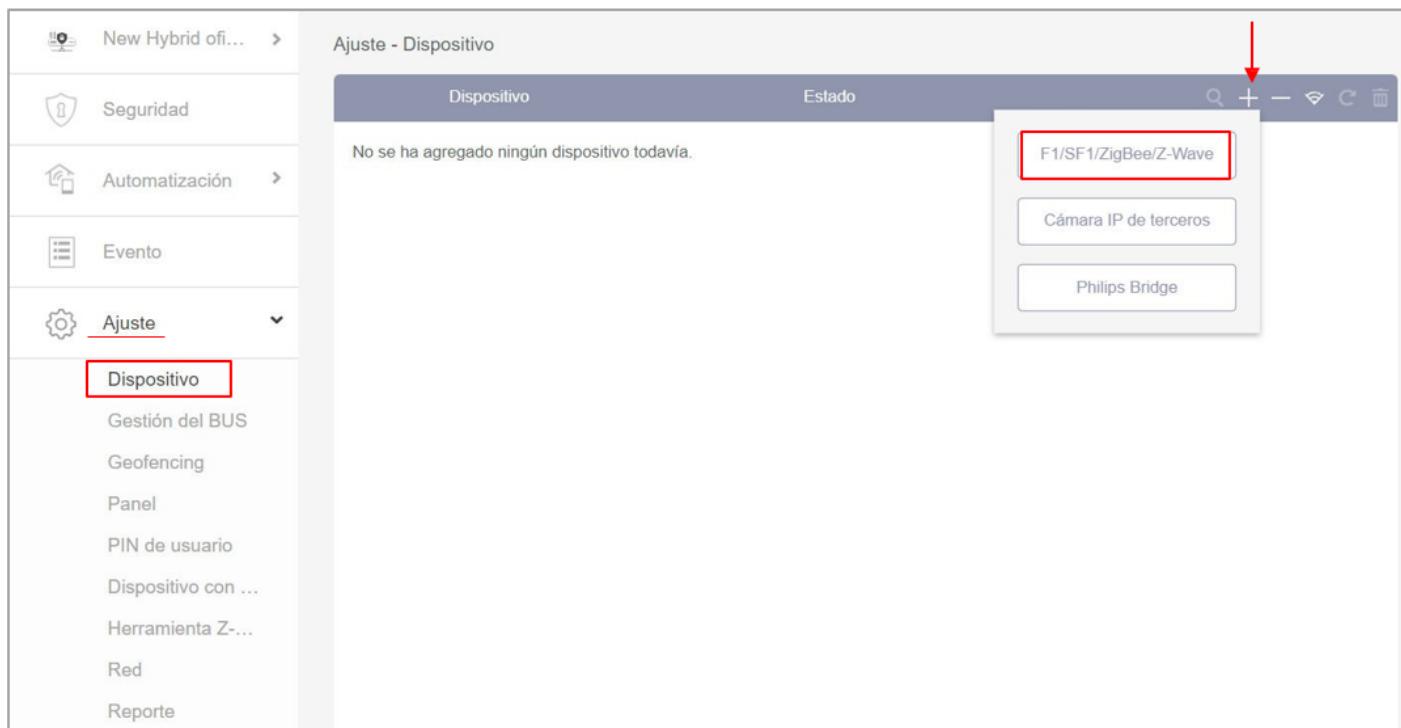


This addendum specifically discusses the software and hardware options available for system configuration and management using the proprietary V-MAX BUS technology. V-MAX devices are compatible with HYBRID-IMAX panel models only. In addition, the document will specify connection topologies, current V-MAX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

INDEX

1. Registration of V-MAX BUS devices
2. Zone and sensitivity settings
3. BUS Management
4. Hybrid Panel Architecture
5. V-MAX BUS Topologies
6. TIPs: General Installation Rules and Tips
7. BUS Calculator
8. Amplifier & isolator
9. Supervised Source
10. List of featured BUS equipment
11. Examples of unique solutions
 - a) V-MAX BUS integration of third-party wiegand readers 26
 - b) V-MAX BUS integration of any conventional detector

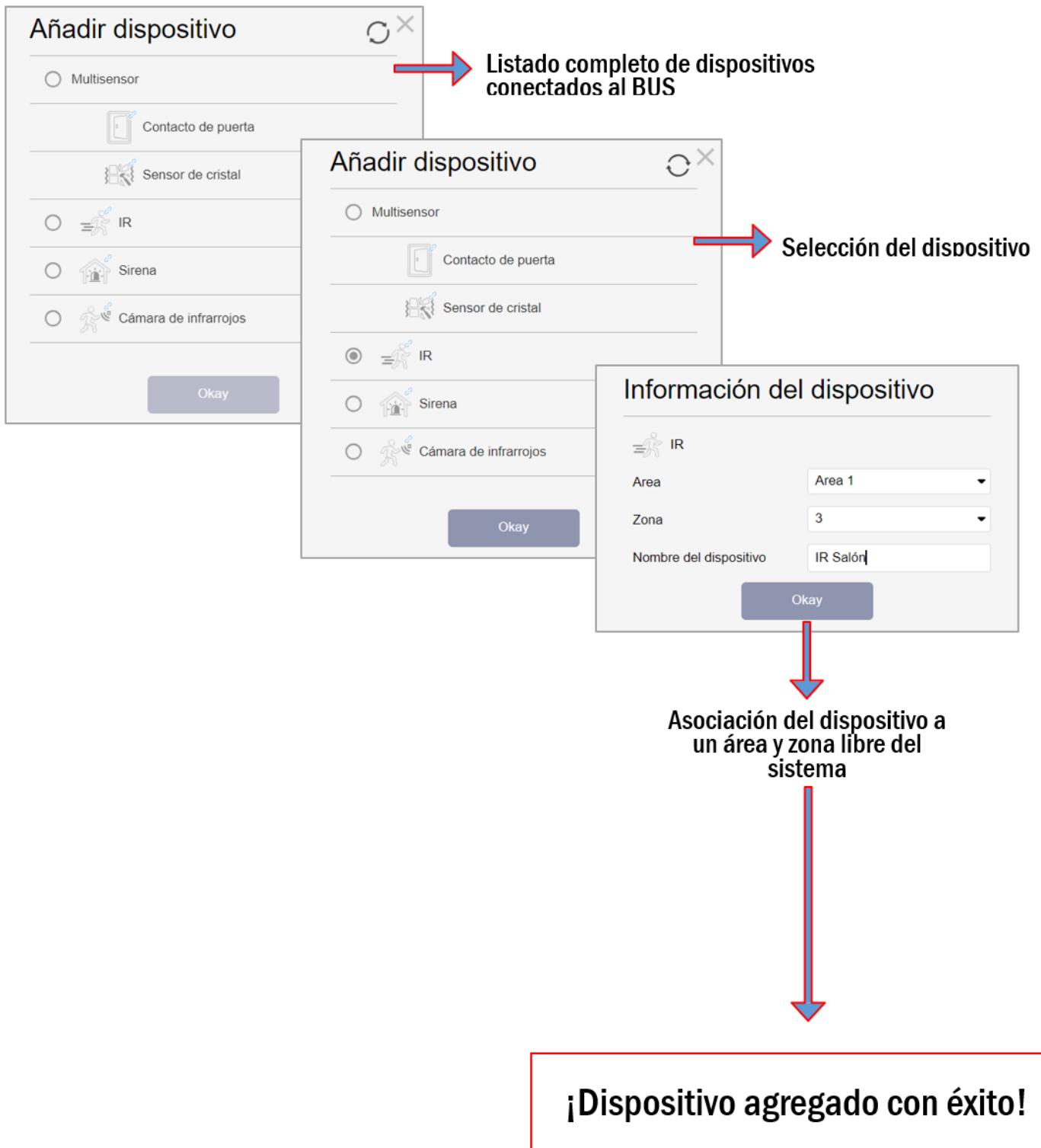
Device: Add Device



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]



Device: Internal device settings

The screenshot shows the 'Ajuste - Dispositivo' (Adjustment - Device) screen. On the left is a sidebar with icons for Seguridad, Automatización, Evento, and Ajuste, with 'Dispositivo' selected. The main area displays a device named 'IR Salón (IN:03078900)' under 'Area 1 (Zona 3)'. A context menu is open, indicated by a red box around the three-dot icon in the top right corner. The menu itself has a yellow border and contains the text 'Please select' at the top, followed by two options: 'Ajuste' and 'Configuración de infrarrojos', with the number '1' next to 'Configuración de infrarrojos'.

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

 IR

Area 1 Area 1 Zona 2 3 Nombre IR Salón Bypass 4 Apagado	24 HR <input type="checkbox"/> Alarma Respuesta Desarmado Ninguna respuesta Respuesta Armado Alarma Instantánea Respuesta Armado en Casa Ninguna respuesta Salida <input checked="" type="checkbox"/> Ninguna respuesta Respuesta de disparo de zona Aplicar escena - reset temp. de ir Respuesta de restauración Ninguna respuesta
Anulación Tamper 5 On Anular Supervisión 6 Apagado Bypass Anti-masking 7 Apagado Anulación automática Inhabilitar Activación 1 min (s) 2	9 1 0 1 1

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.

 IR

Inmunidad a mascotas 1 Inhabilitar
Sensibilidad 2 Alto 3 detecciones sin sleep time
3 Inhabilitar

No actuar

Retardo de entrada 1

Retardo de entrada 2

Timbre

Alarma de seguimiento Alarma instantánea Alarma Exterior

Alarma silenciosa Zona cruzada

New Hybrid of... >

- Seguridad
- Automatización >
- Evento
- Ajuste
 - Dispositivo
 - Gestión del BUS**
 - Geofencing
 - Panel
 - PIN de usuario
 - Dispositivo con ...
 - Herramienta Z-...
 - Red
 - Reporte

Términos y Condiciones
Copyright © 2020 ByDemes SL. Todos los derechos reservados.
v5.21.0

Gestión del BUS

Todos

Dispositivo	ID	EOL	Identificar
CM Universal BUS Area 1 (Zona 2) Contacto de puerta	IN:02ff6602	<input checked="" type="checkbox"/> EOL	Identificar
CM BUS Area 2 (Zona 1) Contacto de puerta	IN:02ff6600	<input type="checkbox"/> EOL	Identificar
IR Salón Area 1 (Zona 3)	IN:03078900	<input type="checkbox"/> EOL	Identificar
CM BUS Entrada Area 1 (Zona 4) 1 Contacto de puerta	IN:0303e800	<input type="checkbox"/> EOL	Identificar
Sismico entrada Sensor de cristal Area 1 (Zona 5)	IN:0303e801	<input checked="" type="checkbox"/> EOL	Identificar
Sirena Area 2 (Zona 1) Sirena	IN:03094400	<input type="checkbox"/> EOL	Identificar
Zona 3 Area 2 (Zona 1) Tecaldo		<input type="checkbox"/> EOL	Identificar
PIR CAM Area 3 (Zona 1) Cámara de infrarrojos	IN:030cf700	<input type="checkbox"/> EOL	Identificar
Sismico entrada Tamper abierto			

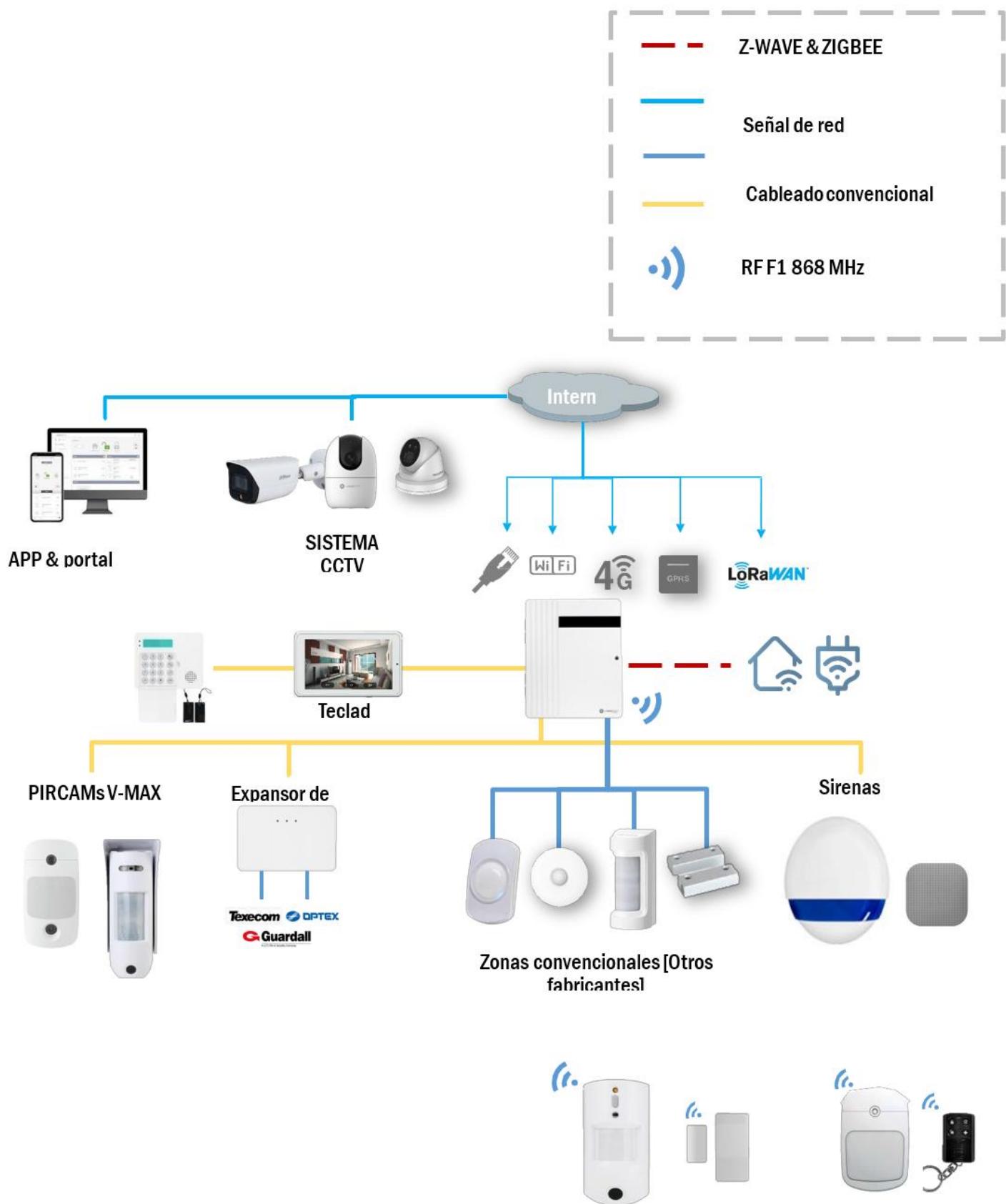
This section filters only the elements that make up the BUS, reflecting the area and zone that each element occupies.

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....

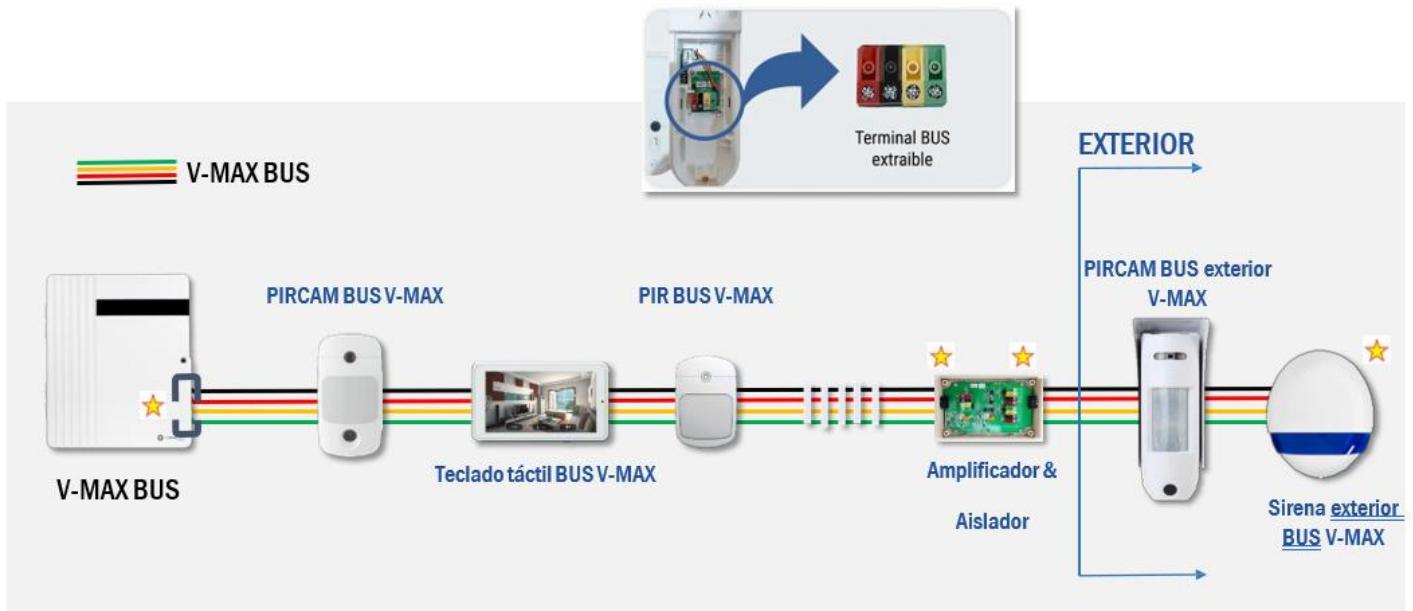
Schematic: jumper configuration (end of line resistance)



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

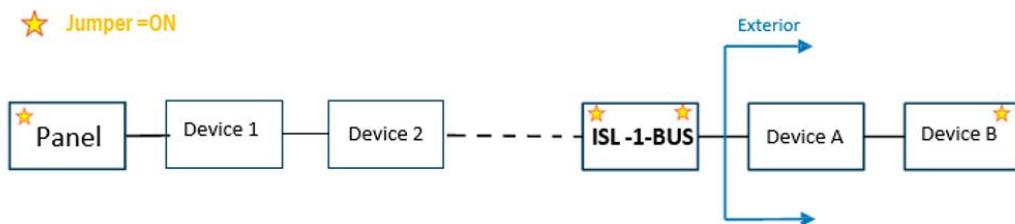


Flexible Cabling

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)

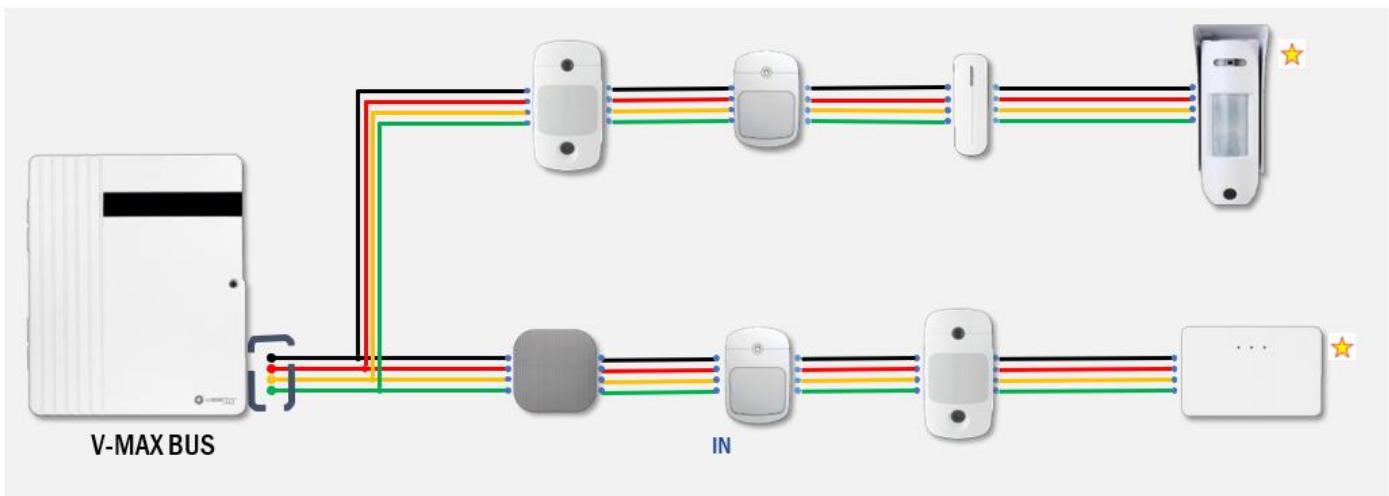
The use of the jumper is recommended to improve BUS communications in terms of reliability and speed. In this case, **the amplifier & isolator behaves as the end and start of a new independent branch** and therefore the jumpers are placed as follows the scheme.



Case 2a: Two (inside) star bus lines

*Max. 128 BUS devices

Flexible Cabling



Outline: jumper configuration (End of Line Resistance)

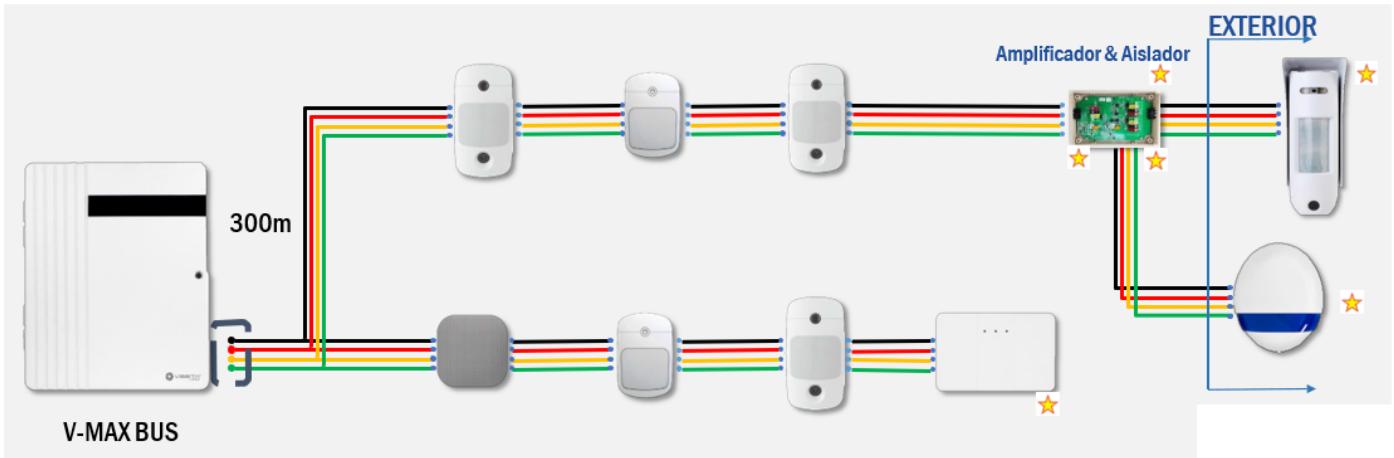


★ Jumper=ON

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

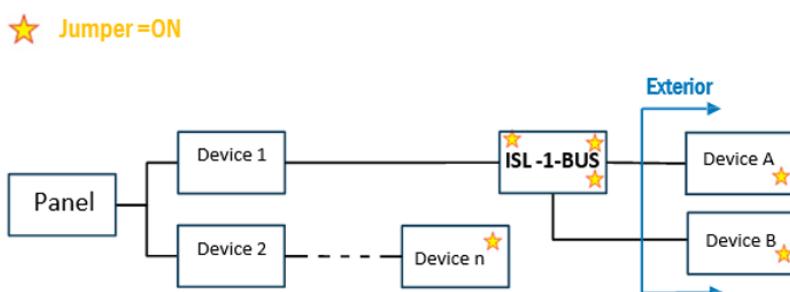
*Max. 128 BUS devices



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

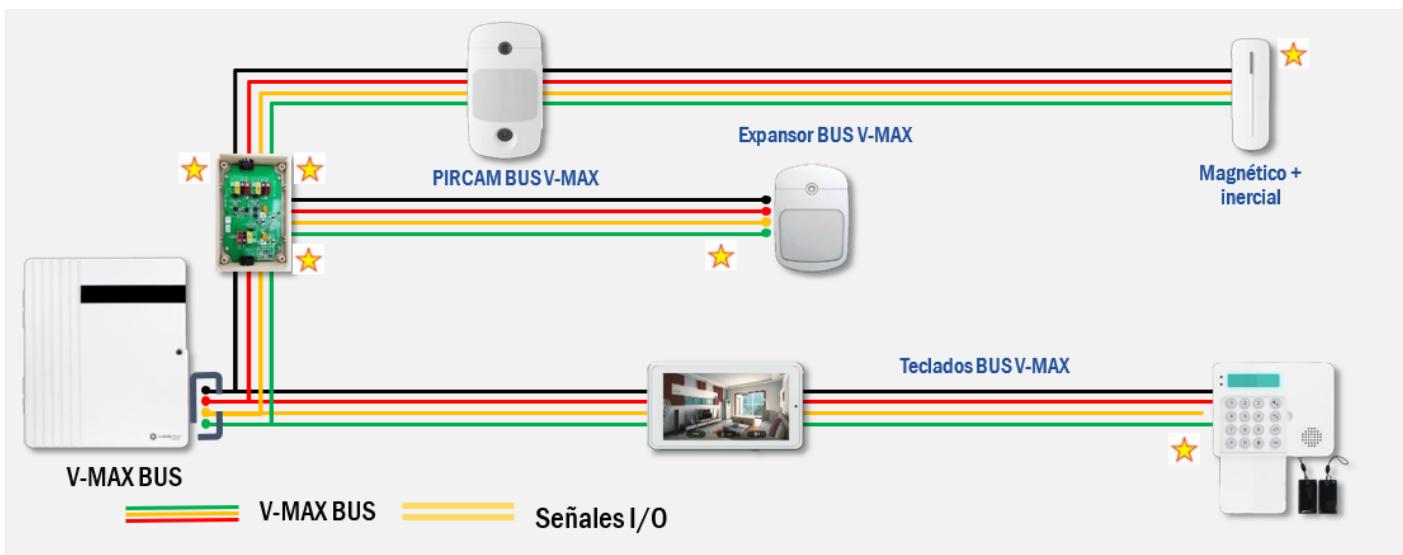
Schematic: jumper configuration (end of line resistance)

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

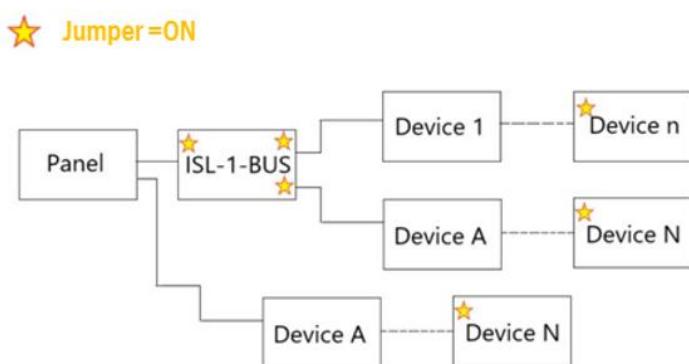


Flexible Cabling

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

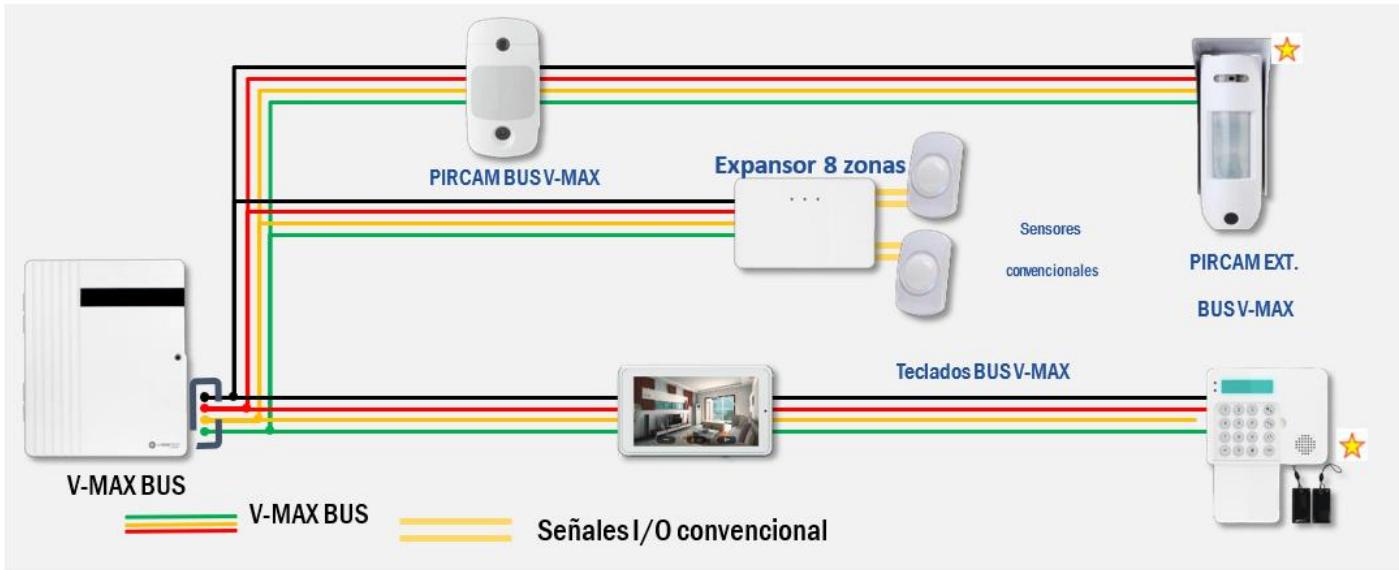
Schematic: jumper configuration (end-of-line resistance)

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

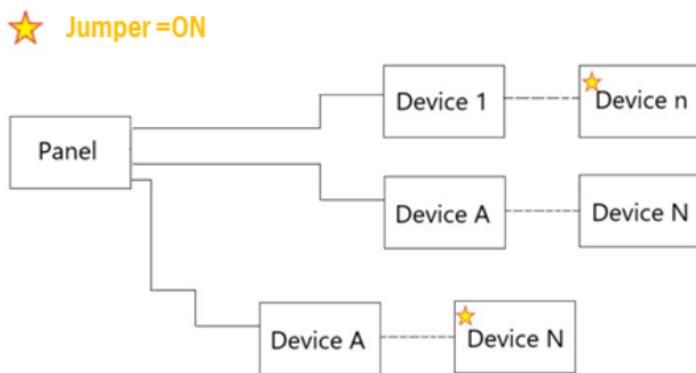


Flexible Cabling

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.

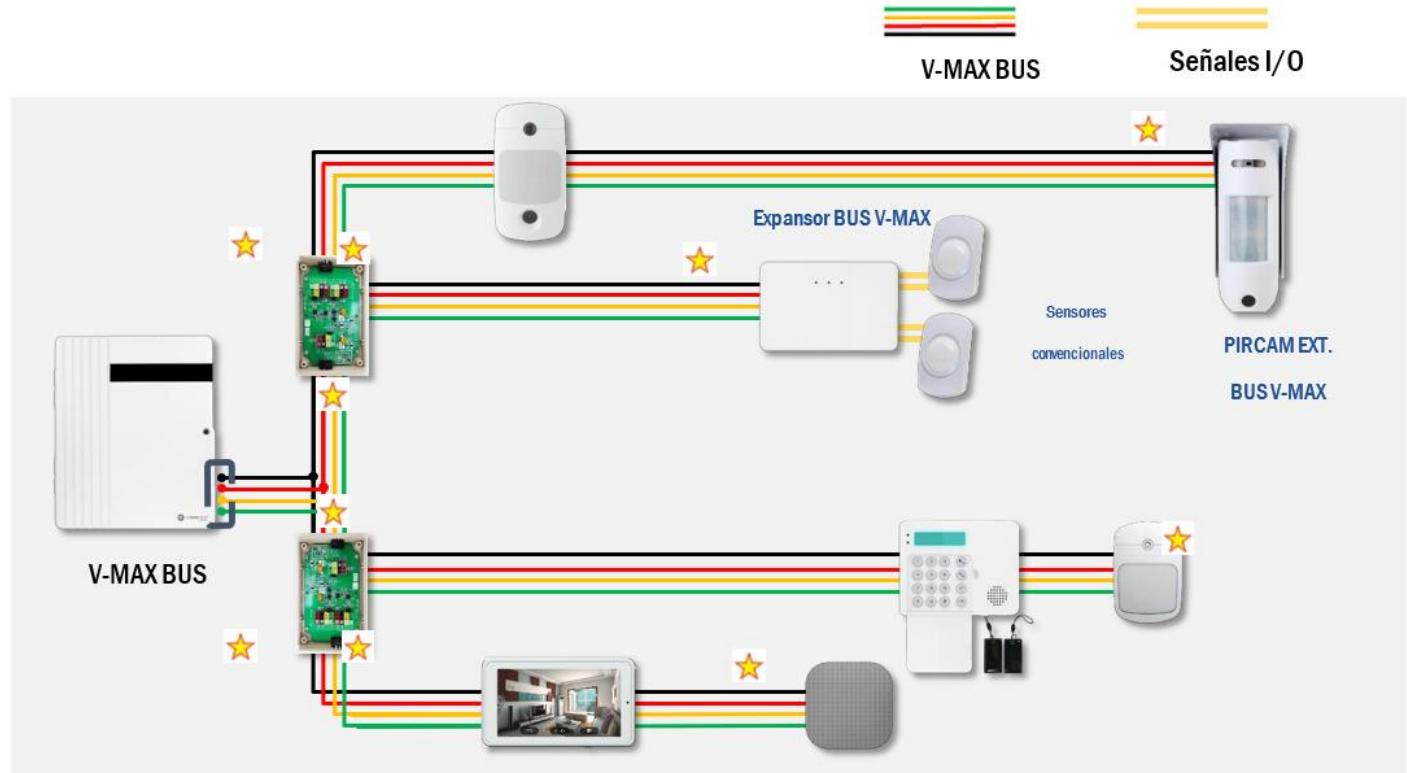
Schematic: jumper configuration (end-of-line resistance)

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



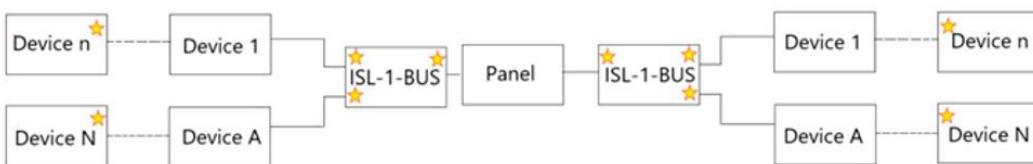
Flexible Cabling

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)

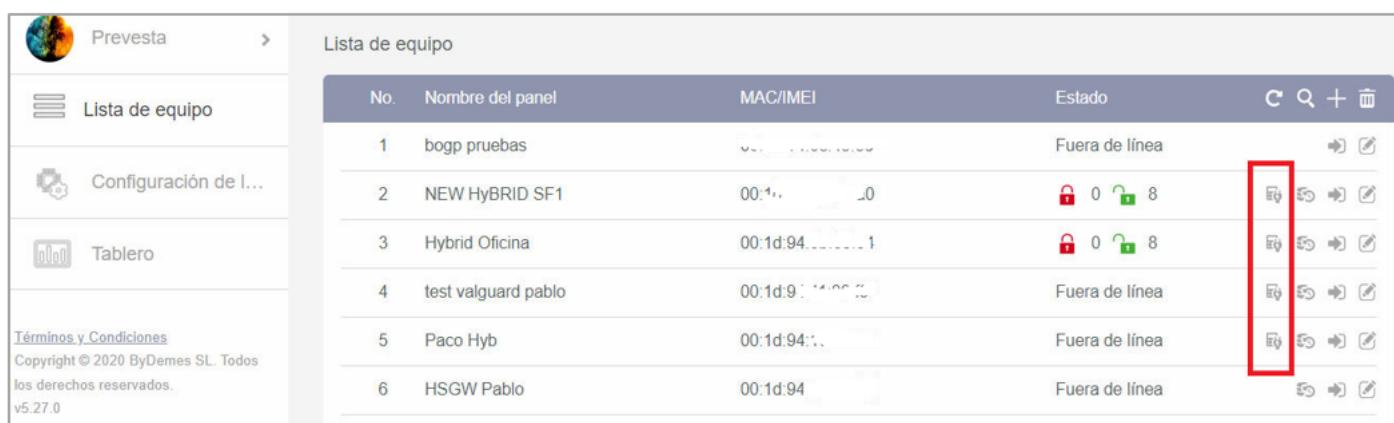
The use of the jumper is recommended to improve BUS communications in terms of reliability and speed. In this case, **the jumper will be placed at the start and end of each of the independent branches that are generated in each amp & isolator module.**

★ Jumper=ON



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)



Lista de equipo					
No.	Nombre del panel	MAC/IMEI		Estado	C Q +
1	bogg pruebas			Fuera de línea	
2	NEW HyBRID SF1	00:1d:94:...:0	0	0 8	
3	Hybrid Oficina	00:1d:94:...:1	0	0 8	
4	test valguard pablo	00:1d:94:...:2		Fuera de línea	
5	Paco Hyb	00:1d:94:...:		Fuera de línea	
6	HSGW Pablo	00:1d:94:...:		Fuera de línea	

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

1

Calculadora sistema Híbrido

Volver

Resultado: Okay

Tolerancia (%) 0

Corriente restante: 2000 mA

Zonas cableadas a bordo

No.	Tipo	Distancia	Potencia
Datos no disponibles.			

2

Dispositivos BUS Línea 1 Tensión restante: 13.5 V

No.	Tipo	Distancia
Datos no disponibles.		

Dispositivos BUS Línea 2 Tensión restante: 13.5 V

No.	Tipo	Distancia
Datos no disponibles.		

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]

Prevista >

Calculadora sistema Híbrido

< Volver

Resultado: Okay

Tolerancia (%) 0 Corriente restante: 2000 mA

Zonas cableadas a bordo

No.	Tipo	Distancia	Potencia
3	AWG22	Datos no disponibles.	+

1 2

Dispositivos BUS Línea 1 Tensión restante: 13.5 V

No.	Tipo	Distancia
4	AWG22	Datos no disponibles.

Dispositivos BUS Línea 2 Tensión restante: 13.5 V

No.	Tipo	Distancia
5	AWG22	Datos no disponibles.

[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

Añadir dispositivo

Tipo: Dispositivo de zona cableada

Distancia (m):

Por favor, introduzca la distancia (metros) entre Hybrid y el dispositivo instalado (la longitud real del cable se multiplicará por dos).

Potencia (mW):

Introduzca el resultado de multiplicar la corriente por la tensión máxima.

[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

Añadir dispositivo

Tipo	892-BUS
Distancia (m)	<input type="text"/>
Introduzca la distancia (metros) entre el dispositivo BUS instalado y el anterior (la longitud real del cable se multiplicará por dos).	
<input type="button" value="Cancelar"/>	<input type="button" value="Enviar"/>

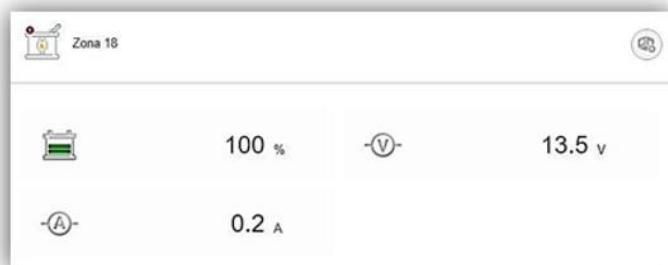
[3] Distance: accumulated cable distance from the immediately preceding BUS element

[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

Calculadora sistema Híbrido

Zonas cableadas a bordo

Dispositivos BUS Línea 1

No.	Tipo	Tensión restante
3	IR-35-BUS	4.6 V
4	IR-35-BUS	3.5 V
5	DC-23-BUS	3.5 V
6	KPT-35 Combo	3.5 V

PWB

No.	Tipo	Distancia
1	892-BUS	300 m

Resultados:

- Resultado: Sobrecarga (en la zona de PWB)
- Resultado: Okay (en la zona de 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 magnéticos



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 NIVELES DE
BATERÍA



CONFIGURACIÓN REMOTA
DESDE APP



AMPLIFICADOR Y AISLADOR
DE SEÑAL

Sirenas



SIRENA DE HASTA 110 dB

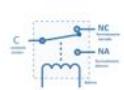


SUPERVISIÓN Y DETECCIÓN DE
MANIPULACIONES



CONFIGURACIÓN REMOTA
DESDE APP

Salidas de relé



SALIDA DE RÉLE
CONTACTO SECO HASTA
10A

Encapsulado, TMP,
batería Backup,
conector DC 12VDC



SALIDA DE RÉLE
CONTACTO SECO HASTA
10A

Detector de incendio



3 EN 1

- Detector de humo

- PIR 360°

- Sirena



SIRENA DE
HASTA 85
dB



SEÑALES DE
ALARMA



CONFIG.
REMOTA
DESDE APP



AUTOMATIZ
ACIONES

Doble tecnología



DETECCIÓN 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



CONFIG.
REMOTA
DESDE APP



F1 2km

V-MAX

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

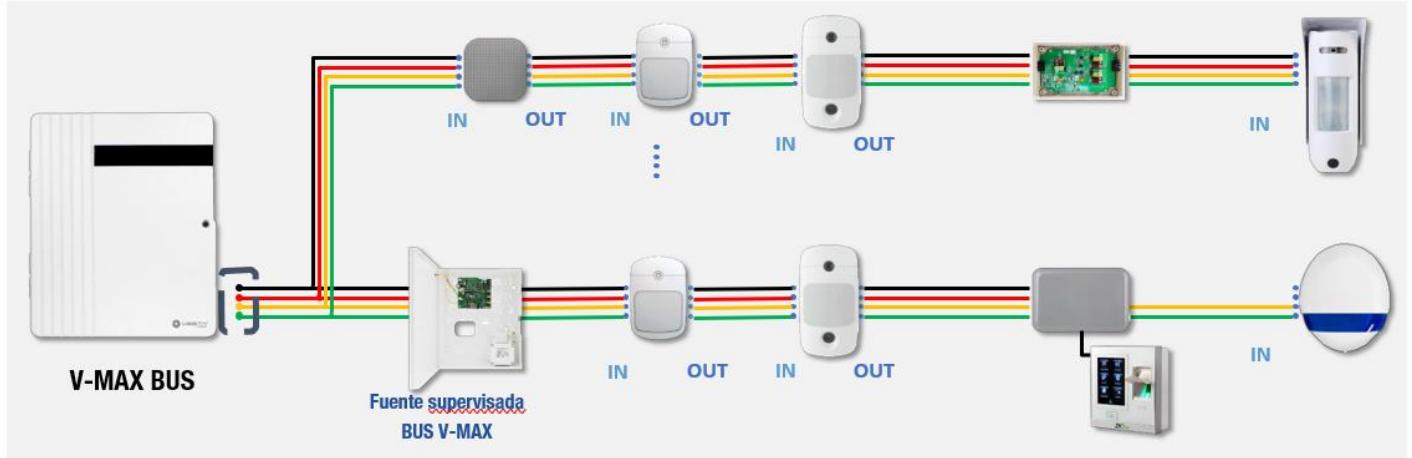


SUPERVISIÓN Y DETECCIÓN DE
MANIPULACIONES



VINCULACIÓN CON
AUTOMATIZACIONES

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

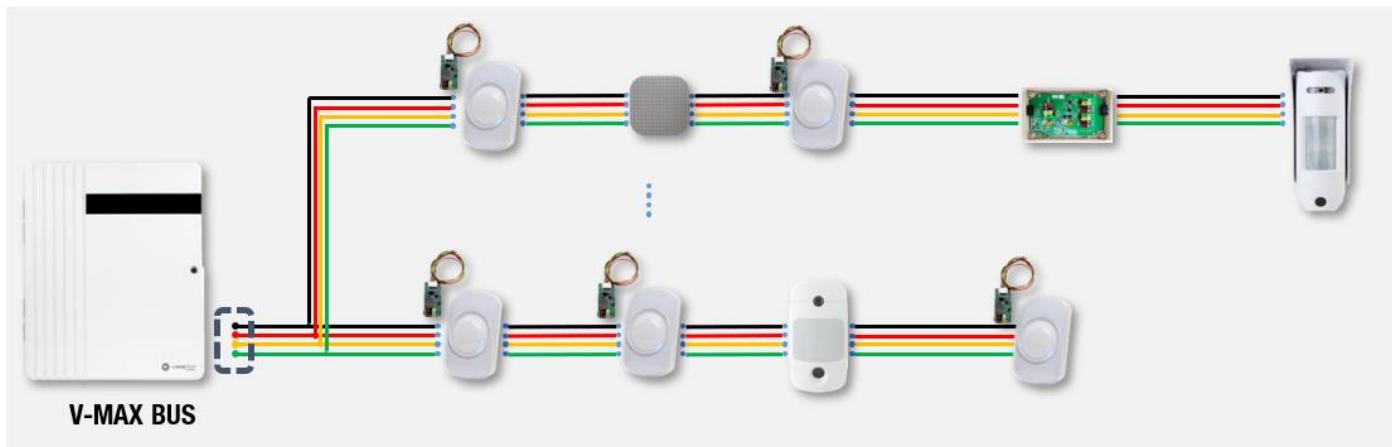


Wiegand 26 controller, vesta-344.

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.