



# AF927PLUS and AF927PLUSTC

Wireless/Wired central units  
with built-in Wi-Fi module



## INSTALLATION AND USER MANUAL

# SUMMARY

<i>AF927PLUS and AF927PLUSTC - INSTALLATION MANUAL</i> .....	3
<i>INTRODUCTION</i> .....	3
<i>TECHNICAL FEATURES</i> .....	4
POWER SUPPLY UNIT .....	5
Sizing of the system .....	6
Protections on the 12-14Vdc power supply and usage limitations .....	6
DISPLAY ELEMENTS.....	6
<i>INSTALLATION</i> .....	7
PRECAUTIONS FOR CORRECT CONTROL UNIT INSTALLATION .....	7
GENERAL INFORMATION .....	7
OPENING THE BOX, WALL MOUNTING .....	7
GUARD PREVENTING OPENING AND REMOVAL.....	8
SECURITY: SUPERVISION, ANTI-TAMPER, BATTERY CHECK, ANTI-SCANNER. ....	8
<i>PROGRAMMING: PRELIMINARY OPERATIONS AND QUICK START-UP</i> .....	9
PRELIMINARY OPERATIONS .....	9
PRELIMINARY OPERATIONS FOR CONNECTION TO AVECLOUD (RECOMMENDED). ....	9
DEFAULT DATA AND QUICK PROGRAMMING FOR AF927PLUS (model without screen) .....	10
RAPID PROGRAMMING FOR AF927PLUSTC (model with screen).....	26
<i>CONTROL UNIT MENU - INSTALLER INSTRUCTIONS</i> .....	29
SUMMARY OF HOME PAGE FUNCTIONS .....	29
MEANING OF MULTI-STATUS ICONS .....	30
Type of user connected to the control unit: .....	30
Cloud status: .....	30
Remote connection status (remote service):.....	30
MEANING OF THE OTHER CONTROL UNIT ICONS.....	31
System activation.....	31
Control Unit Events Memory .....	31
Scenarios Management and Time Programmer .....	31
User Management .....	31
View Cameras .....	31
Test functions .....	31
Communication parameters .....	31
Settings .....	31
Devices and Areas.....	33
INTRUSION DETECTOR PARAMETERS .....	38
Parameters common to all devices .....	38
AF963R-DB (PIR) – AF965R-DB: Double PIR curtain-effect detector - additional parameters .....	39
AF964R-DB: outdoor double PIR radio detector + microwave technology - additional parameters .....	40
AF976R-DB: outdoor double PIR radio detector, long range curtain effect - additional parameters .....	40
AFTR02: universal transmitter for technical alarms .....	40
AF53903R-DB: radio siren.....	41
AFTRA03: signal repeater .....	41
RADIO KEYPAD PARAMETERS.....	41
BYPASSING DEVICES.....	42
VOICE MESSAGES .....	43
GENERAL SETTINGS.....	45
Scenario management.....	46
General control unit parameters .....	48
System information .....	50
Utilities .....	51
Programming summary .....	54
REMOTE SERVICE .....	54
EVENTS.....	55
SYSTEM TEST .....	56
Field meter - Radio range .....	57
Radio range - preventive check .....	57
Device test .....	57

Dialler tests.....	58
Siren test.....	59
Image test.....	59
Relay test.....	59
Monitoring.....	60
Wired inputs.....	61
COMMUNICATION PARAMETERS.....	63
Choose connection type.....	63
Mail.....	66
AVE Cloud.....	67
Other communication parameters and interfacing with AVE home automation system.....	67
USERS.....	69
CODE RECOVERY PROCEDURE.....	71
WIRED BOARD.....	71
DESCRIPTION OF TERMINAL BLOCK.....	72
CONFIGURATION OF INTERNAL WIRED BOARD.....	73
Input configuration.....	74
NC DOUBLE.....	75
Output configuration.....	76
KEYPAD.....	77
WIRED KEYPAD AF990.....	77
ASSOCIATION OF THE KEYPAD TO THE CONTROL UNIT:.....	77
RADIO KEYPAD AF970R-DB.....	78
INTERFACE WITH THE MODULES OF THE CIVIL SERIES AVE SMART IoT.....	79
CONFIGURATION OF THE CONTROL UNIT.....	79
WIRING DIAGRAM FOR WIRED INPUTS.....	81
INPUT CONNECTION TYPES FOR CORRECT BALANCING.....	81
EXAMPLE OF CONNECTION.....	82
GSM TELEPHONE DIALLER MODULES - art. AFGSM04, GSM 4G - art. AFGSM04-4G.....	83
FAQ.....	86
<b>APPENDIX.....</b>	<b>88</b>
AF927PLUS and AF927PLUSTC - AVE Firmware Settings.....	88

## **AF927PLUS and AF927PLUSTC - INSTALLATION MANUAL**

### **INTRODUCTION**

AF927PLUS is a wireless / wired central unit with built-in Wi-Fi module. It can manage up to 99 detectors individually identifiable through the "label" function which, when properly programmed, shows the point of origin of the alarm on the display (eg: living room, kitchen, corridor, etc.). Thanks to a vocal synthesis provided on board, the label can also be of the vocal type. This makes it possible to identify the individual detector by means of a programmable voice message. The vocal synthesis also allows the recording of voice messages that inform the user about the main events that have occurred on the system (eg. door open; system armed; system disarmed; etc.). The wired board allows you to manage n.8 inputs with free balancing and n.16 with NC balancing. A wired output can also be controlled by time, thanks to an internal timer, to manage the load by time slots.

## TECHNICAL FEATURES

Note: the following is valid for both AF927PLUS and AF927PLUSTC models, unless otherwise specified. The difference between the two central units is only relative to the presence of a 7" LCD screen on the AF927PLUSTC central unit which has been replaced by a LED on the AF927PLUS central unit.

- **Main power**
  - 230Vca -15%+10% - 50/60Hz
- **Secondary power source:** To be completed with 2 batteries 12V/1,8 Ah - reference AF911
  - Maximum charging time: 3h
  - Signal for low battery at 10,9V and charged battery at 11,4V
- **Central unit features:**
  - Transmission/Reception RF 433MHz/868MHz GFSK Dual band, UE- standard 300-220-1; 300-330; 300-440, wireless range in free air without interference 100m. The wireless range can undergo a significant reduction in indoor spaces also due to the position of the devices (detectors, sirens, etc.) in relation to the structure of the premises.
  - Wireless Inputs:
    - n.99 wireless channel – n.99 detectors individually identifiable with a text label via LCD display or voice label, individually delayed with AND function.
  - Wired Inputs:
    - n.8 wired inputs with double balancing
    - n.1 double balanced input for wired electro-mechanical activator with at least 300 combinations.
  - Radio outputs:
    - coded 72-bit digital transmission for “alarm” - “total activation” - “partial activation” - “deactivation” + 16 coded commands that can be managed
  - Wired outputs:
    - n.1 for indoor siren control
    - n.1 for outdoor self-powered siren
    - n.2 programmable relays for various free exchange functions (max 500 mA@12V).
  - n.6 activation areas (1,2,3,4,5,6).
  - Radio tamper detection: reception of tamper signal from each individual detector - reception of “alive” signals transmitted every 28 minutes and of low battery signal (SUPERVISION) if necessary.
  - R.F. anomalies: continuous, simultaneous and programmable control of the 2 operating frequencies.
  - Possibility to store n.32 AF943R remote controls, individually identifiable with a text label via LCD display or voice label.
  - Memory of last 500 events (non-volatile memory).
  - Event messages. Voice messages can be recorded to inform the user in real time of the main control unit events (control unit on; control unit off; door open; outdoor detector alarm; pre-alarm; tampering; new event)
  - Timing: activation delay, programmable from 1 to 99 seconds - input delay, programmable on each detector, from 1 to 45 seconds - general alarm time, 3 minutes fixed - programmable 24h clock
  - Displays: 2x16-character display, with the ability to identify each individual peripheral
  - Indoor siren: 106dB alarm siren
  - Acoustic signals: voice messages to guide installation and user communications + low intensity buzzer.
  - Built-in Wi-Fi module
  - DIMENSIONS: 307x200x53mm
  - WEIGHT:
    - AF927PLUSTC 2.0 Kg
    - AF927PLUS 1.5 Kg
  - TEMPERATURE: operating/storage: -25°+55°C – Humidity 95%.

- **Characteristics of dialler AFGSM04, AFGSM04-4G:**

**AFGSM04:** GSM/GPRS module for AF927PLUS and AF927PLUSTC control units with antenna. This device enables the control unit to perform all telephone activities over the mobile network, i.e. caller ID, two-way voice, SMS, MMS, digital transmissions with SIA protocol, e-mail transmissions.

**AFGSM04-4G:** in addition to those described for control unit AFGSM04, the AFGSM04-4G enables remote control unit management via the AVE Cloud service.

### VIA SMS MESSAGES FUNCTIONS

It is possible to control the control unit with SMS messages. These commands are subject to the timing allowed by the SIM manager, so they may not be received immediately.

**Attention!** " " = space

**Command / control from the central unit**

Operazione	SMS to send	Answer from the plant
check the ON-OFF status of the plant	C?	ON ̀ OK    ACF(zone) ̀ OK    OFF ̀ OK
total arming of the control panel	ON	ON ̀ OK
partial arming of zones	ON ̀ ACF(zone)	ON ̀ ACF(zone) ̀ OK
disarming of the control panel	OFF	OFF ̀ OK
reading of the events memory	MEM?	last 3 events as indicated in the historical memory
request for the remaining SIM credit	?	answer € according to the SIM manager's modalities

**EC Declaration of Conformity:**

The manufacturer AVE SPA declares that the radio-based intrusion detection control unit, code AF927PLUSTC and AF927PLUS and related GSM module AFGSM04, comply with Directive 2014/53/EU.

The full text of the EU declaration of conformity is available at: [www.ave.it](http://www.ave.it).

**POWER SUPPLY UNIT**

The internal power supply unit supplies a nominal voltage of 14.5Vdc (@100-240V – 50/60Hz) and a current of 1.6A; to facilitate calculation of total absorption and thus autonomy in the case of mains power outages, the following table is provided:

Code		AF927PLUSTC				AF927PLUS	
Features of the power supply unit		14.5V – 1.6A (@100-240V – 50/60Hz)					
Rechargeable batteries		2x12V – 2.2Ah					
Code		AF927PLUSTC				AF927PLUS	
Power supply condition		230 V OK			Black OUT	230 V OK	Black OUT
LCD brightness		100%	50%	10%	0%	n/a	n/a
Current consumption in stand-by	Control unit	390	300	200	30	150	20
	Wi-Fi module	40	40	40	<del>Wi-Fi</del>	40	<del>Wi-Fi</del>
	Wired board	20	20	20	20	20	20
	2G GSM module (AFGSM04)	10	10	10	10	10	10
	GSM 4G module (AFGSM04-4G)	45-80	45-80	45-80	45-80	45-80	45-80
	Wired Keypad (AF990)	40	40	40	40	40	40
Total		<b>500 (570)</b>	<b>410 (490)</b>	<b>310 (380)</b>	<b>100 (180)</b>	<b>260 (330)</b>	<b>90 (160)</b>

Unless otherwise indicated, the values are given in mA.

In brackets the maximum absorption value with telephone dialler art. AFGSM04-4G.

**Note:**

- In the event of a power failure, the control unit automatically switches the Wi-Fi module off to save energy. However, a special parameter is available so both Wi-Fi module and 4G GSM module can be kept active simultaneously (see chapter GSM programming).
- To guarantee 24-hour system autonomy in the event of a power failure, it is not advisable to exceed a maximum absorption value of 180mA (with two 12V 2.2Ah batteries).
- When using wired devices, a consumption of 120mA should not be exceeded. Should it be necessary to connect a larger number of devices, an additional power supply unit with back-up battery must be used and the fault signal for this power supply reported to the control unit or a wired bus input board (art. AFEX6I-REN).
- The AF927INTLAN interface has a consumption in use of 230 mA.

## Sizing of the system

When using the control units, the installer must pay utmost attention to sizing of the system, with an eye power consumption and resulting autonomy. EN 50131 sets the minimum power failure autonomy for Grade 2 at 12 hours: this must be guaranteed (see table above).

How the system is used involves aspects that affect consumption, in particular the brightness of the display, absorption of any sirens self-powered via cable and of any 12V peripherals connected via cable. These factors must be properly considered in relation to the rating of the power supply unit which must, in turn, be able to ensure that connected batteries are properly charged. The table shows the absorption of the 2 control unit models and any related batteries: for each system the following must be calculated:

- Maximum absorption: this is done by adding the consumption of any other equipment cabled to the control unit; this must never exceed the capacity of the power supply (it is advisable to keep absorption to 80% of nominal capacity)
- Minimum autonomy in the absence of 230V power supply, considering the current available from the battery at 80%.

## Protections on the 12-14Vdc power supply and usage limitations

- a) Max current limit: 200mA to charge internal battery/batteries (EN 50131-1: the maximum 72-hour charging is met)
- b) Current limit, achieved with resettable polyswitch: 650mA to recharge the battery of any wired siren (art. AF53900N)
- c) Limit for current designated to supply wired peripherals, achieved with resettable polyswitch: this must not exceed 200mA if the control unit has 2 batteries, 80mA if it has only one battery.

## DISPLAY ELEMENTS



- **AF927PLUS:** multifunction LED.

Green, on steady = control unit off

Green, flashing: control unit off and not powered from mains

Green, flashing 10 seconds upon deactivation: new event (see event history memory)

Orange, on steady: Initial powering up / Upgrade in progress / Maintenance

Orange, flashing: under maintenance and not powered from mains

Red, on steady: control unit on (flashes for the time it takes to exit)

Red, flashing: control unit on and not powered from mains (continues flashing after the time required to exit)



- **AF927PLUSTC:** 7" colour touch screen LCD display.

Multifunctional colour touch screen,

LCD Dimensions: 7"

Screen saver function with date and time

# INSTALLATION

## PRECAUTIONS FOR CORRECT CONTROL UNIT INSTALLATION

These devices may only be used in the context of an alarm system and only as described in this manual.

They must be installed on site solely by technicians specialized in “electronic security”. Except for the accessible compartments, opening the units immediately voids the industrial warranty. Any other use is considered improper and prohibited. The manufacturer cannot be held liable for any damages resulting from misuse of the product; that is for any use other than that indicated in this manual.

All control units operate by transmitting and receiving radio signals that are compliant with current standards: therefore, they must be wall-mounted using the supplied screws and plugs and under conditions that allow for good propagation of such signals. For this reason, niches and/or columns and/or walls of reinforced concrete should be avoided, as should installation inside metal cabinets. Extensive metal surfaces and metal grates near the control unit must also be avoided, even if embedded in walls. Positioning must take into account the mandatory position of the detectors and sirens, making certain that the control unit is “central” to these units.

The quality of the signal received by control unit can be checked and, when in doubt, this check should be performed before securing the control unit to the wall: when working with radio devices of this type, always remember that moving just a few tens of centimetres can often significantly improve signal transmission/reception.

It is best for the control unit to be hidden from view but, at the same time, installed in a convenient position where all its functions, including voice information, can be used. Useful sites are: behind doors, inside wooden or plastic cabinets, behind pictures and/or pieces of furniture. It is advisable to avoid installation near other electronic devices.

Once the position has been defined, the connection wires that are to enter the back of the device — possibly by breaking through the entry spaces arranged on the container — must be brought together. In particular, the cable carrying power from the mains must be disconnected upstream during installation.

## GENERAL INFORMATION

These devices are the heart and brains of a modern alarm system: equipped with the appropriate peripherals (detectors, sirens, etc.), they manage the burglary/aggression intrusion detectors, both wireless and wired, all types of wireless “technical” alarm sensors (water, smoke, gas, temperature, etc.), self-powered Wi-Fi cameras, remote actuation devices.

Depending on the models and accessories included in the system, the control units can trigger high-powered acoustic alarms and/or local warning messages through the appropriate wired and wireless sirens. They also activate landline and mobile telephone calls, SMS messages, digital calls to surveillance centres. All operating functions can be managed remotely via smartphone, tablet, web page and through the free AVE Cloud application (from activation/deactivation to requesting of control frames and “push” signalling of new events).

The control units operate connected to the power mains and have a power supply able to keep the rechargeable lead batteries optimally charged; these batteries are located in a space at the bottom of the box, together with the cabled portion of the devices, thus enabling convenient wiring. Protection against opening/removal is guaranteed by special break-in sensitive elements. The various functions are always shown in clear text on the display of the device or that of the connected remote devices and are protected by a specific installer and user access codes (PIN).

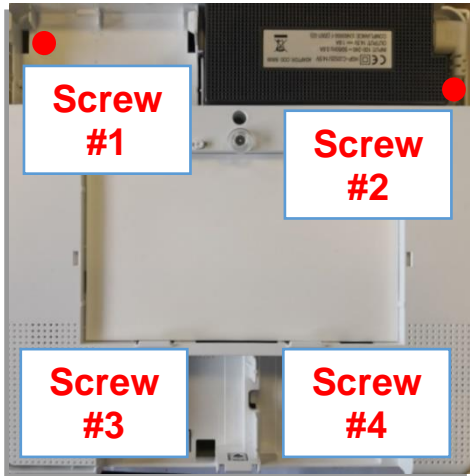
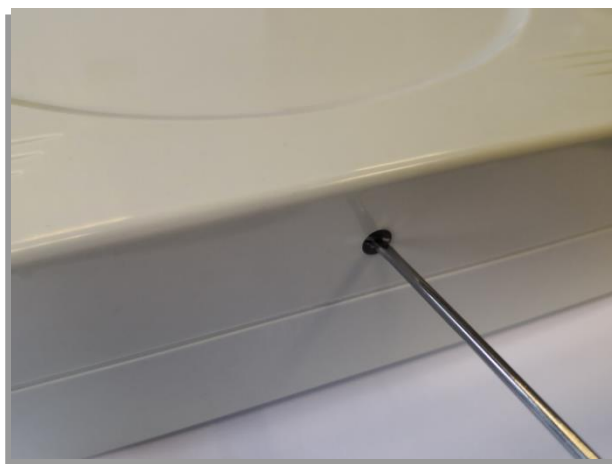
## OPENING THE BOX, WALL MOUNTING

Control unit boxes are opened by unscrewing the single screw on the bottom and removing the cover. On the inside, there are 4 more screws that, with a hinged, “book-like” structure (located to the left of the casing) provide access to the compartment containing the wired board and batteries.

The cables are routed through the pre-formed compartments at the bottom of the boxes. All electrical connections must be made in a workmanlike manner, in compliance with the standards and using cables of suitable section.

**Secure the device’s removal protection magnet** on the back **before securing the control unit** to the wall using the provided template.

The control unit must be secured to a wall, at a suitable height, using the screws and plugs provided.



## GUARD PREVENTING OPENING AND REMOVAL

The opening signal is guaranteed by spring-loaded buttons, the removal prevention signal by a magnet that must be secured to the wall/support that will hold the control unit using a special template.

## CONNECTION TO THE 230Vac POWER SUPPLY

Carefully follow the precautions given below:

- Use flexible cable with conductor having a cross-section of at least 0.75mm<sup>2</sup>
- The cable connection terminal is located in the centre of the battery compartment.
- Secure the cable well by tightening the screw of the cable block, after having connected it to the terminals. The control units do not require earthing.
- Always disconnect the mains power supply before working on the control unit: always connect the device to the power mains using a 16A C curve Circuit Breaker.

## SECURITY: SUPERVISION, ANTI-TAMPER, BATTERY CHECK, ANTI-SCANNER.

The various system devices communicate with one another via two-way radio communication in which each signal is followed by confirmation: this enables the supervision of all wireless devices, with warning in case of failure, and control of battery charge, with signalling when replacement is needed. In addition, in each device, the anti-tamper controls are always active so that any attempt to open the casings and/or detach the unit from its housing are immediately reported and cause an alarm, even when the system is disconnected. For this reason, the control unit must be set in TEST mode before the batteries are replaced. The control unit checks whether there is any radio interference that could prevent system function and signals this when needed. Network connection: the control unit accommodates all security systems that must be properly enabled to prevent unauthorized access.

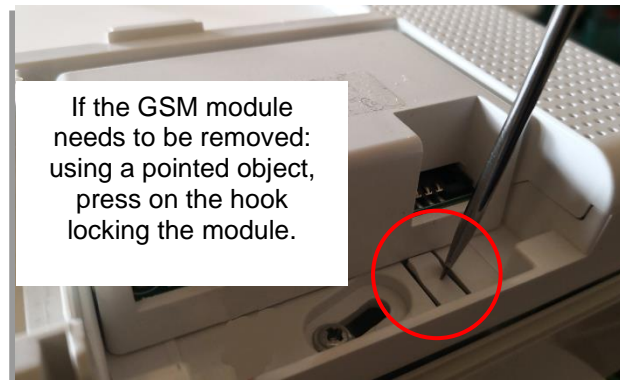
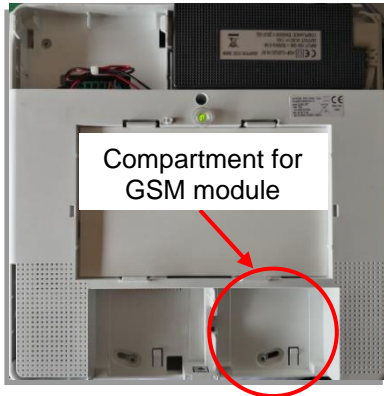
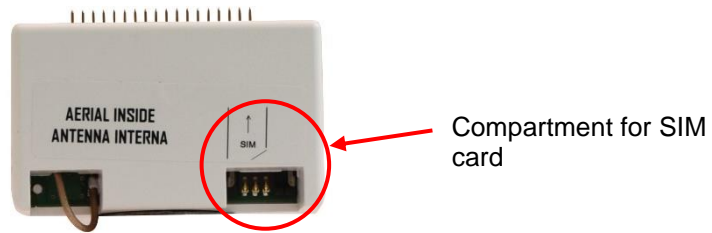
**Warning!** The manufacturer declines all responsibility for any unauthorized access that may occur.



## PROGRAMMING: PRELIMINARY OPERATIONS AND QUICK START-UP

### PRELIMINARY OPERATIONS

- With the control unit completely switched off, if applicable, insert the AFGSM04, AFGSM04-4G, AFGSM04-AE modules with its SIM card (note: deactivate the SIM card PIN before inserting it);



- Connect the control unit to the power supply and start it up;
- Connect the back-up batteries (code AF911).  
**Note:** for AF927PLUS (version without LCD touch screen), make certain that a charged AF911 battery is available at the installation site.
- Prepare a tablet or a PC to be connected to the control unit. This is not necessary for the model with screen (code AF927PLUSTC).

### PRELIMINARY OPERATIONS FOR CONNECTION TO AVECLOUD (RECOMMENDED).

- Download the AVE Cloud app from the APP Store or Google Play.
- Access the AVE Cloud site: <https://avecloud.ave.it/>
- Create a new user and request credentials for a new system to be supervised.
- Make note of the credentials for the selected system (the system sends an email confirming the new system request and indicating the credentials selected during activation).

**Note:** to connect the system to the “AVE Cloud” remoting system, the control unit must be connected to the home Wi-Fi network and it must have an Internet connection. Without an Internet connection, the control unit cannot be remoted.

## DEFAULT DATA AND QUICK PROGRAMMING FOR AF927PLUS (model without screen)

**Note: for version AF927PLUSTC with screen, skip to page 26.**

The control unit has a Wi-Fi module that can be accessed from any device with a WEB browser. The main data required to connect to the control unit are given below:

- a) At initial start-up, the control unit is in ACCESS POINT mode: it generates a Wi-Fi network whose SSID is encoded with the name AF927\_XXXXX, for example: AF927\_C6HAB;
- b) **IP address: 192.168.100.1;**
- c) No password is required to access the AF927\_XXXXX network;
- d) The first screen proposed by the system is the control unit start-up screen.



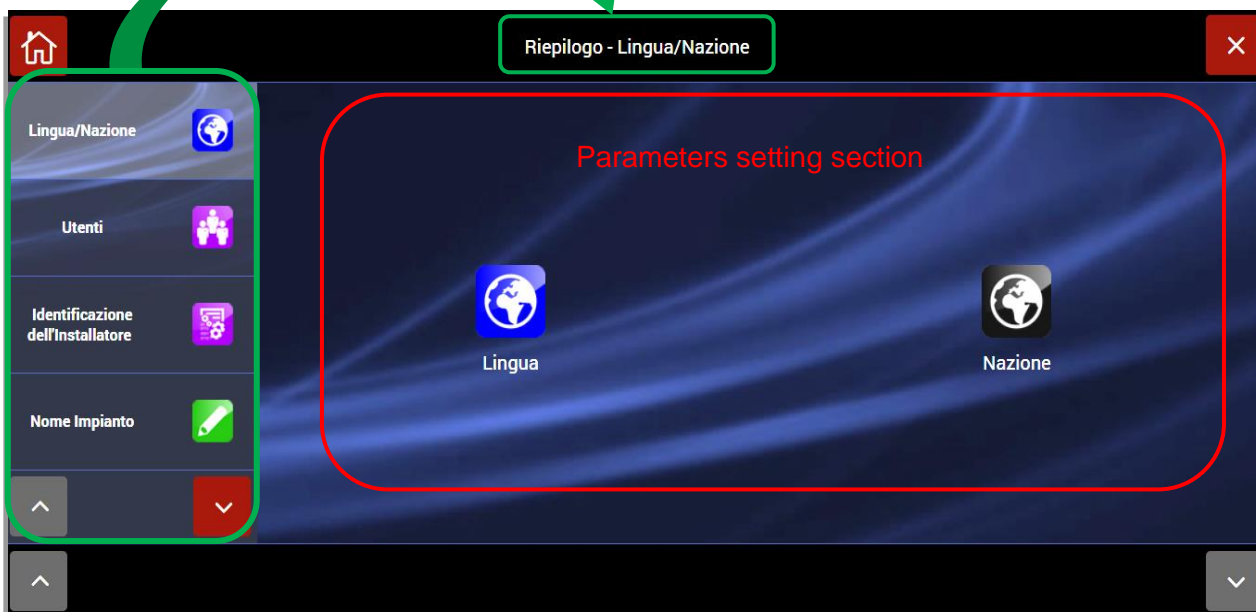
Meaning of the various terms used on the system access page:

- **UPD:** version of the software package including the control unit
- **SOM:** version of the control unit SOM (System ON Module) firmware
- **WEB:** version of the firmware for the WEB graphical interface
- **CARRIER:** software version for the low-level firmware module
- **IMEI:** IMEI (International Mobile Equipment Identity) number of the previously connected AFGSM04 module (if any). If the module is not present, the message "NO GSM" will appear.

- e) Press the “START” screen to call up the programming WIZARD: the column on the left is used to scroll through the various system programming menus. Pressing any one of them (e.g.: language/country) causes the box to turn grey and the page used to set the parameters of each function appears in the box on the right.

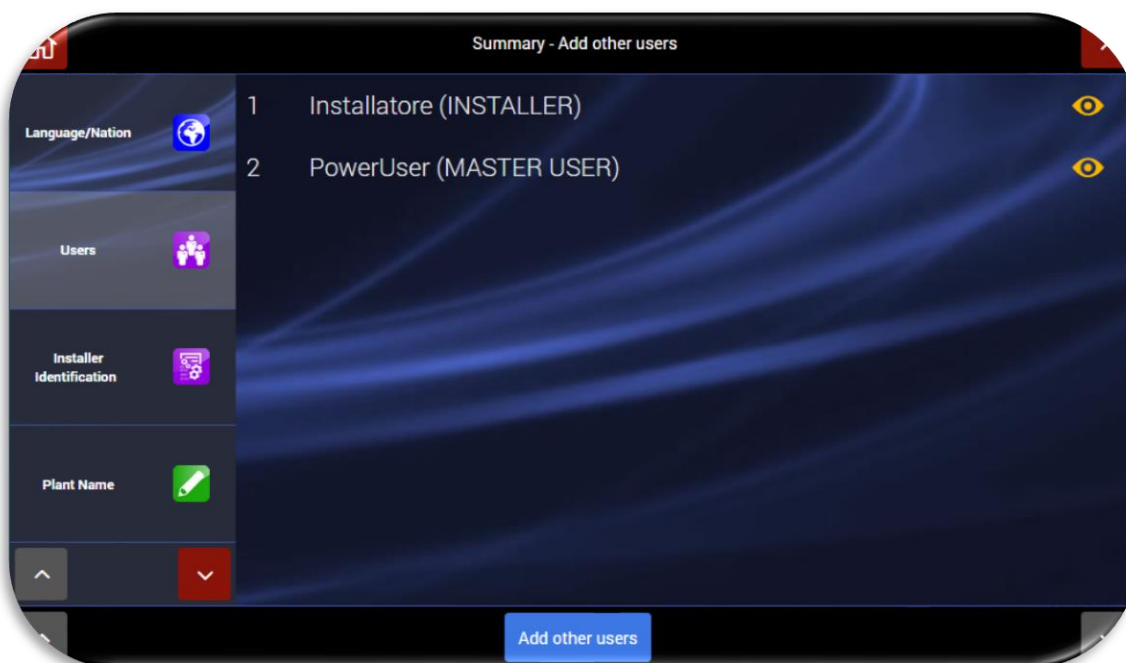
Scroll section to choose the various settings


Indication of the setting selected

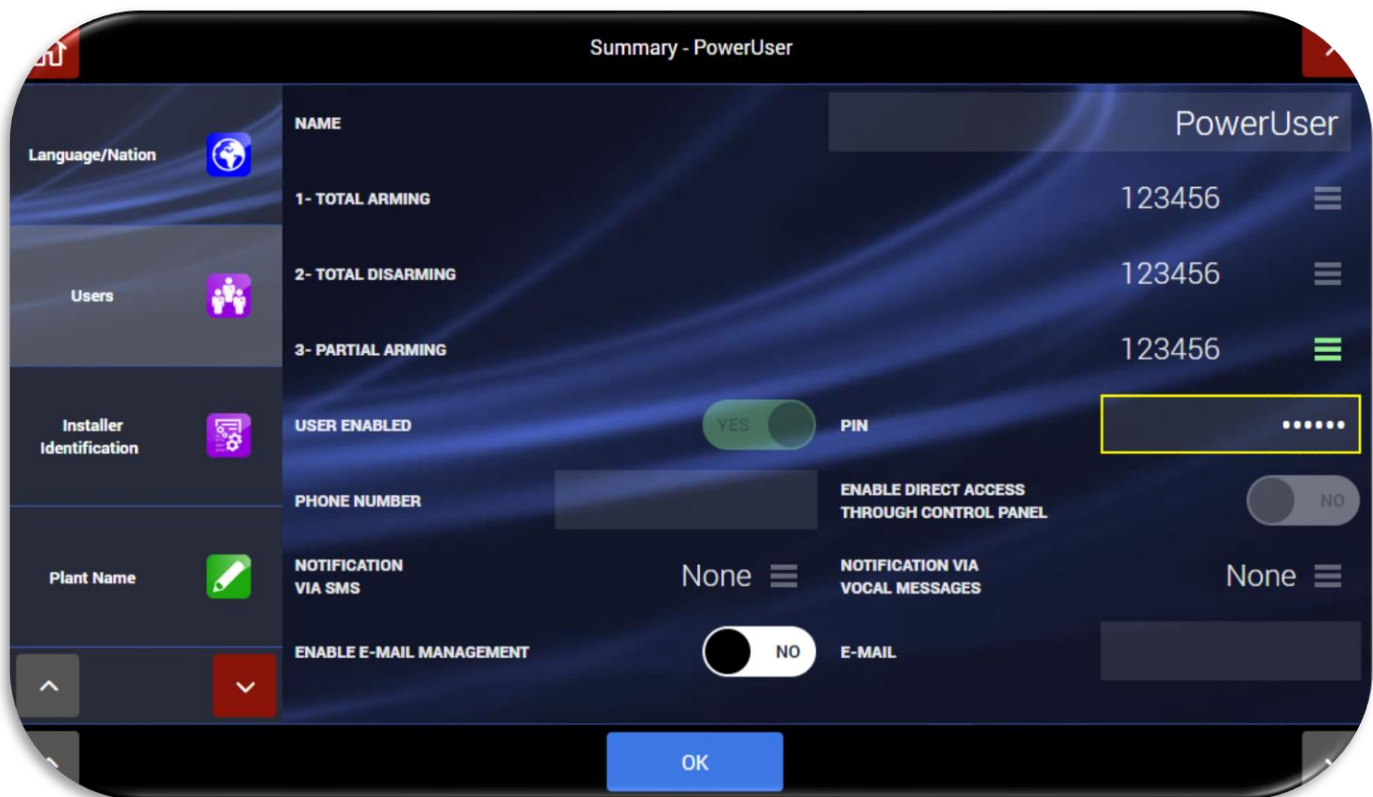


The operations that must be performed to program the main settings and system peripherals (for advanced settings and/or specific details related to the various functions, check the specific system sections) are indicated below:

1. Set language and country
2. Set at least one **user code**; entering the code for the **POWER USER (MASTER USER)** is mandatory and is performed as follows:
  - a. Click on the **Users** menu:



- b. Click on the  symbol for the POWER USER (MASTER USER) and set the PIN (5- or 6-digit) and the other user parameters:



The meanings of the various parameters are given below:

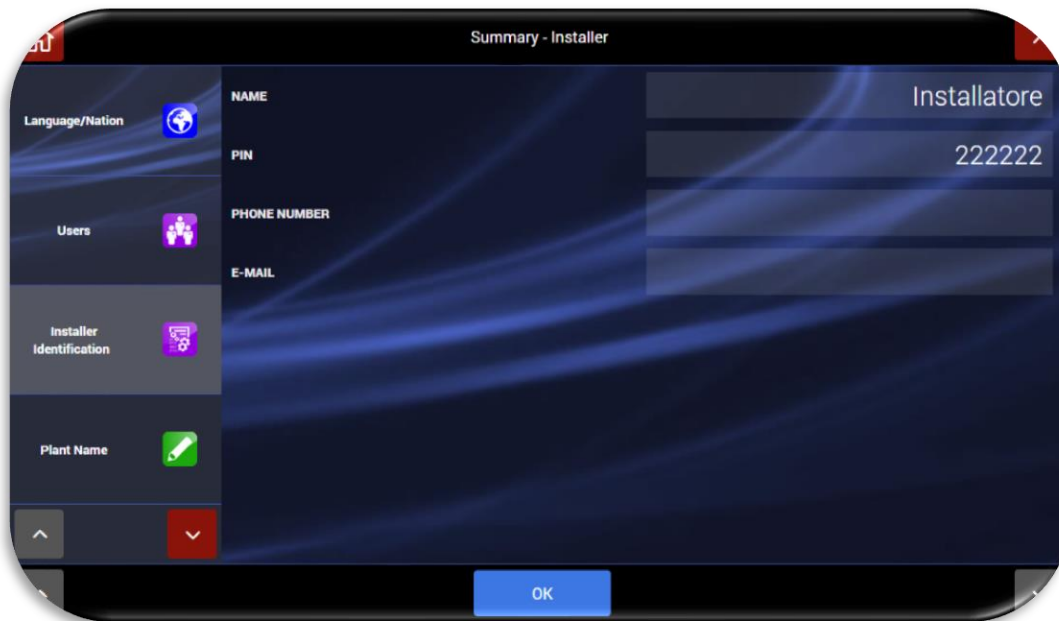
- **Total activation** (cannot be edited by the Power User): enables activation of all system areas;
- **Total deactivation** (cannot be edited by the Power User): enables deactivation of all system areas;
- **Partial activation**: calls up a quick partial activation (future setting – not currently implemented);
- **User enabled** (cannot be edited by the Power User): makes it possible to disable the user and relative system privileges;
- **PIN**: enter a 5- or 6-digit user code.  
     Note: the user code cannot be the same as the installer code and the code “000000” cannot be used;
- **Phone**: user's telephone number;
- **Enable direct access to control unit**: to enable the user to manage the control unit remotely via SMS sent from his/her cell telephone;
- **SMS notifications**: select the SMS messages to be sent to the user in response to intrusion detection system events.  
     Note: the send notifications via GSM function is active and can only be set if on the control unit has a GSM module installed (code AGSM04);
- **Voice message notifications**: select the voice messages to be sent to the user in response to intrusion detection system events.  
     Note: the send notifications via GSM function is active and can only be set if on the control unit has a GSM module installed (code AGSM04);
- **Enable e-mail**: enables sending the user an e-mail in response to intrusion detection system events;
- **E-mail**: user's e-mail address;

c. Confirm by pressing OK.

## 1. Set Installer Code


The **installer identification** code must be entered as follows:

- a) Enter:
  - **Name:** name of the installer;
  - **CURRENT PIN:** 5 or 6-digit installer code;
  - **Note:** the installer PIN cannot be the same as the user PIN and cannot be "000000";
  - **Phone:** installer's telephone phone number;
  - **E-mail:** installer's e-mail address;

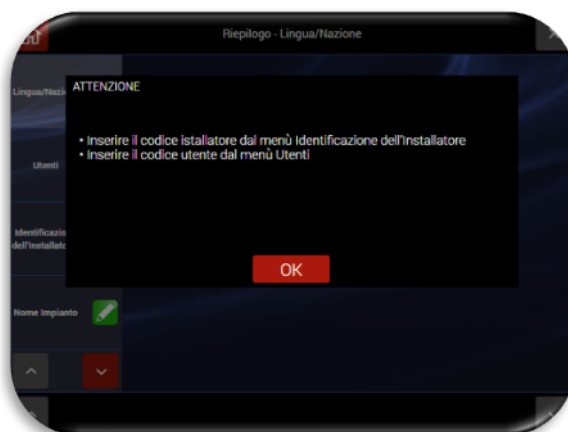


- b) Confirm by pressing OK.

### **NOTES** regarding USER code and INSTALLER code:

It is only possible to exiting the programming wizard (by pressing the home key ) after both the user code and installer code have been set.

If one of the two codes has not been set, it is not possible to exit the programming Wizard and the following Pop-Up warning appears:

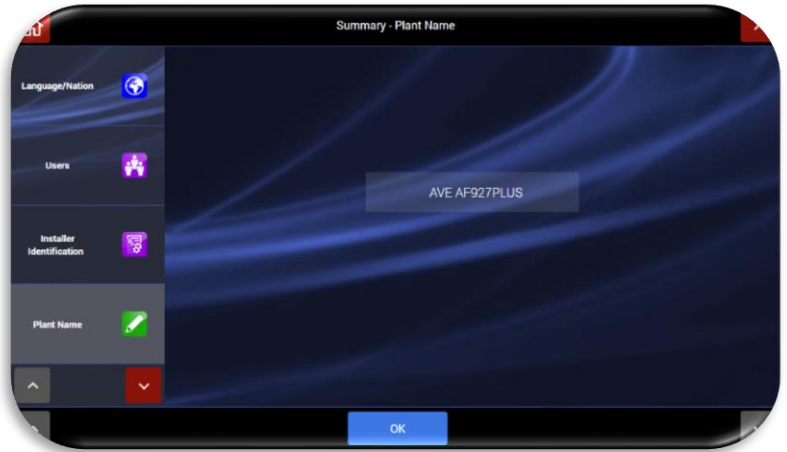


**Note:** if the user and installer codes are lost, after rebooting the control unit (disconnect the mains power supply and battery, wait 1 minute and then reconnect everything), it is possible to enter both menus (user and installer) using the temporary code 00000 (five zeros; this code is valid for about 3 minutes from moment the control unit is powered up).

**WARNING:** the first operation to be performed is to call up the control unit activation/deactivation menu and run complete control unit deactivation (ex. deactivation of all the areas) using code 00000 to accept any anomalies present on the control unit. If this is not done, it will not be possible to enter any of the other menus.

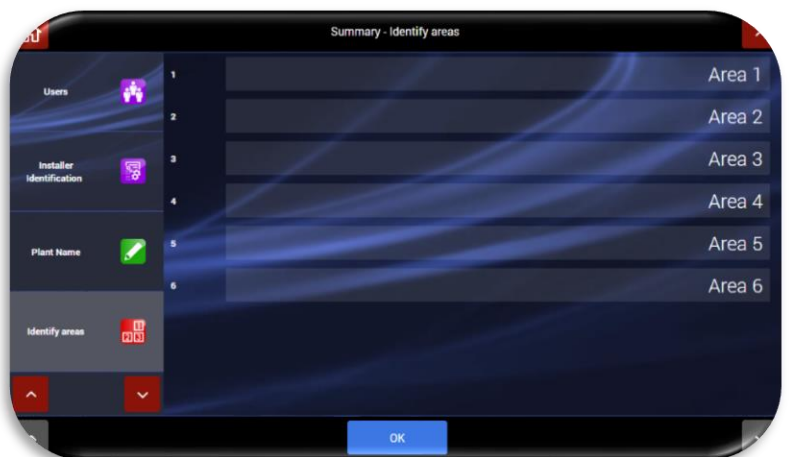
## 2. Set System Name

- a. This operation is required to identify the system and to distinguish it from other systems if the same supervision account (via AVE CLOUD and related APP) is used for several systems.
- b. Confirm by pressing OK.



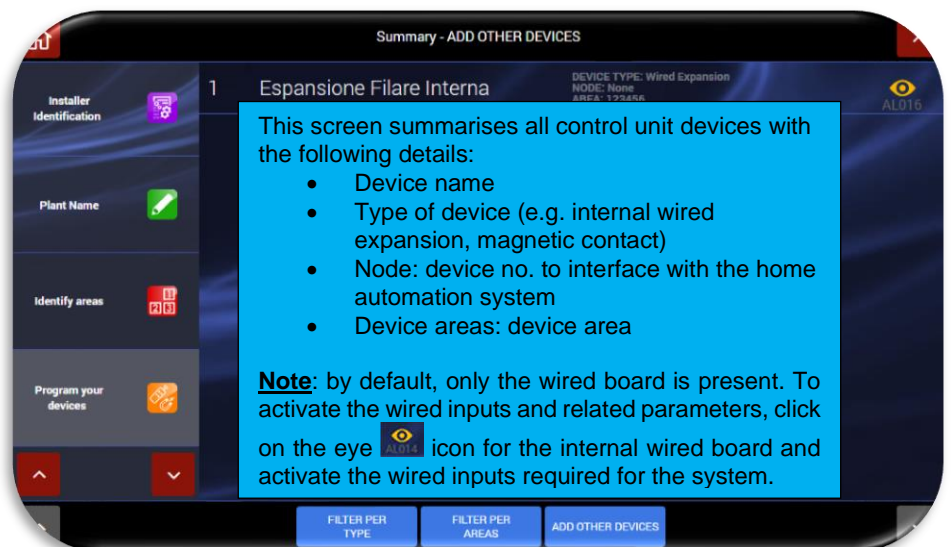
## 3. Set Name of the various areas used to group together the detectors installed on the system:

- a. Enter the field for the area to be edited and enter in its name. Repeat this for all necessary areas.
- b. Confirm by pressing OK.



## 4. Program the devices that will be installed on the system:

- a. Select the “Program your devices” function. This calls up the screen shown to the side:



The buttons at the bottom of the screen have the following meanings:

- “Filter by type of device”: displays only devices of the given type;
- “Filter by areas”: displays only the devices present for the given area;
- “Add other devices”: makes it possible to add more radio devices.

b. To add further devices, press “Add other devices”. This calls up the following screen.

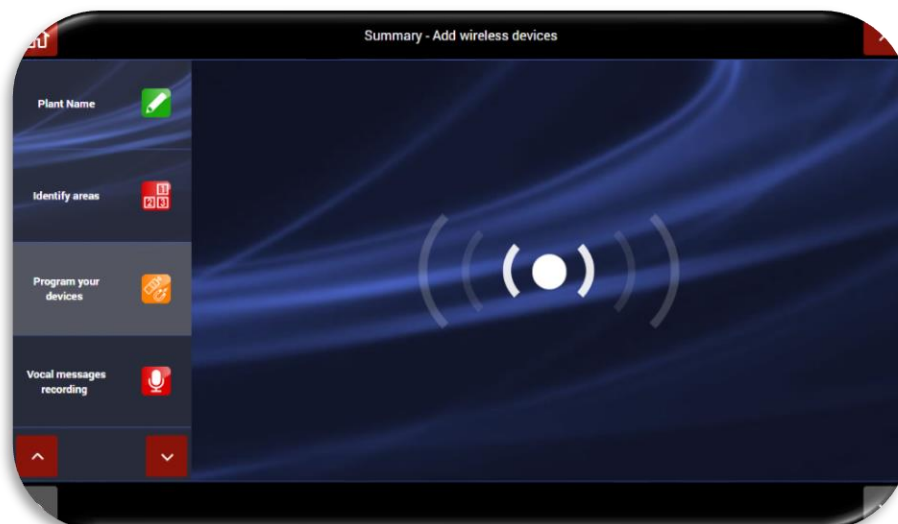
Click:

- “Add devices via radio” to acquire devices via radio (detectors, remote controls, sirens, etc.).
- “Add BUS devices” to acquire the input/output boards connected downstream of the AF927INTFIL board (wired BUS generation card) using either the manual procedure (using the cable supplied with the wired BUS interface board) or automatic procedure.



- “Camera IP” to acquire the IP for the cameras that can be polled via HTTP using JPEG polling (HTTP snapshot) - For compatibility and other info, log onto <https://www.ispyconnect.com/sources.aspx> and/or see the list of products tested by the AVE INTEAM service.

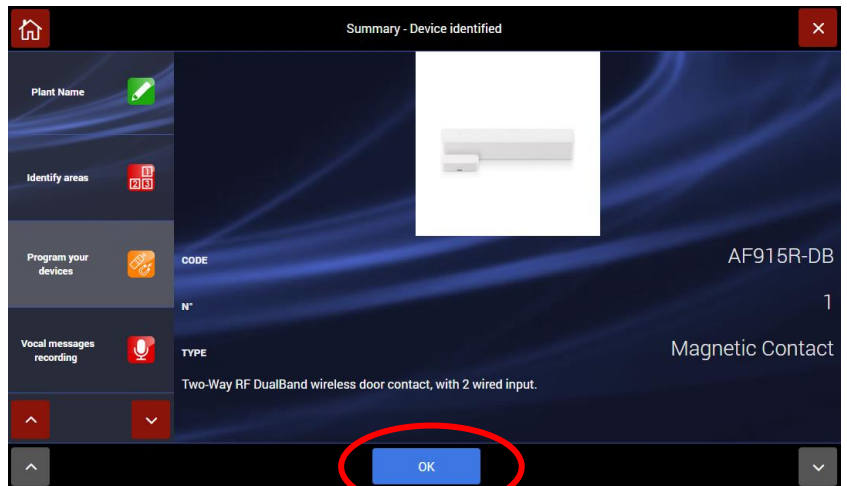
c. If you wish to acquire a new intrusion detection device (detectors, remote controls, sirens), click on “**Add devices via radio**”, the control unit enters listening mode while awaiting the association request message from a peripheral radio device.



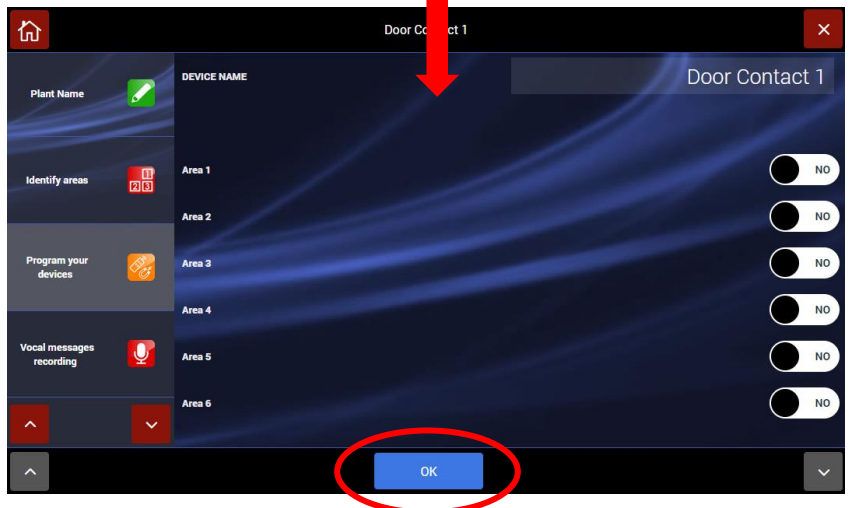
To acquire peripheral devices, proceed as follows:

Code	Description	Acquisition mode	Actions to be completed for acquisition
AF943R	Remote control	Press RED+GREEN	Enter name and configure keys
AF915R-DB AD915R-MDB AF963R-DB AF964R-DB AF965R-DB AF976R-DB	Detectors	Insert battery	Enter name, match areas
AF53903R-DB	Siren	Insert battery	Enter name, match areas
AFTR02	Interface for technical alarms	Insert battery	Enter name
AFINTFIL	Interface for wired bus	Plug into control unit	Match areas
AFTR03	Signal repeater	Plug into a mains power outlet (230Vac)	Enter name, match areas
AF340-T	Tag	Bring the tag at the bottom left-hand side of the control unit close to the microphone	Enter name, match areas (by default, all are matched)
AF970R-DB	Radio Keypad	Insert battery	Enter name, match areas
AF990	Wire Keypad	Connect the keyboard to the wired bus and start the affiliation procedure	Enter name, match areas

**NOTE:** after the correct device save procedure has been run, the control unit emits a confirmation sound (BEEP) and displays the image of the device saved (see example of magnetic contact AF915R-DB). **The device acquisition procedure involves finalising the operation by pressing “OK” within no more than 10 seconds. Waiting longer makes it necessary to repeat acquisition.**

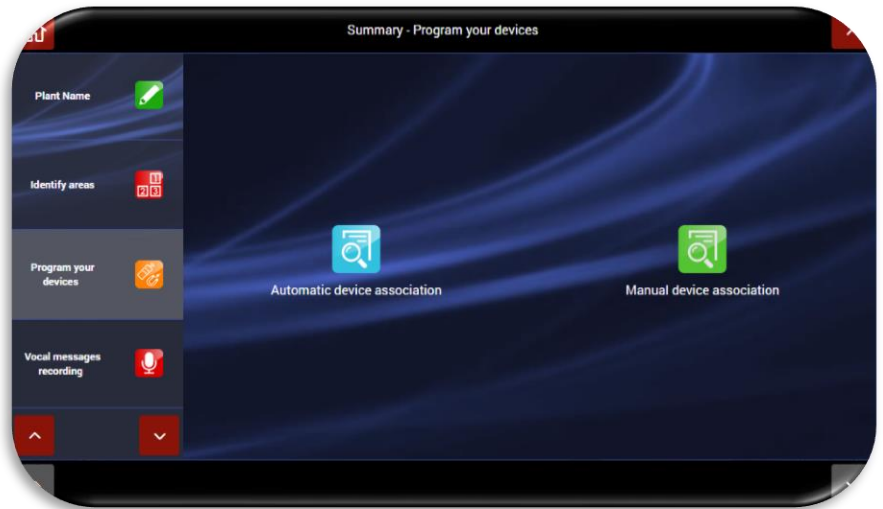


- Enter name of the device, match desired areas and confirm.
- Repeat the procedure for all devices





- d. To acquire a new intrusion detection device connected to the wired bus generated by the AF927INTFIL interface board, click on “**Add wired BUS devices**”; this calls up the following screen:

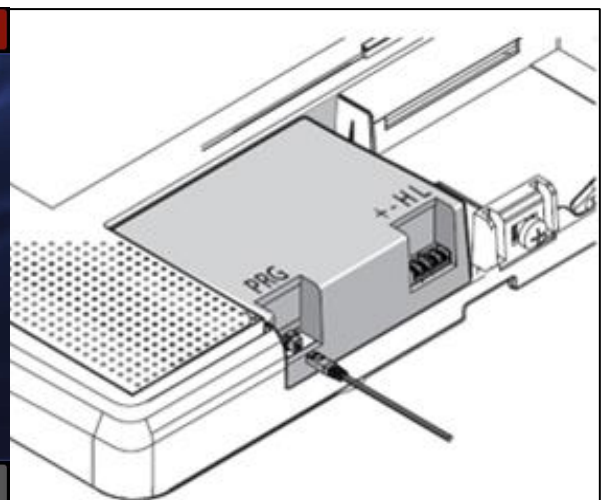
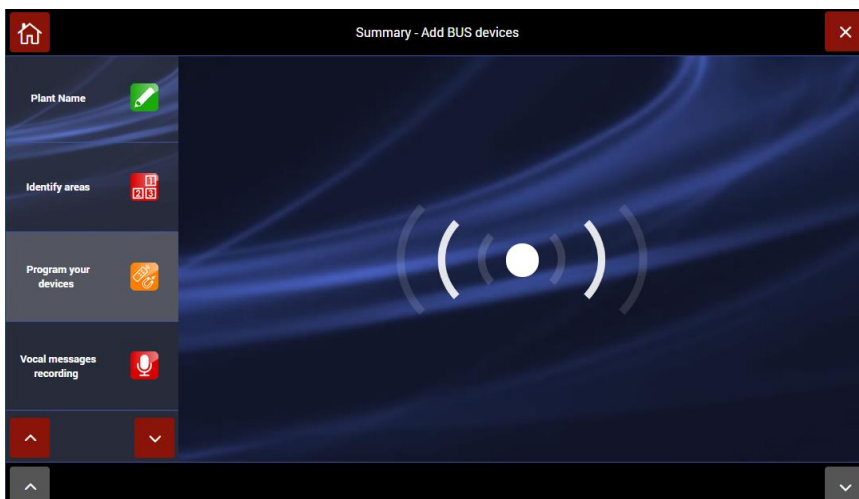


To enable the control unit to associate the input/output boards connected to the wired bus, just select the manual or automatic device association procedure.

- Press “Automatic device association” and the control unit will start scanning the wired Bus to acquire the connected boards. Repeat the scanning procedure until all connected boards are recognised.



- If “Manual device association” is selected, the programming cable supplied with the wired interface board must be connected to the appropriate connector for the AF927INTFIL board. The control unit enters “listening” mode while waiting connection of a board: After hooking up the connection cable, connect one board at a time until the all modules have been connected.



## 5. Voice messages:

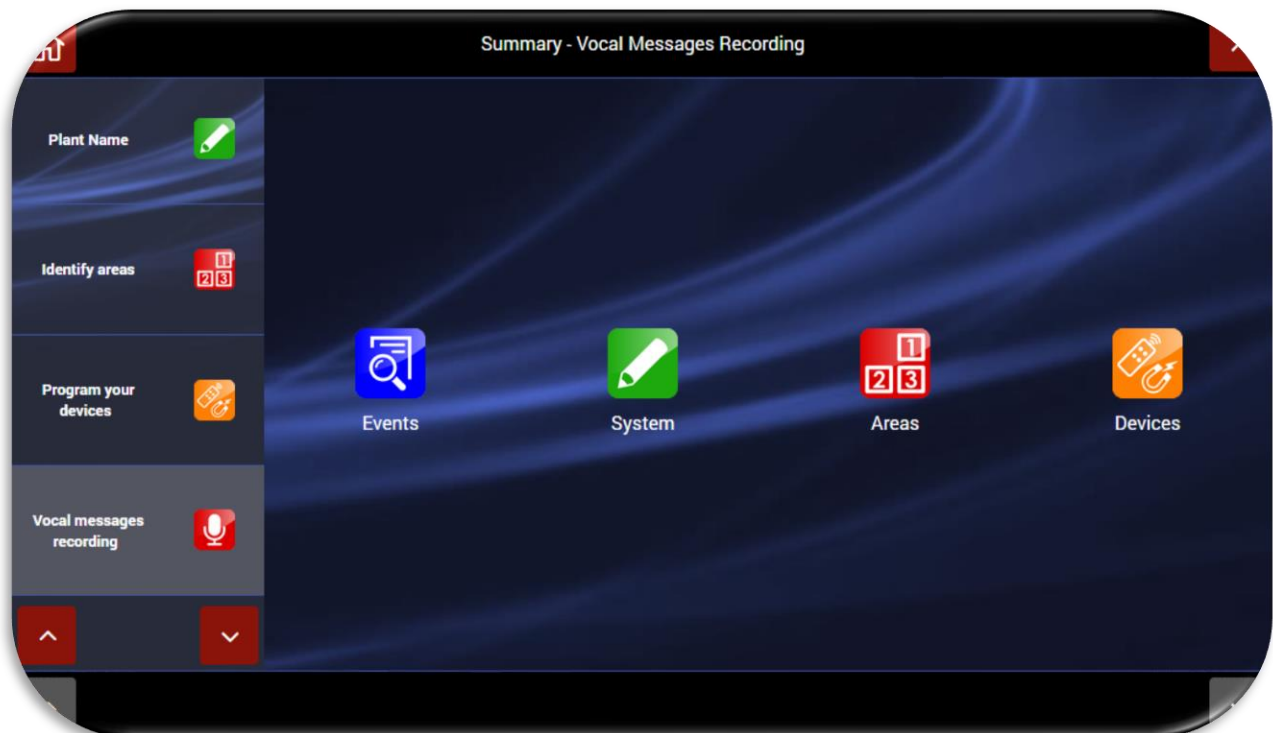
The control unit has voice messages for differentiated, type-specific alerts: *EVENTS*, *AREAS*, *SYSTEM*, *DEVICES*.

The control unit software contains pre-recorded messages for the main system events:

- *EVENTS*:
  - Alarm = "Intrusion Alarm"
  - Tamper = "Tampering in progress"
  - Battery dead = "Battery dead"
  - Aggression rescue = "Robbery in progress"
- *AREAS*:
  - AREA 1 = "Perimeter detectors area"
  - AREA 2 = "Volumetric detectors area"

Messages are automatically available in the language selected for the control unit.

Selecting "**Record voice messages**" lets select the category of messages to be edited.



If, for example, you wish to change the alarm message:

- a. Click on the “Events” icon to call up the following screen:



- b. Edit the necessary voice messages:

- The speaker icon has two states:



voice message recorded

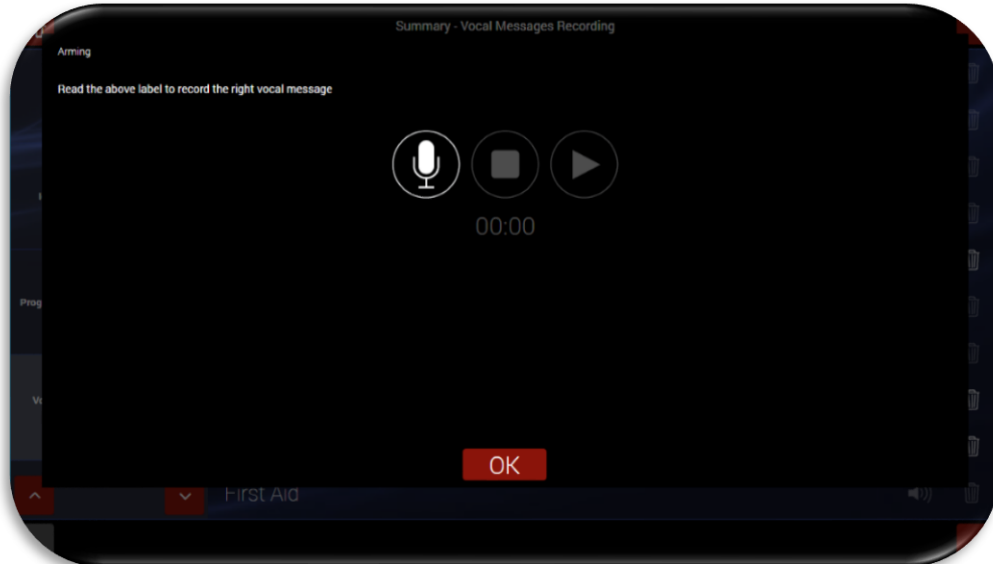


voice message not recorded

- Click on the “trash” icon to delete the voice message



- Clicking on the message name icon makes it possible to record/edit the voice message. This calls up the following screen.



The meanings of the icons present in the Pop-Up are given below:



= start recording key



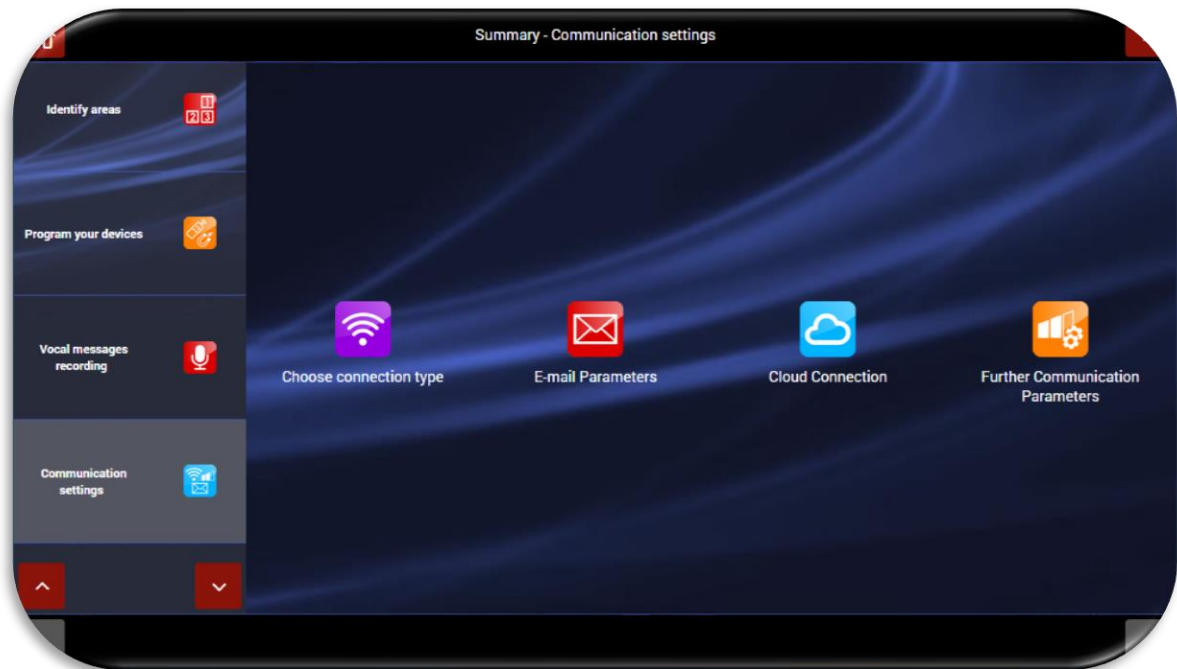
= start playback key



= stop playback or recording key

- When finished, confirm by pressing OK.

## 6. Communication parameters



This function is used to define the control unit connection parameters.  
The 4 icons make it possible to:



Choose whether to use the control unit in ACCESS POINT mode or make the control unit a CLIENT of a master router that enables Internet connection.



Specify the e-mail parameters for the account that will be used as control unit sender



Set the parameters for connection to AVE CLOUD

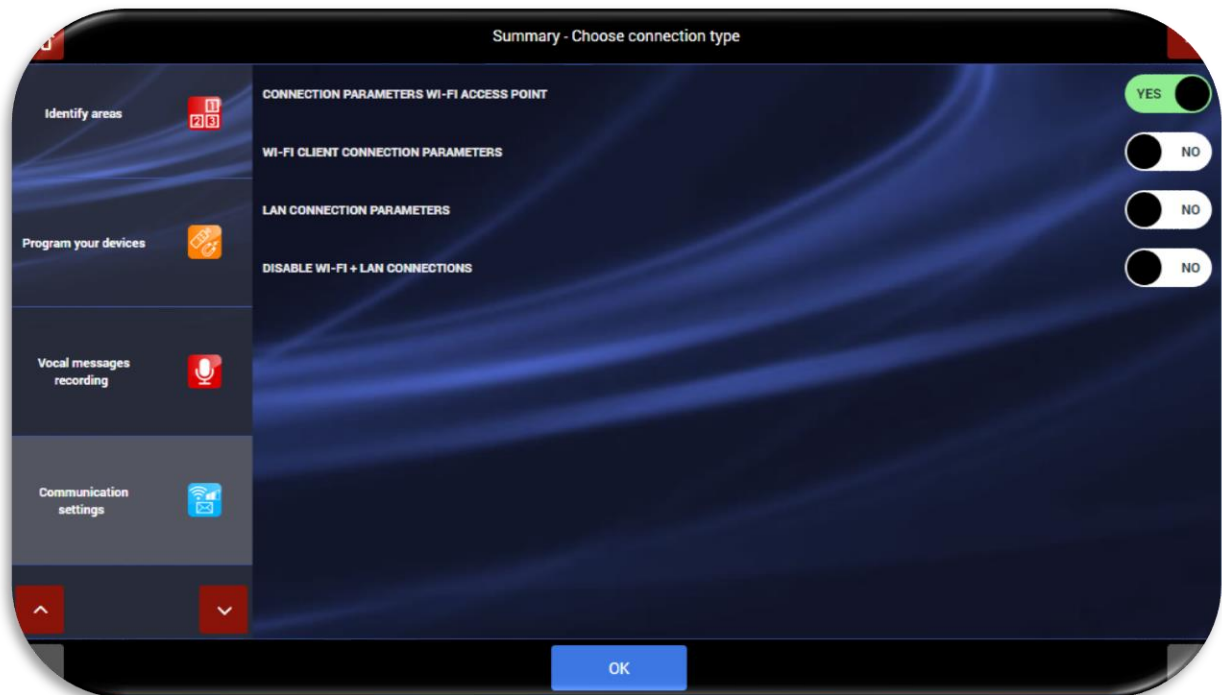


Set the advanced communication functions, including digital surveillance protocols (ADM, SIA, etc.)

## a. Wi-Fi parameters

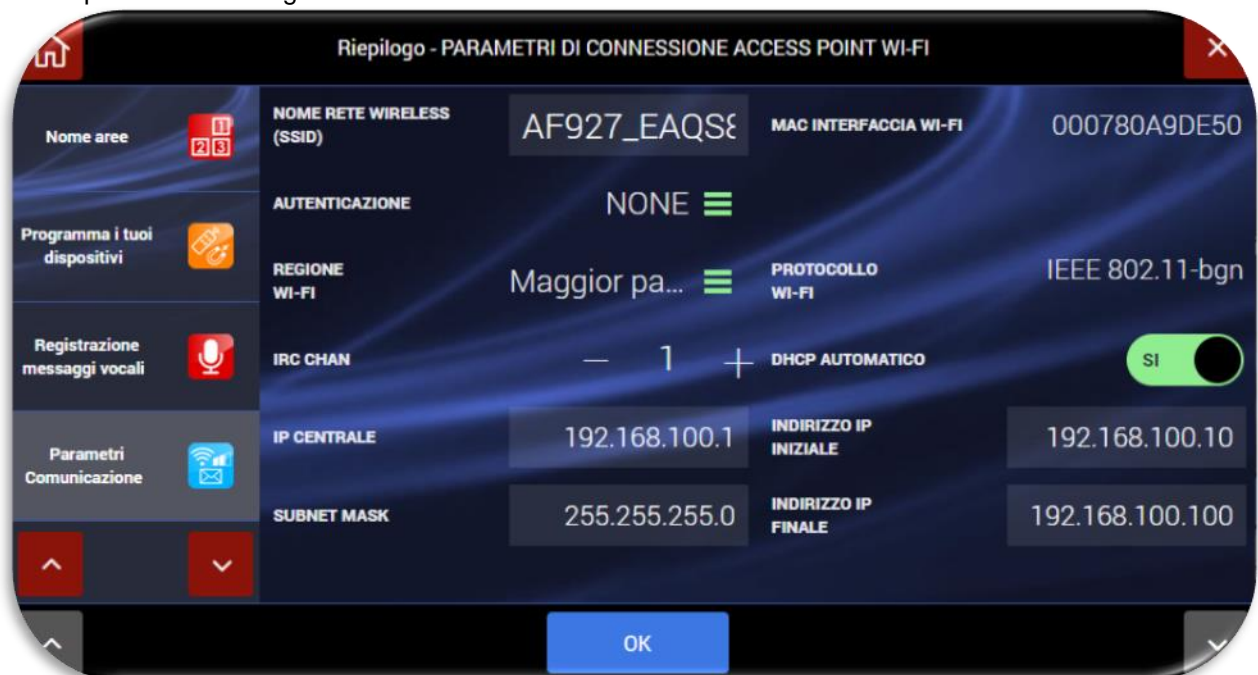
It is possible to define different control unit operating modes:

- Wi-Fi ACCESS POINT CONNECTION PARAMETERS
- Wi-Fi CLIENT CONNECTION PARAMETERS
- LAN CONNECTION PARAMETERS
- WI-FI DISABLED (the Wi-Fi module can only be switched off for control units with LCD screen art. AF927PLUSTC)

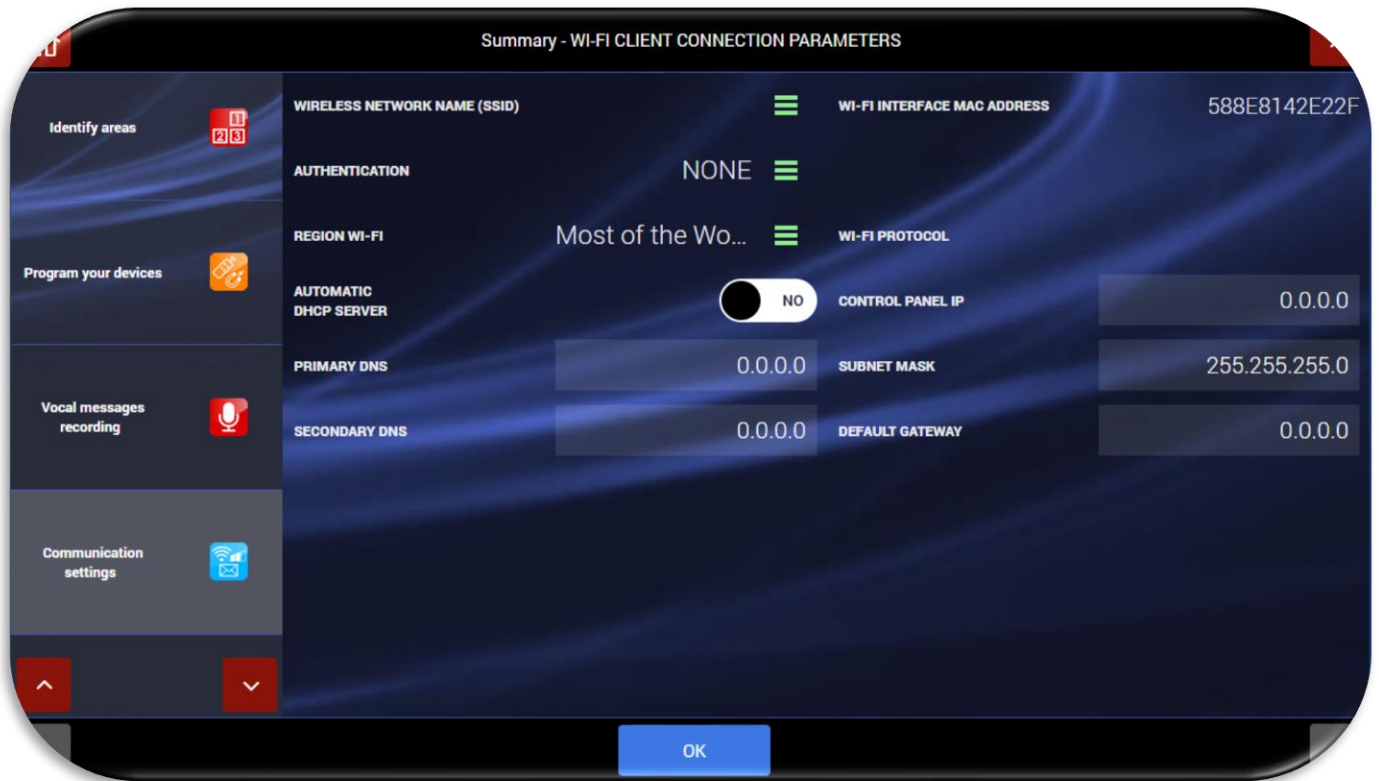


Activating the selected mode calls up a screen used to set the network parameters. Three examples are given below. When finished, confirm by pressing OK.

Example of Wi-Fi configuration in **ACCESS POINT** mode



Example of Wi-Fi configuration in **CLIENT** mode

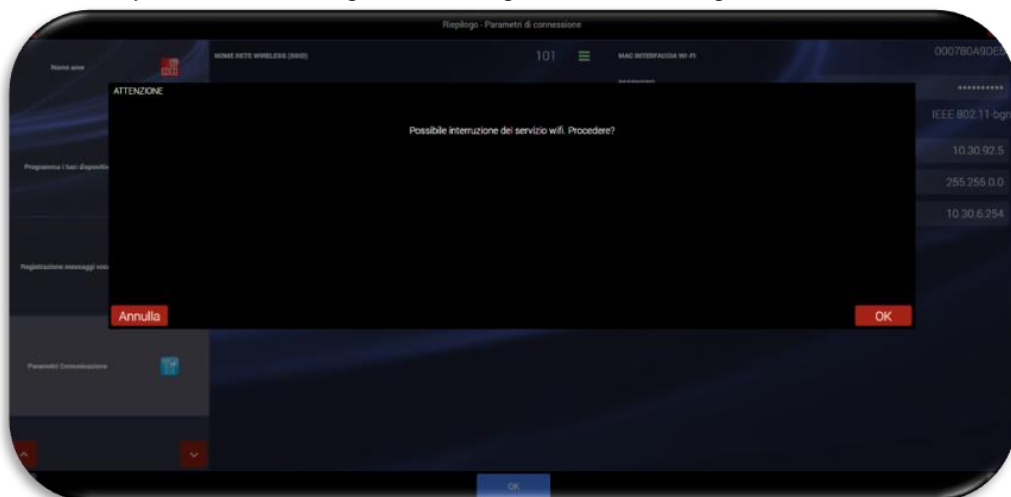


The meaning of the main network parameters to be set are given below:

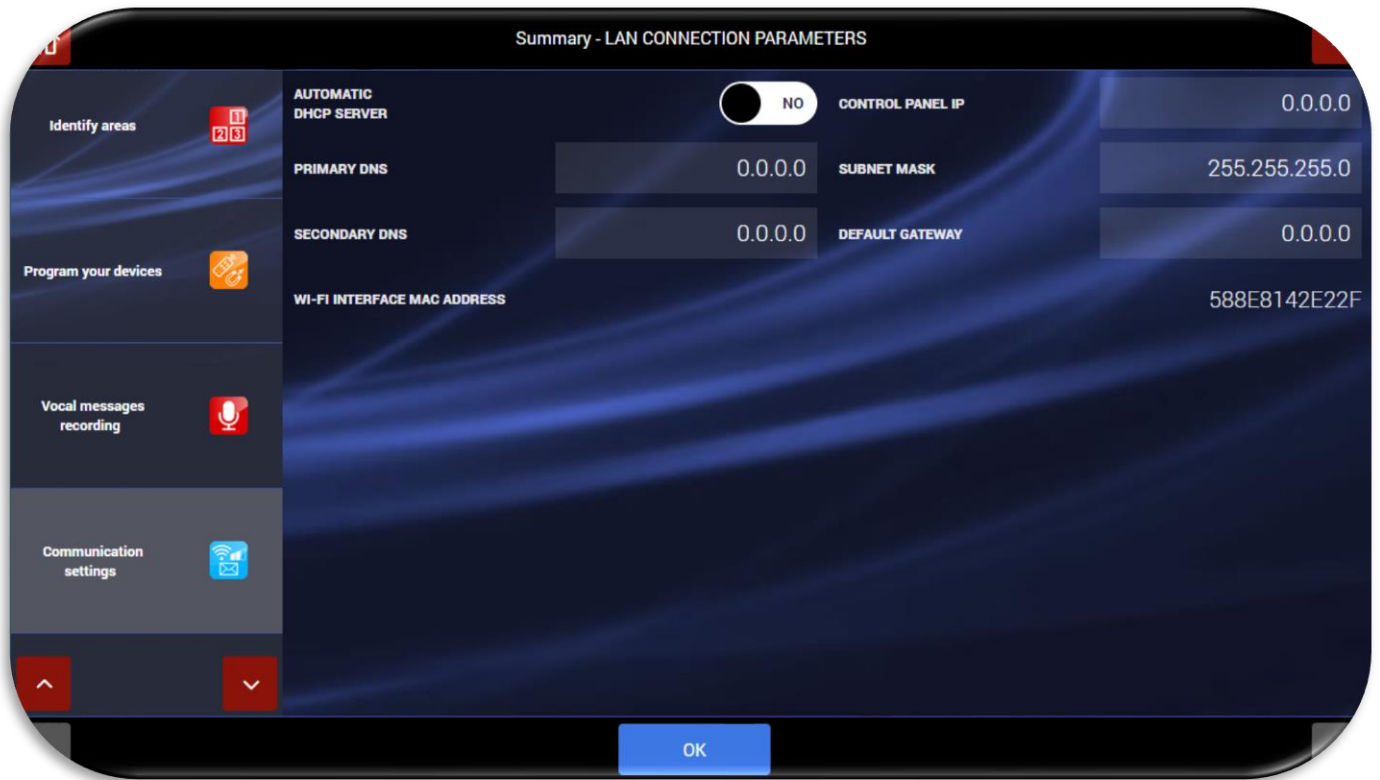
- **CONTROL UNIT IP:** IP address assigned to the control unit;
- **SUBNETMASK:** defines the size (understood as address range) of the IP subnetwork. Typically, in a home network, the parameter is set to 255.255.255.0;
- **DEFAULT GATEWAY=** network gateway address. Typically, in a home network, the address is the address of the network modem/router (ex. 192.168.0.1);
- **PRIMARY DNS** and **SECONDARY DNS** are the DNS used within the network. Typically, in a home network and/or a network which does not have its own DNS, the following values can be used:
  - PRIMARY DNS = 8.8.8.8
  - SECONDARY DNS= 8.8.4.4

**Notes on Wi-Fi connection:**

- When switching from access point Wi-Fi or when changing the configuration parameters of the Wi-Fi connection, the control unit reboots the Wi-Fi module. Before confirming by pressing OK in the following POP-UP, it is essential that parameters be set correctly.
- In the transition from Wi-Fi to access point or in case of changes to the configuration parameters of the Wi-Fi connection, the control unit restarts the Wi-Fi module. It is necessary to be sure that you have set the parameters correctly before confirming the following POP-UP message with OK.



## Exemplar of a **Wired LAN** configuration



The control unit can be connected to the wired LAN using the interface AF927INTFIL (optional). To connect the interface, the cover of the control unit needs to be opened; the interface must be connected in the mini USB port located on the left side of the control unit.

The meaning of the main network parameters to be set are given below:

- **AUTOMATIC DHCP:** enables the router to automatically associate an address with the control unit. It is advisable to use a DHCP address that is set manually thus ensuring that the IP address assigned to the product is always known.
- **CONTROL UNIT IP:** IP address assigned to the control unit;
- **SUBNETMASK:** defines the size (understood as address range) of the IP subnetwork. Typically, in a home network, the parameter is set to 255.255.255.0;
- **DEFAULT GATEWAY=** network gateway address. Typically, in a home network, the address is the address of the network modem/router (e.g., 192.168.0.1);
- **PRIMARY DNS** and **SECONDARY DNS** are the DNS used within the network. Typically, in a home network and/or a network which does not have its own DNS, the following values can be used:
  - PRIMARY DNS = 8.8.8.8
  - SECONDARY DNS= 8.8.4.4





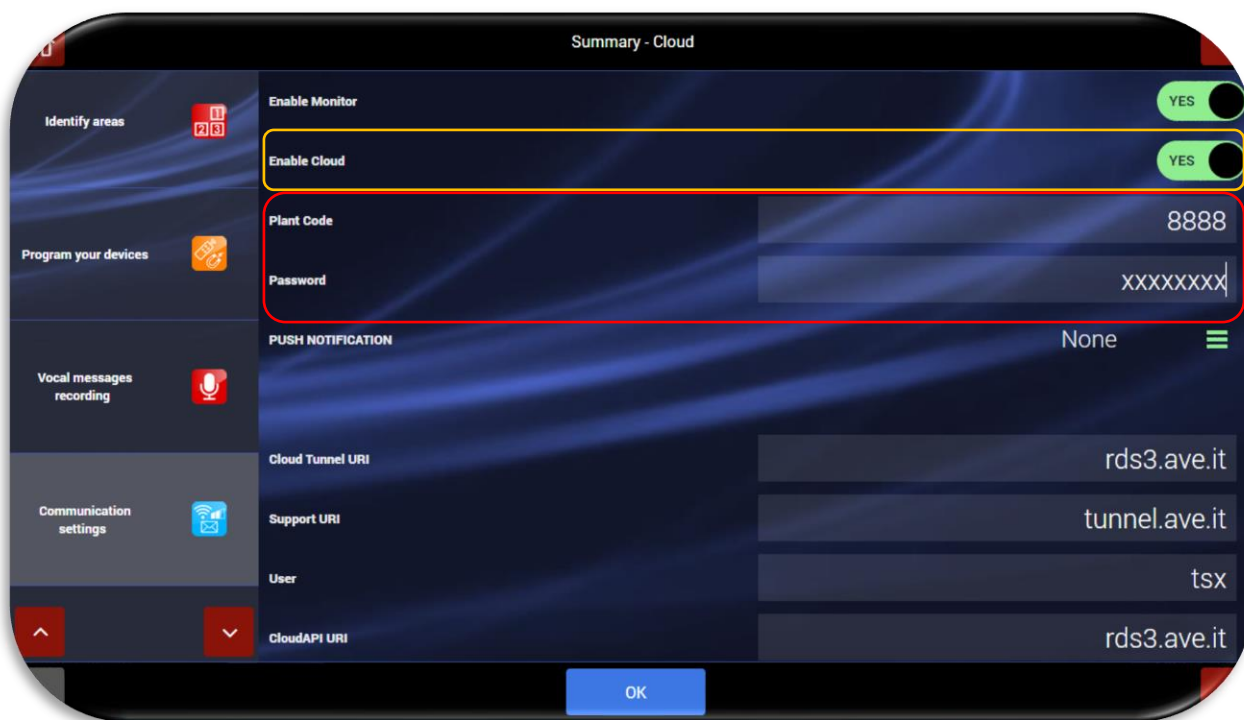
- In the AF927PLUS control unit (without LCD touch screen), if the Wi-Fi parameters or the ACCESS POINT to which it is connected are set incorrectly, the control unit cannot be reached and the ACCESS POINT mode will have to be rebooted as follows:

- Completely switch off the control unit by unplugging it from the mains power supply and removing the batteries.
- Restart the control unit with a single charged battery (code AF911).
- Wait for the control unit to reboot. For the first 3 minutes, the control unit will start up using the default parameters:
  - At initial start-up, the control unit is in ACCESS POINT mode: it generates a Wi-Fi network whose SSID is encoded with the name AF927\_XXXXX, for example: AF927\_C6HAB
  - **IP address: 192.168.100.1**
  - No password is required to access the AF927\_XXXXX network
- Go to the Wi-Fi settings menu and enter the correct parameters. Confirm by pressing OK.
- Continue by reconnecting to the control unit using the settings entered
- Proceed with programming


- b. **Cloud:** to connect the control unit to the “AVE CLOUD” remoting system, in the control unit parameters, enter the codes received by e-mail when the system was registered on the <https://avecloud.ave.it/> website. These parameters are:

- System code
- Password

After setting the parameters and having enabled the “Enable Cloud” option, confirm by pressing OK.



- 7. Exit and Home page:

pressing the home page  button calls up the main system screen: the system is ready to be used.



## RAPID PROGRAMMING FOR AF927PLUSTC (model with screen)

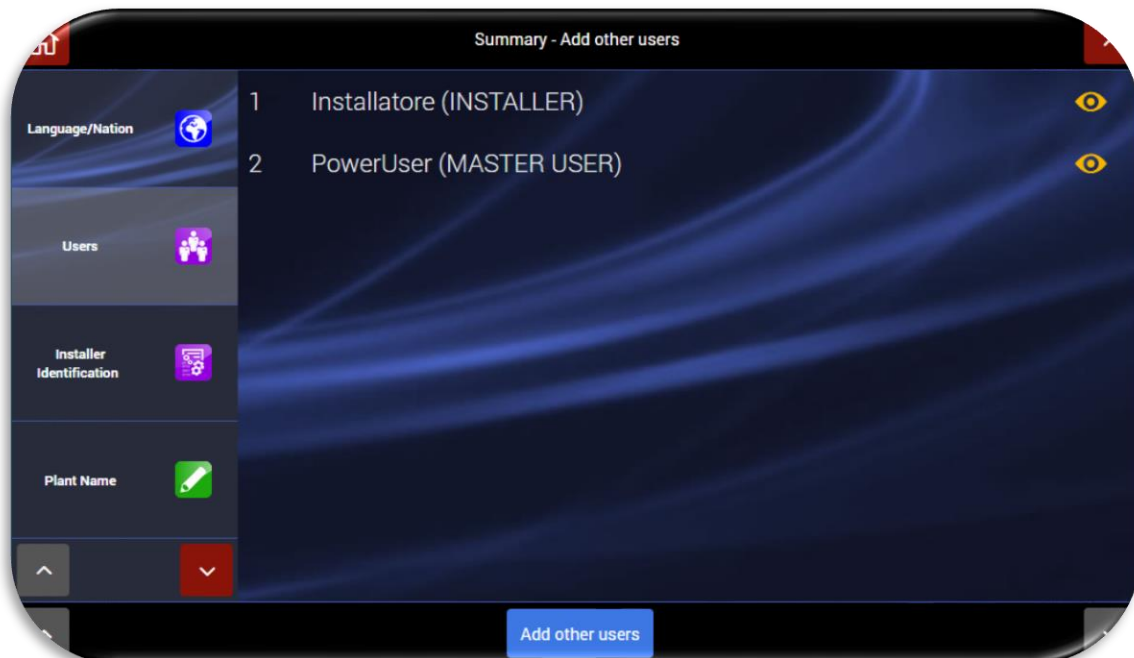
When the control unit is switched on for the first time, the following screen appears:




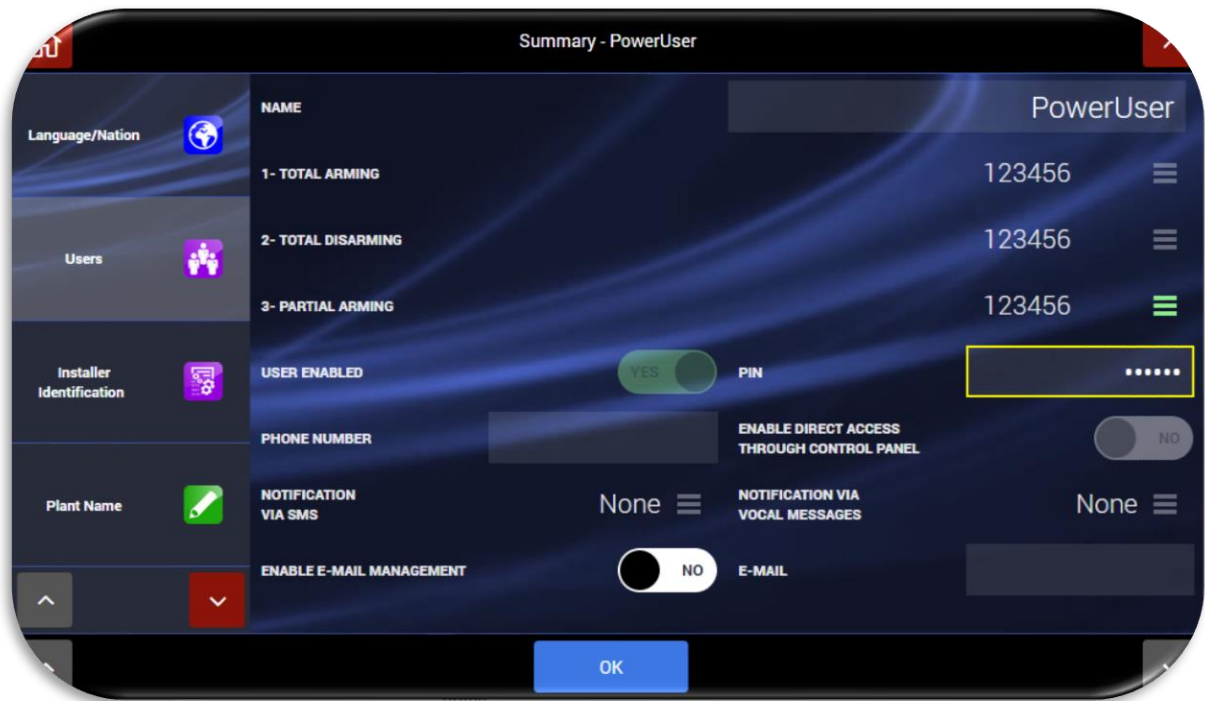
Quick programming from a PC and/or other device equipped with a browser cannot be performed at initial start-up, and without entering the user and installer codes. The operations described in this document and illustrated from page 10 to page 25 can be performed directly on the screen of the control unit AF927PLUSTC.


To run the programming shown, the following operations must be performed directly on the control unit screen:

1. Press "START"
2. To use a language other than Italian, set the language and country. If not, go to point 2.
3. Set at least one **POWER USER (MASTER USER) user code** as follows:
  - a. Click on the "Users" menu:

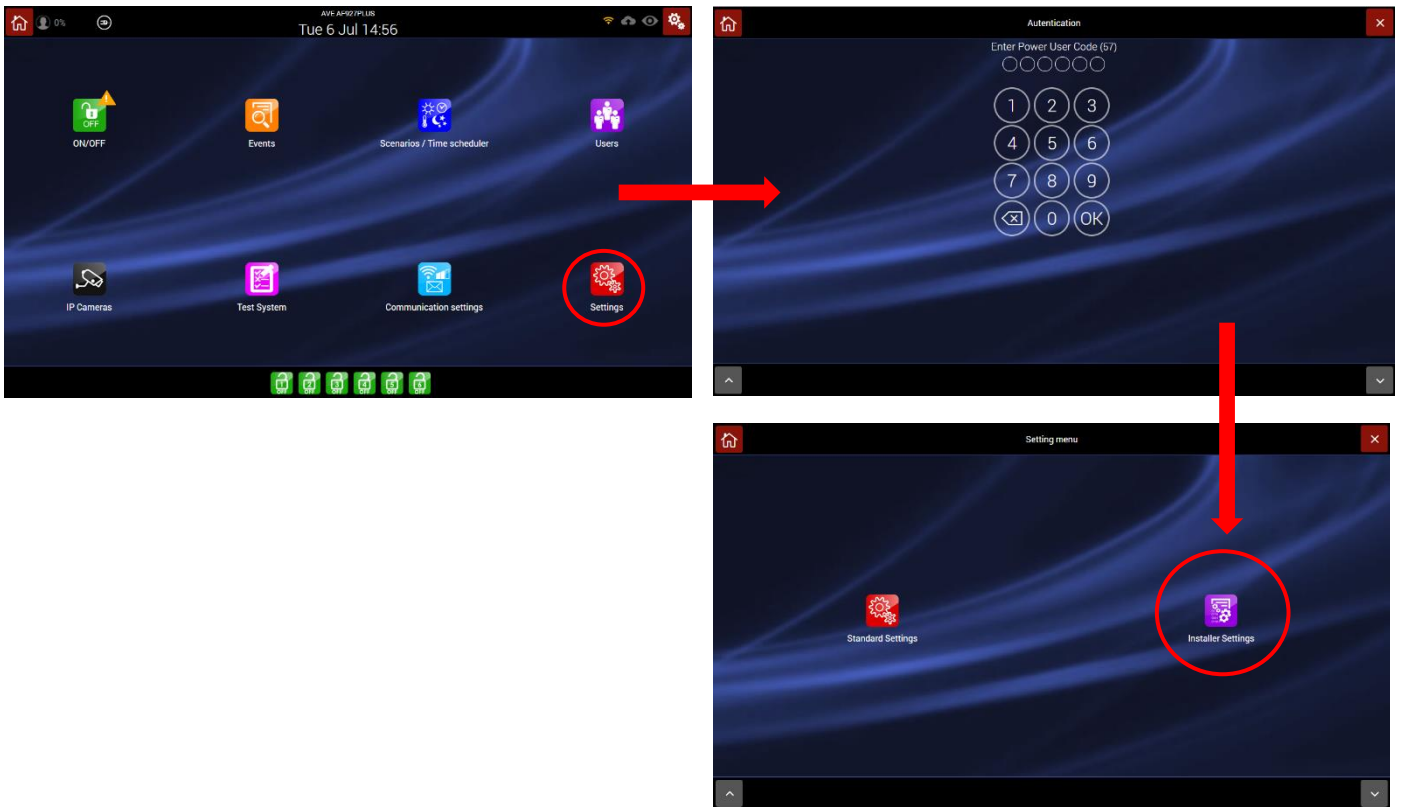


- b. Click on the  POWER USER (MASTER USER) symbol. This calls up a screen used to set the PIN (6 digits) and other user parameters:

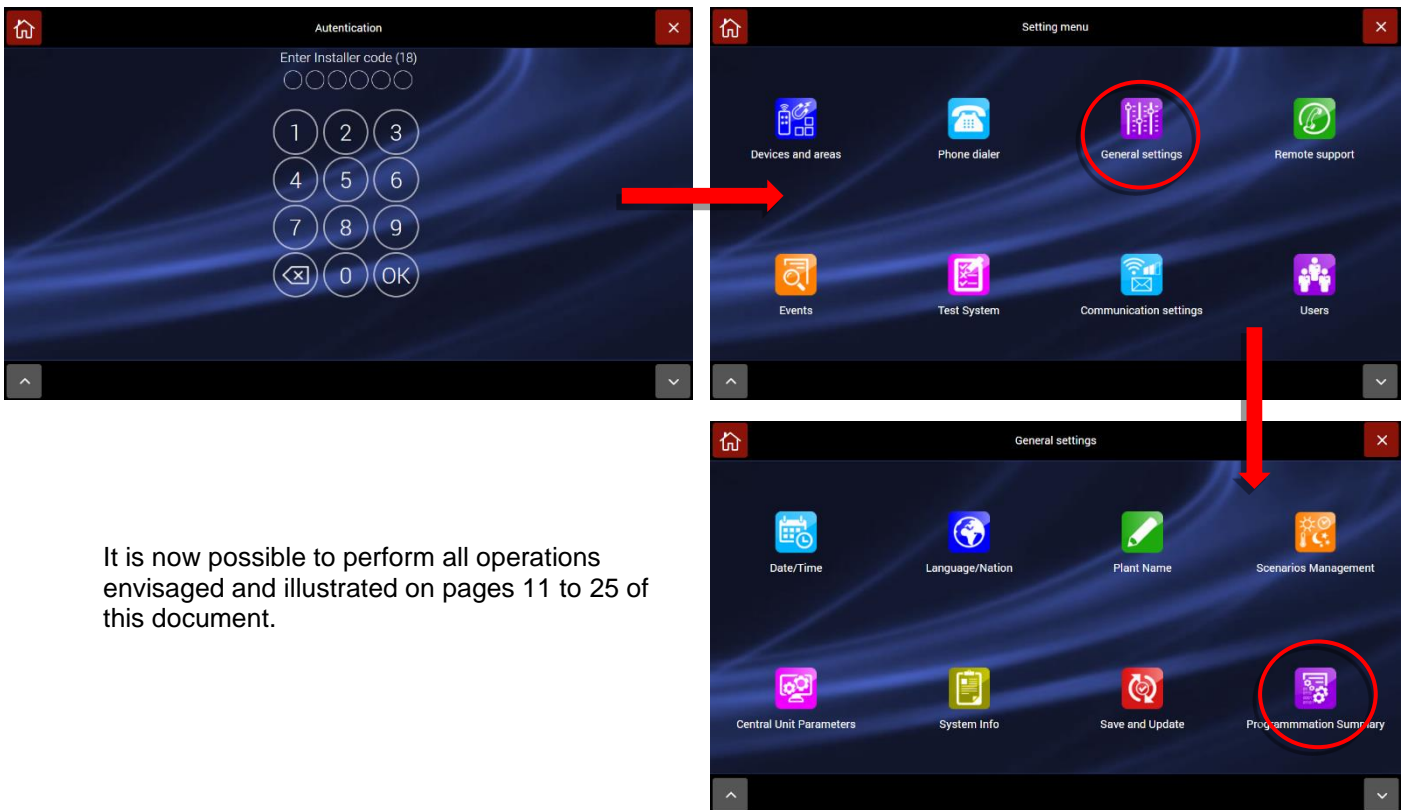


- c. Confirm by pressing OK.
- d. Exit the programming wizard (by pressing the home button ).
- e. Connect a PC or other device equipped with a browser to the Wi-Fi network generated by the control unit:
- I. At initial start-up, the control unit is in ACCESS POINT mode: it generates a Wi-Fi network whose SSID is encoded with the name AF927\_XXXXX, for example: AF927\_C6HAB
  - II. **Default IP address: 192.168.100.1**
  - III. No password is required to access the AF927\_XXXXX network
  - IV. After entering the IP address in the browser, the first screen that appears is the control unit start-up screen.

- f. From any browser click “Settings” on the home page and enter the code for the Power User (Master User)



Press “installer settings” and enter the installer code:  
This calls up the first of the following screens; from here select “General settings” and then “Programming summary”.



It is now possible to perform all operations envisaged and illustrated on pages 11 to 25 of this document.

# CONTROL UNIT MENU - INSTALLER INSTRUCTIONS

## SUMMARY OF HOME PAGE FUNCTIONS

The main screen (**home page**) summarises control unit status.



Home page button  
 Connected user type icon  
 Back-up battery charge level  
 Mains power supply present  
 System name  
 Date/Time  
 GSM signal level  
 Wi-Fi signal level  
 Cloud status and cloud menu  
 Remote assistance connection status  
 Settings menu button

ON/OFF  
 Eventi  
 Scenari / Prog.Orario  
 Utenti  
 Camera  
 Test Impianto  
 Parametri Comunicazione  
 Impostazioni

ALARM 1  
 ALARM 2  
 ALARM 3  
 ALARM 4  
 ALARM 5  
 ALARM 6

AREAS Status

ICONS for the various menus/functions  
 ON/OFF and system status button

System deactivated  
 System activated

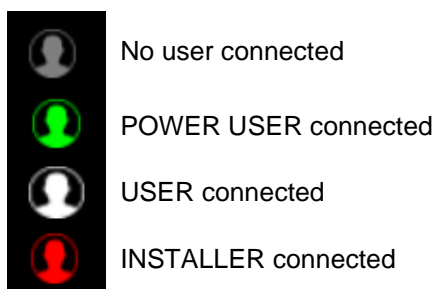
Rest condition: area switched off  
 Area being activated  
 Area activated  
 Area in alarm

**Note:** The display modes may vary depending on whether the "ENABLE IMMEDIATE INFORMATION" function is activated (ask your installer for details).

## MEANING OF MULTI-STATUS ICONS

### Type of user connected to the control unit:

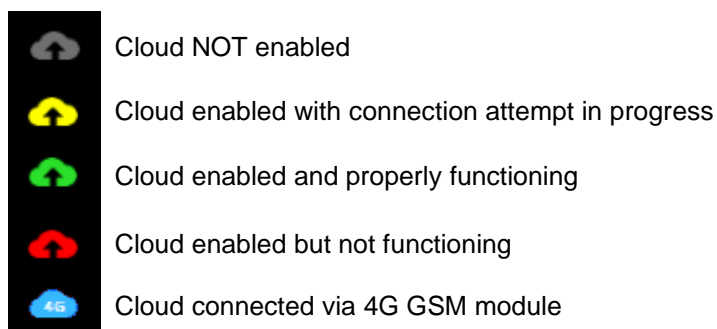
**Note:** indication of the type of user connected can only be activated from the WEB BROWSER and only if the "ENABLE IMMEDIATE INFORMATION" function is active.



Click on the user icon to disconnect the user type. This calls up the following POP-UPS:

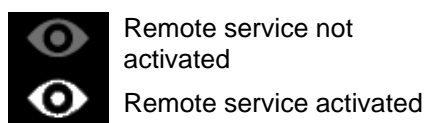


### Cloud status:



**Note:** clicking on the icon calls up the cloud connection parameter settings menu.

### Remote connection status (remote service):



## MEANING OF THE OTHER CONTROL UNIT ICONS

### System activation



See user manual - Function not permitted for installer.

### Control Unit Events Memory



See settings menu - the installer can only access this by first calling up the settings menu.

### Scenarios Management and Time Programmer



See settings menu - the installer code can access this via the settings menu – general settings.

### User Management



See settings menu - the installer can only access this by first calling up the settings menu.

### View Cameras



See user manual - Function not permitted for installer.

### Test functions



See settings menu - the installer can only access this by first calling up the settings menu.

### Communication parameters



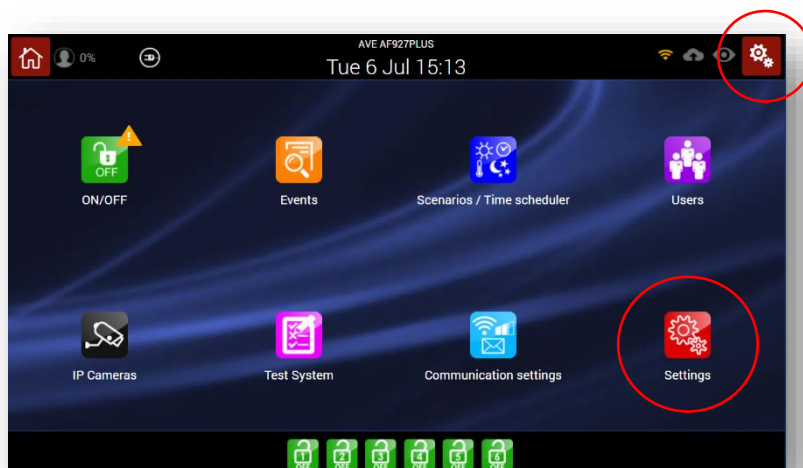
See settings menu - the installer can only access this by first calling up the settings menu.

### Settings

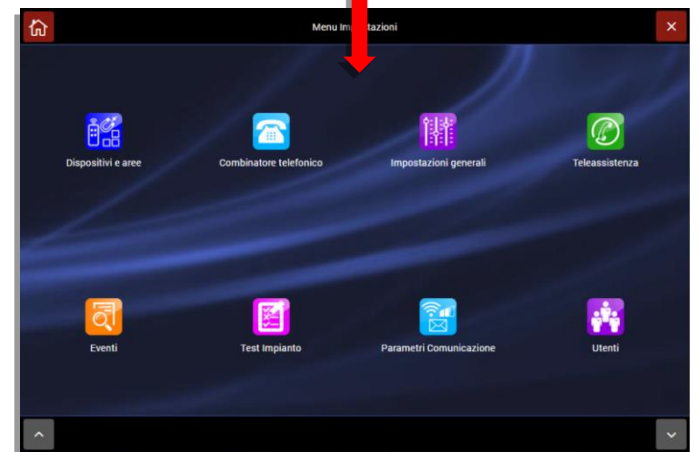
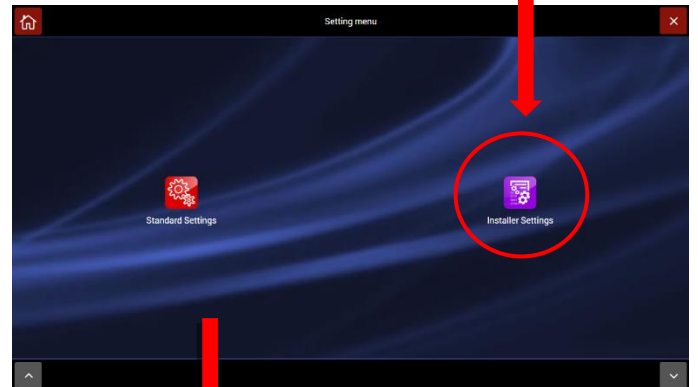
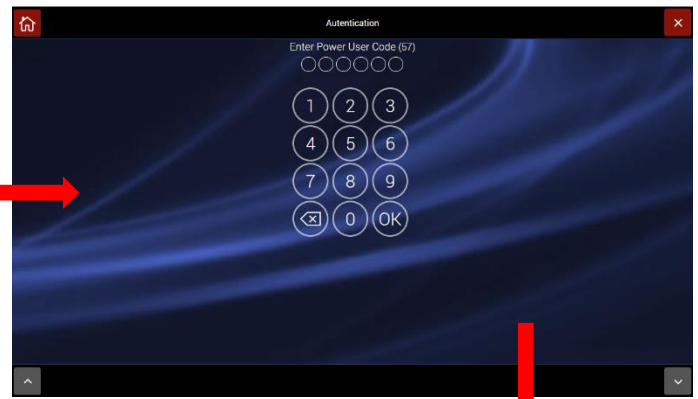


Enter to the settings menu.

1. To call up the settings menu, click on the “SETTINGS” icon



2. Enter the Power User code and press the “Installer Settings” icon;



3. enter the installer code and press “OK”

4. This calls up the menus with the settings enabled for the installer:



## Devices and Areas

Clicking on the Devices and Areas icon calls up the screen shown below:

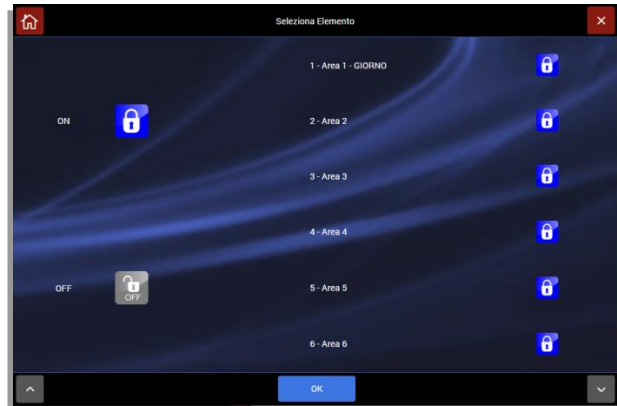
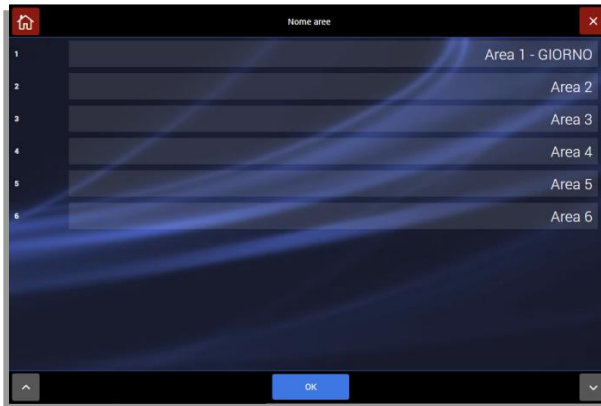


### 1. Areas

To set the name of the areas, press the corresponding button

Enter the box for the desired area and edit its name. After completing the operation, confirm by pressing OK.

When the control unit is switched on/off, the area name is displayed in the area activation screen.




### 2. Devices

This screen summarises all control unit devices with the following details:

- Device name;
- Type of device (e.g. internal wired expansion, magnetic contact);
- Node: device number for interfacing with the AVE Domina SMART home automation system;
- Device areas: device area;



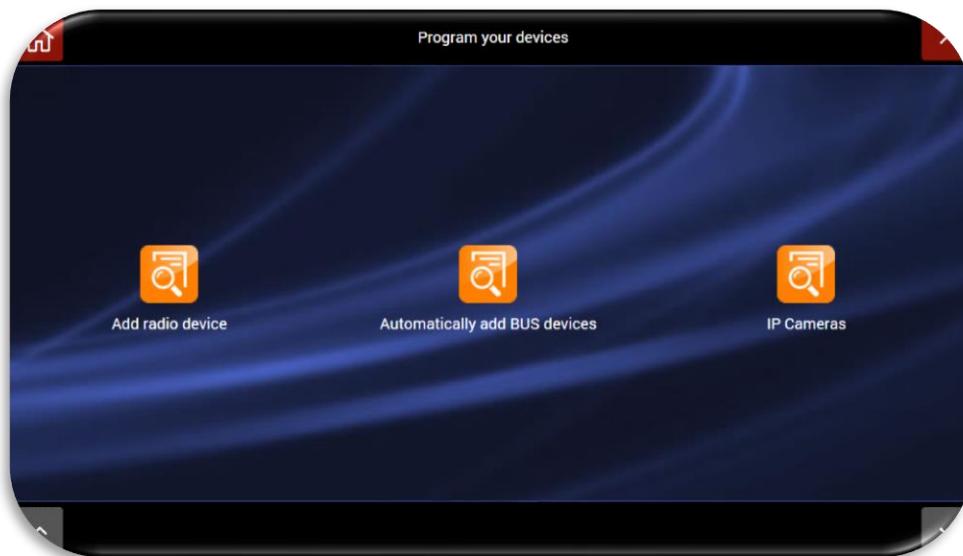
Note: the control unit default configuration only displays the

wired board inside the control unit itself. To activate the wired inputs and related parameters, click on the eye  icon and activate the wired inputs required for the system.

Meaning of the buttons present:

- “Filter by type of device”: displays only devices of the given type
- “Filter by areas”: displays only the devices present for the given area
- “Add other devices”: makes it possible to add more radio devices.

To add further devices, press “Add other devices” at the bottom of the screen. This calls up the following screen:

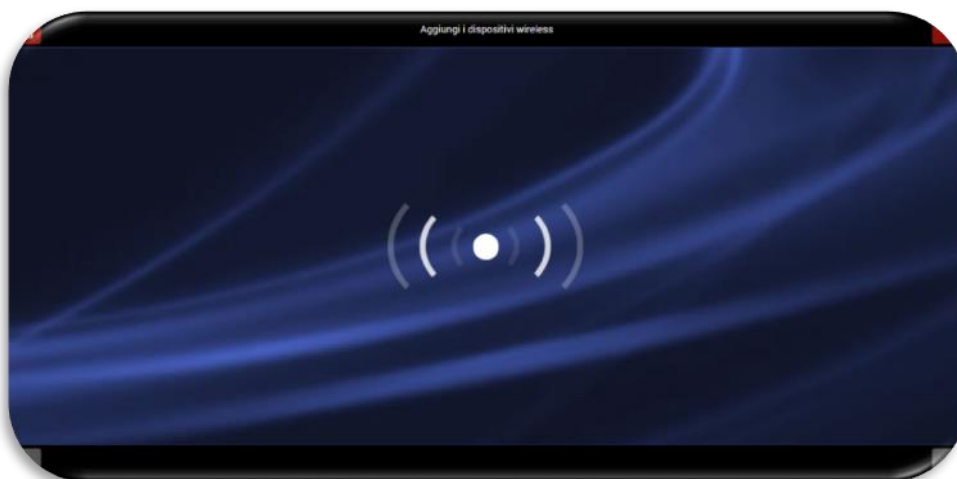


Press the button:

- “Add devices via radio” to acquire devices (detectors, remote controls, sirens, etc.) via radio.
- “Camera IPs” to acquire the IP for the cameras that can be polled via HTTP using JPEG polling (HTTP snapshot) - For compatibility and other info, log onto <https://www.ispyconnect.com/sources.aspx> and/or see the list of products tested by the AVE INTEAM service.

## RADIO DEVICE ACQUISITION

- a. To acquire a new intrusion detection device (detectors, remote controls, sirens, etc.), press “**Add devices via radio**”. This calls up the following screen.



To acquire peripheral devices, proceed as follows:

Code	Description	Acquisition mode	Actions to be completed for acquisition
AF943R	Remote control	Press RED+GREEN	Enter name and configure keys
AF915R-DB AD915R-MDB AF963R-DB AF964R-DB AF965R-DB AF976R-DB	Detectors	Insert battery	Enter name, match areas
AF53903R-DB	Siren	Insert battery	Enter name, match areas
AFTR02	Interface for technical alarms	Insert battery	Enter name
AFINTFIL	Interface for wired bus	Plug into control unit	Match areas
AFTR03	Signal repeater	Plug into a mains power outlet (230Vac)	Enter name, match areas
AF340-T	Tag	Bring the tag at the bottom left-hand side close to the microphone	Enter name, match areas (by default, all are matched)
AF970R-DB	Radio keypad	Insert battery	Enter name, match areas

**Note:**  
after

the correct device save device procedure has been run, the control unit emits a confirmation BEEP and displays the image of the device saved (see example of magnetic contact AF915R-DB).

**The device acquisition procedure involves finalising the operation by pressing “OK” within no more than 10 seconds.**  
**Waiting longer makes it necessary to repeat acquisition.**



- b. Device acquisition: enter name, match desired areas and confirm by pressing OK.
- c. Repeat the procedure for all devices to be associated with the control unit.

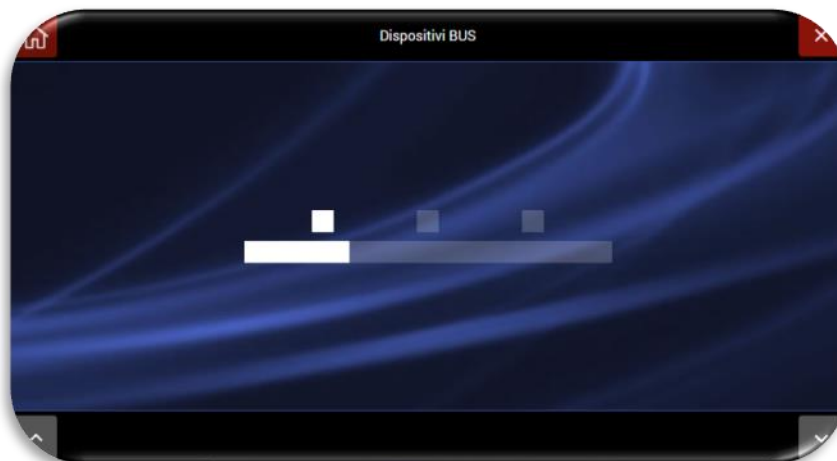
## ACQUISITION OF DEVICES OVER WIRED BUS

To acquire a new intrusion detection device connected to the wired bus generated by the AF927INTFIL interface board, click on “**Add wired BUS devices**”; this calls up the following screen:

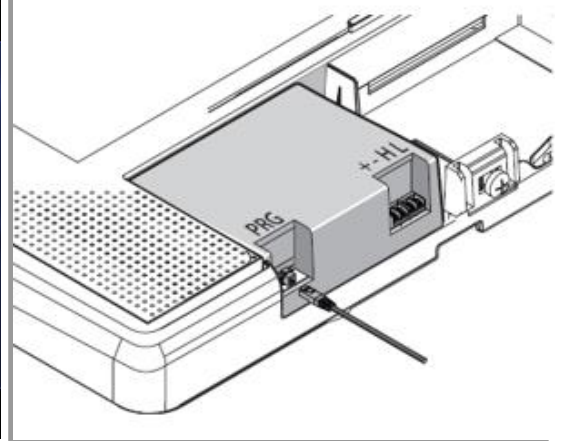
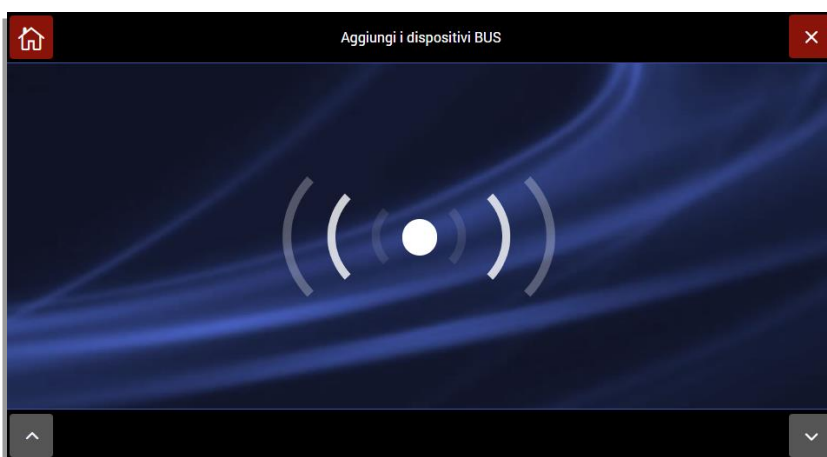


To enable the control unit to associate the input/output boards connected to the wired bus, just select the manual or automatic device association procedure.

Press “Automatic device association” and the control unit will start scanning the wired Bus to acquire the connected boards. Repeat the scanning procedure until all connected boards are recognised.



If “Manual device association” is selected, the programming cable supplied with the wired interface board must be connected to the appropriate connector for the AF927INTFIL board. The control unit enters “listening” mode while waiting connection of a board: After hooking up the connection cable, connect one board at a time until the all modules have been connected.



## ACQUISITION OF IP CAMERA

To configure an IP camera to be associated with the system:

- a. press the “**IP cameras**” button. This calls up the following screen.



Enter the parameters for the IP camera:

- **DEVICE NAME:** enter a text label for the camera name;
- **USER:** see IP camera manual (e.g.: admin);
- **PASSWORD:** see IP camera manual (e.g.: password, 0000, 1234);
- **LINK ADDRESS:** enter the network path for the camera images;
- **IP/MAC:** select whether to set the IP camera via MAC ADDRESS or IP address;
- **CAMERA MAC ADDRESS / CAMERA IP.** Enter the camera MAC ADDRESS or IP address following the previous step;
- **TCP PORT:** the control unit proposes an access port, normally 80, which must not be modified;
- **INTERVAL BETWEEN FRAMES:** then select the time interval between frames, from 1 to 5 seconds;
- **NUMBER OF FRAMES:** Select the desired number of frames, from 1 to 5;

- b. Confirm by pressing OK.

**Note:** the control unit can control from 1 to 4 cameras, show them on the display and transmit frames to programmed addresses, either in the event of an alarm or upon request. The cameras must be Wi-Fi units if the control unit is programmed as an Access Point; both Wi-Fi and LAN are possible if the control unit is programmed as a Client: obviously the Wi-Fi section cannot be disabled

**Warning!** Camera resolution: set the cameras connected to the system to a resolution of 640x480 (VGA - 65Kbytes per frame) or 1280x720 (167Kbytes per frame). With higher resolutions, a part of the image may be lost and the time required for viewing and transmission via Cloud will be significantly longer.

# INTRUSION DETECTOR PARAMETERS

## Parameters common to all devices

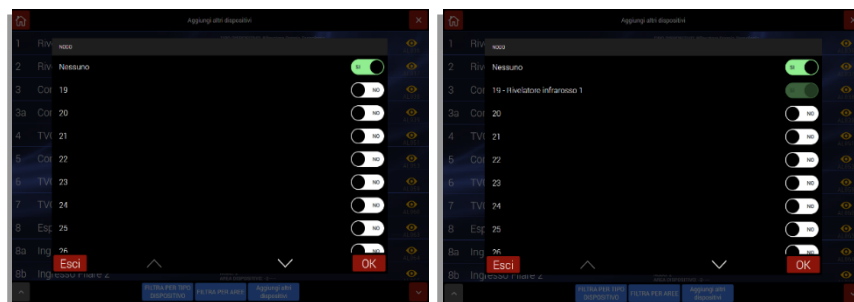
- **Area:** the device is activated by entering the area to which it belongs, which may differ for each type of alarm. More than one area can be assigned to a given device, which will sound an alarm even if only one of its assigned areas is activated.
- **Alarm delay:** the alarm given by the device is activated after the time set for each type of alarm.
- **Type of alarm:** alarms generated by the device may give rise to an “acoustic alarm” (siren and external communications) or “voice alarm” (pre-recorded voice message broadcast by the sirens and control unit in addition to external communications). Two voice alarms are possible, with different messages.
- **Alarm LED:** normally enabled, can be disabled.
- **Disablement time after an alarm (temporary blocking of operation):** adjustable from 0 to 180 seconds, depending on the frequency of alarm transmission. If the detectors are subject to continuous use (heavily frequented areas/passageways, windows constantly opened and closed), this time should be increased to reduce battery consumption.
- **Chime function:** this function is operative if the control unit is off and involves signalling entry into the room protected by this detector. When this function is enabled, at each entry, the control unit emits a brief acoustic signal (ding-dong) for the set amount of time; one or more sirens can be programmed to emit voice message 2, to be recorded for the purpose (welcome or other).
- **Interactive configurations (AND)**  
With the AND function, the control unit alarm status occurs only if at least two detectors in a given area (1-6) transmit an alarm within an adjustable time (10-180 seconds - by default 30 seconds): in this case the likelihood of a false alarm occurring in environments subject to disturbance (particularly outdoors) is reduced by suitably positioning two detectors to protect the same area.  
The possibilities for enabling the AND configuration are:
  - AND regarding two detectors: this involves the detector currently being set and another, to be chosen from the list of those already programmed (which can be viewed on the list in the control unit). The alarm signal will only be given if both detectors signal the event.
  - Area-related AND: all detectors in the area are involved. A control unit alarm occurs if at least two detectors enter alarm mode within the programmed amount of time.

**Warning!** To prevent the degree of system security from being compromised, it is not advisable to program two non-volumetric detectors in AND mode.

Raising the detector alarm higher can trigger capturing frames by one or more of the Wi-Fi cameras associated at this stage. These images can be transmitted as e-mail attachments as quickly as possible, depending on the set connections (GPRS-Web).

- **Note:** this corresponds to the number of the input that must be set (using the home automation configuration program AVE Domina Plus Configurator) in the database of the AVE home automation supervisor (if present in the system and interfaced with the control unit), thus enabling the home automation supervisor to read the detector-related data. Node numbering follows the logic indicated below:
  - numbers 1 to 16 are reserved for detectors connected to the internal wired expansion board
  - numbers 17 and 18 are reserved for the outputs connected to the internal wired expansion board
  - numbers 19 and up are reserved for radio devices

Clicking on the word “NODE” calls up a box used to associate the desired number; this box must be entered in the Home automation database for that detector. If not already occupied by detectors (figure on the left), the system proposes all available numbers. If some detectors have already been assigned numbers, the system only proposes the numbers still available. In this way, a given “NODE” number cannot be associated with two different detectors (figure on the right).



- **AF915R-DB and AF915R-MDB: Magnetic contact - additional parameters**

- Door-open detection:** normally enabled (EN 50131), can be disabled.
- Magnet tamper detection:** normally disabled, can be enabled.
- Impact sensor (break-in detection):** normally active, can be bypassed or its sensitivity adjusted.
- Cable inputs 1 and 2:** these are displayed in the list of devices if, during programming, they have been enabled for use. In this case, each can be configured as NC-NO-Balanced-Double Balanced, with or without pulse counting (see device instructions).

ID	Nome	TIPO DISPOSITIVO	NODO	AREA DISPOSITIVO	Icona
3	Rivelatore Dual Tech 1	Rilevatore Doppia Tecnologia	Nessuno	-2----	AL036
4	Rivelatore infrarosso 1	Rilevatore Infrarosso	Nessuno	-2----	AL037
5	Contatto Magnetico 1	Contatto Magnetico	Nessuno	--3--	AL038
5a	Contatto Magnetico 1a	Contatto Magnetico	Nessuno	--3--	AL039
5b	Contatto Magnetico 1b	Contatto Magnetico	Nessuno	--3--	AL040
6	TVCC 1	Telecamera	Nessuno	123456	AL051
7	Contatto Magnetico 2	Contatto Magnetico	Nessuno	--3--	AL053
8	TVCC MACNORMALE	Telecamera	Nessuno	123456	AL059
9	TVCC 2N	Telecamera	Nessuno	123456	AL060

Magnetic contact on which the 2 auxiliary inputs have been enabled. The triangle next to the “eye” icon means that the control unit has yet to send the information to the devices in the field. Upon first transmission from control unit to device, the icon will automatically be deleted.

- **AF963R-DB (PIR) – AF965R-DB: Double PIR curtain-effect detector - additional parameters**

- Range adjustment (Sensitivity):** assign a range suitable to the unit model and to the dimensions of the room to be protected, from level 1 (minimum - about 4m) to level 4 (maximum - about 15m).
- Note:** units AF965R-DB require that each of the two infrared sensors be specifically adjusted.
- Integration adjustment (alarm validation time):** adjust from 1 (minimum - 50 msec.) to 8 (maximum - 400 msec.), increasing as needed in response to any possible disturbance within the room (air currents, convection heaters, random presence of large insects, moving curtains and the like).
- Pulse count adjustment:** adjust from 1 (alarm at first valid signal) to 3 (alarm at third signal) according to the possibility of potential false alarms.
- Temperature compensation:** enable the function (Y) only in installations where the average temperature is very high.
- Double detection:** enable (Y) to drastically reduce the possibility of false alarms in particularly disturbed environments or in the case of installations outside the rooms.
- Models with anti-blinding function:** the function can be activated (Y) or excluded (N). Warning! Blinding triggers the tampering alarm and is active 24/7.

### AF964R-DB: outdoor double PIR radio detector + microwave technology - additional parameters

The device has two PIR sensors (sensor A located at the top, sensor B at the bottom of the device) plus a microwave sensor.

- a) **Protection against opening:** this parameter involves tampering to open the device cover;
- b) **Protection against removal:** this parameter involves tampering to remove device from wall;
- c) **Temperature compensation:** increases the sensitivity of both PIRs (A and B) when room temperature is very close to the external temperature of a human body, around 31/32°C;
- d) **Alarm LED:** used to deactivate sensor LEDs under normal operation; the option is by-passed when the sensor is in test mode;
- e) **Anti-blinding:** this parameter is not linked to either the PIR or the microwave sensor since it is a separate infrared TX/RX circuit that checks whether the sensor is covered and/or painted over; when tripped, the sensor triggers a tampering event;
- f) **Sensitivity adjustment - upper PIR:** the parameter refers to the sensitivity of PIR "A": the higher the parameter value, the greater the sensor range;
- g) **Sensitivity adjustment - lower PIR:** as above, but for sensor "B";
- h) **Sensitivity adjustment - MW:** the higher the parameter value, the greater the microwave sensor distance range;
- i) **Pulse count adjustment - upper PIR:** the parameter refers to the pulse count for PIR "A": the lower the number, the more sensitive the sensor (e.g., if the value is set to 2, it means that two sectors of the Fresnel lens must be crossed to trigger an event)
- j) **Pulse count adjustment - lower PIR:** as above, but for sensor "B";
- k) **Integration adjustment - upper PIR:** the parameter refers to sensor "A"; increasing the value, lengthens the time required to detect an intruder in the protected area; on the contrary, for greater sensor reactivity, decrease the value.
- l) **Integration adjustment - lower PIR:** as above, but for sensor "B";
- m) **Double detection alarm:** before transmitting the true and proper alarm to the control unit, the sensor must pick up the presence of the human target in the protected area twice: the first detection — whether PIR A / PIR B and MW — does not transmit the alarm.

### AF976R-DB: outdoor double PIR radio detector, long range curtain effect - additional parameters

The device has two PIR sensors (sensor A located at the top, sensor B at the bottom of the device).

- a) **Protection against opening:** this parameter involves tampering to open the device cover;
- b) **Protection against removal:** this parameter involves tampering to remove device from wall;
- c) **Temperature compensation:** increases the sensitivity of both PIRs (A and B) when room temperature is very close to the external temperature of a human body, around 31/32°C;
- d) **Alarm LED:** used to deactivate sensor LEDs under normal operation; the option is by-passed when the sensor is in test mode;
- e) **Anti-blinding:** this parameter is not linked to either the PIR or the microwave sensor since it is a separate infrared TX/RX circuit that checks whether the sensor is covered and/or painted over; when tripped, the sensor triggers a tamper event;
- f) **Sensitivity adjustment - upper PIR:** the parameter refers to the sensitivity of PIR "A": the higher the parameter value, the greater the sensor range;
- g) **Sensitivity adjustment - lower PIR:** as above, but for sensor "B";
- h) **Pulse count adjustment - upper PIR:** the parameter refers to the pulse count for PIR "A": the lower the number, the more sensitive the sensor (ex. if the value is set to 2, it means that two sectors of the Fresnel lens must be crossed to trigger an event)
- i) **Pulse count adjustment - lower PIR:** as above, but for sensor "B";
- j) **Integration adjustment - upper PIR:** the parameter refers to sensor "A"; increasing the value, lengthens the time required to detect an intruder in the protected area; on the contrary, for greater sensor reactivity, decrease the value.
- k) **Integration adjustment - lower PIR:** as above, but for sensor "B";
- l) **Double detection alarm:** before transmitting the true and proper alarm to the control unit, the sensor must pick up the presence of the human target in the protected area twice: the first detection — whether PIR A / PIR B and MW — does not transmit the alarm.

### AFTR02: universal transmitter for technical alarms

The device makes it possible to control up to two autonomous probes/sensors, which provide a potential-free electrical output, to be connected to one of the wired inputs on the transmitter itself.

In addition to what is envisaged in the technical sensor programming, the inputs must be configured as for wired alarms (NC-NO-BIL-DBIL) and the pulse count, when used, and the cut-off time must be adjusted.



### AF53903R-DB: radio siren

Sirens can sound at full power or they can emit voice messages that are pre-recorded (on the board in the siren) or, in their absence, brief acoustic signals. The following parameters can be configured:

- a) Volume of the acoustic signals and alarm voice messages
- b) Volume of the acoustic signals and pre-alarm voice messages (input delay)
- c) Volume of activation/deactivation signal
- d) Sensitivity of break-in detection sensor
- e) Bypass protection against removal
- f) Ring times
- g) Pre-alarm flashing
- h) Flashing when activated (3 flashes) and deactivated (1 flash)
- i) Flashing when "activated" (once every 10 seconds - twice in case of alarms)

### AFTRA03: signal repeater

The device is useful when there are problems in the radio range between control unit and certain peripheral devices due to excessive distance between devices or the presence of numerous physical obstacles. The signal repeater must be plugged into a 230V outlet that is equidistant from the control unit and the distant devices: it is necessary to "teach" the device the control unit RF codes and only those for the devices to be repeated: these operations are guided by the control unit Settings-Devices and Areas-Device's menus. Also see the unit manual. Each system can handle from 1 to 4 repeaters.

### RADIO KEYPAD PARAMETERS

The AF970R-DB radio keypad enables the system to be activated, deactivated and partialized.

Press any button on the keypad to turn its LCD on.

Use the ▲ (Up) and ▼ (Down) buttons to move between menu items.

To select an area, enter the digits for that area (e.g., Area 2 = button 2).

If an incorrect user code is entered three times, all operations are blocked for 180 seconds.

1. TOTAL ENTRY: enter the user code and wait for the activation/deactivation menu to appear;  
Press ON, making sure that "TOTAL" has been selected;
2. PARTIAL ACTIVATION:  
enter the user code and wait for the activation/deactivation menu to appear;  
Set the cursor on the 'Areas' line and press ENTER;  
Select the areas to be activated by pressing the button with the number corresponding to the desired area;  
Press ON to activate partial activation of the control unit.
3. DEACTIVATION: enter the user code and wait for the activation/deactivation menu to appear;  
Press OFF

Total activation/deactivation of the system can also be performed using a transponder key art. AF340-T.

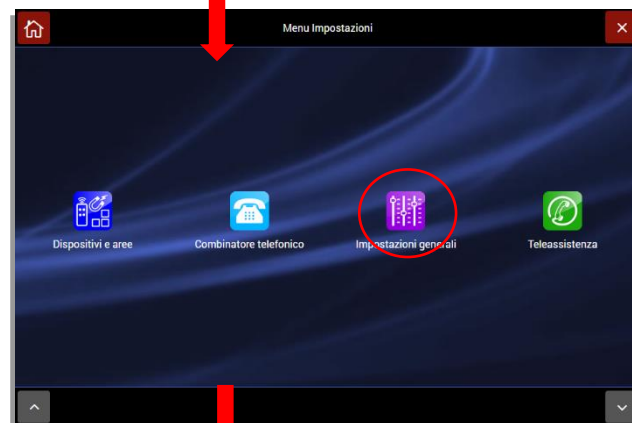
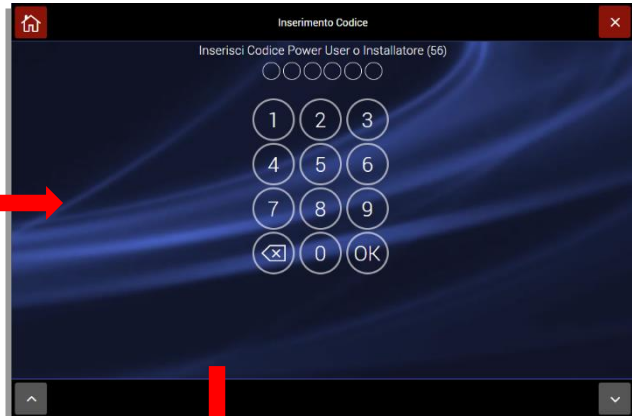
1. TOTAL ACTIVATION: with the system switched off, bring the transponder key near the keypad for one second and remove it from the reader;
2. PARTIAL ACTIVATION: when the system is activated, hold the transponder key close to the keypad until the system is partially activated;
3. TOTAL DEACTIVATION: with the system deactivated, bring the transponder key near the keypad for one second and remove it from the reader;

**Note1:** when the keypad is switched on, the user interface menu is displayed on the LCD. If the menu is not displayed or the antenna symbol is displayed, the keypad is outside the maximum range. Move closer to the control unit and press a button to realign the system.

**Note2:** the AF970R-DB radio keypad cannot be associated with an AFTA03 signal repeater.

## BYPASSING DEVICES

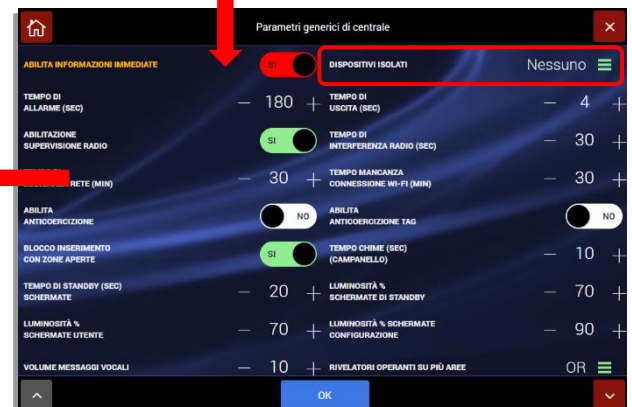
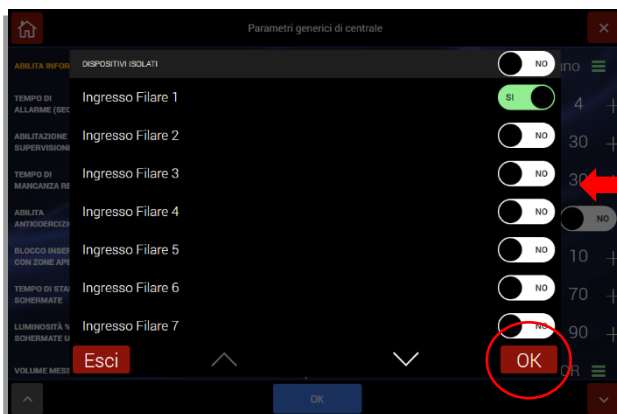
Both the installer and customer can always bypass a malfunctioning device.  
To perform this operation:



1. Call up the "Settings" menu;
2. Enter the installer code;
3. Call up the "General settings" menu;
4. Select the "Control unit parameters" menu;
5. Call up the "Bypass devices" parameter;
6. From the list of devices, select the one to be bypassed and press "OK".

### WARNING:

The bypassed device or devices will remain permanently in that state. To restore correct operation of the device, run the same operation performed to bypass it and delete the active bypass parameter.



## VOICE MESSAGES



The control unit has multiple voice messages relating to different categories:

- **EVENTS:** these are the messages relating to the main events generated by the control unit (e.g. ALARM, AGGRESSION RESCUE, etc.).  
Briefly record the selected event by reading it on the display or adapting it to the local situation (e.g. for “power failure” clearly spell out POWER FAILURE; for “panic rescue” clearly spell out PANIC RESCUE or I AM AT HOME AND I AM AFRAID; for “medical aid” it can be MEDICAL ASSISTANCE or I AM AT HOME AND I FEEL ILL  
**Note for Voice Alarm 1 and 2:** the control unit sends these messages out at the same time as the voice alarm command sent to both internal and external sirens and are used to alert the user. Example: control unit voice message 1: INTRUSION DETECTED WARNING (location information will follow, i.e. Area and Device); control unit voice message 2: ATTENTION, SOMEONE HAS ENTERED THE SHOP (bell function).
- **AREAS:** these are the messages that describe the area into which the system is divided (e.g. OFFICE FIRST FLOOR).
- **SYSTEM:** two separate messages are available:
  - Description of call source: if the message is addressed to unknown persons (police), the user's name and address must be included; if it is addressed to persons who are known, a brief reference to the protected premises may be enough for them to identify the source.
  - Answer to incoming call: if necessary, record a message to the user calling the control unit, telling them what they must/can do.
- **DEVICES:** this is a voice message that can be associated with each device in the system (e.g. “Room detector”). If there is an alarm, the dialler first plays the alarm event message followed by the message regarding the device that generated the alarm.

The control unit contains pre-recorded messages for the main system events:

- **EVENTS:**
  - Alarm = “Intrusion Alarm”
  - Tamper = “Tampering in progress”
  - Battery dead = “Battery dead”
  - Aggression rescue = “Robbery in progress”
- **AREAS:**
  - AREA 1 = “Perimeter detectors area”
  - AREA 2 = “Volumetric detectors area”




Messages are automatically available in the language selected for the control unit. Selecting “**Record voice messages**” lets you select the category of messages to be edited.

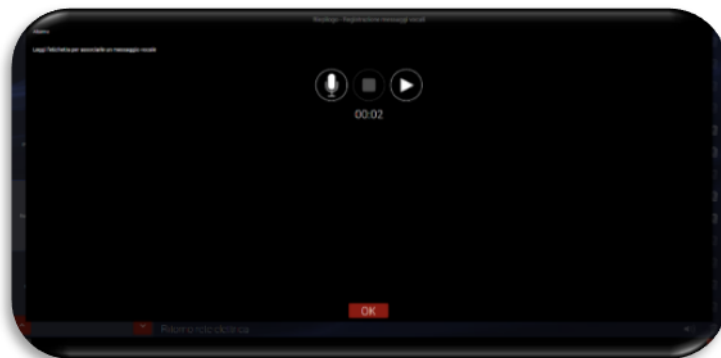
If, for example, the alarm message is to be edited:






a. Press the “Events” icon to call up the screen shown above on the right.

All voice messages can be edited:

- The speaker icon has two states:
  - I.  = voice message recorded
  - II.  = voice message not recorded
- Click on the “trash” icon  to delete the voice message
- Clicking on the message name icon calls up the screen shown below where the voice message can be recorded/edited.



The meaning of the Pop-Up icons is given below:

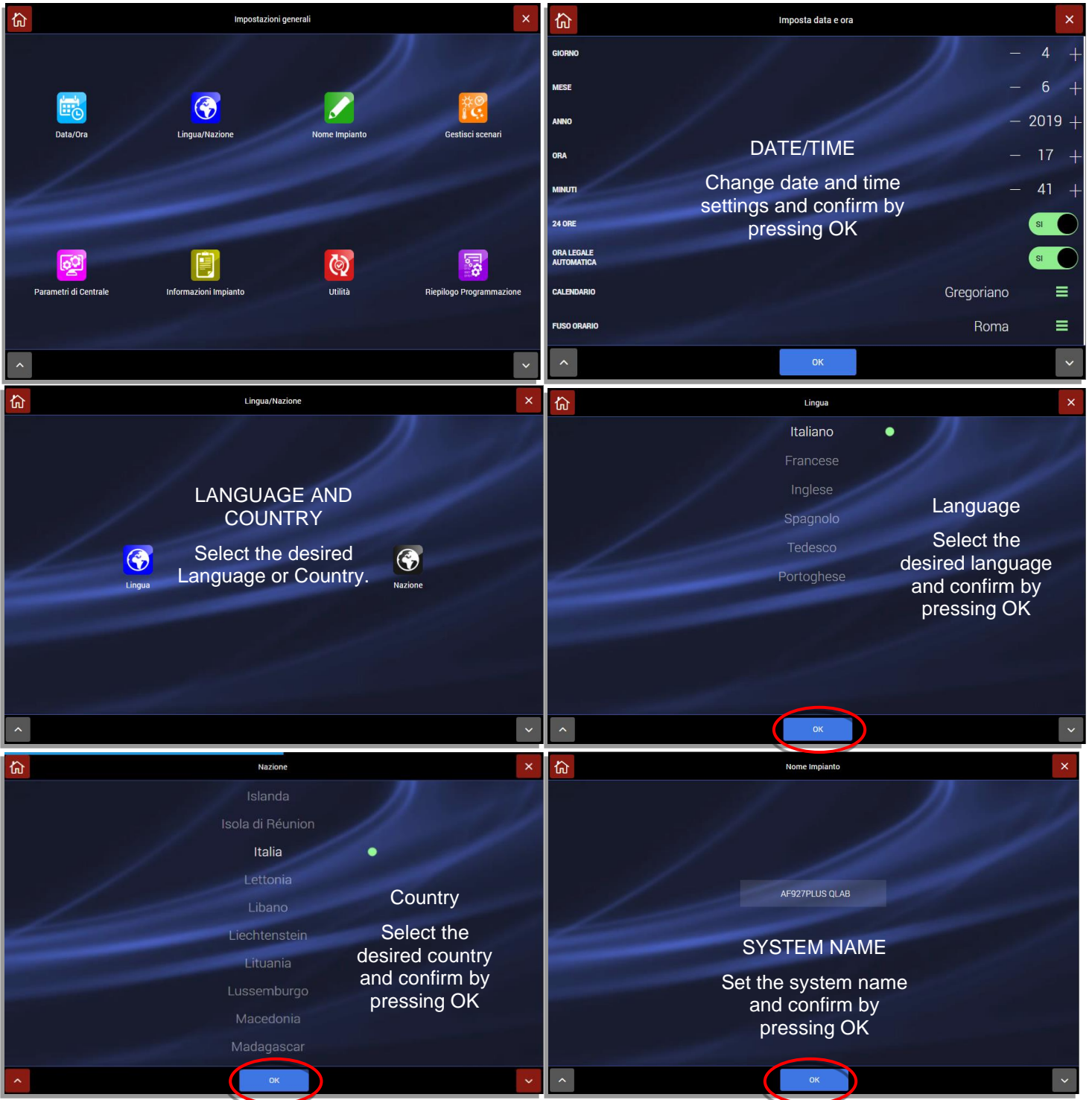
-  = start recording key
-  = start playback key
-  = stop playback or recording key

b. When finished recording, confirm by pressing OK.

## GENERAL SETTINGS

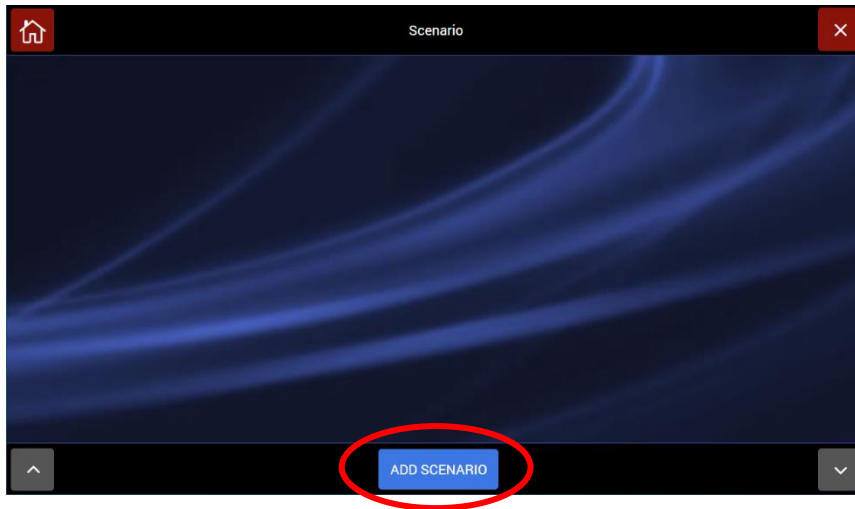
From the “General Settings” menu, it is possible to make all changes for the following parameters:

- Date/Time
- Language
- Country
- System name

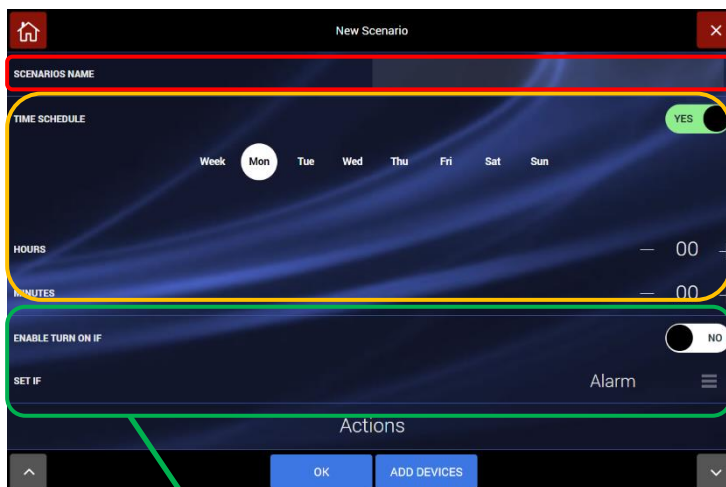


## Scenario management

- a. Press “ADD SCENARIO” to add a scenario or press on the icon for the scenario to be edited:



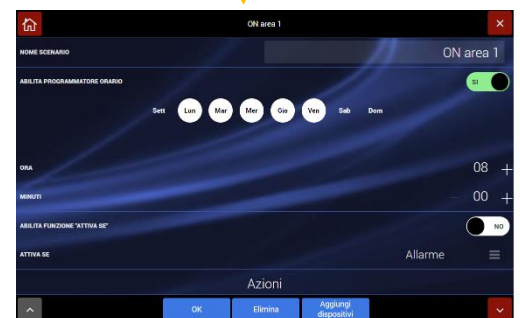
- b. This calls up a page where the scenario data can be added:



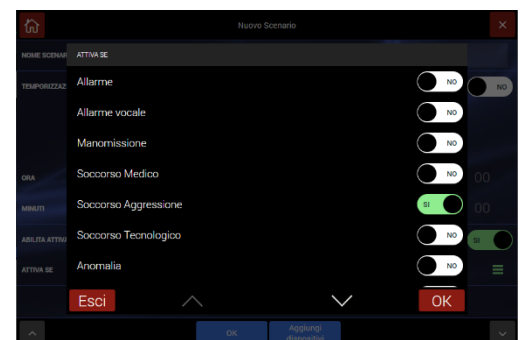
a) Scenario name

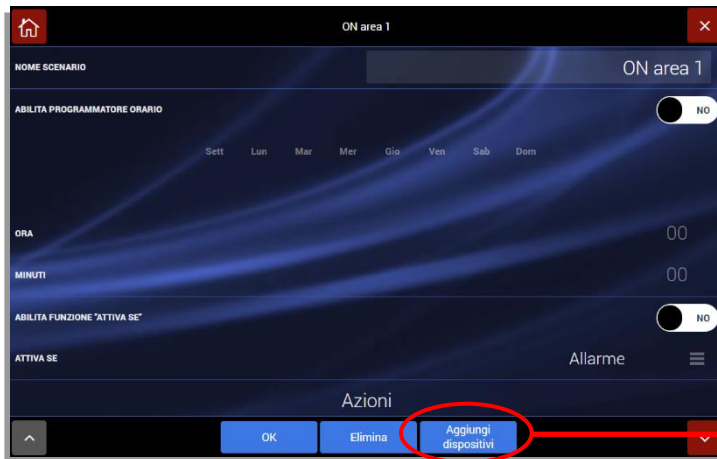
b) For each scenario, it is possible to set the activation time and days on which it is to be activated.

**Note:** the time is the same for all days chosen.

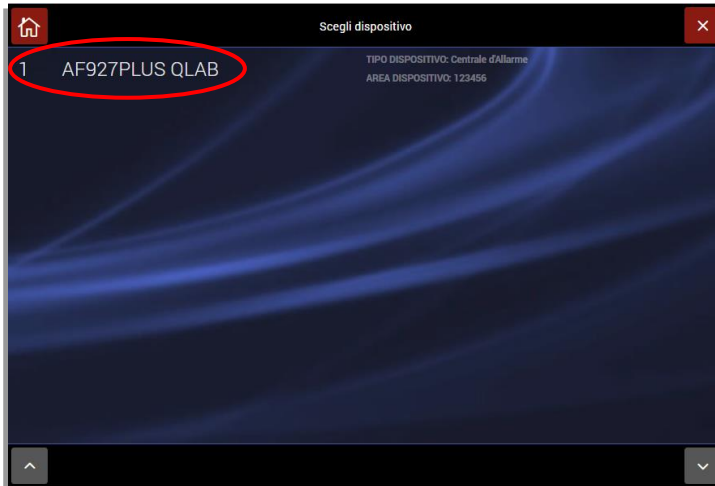


c) For each scenario, activation can be generated not only by time but also following a specific event. Enabling the “ENABLE ACTIVATE IF FUNCTION” and pressing “ALARM” displays the event selection POP UP.





d) Press "Add Devices" to add devices to the scenario.

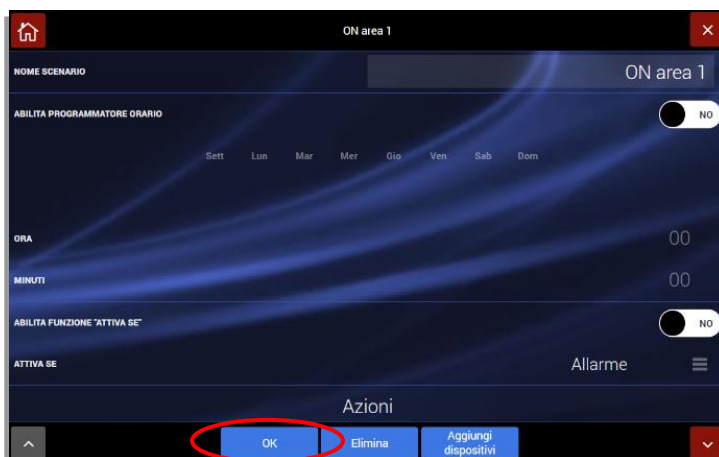


e) From the list, select the device to be added.



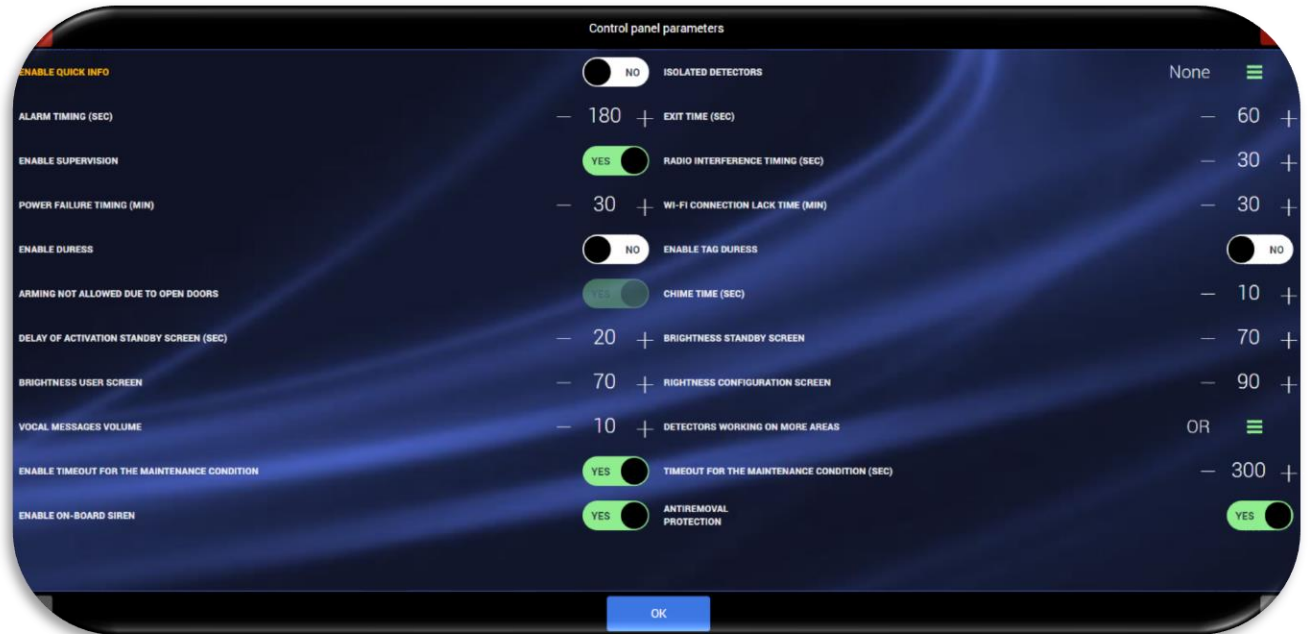
f) For the selected device, set the action to be performed and confirm by pressing "ADD SCENARIOS".

**Note** Just one action is possible for each device (e.g. for the intrusion detection control unit, only activate or deactivate can be selected).



g) From the control unit home page, confirm by pressing OK.

## General control unit parameters



- **ENABLE IMMEDIATE INFORMATION:** the control unit and keypads display the event without the need to enter codes. This function is very convenient for the user as it simplifies control unit management and displaying of the various events.

**Warning!** This function is against regulations: enabling it also provides the installer with direct access to control unit programming (with his own PIN). Remember that enabling this function is contrary to the requirements of EN50131-3 - Grade 2. For further details see APPENDIX.

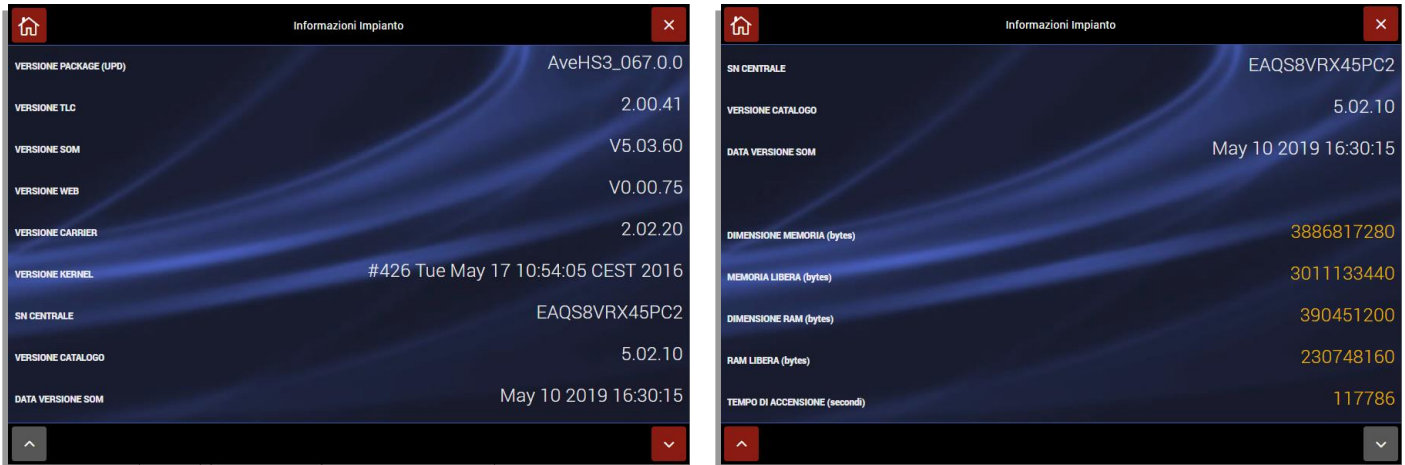
- **BYPASS DEVICES:** makes it possible to bypass wired control unit devices and/or inputs.
- **ALARM TIME:** this is the length of time for the acoustic or voice alarm, set by default to 180 seconds and variable up to 999 seconds.
- **OUTPUT TIME:** this is the length of the delay before alarm activation after the operation has been activated, set by default to 60 seconds and variable up to 99 seconds.
- **ENABLE SUPERVISION:** each peripheral device transmits signals at regular intervals to indicate that it is “alive”. The absence of these signals for more than the time specified in EN 50131 gives rise to an anomaly signal, thus this function must be enabled.
- **RADIO INTERFERENCE TIMES:** in the presence of radio interference on both frequencies and both operating channels, the control unit cannot communicate with the peripheral devices. If the disturbance lasts for more than the set time — by default 60 seconds and variable from zero to 180 seconds — a tamper alarm occurs. Obviously, the shorter the time set, the sooner the alarm will sound: however, it is advisable never to set it below 10 seconds, except in maximum security installations.
- **POWER FAILURE:** after 10 seconds with no 230V power supply, the control unit shows the event on the display. On the other hand, communication will be sent to the outside, by all means envisaged, once the programmable amount of time has elapsed after the indicated 10 seconds. Therefore a reasonable amount of time should be set.
- **TIME WITHOUT Wi-Fi CONNECTION:** after 5 minutes have elapsed with no Wi-Fi connection, the control unit shows the event on the display. On the other hand, communication will be sent to the outside, by all means envisaged, once the programmable amount of time has elapsed after the indicated 5 minutes.
- **ENABLE ANTI-COERCION:** this function is useful to deactivate the control unit when under threat: besides deactivating the system, which takes place smoothly, the robbery/aggression in progress messages are transmitted silently. Functions are normally disabled and can be enabled if desired. Anti-coercion operations are performed as follows: enter user PIN +1 (example: User PIN = 12345 - Anti-coercion PIN = 12346).
- **ENABLE ANTI-COERCION TAG:** this enables deactivation of the control unit under threat. The control unit is deactivated smoothly but, at the same time, the robbery/aggression in progress messages are transmitted silently. The functions are normally disabled. Anti-coercion operations are performed as follows: bring the TAG close to the sensor on the left-hand side of the control unit, then enter the PIN within 30 seconds.



- **BLOCK ACTIVATION WITH WINDOWS/DOORS OPEN:** this is normally enabled - if it is disabled, the system is no longer EN 50131 compliant.
- **CHIME TIME (BELL):** length of time the signal and/or vocal message 2 recorded on the sirens sounds. This only functions with “Chime”-enabled control unit and devices.
- **SCREEN STAND-BY TIME:** length of time (after the last operation performed) after which the stand-by screen is reactivated, in seconds.
- **STAND-BY SCREEN BRIGHTNESS %:** adjust brightness of display in stand-by mode as needed taking into account aspects related to power consumption.
- **USER SCREEN BRIGHTNESS %:** adjust user screen brightness as needed taking into account aspects related to power consumption.
- **CONFIGURATION SCREEN BRIGHTNESS %:** adjust screen brightness as needed taking into account aspects related to power consumption.
- **VOICE MESSAGE VOLUME:** adjust the desired volume for control unit voice messages and acoustic signals (BEEP and/or alarm sound). Setting the volume to zero disables the internal siren.
- **DETECTORS OPERATING ON MULTIPLE AREAS:** when a detector is programmed into more than one area, it can be set to issue an alarm if just one of the areas is activated or only if all of its areas are activated.
- **ENABLE MAINTENANCE TIME:** this enables the control unit to be automatically taken out of maintenance status. This function is particularly useful for screenless control units to prevent situations where, should an installer forget the control unit in maintenance mode, it would no longer be possible to access the control unit. This function is active by default. We recommend not modifying it.
- **MAINTENANCE TIMEOUT:** indicates the time after which, if no actions are performed on the control unit maintenance pages, the control unit automatically returns to the home page.

## System information

The main system data are summarised in the menu



The meanings of the various information are given below:

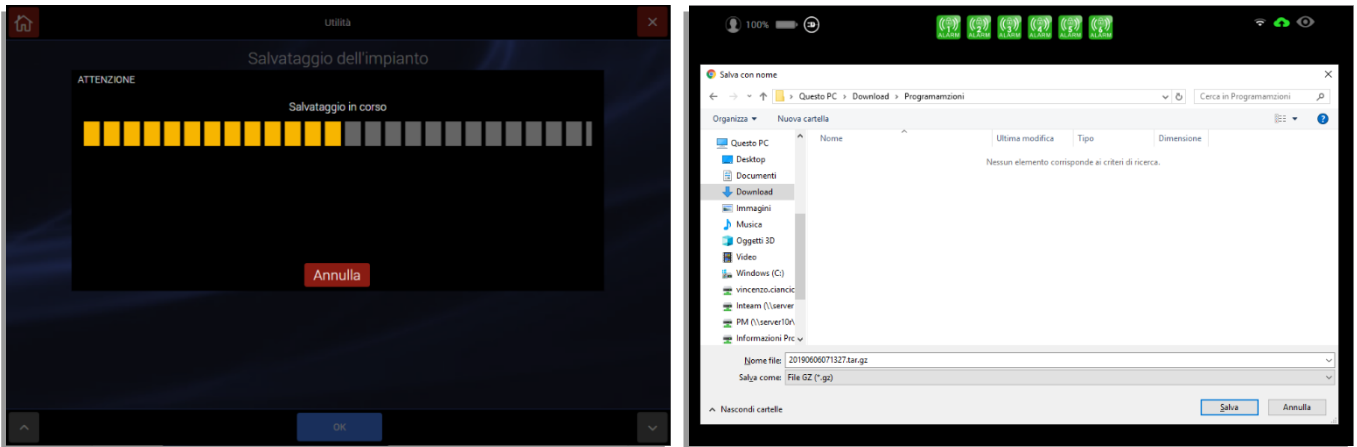
Information	Meaning
Package version (UPD)	version of the software package including the control unit
TLC version	version of TLC software
SOM version	version of the SOM (System On Module) firmware for the control unit
WEB version	version of the firmware for the WEB graphical interface
CARRIER version	software version for the low level firmware module
Kernel Version	version of the control unit operating system kernel
Control unit SN	control unit serial number
Catalogue version	Version of the catalogue of devices managed by the control unit
SOM version date	SOM version date
Memory size	Size of control unit's physical memory
Free memory	Portion of the control unit's physical memory that is free
RAM size	Size of control unit RAM
Free RAM	Portion of the control unit's RAM that is free
Start-up time	Time it takes the control unit to go on (Note: This is reset each time the control unit is rebooted and/or completely switched off)

## Utilities

The Utilities menu contains the functions required to save and restore the system database, the firmware update functions and the function to restore control unit default conditions.



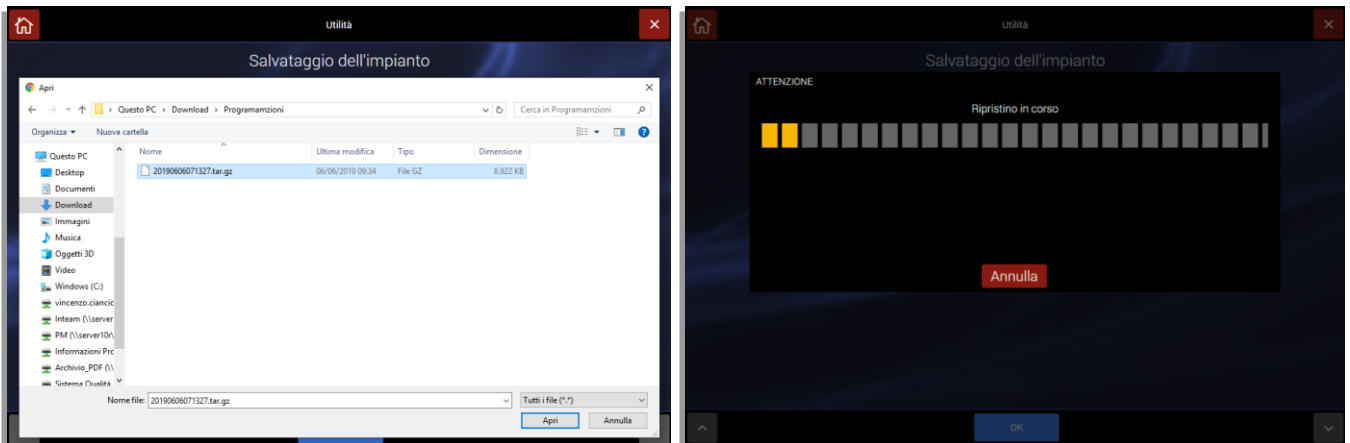
a. **System save:** pressing the icon calls up the “Save” screen.



When the procedure has been completed, the screen shown in the image to the right appears; this screen is used to select the folder where the back-up file is to be saved.

**Note:** the file saved contains all system data, including communication parameters, devices saved along with their radio codes, etc.

b. **System reset:** press the icon to call up the system reset screen.



**Note:** the file loaded overwrites all system data, including communication parameters, devices saved along with their radio codes, etc.

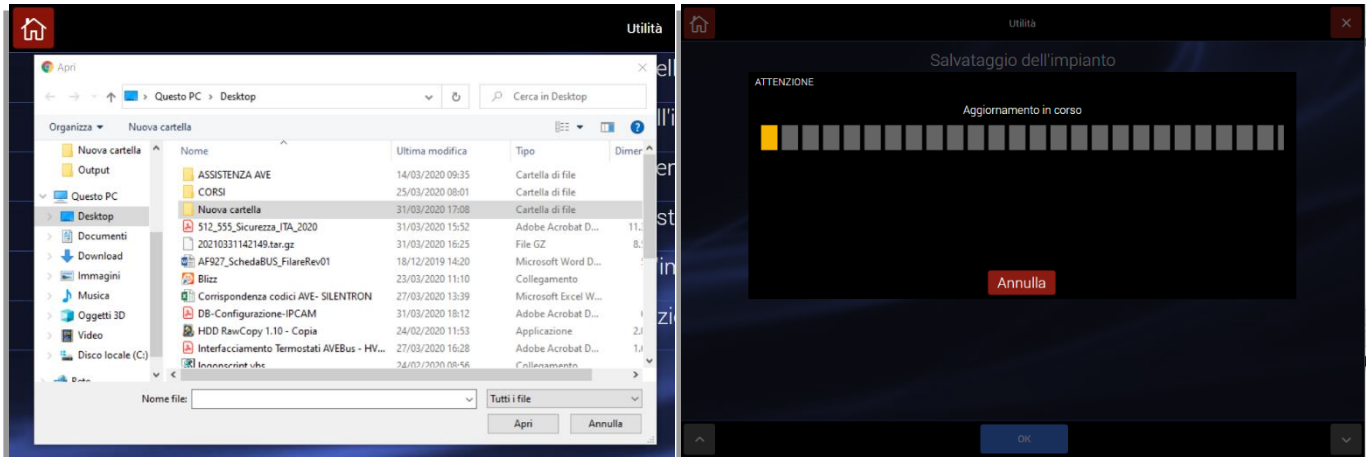
- c. **System update via browser:** the procedure makes it possible to update the intrusion detection control unit software.

**The procedure is available only if the “ENABLE IMMEDIATE INFORMATION” setting is active (see General control unit parameters).**

When the screen indicated below to the left appears, select the file containing the version of the control unit software. The name of the file and its extension are as follows:

AveHS3\_XXX.0.0.tar

where XXX is the software version number (e.g. AveHS3\_067.0.0.tar)



**Note:** do not disconnect the control unit while the firmware is being updated. Interrupting the procedure could compromise correct control unit operation.

**Note:** the control unit firmware update procedure can also be carried out from the user's own page on the AVECLOUD site (<https://avecloud.ave.it/>), by connecting to the system to be updated. This requires prior user consent.

Once the software package has been loaded, the control unit must be rebooted.

- d. **System update via USB:** The control unit software can also be updated using an OTG cable connected to the micro-USB 2.0 port on the left side of the control unit.

**The procedure is available only if the “ENABLE IMMEDIATE INFORMATION” setting is active (see General control unit parameters).**

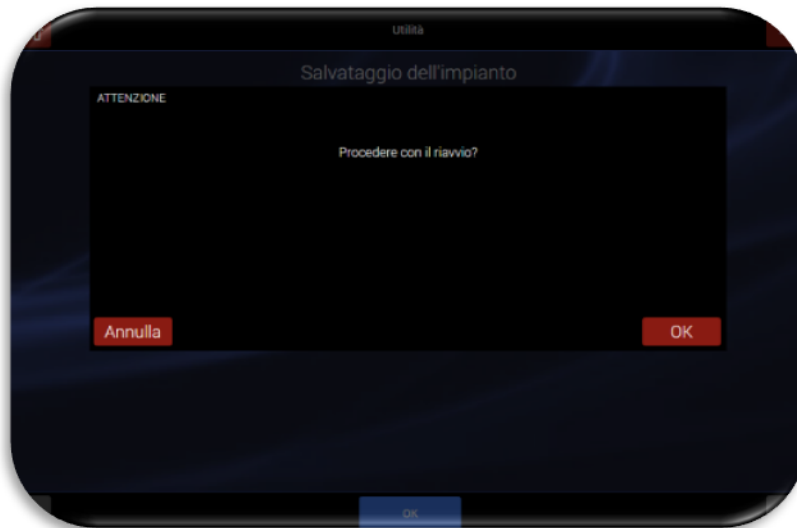
**Note:** this procedure should only be used in exceptional cases (for further details, contact the AVE technical support service).



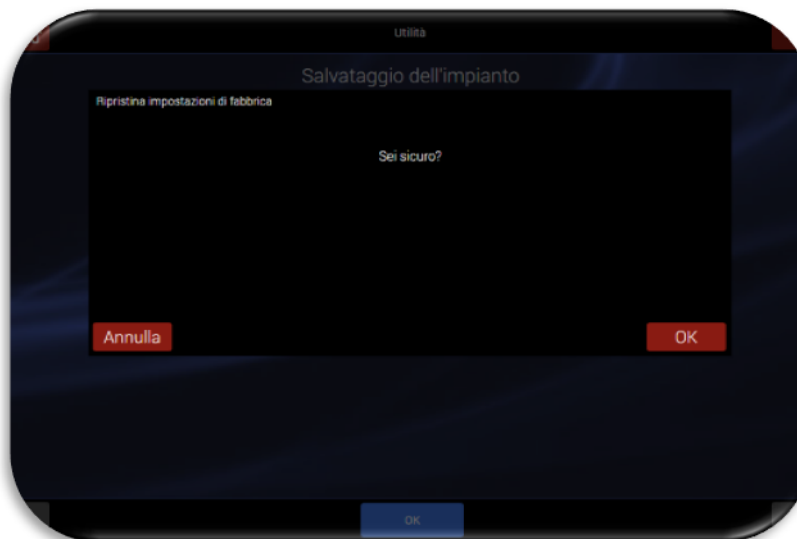
To update the control unit, use the procedure described at point c.

- e. **Rebooting the system:** this makes it possible to restart the control unit. To perform the operation, the Pop-Up message must be confirmed.

**The procedure is available only if the “ENABLE IMMEDIATE INFORMATION” setting is active (see General control unit parameters).**



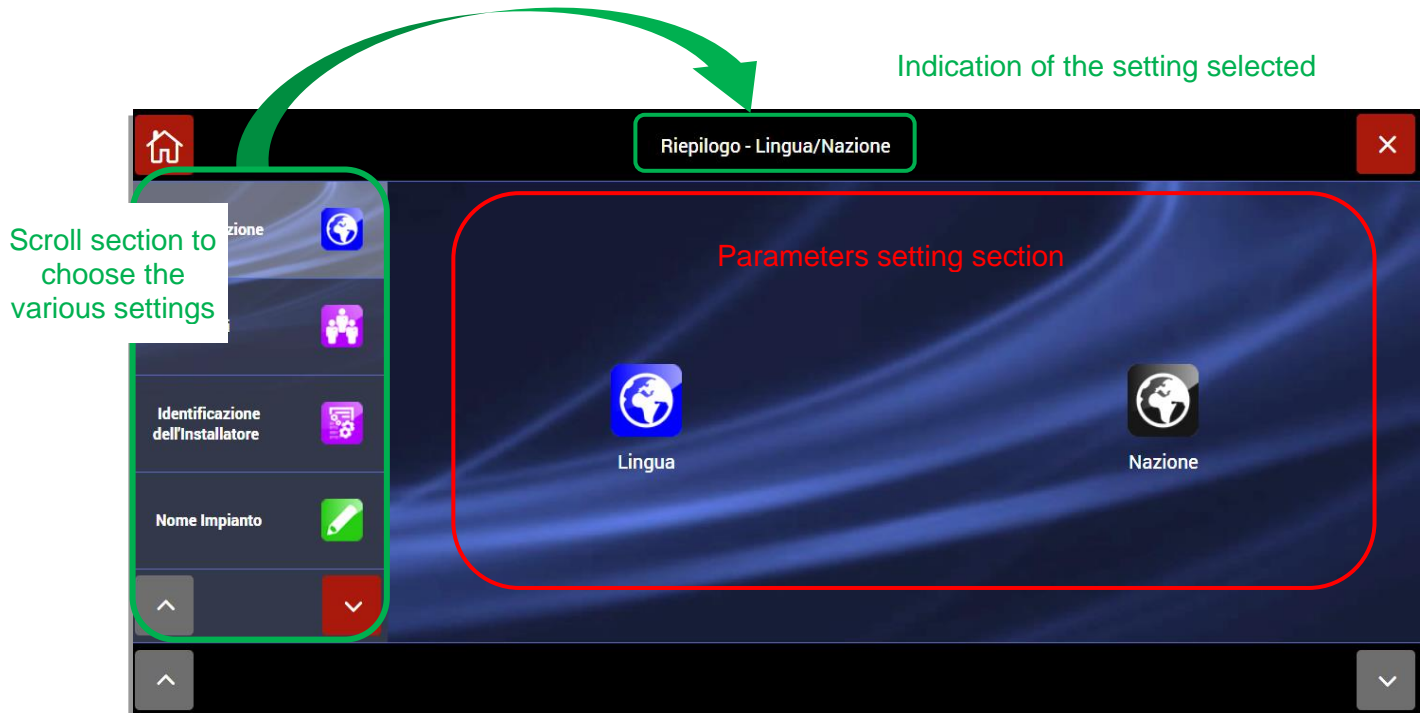
- f. **Restore Default Settings:** This makes it possible to return the control unit to its default, factory settings. To perform the operation, the Pop-Up message must be confirmed.



**Note:** if this is confirmed by pressing OK, all control unit data will be deleted.  
**When rebooted, the control unit will once again display the initial programming wizard.**

## Programming summary

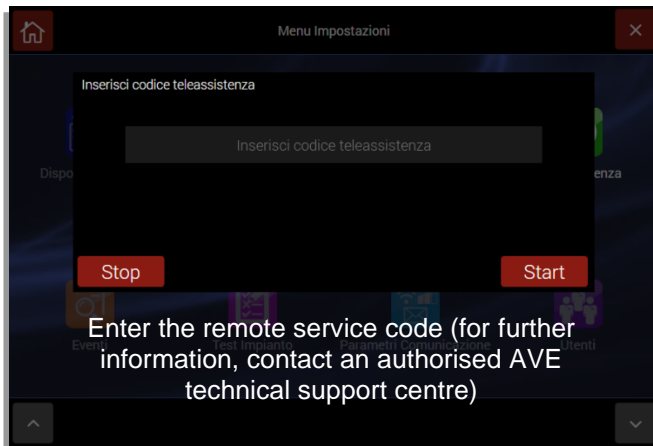
The programming summary makes it possible to access the wizard menu which, in turn, enables management of all control unit programming parameters: scroll through the menus in the left-hand column to select the desired one (ex. language/country); the box will be “greyed out” and the page for the setting of each parameter appears in the right-hand panel.



To manage the various parameters, see the section on each ICON/function.

## REMOTE SERVICE

The remote service is available only for the AVE internal support office and for authorised AVE S.p.A. Technical Support Centres.



## EVENTS

Pressing “EVENTS” calls up the control unit events log.

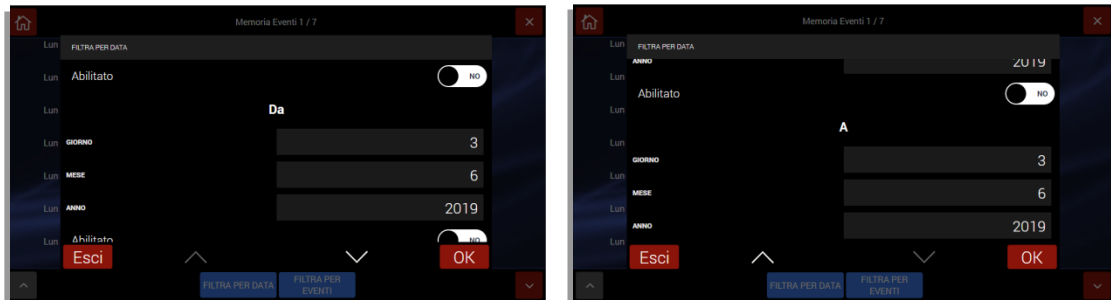


For each event, the following are indicated:

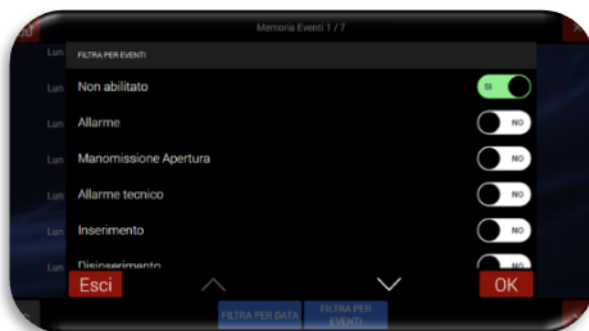
- Date/Time
- Description – The colour identifies the type of event (e.g. red=alarm, green=deactivation)
- User/device that generated the event.

It is also possible to filter events by

- Date - by pressing the “FILTER BY DATE” button



- By event type - by pressing the “FILTER BY EVENTS” button.

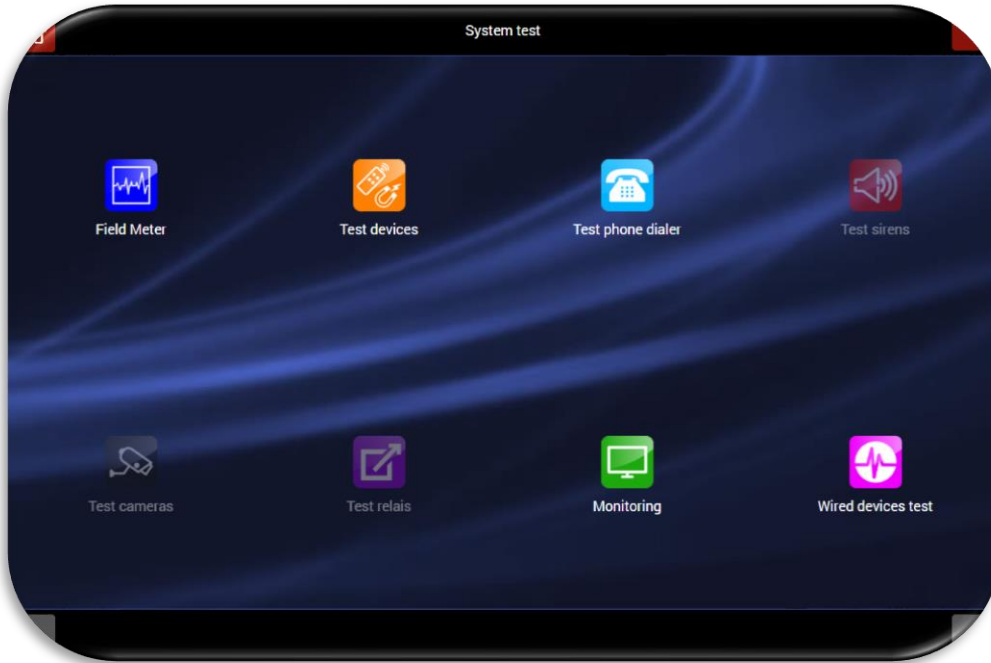


The control unit event log can also be exported by pressing the “DOWNLOAD EVENTS” button. The control unit exports a .csv file proposing the destination file.

To exit, press the “X” key or the “Home page” key.

## SYSTEM TEST

Press "SYSTEM TEST" to call up the screen from which to select the desired test function.



**FIELD METER:** this is used to assess correct control unit reception of the detector radio signal and to check whether the transmission bands are disturbed by external agents.



**DEVICE TEST:** this is used to run the detector function tests, both alarm and tamper detection.



**DIALLER TEST:** this is used to run the test, checking that telephone dialler installed on the control unit actually sends the SMS and/or voice messages.



**SIREN TEST:** this is used to test the acoustic alarm and/or voice messages programmed on the radio siren.



**IMAGE TEST:** this is used to test the image frames.



**RELAY TEST:** this is used to test any radio relays configured on the control unit (products to be added to the catalogue in the future).



**MONITORING:** this provides a complete picture of overall control unit parameters and is used to run detailed tests (these tests should only be performed in the presence the installer).



**WIRED TEST:** this is used to test of the devices connected both to the wired inputs board inside the control unit and to all inputs connected to the AFEX6I-REN boards hooked up to the external wired bus.



Select the desired test function:

### Field meter - Radio range

This displays any radio interference affecting the indicated band, while transmissions issued by the system units appear as a value saved for a few seconds on one of the available channels. If background noise is detected on all 4 radio channels, it means that the band is subject to such local disturbance that correct operation is not possible.



### Radio range - preventive check

The control unit communicates via two-way radio with “wireless” peripherals and such communication is secure and extensive enough to enable installation of a system in a large villa (300-400sqm) or comparable building. However, the radio range is subject to limitations due to the presence of various physical obstacles (thick walls, metal doors, metal shelves, etc.); therefore it is advisable to run a correct radio communication TEST before fixing the devices. In particularly difficult environments, any problems of radio range can be resolved by installing repeaters (code AFTRA03) at the midpoint between the two elements that do not communicate.

### Device test

Device radio range is normally more than adequate for operation in sites similar to a large villa. As outlined in EN50131, the test is run by reducing sensitivity which causes an alarm or signal. Remote controls, keypads and TAGs are always bypassed; testing of these is linked to normal use.

**Note:** When testing magnetic contacts (AF915R-DB), remember that these devices require saving the operating side of the magnet beforehand; this is defined when the magnet is brought close to the body of the sensor for at least 5 seconds. This operation must be performed before the test, which would otherwise yield no results.

The initial test screen is shown below:

Test the desired detectors: as they are tested, the name of the detector is listed with a description of the function being tested (ex. alarm, shock, tampering).

Note: If the control unit is set with the “ENABLE IMMEDIATE INFORMATION” function disabled, generating a tamper detection signal automatically causes the unit to exit the TEST.



When the test has been completed, press OK. This calls up the following screen:



**Note:** The devices that have been tested are indicated in green and the type of test performed (ex. alarm, alarm + tampering) is described to the side. Press OK to exit the device test.

## Dialler tests

The installed diallers and Wi-Fi module can be tested. Select the type of dialler to be tested:

Example 1: TEST of the GSM Module. To test the sending of SMS messages, press “SMS Test”.

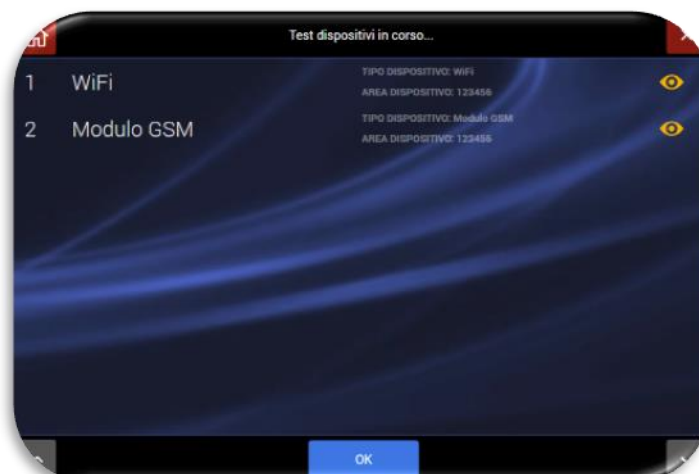


**Note:** only functions highlighted in white can be tested. The functions that are greyed out are not enabled (contact your installer to enable the functions).

Enter the telephone number to which the test message is to be sent and press OK. The control unit confirms sending with the “SEND SMS” message:

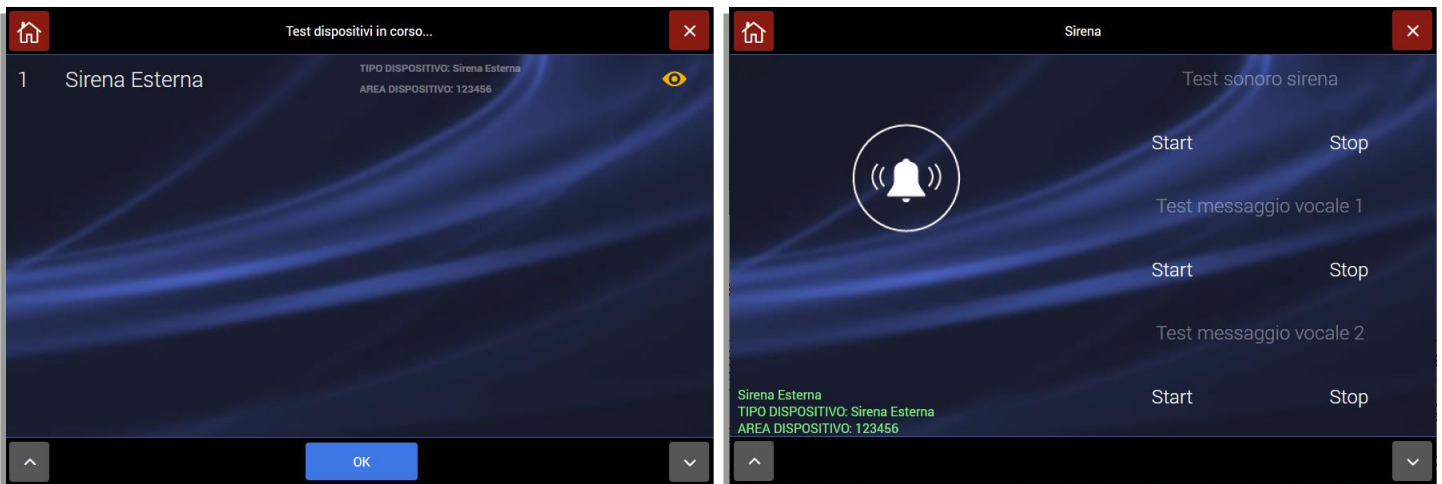


Proceed in the same way for voice messages.




## Siren test

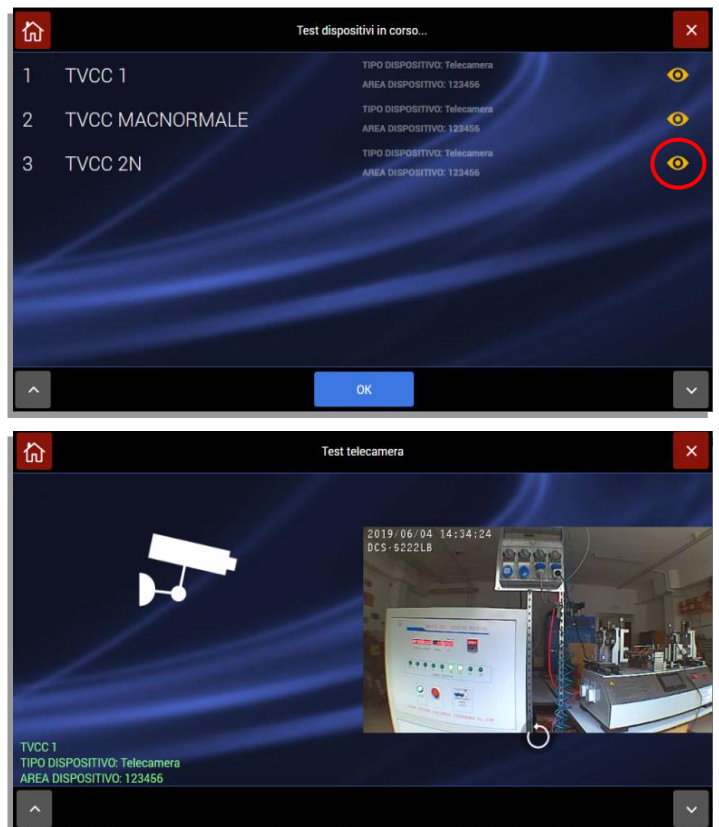
This is used to test the acoustic and/or voice messages programmed on the radio siren. Press the desired siren and run the acoustic and/or voice message test.



## Image test

It is possible to run a test showing which images will be sent by the IP camera/detector with camera if an alarm occurs and/or upon consultation by the user.

Press on the symbol  next to the camera to be tested: this calls up the image of the device:

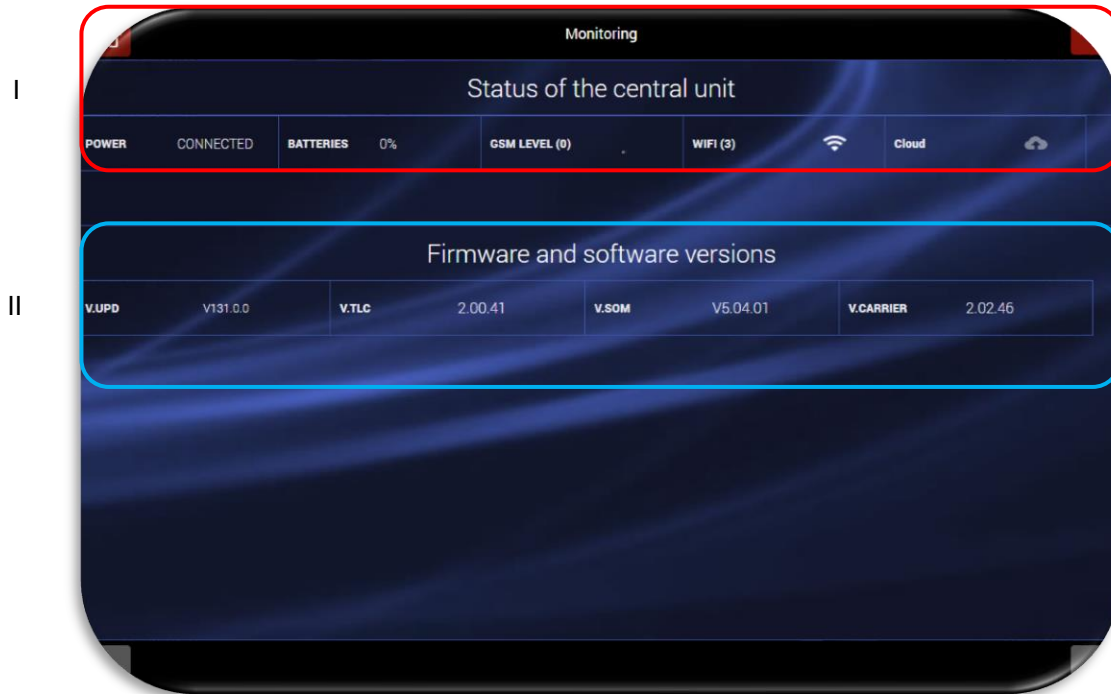


## Relay test

This is used to test any radio relays configured on the control unit (products to be added to the catalogue in the future).

## Monitoring

This provides a complete overview of all control unit parameters.



I. **CONTROL UNIT STATUS.** the following can be verified:

- POWER SUPPLY: mains voltage present/absent
- BATTERY: % battery charge
- GSM LEVEL: level of the GSM signal
- Wi-Fi: level of the Wi-Fi signal
- CLOUD: cloud connection status and check to determine whether the connection is via data network or 4G GSM module

II. **FIRMWARE AND SOFTWARE VERSIONS.** Meaning of the various terms present:

- V.UPD: version of the software package including the control unit
- V.SOM: version of the control unit SOM (System On Module) firmware
- V.WEB: version of the firmware for the WEB graphical interface (GUI)
- V. Carrier: software version for the low level firmware module

## Wired inputs

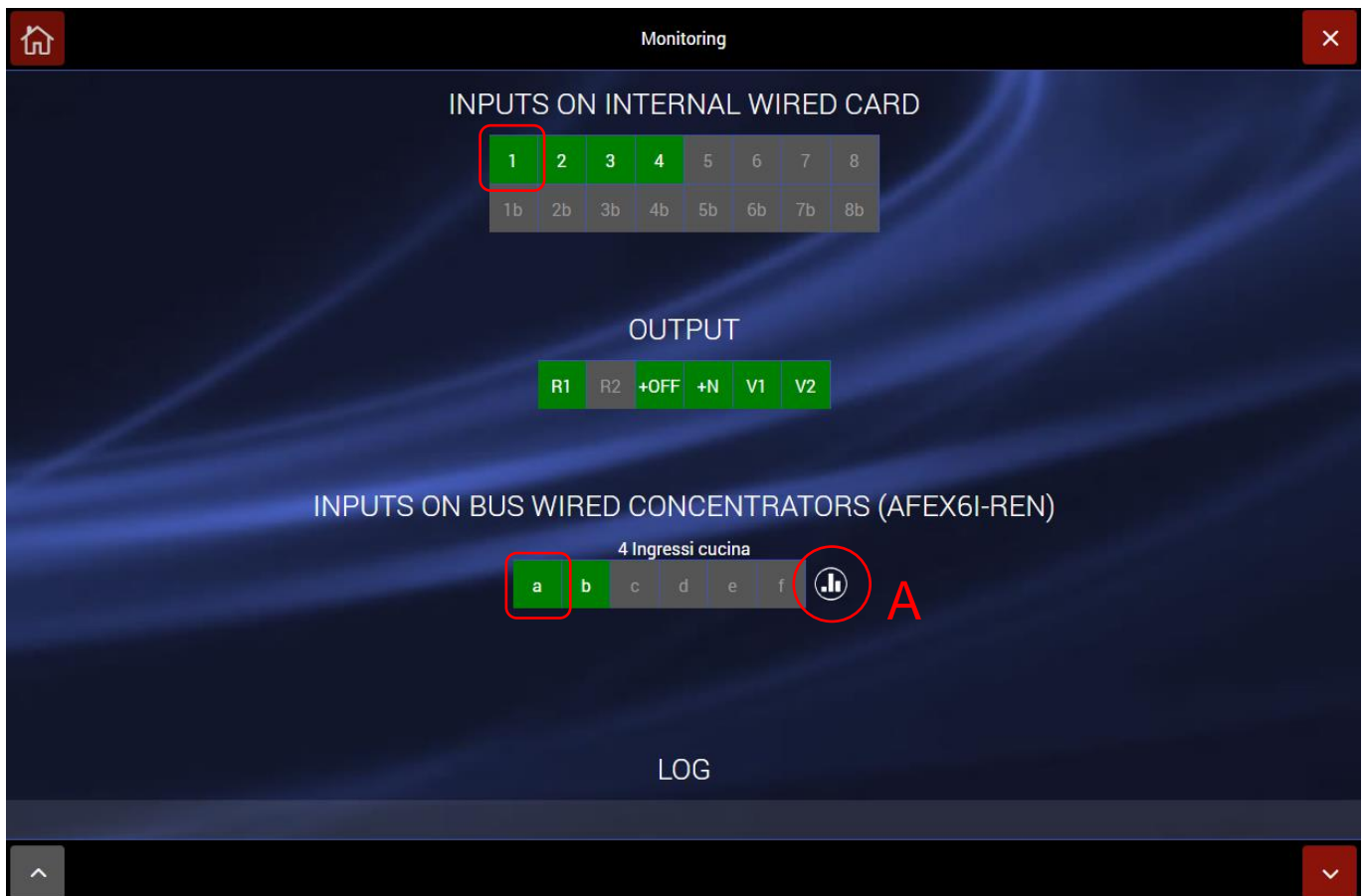
This makes it possible to test all wired inputs of the control unit connected to the internal wired board, the external concentrator boards AFEX6I-REN and the radio devices connected to the wired bus via the radio interface board AF909RR (the latter used by previous AVE wired/radio and radio control units: e.g. AF926, AF926PLUS, AF949PLUS, AF999PLUS).

When each of the inputs is thrown out of balance, the input box changes colour, thus indicating correct operation.

Pressing on the box for each input displays the name associated with that input.

Throwing a **radio sensor** out of balance causes a sensor alarm to occur; the alarm status remains in force until the button on the pertinent box is pressed, thus returning the sensor to the “resting condition”.

Pressing the circular icon (A) activates a one-way communication towards the AFEX6I-REN input concentrator board, thus causing the red LED on the board to start flashing: this makes it easy to find the position of the board within the system.



**INPUTS AND OUTPUTS ON INTERNAL WIRED BOARD:** this displays the status of the wired inputs and outputs on the wired board inside the control unit in real time.

The meaning of the terms are as follows:




**Inputs:**

1 2 3 4 5 6 7 8 → Wired inputs from 1 to 8  
1b 2b 3b 4b 5b 6b 7b 8b → Wired inputs from 1b to 8b: inputs with “NC DOUBLE” function (if active), see SETTINGS - DEVICE PROGRAMMING - WIRED BOARD

**Outputs:**

R1 R2 +OFF +N V1 V2 R1 Relays 1  
R2 Relays 2  
+ OFF Positive when system is activated (system status)  
+N Output for outdoor siren control (control when there is no positive)  
V1 Not used  
V2 Not used

The colours of the inputs and outputs have the following meaning:

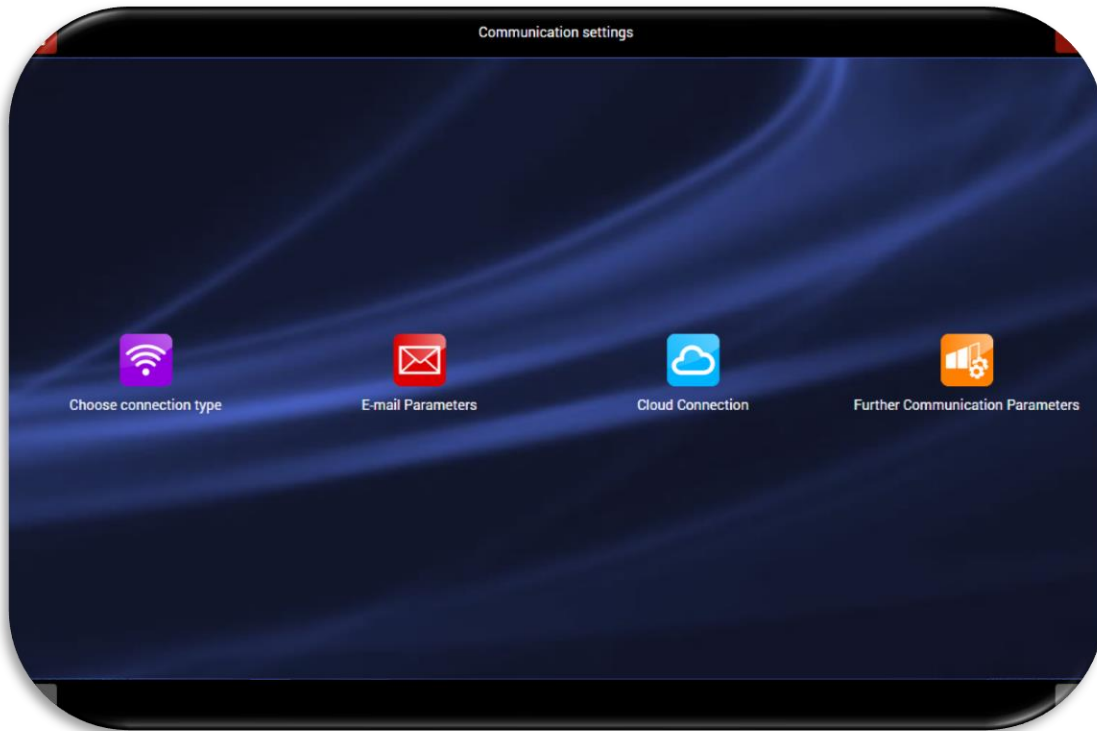
-  Input/output not enabled
-  Input/output at rest
-  Input/output activated

**INPUTS ON WIRED CONCENTRATOR BUS (AFEX6I-REN):** this displays the inputs on the AFEX6I-REN wired concentrator boards in real time.

**LOG:** summarises all events occurring on the control unit. The following are indicated for each event: time, device name, type of event.

## COMMUNICATION PARAMETERS

This function is used to define the parameters for control unit connection mode.



The four icons shown have the following meanings:



Makes it possible to select whether the control unit is to operate in ACCESS POINT or CLIENT mode.



Makes it possible to specify the parameters for the account to be used as control unit sender.



Sets the parameters for connection to AVE CLOUD.



Sets the advanced communication functions, including digital surveillance protocols (ADEM-Contact ID, SIA etc.).

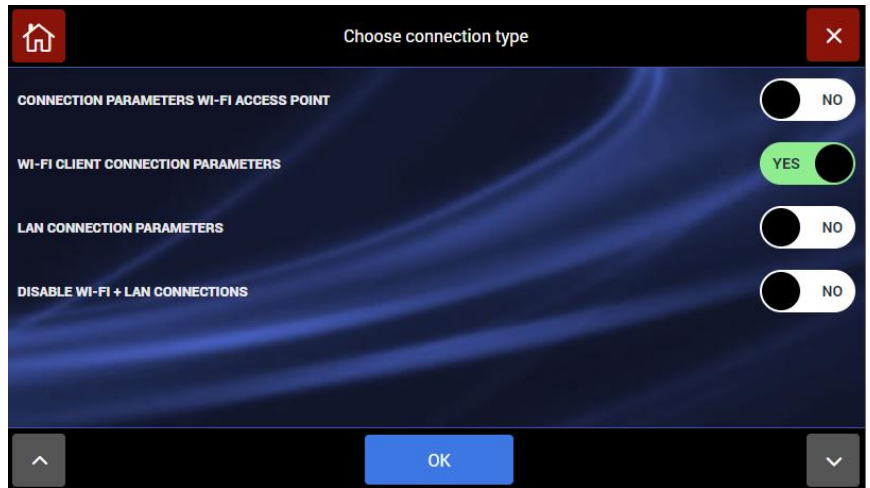
### Choose connection type

The control unit enables three different types of data connection:

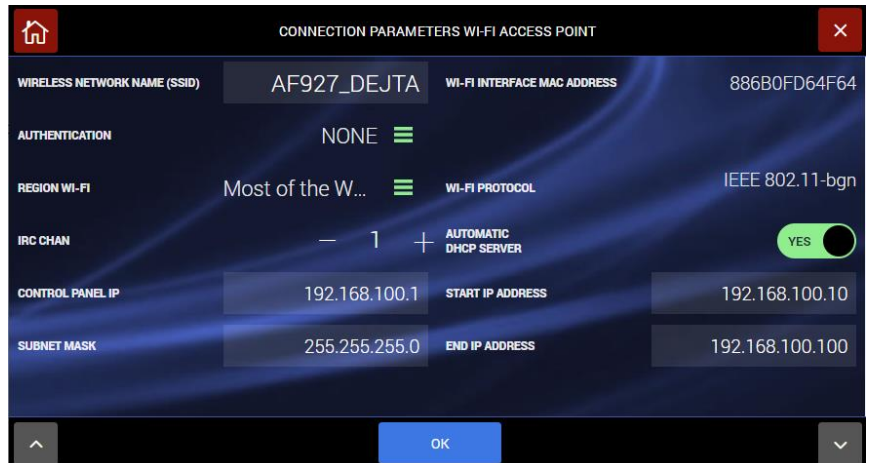
- Wi-Fi ACCESS POINT CONNECTION PARAMETERS
- Wi-Fi CLIENT CONNECTION PARAMETERS
- LAN CONNECTION PARAMETERS
- Wi-Fi DISABLED (the Wi-Fi module can only be switched off for control units with LCD screen art. AF927PLUSTC)

Activating the selected mode calls up a screen used to set the network parameters.

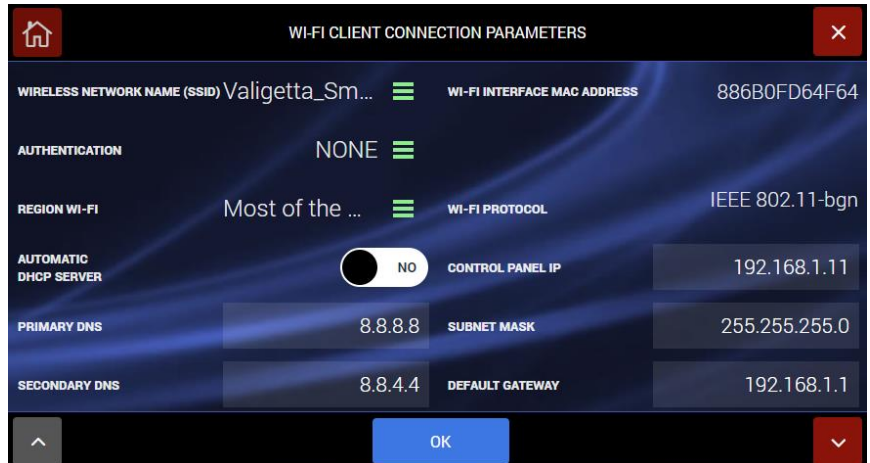
Three examples are given below. Once the desired connection type has been chosen and configuration of the settings completed, confirm by pressing OK.



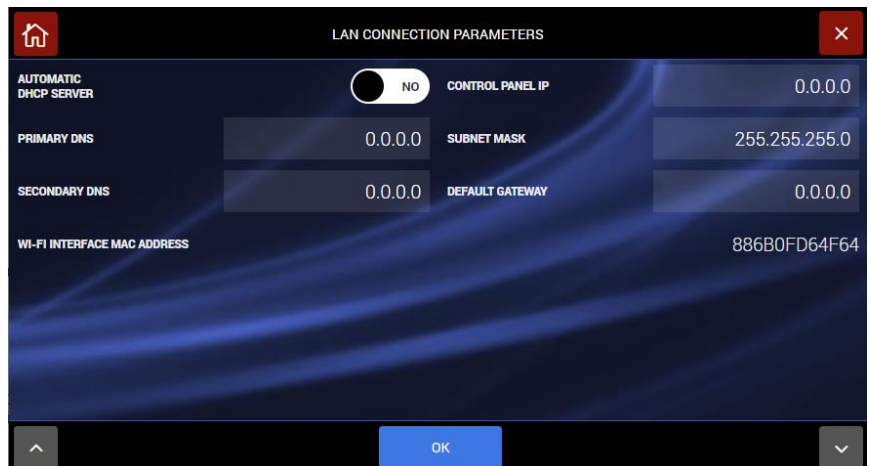
Example of Wi-Fi configuration in **ACCESS POINT** mode



Example of Wi-Fi configuration in **CLIENT** mode



Example of wired **LAN** configuration





The control unit can be connected to the wired LAN using the interface AF927INTFIL (optional). To connect the interface, the cover of the control unit needs to be opened; the interface must be inserted into the mini USB port located on the left side of the control unit; this is done using the special interface connector.

The meaning of the main network parameters to be set are given below:

- **AUTOMATIC DHCP:** enables the router to automatically associate an address with the control unit. It is advisable to use a DHCP address that is set manually thus ensuring that the IP address assigned to the product is always known.
- **CONTROL UNIT IP:** IP address assigned to the control unit;
- **SUBNETMASK:** defines the size (understood as address range) of the IP subnetwork. Typically, in a home network, the parameter is set to 255.255.255.0;
- **DEFAULT GATEWAY=** network gateway address. Typically, in a home network, the address is the address of the network modem/router (ex. 192.168.0.1);
- **PRIMARY DNS** and **SECONDARY DNS** are the DNS used within the network. Typically, in a home network and/or a network which does not have its own DNS, the following values can be used:
  - PRIMARY DNS = 8.8.8.8
  - SECONDARY DNS= 8.8.4.4

Notes on the Wi-Fi connection

- When switching from access point Wi-Fi or when changing the configuration parameters of the Wi-Fi connection, the control unit reboots the Wi-Fi module. Before confirming by pressing OK, it is essential that the parameters have all been set correctly.  
**If incorrect configuration parameters are entered, it may no longer be possible for the control unit to be reached by the WEB browser.**
- **In the AF927PLUS control unit (without LCD touch screen), if the Wi-Fi parameters or the ACCESS POINT to which it is connected are set incorrectly, the control unit cannot be reached and the ACCESS POINT mode will have to be rebooted as follows:**
  - Completely switch off the control unit by unplugging it from the mains power supply and removing the batteries.
  - Restart the control unit with a single charged battery (code AF911).
  - Wait for the control unit to reboot. For the first 5 minutes, the control unit will start up using the default parameters:
    - At initial start-up, the control unit is in ACCESS POINT mode: it generates a Wi-Fi network whose SSID is encoded with the name HS3\_XXXXX, for example: HS3\_C6HAB
    - **IP address: 192.168.100.1**
    - No password is required to access the HS3\_XXXXX network
  - Go to the Wi-Fi settings menu and enter the correct parameters. Confirm by pressing OK. Note: After 5 minutes, the control unit will restore the last WEB settings saved
  - Continue by reconnecting to the control unit using the settings entered
  - Proceed with programming.

#### **Warning!**

- **Connection security:** security is guaranteed by WPA/WPA2/WEP-type passwords, which must be programmed and/or enabled where necessary, as well as by the SSL communication protocol.
- **Wi-Fi range:** this must be checked beforehand to prevent connection interruptions. If necessary, commercially available Wi-Fi repeaters can be used; installation of a UPS is recommended to ensure that the Wi-Fi network will function in case of a power blackout.

## Mail

Makes it possible to specify the parameters for the account to be used as control unit sender.



This page enables the control unit to send e-mails with attachments (frames). An e-mail account can be created specifically for the control unit or an existing user account may be used. The data to be entered are those for the account used. For example, for Google Gmail this will be:

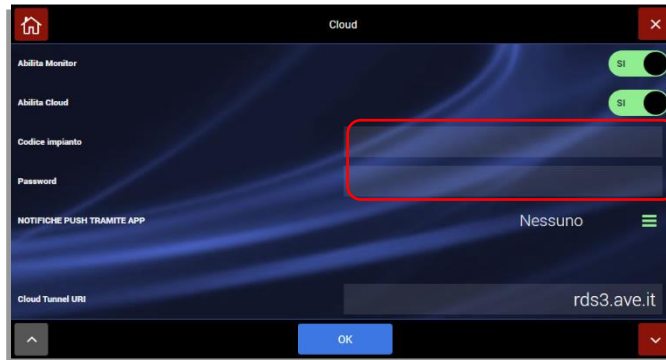
- IP SMTP: smtp.gmail.com
- Port: SMTP 587
- SSL/TLS: enable encryption
- USER: xxxxxx@gmail.com
- PASSWORD: that of the account
- FROM: xxxxxx@gmail.com

It takes just a few sections for Wi-Fi transmission of e-mails if the control unit is Client with WEB connection; if there is no WEB connection, e-mails are transmitted via GPRS.

## AVE Cloud

To connect the control unit to the “AVE CLOUD” remoting system, the parameters received when the system was registered on the [i](#) website. These parameters are:

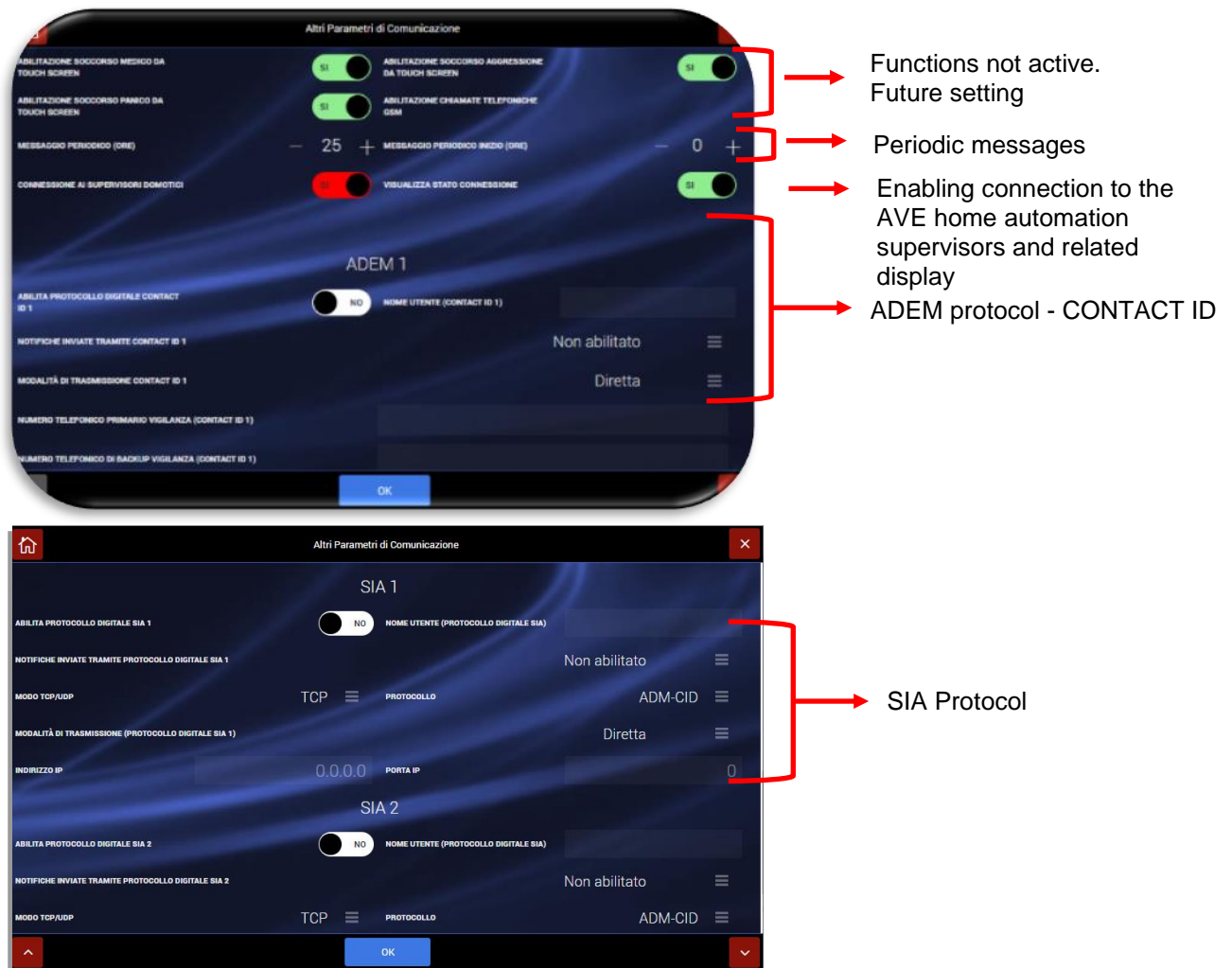
- System code
- Password



After setting the parameters, confirm by pressing OK.

**If incorrect configuration parameters are entered, it may no longer be possible for the control unit to be reached by the AVE CLOUD service and its APP.**

Other communication parameters and interfacing with AVE home automation system



- **Rescue requests:** enable the control unit to send requests for medical, panic and aggression rescue. Functions currently not active (future setting).
- **Connection to home automation supervisors:** the default option is disabled. If activated, it makes it

possible to interface the control unit with the AVE home automation supervisors (this function does not comply with EN50131 regulations).

**Note: to complete interfacing, a “NODE” call number must be entered on each detector** and this must uniquely identify the specific detector in the Home automation supervisor database. For further details see section “Parameters common” on page 38.

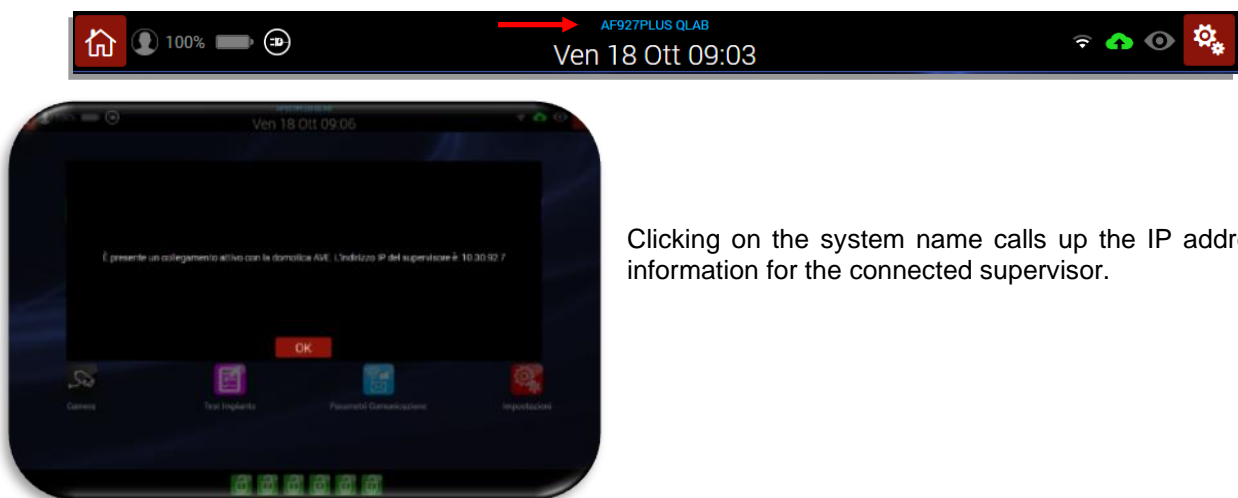
Interfacing with the DOMINA SMART IoT burglar alarm platform (based on AF927PLUS and AF927PLUSTC control units) is supported by the range of DOMINA plus Supervisors: codes 53AB-WBS, TS01, TS03...-V [ARM], TS04X-V and TS05N-V. The minimum version of the software interfacing with each supervisor is given below. In the case of older versions, the devices must be updated.

Product code	53AB-WBS	TS01	TS03...-V [ARM]	TS04X-V	TS05N-V
Software version	01/10/1975	1.0.80	1.10.55A	1.10.55A	1.10.55A

Note: Depending on the device, the version can be consulted in the “Technical” menu or “System Information” menu. Regarding device code TS03...-V, the presence of the letter A in the Software version (e.g. TSLinux 1.10.xxA) indicates that the device hardware architecture supports upgrading to the version of the software compatible with Cloud and IoT services. Devices that are not listed cannot be interfaced with control units AF927PLUS and AF927PLUSTC.

The software update is available from the network of AVE Technical Support Centres at [www.ave.it/it/contatti/rete-centri-assistenza](http://www.ave.it/it/contatti/rete-centri-assistenza).

- **Display connection status:** if the “connection to Home automation supervisors” option is enabled, the “display connection status” function is also automatically enabled. Enabling this function renders the system name field on the home page (see arrow in the example - AF927PLUS QLAB) blue and clickable.



Clicking on the system name calls up the IP address information for the connected supervisor.

- **Periodic message:** the control unit transmits periodic control messages, the period to be programmed in hours. Messages can be Voice and/or SMS messages, to be configured from the USERS menu - SMS Notifications/Voice Messages

**Digital Protocols:** this is to be programmed by enabling and configuring one of the available digital protocols (ADEM Contact-Id; SIA-DCS; ADM-CID) and the relative messages agreed upon with the surveillance control unit; the configuration parameters must be requested from the latter and entered in the appropriate fields, as follows:

“ADEM 1” and “ADEM 2” are related to the Contact ID:

- Enter the user ID assigned to the customer by security;
- Notifications sent: pressing the button calls up the list of events to be enabled for transmission;
- Direct or inverse transmission mode: change only if, during the test, the events transmitted are received inverted from the real situation
- Telephone numbers: enter those of the receiving security.

SIA 1 and SIA 2: as above for operations a); b); c); Transmission Mode (TCP - UDP), Protocol (ADM-CID or SIA-DCS), IP Address and IP Port: request from surveillance.

The SIA protocol is AES encrypted and can be used in TCP or UDP mode. A second IP address (back-up) and a second port can be entered.

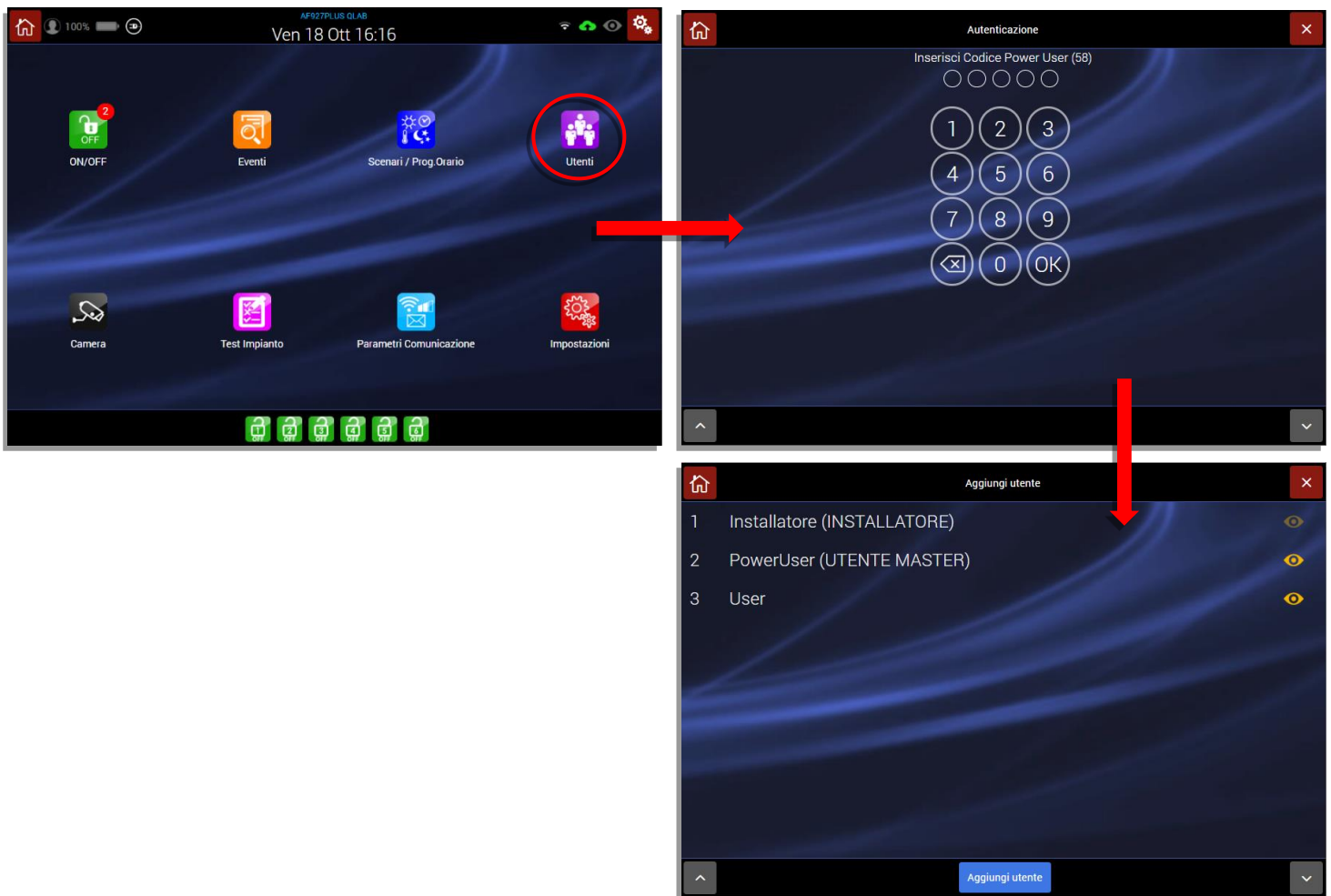
## USERS

The control unit manages two types of users:

- **POWER USER** (MASTER user) with 6-digit PIN: the main user can interact with some control unit parameters. This user always has access to all areas (this parameter cannot be changed). Quick activation zones (function currently not active-future setting) can be assigned; the required data must be entered correctly and this user must be enabled for the various functions: when this is done, the keys to enable the individual functions to be managed will be highlighted. Warning! If any function is not enabled, it will not work even if correctly configured.
- **USER** - other user codes with 6-digit PIN: up to an additional 62 users can be added and, for these, the ability to operate and receive notifications must be configured by the installer and/or Power User by entering the required fields and enabling the relevant functions as indicated above. In particular, each individual User can be enabled to operate only on certain zones, to be selected in the field that appears when the numbers 123456 are pressed.

To manage users, proceed as follows:

1. Press the "USERS" icon, enter the Power USER (MASTER USER) code and select the user to be edited.



- This calls up two screens that are similar but which contain different parameters depending on the type of user (POWER USER or USER) selected:

## POWER USER

## USER

For each user the following can be set:

- **TOTAL ACTIVATION:** areas that will be totally activated (for POWER USER, this cannot be modified);
- **TOTAL DEACTIVATION:** areas that will be deactivated (for POWER USER, this cannot be modified);
- **PARTIAL ACTIVATION** (future setting - not active);
- **USER ENABLED:** all functions associated with the user can be disabled (for POWER USER, this cannot be modified);
- **CURRENT PIN:** 6-digit user code;
- **Phone:** user's telephone number;
- **ENABLE DIRECT ACCESS VIA THE CONTROL UNIT:** this enables the user to manage the control unit in two-way mode using SMS and/or voice calls;
- **SMS NOTIFICATIONS:** a special POP UP makes it possible to select the SMS to be sent to the user;
- **VOICE MESSAGE NOTIFICATIONS:** a special POP UP makes it possible to select the voice messages to be sent to the user;
- **ENABLE E-MAIL MANAGEMENT:** makes it possible to send information on control unit events by e-mail;
- **E-MAIL:** user's e-mail address;

## CODE RECOVERY PROCEDURE

**Note:** if the user and installer codes are lost, after rebooting the control unit (disconnecting the mains power supply and battery and then reconnecting them again), it is possible to enter both menus (user and installer) using the temporary code 00000 (valid for about 3 minutes from moment the control unit is powered up). **ATTENTION:** the first operation to be performed is to call up the control unit's activation/deactivation menu and run complete control unit deactivation (i.e. of all the areas) using code 00000 to accept any anomalies present on the control unit. If this is not done, it will not be possible to enter any of the other menus.

## WIRED BOARD

This supplementary board enables wired connection of detectors and sirens as well as other devices that use the two available programmable relays, which are configured in the control unit and can be used to repeat signals from the control unit or for selected home automation commands. The inputs and outputs are configured by enabling and completing the various options proposed on the screen. Possible connections:

- 8 configurable single- or double-balanced inputs, balanced pulse counter, NC DOUBLE (compliant with EN 50131 grade 2) or NC, NO and NC signal input counter (not compliant with EN50131).
- 1 In Key input (double balanced): this makes it possible to activate/deactivate the control unit with a programmable impulsive or bistable contact.
- 2 tamper alarm inputs, to be used only if alarm inputs are configured as NC (not compliant with standard).
- 1 balanced tamper alarm input that is always active as back-up for connection of a self-powered siren.
- 1 balanced fault input.
- 2 relay outputs (1 and 2): the home automation devices display the status of each relay by a green plug-socket indicating that it is dormant; this turns red when active.

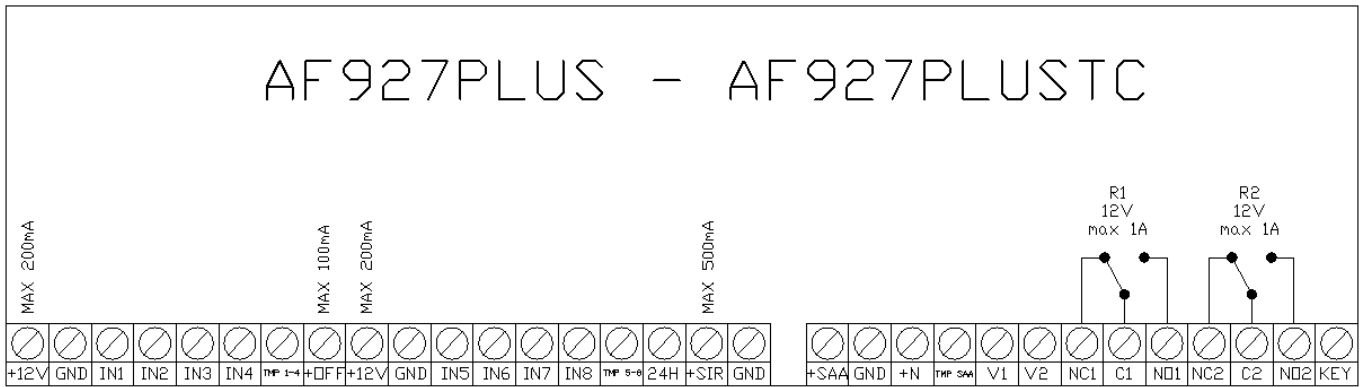
**Warning!** Connection of appliances via cable must take into account their current power consumption — which must enable normal operation when powered from the mains — as well as the autonomy required by EN 50131 in the event of a power mains failure (see power consumption table at the end).

**Warning!** Normally closed cable inputs (both balanced or non-balanced) start working after being closed at least once for 5 seconds.

Code		AF927PLUSTC				AF927PLUS	
Features of the power supply unit		14.5V – 1.6A (@100-240V – 50/60Hz)					
Rechargeable batteries		2x12V – 2.2Ah					
	Code	AF927PLUSTC				AF927PLUS	
	Power supply condition	230 V OK			Black OUT	230 V OK	Black OUT
	LCD brightness	100%	50%	10%	0%	n/a	n/a
Current consumption in	Control unit	390	300	200	30	150	20
	Wi-Fi module	40	40	40	<del>Wi-Fi</del>	40	<del>Wi-Fi</del>
	Wired board	20	20	20	20	20	20
	GSM (AFGSM04) module	10	10	10	10	10	10
	GSM 4G module	45-80	45-80	45-80	45-80	45-80	45-80
	<b>Total</b>	<b>460 (530)</b>	<b>370 (440)</b>	<b>270 (340)</b>	<b>60 (140)</b>	<b>220 (290)</b>	<b>50 (120)</b>

Unless otherwise indicated, the values are given in mA. In brackets the maximum absorption value with telephone dialler art. AFGSM04-4G.

## DESCRIPTION OF TERMINAL BLOCK



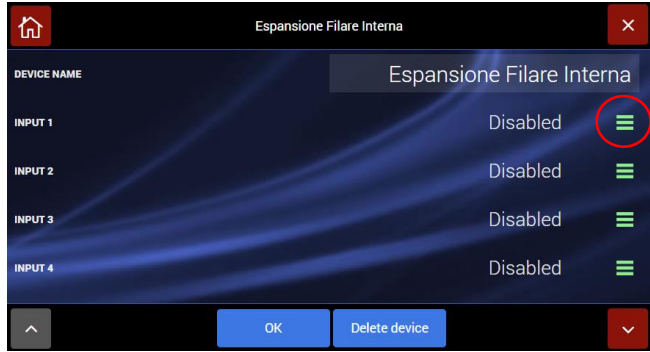
Terminal	Description
<b>+12V</b>	Detector power supply (+12Vdc - max 200mA)
<b>GND</b>	GND
<b>IN1</b>	Alarm input via wire IN1
<b>IN2</b>	Alarm input via wire IN2
<b>IN3</b>	Alarm input via wire IN3
<b>IN4</b>	Alarm input via wire IN4
<b>TMP 1-4</b>	Tamper inputs 1,2,3 and 4
<b>+OFF</b>	System status output (positive when the system is switched off) - max 100 mA
<b>+12V</b>	Detector power supply (+12Vdc - max 200mA)
<b>GND</b>	Gnd
<b>IN5</b>	Alarm input via wire IN5
<b>IN6</b>	Alarm input via wire IN6
<b>IN7</b>	Alarm input via wire IN7
<b>IN8</b>	Alarm input via wire IN8
<b>TMP 5-8</b>	Tamper inputs 5,6,7 and 8
<b>24H</b>	Fault input. Balanced input with 22kΩ resistance
<b>+SIR</b>	Indoor auxiliary siren control (12 Vdc - max 500 mA)
<b>+SAA</b>	Outdoor siren power supply (14 Vdc)
<b>GND</b>	Gnd
<b>+N</b>	Output for outdoor siren control (control missing positive)
<b>TMP SAA</b>	Wired siren tamper - Double balanced input with 22 kΩ resistors
<b>V1</b>	Not used
<b>V2</b>	Not used
<b>GND</b>	Gnd
<b>NC1</b>	NC contact relay output 1 (max 1A@12 Vdc)
<b>C1</b>	Shared contact relay output (max 1A@12 Vdc)
<b>NO1</b>	NA contact relay output 1 (max 1A@12 Vdc)
<b>NC2</b>	NC contact relay output 2 (max 1A@12 Vdc)
<b>C2</b>	Shared contact relay output 2 (max 1A@12 Vdc)
<b>NO2</b>	NA contact relay output 2 (max 1A@12 Vdc)
<b>KEY</b>	Input ON OFF (Closed to GND: OFF)




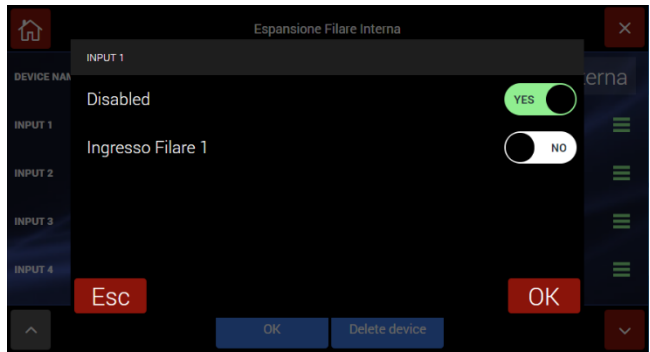
# CONFIGURATION OF INTERNAL WIRED BOARD

The wired board is automatically acquired the first time the control unit is started up. To use the inputs and outputs on the unit, enter the dedicated menu (see "SETTINGS" menu - paragraph Devices and Areas).

This calls up the device screen which presents the wired board along with any other devices:



After selecting the relevant screen, click on the symbol  to enable the various inputs/outputs:



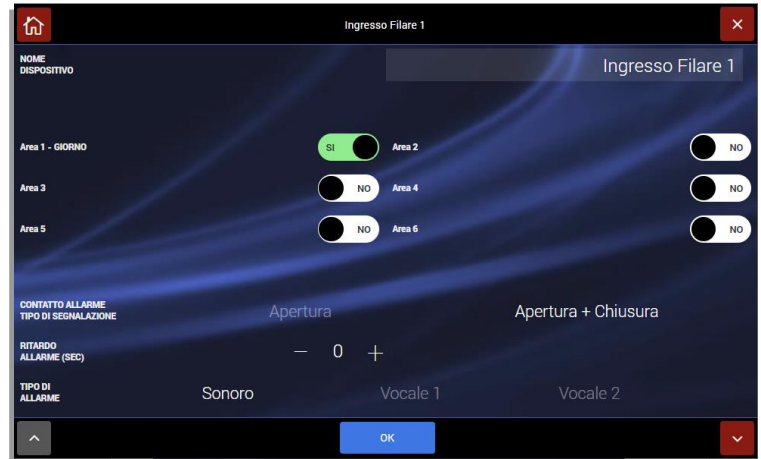
All enabled inputs will appear on the screen



Once activated, the control unit will see the individual inputs/outputs as independent devices on which individual parameters can be set.

## Input configuration

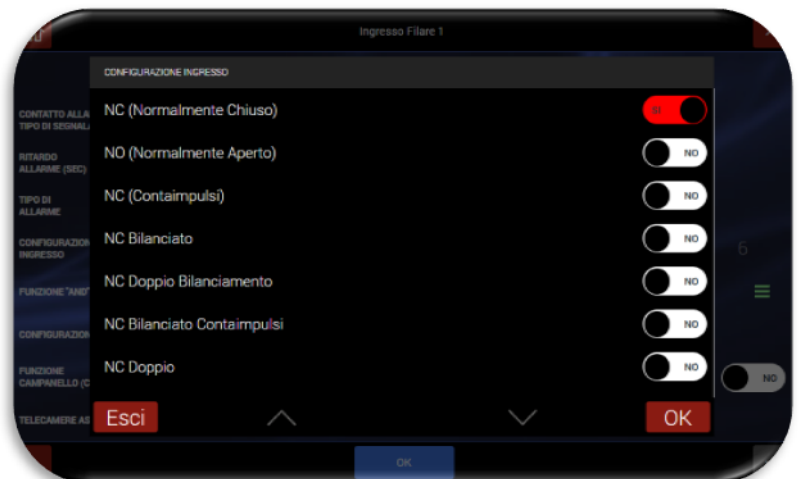
To configure the input, press the “eye” symbol next to the desired input; this calls up the input parameters page.



The following parameters can be set:

- **Device name:** enter the description of the input (ex. “ROOM contact”);
- **Area:** the input is activated by entering the area to which it belongs, which may differ for each type of alarm. For AND or OR operation of the inserted areas, see *Settings-General Settings-Detectors operating on multiple areas*;
- **Alarm contact - Type of signal:** choose whether the detector is to signal only opening or both opening + closing;
- **Alarm delay:** the alarm given by the unit is triggered after the amount of time set for each type of alarm.
- **Type of alarm:** alarms generated by the unit may give rise to an “acoustic alarm” (siren and external communications) or “voice alarm” (pre-recorded voice message broadcast by the sirens and control unit in addition to external communications). Two voice alarms are possible, with different messages.
- **Chime function:** this function is operative if the control unit is deactivated and involves signalling entry into the room protected by this detector. When this function is enabled, at each entry, the control unit emits a brief musical signal for the set amount of time; one or more sirens can be programmed to emit voice message 2, to be recorded for the purpose (welcome or other);
- **Input configuration:** the type of input balance can be configured. Remember, to comply with EN50131, select the following input configuration types:
  - NC BALANCED
  - NC DOUBLE BALANCED
  - NC BALANCED PULSE COUNT
  - NC DOUBLE

For correct connection of balancing resistors, see the following paragraph **WIRING DIAGRAM**.

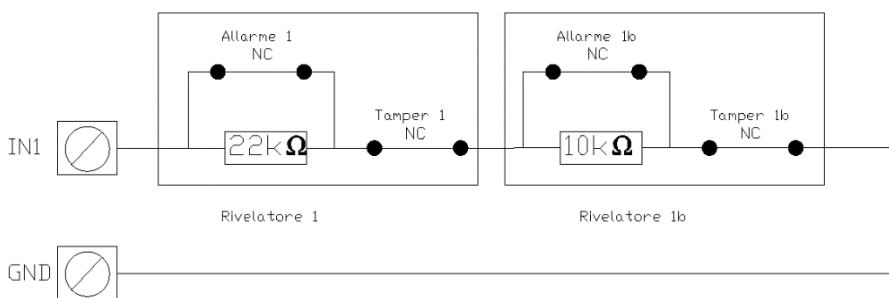


- **Pulse count:** if the type of input configuration chosen includes the use of pulses, the pulses can be adjusted from 1 to 8.

- **Configurations (AND).** With the AND function, the control unit alarm status occurs only if at least two detectors in a given area (1-6) transmit an alarm within an adjustable amount of time (10-180 seconds - by default 30 seconds): in this case the likelihood of a false alarm occurring in environments subject to disturbance (particularly outdoors) is reduced by suitably positioning two detectors to protect the same area. The possibilities for enabling the AND configuration are:
  - AND regarding two detectors: this involves the detector currently being set and another, to be chosen from the list of those already programmed (which can be viewed on the list in the control unit). The alarm signal will only be given if both detectors signal the event.
  - Area-related AND: all detectors in the area are involved. A control unit alarm occurs if at least two detectors enter alarm mode within the programmed amount of time.
- **Warning!** To prevent the degree of system security from being compromised, it is not advisable to program two non-volumetric detectors in AND mode.
- **Camera associated with the control unit:** the detector alarm can trigger the capturing of frames from one or more of the cameras associated at this stage. These images can be transmitted as e-mail attachments depending on the set connections (GPRS-Web).

## NC DOUBLE

Two detectors can be connected using a single terminal following the diagram below:



To enable this function, simply select NC DOUBLE as “connection type” on the terminal to which two detectors are connected. At that point, after confirming the entry, a double entry will appear. For example, taking input 1 as a reference, this would be:

- Wired input 1: identified by 22kΩ resistor
- Wired input 1b: identified by the 10kΩ resistor (the detector label will be yellow)



**Note:** the two inputs are recognised as separate and different areas can be set.

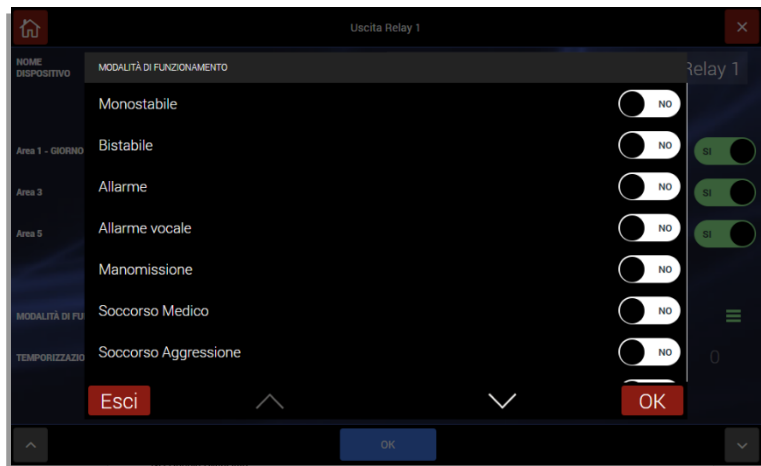
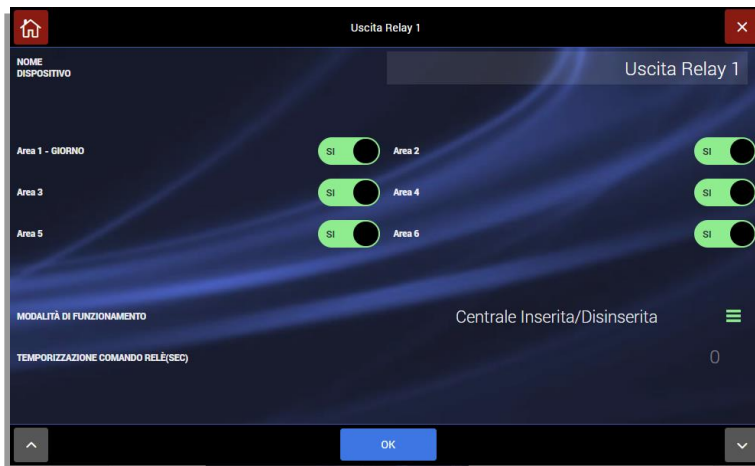
## Warning, Important notes!

- In accordance with EN 50131... connections to any additional sirens, whether self-powered or not, must be protected with a balanced TAMPER line using the alarm inputs.
- The relay outputs must be used within the voltage and current limits shown in the figure.
- Conventional detectors connected directly to the control unit must be certified EN 50131... grade 1 or higher and must operate with line balancing; therefore, the appropriate resistors must be inserted as shown (only 3 wires, of suitable diameter).
- The +OFF signal is positive when the control unit is off and is used to block those detectors/sirens with the appropriate input.
- When used, the fault input causes an ANOMALY signal and issues the related telephone calls.
- All unused inputs can be left unconnected (no need to balance them), unless they are accidentally closed, even temporarily. In this case, the power must be cut off and then turned on again (line reset).

## Output configuration

The following parameters can be set:

- Device name: give the output an explanatory name
- Areas: for some functions (e.g., activation/deactivation of control unit) it is possible to indicate for which control unit areas the function is active.
- Mode of operation: choose the function/event that activates the output.



# KEYPAD

## WIRED KEYPAD AF990

The AF990 keyboard allows you to:

1. View the system status;
2. Completely arm/disarm the system using the user code: enter the user code and wait for the arm/disarm menu to appear. Press the ON/OFF button.
3. Manage the relays on the control unit or the auxiliary relays installed on the wired bus: access the menu and press the device you wish to activate/deactivate (only the relays associated with the function are managed)
4. Partly arm/disarm the system using the user code or RFID tag: enter the user code and wait for the arm/disarm menu to appear;
5. Place the cursor on the "Areas" line and press the ENTER button;
6. Select the areas to be armed by pressing the button with the number corresponding to the desired area;
7. Press the ON button to activate partial arming of the control unit.
8. Consult the control unit event log: press the "events" button to consult the log of the latest activities that occurred on the control unit.

### ASSOCIATION OF THE KEYPAD TO THE CONTROL UNIT:

A maximum of two keypads can be associated with the AF927 control unit.

The AF990 keypad can be used with AF927 range intrusion control units that have Firmware version 167 or later installed.

The keypad can be associated with the control unit automatically or manually.

To associate the keypad with a control unit, you must:

1. Update the control unit's firmware to a compatible version;
2. Turn off the control unit completely by disconnecting the power supply (230VAC) and the batteries;
3. Connect the keypad;
4. Power up the control unit again;
5. Wait for the control unit's initialization procedure with the new firmware version;
6. Proceed with the automatic or manual association procedure

#### MANUAL ASSOCIATION:

7. Connect the affiliation cable to the AF927INTFIL board without connecting anything to the AF990 keyboard;
8. Access the "Settings" menu of the AF927 control unit and enter the installer code;
9. Access the "Devices and areas" menu and then press the "Devices" button;
10. Press the "Add other devices" button and then press the "Add BUS devices" button;
11. Press the "Manual device association" button;
12. Connect the affiliation cable to the AF990 keyboard, wait for it to be affiliated with the AF927 control unit and complete the configuration of the keyboard parameters;
13. Disconnect the affiliation cable from the AF927 control unit and the AF990 keyboard.
14. Connect the keyboard to the wired BUS.

#### AUTOMATIC ASSOCIATION:

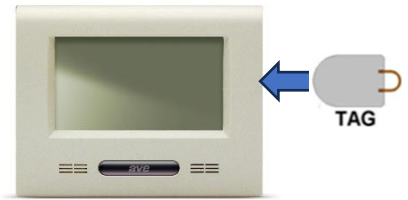
1. Connect the AF990 keypad to the system's wired bus (attention: until the end of the affiliation procedure, the keypad will not display any message).
2. Access the "Settings" menu of the AF927 control unit and enter the installer code;
3. Access the "Devices and areas" menu and then press the "Devices" button;
4. Press the "Add other devices" button;
5. Press the "Add BUS devices" button;
6. Press the "Automatic device association" button;
7. Wait for the keypad to be affiliated with the AF927 control unit and complete the configuration of the keypad parameters;
8. Exit the control unit configuration menu.

Note:

Any firmware updates for the keypad, if necessary, are contained in the firmware update file of the AF927 control unit.

The system arming/disarming procedure is also possible using a transponder key art. AF340-T, positioning it near the RFID reader on the keypad (right side of the keypad).

1. **TOTAL ARMING:** with the system disarmed, bring the transponder key close to the keypad for one second and remove it from the reader;
2. **PARTIAL ARMING:** with the system disarmed, bring the transponder key close to the keypad for approximately 3 seconds until the system is partially armed;
3. **DISARMING:** with the system armed, bring the transponder key close to the keypad until the system is disarmed;



## RADIO KEYPAD AF970R-DB

The AF970R-DB radio keypad allows you to arm, disarm and partially arm the system.

Press any button on the keypad to turn on the LCD.

Use the ▲ (Up) and ▼ (Down) buttons to move between the items in the menus.

To select an area, enter the numbers that represent the area itself (e.g. Area 2 = button 2).

If an incorrect user code is entered three times, all operations will be inhibited for 180 seconds.

1. **TOTAL ARMING:** enter the user code and wait for the arming/disarming menu to appear;  
Press the ON button, making sure that the "TOTAL" item is selected;
2. **PARTIAL ARMING:**  
Enter the user code and wait for the arming/disarming menu to appear;  
Position the cursor on the "Areas" line and press the ENTER button;  
Select the areas to be armed by pressing the button with the number corresponding to the desired area;  
Press the ON button to activate partial arming of the control unit.
3. **DISARMING:** enter the user code and wait for the arming/disarming menu to appear;  
Press the OFF button

The total system arming/disarming procedure is also possible using a transponder key art. AF340-T.

4. **TOTAL ARMING:** with the system disarmed, bring the transponder key close to the keypad for one second and remove it from the reader;
5. **PARTIAL ARMING:** with the system disarmed, bring the transponder key close to the keypad until the partial arming of the system has taken place;
6. **DISARMING:** with the system armed, bring the transponder key close to the keypad for one second and remove it from the reader;

**Note<sub>1</sub>:** When the keypad is turned on, the LCD shows the user interface menu. If the menu is not displayed or the antenna symbol is displayed, the keypad is out of maximum range. Move closer to the control panel and press a button to realign the system.

**Note<sub>2</sub>:** The AF970R-DB radio keypad cannot be associated with an AFTA03 signal repeater.

# INTERFACE WITH THE MODULES OF THE CIVIL SERIES AVE SMART IoT

The control units of the AF927 range can be interfaced with the devices of the connected civil series AVE SMART 44 without having to add additional devices.

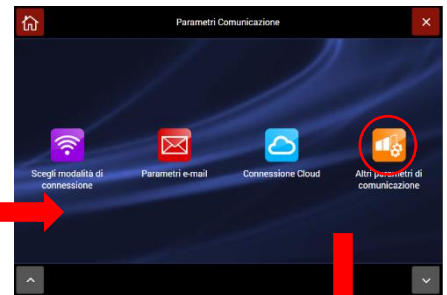
The control units will then be able to respond to a "Scene" command sent by a SMART fruit by carrying out the action associated with it (eg inserting the system) or to send a scene to the devices themselves.



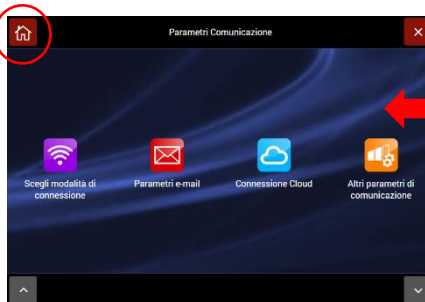
## CONFIGURATION OF THE CONTROL UNIT

The procedure for activating the interface between the systems is as follows:

Press the "Communication Parameters" button, enter the "Installer code" and access the "Other communication parameters" menu.



Then activate the parameter: "Connection to IoT modules", press the "OK" button to confirm the choice and return to the home page by pressing the appropriate button.



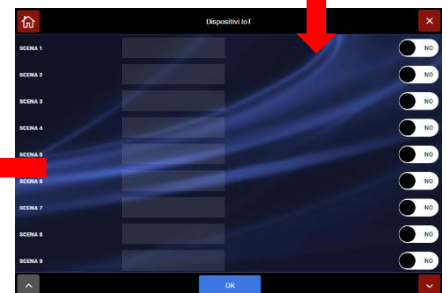
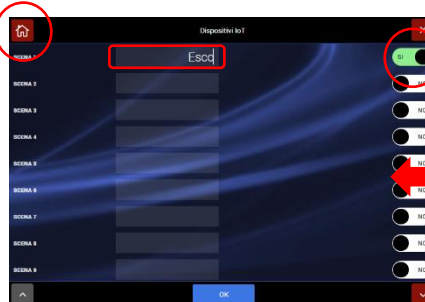
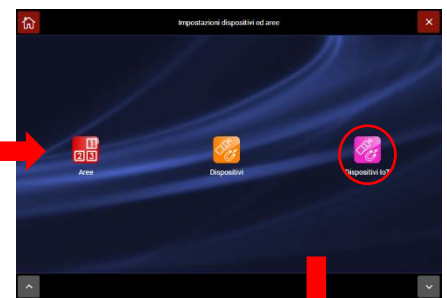
Access the "Settings" menu and then the "IoT devices" menu.

Activate the IoT scene (s) to which the control panel must respond and confirm with the "OK".

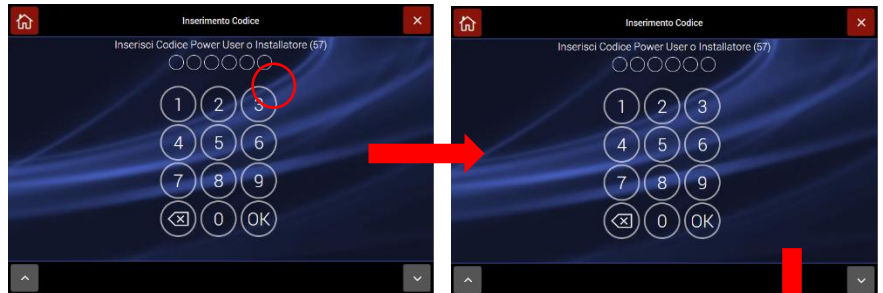
Warning: the control unit can manage a maximum number of 16 scenes.

N.B. : scene configuration is an integral part of the AVE SMART IoT system.

At the end of activating the scenes, press the "Home" button to return to the main page.



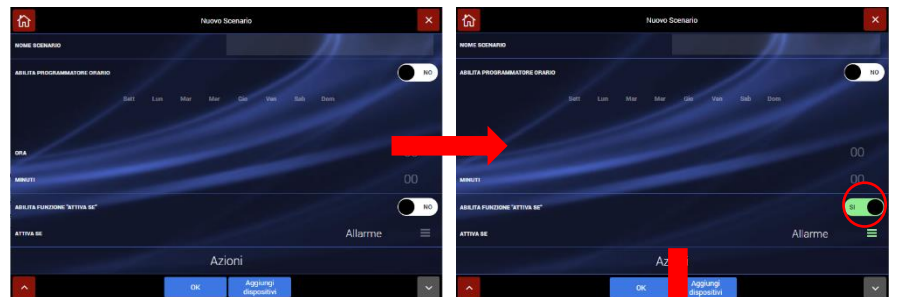
Press the icon that identifies the installer and disconnect.



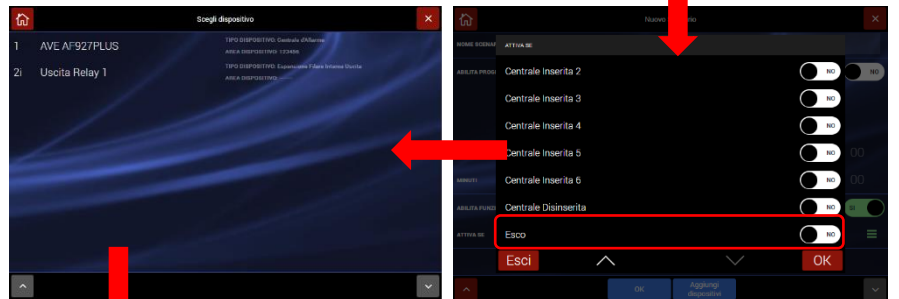
Now access the "Scenarios / Timetable Program" menu, enter the user code, press the button "OK" and then the button "Add scenario".



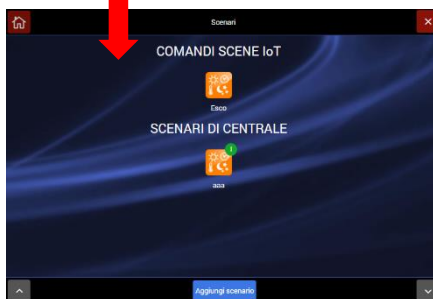
Enter all the data relating to the scenario (refer to the appropriate chapter of this manual). Activate the "Activate if" function and select the scene (s) that have previously been activated.



Confirm by pressing the "OK" button and press the "Add devices" button to set which function the control unit should perform when the selected scene is intercepted. Confirm your choice by pressing the "Add scenario" button and press the "OK" button to confirm.



Repeat the action with other scenarios if necessary or press the button "Home" to return to the home page.



The control panel is now configured to be able to respond to a sent IoT scene or you can send an IoT scene to the system yourself by pressing the appropriate icon.



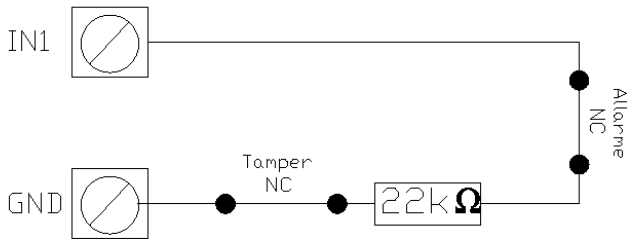


# WIRING DIAGRAM FOR WIRED INPUTS

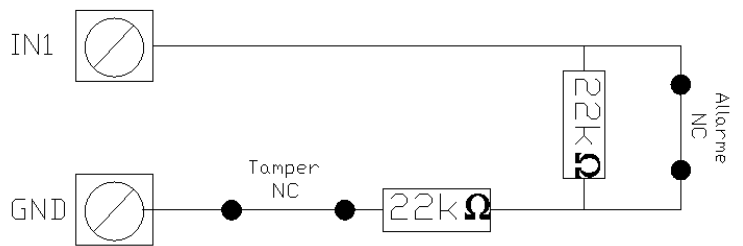
## INPUT CONNECTION TYPES FOR CORRECT BALANCING

The wiring diagrams are given below for the various types of sensor connections accepted:

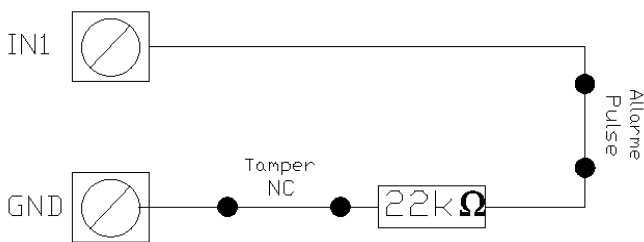
### NC BALANCED



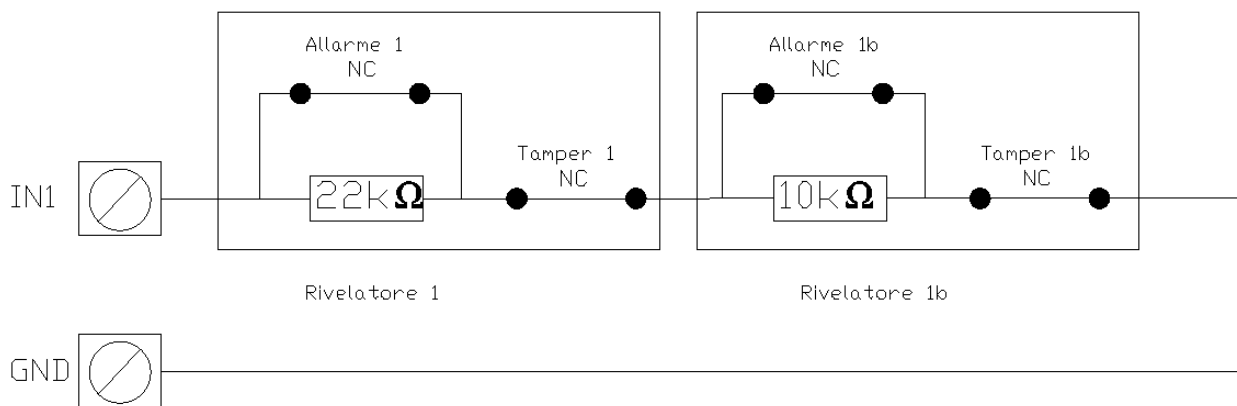
### NC DOUBLE BALANCED



### NC BALANCED PULSE COUNT



### NC DOUBLE

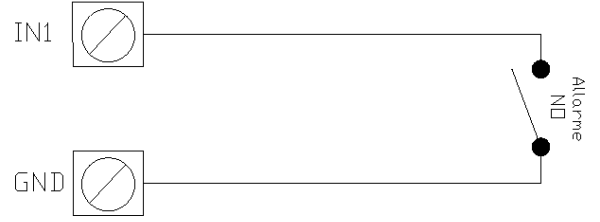
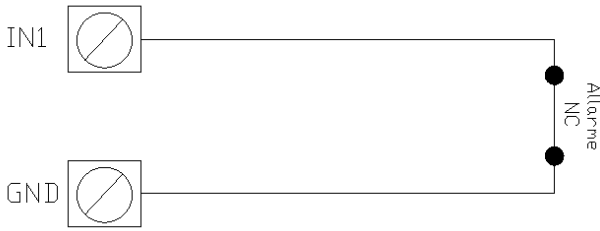


NC – NORMALLY CLOSED

(Connection type not compliant with EN50131)

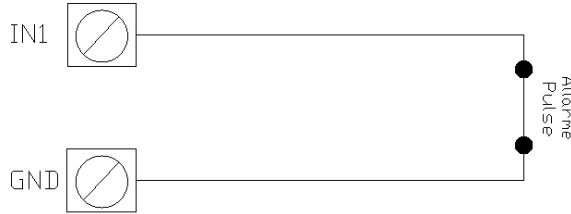
NO – NORMALLY OPEN

(connection type not compliant with EN50131)



NC - PULSE COUNT OPEN

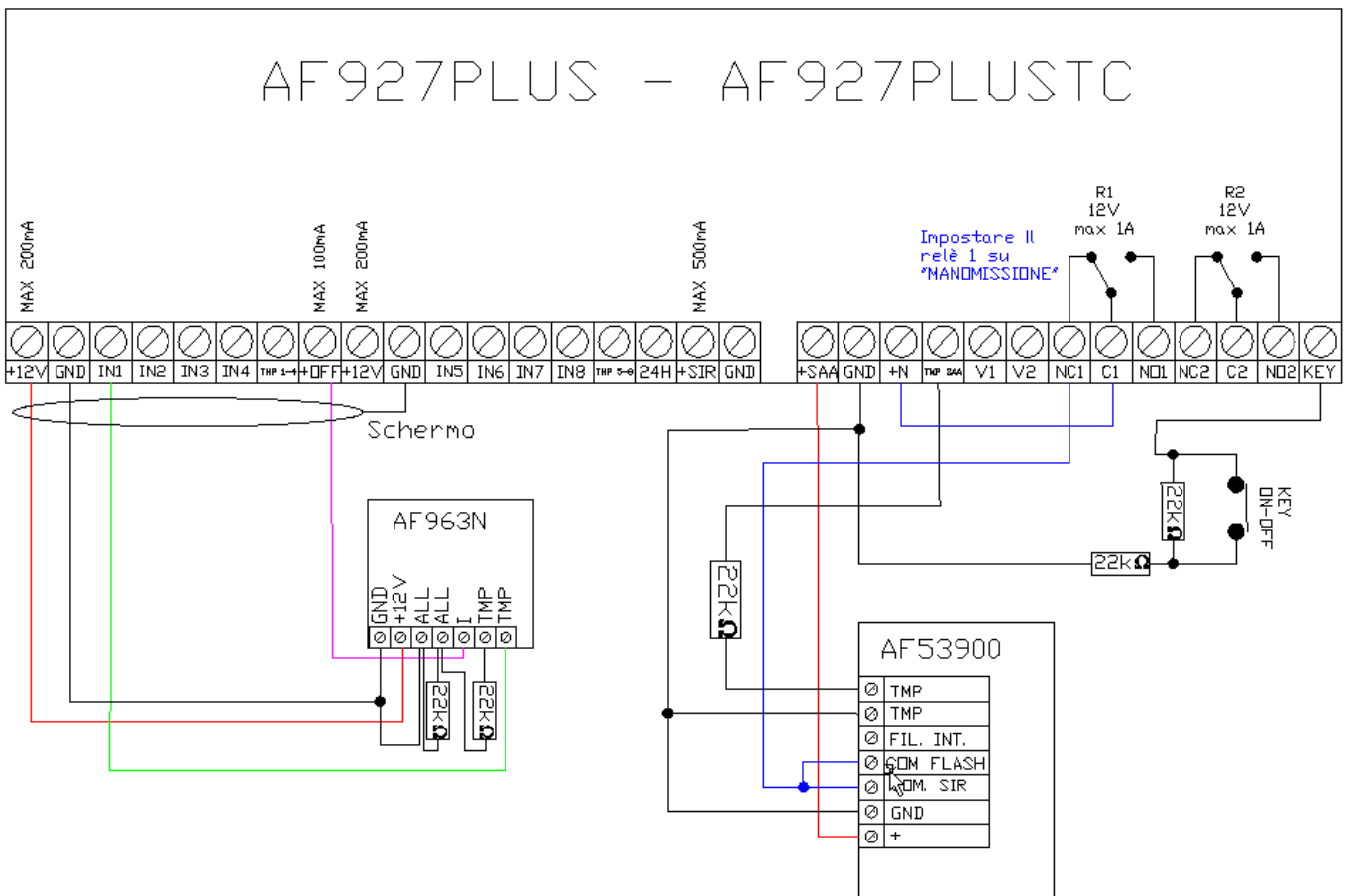
(Connection type not compliant with EN50131)



**NOTE:** use only shielded cables to connect the detectors to the control unit.

The cable shield must be connected to GND from the control unit side only (see EXAMPLE OF CONNECTION).

**EXAMPLE OF CONNECTION**



**NOTE:** use only shielded cables to connect the detectors to the control unit. The cable shield must be connected to GND from the central side only.

## GSM TELEPHONE DIALLER MODULES - art. AFGSM04, GSM 4G - art. AFGSM04-4G

The control unit can handle either a 2G GSM module (art. AFGSM04) or a 4G GSM module (art. AFGSM04-4G).

These devices are dialler modules that operate on the following bands:

2G: 900/1800MHz

3G: B1/B8

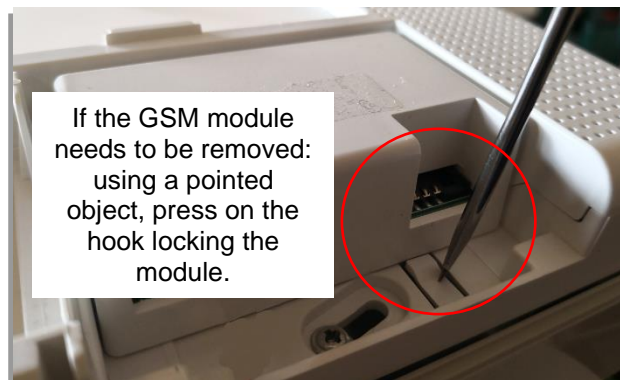
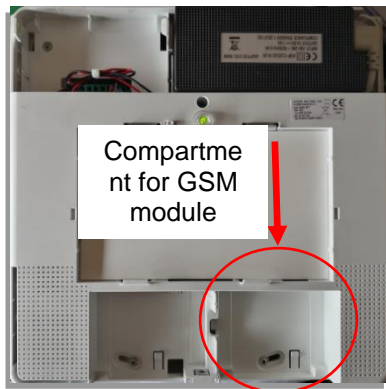
4G: B1/B3/B7/B8/B20/B28A

Before installing, check that the AF927PLUS or AF927PLUSTC control unit is located in a place with adequate 4G signal coverage for the chosen telephone operator.

**WARNING: device must only be installed and the SIM card inserted/withdrawn while the control unit is completely off (no 230Vac power supply and batteries disconnected).**

see the indications given below for proper installation:

The AFGSM04 and AFGSM04-4G must be set inside the control unit, positioned in the special space located at the bottom right-hand side of the device (see image below).



The SIM card used must be a MINI SIM.

For MICRO SIM cards, use a commercially available adapter.

NANO SIM cards cannot be used in the dialler.


Insert the SIM card into any telephone and check that the:

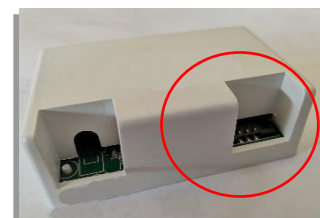
- card is active
- PIN code is disabled
- any messages, address books or telephone operator services are disabled
- make note of the SIM card telephone number to be entered into the control unit parameters

Remove the card from the telephone and insert it (with the control unit completely switched off) into the slot on the AFGSM04 or AFGSM04-4G telephone dialler (see image below).

Install the GSM module inside the control unit.

Power up the control unit and wait a few minutes for 4G telephone network reception.

1. Completely disconnect the control unit (cut off 230Vac mains power supply and remove batteries).
2. Insert the GSM module into the control unit.
3. Access the control unit
4. Call up SETTINGS-DEVICES and AREAS-DEVICES. The GSM module will appear in the list of peripheral devices installed:
5. Press on the symbol  next to the module to edit the GSM module settings:



**Art. AFGSM04:**

- **NAME:** GSM identification label;
- **SIM PIN:** Enter “0000” or leave blank if the SIM does not have a PIN or enter the PIN code. Note: Inserting a SIM without PIN is recommended (see point 1);
- **IMEI:** IMEI (International Mobile Equipment Identity) number of the previously connected AGSM04 module (if any).
- **TELEPHONE OPERATOR:** the system automatically displays the name of the telephone operator;
- **SIM EXPIRY:** used to enter the number of months after which the control unit will send out a SIM expiry SMS;
- **CREDIT REQUEST COMMAND:** enter the SMS command required to send a credit request; this number depends on the SIM card telephone provider;
- **SIM PROVIDER NUMBER:** number used by the SIM provider to issue its services (parameter acquired automatically).
- **GPRS PARAMETERS:**
  - SERVER IP ADDRESS
  - APN
  - USER
  - PASSWORD



**Note:** complete the parameters for your telephone operator.

**Warning!** In Access Point configuration, remote management can only be performed by exchanging DTMF telephone tones and/or SMS.

**Warning!** For Italy only: the configuration data for the providers Tim, Vodafone, Wind appear automatically depending on the SIM used.

- **VOICE MESSAGE VOLUME:** adjusts the volume with which voice messages are played;
- **FW VERSION:** FW version for GSM module.

## AFGSM04-4G:

- **NAME:** GSM identification label;
- **SIM PIN:** Enter “0000” or leave blank if the SIM does not have a PIN or enter the PIN code. Note: Inserting a SIM without PIN is recommended (see point 1);
- **IMEI:** IMEI (International Mobile Equipment Identity) number of the previously connected AGSM04 module (if any).
- **TELEPHONE OPERATOR:** the system automatically displays the name of the telephone operator;
- **SIM EXPIRY:** used to enter the number of months after which the control unit will send out a SIM expiry SMS;
- **CREDIT REQUEST COMMAND:** SMS command required to send a credit request; this number depends on the SIM card telephone provider;
- **SIM PROVIDER NUMBER:** number used by the SIM provider to issue its services (parameter acquired automatically).
- **SERVER IP ADDRESS:** future setting.
- **APN:** (*Access Point Name*) Access Point Name. This is a configuration that enables the smartphone to log onto the Internet via your provider (parameter acquired automatically).

**USER:** future setting.

**PASSWORD:** future setting.

**VOICE MESSAGE VOLUME:** volume of messages sent by the control unit to the set telephone number.

**MOBILE DATA:** If activated, enables data connection. If the control unit is configured as a router client, in the absence of a Wi-Fi connection, the AFGSM04-4G module enables remote management (if the 4G mobile network is present).

**DATA-SMS ONLY:** the control unit only manages connection to the AVE Cloud service (if the 4G mobile network is present) and the sending/receipt of SMS messages; it blocks voice call management.

- **FIRMWARE VERSION:** firmware version installed on the device.

**WARNING:** in the event of a mains power failure, the control unit automatically blocks management of the Wi-Fi and 4G GSM modules, thus making management via the AVE Cloud service impossible. However, this parameter can be changed so that the Wi-Fi network and GSM 4G can always be used by entering the “Communications parameters/Other configuration parameters” menu and activating the parameter “Connect to Cloud when network not available”. Use of the Wi-Fi or GSM 4G module significantly increases control unit battery consumption, thus reducing its length of time it remains operative in the case of power supply failure.









## FAQ

**WARNING!!!** The following operations may only be performed by professional electrical installers trained for product maintenance.

For information on the product warranty, log onto [www.ave.it](http://www.ave.it).

Question	Answer
The control unit is completely off: AF927PLUS: front LED off AF927PLUSTC: LCD off	Check that the 230Vac mains power supply is present and that the backup batteries are charged
	Open the cover of the control unit and check that the 230Vac mains power supply connector is hooked up and that the terminals on the top left are inserted in their housings
The control unit cannot be reached by the APP and AVE Cloud web page	Check that the home data network is present
	If the internet provider has been changed, check that the parameters of the new network are in line with those entered in the control unit network settings
	Check that the AVE Cloud Account is active and configured correctly
	Check that the AVE Cloud parameters entered in the control unit match those sent by the AVE Cloud service during system activation (Warning! in compliance with current legislation on privacy, AVE S.p.A. does not know customer passwords)
	If connection to the service is established via a 4G card, check that the provider subscription is active
	Check that the mobile device being used to attempt connect to the control unit has a 4G connection
The siren inside the control unit does not sound	In the configuration menu, check that the siren is active
The external radio siren does not sound	Check the charge of the siren batteries
	Check that the connection between external siren and control unit is stable and not disturbed by external factors (to be performed by the installer).
False alarms on a wired perimeter detector	Check that the sensor is connected correctly
	Check that detector balancing matches that configured for the control unit
	Check that the detector has correctly acquired the magnet; if not, bring the magnet close to the detector
One of the radio detectors is not working	Check the charge of the batteries inside the detector
	Check that the connection between detector and control unit is stable and not disturbed by external factors (to be performed by the installer)
User code forgotten	Contact the installer to perform the user code recovery operation via the installer code
Unit no longer sends confirmation/alarm SMSs	Check that the SIM card inserted in the telephone dialler is active and has an active credit
	Check that the SIM card security PIN is deactivated or that the PIN configured in the control unit matches that of the inserted SIM card
	Check GSM signal coverage at the control unit location
The "NO SIM" alarm icon appears at the top right-hand side of the LCD	Possible SIM card failure or SIM disabled
The control unit displays the "Opening tamper" alarm	Check that the control unit cover is properly closed
The numerical percentage indicated beside the battery symbol is close to zero	Replace the control unit back-up batteries (no. 2 x 12V - 2.2 Ah)
Question	Answer
The remote control does not work	Check that there are no obstacles preventing the device from functioning properly
	Check that the battery is charged
	Check that the remote-control operating mode is AF927PLUS-AF927PLUSTC (see instructions for remote control)

Upon attempting to connect with the control unit, the message "System under maintenance by Client..." appears.	Another user/installer is connected to the control unit to run a test
Upon calling up the settings menu, the control unit requests an additional deactivation	Normal deactivation procedure upon deactivation to reset internal memory
The user code cannot be entered from the keypad	If the User Pin is entered incorrectly three times in a row, the control unit blocks all access for 180 seconds. Wait and then try to enter the code once more
Meaning of the icon 	AVE Cloud service NOT enabled
Meaning of the icon 	AVE Cloud service enabled with connection attempt in progress
Meaning of the icon 	AVE Cloud service enabled and functioning properly
Meaning of the icon 	AVE Cloud service enabled but not functioning
Meaning of the icon 	AVE Cloud service connected via 4G data network
Meaning of the icon 	Remote technical service with AVE technicians in progress

**PRIMA DI INSTALLARE SISTEMI E AUTOMATISMI È VIVAMENTE CONSIGLIABILE FREQUENTARE UN CORSO DI FORMAZIONE, OLTRE LA LETTURA ATTENTA DELLE ISTRUZIONI**

BEFORE INSTALLING SYSTEMS AND AUTOMATION IT IS STRONGLY RECOMMENDED TO ATTEND A TRAINING COURSE AND READ THE INSTRUCTIONS CAREFULLY  
 AVANT D'INSTALLER SYSTÈMES ET APPAREILLAGES D'AUTOMATISATION, IL EST FORTEMENT RECOMMANDÉ D'ASSISTER À UN COURS DE FORMATION ET DE LIRE ATTENTIVEMENT LES INSTRUCTIONS  
 ANTES DE INSTALAR LOS SISTEMAS AUTOMATIZADOS ES MUY RECOMENDABLE ASISTIR A UN CURSO DE FORMACIÓN, MÁS ALLÁ DE LA LECTURA CUIDADOSA DE LAS INSTRUCCIONES

**NOTE**

Per la durata e le condizioni di garanzia dei singoli prodotti vedasi [www.ave.it](http://www.ave.it) e il catalogo commerciale vigente.

I prodotti devono essere commercializzati in confezione originale, in caso contrario al rivenditore e/o installatore è fatto obbligo di applicare e di trasmettere all'utilizzatore le istruzioni che accompagnano il prodotto e/o pubblicate su [www.ave.it](http://www.ave.it) e sul catalogo commerciale vigente.

I prodotti AVE sono prodotti da installazione. Vanno installati da personale qualificato secondo le normative vigenti e gli usi, rispettando le istruzioni di conservazione, d'uso e di installazione di AVE S.p.A.

Si richiede inoltre il rispetto delle condizioni generali di vendita, note, avvertenze generali, avvertenze garanzie, reclami e avvertenze tecniche per l'installatore riportate su [www.ave.it](http://www.ave.it) e sul catalogo commerciale vigente.

**NOTES**

For duration and warranty conditions regarding the single products, please visit [www.ave.it](http://www.ave.it) and see the current commercial catalogue.

Products shall be sold in the original packaging otherwise the dealer and/or installer has the obligation to apply and submit the instructions provided alongside the product and/or published in [www.ave.it](http://www.ave.it) and on the current commercial catalogue to the user.

Ave products are installation products. They should be installed by skilled personnel in compliance with the laws in force and uses, in accordance with the AVE S.p.A. storage, use and maintenance instructions.

Installers are also required to meet the general sales conditions, notes, general warnings, warranty conditions, claims and technical instructions indicated in [www.ave.it](http://www.ave.it) and in the current commercial catalogue.

**RAEE - Informazione agli utilizzatori**



Il simbolo del cassonetto barrato riportato sull'apparecchiatura o sulla sua confezione indica che il prodotto alla fine della propria vita utile deve essere raccolto separatamente dagli altri rifiuti. L'utente dovrà, pertanto, conferire l'apparecchiatura giunta a fine vita agli idonei centri comunali di raccolta differenziata dei rifiuti elettrotecnici ed elettronici. In alternativa alla gestione autonoma, è possibile consegnare gratuitamente l'apparecchiatura che si desidera smaltire al distributore, al momento dell'acquisto di una nuova apparecchiatura di tipo equivalente. Presso i distributori di prodotti elettronici con superficie di vendita di almeno 400 m<sup>2</sup> è inoltre possibile consegnare gratuitamente, senza obbligo di acquisto, i prodotti elettronici da smaltire con dimensioni inferiori a 25 cm. L'adeguata raccolta differenziata per l'avvio successivo dell'apparecchiatura dismessa al riciclaggio, al trattamento e allo smaltimento ambientalmente compatibile contribuisce ad evitare possibili effetti negativi sull'ambiente e sulla salute e favorisce il reimpiego e/o riciclo dei materiali di cui è composta l'apparecchiatura.

**NOTES**

Pour la durée et les conditions de garantie de chacun des produits, veuillez consulter le site [www.ave.it](http://www.ave.it) et le catalogue commercial en vigueur.

Les produits doivent commercialisés dans l'emballage d'origine. Dans le cas contraire, le revendeur et/ou l'installateur sont obligés d'appliquer et de transmettre à l'utilisateur les instructions qui accompagnent le produit et/ou qui sont publiées sur [www.ave.it](http://www.ave.it) et sur le catalogue commercial en vigueur.

Les produits AVE sont des produits d'installation. Ils doivent être installés par des personnes qualifiées conformément aux normes en vigueur et aux usages, en respectant les instructions de conservation, d'utilisation et d'installation d'AVE S.p.A.

De plus, il faut que soient respectées les conditions générales de vente, les notes, les consignes générales, les consignes sur la garantie, les réclamations et les consignes techniques pour l'installateur indiquées sur le site [www.ave.it](http://www.ave.it) et sur le catalogue commercial en vigueur.

**NOTAS**

Para obtener información sobre la duración y las condiciones de garantía de cada uno de los productos, consulte el sitio [www.ave.it](http://www.ave.it) y el catálogo comercial vigente.

Los productos deben ser comercializados en su embalaje original; de lo contrario, el vendedor y/o instalador deberá aplicar y transmitir al usuario las instrucciones que acompañan al producto y/o que se encuentran publicadas en el sitio [www.ave.it](http://www.ave.it) y en el catálogo comercial vigente.

Los productos AVE son artículos que requieren instalación. La misma debe ser efectuada por personal cualificado, conforme a las normativas vigentes y a los usos, respetando las instrucciones de conservación, uso e instalación establecidas por AVE S.p.A.

Asimismo, es necesario respetar las condiciones generales de venta, notas, advertencias generales o de garantía, reclamos y advertencias técnicas para el instalador detalladas en el sitio [www.ave.it](http://www.ave.it) y en el catálogo comercial vigente.



**WEEE - User information**



If the crossed-out bin symbol appears on the equipment or packaging, this means the product must not be included with other general waste at the end of its working life. The user must take the worn product to a sorted waste center, or return it to the retailer when purchasing a new one. Products for disposal can be consigned free of charge (without any new purchase obligation) to retailers with a sales area of at least 400 m<sup>2</sup>, if they measure less than 25 cm. An efficient sorted waste collection for the environmentally friendly disposal of the used device, or its subsequent recycling, helps avoid the potential negative effects on the environment and people's health, and encourages the re-use and/or recycling of the construction materials.

## APPENDIX

### AF927PLUS and AF927PLUSTC - AVE Firmware Settings

**AVE firmware for control unit versions AVEHS3\_067.0.0 and higher. Warning! This part of the manual is additional to previous paragraphs and reports only those variants of the AVE firmware whose function varies from that strictly compliant with the EN 50131. Points not covered here are considered identical to the corresponding points given in the manual above.**

FEATURES	AVE FIRMWARE	EN 50131-COMPLIANT FIRMWARE
EXTERNAL ALARM	Voice-only alarm activation	Cannot be used
BLOCK ACTIVATION WITH WINDOWS/DOORS OPEN	Automatic activation – possible cancellation	Block activation with mandatory event reading
BLOCK ACTIVATION WITH WINDOWS/DOORS OPEN	Reading of immediate events on display	Reading of events after entering the Power-user code
BLOCK ACTIVATION WITH WINDOWS/DOORS OPEN	Forcing not possible	Forced activation after mandatory reading
INSTALLER ACCESS	Immediate with relevant code	Subordinate to user access
ANTI-COERCION	Deactivation and telephone calls	Deactivation, display and telephone call notification
ALARM	Immediate display of source	No display - Notification upon deactivation
ROBBERY	Immediate display of source	No display - Notification upon deactivation
TAMPERING	Immediate display of source	No display - Notification upon deactivation
TRANSMISSION OF REMOTE ALARMS	Immediate alarm transmission	Transmission delay with delayed detectors if, during the input time, an alarm is triggered by an instantaneous sensor. Calls will not start until the input delay and the siren has sounded for at least 30 seconds.
PERIODIC PSTN CALL	Call every 1/999 hours	Call every 1/25 hours
PERIODIC GSM CALL	SMS transmission every 1/999 hours	SMS transmission every 1/25 hours
USER CODE ACCESS - TEST	Tamper alarm blocked	Tamper alarm active
USER DIRECTORY ACCESS	Management possible	Management not possible - installer only
FORCED USER ACCESS	Management possible	Management not possible - Power User only
ACTIVATION		
INPUT DELAY	1-45 seconds	1-45 seconds
NETWORK FAILURE	1-999 minutes	1-60 minutes
PANIC ALARM	Can be used	Cannot be used
TECHNOLOGICAL ALARM	Can be used	Cannot be used
SUPERVISION	Can be deactivated	Mandatory (*) - Activation forced by control unit
SCANNER	1-60 sec. Can be bypassed	1-30 sec. Mandatory
TLC/RADIO KEYPAD BATTERY LOW	Activation always possible	Activation forced by control unit (**) If the battery is low and a month or 25 alarms notifications has not elapsed, the activation key must be pressed twice as it is not activated by pressing it just once.
USER LOG WITH INDICATION TYPE	Green if USER or POWER USER is logged in Red if INSTALLER is logged in	Cannot be used

(\*) Activation is blocked if a supervision signal is missing and if, during the previous 60 minutes, even one peripheral device is missing.

(\*\*) Activation is blocked if the control unit receives more than 25 low battery signals and if more than one month has passed since the first signal.

**Note:** In compliance with general regulatory criteria, the AVE firmware enables operations that differ from EN 50131 standards. These mainly involve: 1) differentiated management of alarms coming from external detectors which are not covered by the standard; 2) immediate transmission of alarms as the standard requires these to be delayed; 3) immediate signalling of the source of the alarms on the display and on some keypads, which is not accepted by the standard. The other differences are indicated specifically for each topic. The decision to use such firmware invalidates EN 50131 certification: the installer, together with the user, is responsible for the choice of firmware. The manufacturer is willing to support operational choices envisaged in its firmware as they improve user security and usability.



**PRIMA DI INSTALLARE SISTEMI E AUTOMATISMI È VIVAMENTE CONSIGLIABILE FREQUENTARE UN CORSO DI FORMAZIONE, OLTRE LA LETTURA ATTENTA DELLE ISTRUZIONI**

*BEFORE INSTALLING SYSTEMS AND AUTOMATION IT IS STRONGLY RECOMMENDED TO ATTEND A TRAINING COURSE AND READ THE INSTRUCTIONS CAREFULLY*

*AVANT D'INSTALLER SYSTÈMES ET APPAREILLAGES D'AUTOMATISATION, IL EST FORTEMENT RECOMMANDÉ D'ASSISTER À UN COURS DE FORMATION ET DE LIRE ATTENTIVEMENT LES INSTRUCTIONS ANTES DE INSTALAR LOS SISTEMAS AUTOMATIZADOS ES MUY RECOMENDABLE ASISTIR A UN CURSO DE FORMACIÓN, MÁS ALLÁ DE LA LECTURA CUIDADOSA DE LAS INSTRUCCIONES*

**NOTE**

Per la durata e le condizioni di garanzia dei singoli prodotti vedasi [www.ave.it](http://www.ave.it) e il catalogo commerciale vigente.

I prodotti devono essere commercializzati in confezione originale, in caso contrario al rivenditore e/o installatore è fatto obbligo di applicare e di trasmettere all'utilizzatore le istruzioni che accompagnano il prodotto e/o pubblicate su [www.ave.it](http://www.ave.it) e sul catalogo commerciale vigente.

I prodotti AVE sono prodotti da installazione. Vanno installati da personale qualificato secondo le normative vigenti e gli usi, rispettando le istruzioni di conservazione, d'uso e di installazione di AVE S.p.A.

Si richiede inoltre il rispetto delle condizioni generali di vendita, note, avvertenze generali, avvertenze garanzie, reclami e avvertenze tecniche per l'installatore riportate su [www.ave.it](http://www.ave.it) e sul catalogo commerciale vigente.

**NOTES**

For duration and warranty conditions regarding the single products, please visit [www.ave.it](http://www.ave.it) and see the current commercial catalogue.

Products shall be sold in the original packaging otherwise the dealer and/or installer has the obligation to apply and submit the instructions provided alongside the product and/or published in [www.ave.it](http://www.ave.it) and on the current commercial catalogue to the user.

Ave products are installation products. They should be installed by skilled personnel in compliance with the laws in force and uses, in accordance with the AVE S.p.A. storage, use and maintenance instructions.

Installers are also required to meet the general sales conditions, notes, general warnings, warranty conditions, claims and technical instructions indicated in [www.ave.it](http://www.ave.it) and in the current commercial catalogue.

**NOTES**

Pour la durée et les conditions de garantie de chacun des produits, veuillez consulter le site [www.ave.it](http://www.ave.it) et le catalogue commercial en vigueur.

Les produits doivent commercialisés dans l'emballage d'origine. Dans le cas contraire, le revendeur et/ou l'installateur sont obligés d'appliquer et de transmettre à l'utilisateur les instructions qui accompagnent le produit et/ou qui sont publiées sur [www.ave.it](http://www.ave.it) et sur le catalogue commercial en vigueur.

Les produits AVE sont des produits d'installation. Ils doivent être installés par des personnes qualifiées conformément aux normes en vigueur et aux usages, en respectant les instructions de conservation, d'utilisation et d'installation d'AVE S.p.A.

De plus, il faut que soient respectées les conditions générales de vente, les notes, les consignes générales, les consignes sur la garantie, les réclamations et les consignes techniques pour l'installateur indiquées sur le site [www.ave.it](http://www.ave.it) et sur le catalogue commercial en vigueur.

**NOTAS**

Para obtener información sobre la duración y las condiciones de garantía de cada uno de los productos, consulte el sitio [www.ave.it](http://www.ave.it) y el catálogo comercial vigente.

Los productos deben ser comercializados en su embalaje original; de lo contrario, el vendedor y/o instalador deberá aplicar y transmitir al usuario las instrucciones que acompañan al producto y/o que se encuentran publicadas en el sitio [www.ave.it](http://www.ave.it) y en el catálogo comercial vigente.

Los productos AVE son artículos que requieren instalación. La misma debe ser efectuada por personal cualificado, conforme a las normativas vigentes y a los usos, respetando las instrucciones de conservación, uso e instalación establecidas por AVE S.p.A.

Asimismo, es necesario respetar las condiciones generales de venta, notas, advertencias generales o de garantía, reclamos y advertencias técnicas para el instalador detalladas en el sitio [www.ave.it](http://www.ave.it) y en el catálogo comercial vigente.

