DUEVI®

YOUR SECURITY. OUR TECHNOLOGY

CE-LAN

TECHNICAL MANUAL

2.2019

MT: 2.4

H: 1.0+

F: 2.9.3+

WIN: 1.0.7.0+

APP: 1.0.24+

ENG

⚠ **BEFORE INSTALLING THE SYSTEM READ CAREFULLY ALL THE PARTS OF THIS MANUAL AND KEEP IT CAREFULLY FOR FUTURE REFERENCE.**

⚠ **THE INSTALLATION OF THE PRODUCT MUST BE CARRIED OUT BY QUALIFIED TECHNICAL PERSONNEL. THE INSTALLER IS TAKEN TO FOLLOW THE APPLICABLE RULES..**

SAFETY AND MAINTENANCE RECOMMENDATION

⚠ BEFORE POWERING THE CONTROL PANEL, MAKE SURE THAT THE MAINS VOLTAGE IS THE ONE DESCRIBED ON THIS MANUAL.

⚠ IN THE ELECTRICAL SYSTEM TO BE CONNECTED TO THE CONTROL PANEL, A BIPOLAR SECTIONAL DEVICE MUST BE PROVIDED THAT IT IS EASILY ACCESSIBLE.

⚠ DO NOT CONNECT THE UNIT IN VERY WET OR VERY HOT ENVIRONMENT OR CLOSE TO BATHROOM, ETC.

⚠ THE COMMUNICATION BETWEEN THE VARIOUS COMPONENTS OF THE SYSTEM COMES IN RADIOFREQUENCY. BEFORE PERFORMING INSTALLATION, MAKE SURE THAT THE CONTROL PANEL COMMUNICATES CORRECTLY WITH ALL PERIPHERALS. IT MAY HAPPEN THAT THE CONTROL PANEL DOESN'T RECEIVE CORRECTLY THE SIGNALS FROM SOME DEVICE. THIS IS DUE TO THE CHARACTERISTICS OF THE ENVIRONMENT IN WHICH THE SYSTEM WORKS; WALLS IN CONCRETE, METAL BOXES, METALLIC SHELVES, ETC. CAN CREATE PARTICULAR CONDITIONS OF REFRACTION OF THE SIGNAL OR ATTENUATIONS (FOR EXAMPLE IT IS THE COMMON EXPERIENCE THE LACK OF SIGNALING OF THE CELL PHONE IN SOME PLACES). TO AVOID THESE INCONVENIENCES AND ALWAYS GET THE MAXIMUM PERFORMANCE FROM YOUR SYSTEM, IT IS RECOMMENDED TO ALWAYS PERFORM ANY PRELIMINARY POSITIONING TESTS, IN ORDER TO ENSURE THE ACTUAL QUALITY OF RADIO TESTS.

⚠ WARNING: IN THE ELECTRICAL SYSTEM IN WHICH THE CONTROL PANEL IS INSTALLED, AN EXTERNAL PROTECTION DEVICE SHOULD BE PRESENT AGAINST THE OVERCURRENT AND TROUBLESHOOTING TO THE GROUND 230V ~ 16A.

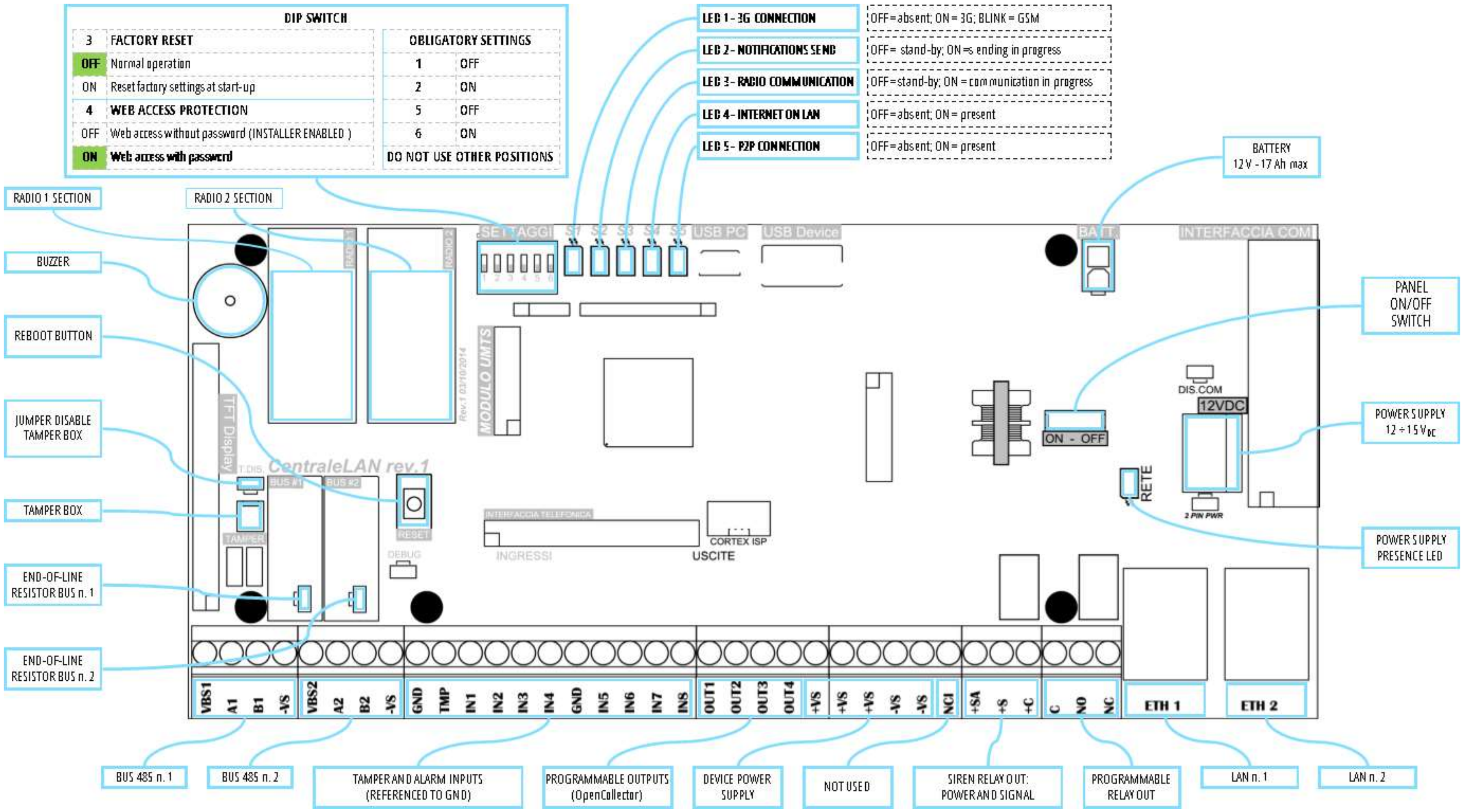
⚠ ATTENZIONE: NELL'IMPIANTO ELETTRICO IN CUI SI INSTALLA LA CENTRALE DEVE ESSERE PRESENTE UN DISPOSITIVO ESTERNO DI PROTEZIONE CONTRO LE SOVRACORRENTI E I GUASTI VERSO TERRA (DISPOSITIVO SALVAVITA) 230V~16A.

⚠ THE MANUFACTURER IS NOT LIABLE IN THE EVENT OF IMPROPER USE OF THE PRODUCT, WRONG INSTALLATION OR FAILURE TO OBSERVE THE INDICATIONS OF THIS MANUAL AND THE FAILURE TO OBSERVE THE LEGISLATION RELATED TO THE ELECTRICAL SYSTEMS.

SUMMARY

1 SPECIFICATION

1.1 PCB CONTROL PANEL

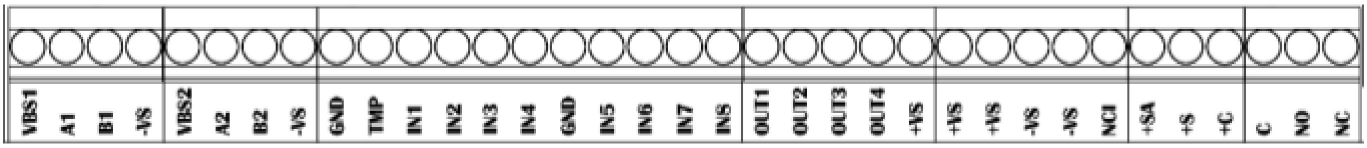


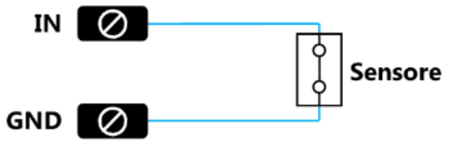
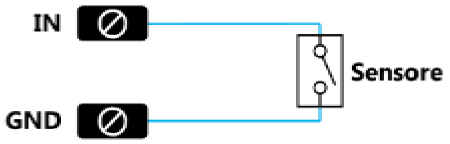
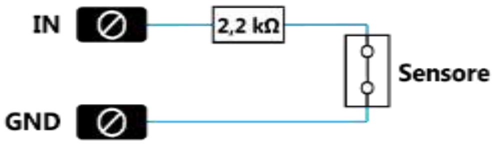
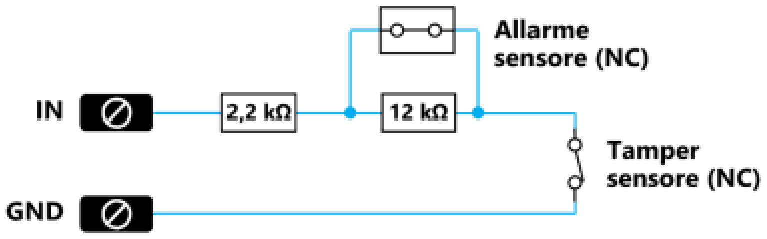
DIP SWITCH			
3	FACTORY RESET	OBLIGATORY SETTINGS	
OFF	Normal operation	1	OFF
ON	Reset factory settings at start-up	2	ON
4	WEB ACCESS PROTECTION	5	OFF
OFF	Web access without password (INSTALLER ENABLED)	6	ON
ON	Web access with password	DO NOT USE OTHER POSITIONS	

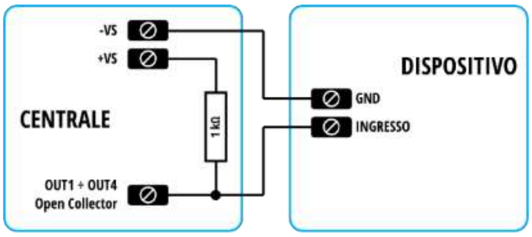
LED 1 - 3G CONNECTION	OFF=absent; ON = 3G; BLINK = GSM
LED 2 - NOTIFICATIONS SEND	OFF= stand-by; ON =s ending in progress
LED 3 - RADIO COMMUNICATION	OFF=stand-by; ON = communication in progress
LED 4 - INTERNET ON LAN	OFF=absent; ON = present
LED 5 - P2P CONNECTION	OFF=absent; ON = present

Figure 1 – Electric diagram of the control panel

1.2 TERMINAL BOARD



VBS1 **A1** **B1** **-VS**	BUS485 n. 1 **VBS1** = BUS power supply positive (+12 V) / **-VS** = BUS power supply negative Max 450 mA (protected by self-resetting polyswitch) **A1** / **B1** = BUS data
VBS2 **A2** **B2** **-VS**	BUS485 n. 2 **VBS2** = BUS power supply positive (+12 V) / **-VS** = BUS power supply negative Max 450 mA (protected by self-resetting polyswitch) **A2** / **B2** = BUS data
GND	Mass reference exclusively for **TMP** tamper line and zone inputs **IN1** ÷ **IN8**
TMP	TMP Input by wire tamper line (Normally Closed to GND)
IN1 ÷ IN8	Zone inputs: typically used as alarm zones, they can also be used for other functions (control of devices 24h / 24, panic, activator…). Electrically you can choose: • NORMALLY CLOSED = zone at rest when closed to GND  • NORMALLY OPEN = zone at rest when opened to GND  • SINGLE BALANCE = connection with the zone at rest when closed towards GND by resistance 2.2 kΩ, can detect short-circuit attempts  • DOUBLE BALANCE = connection with zone at rest when closed towards GND by resistance 2.2 kΩ and 12 kΩ; it can detect attempts to short-circuit and tamper/cable cut  Allarme sensore (NC) IN 2,2 kΩ 12 kΩ Tamper sensore (NC) GND

OUT1 ÷OUT4 **+VS**	Open Collector programmable outputs (max 20 VDC / 500 mA). Use the + VS terminal for the positive connection of the outputs according to the following diagram:  -VS +VS CENTRALE 1 kΩ OUT1 ÷ OUT4 Open Collector DISPOSITIVO GND INGRESSO Output status: positive + 12V = at rest; GND = active (this behaviour can be reversed in: SETUP> OUTPUTS> Output Settings). The outputs can be set to IMPULSIVE or MONOSTABLE. The OpenCollector outputs are electronic, so they cannot be connected directly to a load or to an input as for the relay outputs and OptoMOS (solid state relay).
+VS **+VS** **-VS** **-VS**	**+VS** = Positive +12 V— output for powering sensors and devices **-VS** = Negative reference for powering sensors and devices (DO NOT USE as a reference of the inputs zone **IN1** ÷ **IN8** and / or **TMP** tamper line)
NCI	NOT USED
+SA	**+SA** = Positive +12 V— output for powering a siren (max 450 mA)
+S **+C**	Output relay designed for the sound command of the wired sirens. This output is identified as "**OUT.SIR**" / "**RELE 5**". The output is available in the two opposite modes of operation: ▪ **+S** = Positive control +12 V given in alarm (REST=0 V / ACTIVE = +12 V) ▪ **+C** = Positive control +12 V missing in alarm (REST=+12 V / ACTIVE = 0 V) Note: this output must be associated with the "ALARM" and / or "PRE-ALARM" event (it is however possible to associate it freely also to other events)
C **NO** **NC**	Dry contact relay output, programmable (max 24 V_{DC} / 500 mA or 120 V_{AC} / 500 mA) This output is identified as "**OUT.REL**" / "**RELE 6**". **C** = Common terminal; **NO** = Normally Open Terminal; **NC** = Normally Closed Terminal

1.3 DIP SWITCH AND LED

1.3.1 DIP-SWITCH ON MAIN BOARD

Num	Function	OFF	ON
1	RESERVED	OBLIGATORY POSITION	DO NOT USE
2	RESERVED	DO NOT USE	OBLIGATORY POSITION
3	FACTORY RESET	Normal operation	Reset factory settings at start-up
4	WEB ACCESS PROTECTION	Web access without password INSTALLER ACCESS ALWAYS ENABLED	Web access with password
5	RESERVED	OBLIGATORY POSITION	DO NOT USE
6	RESERVED	DO NOT USE	OBLIGATORY POSITION

1.3.2 LED ON MAIN BOARD

Num	Function	OFF	ON
1	3G CONNECTION	Absent	Solid ON = 3G Flashing = GSM
2	NOTIFICATIONS SEND	stand-by	sending in progress
3	RADIO COMMUNICATION	stand-by	communication in progress
4	INTERNET ON LAN	Absent	Present
5	P2P CONNECTION	Absent	Present

1.4 BUS485

! Always check the maximum consumption reached on the BUS under maximum load conditions!

Features	Double RS485 BUS
Maximum consumption (for BUS)	Max 450 mA
BUS protection	Poliswitch 750 mA max, self-resetting
Compatibility	Activators: ▪ transponder key reader mod. LET-485 ▪ keypad with display mod. DVT-LCD or DVT-OLED Sirens: ▪ siren mod. VV-ZELA-BUS Accessories: ▪ wired zone expansion card and outputs mod. ESP8-BUS ▪ 433.92 MHz radio zone expansion card mod. ESP-R

1.5 WIRELESS SECTION

Features	n. 2 bi-directional radio sections (RTX): ▪ n. 1 section dedicated to alarm ▪ n. 1 section dedicated to wireless video-verification
Working frequency	869,65-867,00 MHz
Type of communication	Bidirectional, multi-channel FM with Listen Before Talk and Frequency Hopping
Range (open field)	▪ Alarm section: approx. 200 m ▪ Video-verification section: approx. 100 m
Wireless encoding	AES 128 bit
Wireless zones	Programming by auto-learning or serial code

1.6 ZONES

Total number of zones (wired and / or radio): 128

It is possible to add / create any number of radio or wired zones within the total limit:

- the wired zones are added by connecting the appropriate expansion cards (model ESP8-BUS) or other peripherals (ex: each keypad mod. DVT-LCD / OLED adds a wired zone)
- Wireless zones are added by programming (memorizing) radio sensors or other radio devices (ex: each MINI-C sensor adds 4 zones, one for each detection technology inside it)

WIRED ZONE ON BOARD

Factory reference	Name: "IN 1_1" ÷ "IN 8_1" Description: "IN x on Main Board"
Number	n. 8 wire zones (reference to GND)
Type	• Normally Closed • Normally Open • Single Balance (with 2.2 kΩ resistance) • Double balance (with 2.2 kΩ and 12 kΩ resistance)
Mode	• PRE-ALARM (L1) - Low level alarm.

A violation of a PRE-ALARM zone generates a low-level alarm.

If - within a pre-established time - a second violation of a PRE-ALARM zone occurs (ex: violation of the same zone or another PRE-ALARM zone) then a high level ALARM begins (see description ALARM).

If the second violation of a PRE-ALARM zone occurs after the pre-set time, there is again a PRE-ALARM low-level alarm.

It is possible to completely customize which actions the control panel will perform in case of PRE-ALARM (ex.: no sound of sirens, sending only SMS ...).

- ALARM (L2) - High level alarm.
  The violation of an ALARM zone always generates a high level alarm.
  It is possible to completely customize which actions the control panel will perform in case of ALARM (ex.: high-power sirens sound, sending calls and SMS ...).
- AND
  The alarm is generated if the two zones selected detect both intrusion within an AND time. It is possible to set the alarm level (PRE-ALARM or ALARM).
- INSTANTANEOUS
  Instantaneous zones immediately generate an alarm (of the PRE-ALARM or ALARM type) when they detect.
- DELAYED
  The delayed zones - when violated - start the Entry time before generating an alarm (PRE-ALARM or ALARM type).
  If the control panel is disarmed within the Entry time, there will be no alarm.
- SILENT
  When the Silent zone is violated, there will be no warning (no sirens sound or visible signals) but Silent Alarm communications will start (SMS and calls to programmed numbers).
- TECHNOLOGICAL
  The Technology zones are active 24h / 24 even when the system is disarmed.
  These zones are intended for use with detectors such as: flooding, smoke, gas ...
- PANIC
  When a panic zone is violated, the sirens sound to get immediate attention. Panic Alarm messages are sent (SMS and calls to programmed numbers).
- ACTIVATOR (IMPULSIVE / MONOSTABLE)
  The Activator zones are used to arm / disarm the system by means of a button or key. It is activated each Sector in which the zone has been added.
- INSTANTANEOUS + ALERT
  Like the Instant zones; when the panel is disarmed - their detection starts an acoustic warning.
- DELAYED + ALERT
  Like the Delayed zones; when the panel is disarmed - their detection starts an acoustic warning.

1.7 EXPANSION OF THE WIRED ZONES (OPTIONAL)

Device	ESP8-BUS (BUS485 expansion card for wired zones)
Factory reference	Name: "IN 1_n" ÷ "IN 8_n" (n = depends on the order in which the device was added) Description: “IN x on ESP8-BUS”
Number	n. 8 wired zones (reference to GND)
Type	• Normally Closed • Normally Open • Single Balance (with 2.2 kΩ resistance)

	• Double balance (with 2.2 kΩ and 12 kΩ resistance)
Mode	(see description "Wired zones on board")

1.8 EXPANSION OF WIRELESS ZONES 433 (OPTIONAL)

Device	ESP-R (BUS485 expansion card for wireless zones)
Working frequency	433,92 MHz
Range	100 m (in open field)
Factory reference	Name: "IN 1_n" ÷ "IN 8_n" (n = depends on the order in which the device was added) Description: "IN x on ESP-R"
Number	n. 8 wireless zones
Mode	(see description "Wired zones on board")

1.9 OUTPUTS (ON MAIN BOARD)

Features	All the outputs on the control panel are programmable. The outputs can be associated to any Area (even to several Areas at the same time) Each output can be programmed for multiple EVENTS at the same time
TYPE	▪ ON / OFF ON EVENT: the output follows the event state to which it is associated, it remains active as long as the event remains ▪ ON / OFF ON COMMAND: the output is controlled manually by the App ▪ IMPULSIVE (pulse duration adjustable from 1 to 255 seconds): the output activates when the event takes place and for the set time, then goes back to rest. It can also be manually controlled by the App.
State at rest (MODE)	▪ Normally Open ▪ Normally Closed
Events	▪ PANEL STATUS: DISARMED ▪ PANEL STATUS: ARMED ▪ ARMING ▪ PRE-ALARM ▪ ENTRY TIME ▪ MANUMISSION ▪ ALARM ▪ MAINTENANCE ▪ TECHNOLOGICAL ▪ PANIC ▪ SILENT ▪ TAMPER ▪ MANUAL CONTROL
Open Collector outputs	No. 4 Open Collector outputs
"Siren" output	N. 1 Alarm relay per siren (positive command to give/missing) Terminals: (**+S** / **+C**)
"Dry contact" relay output	N. 1 dry contact Alarm relay (**C**, **N.O.**, **N.C.**)

1.10 USERS

Maximum number of Users per Panel	128	
User Features	User Name	Customizable (max 14 characters)
	User Type (global)	▪ Normal: this type of User can arm / disarm the Area (or Areas) to which it is associated. It cannot display the general information of the system.

		▪ Administrator: as the normal user, but he can view the general information of the system and enable the Installer access
	User Type (Area)	▪ Master: User without limitations ▪ Service: Service user, he can only disarm
	Permits on the sectors of an area	It is possible to limit the permission of the User to arm / disarm on one or more Sectors of the Area
	Timetable (Area)	It is possible to define a weekly timetable in which the User is enabled or not on the Area
	SMS / MAIL / PUSH alerts	Global information from the system: ▪ Power supply information ▪ Service information ▪ Panel malfunctions ▪ LAN / 3G Status ("LAN / 3G Information") Information from the Area: ▪ Alarm / Pre-alarm events ▪ Panic Events / Silent Alarm / 24H Zones ▪ Change of the Area status
Maximum number of Activators per User	6 (total)	▪ Keypad User Code (max 1) ▪ Web / email access (max 1) ▪ Remote control ▪ Transponder Keys
Maximum number of emails per User	2 (only the main one is used for web / app access)	
Telephone numbers	Landline Telephone	Max n. 1 landline phone number
	Mobile phone	Max n. 1 mobile phone number

1.11 AREAS AND SECTORS

Characteristics of the Areas	Max number Areas	8
	Names of the Areas	Each Area can be named as desired (max 14 characters). The name is displayed in the warning messages (SMS, e-mail), in the events, in the keypad display, read in voice calls (only if TTS is available)
	Functions of the Areas	The list of the settings of each Area follows: ▪ Entry Time ▪ Exit Time ▪ Pre-Alarm Time ▪ Alarm Time ▪ AND time ▪ Open Doors Function ▪ Sounds and Alerts ▪ Auto-Arm / Disarm
	Number of Sectors by Area	4
	Max number of Users per Area	50 Standard Users (without weekly time limitation) PLEASE NOTE: Users limited to weekly time occupy the equivalent space of about 3 standard Users
	Max number of Zones per Area	128 (see Sector limits)
	Max number of Outputs per Area	16

	Max number of Activators per Area	8
Characteristics of Sectors	Max number of zones per Sector	32
	Sector names	Each Sector can be named as you like (max 13 characters)
	Zones in the Sectors	All zones of the control panel can be added to a Sector. The same zone can be added to several Sectors at the same time. Within Sectors it is possible to create the zone AND.
	Sectors in Common between Areas	Sector 4 of an Area may be associated with other Sectors 4 of others Areas to create a Common Group of Sectors 4 (max 3 groups). There will be an alarm from the Sectors 4 of a Common Group only if ALL the Areas involved in the Group are armed with Sector 4 active.

1.12 ACTIVATION, COMMAND AND INTERFACE TOOLS

Activators on BUS	Maximum total number of activators on BUS485	8 [always check the maximum consumption reached on BUS in maximum load conditions]
	Keypads with display	Mod. DVT-LCD / DVT-OLED
	Transponder key readers	Mod. LET-485
App / Web / Software	Local and remote access interface (LAN / Internet connection)	
Hardware keys	Zone inputs set as "Arming"	
Remote controls	Mod. TX6C	

1.13 EVENT MEMORY

GLOBAL event memory	Up to 5000 events recorded in permanent memory (consulted by Installer and Administrators)
AREAS events memory	Memory of events since the last arming (available to all belonging Users of the Area)

1.14 LAN

Connection type	10/100 Mbps Ethernet LAN \ Integrated switch, n. 2 RJ45 LAN connectors
Integrated Peer to Peer (P2P)	The control panel is equipped with an automatic network configuration system for remote access (it does not require modem / router configuration)

1.15 GSM / 3G MODULE

Module features *****	Functions that can be used thanks to the module: • Sending voice calls EVENTS (with / without TTS ******): alarm, panic, rescue... • Sending SMS events
Data connection *****	Data connection via GSM / 3G
TTS ******	Voice reading of Alarms / Areas / Sectors / Zones / Address for voice calls

***** The characteristics may vary depending on the model of GSM / 3G module installed and the services active on the SIM

****** The TTS feauture is only available for ITALIAN LANGUAGE and depends from the GSM / 3G module model installed

1.16 FIRMWARE

The control panel firmware can be updated (see the "FW update" settings from Installer access> SETUP)

1.17 COMPATIBILITY TABLE

Code	Product	Firmware (minimum version)
DVT-LCD / DVT-OLED	Keypad with display on BUS	1.61
LET-485	Transponder key reader on BUS	1.44
ESP8-BUS	Zone expansion card on BUS	2.1
VV-ZELA-BUS	Siren on BUS	1.1
ESP-R	433 Wireless zone expansion card on BUS	1.1

THE CE-LAN PANEL HAS BEEN DESIGNED FOR SMALL / MEDIUM DIMENSION PLANTS.

THE TECHNICAL CHARACTERISTICS OF THE PANEL - WHICH ARE TYPICAL OF THE BIG INSTALLATIONS (EX: 128 ZONE MAX) - CANNOT BE USED TO THE MAXIMUM LIMIT IN ALL CONDITIONS.

PAY PARTICULAR ATTENTION TO THE CONSUMPTION TO WHICH YOU SUBMIT EVERY SECTION OF THE PANEL (BUS, POWER OUTPUTS, SIREN OUTPUTS, ETC.).
DRAWING THE ALARM SYSTEM AND BE AWARE THAT THE MAXIMUM CONFIGURATION MUST ALWAYS RESPECT THE MAXIMUM CONSUMPTION LOAD.

Following are some basic considerations:

- The maximum number of connectable peripherals depends on the total consumption

Code	Consumption
DVT-LCD	30 mA (at stand-by) / 160 mA (active)
DVT-OLED	50 mA (at stand-by) / 120 mA (attiva)
LET-485	23 mA (at stand-by) / 30 mA (attivo)
ESP8-BUS	50 mA (without powering sensors from the card)
W-ZELA-BUS	9 mA (at stand-by) / 13 mA (con LED) *****
ESP-R	60 mA

***** ATTENTION: the sirens must be connected only if they have a battery (charged and in good condition) because the consumption in alarm – that exceeds the maximum values of the BUS - it is supplied by the battery itself without overloading the BUS

- The quality of the connections plays an important role especially for the BUS.
  In the following table we can see an estimate of the voltage drop caused by two typical cables normally used for alarm connections in different working conditions; appropriately select the most suitable one for the installation (section, distance, measured voltage…):

Cable type (sections: power + signals)	Current consumption	Distance	Voltage drop at the end of BUS connection
2 x 0,50 + 4 x 0,22 [mm^2]	450 mA	20 m	0,6 V
		40 m	1,2 V
		80 m	2,5 V
	200 mA	20 m	0,3 V
		40 m	0,5 V
		80 m	1,1 V
2 x 0,75 + 4 x 0,22 [mm^2]	450 mA	20 m	0,4 V
		40 m	0,8 V
		80 m	1,6 V
	200 mA	20 m	0,2 V
		40 m	0,4 V
		80 m	0,8 V

As you can see, the voltage drop strongly depends on the section of the power cable (it improves increasing the section), from current absorption (it worsen by increasing the consumption) and from the distance (it worsen by increasing the distance)

- Consider the installation position of both the control panel and the wireless peripherals, in order to optimize the radio range of the system; the panel should be in the hypothetical centre of the radio space to be covered: in this way the distance towards the radio peripherals is always the minimum, ensuring better communication quality and lower consumption.
- The maximum number of zones available (128) can only be reached if absorption limits are not exceeded; pay attention to the number of zones that each device (BUS and radio) adds / occupies
- When creating Areas, the various resources (zones, users, outputs...) must be appropriately distributed in a balanced way
- The higher the number of notifications (SMS, VOICE, E-MAIL) the longer it will take to complete the communications

2.1 EXAMPLE OF MAXIMUM CONFIGURATION

In the following configuration example we assume to create a system with these features:

- n. 4 Areas
- n. 1 Keyboard for each Area
- n. 1 Transponder key reader for each area
- n. 128 total zones (76 wired zones / 36 radio zones 868 MHz / 16 radio zones 433 MHz)
- n. 1 Wired siren
- Power supply of peripherals on the appropriate outputs [+ VS | + VS | -VS | -VS]

The sizing of the system - verifying the absorptions, the number of zones and the distribution of loads - is:

Device	**Quantity**	**Consumption ***	**Zones**
PANEL	1	-	8 wired
ESP8-BUS	8	8 x 50 mA = 400 mA	8 x 8 wired = 64 zones
ESP-R	2	2 x 60 mA = 120 mA	2 x 8 wireless 433 MHz = 16 zones
DVT-OLED	4	4 x 120 mA = 480 mA	4 x 1 wired = 4 zones
LET-485	4	4 x 30 mA = 120 mA	-
MINI-C	7	-	7 x 4 wireless = 28 zones
MINI-M	4	-	4 x 1 wireless = 4 zones
DIRRV2	4	-	4 x 1 wireless = 4 zones
W-ZELA-F	1	25 mA (stand-by) / 1,9 A (in alarm)	-
	TOTAL	1,14 A	128 zones

***** Note: for the calculation, the maximum consumption of each peripheral (usually of limited duration) were taken, except for the siren (whose peak of absorption must necessarily supplied by the battery on board)

A connection diagram can be summarized in the following table (as you can see, you need to deploy the devices on the two BUSs to balance the absorption):

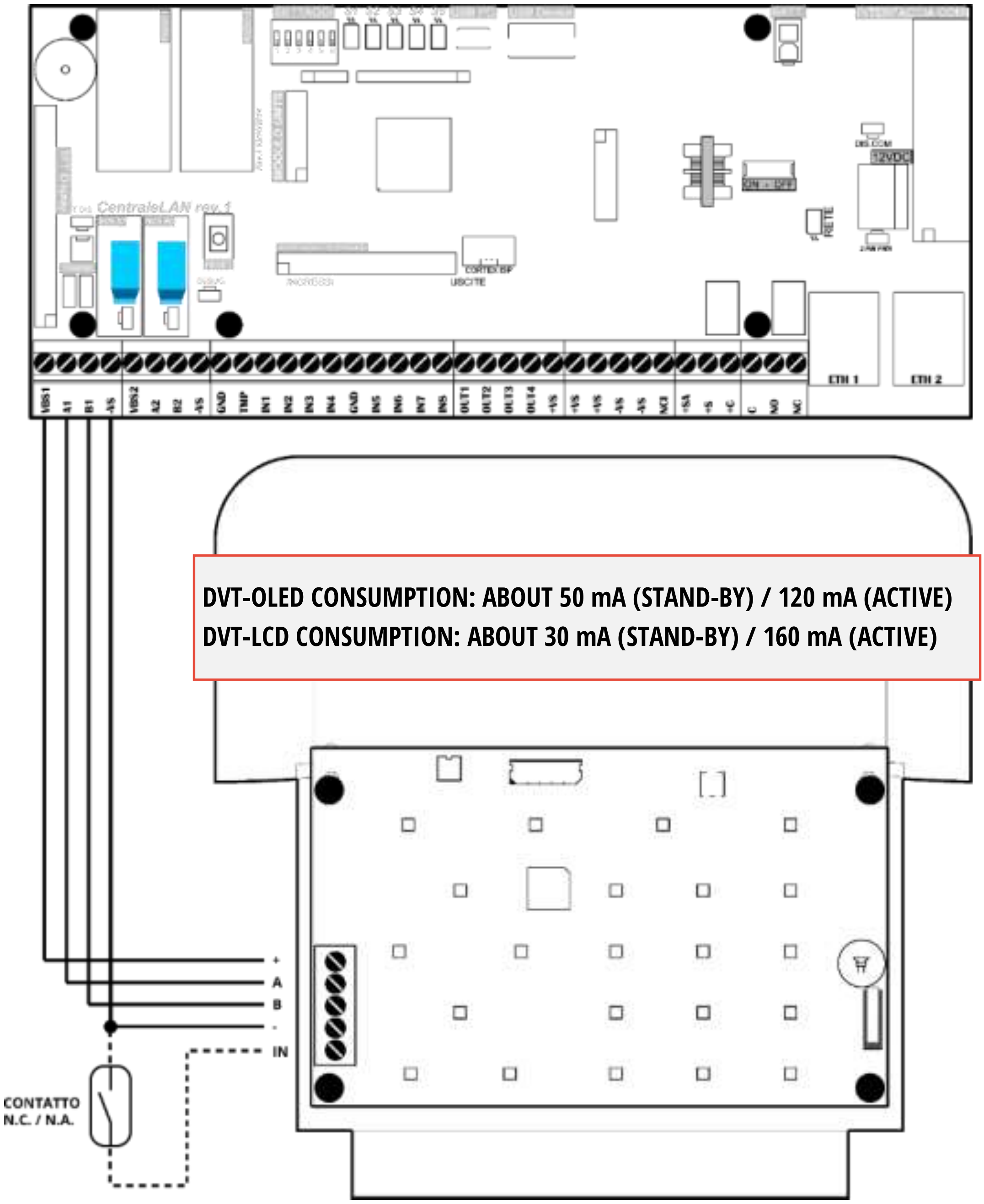
	BUS 1 **[VBS1 | A1 | B1 | –VS]**	**BUS 2** **[VBS2 | A2 | B2 | –VS]**	**OUT SIREN** **[+SA | +S | +C]**	**OUT POWER** **[+VS | +VS | –VS | –VS]**
	n. 2 DVT-OLED	n. 2 DVT-OLED	n. 1 W-ZELA-F	
	n. 2 LET-485	n. 2 LET-485		
	n. 4 ESP8-BUS	n. 4 ESP8-BUS		
	n. 1 ESP-R	n. 1 ESP-R		
Absorption	410 mA (peak 560 mA *****)	410 mA (peak 560 mA *****)	25 mA (peak 1,9 A ******)	Max 450 mA

***** In conditions of maximum consumption

****** The consumption peak in alarm must be supported by the siren battery

2.2 KEYPADS WITH DISPLAY ON BUS485 - MOD. DVT-LCD / DVT-OLED

! Pay attention to the maximum consumption (450 mA per BUS), MAX 8 ACTIVATION DEVICES ON EACH BUS!



DVT-OLED CONSUMPTION: ABOUT 50 mA (STAND-BY) / 120 mA (ACTIVE)
DVT-LCD CONSUMPTION: ABOUT 30 mA (STAND-BY) / 160 mA (ACTIVE)

Figure 2 – Example of keyboard connection with display mod. DVT-LCD / OLED to BUS1

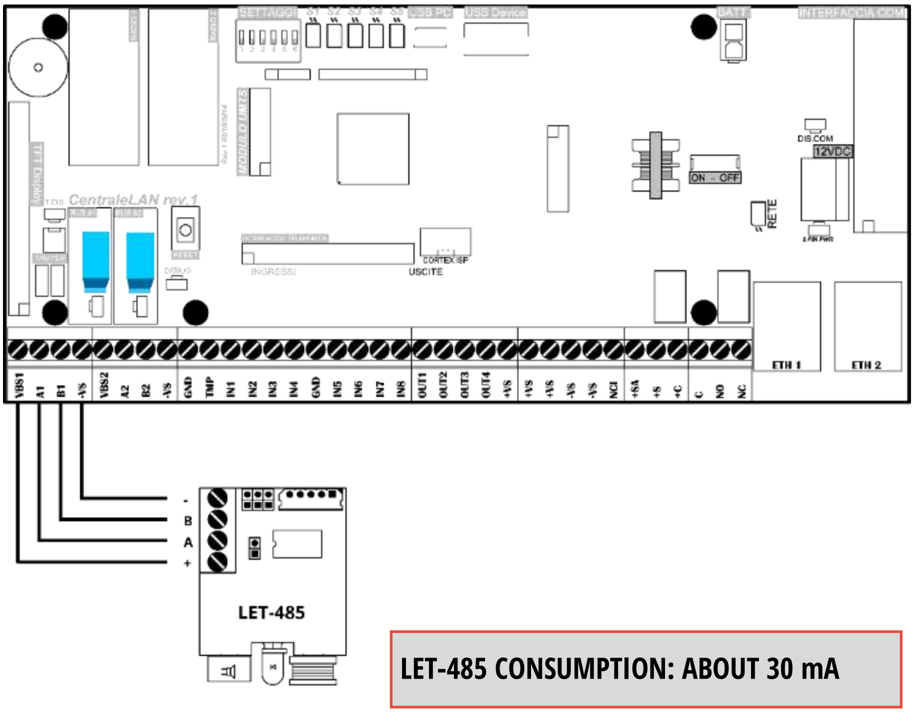
The keypads can be connected indifferently on the BUS1 or BUS2. The addressing is independent on the two BUS.

To program the address of the keypads:

- On the keypad, set **DIP2 = ON**
- Power supply the keypad (the keypad is powered by the BUS)
- Press the **F1** and **1** buttons simultaneously: the **KEYPAD PROGRAMMING** menu appears
- Select the **ADDRESS** item and confirm with ✓
- Set an address from 01 to 08 (be careful not to give the same address of other keypads on the same BUS!) Then press ✓
- Exit the menu, the keypad is programmed

2.3 TRANSPONDER KEY READERS ON BUS485 - MOD. LET-485

! Pay attention to the maximum consumption (450 mA per BUS), MAX 8 ACTIVATION DEVICES ON EACH BUS!

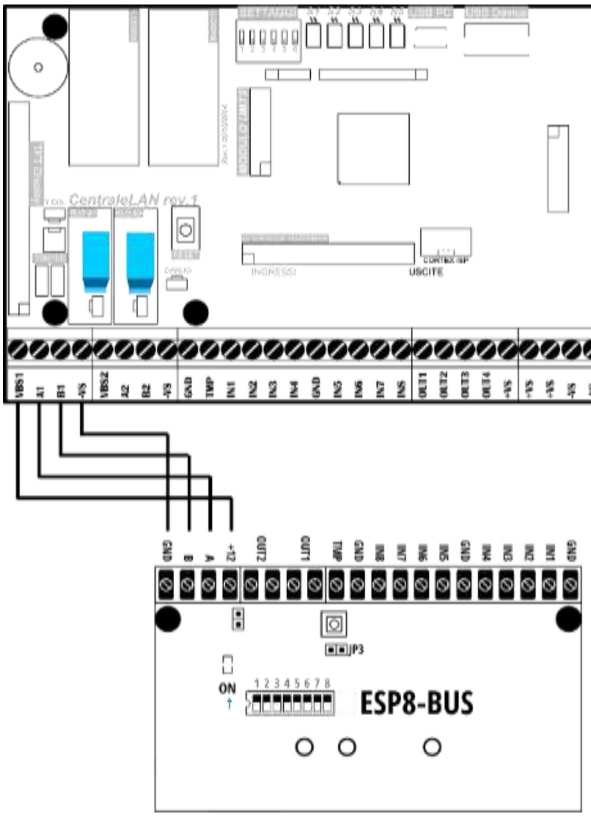


LET-485 CONSUMPTION: ABOUT 30 mA

Figure 3 – Example of connection of the transponder key reader mod. LET-485 to BUS1

2.4 WIRED ZONES EXPANSION CARDS ON BUS485 - MOD. ESP8-BUS

! Pay attention to maximum consumption (450 mA per BUS)!



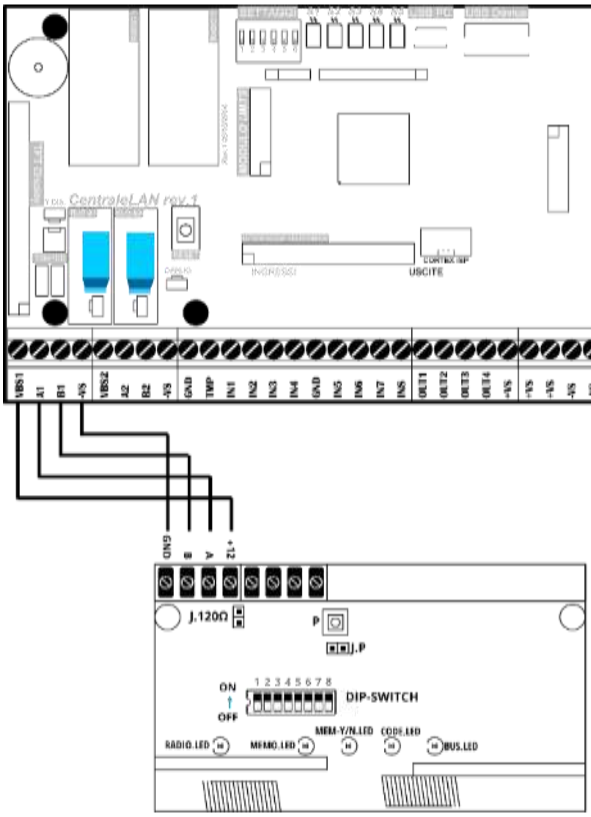
ESP8-BUS CONSUMPTION: ABOUT 50 mA

! WARNING!
TO USE CORRECTLY THE ESP8-BUS CARD WITH THE PANEL, PUT DIP6 AND DIP7 ON ON

Figure 4 – Example of connection of the zones expansion card mod. ESP8-BUS

2.5 WIRELESS ZONE EXPANSION CARDS 433.92 MHz ON BUS485 - MOD. ESP-R

! Pay attention to maximum consumption (450 mA per BUS)!

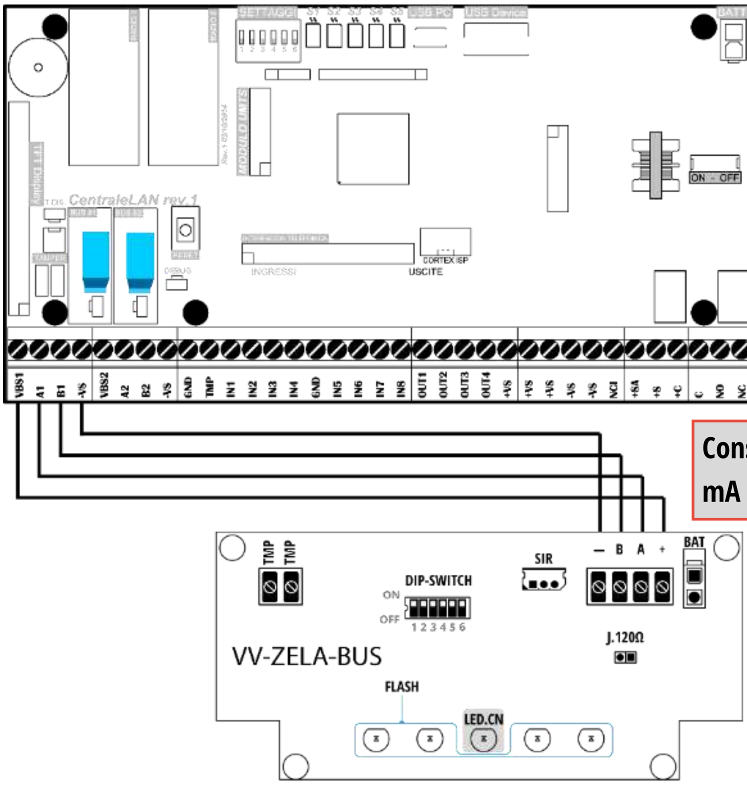


ESP-R consumption: approx. 60 mA

Figure 5 – Example of connection of the 433.92 MHz radio expansion card mod. ESP-R

2.6 OUTDOOR SIRENS ON BUS485 - MOD. VV-ZELA-BUS

! Pay attention to maximum consumption (450 mA per BUS)!



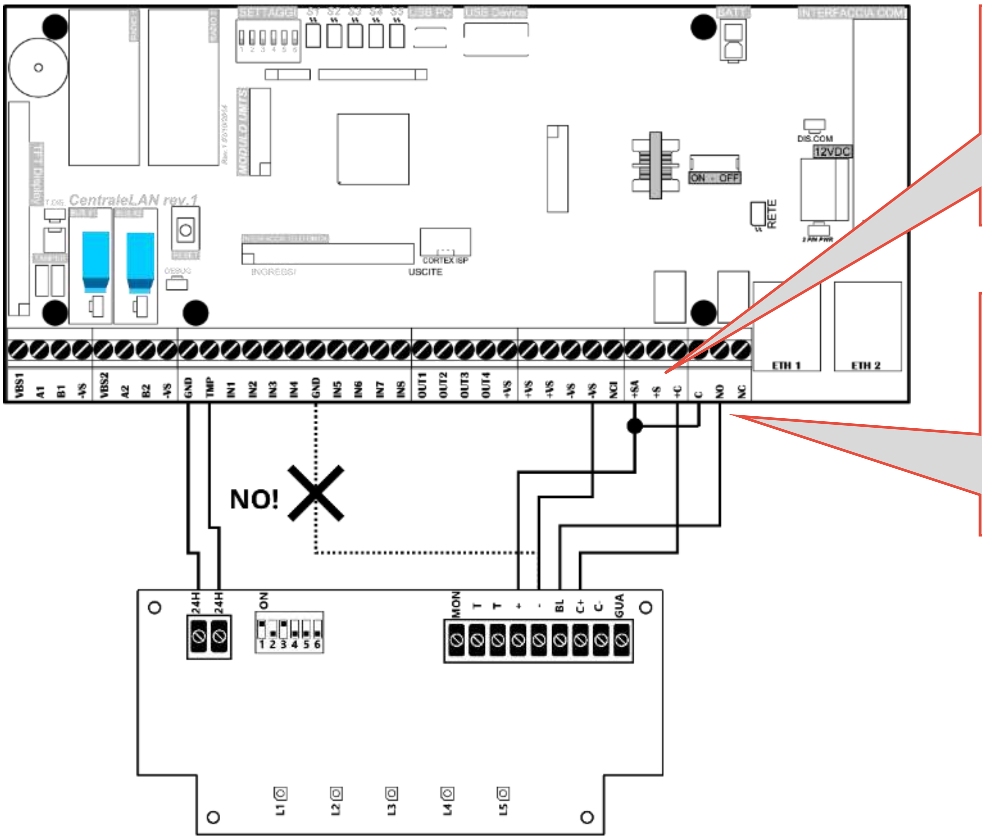
Consumption VV-ZELA-BUS: about 13 mA (stand-by!)

!WARNING!
THE SIREN MUST MANDATORY TO BE EQUIPPED WITH A WORKING AND CHARGED BATTERY.

Figure 6 – Example of connection of the siren on BUS mod. VV-ZELA-BUS

2.7 OUTDOOR WIRED SIREN - MOD. VV-ZELA-F

! THE SIREN MUST MANDATORY TO BE EQUIPPED WITH A WORKING AND CHARGED BATTERY, TO AVOID AN EXCESSIVE CONSUMPTION IN ALARM (WHICH COULD DAMAGE THE CONTROL PANEL)!
! PAY ATTENTION TO THE MAXIMUM CONSUMPTION (450 mA PER + SA)!



!WARNING!
Set the OUT.SIR output (terminals + S / + C) as ON / OFF ON EVENT and associate it with the ALARM and PRE-ALARM events

!WARNING!
Set the OUT.REL output (terminals C / NO / NC) as ON / OFF ON EVENT and associate it with the ARMED event in the Area.

!WARNING!
Set the siren as follows:

- DIP1 = ON
- DIP3 = ON

Figure 7 – Example of connection of the wired siren mod. VV-ZELA-F

2.8 WIRED SENSOR (GENERIC, NC TYPE ALARM CONTACT)

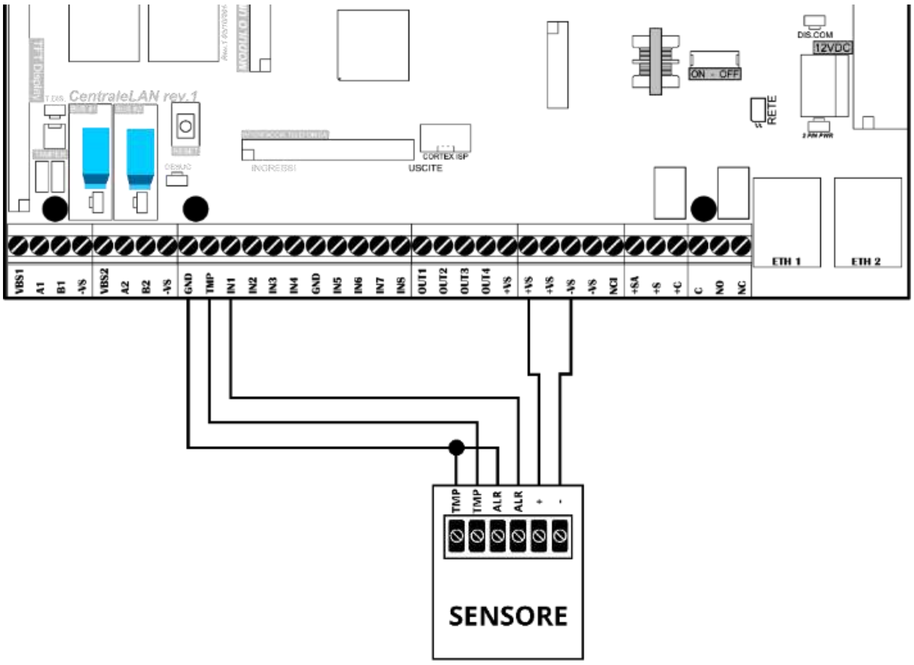
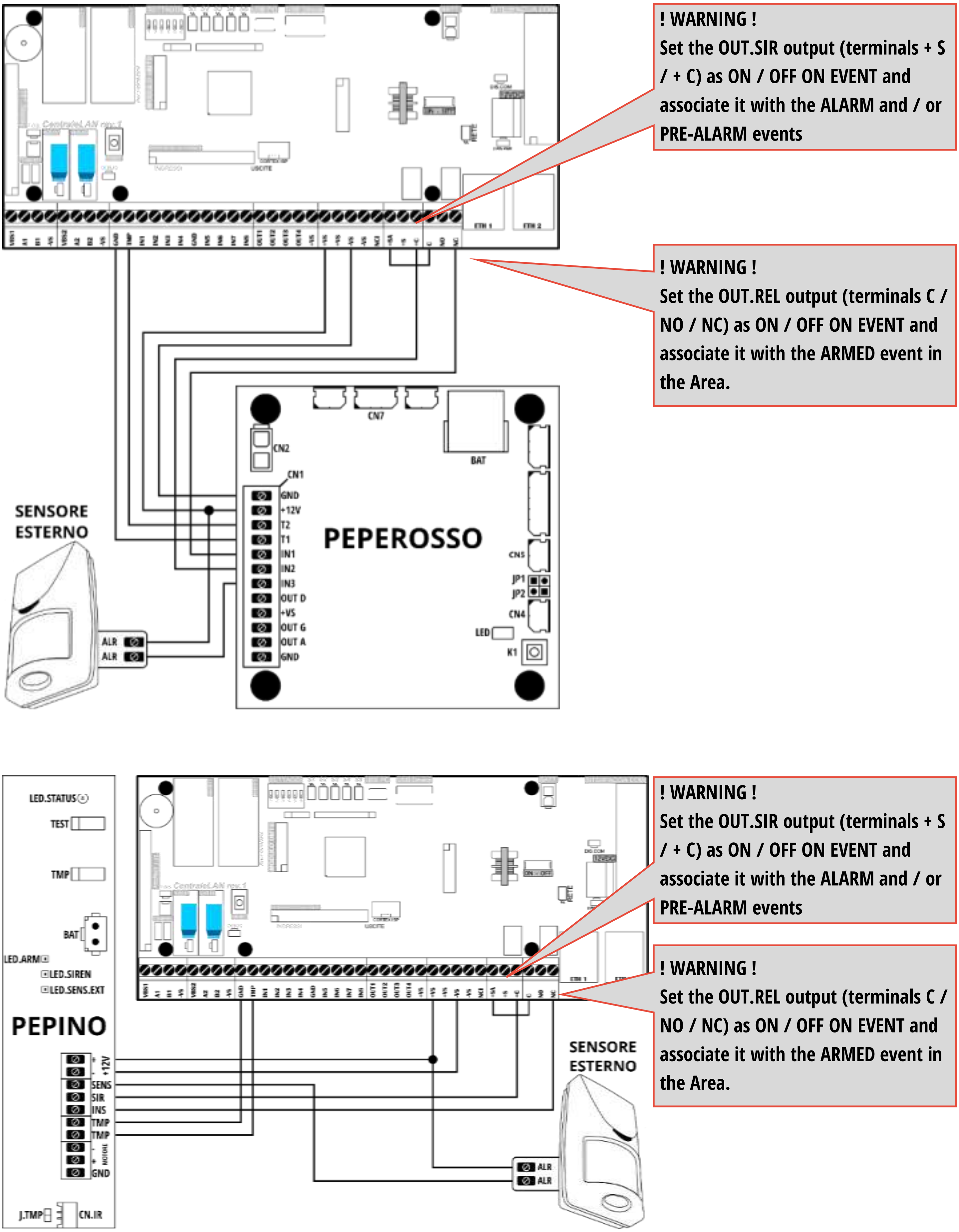


Figure 8 – Example of connection of a generic sensor

2.9 PEPPER SPRAY DEVICES - MOD. PEPEROSSO AND PEPINO



! WARNING !
Set the OUT.SIR output (terminals + S / + C) as ON / OFF ON EVENT and associate it with the ALARM and / or PRE-ALARM events

! WARNING !
Set the OUT.REL output (terminals C / NO / NC) as ON / OFF ON EVENT and associate it with the ARMED event in the Area.

! WARNING !
Set the OUT.SIR output (terminals + S / + C) as ON / OFF ON EVENT and associate it with the ALARM and / or PRE-ALARM events

! WARNING !
Set the OUT.REL output (terminals C / NO / NC) as ON / OFF ON EVENT and associate it with the ARMED event in the Area.

Figure 9 – Example of connection of the pepper spray mod. PEPEROSSO and mod. PEPINO

2.10 LAN CONNECTION

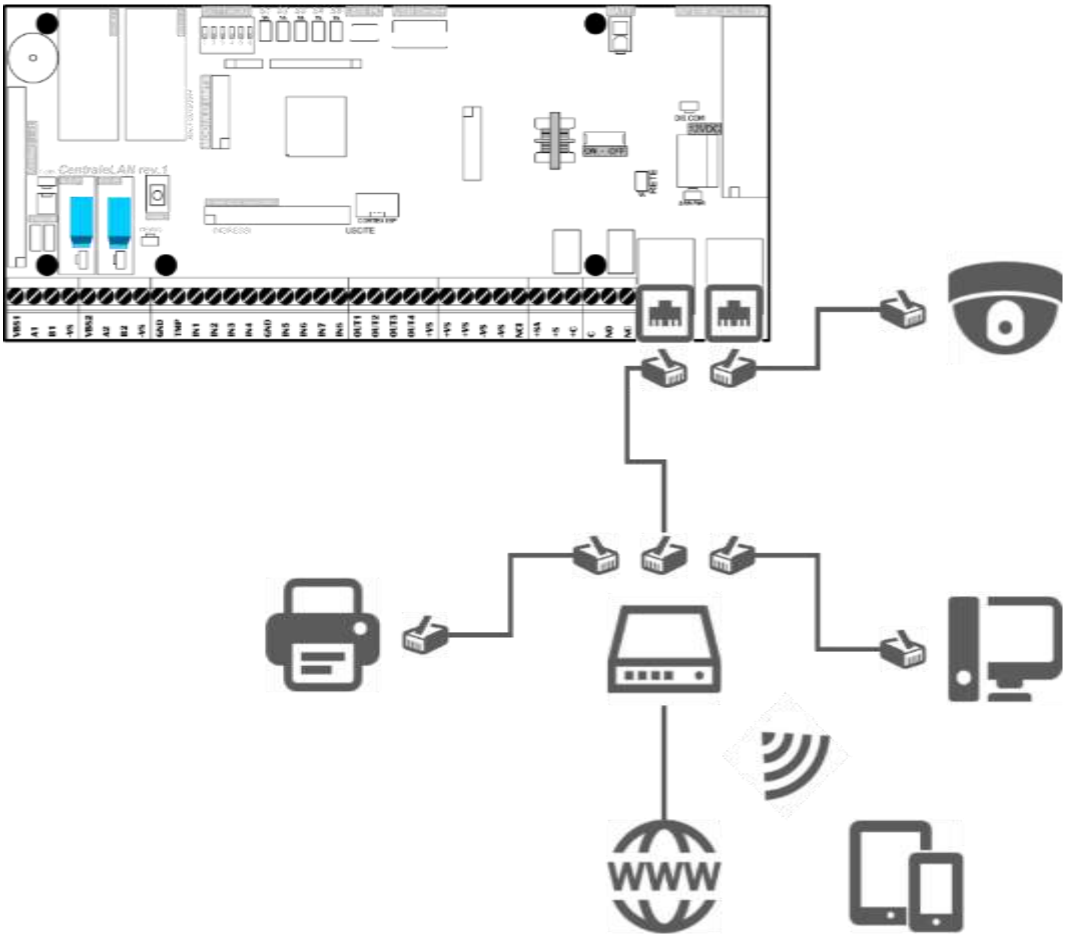


Figure 10 – Example of connection to the local network

IN CASE OF DIRECT CONNECTION BETWEEN PC AND PANEL, IT IS NECESSARY TO SET THE PC IN DHCP (AUTOMATION ASSIGNMENT OF IP ADDRESS). OTHERWISE, IT IS NOT POSSIBLE TO COMMUNICATE THE PANEL WITH THE PC.

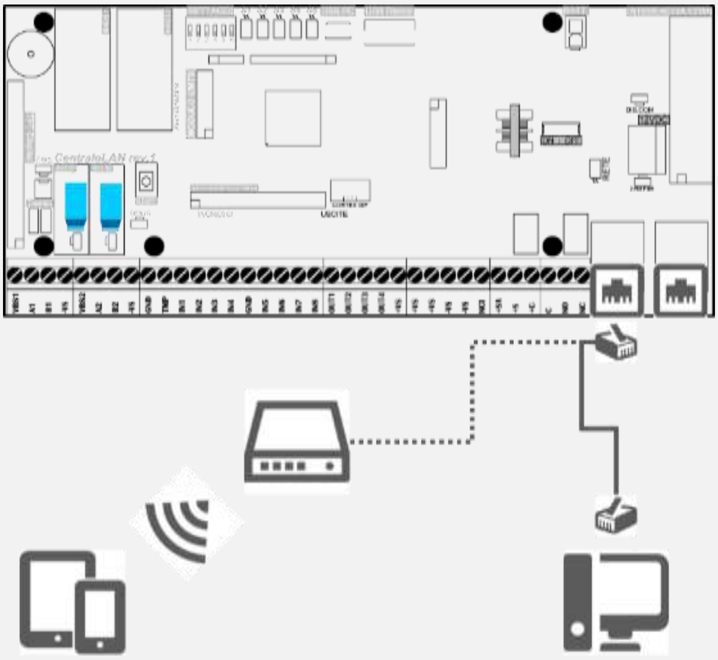


Figure 11 – Direct connection to the control panel: set the PC / device in DHCP

3 MAIN CHARACTERISTICS

CE-LAN is a new-generation Cortex dual-core microprocessor control and alarm panel.

The main features are:

- **AREAS CONTROL PANEL**

  An AREA is comparable to an independent alarm system, with its own partitions (SECTORS) of the zones, adjustable arming/disarming, versatile control and user management.

  With this control panel, up to **eight AREAS** can be created.

  Each AREA is divided into **four SECTORS** of zones, which can be configured as desired and can be activated independently.

  The **common zones** between the AREAS are managed.

- **USERS AND ACCESS**

  The use of the system by users is highly configurable.

  The control panel can manage up to 128 users.

  Each user can interact with the alarm system through:

  - Web access (practically from every device: smartphone, tablet, PC ...)
  - Bidirectional wireless remote controls
  - Keypads with display
  - Transponder keys
  - SMS text messages

  It is possible to limit access to certain time slots, only to certain sectors, or to allow only temporary bypassing of some zones (patrol or service user).

- **P2P INTERNET CONNECTION**

  The network connection (local or via internet) is the main and powerful means of communication of the control panel.

  As long as the control panel is connected (to the LAN or to the 3G module) with Internet access, you can immediately access it from anywhere! In fact, the control panel is equipped with TUNNELING technology: without any configuration of the network it is immediately visible both locally or remotely from Internet (communication is always safe and secure).

  The control panel is equipped with a switch with two ethernet ports to share the same LAN connection with other devices.

- **SIMPLE CONFIGURATION**

  The connection of accessories on BUS 485 and the addition of all the radio accessories is simple:

  - BUS devices are automatically recognized and added with just one click
  - all the radio sensors are programmed by only closing the tamper switch or by serial code
  - remote controls are added to the users by pressing some keys

  The web interface (rich in information and on-screen help) makes configuration of the functions remarkably intuitive.

- **BIDIRECTIONAL**

  All wireless accessories are BIDIRECTIONAL, creating an intelligent anti-intrusion environment.

  Each radio device communicates with the control panel, a communication that adapts the system's response in real time.

  For example: the remote controls display the status of arming and allow the control of the individual sectors of the area, it is always known the opening state of the doors / windows, the transmission power is calibrated at the lowest level necessary (with consequent battery savings), etc.

4 FIRST SWITCH-ON / RESET OF THE PANEL

For the installation and the first switch-on of the CE-LAN unit it is necessary to follow the following steps:

1. Set **INT** = **OFF** (panel off)
2. Connect the panel to the LAN via the **LAN1** port
3. Connect the RS485 peripheral devices (keypads, transponder readers, zone expansion cards, sirens) to one of the two 485BUS
4. Connect the wired zones (NC, single balance or double balance) both of the control panel and of the expansion cards
5. Set the DIP SWITCHES as follows:
    - **DIP1** = **OFF**
    - **DIP2** = **ON**
    - **DIP3** = **ON** (reset settings)
    - **DIP4** = **OFF** (web access without password / Installer access enabled)
    - **DIP5** = **OFF**
    - **DIP6 = ON**
6. Connect the 230 V$_{AC}$ power supply.
7. Set **INT** = **ON** (the control panel switch-on).
8. Wait for the complete control panel to start up (about 30 seconds) then return **DIP3** = **OFF**.
9. At this point it is possible to access the configuration of the control panel using the CELan Connect application.

WARNING!
AFTER THE FIRST BOOT, REMEMBER TO SWITCH DIP3=OFF, OTHERWISE THE PANEL WILL RESET TO DEFAULT AT EACH REBOOT.

5 PREPARATION OF PROGRAMMING SOFTWARE

NOTE: SINCE PERIODICALLY NEW VERSIONS OR SOFTWARE UPDATES ARE RELEASED, PICTURES AND FIGURES PRESENT IN THIS MANUAL CAN DIFFER FROM THE SCREEN DISPLAY.

THE PANEL IS PROGRAMMABLE ONLY THROUGH A NETWORK CONNECTION (DIRECT CABLE, NETWORK LOCAL OR INTERNET) THROUGH "CE-LAN CONNECT" DEDICATED APPLICATION (FOR WINDOWS, IOS AND ANDROID).

To program and use the control panel, supply power and connect it to the local LAN, preferably with Internet access [1].
The computer, smartphone or device used for programming must be connected:

- **locally**: on the same local network where the panel is located (via ethernet or WiFi)
- **remotely**: to the Internet, in this case the remote panel must also have an Internet connection

5.1 "CE-LAN CONNECT" APPLICATION

To connect to the control panel, launch the application:

CELAN CONNECT (WINDOWS)	APP FOR WINDOWS
CELAN CONNECT	iOS / ANDROID

The application provides the **control and programming interface of the control panel** [2].

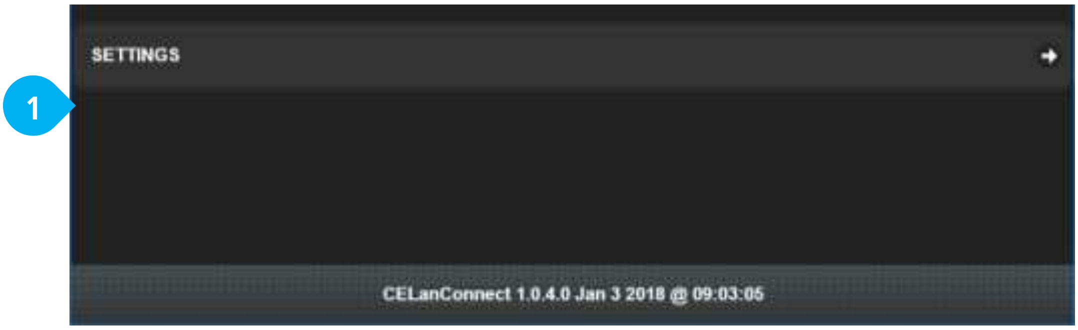


Figure 12 – Home page of the APP

EVERY FIRMWARE VERSION OF THE PANEL HAS ITS OWN GRAPHIC INTERFACE.
BEFORE STARTING THE INSTALLATION OF A NEW SYSTEM CHECK AND UPDATE THE APPLICATION TO HAVE THE INTERFACE CORRESPONDING TO THE CONTROL PANEL FIRMWARE VERSION.

[1] Internet connection is necessary if the control panel version is more up-to-date than the application.
It is sufficient to update the application in order to solve the problem (see "SETTINGS").

[2] It is necessary to regularly update the CELAN application to have available the interfaces of the different versions of the control panel.

5.1.1 MANAGEMENT AND UPDATING OF INTERFACES

Pressing "SETTINGS \ MANAGE GRAPHIC INTERFACES" opens the window to manage the interfaces and create virtual panels (Figure 13)

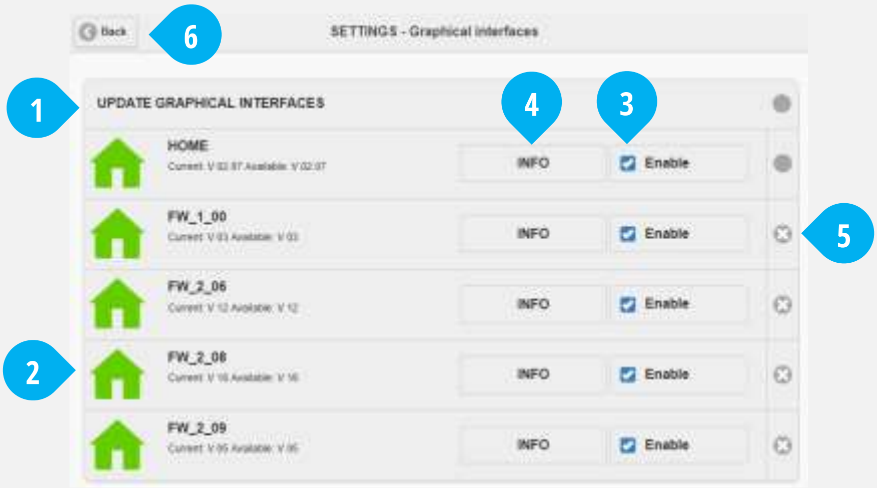

Back
6
SETTINGS - Graphical interfaces
1
UPDATE GRAPHICAL INTERFACES
4
3
HOME
Current: V 02.07 Available: V 02.07
INFO
☑ Enable
FW_1_00
Current: V 03 Available: V 03
INFO
☑ Enable
5
FW_2_06
Current: V 12 Available: V 12
INFO
☑ Enable
2
FW_2_08
Current: V 16 Available: V 16
INFO
☑ Enable
FW_2_09
Current: V 05 Available: V 05
INFO
☑ Enable

Figure 13 – Interfaces management page

1. UPDATE GRAPHICAL INTERFACES: check online for updates and downloads new versions (requires Internet connection):

- when the symbol is 🏠 (grey) it means that the interface is available for that version of control panel but it has not been downloaded (so can not be used) or has been deleted
- when an update is available for an interface, the ⓘ icon is added to the symbol 🏠 (green)

2. INTERFACE: this line indicates the presence of the interface for a specific firmware version of the control panel:

- 🏠 (grey): the interface is available but has not been downloaded or has been deleted
- 🏠 (green): the interface is available and is updated
- 🏠 (green) + ⓘ: the interface is available and usable but there is an update (press " UPDATE GRAPHICAL INTERFACES")

3. ENABLE checking and downloading of updates for this interface / firmware version

4. INFO Open the informations on the interface versions

5. DELETE the files of the selected interface (ex. because it is no longer in use): in this way the space on the device is freed, but it will not be possible to connect to the control panels with that firmware version (you will need to download the interface again)!

6. BACK: return to the previous screen

OFFLINE VIRTUAL PANEL

Touching an interface row creates a VIRTUAL PANEL for that firmware version. This is useful when a control panel is not available (for example: it is not connected or reachable, it will be installed at a later time ...) for:

- prepare the programming of a generic control panel (only configuration of the control panel / users / zones / outputs / areas without adding BUS or radio peripherals)
- create a control panel in which to load a saved configuration file, in order to consult the programming

5.1.2 MANAGEMENT OF DEVICES (PANELS)

Initially, the **list of control panels** is empty (Figure 12).

On the body of the central unit or on the electronic board there are the reference data of the control panel:

- MAC ADDRESS and SERIAL / DEVICE ID
- QR CODE (to use with appropriate function on the app)

To **add / delete** a control panel, open the "SETTINGS / MANAGE DEVICES" screen:

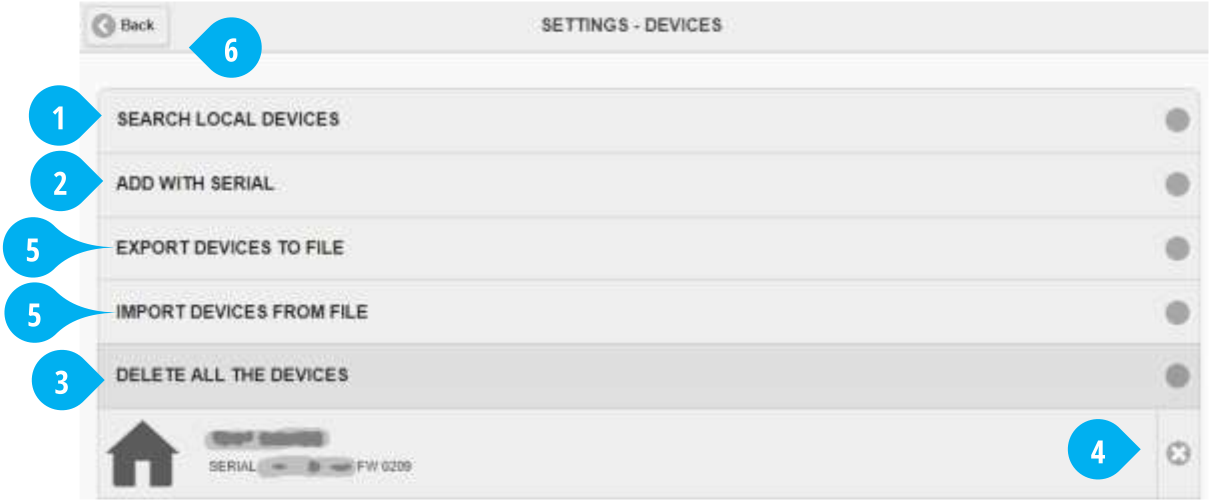


Figure 14 – "Device Management" page of the application

The different ways to add a control panel are:

- **SEARCH LOCAL DEVICES** perform a RESEARCH of the panels in the local network and add them to the list (Figure 14-1).
- **ADD WITH SERIAL** performs a MANUAL addition of a control panel via a UNIQUE SERIAL CODE. (Figure 14-2)
- (ONLY IOS AND ANDROID APP) **ADD WITH QR CODE** scan the QR CODE of the control panel.

To delete all the already added control panels, press the **DELETE ALL THE DEVICES** button (Figure 14-3).

To delete a single control panel, press the **X** key on the control panel line (Figure 14-4).

(ONLY WINDOWS) To export/import from file the complete list of the panels of the software, press the buttons **EXPORT/IMPORT DEVICES FROM FILE** and select the file (Figure 14-5).

To go back to the previous screen, press the button **Back** (Figure 14-6)

5.1.3 LIST OF CONTROL PANELS (MAIN PAGE)

Once added to the management menu, the control panels appear on the main application screen:

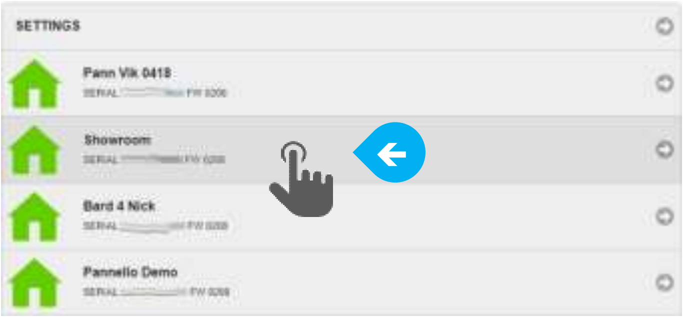

SETTINGS
Pann Vik 0418
SERIAL [redacted] FW 0206
Showroom
SERIAL [redacted] FW 0208
Bard 4 Nick
SERIAL [redacted] FW 0208
Pannello Demo
SERIAL [redacted] FW 0209

Figure 15 – List of panels managed by the app

The colour of the 🏠 icon indicates:

- 🏠 (green) = The control panel is online and can be programmed / used
- 🏠 (green + orange arrow) = The control panel is online and can be programmed / used; an interface update is available (see "SETTINGS> MANAGE GRAPHIC INTERFACES")
- 🏠 (green + red cross) = The control panel is online but the graphical interface was not donlowaded (see "SETTINGS> MANAGE GRAPHIC INTERFACES")
- 🏠 (grey) = The control is not connected at the moment

6 ACCESS TO THE PANEL

6.1 LOGIN and LOGOUT

Click the name of a control panel in the list to connect (Figure 15), the login page will open (**login**, Figure 16):

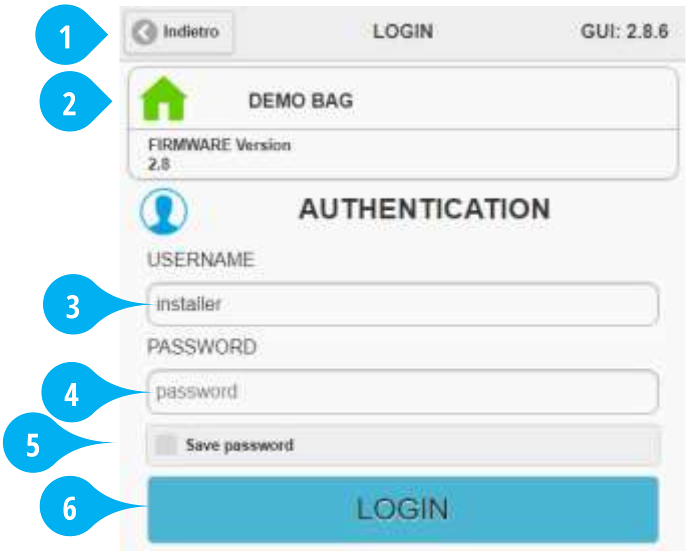


Figure 16 – Login page

The factory data of access as an installer are:

- **USERNAME = installer (all lowercase letters)**
- **PASSWORD = admin (all lowercase letters)**

NOTE: WHEN THE PANEL IS RETURNED TO FACTORY SETTINGS (RESET) THROUGH DIP3=ON, THE INSTALLER ACCESS IS ENABLED WITH FACTORY USER AND PASSWORD.

INSTALLER USER CAN ACCESS THE PANEL ONLY IF HE IS ENABLED BY AN ADMINISTRATOR USER OR IF THE PANEL HAS DIP4=OFF, MEANS WEB ACCESS WITHOUT PASSWORD PROTECTION.

1.
2. Press the button **Back** to go back to the panel list
3. Name assigned to the control panel and connection status with the panel:
   - “GREEN HOME” = the control panel is online and the connection is established
   - “GREY HOME” = the control panel is not reacheable at the moment. Communication problems or panel offline.

   FIRMWARE Version: indicates the firmware version of the control panel.
4. "USERNAME" field - Enter here the user name for access to the control panel.
5. "PASSWORD" field - Enter the password chosen for the user. The password must be at least 8 characters and no more than 15.
6. SAVE PASSWORD - If you enable this function, the access datas will be stored for the future connection.
7. LOGIN - After entering "user name" and "password", press the LOGIN button to access the control panel.

Once logged in, the interface shows the "Menu" button (Figure 17-2) and - depending on the type of user who logged in - a different content on the main page (see the following paragraphs).

Once logged in as an INSTALLER, the status of the control panel is displayed in **NORMAL MODE** (Figure 17).

To open / close the side panel, press the " ≡ MENU" button (Figure 17-1).

To perform the installation operations, enter **SETUP MODE** ("ENTER SETUP" button, Figure 17-2)

To **LOGOUT** (disconnect the user from the system), press the "Menu" button and then "LOGOUT" (Figure 17-2).

6.2 NORMAL MODE

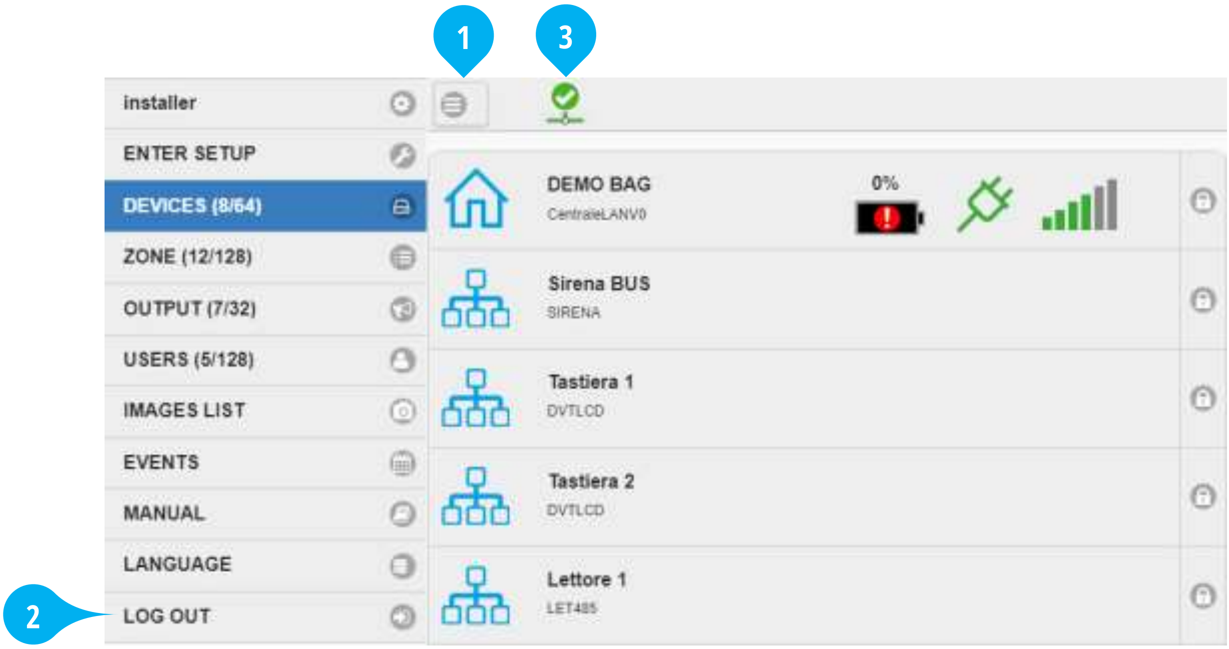


Figure 17 – Installer window in NORMAL MODE

The "NORMAL" mode only allows the DISPLAY of the information and the status of all the menus.
In this view the information is in real time (so, for example, if a zone is opened / closed it will be displayed immediately its status, as well as the state of the batteries, the quality of radio communication, etc.).
The numbers in brackets in the menu items [example: DEVICES **(4/64)**] indicate the number of used elements compared to available.

NOTE: The connection icon (Figure 17-3) indicates in real time the connection status with the control panel. In the case of a non-stable remote connection, it is possible that the software temporarily loses its connection to the control panel. This is normal and depends on the quality of the connection. **Consider that the information displayed in this condition will not be updated until the connection is re-established.**

✓ **= ONLINE** ✗ **= OFFLINE**

6.2.1 DEVICES MENU

It shows - in addition to the control panel - all the wired / radio devices already added to the control panel (Figure 18).

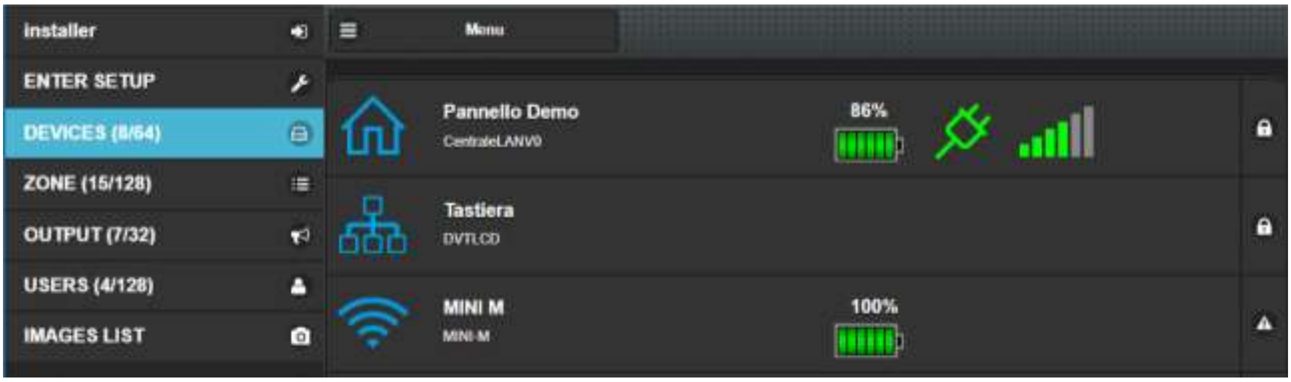


Figure 18 – DEVICES panel (Normal mode)

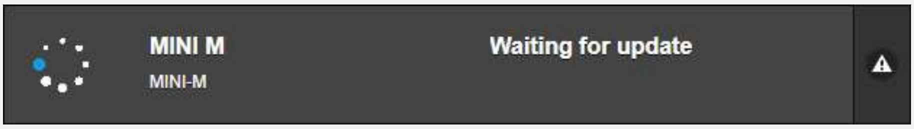
For each device are shown: Name and description, Power status and battery level, System connection status, Status of on board Tamper (the tamper alarm is given only once for arming).

Pressing the device name displays additional details (they vary depending on the selected device).
Pressing the row of the device panel, there will be the following information:

- PANEL NAME, HARDWARE AND FIRMWARE VERSION, DEVICE ID
- CURRENT DATE / TIME
- LAN AND GSM/3G MODULE CONNECTION STATE
- P2P CONNECTION STATE

NOTE FOR WIRELESS DEVICES

When you exit from SETUP or after a restart of the control panel, the panel waits for an update transmission from each wireless device: Therefore the indication "**Waiting for update**" is normal and will disappear once the first transmission from the device is received.



Once the first transmission has been received, the interface shows some information on the quality of the communication (Figure 19):

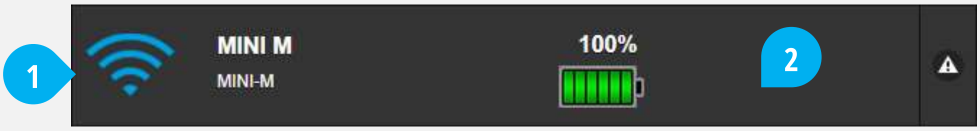
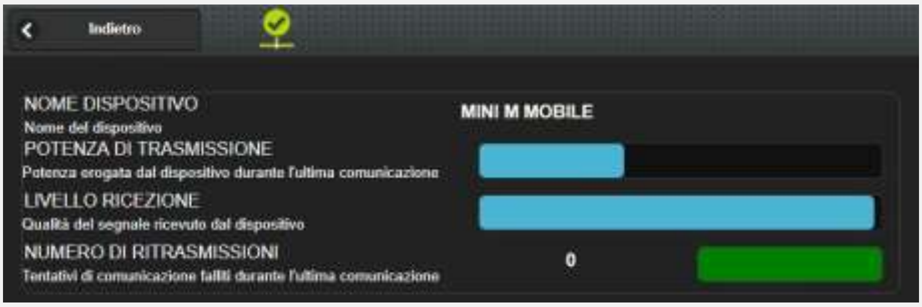


Figure 19 – Wireless devices status

The main icon (Figure 19-1) shows the **level of the radio signal** received from the control panel.

Pressing on the device line (Figure 19-2) the details of the radio transmission are displayed:



NOME DISPOSITIVO
Nome del dispositivo
MINI M MOBILE

POTENZA DI TRASMISSIONE
Potenza erogata dal dispositivo durante l'ultima comunicazione

LIVELLO RICEZIONE
Qualità del segnale ricevuto dal dispositivo

NUMERO DI RITRASMISSIONI
Tentativi di comunicazione falliti durante l'ultima comunicazione
0

- The **transmission power** level bar represents the power at which this device has transmitted in the last communication. The level increases as the distance between the control panel and the device increases and/or the communication gets worse.
- The **reception level** bar represents the level of signal received by the devide (and transmitted by the control panel) in the last communication. The level decreases as the distance between the control panel and the device increases and/or the communication gets worse.
- The **Transmissions Number** (0 ÷ 4) indicates how many times the device had to repeat the transmission before obtaining a reply from the control panel in the last communication.

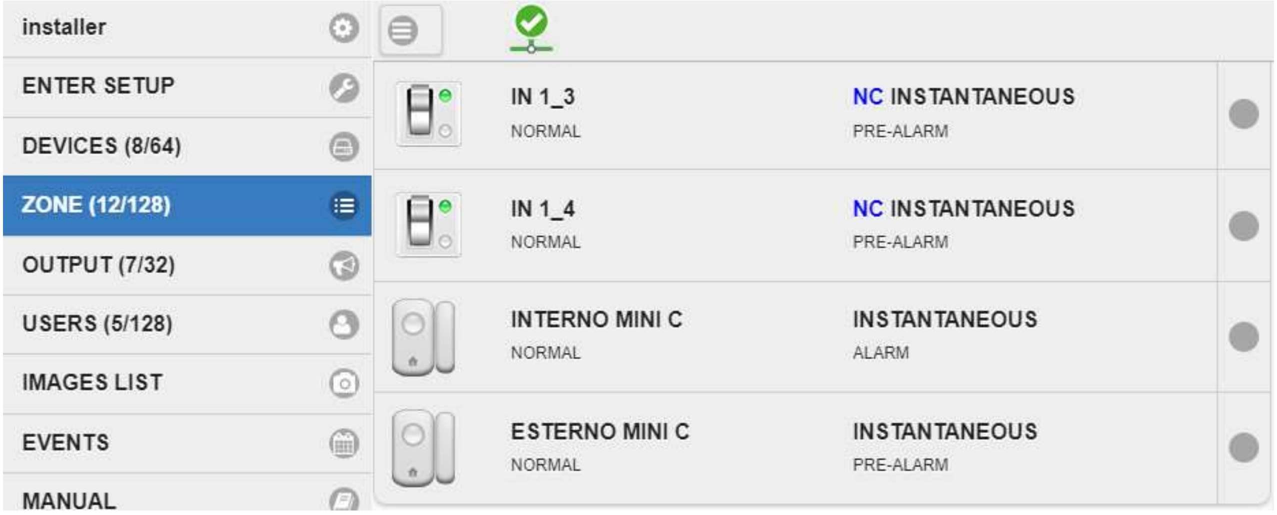
  The **green bar** lights up every time the panel receives a transmission from the device.

The ideal communication condition is when the RECEPTION LEVEL is high, the TRANSMISSIONS POWER is low and the TRANSMISSION NUMBER is zero. It is advisable to place the wireless devices (including the control panel) in a position that optimizes communication.

6.2.2 ZONES MENU

It shows all the wired and wireless zones in the system and their status in real time (Figure 20).

For each zone is shown: name and description, status in real time, programmed operating mode, type of alarm generated



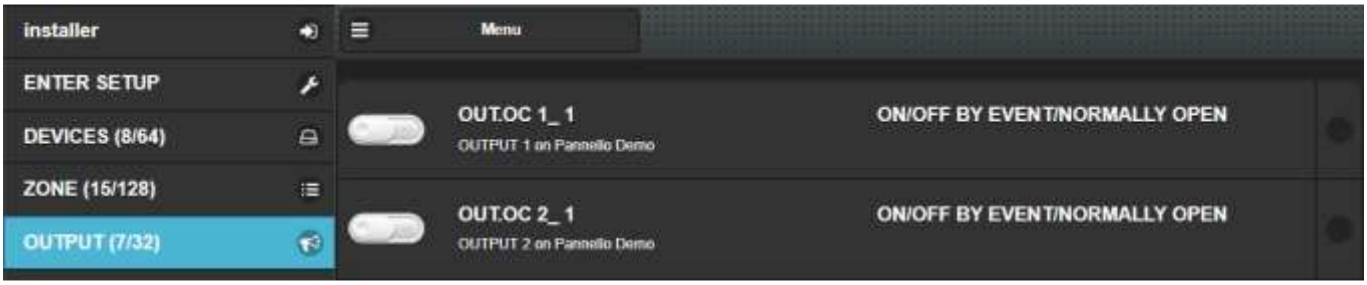
IN 1_3 NORMAL	NC INSTANTANEOUS PRE-ALARM	●
IN 1_4 NORMAL	NC INSTANTANEOUS PRE-ALARM	●
INTERNO MINI C NORMAL	INSTANTANEOUS ALARM	●
ESTERNO MINI C NORMAL	INSTANTANEOUS PRE-ALARM	●

Figure 20 – ZONE panel (Normal mode)

IF A ZONE SIGNALS MORE THAN 5 TIMES AN ALARM - DURING THE SAME INSERTION OF THE AREA - IT IS AUTOMATICALLY EXCLUDED (THE AREA REMAINS ARMED AND WILL ALARMS FROM THE OTHER ZONES).

6.2.3 OUTPUTS MENU

It shows all the outputs in the system and their status in real time (Figure 21). For each output is shown: name and description, status in real time, programmed operating mode. It is possible to trigger outputs with a click (test outputs)



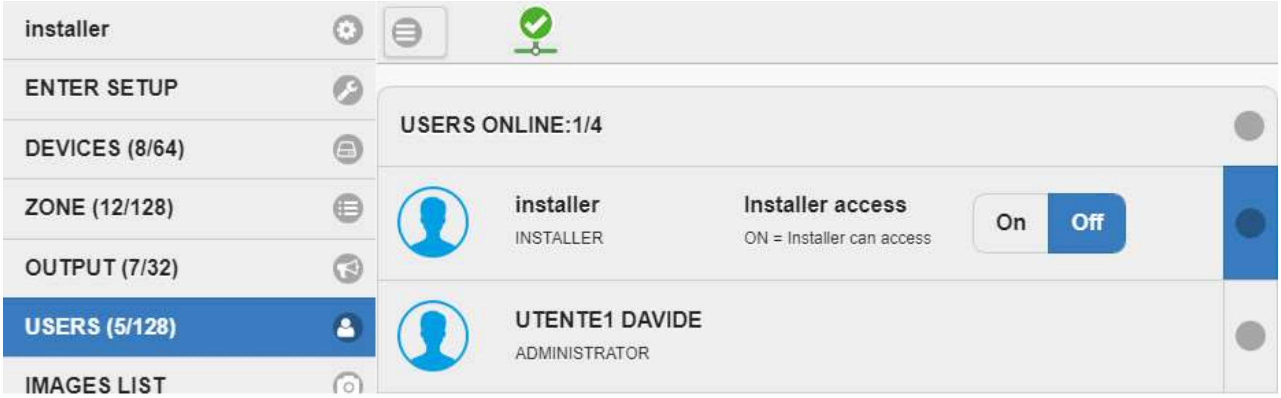
OUT.OC 1_ 1 OUTPUT 1 on Pannello Demo	ON/OFF BY EVENT/NORMALLY OPEN	●
OUT.OC 2_ 1 OUTPUT 2 on Pannello Demo	ON/OFF BY EVENT/NORMALLY OPEN	●

Figure 21 – OUTPUTS panel (Normal Mode)

6.2.4 USERS MENU

It shows the complete list of Users stored in the control panel. The INSTALLER user is always present and can be enabled for remote access via **ON / OFF** command switch. It is possible to see in real time how many and which users are connected to the control panel.

The Administrator can also disable other Normal users through an **ON/OFF** command switch.



USERS ONLINE:1/4

installer INSTALLER	Installer access ON = Installer can access	On Off
UTENTE1 DAVIDE ADMINISTRATOR		

6.2.5 IMAGE LIST MENU

It shows the complete list of events with images of the cameras currently stored in the control panel.

Under "IMAGE CAPTURING STATUS" are shown in real time the phases of images capture by the panel.

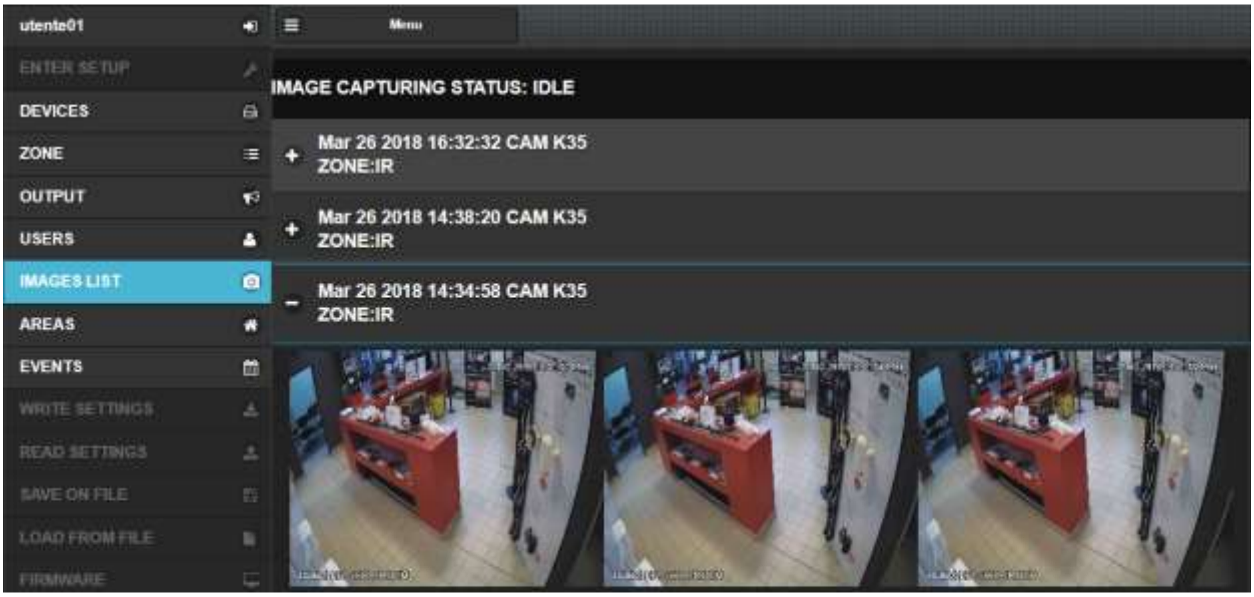


IMAGE CAPTURING STATUS: IDLE

+ Mar 26 2018 16:32:32 CAM K35 ZONE:IR

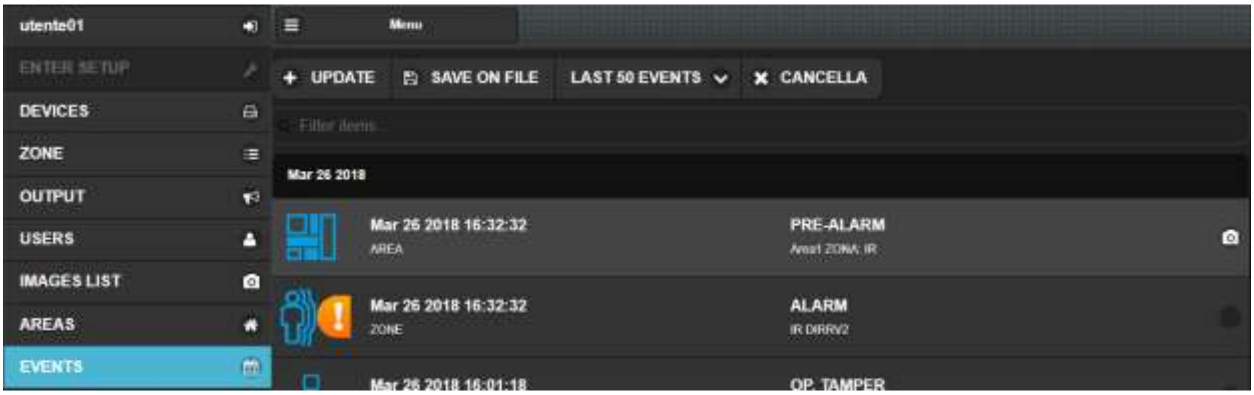
+ Mar 26 2018 14:38:20 CAM K35 ZONE:IR

– Mar 26 2018 14:34:58 CAM K35 ZONE:IR

6.2.6 EVENTS MENU

It shows the complete list of all the panel's events (max 5000).

This list can be exported to a CSV file pressing the button "**SAVE ON FILE**".



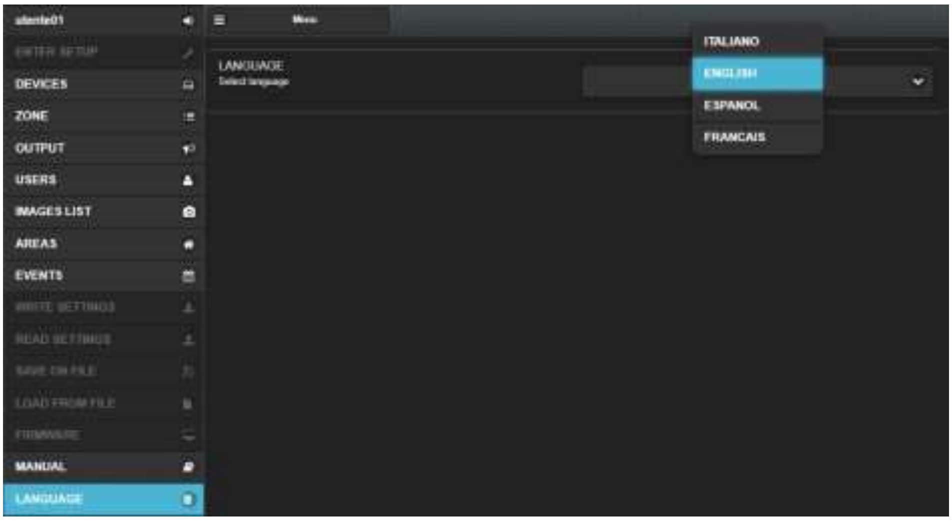
Mar 26 2018

Mar 26 2018 16:32:32 AREA	PRE-ALARM Area1 ZONA: IR	
Mar 26 2018 16:32:32 ZONE	ALARM IR DIRRV2	
Mar 26 2018 16:01:18	OP. TAMPER	

6.2.7 LANGUAGE MENU

It allows changing the language of the programming graphical interface.

NOTE: The language of the control panel firmware must be changed in SETUP mode.



LANGUAGE
Select language

6.3 SETUP MODE

IT IS NOT POSSIBLE TO ENTER IN THE SETUP IF THE CONTROL PANEL IS ARMED (ANY ARMING)

This is the starting point for the installation: here you can configure the whole system.

To switch to the **SETUP MODE**, open the side menu and press the "**ENTER SETUP**" button (Figure 17-2):

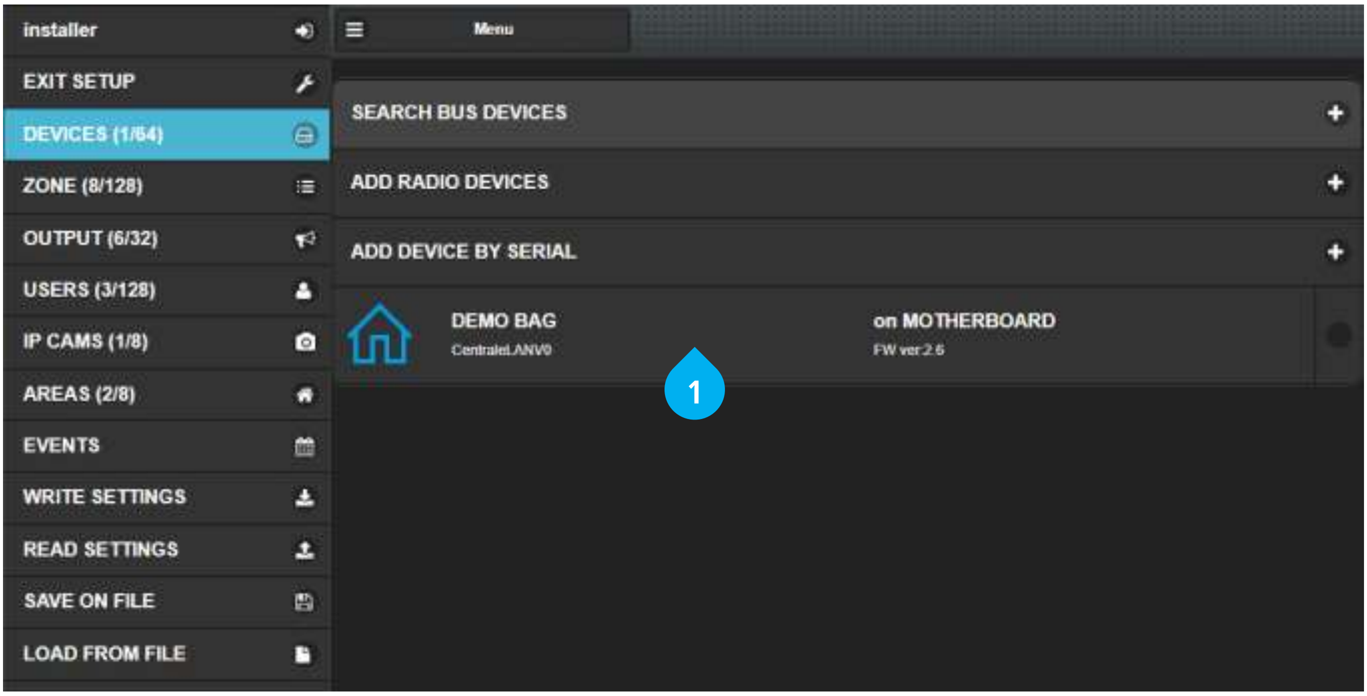


Figure 22 – Installer window in SETUP MODE

To return to the NORMAL MODE, press the "**EXIT SETUP**" (Figure 22).

WHEN YOU PASS IN SETUP, THE CENTRAL ENTERS IN MAINTENANCE.
IT IS NOT POSSIBLE TO ARM / DISARM THE SYSTEM.
THE KEYPADS DISPLAY "MAINTENANCE".
TAMPER AND SUPERVISION CONTROLS ARE DISABLED.
RADIO SIGNALS ARE IGNORED (EXCEPT IN CASE OF PROGRAMMING).

The following chapters describe in detail the use of SETUP options to configure the control panel and the devices connected to it.

7 INSTALLATION - PROGRAMMING STEPS

To program the control panel it is necessary to log in as **INSTALLER** and enter **SETUP** mode.

HOW TO PROGRAM THE PANEL

The control panel is programmed by creating / adding and then combining in the **AREAS** the **OBJECTS**¨ which are:

- CONTROL PANEL
- DEVICES ON BUS *: keypads with display, key readers, sirens, expansion cards (see par. 7.2 - DEVICES ON BUS)
- RADIO DEVICES *: sensors, remote, sirens (see par. 7.3 - WIRELESS SENSORS AND PERIPHERALS)
- ZONES (WIRED OR RADIO) (see par. 7.4 - ZONES)
- OUTPUTS (see par. 7.5 - OUTPUTS)
- USERS ** (see par. 7.6 - USERS)
- IP CAMERAS (see par. 7.7 - IP CAMERAS)
- CONTACT-ID (see par. 7.8 - CONTACT-ID)
- AREAS / SECTORS (see par. 7.9 - AREAS)

The control panel - of course - is the basic device. Initially it has:

- n. 1 user of the INSTALLER type (user name: installer; password: admin)
- n. 8 wired inputs (inputs **IN1**, ..., **IN8** on the control panel)
- n. 6 outputs (outputs **OUT1**, ..., **OUT4**, **SIREN** [**+S**, **+C**], **RELAY** [**C**, **NC**, **NO**] on the control panel)
- n. 1 GSM / 3G module (optional depending on version)

* When adding a device, the related components are added:

ESP8-BUS (wired zone expansion card):	8 zones	+	2 outputs
ESP-R (433.92 MHz wireless zone expansion cards):	8 zones	+	2 outputs
LET-485 (transponder key reader):	1 activator		
DVT-LCD/OLED (keypad with display):	1 activator	+	1 zone
MINI-M (radio contact):	1 zone		
MINI-C (radio contact):	2 zones		
DIRRV2 (Indoor infrared):	1 zone		
VIPER/EWALL/KAPTURE (outdoor sensors):	1 zone		
MOSKITO (outdoor sensor):	3 zones		

** When creating a user, you can add:

- Access codes for keypads (mod. **DVT-LCD** / **DVT-OLED**) and app (**CE-Lan Connect**)
- Remote control mod. **TX6C**
- Transponder key mod. **CHT2**

PROGRAMMING ORDER

To easily program the control panel, it is advisable to carry out the following operations in order:

- Make all necessary wiring (power supply, connections to peripherals, LAN connection,...)
- Access as "INSTALLER" and enter "SETUP": scan the BUS485 and add the radio devices
- Set the general parameters of the control panel (LAN settings, mail services, 3G, supervision...)
- Set the wired and radio zones (name, operating mode,...), and the outputs
- Create and configure users (add remote controls and transponder keys, alerts,...)
- Create the AREAS and the related SECTORS, complete the configuration of the other settings (entry / exit times, alarms,...)
- Exit the SETUP ("EXIT SETUP" button)

READ THE SETTINGS FROMS THE PANEL

To load the current panel settings, press the button "**READ SETTINGS**".

When you **ENTER IN SETUP** the current configuration is automatically loaded.

! APPLY THE CHANGES !

After **each** modification it is **necessary** to write the settings ("**WRITE SETTINGS**") so that they are stored in the control panel memory (otherwise they will be lost).

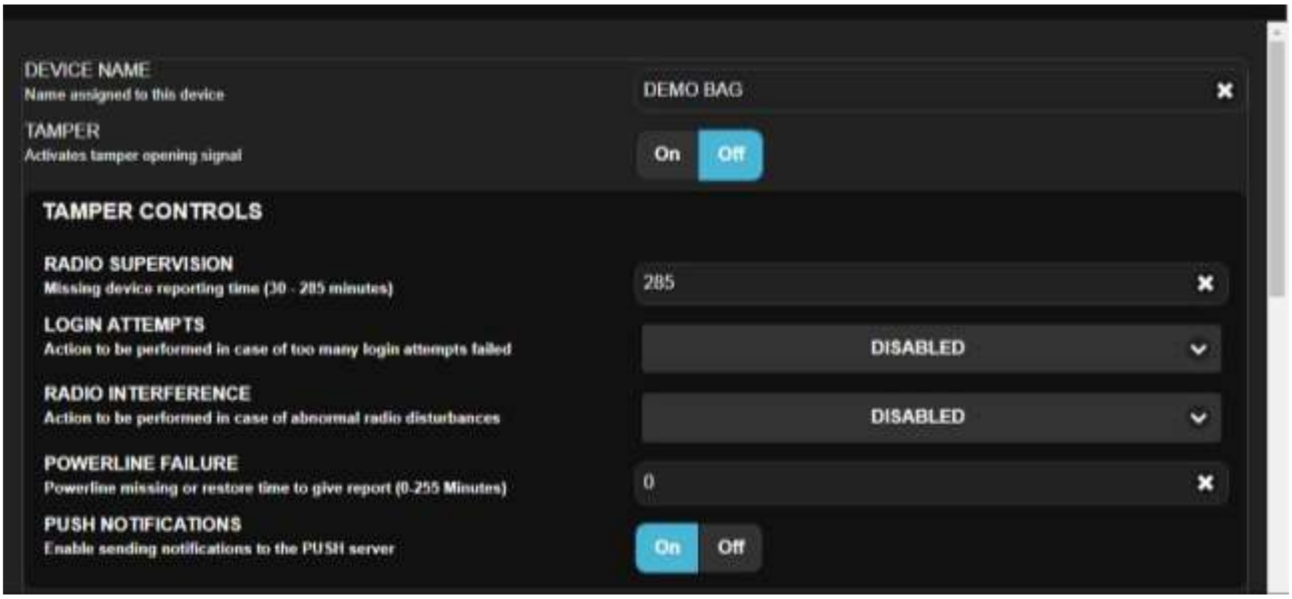
! EXIT THE SETUP !

THE NEW SETTINGS HAVE EFFECT ONLY IF WRITTEN ON THE PANEL BEFORE TO EXIT FROM THE SETUP MODE.

EXITING FROM THE SETUP, THE PANEL WILL BE COMPLETELY OPERATIONAL ONLY AFTER THE UPDATE OF THE STATE OF ALL THE PERIPHERALS.
WAIT MAX. 15 MINUTES OR MANUALLY TRIGGER THE RADIO DEVICES.

7.1 PANEL SETTINGS

To set the general functions of the control panel, select the DEVICE MENU and press on the name of the control panel (Figure 22-1):



DEVICE NAME
Name assigned to this device
DEMO BAG ✖

TAMPER
Activates tamper opening signal
On [✓ Off]

TAMPER CONTROLS

RADIO SUPERVISION
Missing device reporting time (30 - 285 minutes)
285 ✖

LOGIN ATTEMPTS
Action to be performed in case of too many login attempts failed
DISABLED

RADIO INTERFERENCE
Action to be performed in case of abnormal radio disturbances
DISABLED

POWERLINE FAILURE
Powerline missing or restore time to give report (0-255 Minutes)
0 ✖

PUSH NOTIFICATIONS
Enable sending notifications to the PUSH server
[✓ On] Off

Figure 23 – Global settings of the CONTROL PANEL (partial image)

- DEVICE NAME: Name that identifies the control panel, and appears in the device list, in any notification and in the events.
- TAMPER: enable / disable the tamper on the control panel. The tamper alarm is given ONLY OE TIME for each arming.
  The TAMPER of the control panel is also controlled by the **T.DIS** jumper (see diagram Figure 1).
- TAMPER CONTROLS

RADIO SUPERVISION	Maximum time of absence of communication with a supervised radio device, beyond which it reports missing supervision (alarm). Values: 30 ÷ 285 minutes

LOGIN ATTEMPTS	It sets the action to be performed in case of over 10 incorrect access attempts (via web / app or on the keypad): ▪ DISABLED: no action (unlimited number of attempts) ▪ ONLY E-MAIL / SMS NOTIFICATION: send E-MAIL / SMS (to enabled users) In the other cases, the control is activated both on keypads and via web / app: there are 10 attempts; if the maximum number is exceeded, access is blocked for 90 seconds. The options are: ▪ NOTIFICATION + BLOCK: sends E-MAIL / SMS notifications and blocks access for 90 seconds ▪ NOTIFICATION + BLOCK + ALARM: send E-MAIL / SMS notifications, block access for 90 seconds and start the alarm (only if failed attempts from the keyboard, not from web / app)
RADIO INTERFERENCE	It sets the action to be taken in case of anomalies in radio communications (suspected attempt of radio jamming): ▪ DISABLED: no action ▪ ONLY E-MAIL / SMS NOTIFICATION: send E-MAIL / SMS notification (to enabled users) ▪ NOTIFICATION + ALARM: sends E-MAIL / SMS notification and starts the alarm
POWERLINE FAILURE	It sets the time (in minutes) after which the control panel must signal both the POWERLINE ABSENCE (blackout) and the POWERLINE RETURN. Values: 0 ÷ 255 minutes
PUSH NOTIFICATIONS	Enables / disables the sending of notifications to the PUSH server by the control panel

- LAN SETTINGS: This section is dedicated to the network parameters of the control panel.

!WARNING! SET THESE PARAMETERS CORRECTLY, OTHERWISE THE PANEL WILL NOT BE REACHED BY THE APP AND THE MAIL / PUSH NOTIFICATIONS WILL NOT BE SENT.

USE STATIC IP	By default, the control panel automatically keeps its IP address from DHCP service of the network to which it is connected. With this option it is possible to enable the use of a user-defined IP address, in the case in where the DHCP service is not available (for example: the control panel is connected directly to a PC) or you need to specify a specific IP address.
IP ADDRESS	After enabling "USE STATIC IP", it is necessary to set here the static IP address that the panel will have to use.
SUBNET MASK	After enabling "USE STATIC IP", the subnet mask must be set here.
GATEWAY	After enabling "USE STATIC IP", it is possible to set here the IP address of the router / gateway of the network. **! WARNING ! Without this reference, the panel will only be reachable within the local network (except for the use of 3G data)!**
USE GSM/3G MODULE CONNECTION	Enable this option if you want the panel to use the 3G data connection. The 3G data connection will be used when the internet connection on LAN ethernet is absent (due to a fault or not present at the installation site). Note: it is necessary to equip the GSM / 3G Module and SIM with the active data service.

- MAIL SERVICE *

This section is dedicated to the configuration of the e-mail sending service that the panel will use to send notifications by email. The required parameters can be obtained from the e-mail service provider.

! WARNING ! THESE PARAMETERS ARE EXCLUSIVELY DEDICATED TO SUPPLY TO THE PANEL A EMAIL SERVICE TO SEND EMAIL NOTIFICATION, THEREFORE YOU SHOULD NOT BE CONFUSED WITH USER EMAIL ADDRESSES (FOR WHICH SUITABLE FIELDS ARE PRESENT AT "USERS" SECTION).

SMTP SERVER ADDRESS	Mail Out Server Address (SMTP SERVER ADDRESS)
SMTP SERVER PORT	Port used by the mail out server (SMTP PORT)
SECURITY LEVEL OF THE CONNECTION	Type of connection security
AUTHENTICATION	Enable if the mail service requires authentication
USERNAME	E-mail account user name
PASSWORD	Password associated with the e-mail account
EMAIL ADDRESS	Email address of the email account
EMAIL TEST	Send a test email to the email account programmed for the email service. **ATTENTION: The test uses the parameters already stored in the control panel. After each change it is necessary to write settings on the panel before carrying out a new test**

- AUTOMATIC DATE / TIME SERVICE (SNTP)

The control panel uses online services for the date and time. These services are called SNTP (Simple Network Time Protocol) and there are several available. The control panel uses the **`ntp1.inrim.it`** server as factory default.

ENABLE AUTOMATIC TIME UPDATE	Enables / disables automatic time update via SNTP server
DATE AND TIME	It shows the current date and time of the SNTP service. By pressing "UPDATE" the control panel will update its settings from the PC / device to which you are connected instead of to the SNTP service.
SNTP SERVER	Address of the reference service for the SNTP date and time. It is possible to set up other SNTP servers by typing the reference address here.
TIME ZONE	It sets the time zone of the installation location.
DAYLIGHT SAVING TIME	Enables automatic change of time for “Daylight saving time” period.

- GSM/3G MODULE

ENABLE GSM/3G MODULE	To use the GSM / 3G module it is necessary to enable it: ▪ Enable the module then confirm ▪ Save the new setting with "Write settings" ▪ Re-enter the setting of the control panel parameters to complete the programming: wait for the module to signal "READY" before proceeding THE GSM MODULE IS ENABLED BY DEFAULT
GSM/3G MODULE MODEL	Information on the model of GSM / 3G module installed **RESET** button = reboot of the GSM module **NETWORK** button = allows manual selection of the network carrier
SIM PIN	Enter (if active on the SIM) the PIN set in the SIM. Even if the SIM PIN can be set here, it is always recommended to disable it.
MAX NUMBER OF DAILY MESSAGES	Set the maximum number of SMS messages that the panel can send in one day. This limits communication-related spending, especially in the case of reports caused by anomalies (0 = NO LIMIT).
APN	It sets the APN address to be used for the data connection of the SIM inserted in the module
MOBILE NETWORK TYPE	It sets the type of data link to be used with the SIM: ▪ AUTOMATIC: the module automatically selects the connection speed to the network based on the availability of the cell. ▪ GSM: the module uses only the GSM / GPRS connection ▪ 3G: the module uses only the 3G / UMTS connection

- VOCAL MESSAGES SERVICE (TEXT TO SPEECH)

  ! WARNING ! THIS FUNCTION IS AVAILABLE ONLY IN ITALIAN LANGUAGE AND IS PRESENT ONLY IF THE MODULE IS ENABLED AND PROVIDED FOR TTS FUNCTIONS (ONLY ON SOME MODELS) AND.

ENABLE TTS	Enables / disables the use of the TTS for the telephone call. If disabled, the module will perform a mute call
FIXED VOICE MESSAGE	The text written in this box will be read at the end of each voice call that the control panel will make to the phone numbers enabled. Typically this text is reserved to indicate the physical address of the place where it is installed to give indication to the rescue services (ex. police).
TEST MESSAGGIO VOCALE	To use the message test, connect a speaker to the audio connector of the module. Pressing the "PLAY" button the control panel reads the message: in this way it is possible to correct the written text in the case the message is not understandable.

! NOTES ON INTERNET LAN AND 3G CONNECTIONS!

The **primary** Internet connection is the **LAN** (the local network to which the control panel is connected through the LAN1 / LAN2 Ethernet ports). The local network must provide the panel **internet connection**, necessary for remote access and communications (e-mail, push) - otherwise the panel can only be reached locally.

If there is no internet connection in the local network (because it is not present or due to a fault), it is possible to use the **3G data connection**, provided that:

1. The 3G module is present and activated
2. In the 3G module, a **SIM** with a data connection plan including a data connection is inserted
3. The **APN** of the mobile network operator must be set in the configuration of the 3G module
4. In the "LAN SETTINGS" configuration of the control panel the "**USE GSM/3G MODULE CONNECTION**" control must be enabled

In this configuration, if the internet connection on the LAN is missing, the control panel automatically switches to the 3G data connection. If the internet connection on the LAN is restored, the control panel automatically quits the 3G data connection.

In places where there is no internet connection via LAN, the panel will work only with 3G connection.

To find out the connection status, go to "DEVICES" and press the control panel (the status screen of the control panel opens, which includes connection information).

7.2 DEVICES ON BUS

Before connecting the devices on BUS, assign to each one **a different address** (from those of the same family: the keypads have their own numbering, the transponder key readers another independent numbering, and so on...).

At the first start-up of the control panel or after adding / removing BUS devices to the control panel, a "**SEARCH BUS DEVICES**" must be performed (Figure 24-1): the control unit checks the devices present and creates or updates the **LIST** (Figure 24-2).

The search is performed on both **BUS1** (terminals **VBS1**, **A1**, **B1**, **-VS**) and **BUS2** (terminals **VBS2**, **A2**, **B2**, **-VS**).

The panel will only use the devices listed here (always remember to WRITE SETTINGS).

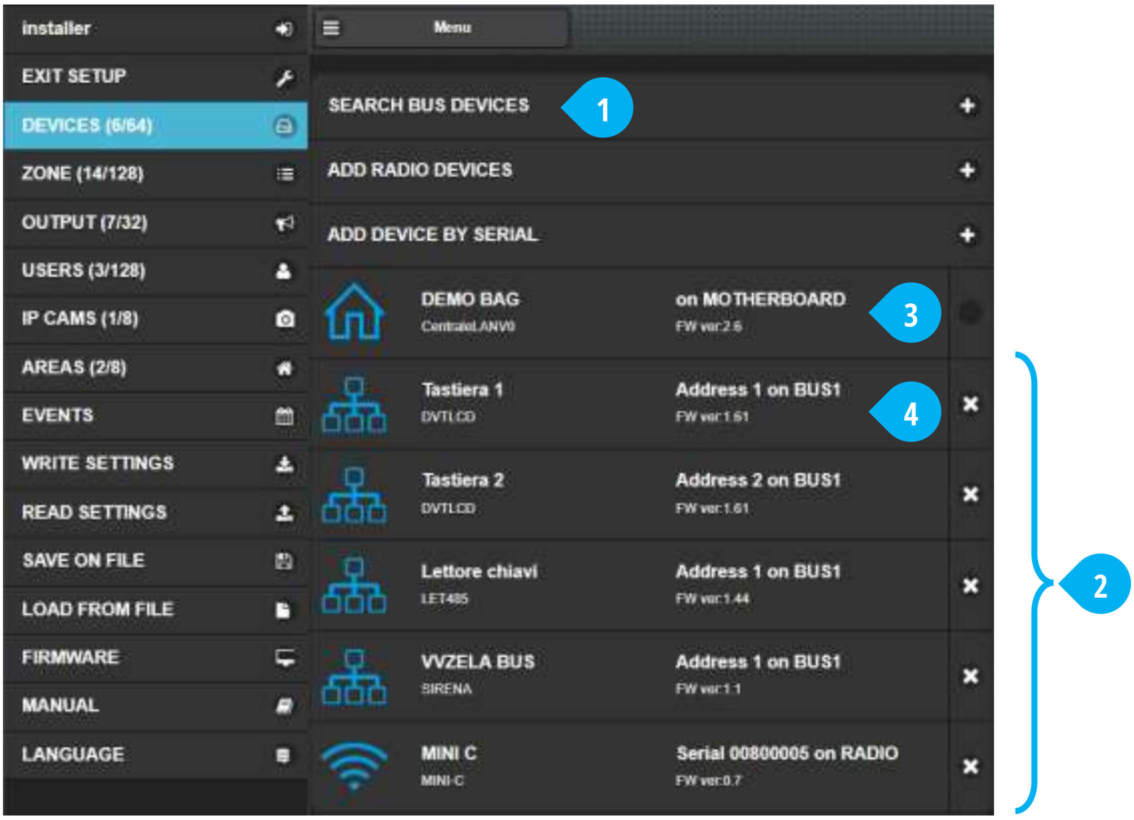


Figure 24 – Adding devices on BUS485

If a BUS device does not appear in the list, check:

- links (missing or incorrect connection)
- connected devices (power on status, error messages, addressing...)
- any conflicts with other devices
- the compatibility of the device with the control panel (hardware and firmware version)
- total absorption on the BUS (must not exceed 450 mA per BUS!)

After checking and resolving the problem, repeat the BUS scan.

The list shows the device **information bar** (Figure 24-3 e 4):

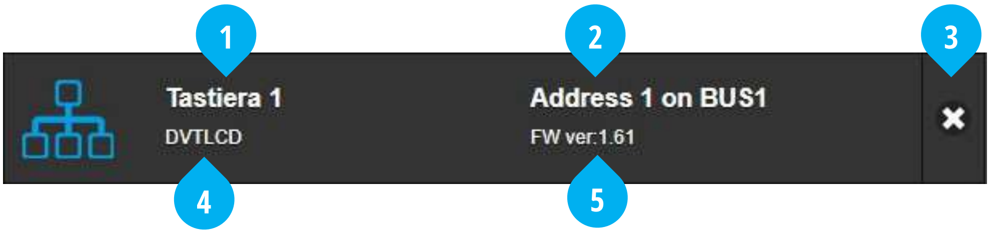
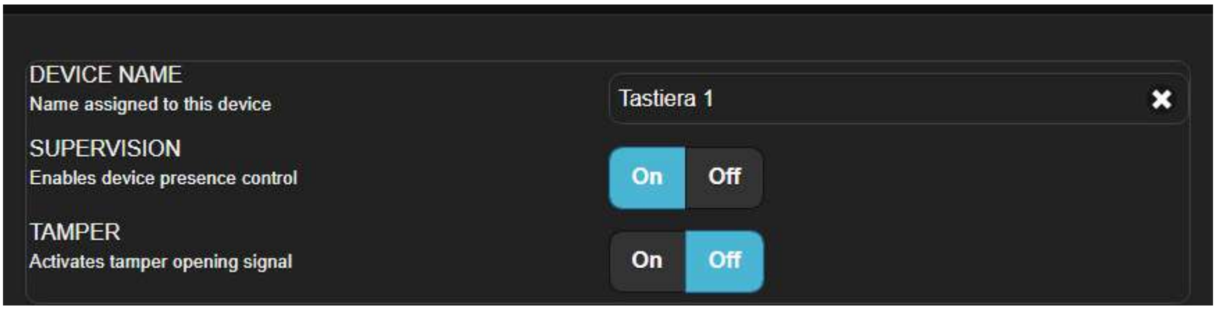


Figure 25 – Device information bar

where:

1	Name assigned (see note below)	4	Model
2	Address and BUS connected to (BUS1 / BUS2)	5	Firmware version
3	Delete from the list		

Touching the information bar opens the control of some parameters of the device:



DEVICE NAME
Name assigned to this device
Tastiera 1 ✖

SUPERVISION
Enables device presence control
[✓ On] Off

TAMPER
Activates tamper opening signal
On [✓ Off]

Figure 26 – Settings options of a BUS device

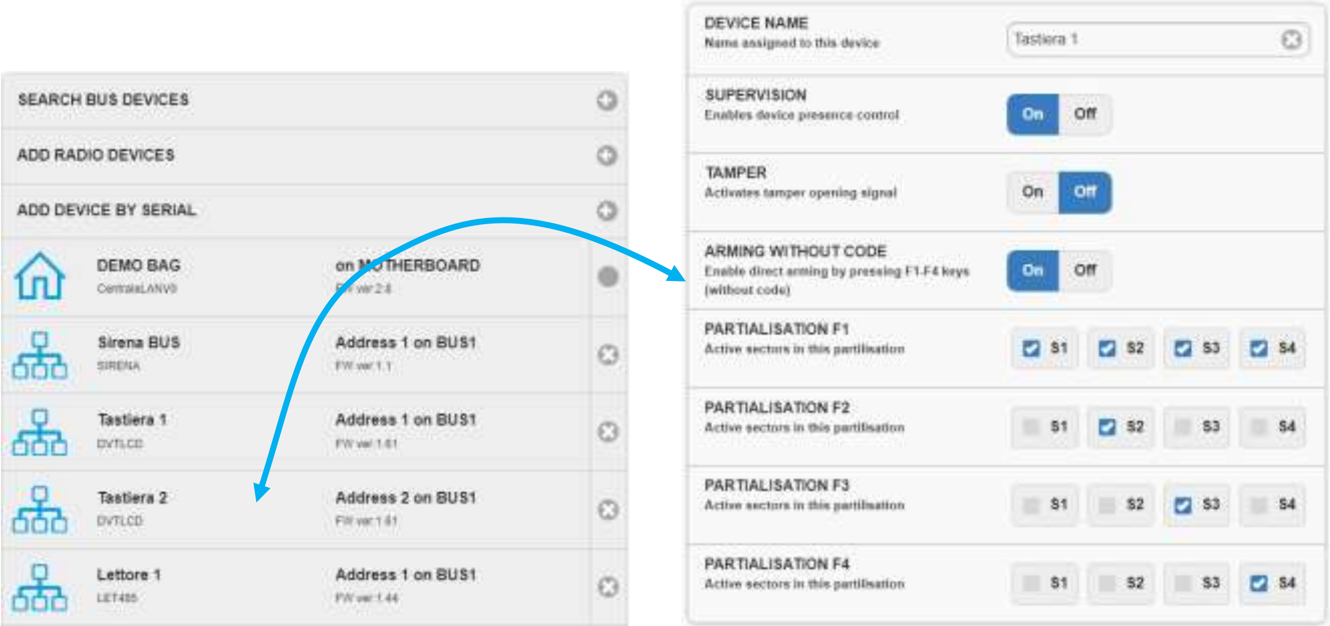
The available options vary depending on the type of device (see the paragraphs dedicated to each device).
Some settings can be programmed directly on the device (ex. via dip-switches or jumpers), depending on the connection or through other control functions of the control panel.

> Note on the device name: the same name is assigned to all similar devices by default (ex. the keypads are all named "DVTLCD / OLED"). It is recommended to assign suitable names to distinguish the various devices.

> **THE TAMPER AND MASKING ALARMS ARE GIVEN ONLY ONE TIME FOR EACH ARMING.**

7.2.1 PROGRAMMING QUICK ARM FOR A KEYPAD

Press on the line relative to the keypad to be programmed to access the settings window (Figura 27).



SEARCH BUS DEVICES
ADD RADIO DEVICES
ADD DEVICE BY SERIAL

DEMO BAG CentraleLANV9	on MOTHERBOARD FW ver 2.8	
Sirena BUS SIRENA	Address 1 on BUS1 FW ver 1.1	
Tastiera 1 DVTLCD	Address 1 on BUS1 FW ver 1.61	
Tastiera 2 DVTLCD	Address 2 on BUS1 FW ver 1.61	
Lettore 1 LET485	Address 1 on BUS1 FW ver 1.44	

DEVICE NAME
Name assigned to this device
Tastiera 1

SUPERVISION
Enables device presence control
[✓ On] Off

TAMPER
Activates tamper opening signal
On [✓ Off]

ARMING WITHOUT CODE
Enable direct arming by pressing F1-F4 keys (without code)
[✓ On] Off

PARTIALISATION F1
Active sectors in this partialisation
☑ S1 ☑ S2 ☑ S3 ☑ S4

PARTIALISATION F2
Active sectors in this partialisation
□ S1 ☑ S2 □ S3 □ S4

PARTIALISATION F3
Active sectors in this partialisation
□ S1 □ S2 ☑ S3 □ S4

PARTIALISATION F4
Active sectors in this partialisation
□ S1 □ S2 □ S3 ☑ S4

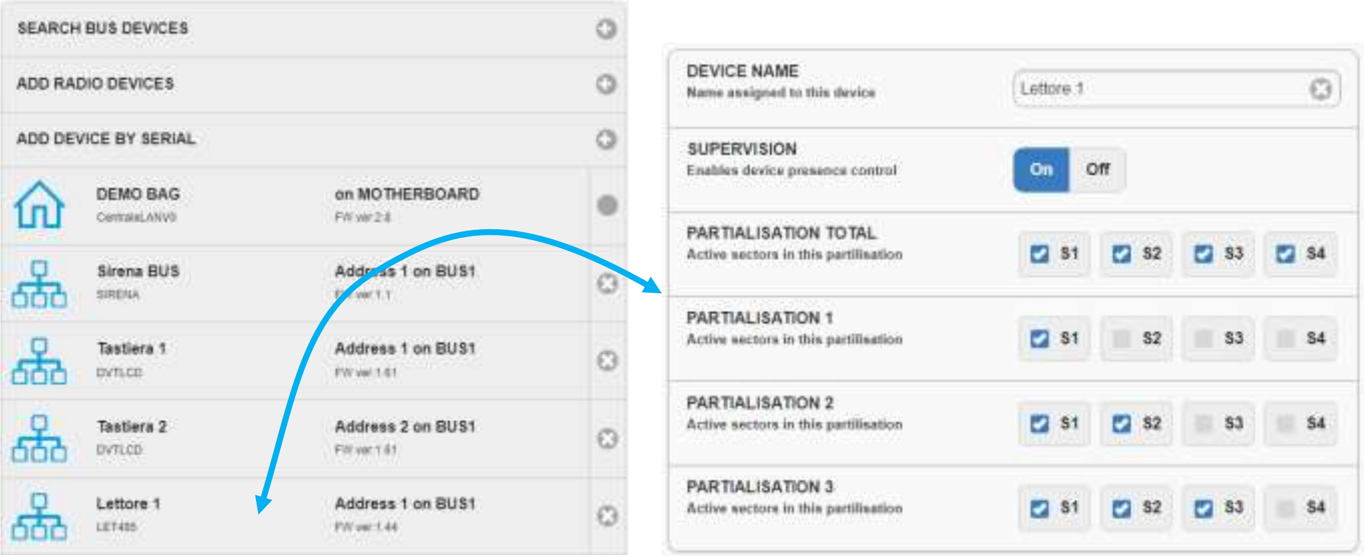
Figura 27 – Setting of the quick arm from Keypad

Here it is possible to enable "ARMING WITHOUT CODE" and to program the partializations of the sectors of the area, which will be carried out by pressing the F1-F4 buttons directly on the keyboard, without having to insert any user code.

7.2.2 PROGRAMMING PARTIALIZATIONS FOR A TAG READER

Press on the line relative to the tag reader to be programmed to access the settings window (Figura 28).

Here it is possible to program the partialisations of the area sectors, which will be executed when the user approaches his key to the reader and selects one of the Partialisations (the Partialisations are displayed by the reader in a cyclic sequence: TOTAL> PARTIAL1> PARTIAL2> PARTIAL3> OFF , with "beeps" and changing the color of the LED: RED> GREEN> BLUE> BLUE> OFF)



DEMO BAG CentraleLANV0	on MOTHERBOARD FW ver 2.8
Sirena BUS SIRENA	Address 1 on BUS1 FW ver 1.1
Tastiera 1 DVTLCD	Address 1 on BUS1 FW ver 1.61
Tastiera 2 DVTLCD	Address 2 on BUS1 FW ver 1.61
Lettore 1 LET485	Address 1 on BUS1 FW ver 1.44

DEVICE NAME Name assigned to this device	Lettore 1			
SUPERVISION Enables device presence control	On	Off		
PARTIALISATION TOTAL Active sectors in this partilisation	☑ S1	☑ S2	☑ S3	☑ S4
PARTIALISATION 1 Active sectors in this partilisation	☑ S1	□ S2	□ S3	□ S4
PARTIALISATION 2 Active sectors in this partilisation	☑ S1	☑ S2	□ S3	□ S4
PARTIALISATION 3 Active sectors in this partilisation	☑ S1	☑ S2	☑ S3	□ S4

Figura 28 – Setting the key reader partialisations

7.3 WIRELESS SENSORS AND PERIPHERALS

To add sensors or other radio devices press "**ADD RADIO DEVICES**" (Figure 29-1, the control panel goes into learning) or "**ADD DEVICE BY SERIAL**" (Figure 29-2).

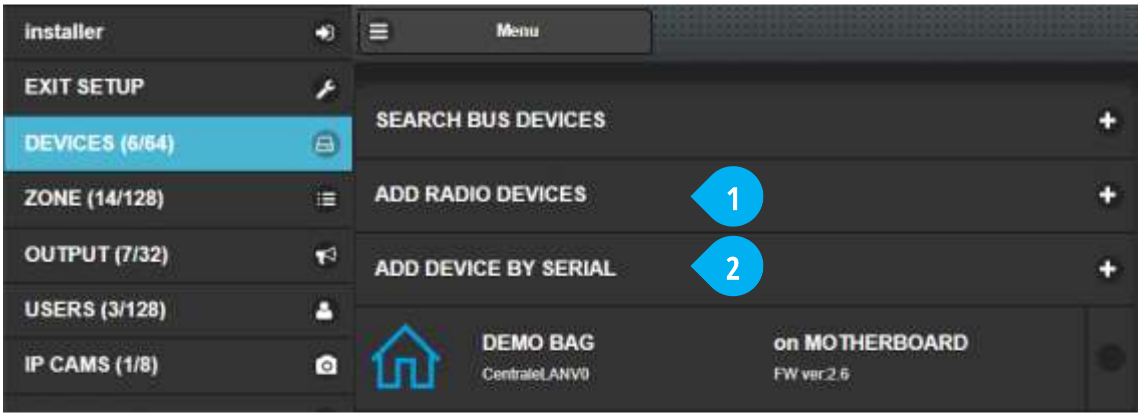


Figure 29 – Adding radio devices

7.3.1 ADD RADIO DEVICES

It opens the window that wait for the radio transmission code by the device (Figure 30). Transmit the learning code from the device to store - after putting it in PROGRAM MODE (refer to the manual of the device).

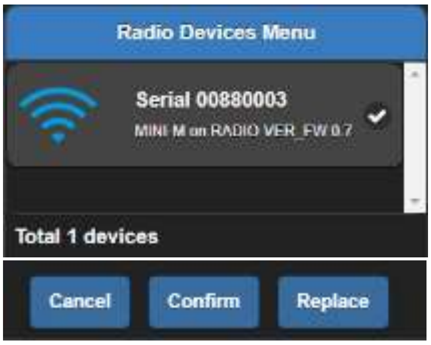


Figure 30 – Window of adding radio devices

To confirm the addition of the devices received and displayed in the control window, press the "**Confirm**" key

After adding a device to the list, you can click on the device to modify some parameters (other settings are available directly on the device, depending on the connections or accessories or controlled by the panel functions).

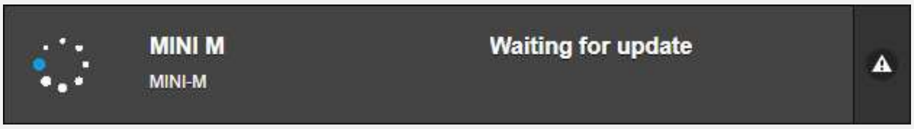
To **replace** a radio device already learned with a new one of the same type, perform the learning as above, press the "**Replace**" key and then select the device to be replaced. The new device will inherit all settings of the replaced one.

! WARNING. TO USE THE REMOTE CONTROL IT'S MANDATORY TO UPDATE PANEL TO FIRMWARE AT LEAST V.2.6.18 !

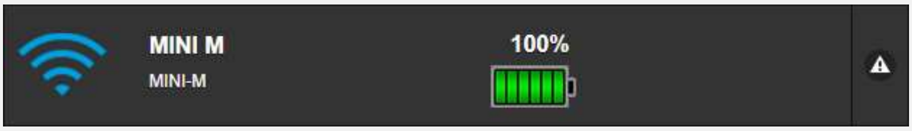
! CAUTION. ONCE STORED, THE RADIO DEVICE MUST BE RETURNED IN NORMAL MODE (NOT PROGRAM MODE), OTHERWISE IT WILL NEVER TRANSMIT ITS STATUS.

! NOTE ON THE STATUS OF RADIO DEVICES !

When you exit from SETUP or after a restart of the control panel, the panel waits for an update transmission from each wireless device:

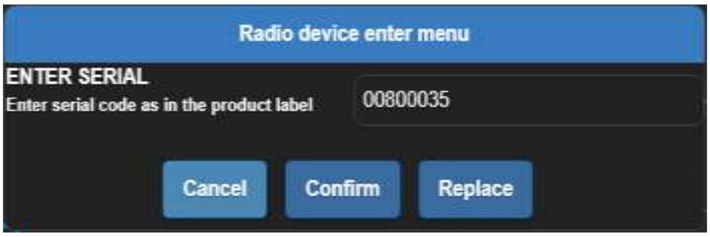


Once the first transmission has been received, the interface shows information of the device:



7.3.2 ADD RADIO DEVICE BY SERIAL

The window for entering the device serial number opens (Figura 31).



Radio device enter menu

ENTER SERIAL
Enter serial code as in the product label: 00800035

Figura 31 – Window for adding devices by serial code

Enter the serial code found on the package or label of the device and press "**Confirm**".

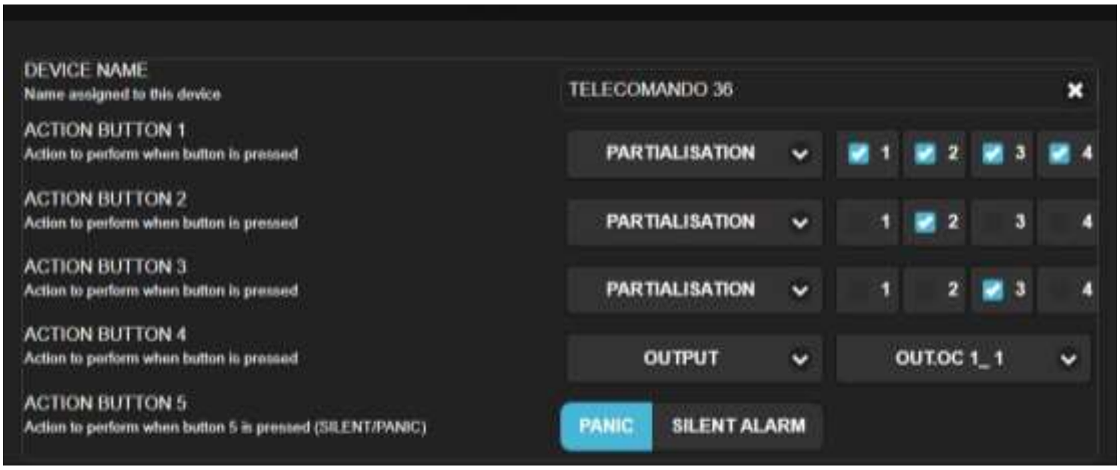
If the serial is correct, the new device is added to the list.

To **replace** a previously stored radio device with a new one of the same type, type the serial code as above, press "**Replace**" then select the device to be replaced.

! CAUTION: IT IS NOT POSSIBLE TO ADD BIDIRECTIONAL REMOTE CONTROL WITH THE SERIAL NUMBER!
TO USE THE REMOTE CONTROL IT'S MANDATORY TO UPDATE PANEL TO FIRMWARE AT LEAST VERSION 2.6.18 !

7.3.3 PROGRAMMING OF REMOTE CONTROL BUTTONS

Press on the row of the remote control to be programmed to access the window of programmable button settings.



DEVICE NAME
Name assigned to this device: TELECOMANDO 36 ✖

ACTION BUTTON 1
Action to perform when button is pressed: PARTIALISATION ☑ 1 ☑ 2 ☑ 3 ☑ 4

ACTION BUTTON 2
Action to perform when button is pressed: PARTIALISATION □ 1 ☑ 2 □ 3 □ 4

ACTION BUTTON 3
Action to perform when button is pressed: PARTIALISATION □ 1 □ 2 ☑ 3 □ 4

ACTION BUTTON 4
Action to perform when button is pressed: OUTPUT OUT.OC 1_1

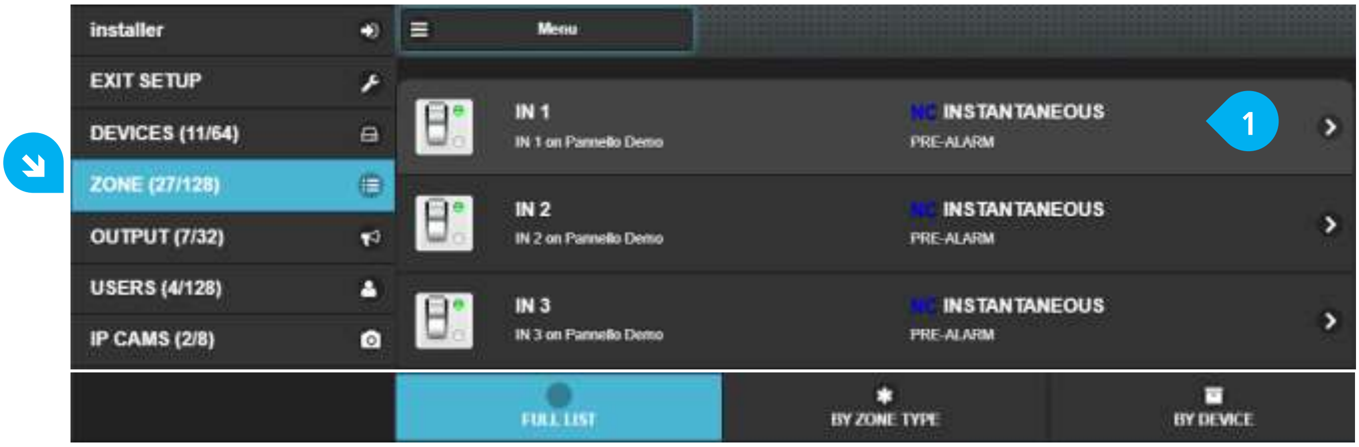
ACTION BUTTON 5
Action to perform when button 5 is pressed (SILENT/PANIC): [✓ PANIC] SILENT ALARM

Here it is possible to program the action to be performed at the direct pressure of each button 1-4. The possible options are:

- DISABLED. The button does not perform any action
- PARTIALISATION. The button performs partial arming of the Area with the selected sectors (1-2-3-4)
  NOTE: The unselected sectors will be DISARMED
- OUTPUT. The button activates the selected output

7.4 ZONES

To configure the parameters of the wired and radio zones, select "ZONE" from the side menu (Figure 32):



IN 1
IN 1 on Pannello Demo
NC INSTANTANEOUS
PRE-ALARM

IN 2
IN 2 on Pannello Demo
NC INSTANTANEOUS
PRE-ALARM

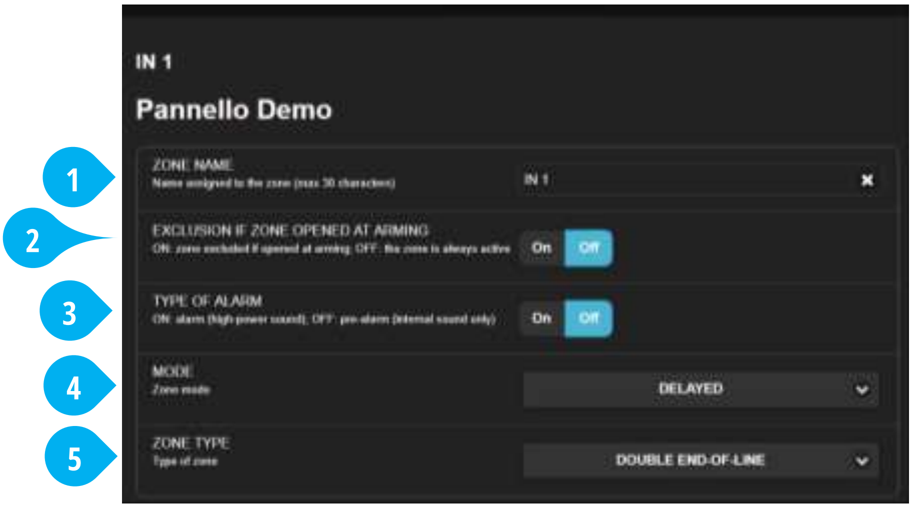
IN 3
IN 3 on Pannello Demo
NC INSTANTANEOUS
PRE-ALARM

Figure 32 – ZONES panel

> **Notes on Zones Names**
>
> The name assigned by factory / automatically to the Zones is of the type: **IN X_Y** where **X** is the position of the input inside the device, and **Y** the order number with which the device was added.
>
> It is important to change the name of the Device with one that makes it easy to identify.
>
> When changing the name to the Zones, there is a certain reference by looking at the description "name_zone ON device_name".
>
> Add the Zones in the Sectors of the Area referring only to the ZONE NAME

> **Full list / by zone type / by device**
>
> The buttons at the bottom of the zone list allow you to choose in which order to display them.

Select a zone to change its parameters (Figure 32-1).



IN 1

Pannello Demo

ZONE NAME
Name assigned to the zone (max 30 characters)
IN 1

EXCLUSION IF ZONE OPENED AT ARMING
ON: zone excluded if opened at arming. OFF: the zone is always active
Off

TYPE OF ALARM
ON: alarm (high-power sound), OFF: pre-alarm (internal sound only)
Off

MODE
Zone mode
DELAYED

ZONE TYPE
Type of zone
DOUBLE END-OF-LINE

Figure 33 – Zone configuration

1 ZONE NAME: name assigned to the zone, max 30 characters

2 EXCLUSION IF ZONE OPENED AT ARMING: it enables the bypass of the zone if found open at the time of arming (applies only to wired/wireless zones with "open door" control)

3 TYPE OF ALARM: select the zone alarm level between PRE-ALARM (low level) or ALARM (high level)

4 MODE: select the type of event that generates the zone when it is violated; the options of choice are:

- INSTANTANEOUS: it immediately generates an alarm (of the PRE-ALARM or ALARM type) when it detects.
- DELAYED: when violated, starts the Entry time before generating an alarm (of the PRE-ALARM or ALARM type). If the control panel is disarmed within the Entry time, there will be no alarm.
- SILENT ALARM: when violated there will be no warning (no sirens sound or visible signals) but the communications will start in Silent Alarm (SMS and calls to programmed numbers).
- 24H: these zones are active 24h / 24 even when the system is disarmed. These zones are intended for use with detectors such as: flooding, smoke, gas ... or to protect high-security areas (ex: safe, armoury...)
- PANIC: when violated, the sound of the sirens starts immediately to attract attention. Panic Alarm communications are sent (SMS and calls to programmed numbers).
- ACTIVATOR (PULSE) / (MONOSTABLE): these zones are used to arm / disarm the system by means of a button or key or home automation system. Each Sector in which the zone has been added is activated.
- INSTANT + CHIME: like the Instant zones; when the panel is disarmed - their detection starts an acoustic warning.
- DELAYED + CHIME: like the Delayed areas; when the panel is disarmed - their detection starts an acoustic warning.

5 ZONE TYPE: sets the type of zone (depending on the device this selection may vary):

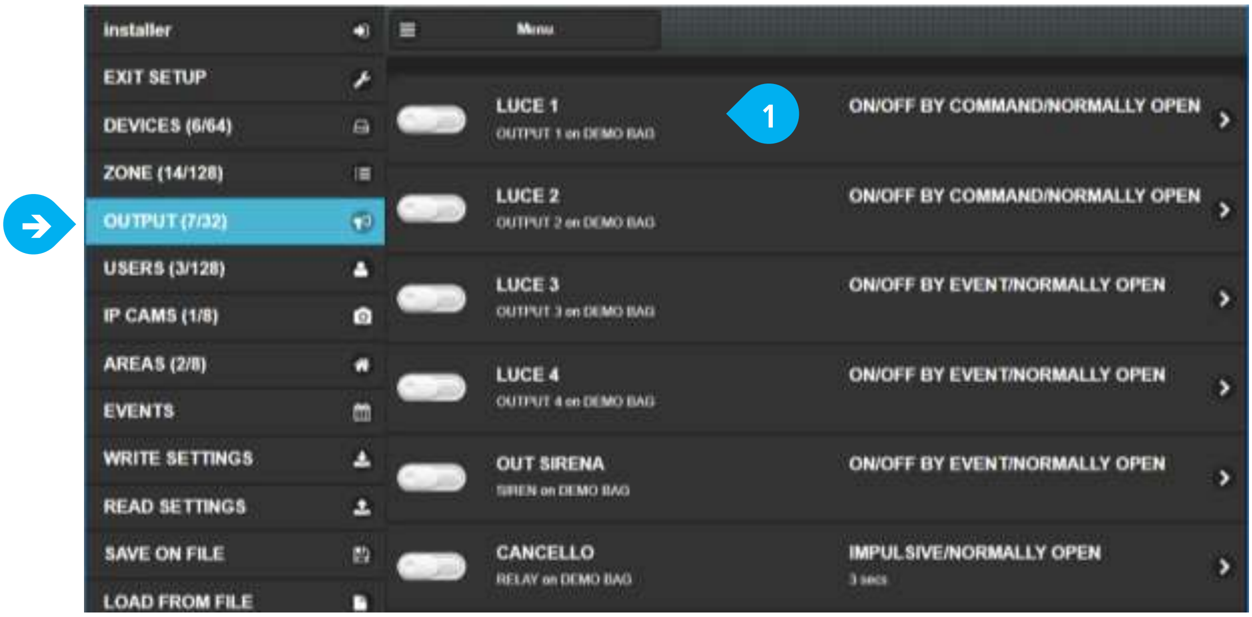
- NORMALLY OPEN: the area is at rest when it is OPEN
- NORMALLY CLOSED: the zone is at rest when it is CLOSED
- SINGLE END-OF-LINE: the zone is at rest when closed with a 2.2 kΩ line resistance; in addition to the alarm (zone open), also detects the short circuit attempt
- DOUBLE END-OF-LINE: the zone is at rest when closed with a 2.2 kΩ line resistance; in addition to the alarm (open area with line resistance of 2.2 kΩ + 12 kΩ), it also detects the tamper and the short circuit attempt

IF A ZONE SIGNALS MORE THAN 5 TIMES AN ALARM - DURING THE SAME ARMING OF THE AREA - IT IS AUTOMATICALLY EXCLUDED (THE AREA REMAINS ARMED AND WILL ALARMS FROM THE OTHER ZONES).

TAMPER ALARM (ZONES IN SINGLE AND DOUBLE END-OF-LINE) OR BY WIRED LINE TAMPER (CLAMP TMP OF PANEL AND EXPANSION BOARDS) OR SENSOR MASKING IS GIVEN ONLY ONE TIME FOR EACH ARMING.

7.5 OUTPUTS

All available outputs are in the "OUTPUTS" menu (Figure 34):



LUCE 1
OUTPUT 1 on DEMO BAG
ON/OFF BY COMMAND/NORMALLY OPEN

LUCE 2
OUTPUT 2 on DEMO BAG
ON/OFF BY COMMAND/NORMALLY OPEN

LUCE 3
OUTPUT 3 on DEMO BAG
ON/OFF BY EVENT/NORMALLY OPEN

LUCE 4
OUTPUT 4 on DEMO BAG
ON/OFF BY EVENT/NORMALLY OPEN

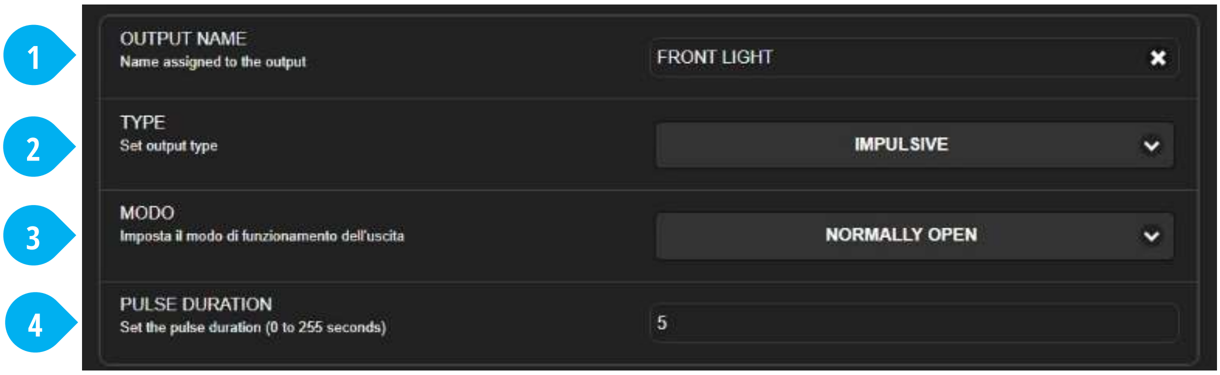
OUT SIRENA
SIREN on DEMO BAG
ON/OFF BY EVENT/NORMALLY OPEN

CANCELLO
RELAY on DEMO BAG
IMPULSIVE/NORMALLY OPEN
3 secs

Figure 34 – Outputs

The list of outputs includes the outputs on board the control panel and those added by other devices.

To change the electrical behaviour of an output, press its name (Figure 34-1):



OUTPUT NAME
Name assigned to the output
FRONT LIGHT

TYPE
Set output type
IMPULSIVE

MODO
Imposta il modo di funzionamento dell'uscita
NORMALLY OPEN

PULSE DURATION
Set the pulse duration (0 to 255 seconds)
5

Figure 35 – Output: settings

1 OUTPUT NAME: assign a name to the output.

2 TYPE: sets the logic behaviour of the output when activated by an event.

- ON/OFF BY EVENT: the output follows the event to which it is associated, it remains active as long as the event remains
- ON/OFF BY COMMAND: the output changes state on manual command by the APP or remote control
- IMPULSIVE: the output activates for the programmed number of seconds when the event occurs, then returns to rest even if the event continues

3 MODE: set the electrical state at rest of the output, normally open or normally closed

4 PULSE DURATION: (only for IMPULSIVE type outputs): set for how long - starting from the associated event - the output remains active. The time can be set from 0 to 255 seconds

FOR THE PROGRAMMING OF THE EVENT THAT ACTIVATES AN OUTPUT, SEE THE PROGRAMMING OF THE AREAS.

7.6 USERS

To add / edit / delete users select "USERS" from the side menu (Figure 36):

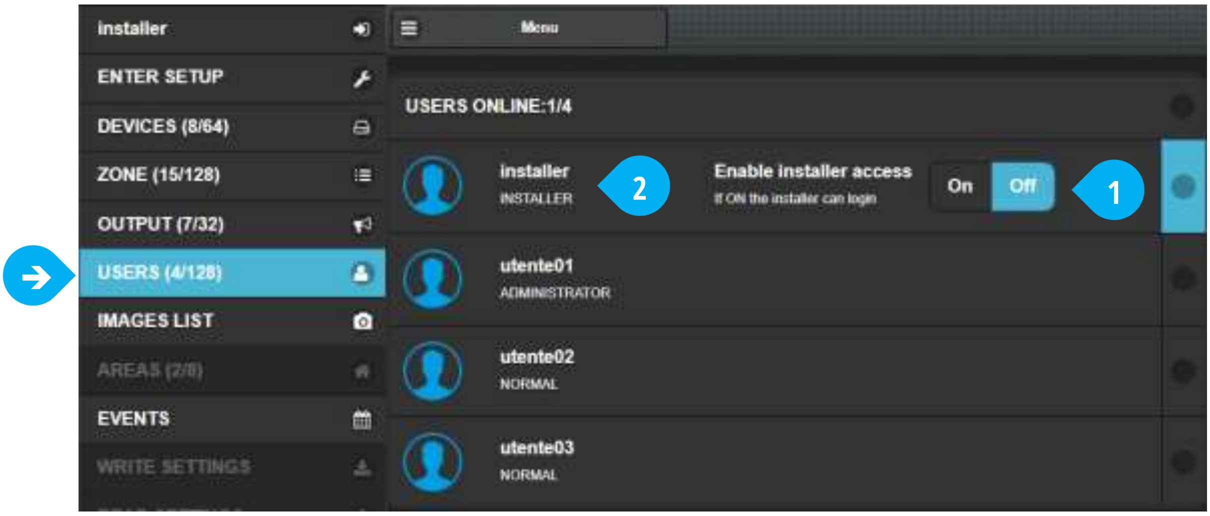


Figure 36 – USERS Panel

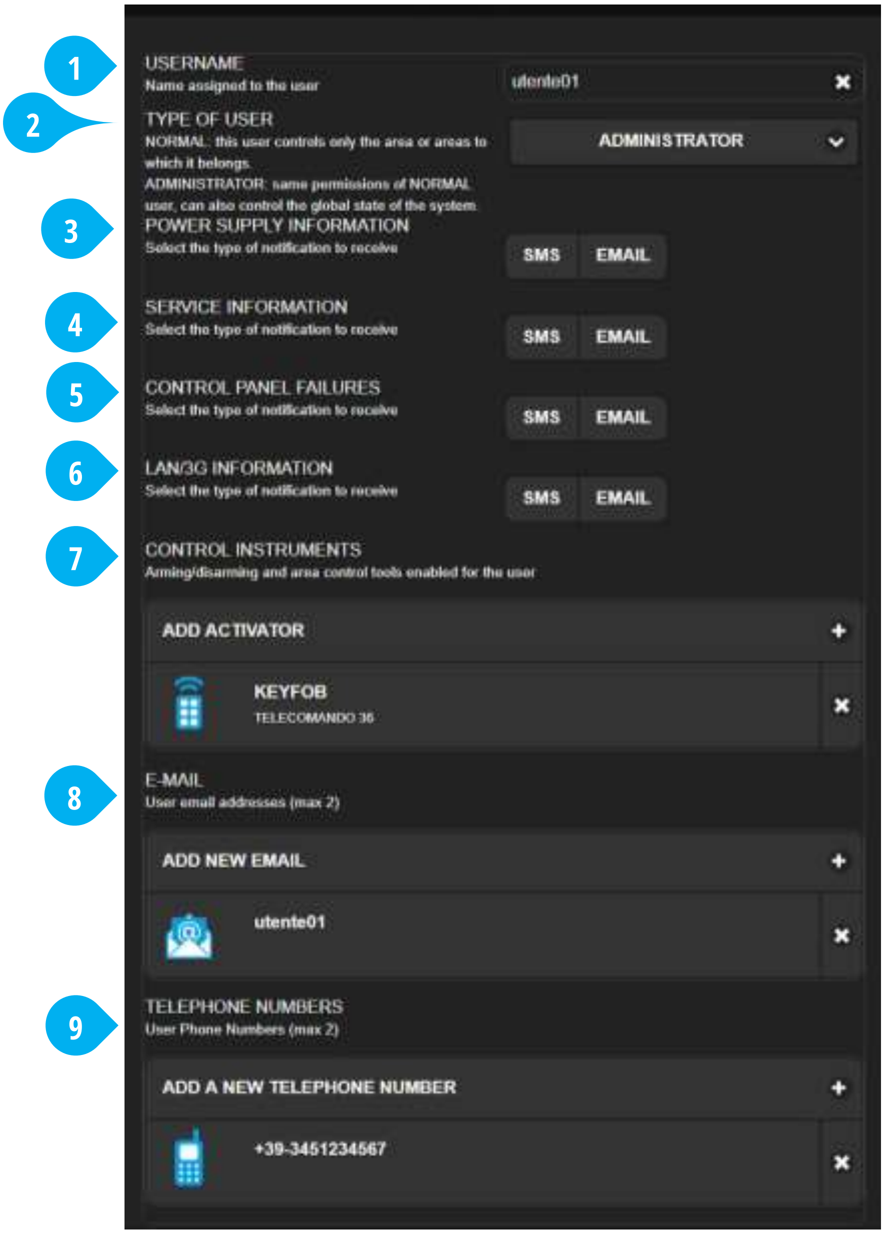
The special user "INSTALLER" is already present by default (Figure 36-2); it is possible to modify the parameters but not to delete it.
The INSTALLER user can access the control panel only if it is enabled by an Administrator user via the ON / OFF button (Figure 36-1) when the panel is OUT OF SETUP MODE or if the control panel has the DIP4 in the OFF position, that is without a password protection of the web access.

Users must be created here at GLOBAL level in order to be able to insert them - as necessary - in the Areas.
The same User can be added in more than one Area simultaneously (in each Area it is then possible to define further permissions and controls, such as enabling only certain modes of arming).

7.6.1 CREATE / MODIFY A USER

To create a new user press "Add new user" or tap an existing one to modify its programming.
Follow the on-screen instructions for programming (Figure 37).

The INSTALLER user is unique and can only be used for programming the control panel (it can not be used to know the status of the areas or to arm / disarm).



USERNAME
Name assigned to the user
utente01

TYPE OF USER
NORMAL: this user controls only the area or areas to which it belongs.
ADMINISTRATOR: same permissions of NORMAL user, can also control the global state of the system.
ADMINISTRATOR

POWER SUPPLY INFORMATION
Select the type of notification to receive

SERVICE INFORMATION
Select the type of notification to receive

CONTROL PANEL FAILURES
Select the type of notification to receive

LAN/3G INFORMATION
Select the type of notification to receive

CONTROL INSTRUMENTS
Arming/disarming and area control tools enabled for the user

KEYFOB
TELECOMANDO 36

E-MAIL
User email addresses (max 2)

utente01

TELEPHONE NUMBERS
User Phone Numbers (max 2)

+39-3451234567

Figure 37 – Creating and editing a user

1 USERNAME: name assigned to the User (max 14 characters)

2 TYPE OF USER:

- NORMAL: can arm and disarm (from: app, keypad, remote control, transponder key) according to the programming assigned, see the status of the Area and its events, receive alerts (e-mails, SMS messages, calls).
- ADMINISTRATOR: has the same characteristics as the normal user, plus displays the status of the control panel devices, other users and the events of the panel (not only of the Area).
- POLICE: is a special user who can only receive voice calls for events concerning the area

3 POWER SUPPLY INFORMATION: receives notification (SMS and/or E-MAIL) in case of power supply anomalies of the control panel and devices (ex: 230 VAC mains failure, low battery of a radio sensor…)

4 SERVICE INFORMATION: receives notification (SMS and/or E-MAIL) in case of service events:

- Setup modifications
- PASSWORD update
- E-MAIL update
- USER CODE Update
- Change zone abilitation (enable / disable / exclude)
- Firmware update

5 CONTROL PANEL FAILURES: receives notification (SMS and/or E-MAIL) in case of anomalies in the control panel:

- System (intrusion attempt, radio interference)
- Devices (tamper, failed supervision)
- Zones (manumission, tamper, supervision failed)

6 LAN / 3G INFORMATION: receives notification (SMS and/or E-MAIL) in case of significant events of LAN and 3G connections

7 CONTROL INSTRUMENTS: these are the activation and control tools the user can use in the Areas to which is assigned:

- WEB LOGIN: access to the app via e-mail address and web password (max 1)
- USER CODE: 6-digit numerical code of the keypads (max 1)
- REMOTE CONTROL: remote control associated to the user
- KEY: electronic transponder key associated to the user

Max 6 control tools per User.

8 E-MAIL: the e-mail address of the User, used to receive E-MAIL notifications and for APP access (max 2)

9 TELEPHONE NUMBERS: the phone number of the User, used to receive SMS notifications or VOICE calls (max 2)

7.7 IP CAMERAS

The control panel can communicate directly with some IP camera models *****, for a maximum of **8 cameras**, with the purpose of giving one visual verification (video verification) in case of detection events.

To use this feature, the IP camera must continuously record the Substream secondary stream on its internal microSD.

Each camera can be associated with one or more sensors (maximum 4): with the control panel armed, for each alarm generated by one of the sensors associated, the control panel will ask the camera for a sequence of **3 images** (VGA resolution 640 x 480) related to this event:

- an image 1 second before the event
- an image at the time of the event
- an image 1 second after the event

The images relating to the alarm events are stored in the RAM memory of the control panel (circular buffer of 2 MB sufficient for approx. 30 images / 10 events) and are made available for viewing directly from the APP, as well as sent as attachments to the alarm e-mails (only to users who have enabled the reception of this type of communications).

NOTES:

1) It is essential that the time of the cameras and that of the control panel are synchronized, as the images acquisition is based on the date-hour-minutes-seconds parameters of the event.

2) The control panel can be programmed to update the time of the cameras every hour. In this case the NTP update on the cameras MUST BE DISABLED.

3) The acquisition of images associated with a DELAYED zone will occur at the end of the Entry time (if in fact, the system is disarmed before it is not considered an alarm), but requiring the images related to moment of detection.

4) Capturing images from the camera can take up to 90 seconds, so it is normal to have a delay in the appearance of images associated with the event or in the reception of e-mails with images attached. However, sending SMS and PUSH alarm messages remains immediate.

5) In case of errors in the recovery of images from the camera, the control panel sends the e-mail message of alarm, and in the EVENT LIST the type of problem encountered is reported.

6) The images are lost in case of restart or complete lack of power supply to the control panel

***** Compatible cameras:

DAHUA mod. IPC-C35 / DAHUA mod. IPC-K35 / DAHUA mod. IPC-HFW1320S-W / DAHUA mod. IPC-HDBW1320E-W

7.7.1 SETTING THE CAMERA

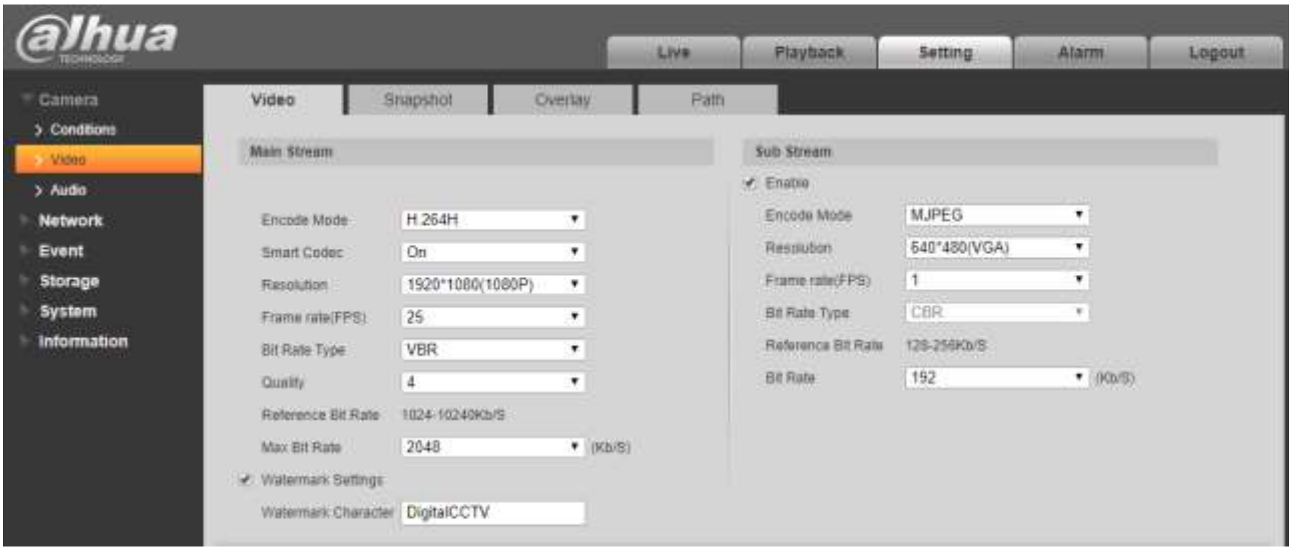
The cameras must be set via the web browser as follows so that the control panel can communicate with them.

Refer to the tools and manuals provided by the camera manufacturer for details on programming the camera.

1. Insert a microSD in the camera with adequate capacities and features (see camera requirements).

2. Assign a fixed IP address to the camera (disable the DHCP service on the camera).
The camera address must belong to the same network as the control panel.
Warning: if there is no DHCP service in the network or if only the 3G data connection is used, the control panel MUST also be assigned a fixed IP address.

3. Set the options "Setting -> Camera -> Video" of the camera as follows:



Main Stream

Encode Mode: H.264H

Smart Codec: On

Resolution: 1920*1080(1080P)

Frame rate(FPS): 25

Bit Rate Type: VBR

Quality: 4

Reference Bit Rate: 1024-10240Kb/S

Max Bit Rate: 2048 (Kb/S)

☑ Watermark Settings

Watermark Character: DigitalCCTV

Sub Stream

☑ Enable

Encode Mode: MJPEG

Resolution: 640*480(VGA)

Frame rate(FPS): 1

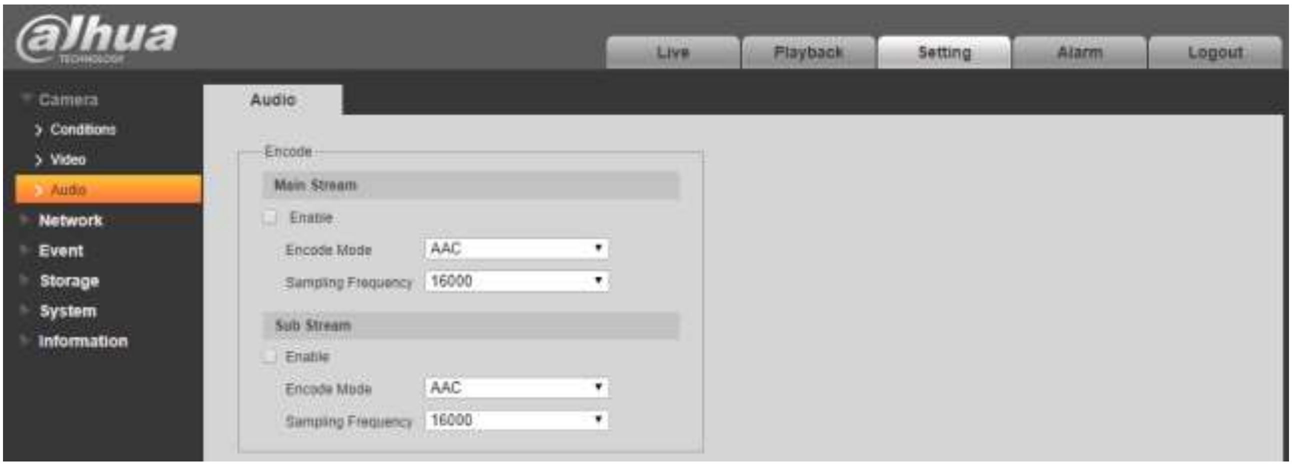
Bit Rate Type: CBR

Reference Bit Rate: 128-256Kb/S

Bit Rate: 192 (Kb/S)

SUBSTEAM = Enabled
Encode mode = MJPEG
Resolution = 640 * 480 (VGA)
Frame rate (FPS) = 1
Bit Rate = 192 Kb/s

4. [IF PRESENT] Set the "Setting -> Camera -> Audio" options of the camera as follows:



Encode

Main Stream

☐ Enable

Encode Mode: AAC

Sampling Frequency: 16000

Sub Stream

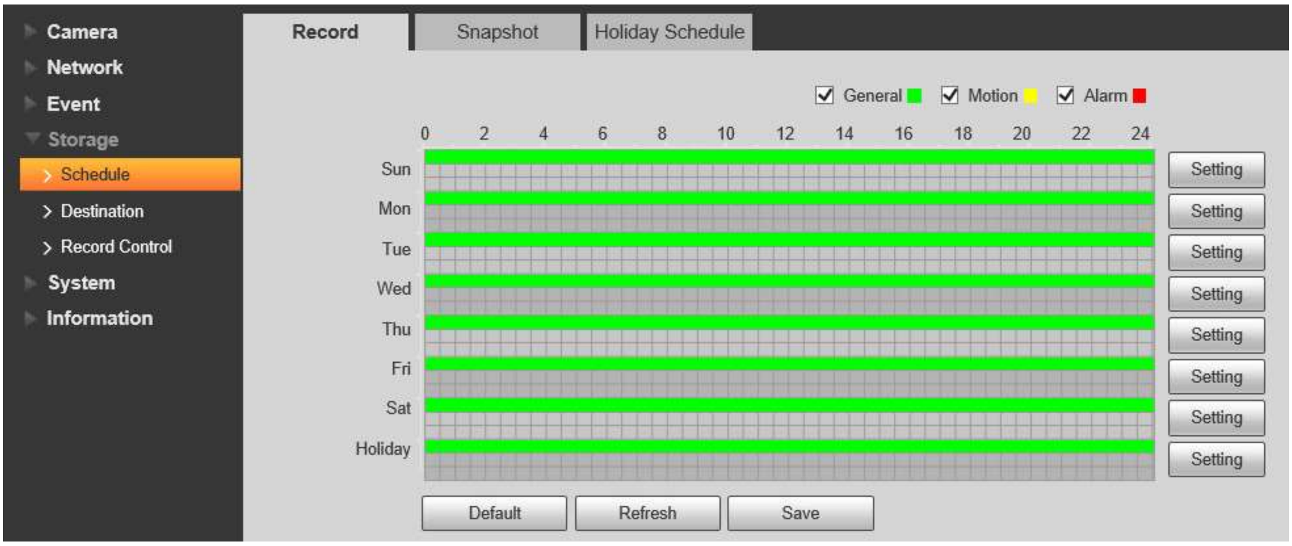
☐ Enable

Encode Mode: AAC

Sampling Frequency: 16000

SUBSTEAM = Disabled

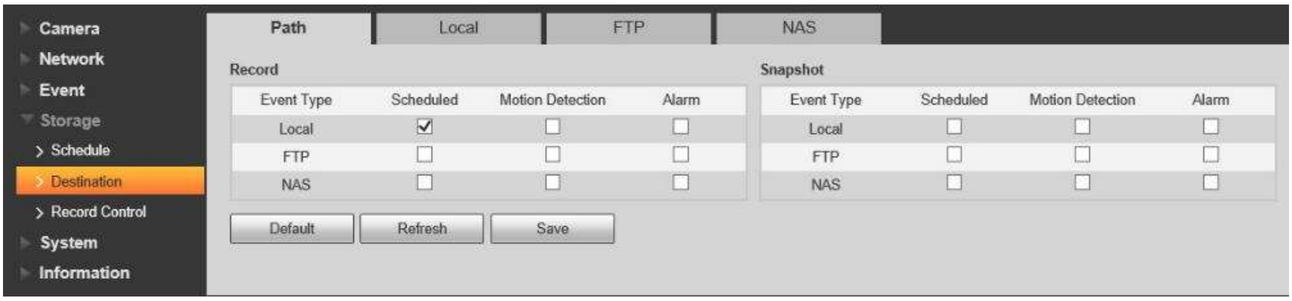
5. Set the "Setting -> Storage -> Schedule" options as follows:



☑ General 🟩 ☑ Motion 🟨 ☑ Alarm 🟥

Sun, Mon, Tue, Wed, Thu, Fri, Sat, Holiday: 0–24 🟩

6. Set the "Setting -> Storage -> Destination" options as follows:



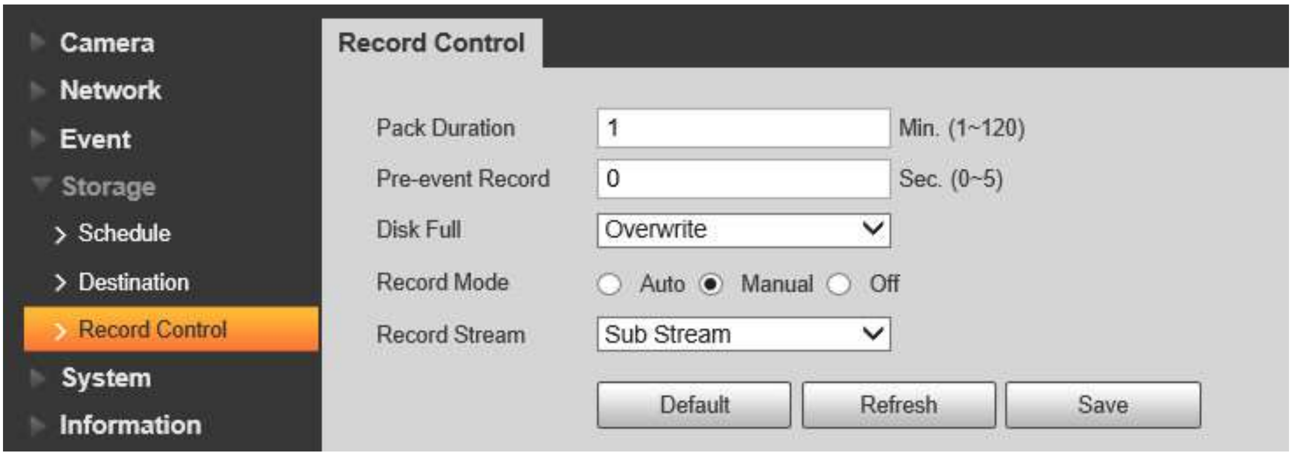
Record

Event Type	Scheduled	Motion Detection	Alarm
Local	☑	☐	☐
FTP	☐	☐	☐
NAS	☐	☐	☐

Snapshot

Event Type	Scheduled	Motion Detection	Alarm
Local	☐	☐	☐
FTP	☐	☐	☐
NAS	☐	☐	☐

7. Set the "Setting -> Storage -> Record Control" options as follows:

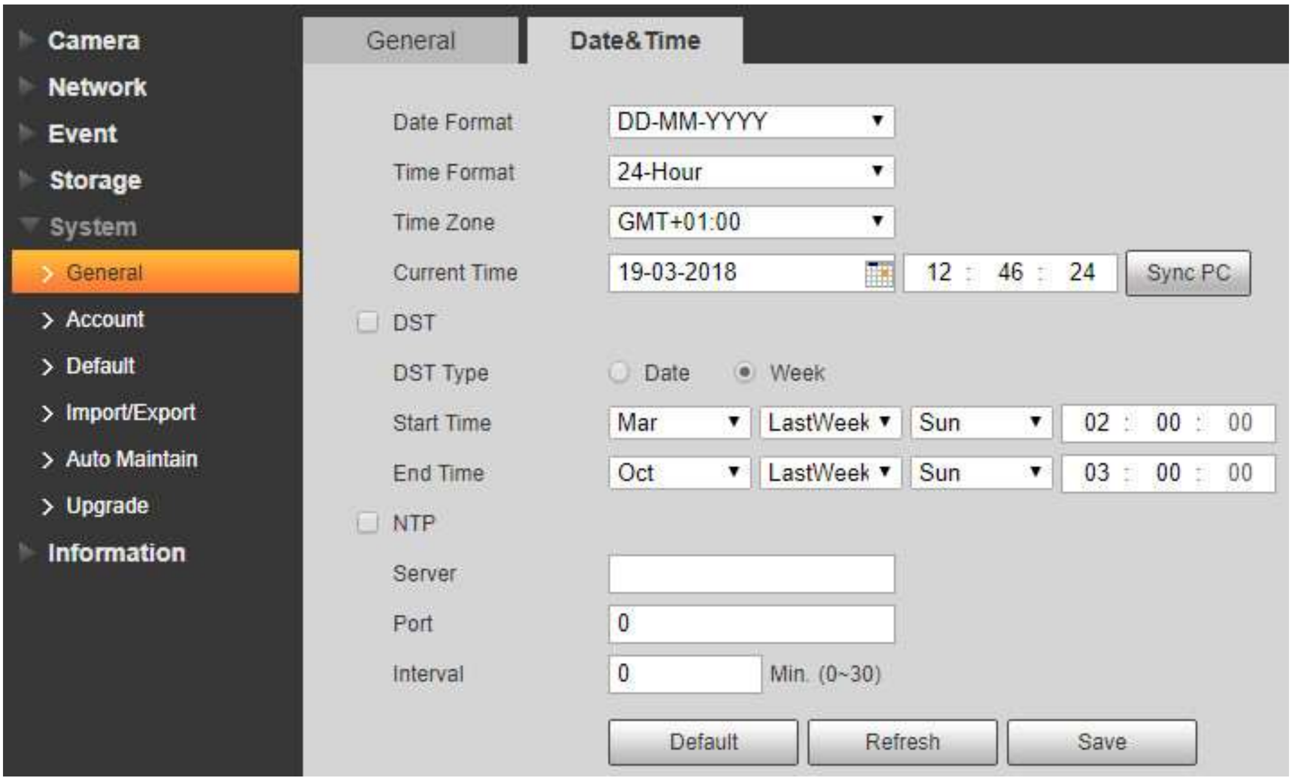


Pack Duration 1 Min. (1~120)
Pre-event Record 0 Sec. (0~5)
Disk Full Overwrite
Record Mode ○ Auto ● Manual ○ Off
Record Stream Sub Stream

Pack Duration = 1 min
Pre-event Record = 0 sec
Disk Full = Overwrite
Record Mode = Manual
Record Stream = Sub Stream

8. Set the "Setting -> System -> General -> Date & Time" options as follows:

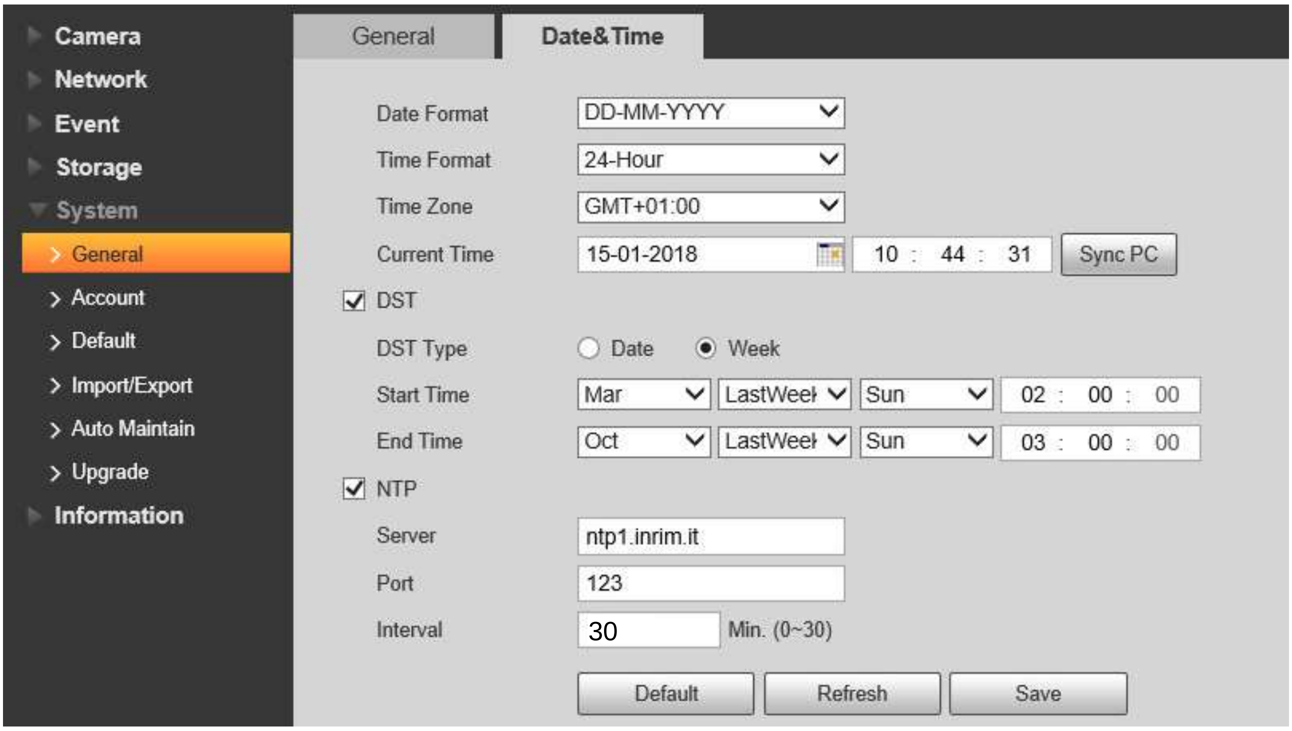
CASE A – CAMERA OPTION IN CONTROL PANEL "TIME UPDATE = ON"



Date Format DD-MM-YYYY
Time Format 24-Hour
Time Zone GMT+01:00
Current Time 19-03-2018 12 : 46 : 24
□ DST
DST Type ○ Date ● Week
Start Time Mar LastWeek Sun 02 : 00 : 00
End Time Oct LastWeek Sun 03 : 00 : 00
□ NTP
Server
Port 0
Interval 0 Min. (0~30)

DST = DISABLED + NTP = DISABLED

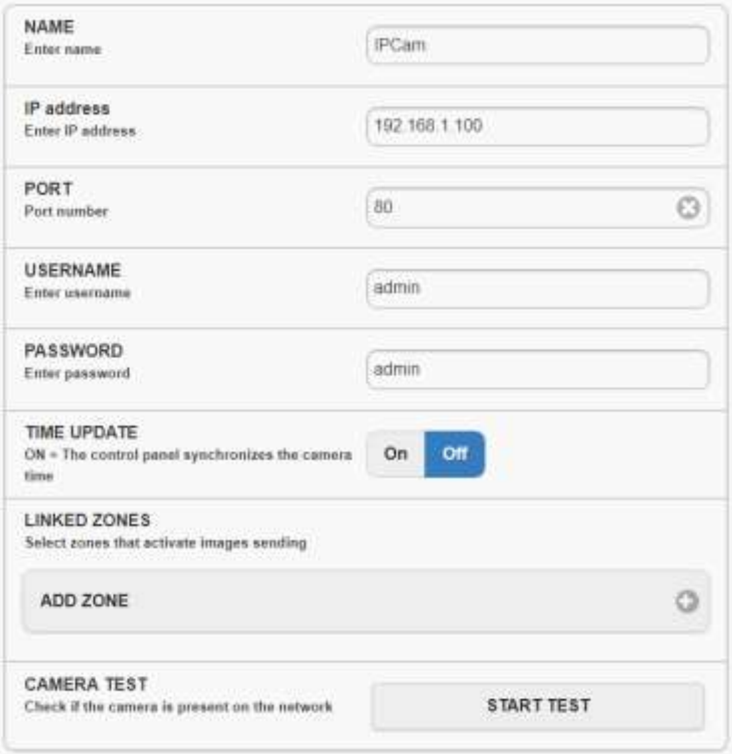
CASE B – CAMERA OPTION IN CONTROL PANEL "TIME UPDATE = OFF"



Date Format DD-MM-YYYY
Time Format 24-Hour
Time Zone GMT+01:00
Current Time 15-01-2018 10 : 44 : 31
☑ DST
DST Type ○ Date ● Week
Start Time Mar LastWeel Sun 02 : 00 : 00
End Time Oct LastWeel Sun 03 : 00 : 00
☑ NTP
Server ntp1.inrim.it
Port 123
Interval 30 Min. (0~30)

7.7.2 ADDING A CAMERA

1. With the control panel in SETUP mode, go to the IP CAMS menu and press the "ADD IP CAMERA" button:
   Fill in the required fields for the camera to be added:



NAME
Enter name
IPCam

IP address
Enter IP address
192.168.1.100

PORT
Port number
80

USERNAME
Enter username
admin

PASSWORD
Enter password
admin

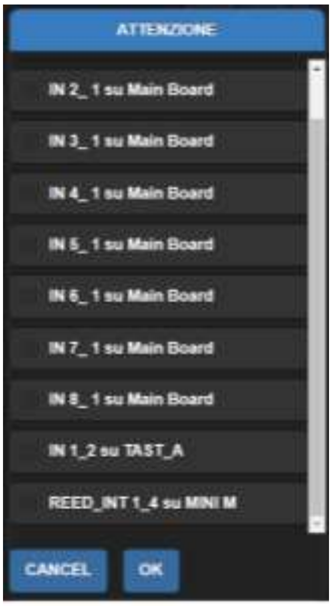
TIME UPDATE
ON = The control panel synchronizes the camera time
On [✓ Off]

LINKED ZONES
Select zones that activate images sending
ADD ZONE

CAMERA TEST
Check if the camera is present on the network
START TEST

NAME	Name that identifies the camera
IP address	IP address of the camera
PORT	HTTP port of the camera
USERNAME	User name for accessing the camera
PASSWORD	Password to access the camera
TIME UPDATE	Select how the camera time is updated **ON** = camera time is updated by the control panel **OFF** = camera time is NOT updated by the control panel
LINKED ZONES	Indicates the zones combined with the video verification function of this camera
CAMERA TEST	Perform a connection test to the camera with the parameters set previously

2. Press the "ADD ZONE" button and select at least one alarm zone to be associated (maximum 4 for each camera):



7.8 CONTACT-ID

The control panel can send events to a monitoring station with a SIA DC-09 receiver, via the internet connection (LAN or 3G).

7.8.1 ADDING A MONITORING STATION

To add a monitoring station that receives events, select "CONTACT-ID" from the side menu (Figure 38) and press the "ADD MONITORING STATION" button, then fill in the required fields related to the station to be added (Figure 39).

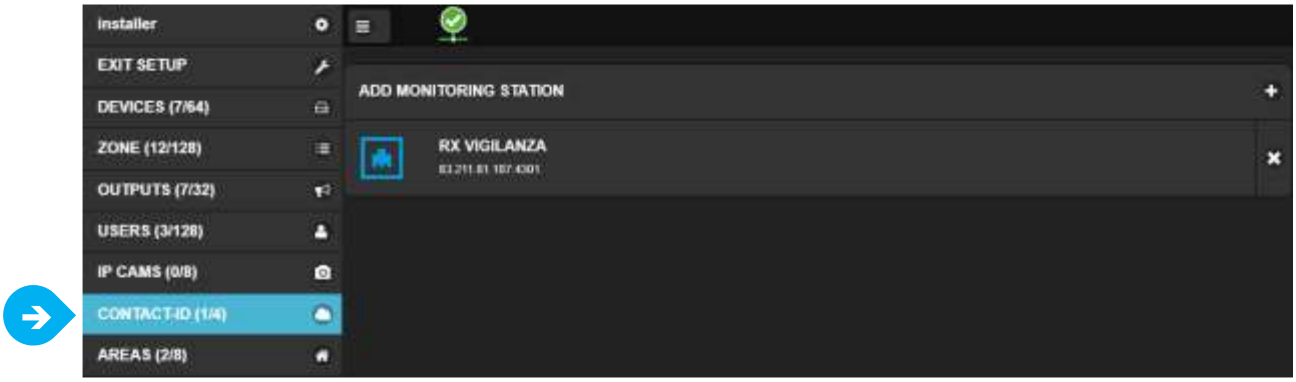
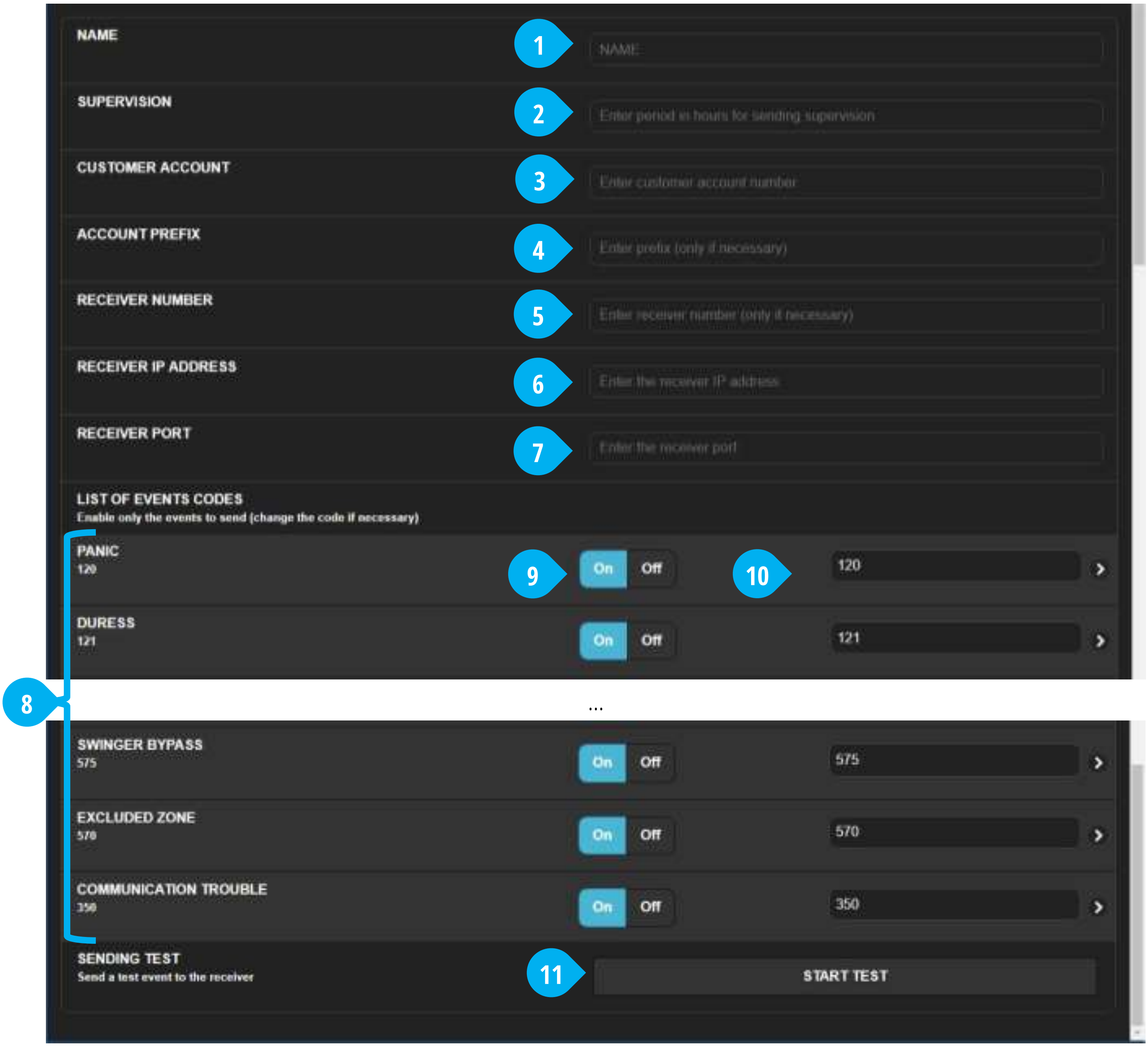


Figure 38 – CONTACT-ID Menu

7.8.2 SETTING THE CONTACT-ID PARAMETERS



NAME — NAME

SUPERVISION — Enter period in hours for sending supervision

CUSTOMER ACCOUNT — Enter customer account number

ACCOUNT PREFIX — Enter prefix (only if necessary)

RECEIVER NUMBER — Enter receiver number (only if necessary)

RECEIVER IP ADDRESS — Enter the receiver IP address

RECEIVER PORT — Enter the receiver port

LIST OF EVENTS CODES
Enable only the events to send (change the code if necessary)

PANIC 120	On Off	120
DURESS 121	On Off	121
…		
SWINGER BYPASS 575	On Off	575
EXCLUDED ZONE 570	On Off	570
COMMUNICATION TROUBLE 350	On Off	350

SENDING TEST
Send a test event to the receiver

Figure 39 –CONTACT-ID Settings

1 NAME: descriptive name of the monitoring station.

2 SUPERVISION: time interval in hours after which the control panel sends the Life Test to the station

3 CUSTOMER ACCOUNT: customer account identification code (provided by the monitoring station)

4 ACCOUNT PREFIX: prefix of the account code (ONLY IF NECESSARY) - provided by the monitoring station

5 RECEIVER NUMBER: receiver number (ONLY IF NECESSARY) - provided by the monitoring station

6 RECEIVER IP ADDRESS: IP address of the receiver - provided by the monitoring station

7 RECEIVER PORT: receiver communication port - provided by the monitoring station

8 LIST OF EVENT CODES: In the Contact-ID standard, each event is identified with a numerical code. This section shows all the events (with the relative standard codes) that the control panel can send to the station.

9 EVENT ENABLING: The sending of each event can be enabled/disabled with the ON/OFF switch

10 EVENT CODE: It is possible to modify the code associated with the event (if the station uses different codes), inserting the code in this box.

11 SENDING TEST: by pressing this key it is possible to send a test event to the monitoring station to check the communication

NOTE: THE EVENTS ARE SENT TO THE MONITORING STATION ONLY IF IT IS ENABLED IN THE AREA SETTINGS

7.9 AREAS

To configure the Areas select "AREAS" from the side menu (Figure 40):

When the control panel is new or after a RESET, no Area is present.

To create / add an area press the "No Area" button (Figure 40-1) and then "ADD NEW" (Figure 40-2).

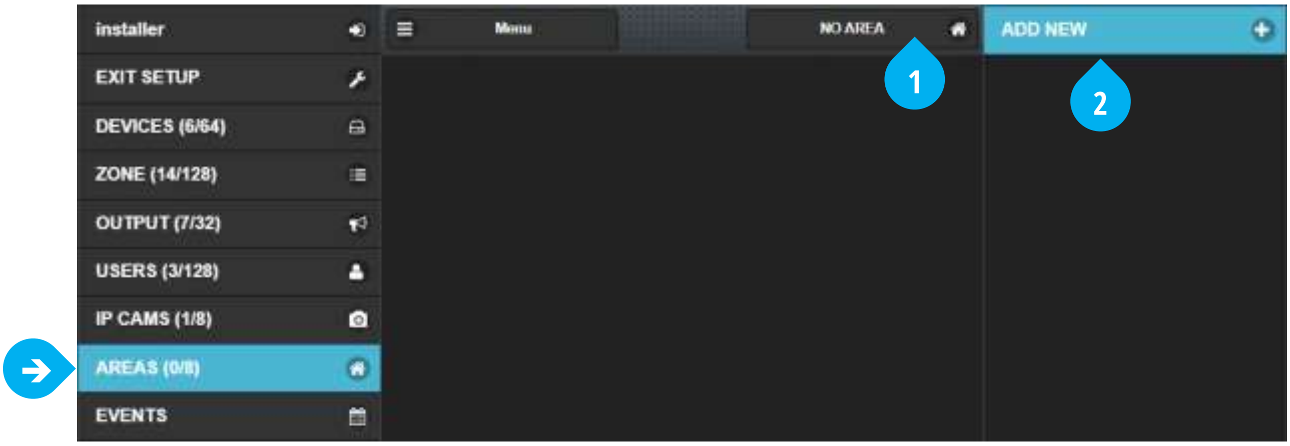


Figure 40 – AREAS Menu

The AREA configuration is divided into five parts (Figure 41):

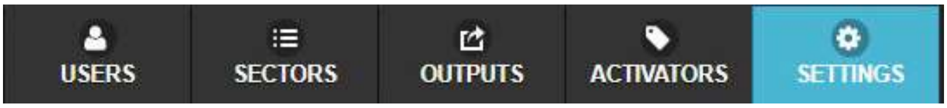
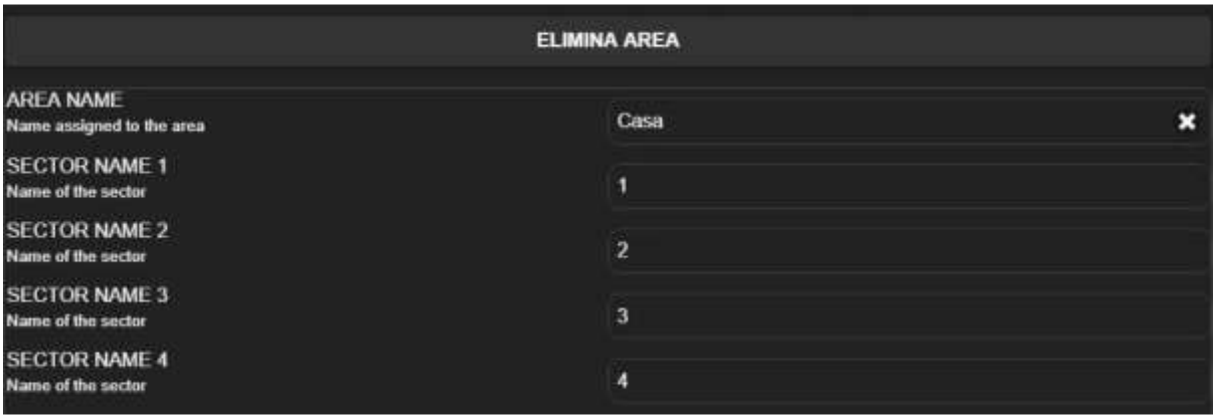


Figure 41 – Area Settings

- SETTINGS: general settings of the Area.

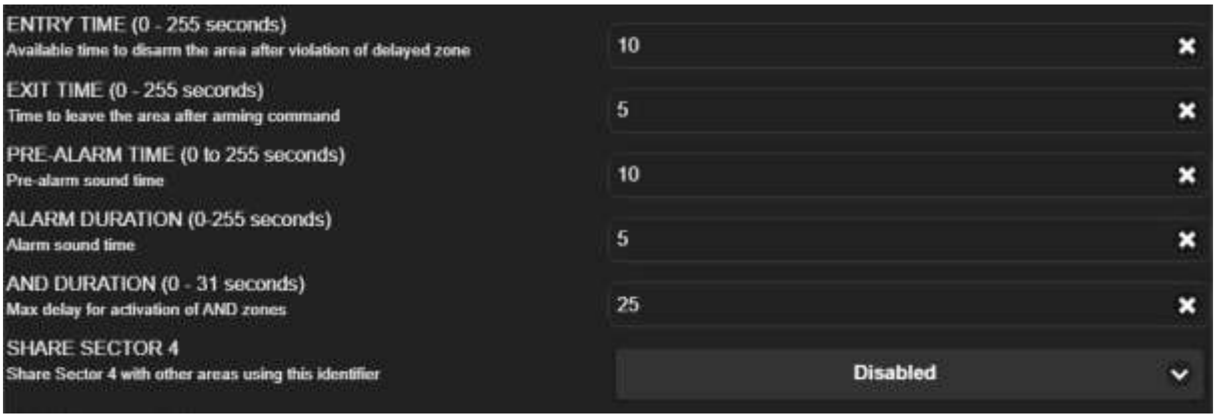


ELIMINA AREA

AREA NAME Name assigned to the area	Casa
SECTOR NAME 1 Name of the sector	1
SECTOR NAME 2 Name of the sector	2
SECTOR NAME 3 Name of the sector	3
SECTOR NAME 4 Name of the sector	4

1 AREA NAME: name assigned to the Area (max 14 characters).
The name is displayed in the warning messages (SMS, e-mail), in events, in the display of the keypads, read in the voice calls (only if TTS available)

2 SECTOR NAME: name assigned to the Sector (max 13 characters)



ENTRY TIME (0 - 255 seconds)
Available time to disarm the area after violation of delayed zone
10 ✖

EXIT TIME (0 - 255 seconds)
Time to leave the area after arming command
5 ✖

PRE-ALARM TIME (0 to 255 seconds)
Pre-alarm sound time
10 ✖

ALARM DURATION (0-255 seconds)
Alarm sound time
5 ✖

AND DURATION (0 - 31 seconds)
Max delay for activation of AND zones
25 ✖

SHARE SECTOR 4
Share Sector 4 with other areas using this identifier
Disabled ⌄

3 **ENTRY TIME**: time available to disarm the system when entering from a Delayed Zone (0 ÷ 255 seconds)

4 **EXIT TIME**: time available to exit the area after the arming command (0 ÷ 255 seconds)

5 **PRE-ALARM TIME**: sound time of pre-alarm events (0 ÷ 255 seconds)

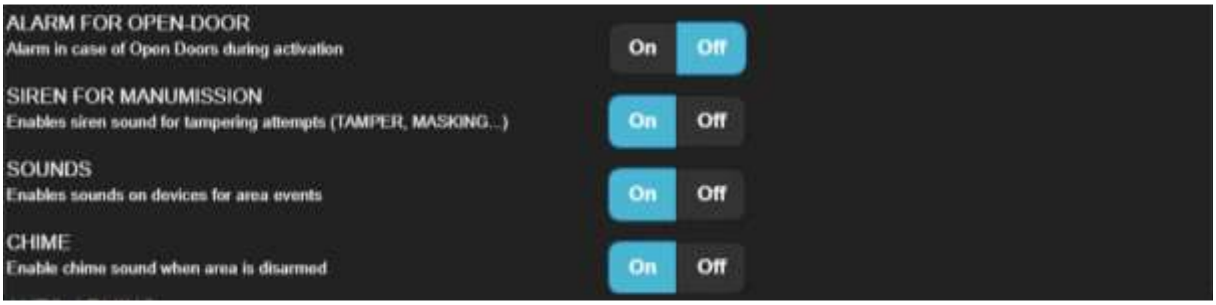
6 **ALARM DURATION:** sound time of alarm events (0 ÷ 255 seconds)

7 **AND DURATION**: window time for activation of the AND zones and of the double detection of Pre-Alarm Zones (elevation to Alarm of the Pre-Alarm event) - (0 ÷ 31 seconds)

8 **SHARE SECTOR 4**

Sector 4 of an Area may be associated with other Sectors 4 of other Areas to create Common Groups (max 3 groups). There will be an alarm from the Sectors 4 of a Common Group only if ALL the Areas involved in the Group have armed the Sector 4 (if only one of the Sectors 4 is not armed, the Group does not generate an alarm).

Values: Disabled (not shared); SHARE 1 (Group 1); SHARE 2 (Group 2); SHARE 3 (Group 3)



ALARM FOR OPEN-DOOR
Alarm in case of Open Doors during activation
On [✓ Off]

SIREN FOR MANUMISSION
Enables siren sound for tampering attempts (TAMPER, MASKING...)
[✓ On] Off

SOUNDS
Enables sounds on devices for area events
[✓ On] Off

CHIME
Enable chime sound when area is disarmed
[✓ On] Off

9 **ALARM FOR OPEN-DOOR**: at the time of activation of the system (at the end of the Exit Time) the control panel checks which Zones are open and can alert the User with an alarm sound (anti-distraction function).

Note: in addition to the Alarm alert, it is possible to decide to automatically exclude the Zones found open (see global Zone settings)

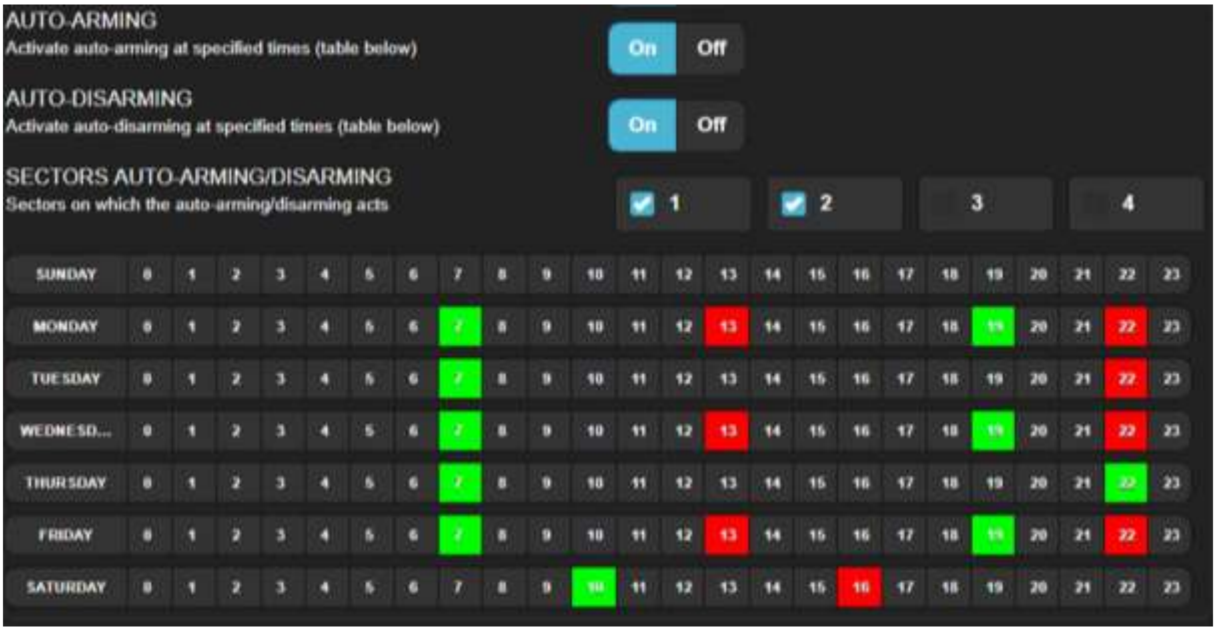
10 **SIREN FOR MANUMISSION**: select if the tampering events (tamper, masking, etc) must generate alarm with sound of the sirens.

11 **AUTOMATIC ALARM**: when enabled, two PRE-ALARM events within the AND time generate an ALARM event

12 **SOUNDS**: activates the sounds on the devices for the events of the Area

13 **CHIME**: activates the "ding-dong" sound when the zones are detecting while the system is disarmed.

Note: it is necessary to enable the Zones from which you want the Chime function (see the global settings of the Zone)



AUTO-ARMING
Activate auto-arming at specified times (table below)
[✓ On] Off

AUTO-DISARMING
Activate auto-disarming at specified times (table below)
[✓ On] Off

SECTORS AUTO-ARMING/DISARMING
Sectors on which the auto-arming/disarming acts
☑ 1 ☑ 2 □ 3 □ 4

SUNDAY	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
MONDAY	0	1	2	3	4	5	6	🟩 7	8	9	10	11	12	🟥 13	14	15	16	17	18	🟩 19	20	21	🟥 22	23
TUESDAY	0	1	2	3	4	5	6	🟩 7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	🟥 22	23
WEDNESD...	0	1	2	3	4	5	6	🟩 7	8	9	10	11	12	🟥 13	14	15	16	17	18	🟩 19	20	21	🟥 22	23
THURSDAY	0	1	2	3	4	5	6	🟩 7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	🟩 22	23
FRIDAY	0	1	2	3	4	5	6	🟩 7	8	9	10	11	12	🟥 13	14	15	16	17	18	🟩 19	20	21	🟥 22	23
SATURDAY	0	1	2	3	4	5	6	7	8	9	🟩 10	11	12	13	14	15	🟥 16	17	18	19	20	21	22	23

14 AUTO-ARMING: the control panel automatically is armed the scheduled times (weekly programming, see point 15); you can create multiple arming times (GREEN colour).
This function can not be activated until at least one User has been assigned to the Area.

15 AUTO-DISARMING: the control panel disarms automatically at the established times (weekly programming, see point 15); it is possible to create several disarming times (RED colour).
This function cannot be activated until at least one User has been assigned to the Area.

16 CONTACT-ID SEND: Select which monitoring station the panel sends contact-ID events related to this area

17 SECTORS AUTO-ARMING/DISARMING: set which Sectors must be armed / disarmed in the events of auto-arming and disarming.

18 Weekly time for Auto-Arming and Auto-Disarming: click on the times in which Auto-arming is desired (first click, the box turns GREEN) or Auto-disarming (second click, the box turns RED).
It is possible to select multiple times for Auto-Arming and Disarming.
To delete the time schedule, click on the boxes until they return GREY.

- **ACTIVATORS**: activation devices for controlling the Area.

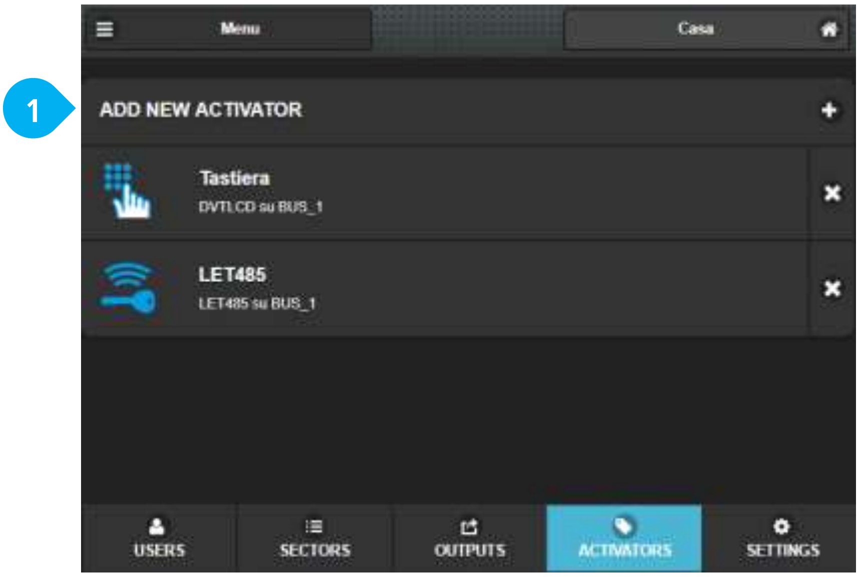


Figure 42 – Area: Activators

To add an Arming device (keypads and transponder key readers) to the Area, press "Add New Activator" and select it from the list:

- Keypads: can be associated to more than one Area at the same time

  A keypad associated with several Areas displays the status of the Area on which it is operating; to select the Area to act on, press the keys left / right arrow (←/→).
- Transponder key readers: can only be associated with an Area.

Note: keyfobs and transponder keys are stored at USER level.

- **OUTPUTS**: outputs associated to the Area. To add an Output (from the main board of the panel or from connected devices) press "Add New Ouput" and select it from the list (Figure 43).

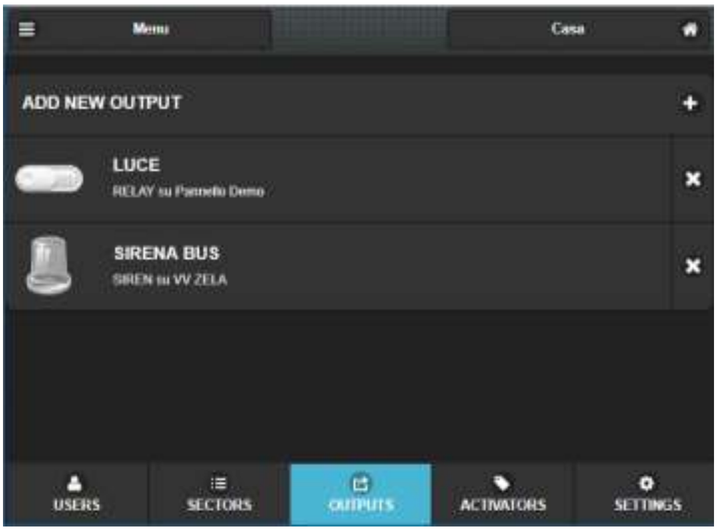


Figure 43 – Area: Outputs

The electrical behaviour (ON / OFF or impulsive) is set in the "OUTPUT" section of the main menu.

After adding an output to the Area, program the event or events that will trigger it (press its name in the list, Figure 44):

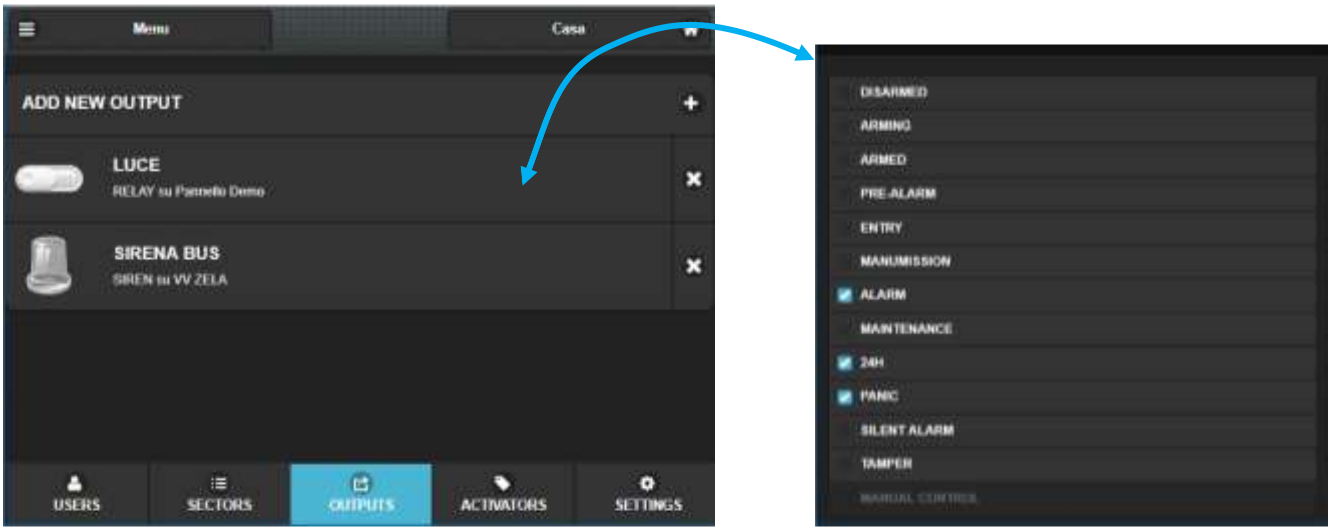


Figure 44 – Area: Output Events

DISARMED	Output active when Area is totally disarmed (any Sector disarmed)
ARMING	Output active during Exit time (any arming mode)
ARMED	Output active when Area is amed (any arming mode)
PRE-ALARM	Output active during Pre-Alarm event
ENTRY	Output active during Entry time
MANUMISSION	Output active when no communication from one or more devices on BUS485
ALARM	Output active during Alarm event
MAINTENANCE	Output active when in "SETUP" mode (installer)
24H	Output active during 24H Alarm event
PANIC	Output active during Panic event
SILENT ALARM	Output active during Silent Alarm event
TAMPER	Output active during Tamper Alarm event
MANUAL CONTROL	Manual control of the output through the App

Note: if the outputs are set as impulsive, they will only be active for the programmed pulse time.

- SECTORS: set the zones belonging to the Sectors of the Area. It is possible to add the same zone in several sectors (even in different areas).

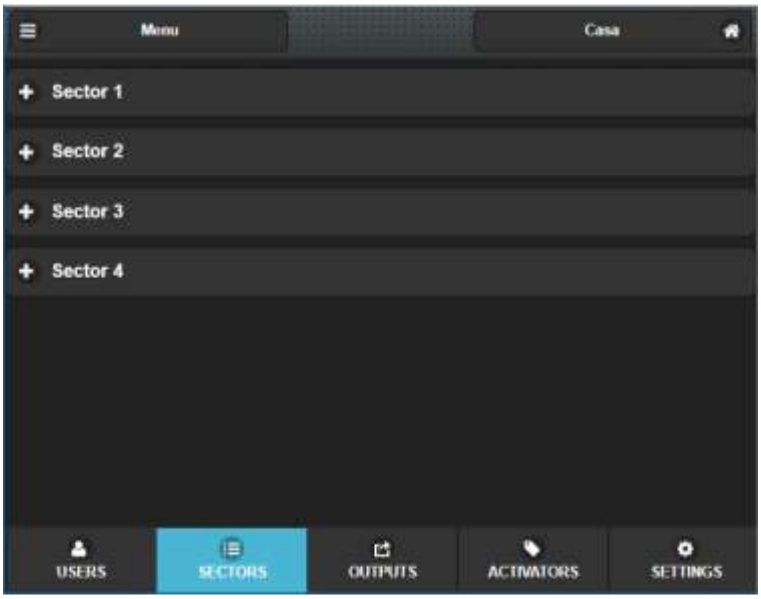


Figure 45 – Area: Sectors

To add Zones to a Sector, press the Sector name (Figure 46-1) and then "Add New Zone" (Figure 46-2) then select the zone/s to be added (Figure 46-3):

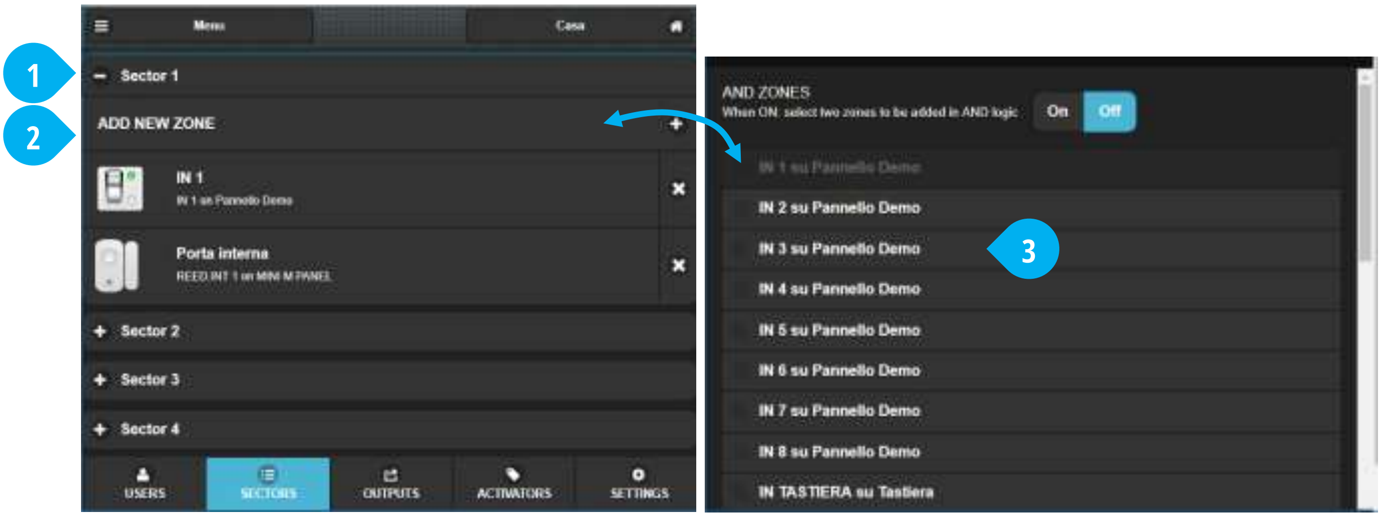


Figure 46 – Area: Zones in the Sectors

To create an AND between TWO Zones, select the two Zones (Figure 47-1) and enable the creation of the AND (Figure 47-2) and finally choose the type of alarm that they will have to generate (Figure 47-3):

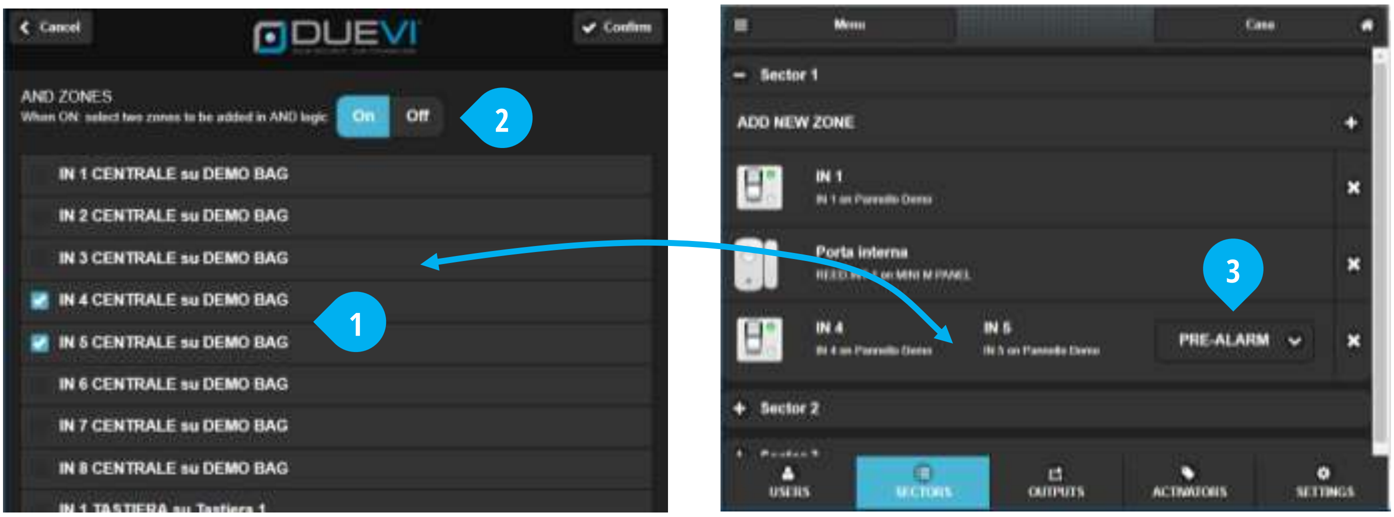

Cancel
DUEVI
Confirm
AND ZONES
When ON select two zones to be added in AND logic
On
Off
2
IN 1 CENTRALE su DEMO BAG
IN 2 CENTRALE su DEMO BAG
IN 3 CENTRALE su DEMO BAG
IN 4 CENTRALE su DEMO BAG
IN 5 CENTRALE su DEMO BAG
1
IN 6 CENTRALE su DEMO BAG
IN 7 CENTRALE su DEMO BAG
IN 8 CENTRALE su DEMO BAG
IN 1 TASTIERA su Tastiera 1
Menu
Casa
Sector 1
ADD NEW ZONE
IN 1
IN 1 on Pannello Demo
Porta interna
REED INT 1 on MINI M PANEL
3
IN 4
IN 4 on Pannello Demo
IN 5
IN 5 on Pannello Demo
PRE-ALARM
Sector 2
USERS
SECTORS
OUTPUTS
ACTIVATORS
SETTINGS

Figure 47 – Area: AND between two zones

Note: it is not possible to do AND between more than two zones

The AND time is defined in the "Settings> AND Duration " tab of the Area.

IF AN ZONE SIGNALS MORE THAN 5 TIMES AN ALARM - DURING THE SAME ARMING OF THE AREA - IT IS AUTOMATICALLY EXCLUDED (THE AREA REMAINS ARMED AND WILL ALARMS FROM THE OTHER ZONES).

- USERS: users who can operate on the area.

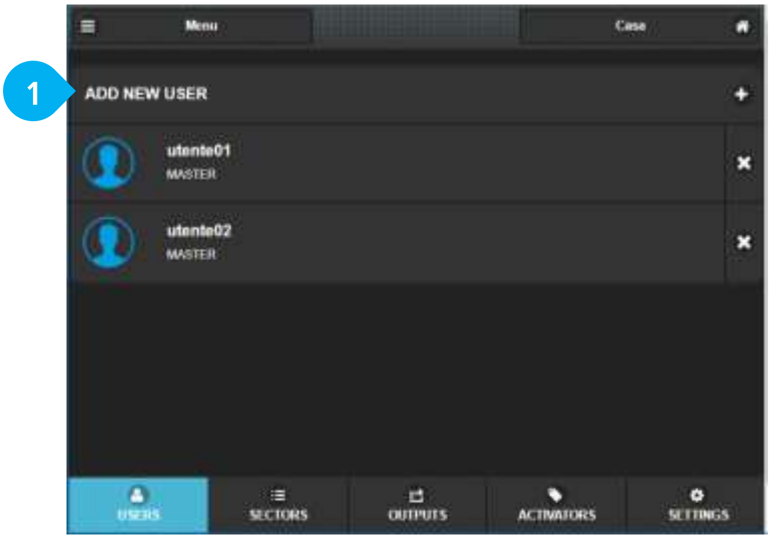
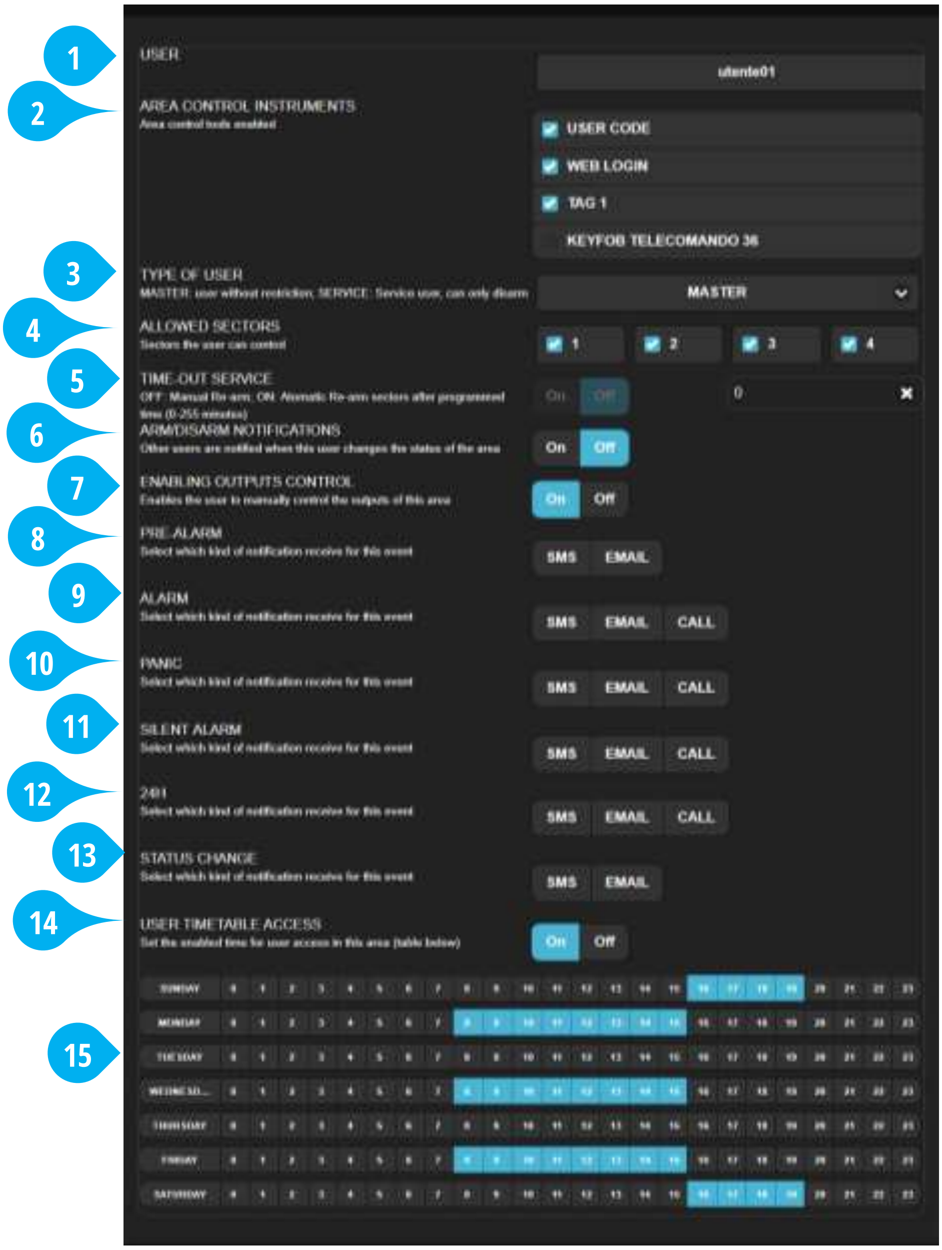


Figure 48 – Area: Users

To add a User, press "Add New User" (Figure 48-1) and select it from the list of available users, then set the options of the user regarding this Area (Figure 49):

Each User can be added to multiple Areas, and have different settings in each Area.



USER — utente01

AREA CONTROL INSTRUMENTS
Area control tools enabled
☑ USER CODE
☑ WEB LOGIN
☑ TAG 1
□ KEYFOB TELECOMANDO 36

TYPE OF USER
MASTER: user without restriction; SERVICE: Service user, can only disarm
MASTER

ALLOWED SECTORS
Sectors the user can control
☑ 1 ☑ 2 ☑ 3 ☑ 4

TIME-OUT SERVICE
OFF: Manual Re-arm; ON: Atomatic Re-arm sectors after programmed time (0-255 minutes)
On [✓ Off] 0

ARM/DISARM NOTIFICATIONS
Other users are notified when this user changes the status of the area
On [✓ Off]

ENABLING OUTPUTS CONTROL
Enables the user to manually control the outputs of this area
[✓ On] Off

PRE-ALARM
Select which kind of notification receive for this event
SMS EMAIL

ALARM
Select which kind of notification receive for this event
SMS EMAIL CALL

PANIC
Select which kind of notification receive for this event
SMS EMAIL CALL

SILENT ALARM
Select which kind of notification receive for this event
SMS EMAIL CALL

24H
Select which kind of notification receive for this event
SMS EMAIL CALL

STATUS CHANGE
Select which kind of notification receive for this event
SMS EMAIL

USER TIMETABLE ACCESS
Set the enabled time for user access in this area (table below)
[✓ On] Off

SUNDAY	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
MONDAY	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
TUESDAY	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
WEDNESD...	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
THURSDAY	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
FRIDAY	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
SATURDAY	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23

Figure 49 – Area: Configuring a User

1 USER: User whose settings are being changed in this area.
Note: Users must be created in the global "Users" menu.

2 AREA CONTROL INSTRUMENTS: enables the arming and control instruments that the user can use in the Area.

- WEB LOGIN: access to the app via e-mail address and web password
- KEYFOB: remote control associated to the user
- USER CODE: 6-digit numerical code through the keypads
- TAG: electronic key associated to the user

3 TYPE OF USER: set the type of access to the Area:

- MASTER: this user can arm and disarm (within the limits of other settings)
- SERVICE: this user can only disarm (within the limits of the other settings); for the SERVICE users an automatic re-arming is available (see option “TIME-OUT SERVICE”).

4 ALLOWED SECTORS: sectors that the user can view and on which he can act. The disabled sectors will not be changed from their status when this user acts to arm / disarm.

5 TIME-OUT SERVICE: automatic re-arming - after the programmed time - of the same sectors that the SERVICE user have disarmed (0 ÷ 255 minutes).

6 **ARM/DISARM NOTIFICATIONS**: enable sending notifications to other users when this user acts to arm and disarm the control panel.
Note: the user never receives arming / disarming notifications for operation made by himself!

7 **ENABLING OUTPUTS CONTROL**: enables manual control by the user of the outputs of this area.

8 **PRE-ALARM**: enables notification reception (SMS or e-mail) in case of Pre-alarm events.

9 **ALARM**: enables notification reception (SMS, e-mail or voice call) in case of Alarm events.

10 **PANIC**: enables notification reception (SMS, e-mail or voice call) in case of Panic events.

11 **SILENT ALARM**: enables notification reception (SMS, e-mail or voice call) in case of Silent Alarm events.

12 **24H**: enables notification reception (SMS, e-mail or voice call) in case of 24H Alarm events (technological events).

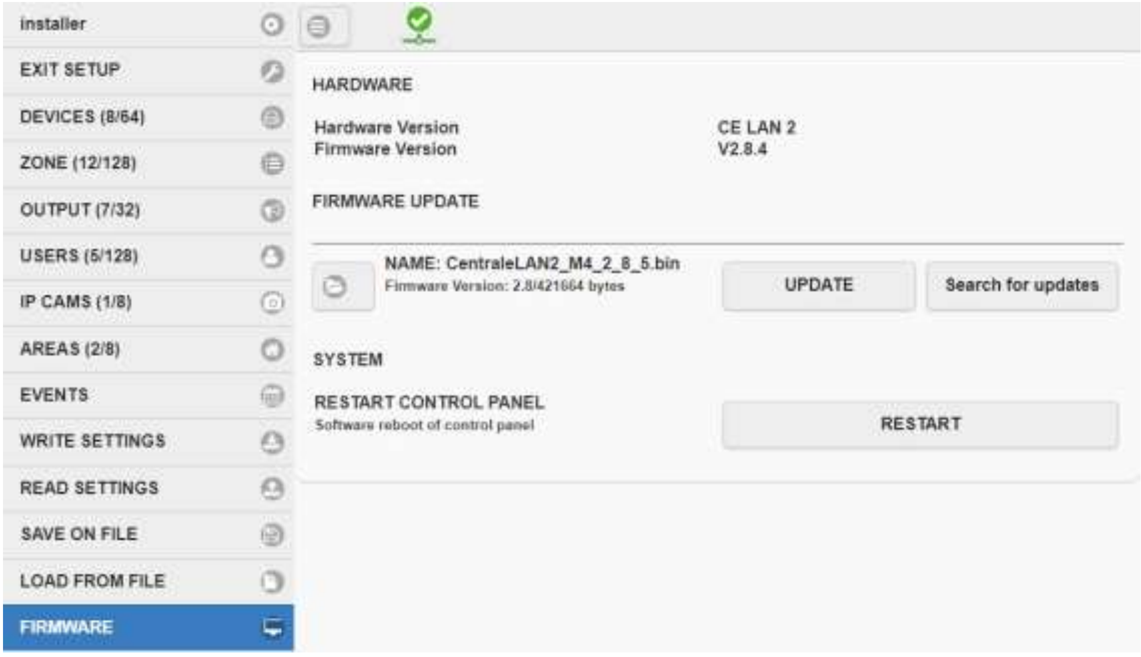
13 **STATUS CHANGE**: enables notification reception (SMS or e-mail) when other users modify the Area's arming.

14 **USER TIMETABLE ACCESS**: enables time limitation to the user, according to the weekly timetable set below.

15 **WEEKLY TIMETABLE**: (only if USER TIMETABLE ACCESS = ON) weekly time schedule of the user; this user can act on the Area only during the selected times (the user's permissions follow the other settings).

7.10 FIRMWARE

In this menu it is possible to update the firmware of the control panel and also to perform a REBOOT of the control unit.



HARDWARE

Hardware Version CE LAN 2
Firmware Version V2.8.4

FIRMWARE UPDATE

NAME: CentraleLAN2_M4_2_8_5.bin
Firmware Version: 2.8/421664 bytes

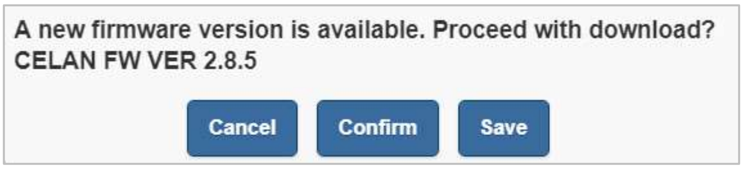
SYSTEM

RESTART CONTROL PANEL
Software reboot of control panel

It is possible to perform a Firmware Update both ONLINE (in the presence of an internet connection) or OFFLINE.

To perform an ONLINE update, proceed as follows:

1) Press "SEARCH FOR UPDATES" to check ONLINE for updates
2) If a new version is present, an information window is displayed.


A new firmware version is available. Proceed with download?
CELAN FW VER 2.8.5

3) Press "CONFIRM" to continue with the update or "SAVE" if you want to save a copy of the .bin file

4) Press "UPDATE" to continue

ATTENTION: SOME UPDATES MAY RETURN THE PANEL TO FACTORY DEFAULT CONDITIONS.

It is advisable to save the configuration on file BEFORE continuing with the update

5) Press "CONFIRM" and wait for the operation to complete

CAUTION: DO NOT TURN OFF THE POWER STATION DURING THE UPDATE OPERATIONS

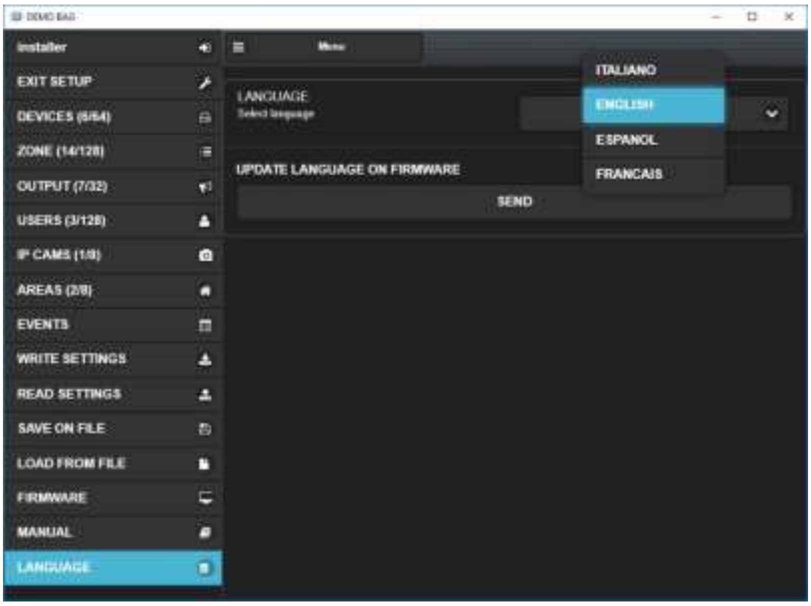
6) If the update operation ends correctly, a confirmation window appears and the control unit automatically restarts

7.11 LANGUAGE

This menu allows you to change:

1) Change in real-time the language of the graphical programming interface
2) SEND to the control panel the language to be stored inside the firmware (text used for keypad and notifications push, SMS, e-mail).

NOTE: The language sent to the panel will be active after the next reboot of the control panel.



8 SAVE / LOAD CONFIGURATION

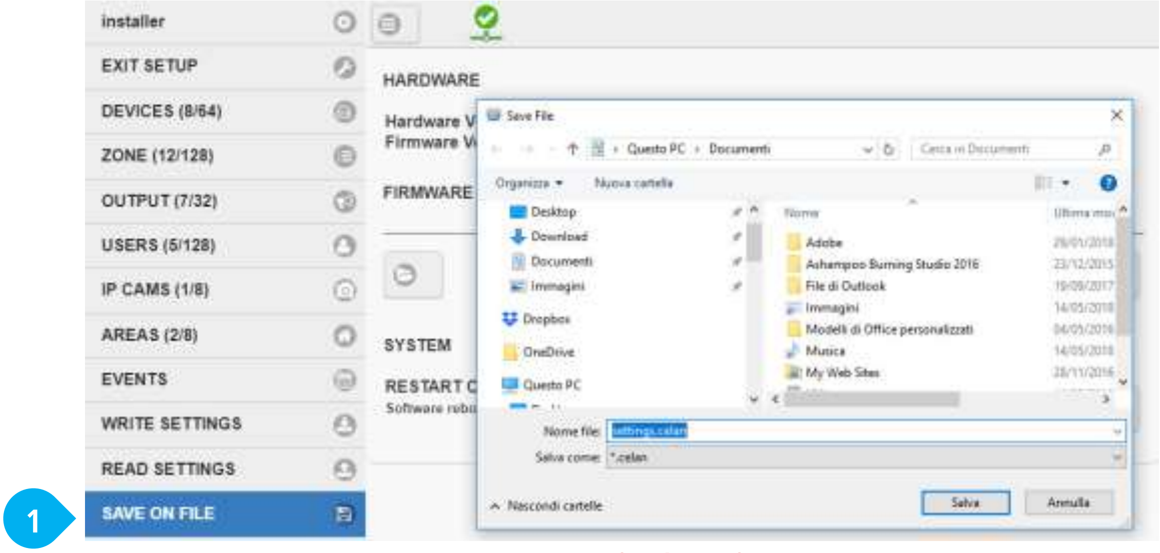
8.1 SAVE THE CONFIGURATION

It is recommended to always save the configuration of the control panel to file.

The saved file contains all the panel configurations (including the programmed devices) except for the web access password of the users.

Therefore, in case of need, it will be easier to restore the control panel without having to run the whole configuration all over again.

To save the current configuration, select "SAVE ON FILE" in the side menu (Figura 50-1):



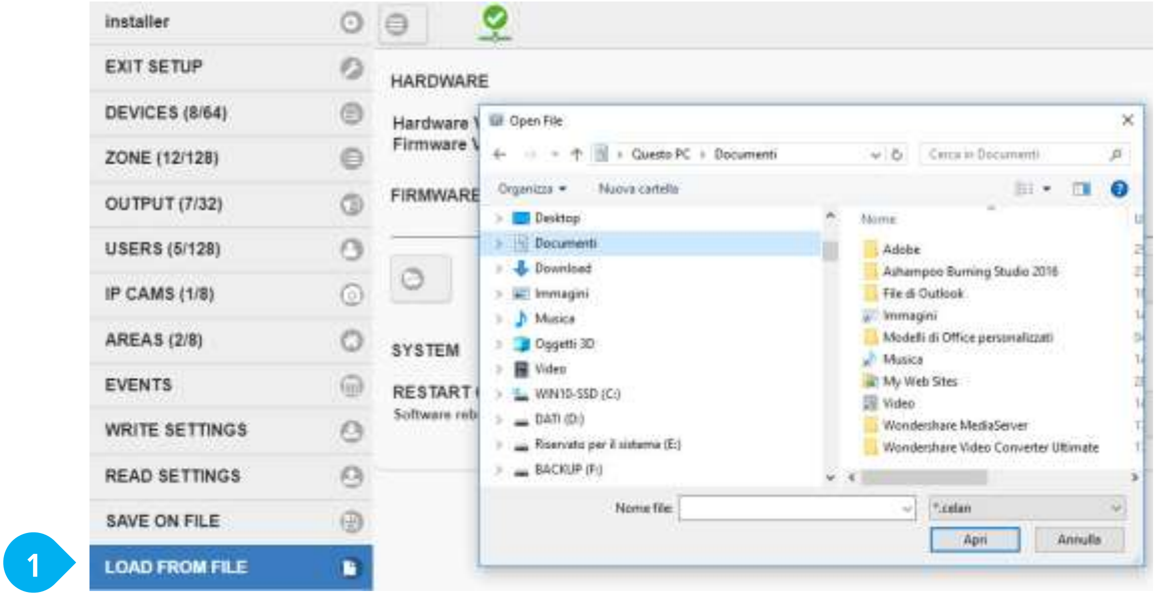
Nome file: settings.celan

Salva come: *.celan

Figura 50 – Save on file the configuration

8.2 LOAD THE CONFIGURATION

To load a saved configuration, select "LOAD FROM FILE" in the side menu (Figura 51-1), select folder and filename to load.



Nome file: *.celan

Figura 51 – Load from file the configuration