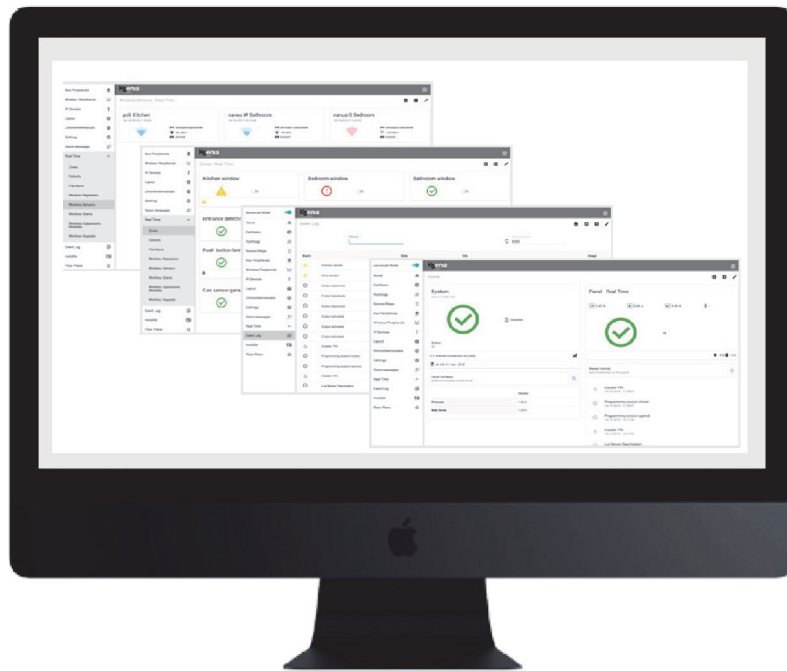


# lares 4.0



## Programming Manual



[www.kseniasecurity.com](http://www.kseniasecurity.com)

All information in this document is subject to change without notice and does not represent a commitment on the part of Ksenia Security.

<b>1. INTRODUCTION</b>	<b>7</b>
Compatibility	7
Software requirements	7
Configuration mode - logging in for the first time	7
Keypad programming	8
How to read the control panel IP address from keypad	9
How to update firmware version	10
How to save the configuration	10
<b>2. CONFIGURATION FROM Ksenia SecureWeb</b>	<b>11</b>
Access to the portal Ksenia SecureWeb	11
Activating the voice licence	14
Description of HOME page of Installer program	15
Description of the dynamic information	15
<b>3. DESCRIPTION OF THE INSTALLER PROGRAM MENU</b>	<b>19</b>
Quick guide to navigate web pages	19
How to change the data - Open session	19
How to save the data - Save session and Apply session	20
How to cancel the data inserted or changed	20
How to export a layout configuration	20
How to import a layout configuration	21
How to exit from Installer	21
Cross checking of data inserted	21
HOME menu	22
Partition menu	22
Hashtags menu	23
Rooms / Maps menu	23
BUS peripherals menu	24
Automatic BUS peripherals acquisition	24
Acquiring a radius siren - Example	24
Read the status of BUS peripherals in real time	26
Programming BUS peripherals	27
Expansion modules	27
Isolators	28
Receivers	29
User interfaces	29
Sirens	31
Sensors	32

domus	33
energia	34
Programming BUS peripherals without configuring the Serial Number	34
Add / cancel the BUS peripherals	34
Wireless peripherals	36
Acquisition of wireless peripherals	36
Read the status of wireless peripherals in real time	37
Programming wireless peripherals	38
Wireless sirens	38
Wireless repeaters	39
Wireless expansion modules	39
Wireless sensors	40
Wireless keypads	47
Programming Wireless peripherals without configuring the Serial Number	49
Cancel wireless peripherals	49
IP Devices	50
Automatic IP Devices acquisition	50
Acquiring an ergo-T keypad - Example	50
Read the status of IP Devices in real time	51
Programming IP Devices	53
ergo-T	53
IP Supervisors	53
IP Cameras	54
gemino IoT	55
Gateway	56
Programming IP peripherals without configuring the Mac Address	57
Add / cancel IP devices	57
Layout	59
Arming modes	59
Outputs	60
Counters	65
Custom Balances	66
Zones	66
Users	76
Start enroll tags	78
Contact ID Receivers	79
SIA IP Receivers	80
Programmable logics	81
Scenarios	81
Events	86
Contact lists	92



Notifications .....	94
Scheduler timers .....	101
Chronothermostats .....	101
Consumption management .....	102
Services .....	103
Konnex .....	103
Gateway HTTP .....	109
Settings .....	109
General options .....	110
Network .....	114
GSM/GPRS/PSTN Communicator .....	116
Voice messages .....	117
Play .....	117
Generate .....	118
Real time .....	119
Event log .....	120
Installer .....	122
Floor plans .....	122
<b>4. FUNCTIONALITIES AND CONFIGURATIONS DESCRIPTION .....</b>	<b>123</b>
Scheduler timers .....	123
Path management .....	123
Pre-alarms management .....	124
Dimmer .....	125
Services on Ksenia Secureweb .....	126
Automatic Backup .....	126
<b>5. APPENDIX .....</b>	<b>129</b>
Programming summary .....	129
Correspondence table of PUSH notification and Events .....	131
Customization forms .....	132
Keypad Keys Customization form .....	132
opera Remote Control Keys Customization form .....	133
volo Customization form .....	133
volo-in Customization form .....	134



## 1. INTRODUCTION

This manual is intended for installers and describes the procedures for configuring the hybrid IoT platform for Security and Home & Building Automation *lares 4.0*, by connecting to the Ksenia SecureWeb cloud:

- **the first chapter** briefly illustrates the different programming methods available to the installer (in local connection from a browser, by APP "Ksenia pro", remotely by connecting to the Ksenia SecureWeb pages);
- **the second chapter** explains how to register to the "Ksenia SecureWeb" cloud, how to enrol the platform and it describes the "Installer" HOME page (name assigned to the programming web interface);
- **the third chapter** is dedicated to the description of the "Installer" programming pages, following the order of the menu items of which it is composed.

### 1.1 Compatibility

This manual is updated to firmware version 1.68.26 of lares 4.0 control panel.  
Compatible with all control panels of the *lares 4.0* family.

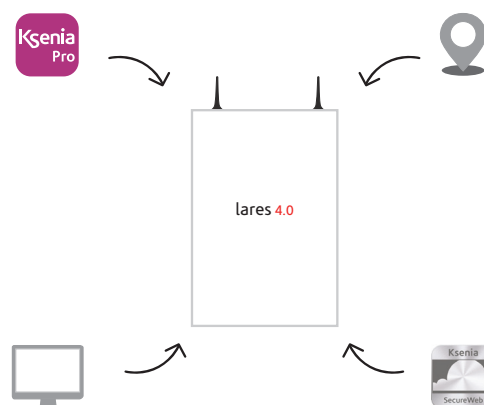
### 1.2 Software requirements

- Recommended browser: Google Chrome

### 1.3 Configuration mode - logging in for the first time

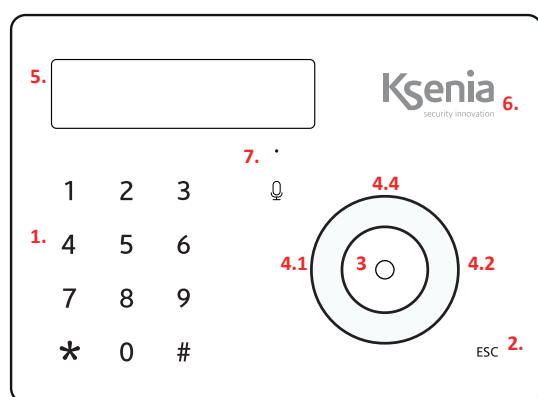
Choose one of the following methods for configuring the *lares 4.0* platform:

1. remotely from PC, through any browser by logging in to **www.kseniasecureweb.com** server (how to do it is described in the paragraph ["Access to the portal Ksenia SecureWeb" page 11](#));
2. remotely from mobile, downloading the dedicated **APP Ksenia PRO** for Security installers for free from Android or iOS stores and scanning the control panel's QR code (how to do it is described in the paragraph ["Access to the portal Ksenia SecureWeb" page 11](#));
3. from PC, via web browser, simply by entering the local IP address of the lares 4.0 control panel (i.e.: <https://192.168.20.200>) (how to acquire IP address is described in the paragraph ["How to read the control panel IP address from keypad" page 9](#));
4. from keyboard (this procedure is limited to a few functions) (see ["Keypad programming" page 8](#)).



### 1.3.1 Keypad programming

Keyboard programming is limited to a few functions listed below.



Legend	Description
1.	Alphanumeric keypad with keys from 1 to 9, * and #
2.	ESC key
3.	ENTER key
4.	Scroll button for using: 4.1 Left arrow 4.2 Down arrow 4.3 Right arrow 4.4 Up arrow
5.	Display LCD
6.	RFID Area
7.	Microphone

Access the installer menu with a **PIN code (default: 123456)**. You can navigate the various items by pressing the keys once you have entered the installer menu:

- **ENTER:** enter the sub-menu, confirm the values displayed or modified.
- **ESC:** exit the sub-menu, return to the previous menu, leave the installer menu.
- **DOWN ARROW (SCROLL CLOCKWISE)/UP ARROW (SCROLL ANTICLOCKWISE):** move from one item to another within the same menu.

A list of some installer menu items:

- **Sys. management:** system management with the following items:  
**Reset alarm:** all the alarms will be stopped, the tamper and alarm memories will be deleted.  
**Stop calls:** all the communications, in progress and in queue, will be deleted (SMS, phone calls, email, etc.).  
**Freeze system:** three possible choices:
  - No freeze: normal activity.
  - Freeze alarms: no action against the alarms will be performed.
  - Freeze actions: freeze all the actions of control panel.
- **User management:** assign a **RF-ID** key to the users configured.
- **Event logger:** list of events occurred with details.
- **Fault list:** list of faults in progress.
- **Zone status:** view of the status of the zones configured in the system.
- **Zone test:** list of zones that were never been in alarm since the TEST started, useful during the installation process.
- **Installer data:** installer data management  
**Change PIN:** change installer PIN code.  
**Description:** installer name.  
**Number:** installer telephone number.
- **Update:** it launches the software upgrade using the file present in the SD card and previously downloaded from [www.kseniasecurity.com](http://www.kseniasecurity.com), reserved area.

- **Programm. Back-up :**
  - **Create new:** backs-up any programming by saving the file on an SD card.
  - **Restore:** any programming data saved previously will be read from the SD card and loaded into the control panel.
- **Networking:** network configuration menu which allows the network parameters to be read/modified
  - **IP Address:** the control panel IP Address
  - **Subnet mask:** subnet-mask
  - **Gateway:** IP address of gateway
  - **DHCP server:** OFF / ON (default ON). This menu item is activated to allow the DHCP to be re-enabled if the control panel has been set to a fixed IP address.
- **Language:** select the language of the keypad from the list.
- **Panel version:** this allows you to view the control panel firmware version (although not the web server).

### 1.3.1.1 How to read the control panel IP address from keypad

If the network, where the control panel is installed, supports DHCP, to read the IP address make the following operations:

- Step 1. make sure the control panel is connected to the network;
- Step 2. enter the installer menu by dialing the PIN code on the numeric keypad (default: 123456);
- Step 3. scroll the menu items up to "Networking" and press OK;
- Step 4. the "IP Address" is displayed, make a note and exit the menu by pressing ESC twice.

Then type the IP address in the browser address bar: <<https://control-panel-IP-address>>.



**Note:** The default address will be 192.168.2.97 in the event that the network to which the control panel is connected does not support the DHCP, so type <<https://192.168.2.97>> in the browser address bar.

*NOTE 1: When you first switch on the keypad, the English menu will be displayed. To change the language, access the installer menu from the keypad via the webserver.*

*NOTE 2: APP Ksenia Pro is also available for "lares WLS 96-IP" platform although not for "lares".*

*NOTE 3: It is not possible to set a configuration if the system is armed, even partially, or if the access with installer code has been disabled by the user.*

## 1.4 How to update firmware version


---

### Update firmware version in local network connection:

- from PC / MAC, by clicking on the button <Load update file> in the Home Page -> Panel software section, it is possible to load the update file.

**WARNING!** This function is available from version FW 1.46.20. Previous versions must use the SD card with the following requirements: maximum capacity 32Gb, FAT 32 formatting, the file containing the FW must be present in the main root.

### Update firmware version in remote network connection:

- In the Home Page-> Panel software section, click on “Update software” icon . It is displayed only when a new version is available for download and installation.

## 1.5 How to save the configuration

---

The control panel reads both .bck files which only contain the control panel programming backup (for backwards compatibility), and .ksa files which can always contain the configuration of the control panel and eventually, the knx.json file which contains the configuration of the konnex device.

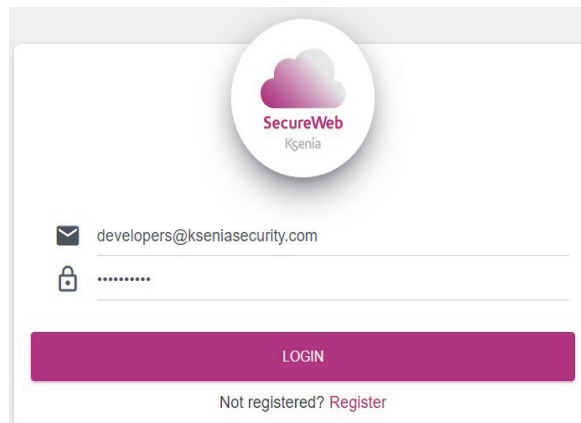
## 2. CONFIGURATION FROM Ksenia SecureWeb

### 2.1 Access to the portal Ksenia SecureWeb

Open the browser and type the name of the site **www.kseniasecureweb.com** in the address bar.

The credentials required to access the SecureWeb service are the same as those used to access the reserved area of the **www.kseniasecurity.com** website (e-mail address + password).

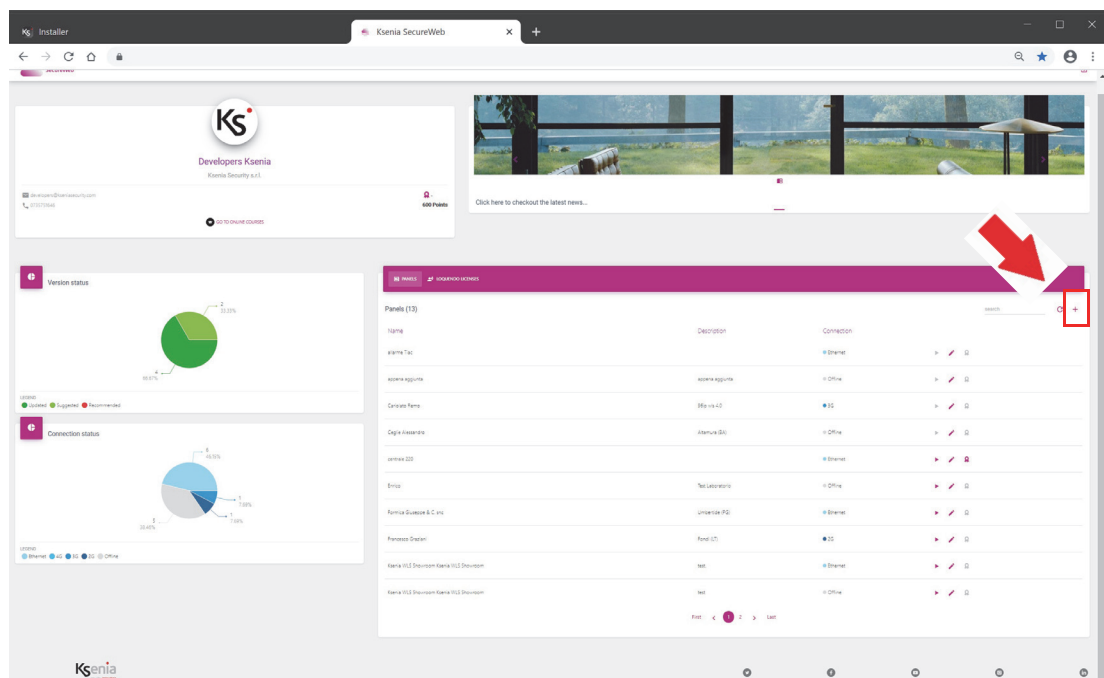
You must register free of charge by clicking on **<Register>** if you do not have these credentials.



The login form features the Ksenia SecureWeb logo at the top. Below it, there is a text input field for the email address, containing 'developers@kseniasecurity.com', and a password input field with masked characters. A prominent purple 'LOGIN' button is centered below the fields. At the bottom, a link reads 'Not registered? Register'.

#### From PC:

1. After successful login, **www.kseniasecureweb.com** page will open;
2. to **add** a new control panel click on **<+> sign in the Panel section**, see the following image;



3. type the serial number printed on the control panel label;
4. give a name and a description to the control panel and possibly also coordinates;
5. click on **<SAVE>** and the new control panel will appear in the list;

**Add Panel**

Serial Number \_\_\_\_\_

Name \_\_\_\_\_

Description \_\_\_\_\_

Coordinates 0,0 \_\_\_\_\_

CLOSE SAVE

6. The following image displays the list of control panels from which the installer can start some operations such as: logging in, editing, deleting, score acquisition, searching by filter, etc.  
See description below:

**Panels (22)**

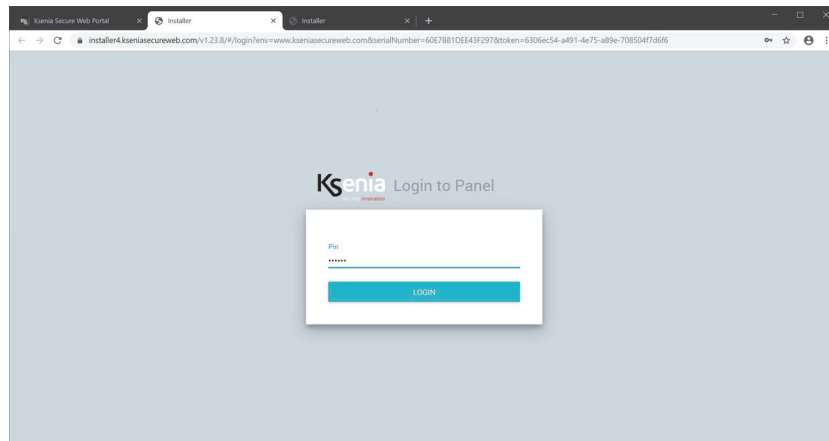
Name	Description	Connection	
220	220	Ethernet	▶ ✎ 🗑
4.0 Creston	Centrale con creston	3G	▶ ✎ 🗑
40ip		Ethernet	▶ ✎ 🗑
Armadio	Armadio laboratorio	3G	▶ ✎ 🗑
centrale prova	fornita per prova	Ethernet	▶ ✎ 🗑
Demo Sala Riunioni	Iares wis 96-IP	Ethernet	▶ ✎ 🗑
Enrico	Laboratorio	Ethernet	▶ ✎ 🗑
ksenia 4.0	Principale	Ethernet	▶ ✎ 🗑
Iares 96wis	Sviluppo	Ethernet	▶ ✎ 🗑
Iares wis	Vicino Tommy	2G	▶ ✎ 🗑

cerca 🔄 +

1. 2. 3. 4. 5. 6.

1. open the login and the Installer configuration web pages (if the symbol is grey, the control panel will not be reachable);
  2. open a new window with the possibility to modify the name, the description and the coordinates of the control panel selected or delete it;
  3. start the score acquisition for the selected panel;
  4. filtering criteria for name, description, connection;
  5. reload the page list;
  6. add new control panel.
7. Click on the <little triangle> symbol to access the control panel, type the **installer PIN code (default 123456)** to open the HOME page.



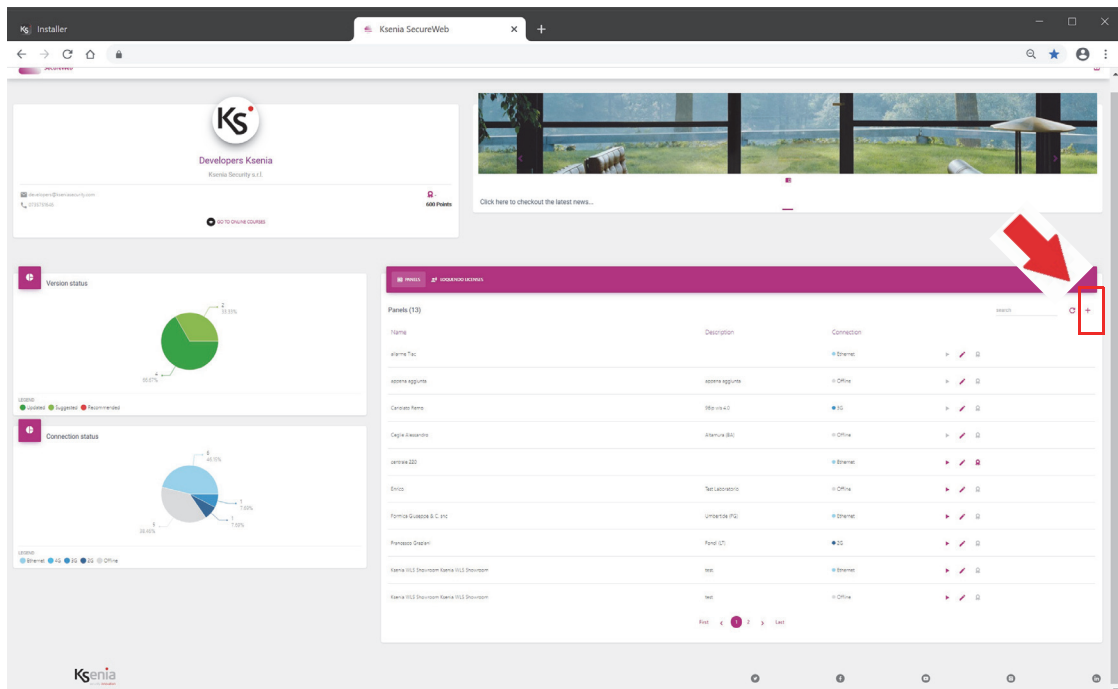
**From APP Ksenia PRO:**

1. Open the APP “Ksenia PRO” and enter the credentials;
2. click on the (+) symbol in the bottom right hand corner (Android) or in the top left hand corner (IOS);
3. type the serial number or click on the camera icon to scan the QR code (this is also shown on the control panel label);
4. make sure you do this if the message appears asking you for access to use the camera;
5. give the control panel a name and a description;
6. click on <Save>.

**The control panel is ready to be configured by using Ksenia SecureWeb and it will be present in the “devices” list.**

## 2.2 Activating the voice licence

1. After successful login, **www.kseniasecureweb.com** page will open;
2. to **add** a new voice licence click on **<+>** sign in the **Loquendo Licence** section, see the following image;

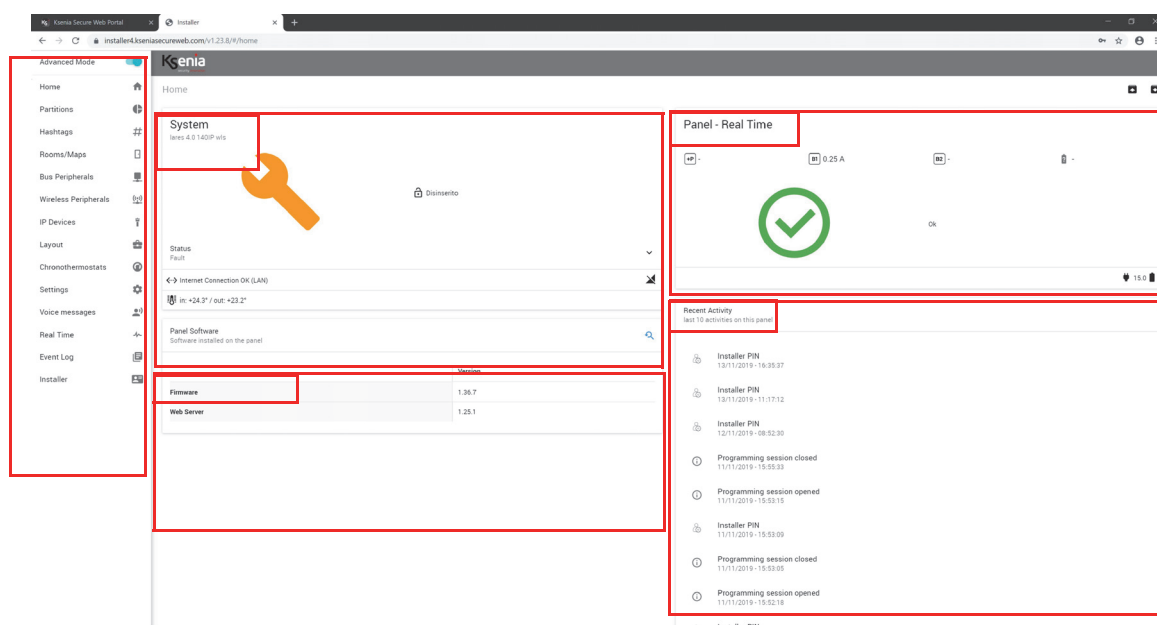


3. insert the serial number printed on the scratch card and click on **<SAVE>**;
4. make the choice of the voice.

## 2.3 Description of HOME page of Installer program

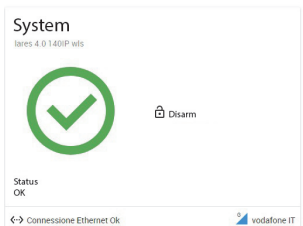
See below the HOME page of a control panel already configured:

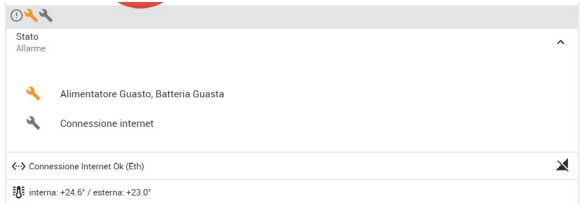
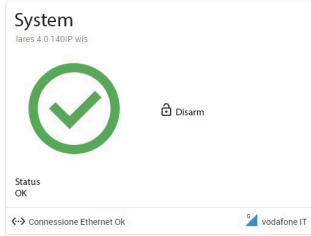
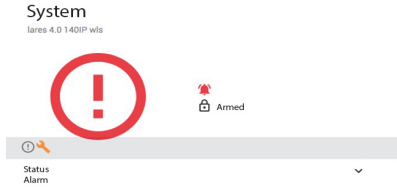
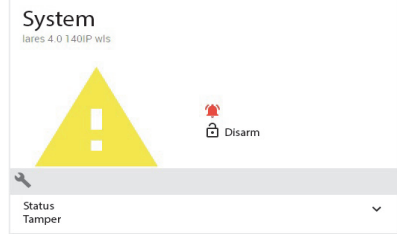
- on the left side of the page the programming menu is present, refer to chapter [“DESCRIPTION OF THE INSTALLER PROGRAM MENU” page 19](#) for all details;
- the space remained is divided into four sections with dynamic information regarding:
  - System:** description of the lares 4.0 control panel connected, armed/disarmed, alarm/fault/sabotage status, eth connections, temperature, GSM signal;
  - Panel Software:** software version installed and updates;
  - Panel Real Time:** card power supply voltage status and battery recharge voltage;
  - Recent activity:** list of the 10 last events occurred in the control panel and stored in the Event log.

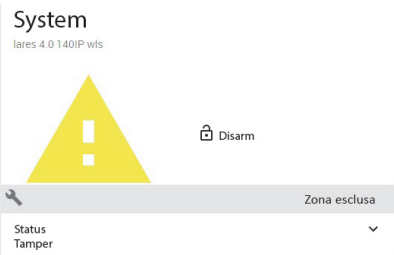

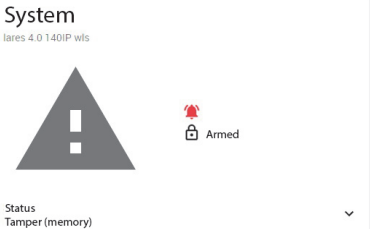


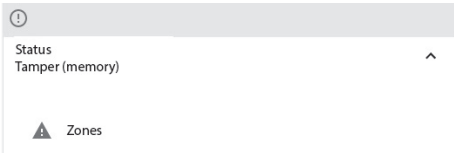
### 2.3.1 Description of the dynamic information

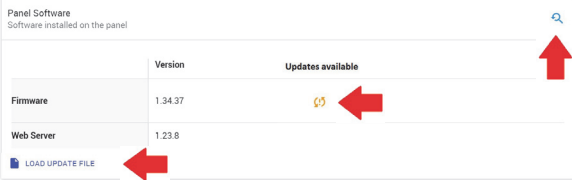


The table below describes the information that you can see in the HOME page, subdivided per section.




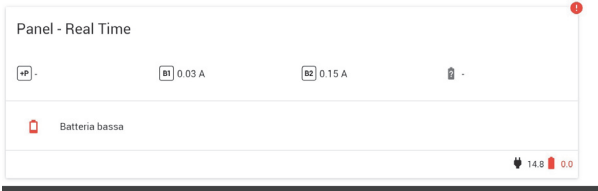
SYSTEM section	Description
	<p>No failure is present.          No fault and tamper memory are present.          Fault memory has been reset from webserver and from keyboard.          The panel is disarmed.</p>

 <p>The screenshot shows the 'Stato Allarme' (Alarm Status) section. It lists 'Alimentatore Guasto, Batteria Guasta' (Power supply fault, Battery fault) and 'Connessione internet' (Internet connection). Below, it shows 'Connessione Internet Ok (Eth)' and temperature readings: 'interna: +24.6° / esterna: +23.0°'.</p>	<p>↔ Internet connection OK (Eth) or Internet connection OK (gemino IoT).</p> <p>⚠ Connection without Internet.</p> <p>👤 This indicates that the user connected is in "programming" session.</p> <p>📶 <b>vodafone IT</b> This indicates the GSM/GPRS provider in use and a full signal strength.</p> <p>📶 <b>vodafone IT</b> This indicates the GSM/GPRS provider in use and the signal strength.</p> <p>📶 There is no GSM or SIM signal.</p> <p>🌡 The temperatures (internal and external) detected by the Bus sirens are displayed.</p>
 <p>The screenshot shows the 'System' status with a large green checkmark. It indicates 'Status OK' and 'Disarm'.</p>	<p><b>SYSTEM FAULT IN PROGRESS</b> Fault conditions are present. The panel is disarmed.</p>
 <p>The screenshot shows the 'System' status with a large red exclamation mark. It indicates 'Status Alarm' and 'Armed'.</p>	<p><b>ALARM IN PROGRESS</b> Alarm signal in progress, zone or partition.</p>
 <p>The screenshot shows the 'System' status with a large yellow triangle containing an exclamation mark. It indicates 'Status Tamper' and 'Disarm'.</p>	<p><b>TAMPER IN PROGRESS</b> Fault or tamper system and alarm condition still in progress (i.e. Sirens still active). Click on the little arrow (right bottom) to open the drop down box with the list of faults or anomalies of the panel.</p>

	<p>Tamper system in progress but alarm condition stopped.</p> <p>Click on the little arrow (right bottom) to open the drop down box with the list of faults or anomalies of the panel.</p>
	<p>List of faults or anomalies of the panel.</p> <p>The image shows the presence of faults/anomalies in one or more zones.</p> <p>More than one events can be displayed.</p>
	<p>List of tampers in the system.</p> <p>The image shows the presence of tampers in one or more zones and there is an Internet connection anomaly in memory.</p>
	<p><b>TAMPER MEMORY</b> <b>ALARM IN PROGRESS</b></p> <p>The image shows a restored tamper condition (tamper memory) but the alarm is still in progress (red little bell).</p>
	<p><b>TAMPER MEMORY</b></p> <p>The image shows that a tamper memory is present.</p> <p>Click on the little arrow (right bottom) to open the drop down box with the list of tampers memory of the panel.</p>
	<p><b>FAULT MEMORY</b></p> <p>The image shows that a fault memory is present.</p> <p>Click on the little arrow (right bottom) to open the drop down box with the list of faults memory of the panel.</p>

	<p>List of tamper memory in the panel. The image shows a zone tamper memory. More than one event can be displayed.</p>
---	--

PANEL SOFTWARE Section	Description
	<p> this icon indicates the presence of new software version available. Click on the icon to start the update and wait until the end of the process.</p> <p> icon for searching updates. For a further search, click on it and wait until the end of the search.</p> <p>“Load update file” button (only for local network connection): from PC/MAC, it starts the firmware update of the control panel.</p>

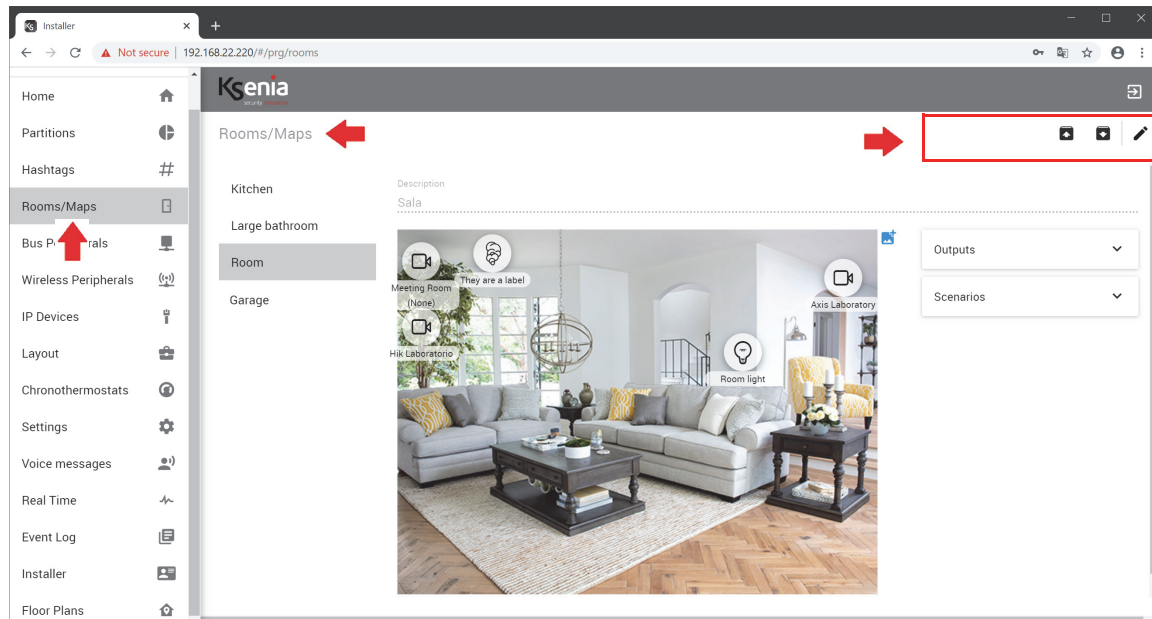
PANEL - REAL TIME Section	Description
	<p>There are no voltage drops:</p> <p> 14.8 Main board voltage supply.</p> <p> 14.3 Battery voltage.</p>
	<p>This image will appear when the battery voltage level drops below the threshold (&lt;11V) or if it has been disconnected from the control panel.</p>

### 3. DESCRIPTION OF THE INSTALLER PROGRAM MENU

Description of the "Installer" program web pages, following the order of the menu items of which it is composed.

#### 3.1 Quick guide to navigate web pages


Clicking on a menu or sub-menu item, the correspondent window will open next to it.



The command keys positioned on the upper side of the programming windows may vary in dynamic mode, depending on the actions required.


#### 3.1.1 How to change the data - Open session





Open a web configuration page and click on "Open session"  to enter insertion or modification mode.

### 3.1.2 How to save the data - Save session and Apply session




You can make so many partial saving as you need just by clicking on “Save session”  icon, every partial saving


can be discarded by clicking on “Cancel changes”  icon.

But only after you click on “Apply session”  icon the control panel receives the new configuration and this operation cannot be undone.

### 3.1.3 How to cancel the data inserted or changed


All the modifications can be undone just by clicking on “Cancel changes”  icon, before you click on “Apply



session”  icon, after that the saving is final and sent to the control panel and cannot be undone.

### 3.1.4 How to export a layout configuration




Click on  “Save configuration on disk” icon to export the configuration file of the control panel on a disk . The control panel reads both .bck files which only contain the control panel programming backup (for backwards compatibility), and .ksa files which can always contain the configuration of the control panel and eventually, the knx.json file which contains the configuration of the konnex device.



### 3.1.5 How to import a layout configuration




Click on  "Load configuration from disk" icon to load the configuration file before saved (.bck extension).

### 3.1.6 How to exit from Installer



If no changes have been made after opening the edit/insert session, click on the "Close session" button  .



Click on the button  to exit from the Installer and return to the login page, whenever you want.

**Warning!** This operation quits the program without saving the data inserted/modified (not saved before).

### 3.1.7 Cross checking of data inserted

If a conflict rises out due to inserted data, the programming won't be complete and won't be saved and an red icon with a red exclamation mark appears in the command bar, as shown in the following image:





Click on this icon, a message will tell you the incomplete structures, so that you can change and save them.

After having adjusted the incomplete structures, "Save session"



icon will appear again and gives you the opportunity to save the new configuration.


## 3.2 HOME menu

See the paragraph ["Description of HOME page of Installer program" page 15](#).

## 3.3 Partition menu

The partitions are groups of sensors/zones that logically can be grouped according arming/disarming zones, for example: "perimeter sensors", "volumetric sensors", "ground floor windows", "first floor windows", "garden lights".

The configuration parameters available are the following:

<b>Description</b>	Give a name to the partition (i.e. outdoor sensors, windows, volumetric, etc.).
<b>Exit</b>	Exit delay timer (expressed in seconds) during which the zones programmed with it, will not generate an alarm, even if violated.
<b>Entry</b>	<p>Entry delay timer (expressed in seconds), during which the zones programmed with it, will not generate an alarm, even it violated.</p>  <p><b>Note:</b> the maximum entry delay timer must not exceed 45 sec., compliant with the EN 50131 standard.</p>
<b>Cycle</b>	Timer (expressed in minutes) which determines the maximum duration of the alarm cycle. The control panel does not generate partition alarm events during all the alarm timer, but only an alarm event for each zone associated with the partition will be generated. This prevents numerous phone calls or reports from being queued.
<b>Patrol</b>	Timer (expressed in minutes) activated when the system has been switched off with a code or a key with patrol attributes. The partitions will be reinserted automatically when this timer elapses.
<b>Negligency</b>	<p>Timer (expressed in hours) which is activated when disarmed.</p> <p>If the partition is not armed before this period has elapsed, then the 'Partition Negligency' event will be generated. Some actions can be associated (i.e. activating outputs, calls, re-arming modes) to this event and this function could be programmed to resolve any potential errors as "forgot to arm" and "re-arm the control panel automatically".</p>
<b>HTTP endpoints on gateway</b>	<p>This section displays the endpoints exposed by Ksenia device, Gateway Http service enabled, applicable to the PARTITIONS.</p> <p>"Read status GET" and "Edit status using PUT method" APIs, display URL and body (JSON) with which the third-party device communicates with the device Ksenia. Copy and paste the messages to the connected device and edit the suggested values.</p>

### 3.4 Hashtags menu

---

The hashtags are functions that can be applied to: **zones, outputs, users** and **user peripherals** (keypads and proximity readers) and allow you to "break down", for example, the limit of the eight outputs that can be activated for each event.

**Example:** from "scenarios" it is possible to individually activate two outputs (i.e. light1 and light2), but if they are associated with a hashtag "#lights" (or any another name), activating the outputs with "#lights", both of them will be switched on.

### 3.5 Rooms / Maps menu

---

The Room is a grouping that can be associated with zones, outputs, IP cameras, domus, counters, energia meters and scenarios. When one of these elements is associated with a Room, it will be displayed in the user app within the associated room. Each element can also be associated with multiple Rooms, in that case it will be displayed multiple times.

The association with the elements to a Room is done within the configuration page of the element itself.

Once the elements are associated with a Room, it is also possible to draw a Floor Plan (only in local connection and not from mobile devices). Each Room can have a background image, in any graphic format, maximum size 200Kb. It is possible to drag and drop any element associated with the Room into the Map, so the end user will be able to see the status of the system and manage it directly from the Floor Plan.

The configuration parameters available are the following:

<b>Description</b>	Give a name to the room (i.e. kitchen, living room, bedroom, etc.).
<b>Choose an image</b>	Choose or drop an image (i.e. kitchen, living room, bedroom, etc.) that will act as background to the elements you are going to associate with it. Any graphic format is accepted, maximum size 200Kb.

## 3.6 BUS peripherals menu


The BUS peripherals are all those devices (expansion modules, user interfaces, isolators and receivers) connected to the BUS of the motherboard of the *lares 4.0* control panel.

The BUS peripherals configuration web pages allow the following operations:

- [“Automatic BUS peripherals acquisition” page 24 ;](#)
- [“Read the status of BUS peripherals in real time” page 26 ;](#)
- [“Programming BUS peripherals” page 27 ;](#)
- [“Programming BUS peripherals without configuring the Serial Number” page 34](#)
- [“Add / cancel the BUS peripherals” page 34 .](#)

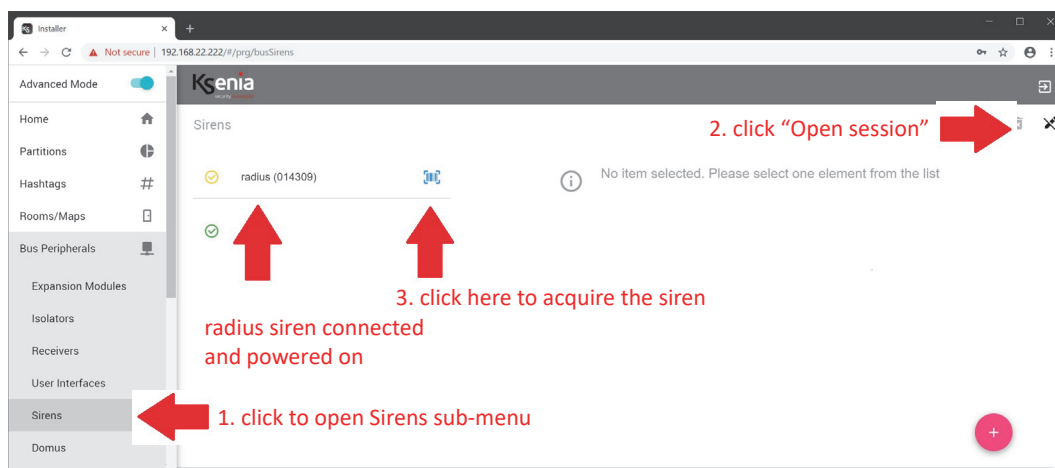
### 3.6.1 Automatic BUS peripherals acquisition

The connected peripherals that communicate with the BUS are shown on the left side of the configuration page under sub-menus: "Expansion modules", "Isolators", "Receivers", "User interfaces", "Sirens", "domus", "energia".

To acquire a connected and powered on peripheral device, click on “Open session”  icon (if not already open).

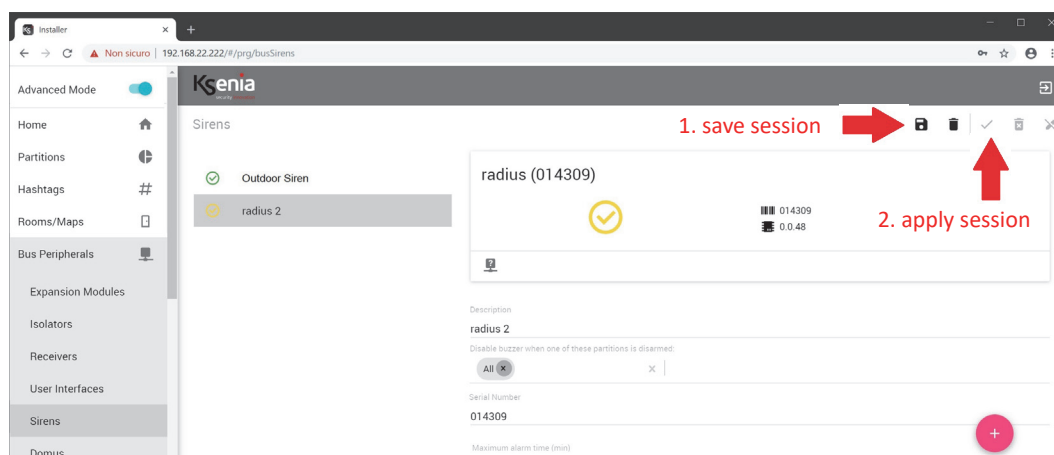
#### 3.6.1.1 Acquiring a radius siren - Example

1. Open BUS Peripheral -> Sirens

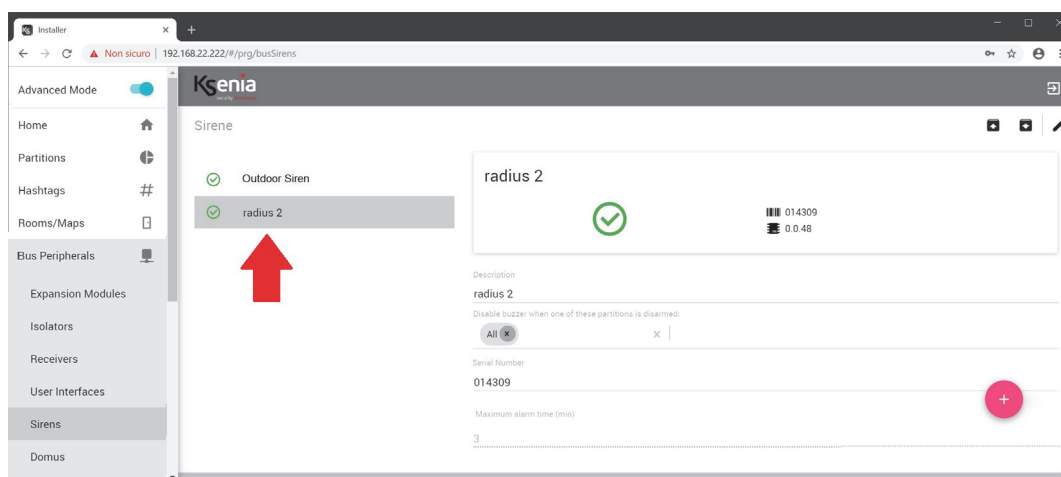


If the device does not appear, may be it has not been connected correctly or it is not powered on or it does not communicate with the BUS.

2. An immediate acquisition occurs and soon after the page appears as shown in the next image. Now it is necessary save and apply the session.



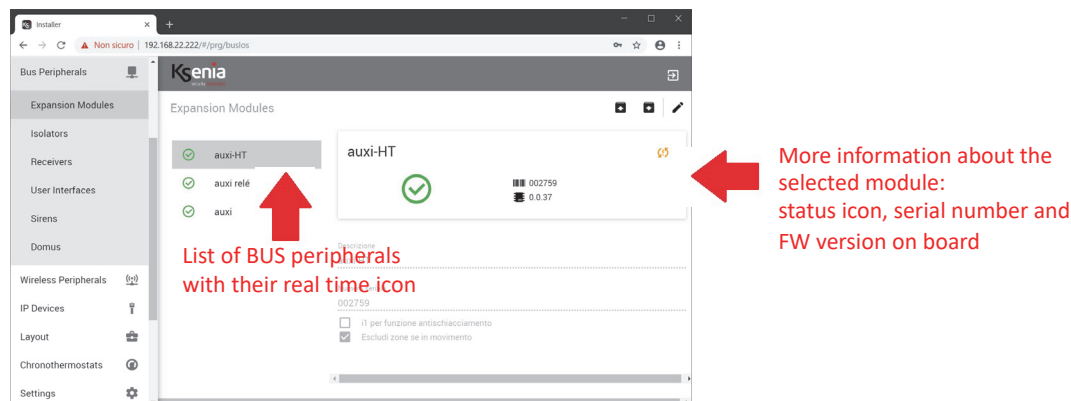
3. The configuration will be sent to the central panel, at the end of the loading the page changes as shown in the image below.



### 3.6.2 Read the status of BUS peripherals in real time

The following image shows the list of “Expansion modules” and their relative real time icon. In the following tables the possible status are described.

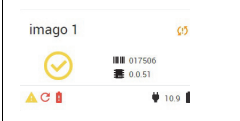
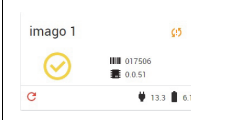

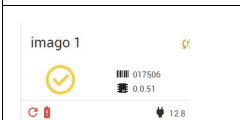
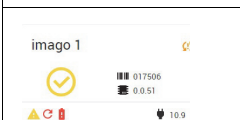
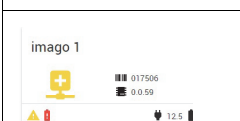
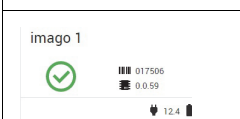
To view more information about the real time, click on a name, as shown in the following image.



The status icons may change as follows:

example: User Interface		Connected and working peripheral. The device name, the serial number and the firmware version are displayed and, if available, also the Firmware Update icon
		Tampering peripheral.
		Missing peripheral.
All the above information are also valid for the BUS peripherals: "Expansion modules", "Isolators", "Receivers". For "domus" and "Sirenes" devices, see the following tables.		

domus		domus is connected and working. Temperature, humidity and light intensity sensor.
-------	--	--

Sirens		Outdoor siren not registered in the central panel. Firmware update detected. Power Supply Failure (missing buffer battery)
		Outdoor siren acquired in the central panel: Firmware to be updated. Power supply voltage detected on board and on buffer battery.
		BUS siren voltage. Buffer battery voltage.
		Siren acquired and updated. Battery failure or missing.
		Siren acquired, tamper and to be updated. Battery failure or missing.
		Siren updated and in synchronization phase with the Bus. Battery failure.
		Updated and working siren.

### 3.6.3 Programming BUS peripherals

See below the description of the configuration parameters available, they are different according to the type of peripheral module.

#### 3.6.3.1 Expansion modules

List of expansion modules programmable:

- **auxi**: 5 inputs/outputs expansion module.
- **auxi 10in**: 10 inputs expansion module.
- **auxi relè / auxi-L**: 5 relay 8A expansion module.
- **auxi-HT**: 2 outputs relay 8A expansion module and 3 inputs (+ 2 local inputs for managing the outputs directly)
- **auxi-HL**: 2 outputs relay 8A expansion module and 3 inputs (+ 2 local inputs for managing the outputs directly)

The configuration parameters available are the following:

<b>Description</b>	Give a name to the peripheral module.
<b>Serial number</b>	6 digits code which identifies the peripheral module. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">“Programming BUS peripherals without configuring the Serial Number” page 34</a> )
For <b>auxi-HT</b> peripheral module it is necessary to configure the following fields as well:	
<b>“i1” for crush prevention</b>	If enabled, “i1” input can be used to connect a safety device (i.e. a photocell). When the safety device is activated during the roller shutter closing, it will stop the closure and completely reopen.
<b>Bypass input “t” while moving</b>	If enabled, when the roller shutter is moving, the counter mode analysis will be deactivated and will not generate any alarm.
For <b>auxi-HL</b> peripheral module it is necessary to configure the following fields as well:	
<b>Inputs mode</b>	It allows to distinguish the processing mode of the two inputs: it is possible to choose between <b>button</b> (once released, it returns to its initial position) or <b>switch</b> (On/Off).

### 3.6.3.2 Isolators

List of isolators programmable:

- **divide**: BUS isolator and repeater.
- **opis**: supervised power supply station

The configuration parameters available are the following:

<b>Description</b>	Give a name to the isolator.
<b>Serial number</b>	6 digits code which identifies the isolator. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">“Programming BUS peripherals without configuring the Serial Number” page 34</a> )



### 3.6.3.3 Receivers

List of receivers programmable:

- **duo**: wireless receiver.

The configuration parameters available are the following:

<b>Description</b>	Give a name to the receiver
<b>Serial number</b>	6 digits code which identifies the receiver. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">“Programming BUS peripherals without configuring the Serial Number” page 34</a> )

### 3.6.3.4 User interfaces

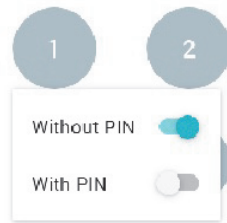
List of user interfaces/keypads programmable:

- **ergo-rev.0**: hw version produced until May 2017.
- **ergo S**: "cap sense" version with temperature sensor.
- **ergo M**: version with mechanical press-buttons.
- **ergo**: keypad version produced after May 2017.
- **volo**: outdoor proximity reader.
- **volo-in**: indoor proximity reader housed in standard box 503.

The configuration parameters available are the following:

<b>Description</b>	Give a name to the user interface
<b>Serial number</b>	6 digits code which identifies the user interface. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">“Programming BUS peripherals without configuring the Serial Number” page 34</a> )
<b>Hashtags</b> (see <a href="#">“Hashtags menu” page 23</a> )	Click on the arrow next to the field to open the menu with the list of hashtags previously programmed. It is possible to associate one or more hashtags to the same device.
<b>Partitions</b> (see <a href="#">“Partition menu” page 22</a> )	Click on the arrow next to the field to open the menu with the list of partitions previously programmed. It is possible to associate one or more partition to the same device.
<b>Display date and time</b>	Enable/disable date and time on the second row of keypad display
<b>Display External temperature</b>	Enable/disable external temperature measured by "imago" siren on the second row of keypad display.
<b>Display Internal temperature</b>	Enable/disable internal temperature measured by "radius" siren on the second row of keypad display.

<b>Display GSM Status</b>	Enable/disable GSM signal and the provider name on the second row of keypad display (a GSM/GPRS communicator must be present in the central panel).
<b>Display arming status</b>	Enable/disable the arm status on the second row of keypad display. Furthermore, by enabling this option it will be possible to view the status of one partition at a time, by pressing the key (#), with the keypad on idle; to pass to the following press the scroll keys of the keypad provided.
<b>Display zones status</b>	Enable/disable the status of zones in alarm on the second row of the keypad display. Furthermore, by enabling this option it will be possible to view the status of one zone at a time, by pressing the key (*), with the keypad on idle; to pass to the following press the scroll keys of the keypad provided. If enabled, the led green will remain steady on, for indicating that all zones of partitions associated to it, are in idle.
<b>Led timeout</b>	Time (seconds) during which the LED is activated to confirm an operation correctly performed
<b>Tamper sensitivity</b>	You can set the sensitivity level of tamper accelerometer according to the following values: 0 = disable completely the management of the accelerometer; values from 1 to 5 = indicate the sensitivity vibration level for the detection of tamper (1 lower sensitivity .... 5 higher sensitivity).
<b>Acoustic feedback during exit time</b>	Enable/disable the acoustic feedback of the keypad during exit time.
<b>Acoustic feedback during entry delay</b>	Enable/disable the acoustic feedback of the keypad during entry delay.
<b>Chime</b>	Enable/disable the acoustic feedback on the keypad associated to the zones with chime (little ringing) as attribute.
<b>Acoustic feedback during warning time</b>	Enable/disable the acoustic feedback of the keypad during warning time.
<b>Warning with pin</b>	The system status is not shown on the first line of the keypad when selecting this option ( <b>SYSTEM OK, ALARM, TAMPER, etc.</b> ) until a valid PIN is entered.
<b>Acoustic feedback during alarm cycle</b>	Enable/disable the acoustic feedback of the keypad during alarm cycle.
<b>Capsense sensitivity</b>	The sensitivity level for detecting keys can be set in this field. You can select between three conditions: low/medium/high. <b>IT IS NOT AVAILABLE for ergo M!</b>
<b>Backlight</b>	In this field you can adjust the keypad brightness level. You can select between three conditions: low/medium/high. Select the low mode if you wish the keypad backlight to be disabled in standby mode.
<b>Volume</b>	in this field you can adjust the loudspeaker volume level. You will be able to select between four conditions: low/medium/normal/high/off.
<b>Keys configuration</b>	(enable/disable scenario). A key can be enabled to execute a scenario. Click on a button, select the option 'With pin' if you want to enable the button for execution only after having entered a valid pin, select 'Without pin' if you want to enable execution without inserting a pin, but simply holding pressed the button for three seconds.



The image shows “Without **PIN**” enabled and “With **PIN**” disabled.

### 3.6.3.5 Sirens

List of sirens programmable:

- **imago**: outdoor siren with temperature sensor on board.
- **radius**: indoor siren with temperature sensor on board and emergency light.

The configuration parameters available for **imago** outdoor siren are the following:

<b>Description</b>	Give a name to the siren
<b>Serial number</b>	6 digits code which identifies the siren. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">“Programming BUS peripherals without configuring the Serial Number” page 34</a> .)
<b>Maximum alarm time (min.)</b>	Maximum alarm time of acoustic and luminous signaling of the siren, occurred after the cutting of wires.
<b>BUS Control</b>	If enabled, in case of absence of communication with the control panel for more than 10 seconds, the siren will make acoustic and luminous signal.
<b>Temperature sensor</b>	If disabled, the siren does not send the temperature to the control panel and the external temperature will not be displayed on the keypad (this is useful if there are two sirens, and one is installed in a position exposed to the sun, making false the external temperature measurement).
<b>Note:</b> Also the keypad must be enabled to display the external temperature.	
<b>Dual-tone buzzer</b>	If enabled, the acoustic signaling is made by a dual-tone sound with two distinct frequencies, otherwise in “sweep” continuous way.

The configuration parameters available for **radius** indoor siren are the following:

<b>Description</b>	Give a name to the siren.
<b>Serial number</b>	6 digits code which identifies the siren. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">“Programming BUS peripherals without configuring the Serial Number” page 34</a> .)

<b>Disable buzzer when one of these partitions is disarmed</b>	The siren will not activate the audible signal if the partition (or the partitions) selected is disarmed (i.e. volumetric sensor). This allows to prevent the siren from ringing if there are persons at home (i.e. arm with volumetric partition disarmed). If you want that the siren sounds independently from the arming mode, do not associate any partition.
<b>Maximum alarm time (min.)</b>	Maximum alarm time of acoustic and luminous signaling of the siren, occurred after the cutting of wires.
<b>Fixed led</b>	If this option is selected, when the output associated in the "Lamp Only" section is activated, the LED lights steadily (instead of blinking).
<b>Emergency light</b>	If enabled, when a mains failure occurs, the siren turns on the power LED, lighting up a medium-sized room. Warning! It is necessary to install the lithium battery on the siren to allow the operation as an emergency light.
<b>Temperature sensor</b>	If disabled, the siren does not send the temperature to the control panel.

### 3.6.3.6 Sensors

Configuration of BUS sensors connected to lares 4.0 BUS.

Sensor programmable:

- **matrix:**
  - select one of the following functions to be programmed:
    - **<universal>** - **<Optex BXS>** - **<Optex VXS>** - **<Optex WXI>** - **<Optex WXS>** - **<Optex QXI>**. Each OPTEX serie open a further menu to choose a model of the selected serie.


The following tables describe the configuration parameters of UNIVERSAL matrix BUS:


UNIVERSAL matrix BUS	
<b>Description</b>	Give a name to the peripheral module (i.e. outdoor terrace sensor).
<b>Serial number</b>	6 digits code which identifies the peripheral module. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Sensor type</b>	Display the sensor chosen.
<b>Enable +P</b>	Enable/disable the +P power supply in case of UNIVERSAL.
<b>Accelerometer</b>	Enable/disable thornproof MEMS accelerometer (default: disabled).

There is a BUZZER on board for identifying the position of the sensor in the system.

The **real time** section of the device displays: the voltage value of the BUS, the fuse status (green icon OK , red icon KO) and the power supply terminal +P and the BUZZER status (ON = red icon / OFF = blue icon).

Always from the **real time** section, the duration of the BUZZER sound can be programmed when the command will

be sent, by clicking on icon  . To stop the timer, set the duration = 1(sec.); just in case matrix BUS is in

UNIVERSAL mode, it is also possible to click on icon  to turn it off for a programmable time of X seconds when the command is sent (useful, for instance, to reset the smoke sensors).

**NOTE!** The configuration of matrix BUS for Optex BXS - VXS - WXI - WXS - QXI, is the same described for the matrix sensor ("Wireless sensors" page 40 -> matrix).

### 3.6.3.7 domus

**domus** is a multi-function sensor with the following characteristics: motion, temperature, humidity and light intensity sensor.

The configuration parameters available for **domus** multi-function sensor are the following:

<b>Description</b>	Give a name to the multi-function sensor.
<b>Serial number</b>	6 digits code which identifies the multi-function sensor. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">"Programming BUS peripherals without configuring the Serial Number" page 34</a> .)
<b>Partitions</b> (see <a href="#">"Partition menu" page 22</a> )	Click on the arrow next to the field to open the menu with the list of partitions previously programmed. It is possible to associate one or more partition to the same device.
<b>Rooms</b> (see <a href="#">"Rooms / Maps menu" page 23</a> )	Click on the arrow next to the field to open the menu with the list of Rooms/Maps previously programmed. It is possible to associate one or more rooms to the domus, in such a way it can be managed directly from "Floor Plans" menu.
<b>Humidity sensor</b>	Enable / Disable humidity sensor.
<b>Humidity event threshold (%)</b>	Humidity threshold used to generate the Dry Environment/Wet Environment events. This value is expressed as a percentage and ranging from 30% to 90%. A fixed hysteresis of 2% will be considered for event generation.
<b>Brightness event threshold (lux)</b>	Brightness threshold (lux) used for generating Lux Sensor events. This threshold is also used to limit the generation of motion detection events in case of high brightness (if enabled). Possible values: from 0 to 1500. A fixed hysteresis of 5% will be considered for event generation.
<b>Filter pir event basing on brightness</b>	If enabled, the movement detection event is generated only in case of brightness below the indicated threshold.
<b>Temperature sensor</b>	Enable / Disable temperature sensor.
<b>Temperature offset</b>	Offset that will be applied to the detected temperature. Possible value: from -5 to +5.

### 3.6.3.8 energia

**energia** module allows the power consumption management, it provides two distinct power lines on which measuring both voltage and current, each line can support loads up to 6kW. The values of the voltage of the two lines expressed in Volts and the current measured on each line L1 and L2 expressed in Ampere are displayed in real time.

The configuration parameters available for **energia** module are the following:

<b>Description</b>	Give a name to identify the module.
<b>Serial number</b>	6 digits code which identifies the module. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">“Programming BUS peripherals without configuring the Serial Number” page 34.</a> )

### 3.6.4 Programming BUS peripherals without configuring the Serial Number

It is possible to add a BUS peripheral configuration without setting its serial number, by enabling the <Ignore> button.

Also, the saving data is allowed, it is indicated by yellow warnings as well as the peripherals name and related menu items are coloured in yellow. The outputs and zones configuration associated to these peripherals is allowed too, but they won't be displayed on the real time page.





The real peripheral association by typing the serial numbers previously ignored, can be performed later.






Quick association can be made by clicking on the barcode button: if some peripherals of the same type with serial number not associated are present, a list of them will appear so you just have to choose one from it.

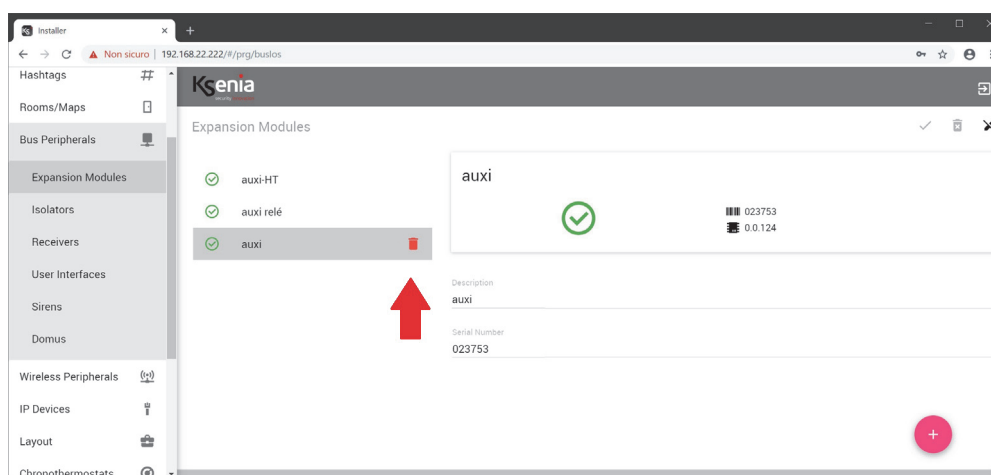
### 3.6.5 Add / cancel the BUS peripherals

In addition to the automatic BUS peripherals acquisition (described in the paragraph [“Automatic BUS peripherals acquisition” page 24.](#)), it is possible to add the BUS peripherals manually.

- **To add manually** the modules, it is necessary to open the menu related to the type of peripheral to be configured:

1. Click on “Open session”  icon (if not already open)
2. Click on  <+> red icon to add a new peripheral
3. Click on the  <+> blue icon relative to the peripheral chosen (among the list of peripherals proposed)
4. Type the serial number printed on the peripheral label
5. To add a new one peripheral and you are in the same session, click again on  <+> red icon
6. Complete or modify the configuration parameters available



7. Click on  Save session icon (until now, still the changes can be discarded by clicking on  cancel changes icon). Click on “Apply session”  icon to make the new configuration effective.
- **To cancel a BUS peripheral**, enter the sub-menu of interest, click on “Open session”  icon (if not already open), click on the peripheral name to cancel and click on  (red bin) icon next to it.



“Confirm Remove” is required: press <Remove> to confirm or <Cancel> to reject.

Confirm Remove

Are you sure you want to remove the item?

 CANCEL  REMOVE

## 3.7 Wireless peripherals

The wireless peripherals are all those devices (sirens, repeaters, expansion modules, sensors, keypads) connected to the *lares 4.0* control panel via radio/wireless on 868 MHz band.








The Wireless peripherals configuration web pages allow the following operations:

- [“Acquisition of wireless peripherals” page 36](#) ;
- [“Read the status of wireless peripherals in real time” page 37](#) ;
- [“Programming wireless peripherals” page 38](#) ;
- [“Programming Wireless peripherals without configuring the Serial Number” page 49](#)
- [“Cancel wireless peripherals” page 49](#).

### 3.7.1 Acquisition of wireless peripherals

The wireless peripherals are grouped according the type and then identified one by one for properly programming even the smallest differences among them.

To add/modify the wireless peripherals, open the sub-menu of the peripheral to be configured (i.e. “Wireless peripherals -> Wireless sensors”):

1. Click on “Open session”  icon (if not already open)
2. Click on  <+> red icon to add a new peripheral
3. Click on the  <+> blue icon relative to the peripheral chosen (among the list of peripherals proposed)
4. Type the serial number printed on the peripheral label
5. To add a new one peripheral and you are in the same session, click again on  <+> red icon
6. Complete or modify the configuration parameters available
7. Click on  Save session icon (until now, still the changes can be discarded by clicking on  cancel changes icon).
8. Click on “Apply session”  icon to make the new configuration effective.



#### About programming “Supervision time”

In some wireless devices, it is required to program the supervision time.

The monitoring interval represents the maximum time that elapses between two transmissions by the same wireless device even if no status change occurred, such as, for example, an alarm.

These periodic communications are used by the control panel to verify the persistence of the radio link with all wireless devices. The higher this value is, later the control panel will notice the radio link loss with the wireless devices.

On the other hand, programming a very low value can shorten the battery life due to more frequent transmission by the devices. Depending on the programmed value, the behaviour of the control panel in the generation of the messages concerning the radio communication fault or tampering varies as described below.

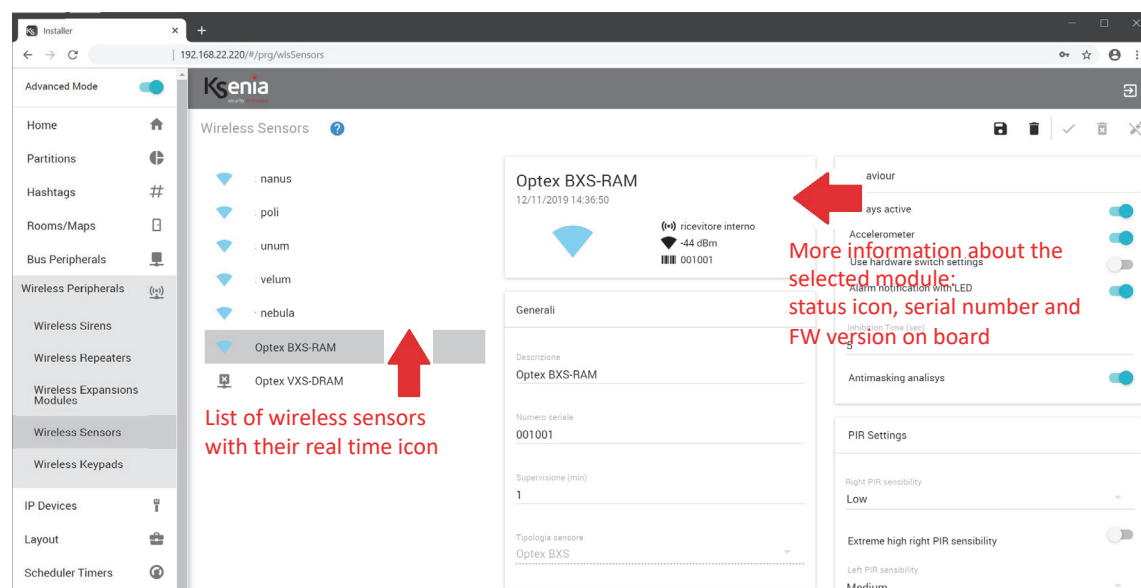


- If the wireless devices are programmed with a monitoring interval equal to 1 minute, the control panel generates a “**wireless fault**” and the “**loss of wireless device**” event if it does not receive any transmission in a 100-second interval.
- If all wireless devices are programmed with a monitoring interval of more than 1 minute, the “**loss of wireless device**” event is generated in case the control panel does not receive any transmission from the single device for a period equal to the greater one of 2 hours and the double of the monitoring interval programmed for the device.
- The control panel does not check the integrity of the radio link for devices that have a monitoring interval = 0 (zero).
- We recommend using this programming only for devices used in home automation applications and not for security applications.


### 3.7.2 Read the status of wireless peripherals in real time

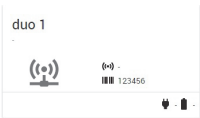

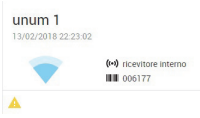

The following image shows the list of “Wireless sensors” and their relative real time icon. In the following tables the possible status are described.

To view more information about the real time, click on a name, as shown in the following image.



The status icons may change as follows:

Wireless signal indicator		Radio signal 1 (greater than -76dBm) Radio signal 2 (between -90dBm and -76dBm) Radio signal 3 (between -100dBm and -91dBm) Radio signal 4 (lower than -101dBm)	
---------------------------	---	--	--

<b>Repeaters wls</b>  <b>Sensors wls</b>  <b>Sirens wls</b>  <b>Expansion modules wls</b>  <b>Keypads wls</b>		Wireless sensor programmed but there isn't communication with the control panel	
		Updated and working wireless sensor  Wireless peripheral updated and working. Date and time of the last transmission. Receiver with communication in progress. Radio signal 1	
		Tampering wireless peripheral	
		Voltage measure.  Buffer battery voltage.	

### 3.7.3 Programming wireless peripherals

See below the description of the configuration parameters available, they are different according to the type of peripheral module.

#### 3.7.3.1 Wireless sirens

List of sirens programmable:

- **imago WLS**

The configuration parameters available are the following:

<b>Description</b>	Give a name to the peripheral module.
<b>Serial number</b>	6 digits code which identifies the peripheral module. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">“Programming Wireless peripherals without configuring the Serial Number” page 49</a> )
<b>Supervision time interval (min)</b>	You can set the supervision interval for wireless diagnostic (minutes) (see also <a href="#">“About programming “Supervision time”” page 36</a> .
<b>Temperature sensor</b>	If disabled, the siren does not send the temperature to the control panel and the external temperature will not be displayed on the keypad.
<b>Note:</b> Also the keypad must be enabled to display the external temperature.	
<b>Dual-tone buzzer</b>	If enabled, the acoustic signaling is made by a dual-tone sound with two distinct frequencies, otherwise in “sweep” continuous way.

### 3.7.3.2 Wireless repeaters

List of sirens repeaters programmable:

- **duo** (external power supply and backup battery).

The configuration field are the following:

<b>Description</b>	Give a name to the peripheral module (i.e. repeater first floor).
<b>Serial number</b>	6 digits code which identifies the peripheral module. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">“Programming Wireless peripherals without configuring the Serial Number” page 49</a> )

### 3.7.3.3 Wireless expansion modules

List of expansion modules programmable:

- **auxi wls**

The configuration parameters available are the following:

<b>Description</b>	Give a name to the peripheral module (i.e. switching on outdoor light).
<b>Serial number</b>	6 digits code which identifies the peripheral module. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">“Programming Wireless peripherals without configuring the Serial Number” page 49</a> )
<b>Output mode</b>	<p>The outputs can be programmed to operate in one of the following modes:</p> <ul style="list-style-type: none"> <li>• <b>Independent output:</b> the outputs associated with the device are completely independent.</li> <li>• <b>Single output:</b> the two outputs on the device are treated as a single logic output. The first one is normally open and the second one is normally closed. This operating mode uses only one control panel output.</li> <li>• <b>Interlocked:</b> in this mode, which is particularly useful for controlling the electric motors, the outputs cannot be simultaneously active. If the activation of an output is commanded, while the other is active, the switching will be preceded by the deactivation of both outputs for half a second.</li> </ul>

### 3.7.3.4 Wireless sensors

Sensors programmable:

- **nanus**

The configuration parameters available are the following:

<b>Description</b>	Give a name to the peripheral module (i.e. kitchen window contact).
<b>Serial number</b>	6 digits code which identifies the peripheral module. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">“Programming Wireless peripherals without configuring the Serial Number” page 49</a> )
<b>Supervision time interval (min)</b>	You can set the supervision interval for wireless diagnostic (minutes) (see also <a href="#">“About programming “Supervision time”” page 36</a> .

Sensor programmable:

- **poli**

The configuration parameters available are the following:

<b>Description</b>	Give a name to the peripheral module (i.e. entrance door contact).
<b>Serial number</b>	6 digits code which identifies the peripheral module. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">“Programming Wireless peripherals without configuring the Serial Number” page 49</a> )
<b>Supervision time interval (min)</b>	You can set the supervision interval for wireless diagnostic (minutes) (see also <a href="#">“About programming “Supervision time”” page 36</a> .

Sensor programmable:

- **unum**

The configuration parameters available are the following:

<b>Description</b>	Give a name to the peripheral module (i.e. living room sensor).
<b>Serial number</b>	6 digits code which identifies the peripheral module. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">“Programming Wireless peripherals without configuring the Serial Number” page 49</a> )
<b>Supervision time interval (min)</b>	You can set the supervision interval for wireless diagnostic (minutes) (see also <a href="#">“About programming “Supervision time”” page 36</a> .

<b>Inhibition time (sec.)</b>	<p>this is the time (expressed in seconds) between the transmission of two alarms. To save the battery power, the detector emits only one alarm during the set interval time, even if the events that generate the alarms are multiple.</p> <p><b>Minimum configurable time:</b> 5 seconds.  <b>Maximum configurable time:</b> 300 seconds.</p> <p>Note: the inhibition time is set at 5 steps interval.</p>
<b>PRI always active</b>	<p>If disabled, the sensor detects any movements only when the system is switched on. When this option is enabled, the detection analysis carried out by the sensor is always active. Use this option in case of home automation applications.</p> <p>After the arming, there may be a maximum delay of 80 seconds before the sensor is fully operational.</p>

Sensor programmable:

- **velum**

The configuration parameters available are the following:

<b>Description</b>	Give a name to the peripheral module (i.e. outdoor terrace sensor).
<b>Serial number</b>	6 digits code which identifies the peripheral module. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">“Programming Wireless peripherals without configuring the Serial Number” page 49</a> )
<b>Supervision time interval (min)</b>	You can set the supervision interval for wireless diagnostic (minutes) (see also <a href="#">“About programming “Supervision time”” page 36</a> .
<b>Inhibition time (sec.)</b>	<p>this is the time (expressed in seconds) between the transmission of two alarms. To save the battery power, the detector emits only one alarm during the set interval time, even if the events that generate the alarms are multiple.</p> <p><b>Minimum configurable time:</b> 5 seconds.  <b>Maximum configurable time:</b> 300 seconds.</p> <p>Note: the inhibition time is set at 5 steps interval.</p>
<b>PRI always active</b>	<p>If disabled, the sensor detects any movements only when the system is switched on. When this option is enabled, the detection analysis carried out by the sensor is always active. Use this option in case of home automation applications.</p> <p>After the arming, there may be a maximum delay of 80 seconds before the sensor is fully operational.</p>
<b>Thornproof</b>	Enable/disable thornproof MEMS accelerometer.
<b>Antimasking analysis</b>	<p>Antimasking analysis can be set as follow:</p> <ul style="list-style-type: none"> <li>- <b>Disabled:</b> the function is disabled.</li> <li>- <b>Standard:</b> masking in 10 minutes.</li> <li>- <b>Fast:</b> masking in 180 seconds</li> </ul>

Sensor programmable:

- **nebula**

The configuration parameters available are the following:

<b>Description</b>	Give a name to the peripheral module (i.e. kitchen optical smoke detector).
<b>Serial number</b>	6 digits code which identifies the peripheral module. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">“Programming Wireless peripherals without configuring the Serial Number” page 49</a> )
<b>Supervision time interval (min)</b>	You can set the supervision interval for wireless diagnostic (minutes) (see also <a href="#">“About programming “Supervision time”” page 36</a> .

Sensor programmable:

- **matrix:**
  - select one of the following functions to be programmed:
    - **<universal>** - **<Optex BXS>** - **<Optex VXS>** - **<Optex WXI>** - **<Optex WXS>** - **<Optex QXI>**. Each OPTEX serie open a further menu to choose a model of the selected serie.

**WARNING!** Configuration of new OPTEX sensors series WXI, WXS, QXI. matrix devices whose serial number is equal or higher than **004000** are compatible with OPTEX sensors series BXS, VXS, WXI, WXS, QXI; those with a lower serial number are only compatible with OPTEX sensors series BXS, VXS.

The following tables describe the configuration parameters available according to the function selected:

<b>matrix Universal function</b>	
<b>Description</b>	Give a name to the peripheral module (i.e. outdoor terrace sensor).
<b>Serial number</b>	6 digits code which identifies the peripheral module. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">“Programming Wireless peripherals without configuring the Serial Number” page 49</a> )
<b>Supervision time interval (min)</b>	Maximum amount of time (in minutes) between two consecutive transmissions. (Value range from 0 to 240). Disabled if value is 0. (see also <a href="#">“About programming “Supervision time”” page 36</a> .
<b>Sensor type</b>	Display the sensor chosen.
<b>Thornproof</b>	Enable/disable thornproof MEMS accelerometer (default: disabled).

<b>Optex BXS-R / BXS-RAM</b>	
<b>Description</b>	Give a name to the peripheral module (i.e. outdoor terrace sensor).
<b>Serial number</b>	6 digits code which identifies the peripheral module. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">“Programming Wireless peripherals without configuring the Serial Number” page 49</a> )
<b>Supervision time interval (min)</b>	Maximum amount of time (in minutes) between two consecutive transmissions. (Value range from 0 to 240). Disabled if value is 0. (see also <a href="#">“About programming “Supervision time”” page 36</a> .
<b>Sensor type</b>	Display the sensor chosen.
<b>Behaviour:</b>	
<b>PIR always active</b>	If disabled, the sensor detects any movements only when the system is switched on. When this option is enabled, the detection analysis carried out by the sensor is always active. Use this option in case of home automation applications. After the arming, there may be a maximum delay of 80 seconds before the sensor is fully operational.
<b>Thornproof</b>	Enable/disable thornproof MEMS accelerometer (default: disabled).
<b>Use hardware switch settings</b>	If enabled, the sensor will use the hardware switch settings on board. If disabled, the sensor will acquire the configuration according to the settings of the next fields (default: enabled).
<b>Alarm notification with LED</b>	Enable/disable the alarm notification with LED. Referring to OPTEX installation instructions: switch 1. (default: disabled).
<b>Inhibition time (sec.)</b>	This is the inhibition time (in seconds) after the transmission of each alarm. Referring to OPTEX installation instructions: switch 6 .
<b>Antimasking analysis</b>	(ONLY BXS-RAM) Enable/Disable the antimasking analysis. Referring to OPTEX installation instructions: switch 7 .
<b>PIR Settings:</b>	
<b>Right PRI sensibility</b>	It allows to adjust the sensibility of right PIR: low, medium, high. (default: medium).
<b>Extreme high right PIR sensibility</b>	Enable/disable extreme high right sensibility. For environments where the temperature between the human body and the background is very small. Referring to OPTEX installation instructions: switch 5. (default: disabled).
<b>Sensibilità PIR sinistra</b>	It allows to adjust the sensibility of left PIR: low, medium, high. (default: medium)
<b>Extreme high left PIR sensibility</b>	Enable/disable extreme high left sensibility. For environments where the temperature between the human body and the background is very small. Referring to OPTEX installation instructions: switch 4. (default: disabled).

<b>Optex VXS-RAM / VXS-DRAM</b>	
<b>Description</b>	Give a name to the peripheral module (i.e. outdoor terrace sensor).
<b>Serial number</b>	6 digits code which identifies the peripheral module. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">“Programming Wireless peripherals without configuring the Serial Number” page 49</a> )
<b>Supervision time interval (min)</b>	Maximum amount of time (in minutes) between two consecutive transmissions. (Value range from 0 to 240). Disabled if value is 0. (see also <a href="#">“About programming “Supervision time”” page 36</a> .
<b>Sensor type</b>	Display the sensor chosen.
<b>Behaviour:</b>	
<b>PIR always active</b>	Enable/disable PIR sensor always ON.
<b>Thornproof</b>	Enable/disable thornproof MEMS accelerometer (default: disabled).
<b>Use hardware switch settings</b>	If enabled, the sensor will use the hardware switch settings on board. If disabled, the sensor will acquire the configuration according to the settings of the next fields (default: enabled).
<b>Alarm notification with LED</b>	Enable/disable the alarm notification with LED. Referring to OPTEX installation instructions: switch 1. (default: disabled).
<b>Inhibition time (sec.)</b>	This is the inhibition time (in seconds) after the transmission of each alarm. Referring to OPTEX installation instructions: switch 3 . (Value range: 5...255, in steps of 5 sec.).
<b>Antimasking analysis</b>	Enable/Disable the antimasking analysis. Referring to OPTEX installation instructions: switch 4 .
<b>PIR settings:</b>	
<b>PIR sensibility</b>	Adjust PIR sensibility: low, medium, high (default: medium).
<b>Number of PIR pulses</b>	It is the number of pulses necessary before the zone alarm is generated (default: 2). (Value range: 1...4).
<b>Microwave:</b>	
<b>Microwave sensibility</b>	(ONLY VXS-DRAM) The microwave sensibility can be set on five levels: very low, low, medium, high (default), very high.
<b>Microwave immunity</b>	(ONLY VXS-DRAM) Enable/disable the microwave immunity (default: disabled).



Optex WXI-R / WXI-RAM	
<b>Description</b>	Give a name to the peripheral module (i.e. outdoor terrace sensor).
<b>Serial number</b>	6 digits code which identifies the peripheral module. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">“Programming Wireless peripherals without configuring the Serial Number” page 49</a> )
<b>Supervision time interval (min)</b>	Maximum amount of time (in minutes) between two consecutive transmissions. (Value range from 0 to 240). Disabled if value is 0. (see also <a href="#">“About programming “Supervision time”” page 36</a> .
<b>Sensor type</b>	Display the sensor chosen.
<b>Behaviour:</b>	
<b>PIR always active</b>	Enable/disable PIR sensor always ON.
<b>Thornproof</b>	Enable/disable thornproof MEMS accelerometer (default: disabled).
<b>Use hardware switch settings</b>	If enabled, the sensor will use the hardware switch settings on board. If disabled, the sensor will acquire the configuration according to the settings of the next fields (default: enabled).
<b>Alarm notification with LED</b>	Enable/disable the alarm notification with LED. Referring to OPTEX installation instructions: switch 1. (default: disabled).
<b>Inhibition time (sec.)</b>	This is the inhibition time (in seconds) after the transmission of each alarm. Referring to OPTEX installation instructions: switch 6 . (Value range: 5...255, in steps of 5 sec.).
<b>Antimasking analysis</b>	(ONLY WXI-RAM) Enable/Disable the antimasking analysis. Referring to OPTEX installation instructions: switch 8 .
<b>PIR settings:</b>	
<b>Right PIR sensibility</b>	Adjust right PIR sensibility: low, medium, high (default: medium).
<b>Number of right PIR pulses</b>	It is the number of pulses necessary before the zone alarm is generated (default: 2). (Value range: 1...4).
<b>Left PIR sensibility</b>	Adjust left PIR sensibility: low, medium, high (default: medium).
<b>Number of left PIR pulses</b>	It is the number of pulses necessary before the zone alarm is generated (default: 2). (Value range: 1...4).

Optex WXS-R / WXS-RDAM	
<b>Description</b>	Give a name to the peripheral module (i.e. outdoor terrace sensor).
<b>Serial number</b>	6 digits code which identifies the peripheral module. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">“Programming Wireless peripherals without configuring the Serial Number” page 49</a> )

<b>Supervision time interval (min)</b>	Maximum amount of time (in minutes) between two consecutive transmissions. (Value range from 0 to 240). Disabled if value is 0. (see also <a href="#">“About programming “Supervision time”” page 36</a> ).
<b>Sensor type</b>	Display the sensor chosen.
<b>Behaviour:</b>	
<b>PIR always active</b>	Enable/disable PIR sensor always ON.
<b>Thornproof</b>	Enable/disable thornproof MEMS accelerometer (default: disabled).
<b>Use hardware switch settings</b>	If enabled, the sensor will use the hardware switch settings on board. If disabled, the sensor will acquire the configuration according to the settings of the next fields (default: enabled).
<b>Alarm notification with LED</b>	Enable/disable the alarm notification with LED. Referring to OPTEx installation instructions: switch 1. (default: disabled).
<b>Inhibition time (sec.)</b>	This is the inhibition time (in seconds) after the transmission of each alarm. Referring to OPTEx installation instructions: switch 6 . (Value range: 5...255, in steps of 5 sec.).
<b>Antimasking analysis</b>	(ONLY WXI-RAM) Enable/Disable the antimasking analysis. Referring to OPTEx installation instructions: switch 8 .
<b>Day/Night</b>	If enabled, the analysis is performed “night only”, otherwise “day&night” (default: disabled). Refer to OPTEx installation instructions: switch 7.
<b>PIR settings:</b>	
<b>Right PIR sensibility</b>	Adjust right PIR sensibility: low, medium, high (default: medium).
<b>Number of right PIR pulses</b>	It is the number of pulses necessary before the zone alarm is generated (default: 2). (Value range: 1...4).
<b>Right PIR Immunity</b>	Enable/disable right PIR immunity (default:disabled)
<b>Left PIR sensibility</b>	Adjust left PIR sensibility: low, medium, high (default: medium).
<b>Number of left PIR pulses</b>	It is the number of pulses necessary before the zone alarm is generated (default: 2). (Value range: 1...4).
<b>Left PIR Immunity</b>	Enable/disable left PIR immunity (default:disabled)
<b>Right Microwave sensibility</b>	The right microwave sensibility can be set on five levels: very low, low, medium, high (default), very high.
<b>Right Microwave immunity</b>	Enable/disable the right microwave immunity (default: disabled).
<b>Left Microwave sensibility</b>	The left microwave sensibility can be set on five levels: very low, low, medium, high (default), very high.
<b>Left Microwave immunity</b>	Enable/disable the left microwave immunity (default: disabled).

Optex QXI-R / QXI-RDT	
<b>Description</b>	Give a name to the peripheral module (i.e. outdoor terrace sensor).
<b>Serial number</b>	6 digits code which identifies the peripheral module. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">“Programming Wireless peripherals without configuring the Serial Number” page 49</a> )
<b>Supervision time interval (min)</b>	Maximum amount of time (in minutes) between two consecutive transmissions. (Value range from 0 to 240). Disabled if value is 0. (see also <a href="#">“About programming “Supervision time”” page 36</a> .
<b>Sensor type</b>	Display the sensor chosen.
<b>Behaviour:</b>	
<b>PIR always active</b>	Enable/disable PIR sensor always ON.
<b>Thornproof</b>	Enable/disable thornproof MEMS accelerometer (default: disabled).
<b>Use hardware switch settings</b>	If enabled, the sensor will use the hardware switch settings on board. If disabled, the sensor will acquire the configuration according to the settings of the next fields (default: enabled).
<b>Alarm notification with LED</b>	Enable/disable the alarm notification with LED. Referring to OPTEX installation instructions: switch 1. (default: disabled).
<b>Inhibition time (sec.)</b>	This is the inhibition time (in seconds) after the transmission of each alarm. Referring to OPTEX installation instructions: switch 5 . (Value range: 5...255, in steps of 5 sec.).
<b>PIR settings:</b>	
<b>PIR sensibility</b>	Antimasking analysisEnable/Disable the antimasking analysis. Referring to OPTEX installation instructions: switch 3/4.
<b>Number of PIR pulses</b>	It is the number of pulses necessary before the zone alarm is generated (default: 2). (Value range: 1...4).
<b>Microwave:</b>	
<b>Microwave sensibility</b>	(ONLY QXI-RDT) The microwave sensibility can be set on five levels: very low, low, medium, high (default), very high.
<b>Microwave immunity</b>	(ONLY QXI-RDT) Enable/disable the microwave immunity (default: disabled).

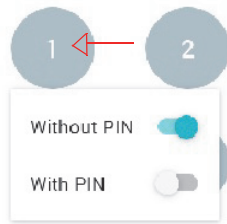
### 3.7.3.5 Wireless keypads

Keypads programmable:

- ergo-wls

The configuration parameters available are the following:

<b>Description</b>	Give a name to the keypad (i.e. entrance keypad).
<b>Serial number</b>	6 digits code which identifies the keypad. Simply update the serial number to acquire the new peripheral and to keep any previously saved settings if the device is being replaced.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Serial number. (see also <a href="#">“Programming Wireless peripherals without configuring the Serial Number” page 49</a> .)
<b>Hashtags</b> (see <a href="#">“Hashtags menu” page 23</a> )	Click on the arrow next to the field to open the menu with the list of partitions previously programmed. It is possible to associate one or more partition to the same device.
<b>Partitions</b> (see <a href="#">“Partition menu” page 22</a> )	Click on the arrow next to the field to open the menu with the list of Rooms/Maps previously programmed. It is possible to associate one or more rooms to the ergo-wls, in such a way it can be managed directly from “Floor Plans” menu.
<b>Display date and time</b>	Enable/disable the display of date and time on the second line of the keypad display.
<b>Display external temperature</b>	Enable/disable the display of the temperature detected by the "imago" siren, on the second line of the keypad display.
<b>Display internal temperature</b>	Enable/disable the display of the temperature detected by the "radius" siren, on the second line of the keypad display.
<b>Display GSM status</b>	Enable/disable the display of the mobile provider and the GSM signal on the second line of the display (if the GSM/GPRS communicator is configured in the system).
<b>Display arming status</b>	Enable/disable the display of the arming status on the second line of the keypad display. Furthermore, by enabling this option it will be possible to view the status of one partition at a time by pressing the key (#) when the keypad is on idle, to move on to the next, press the scroll keys of the keypad supplied.
<b>Display zones status</b>	Enable/disable the display of the status of the zones in alarm. It is possible to view the status of one zone at a time on the second line of the display by pressing the key (*) when the keypad is on idle, to move on to the next, press the scroll keys of the keypad supplied. If enabled, the green LED will remain on to indicate that all the areas of the partitions associated with it are in idle.
<b>Acoustic feedback during exit time</b>	Enable/disable the acoustic feedback of the keypad during exit time.
<b>Acoustic feedback during entry delay</b>	Enable/disable the acoustic feedback of the keypad during entry delay.
<b>Supervision time interval (min)</b>	You can set the supervision interval for wireless diagnostic (minutes) (see also <a href="#">“About programming “Supervision time”” page 36</a> .
<b>Keys configuration</b>	(enable/disable scenario). A key can be enabled to execute a scenario. Click on a button, select the option 'With pin' if you want to enable the button for execution only after having entered a valid pin, select 'Without pin' if you want to enable execution without inserting a pin, but simply holding pressed the button for three seconds.



The image shows “Without **PIN**” enabled and “With **PIN**” disabled.

### 3.7.4 Programming Wireless peripherals without configuring the Serial Number



It is possible to add a wireless peripheral configuration without setting its serial number, by enabling the <Ignore> button.

Also, the saving data is allowed, it is indicated by yellow warnings as well as the peripherals name and related menu items are coloured in yellow. The outputs and zones configuration associated to these peripherals is allowed too, but they won't be displayed on the real time page.

The real peripheral association by typing the serial numbers previously ignored, can be performed later.

Quick association can be made by clicking on the barcode button: if some peripherals of the same type with serial number not associated are present, a list of them will appear so you just have to choose one from it.

### 3.7.5 Cancel wireless peripherals

- To cancel a wireless peripheral, enter the sub-menu of interest, click on “Open session”  icon (if not already open), click on the peripheral name to cancel and click on  (red bin) icon next to it.

“Confirm Remove” is required: press <Remove> to confirm or <Cancel> to reject.

Confirm Remove

Are you sure you want to remove the item?

✕ CANCEL    ✓ REMOVE

## 3.8 IP Devices


The IP devices are all those devices (user interfaces, cameras, communicators and third parties devices) connected via LAN to the motherboard of the *lares 4.0* control panel.

The IP devices configuration web pages allow the following operations:

- [“Automatic IP Devices acquisition” page 50](#) ;
- [“Read the status of IP Devices in real time” page 51](#) ;
- [“Programming IP Devices” page 53](#) ;
- [“Programming IP peripherals without configuring the Mac Address” page 57](#)
- [“Add / cancel IP devices” page 57](#) .

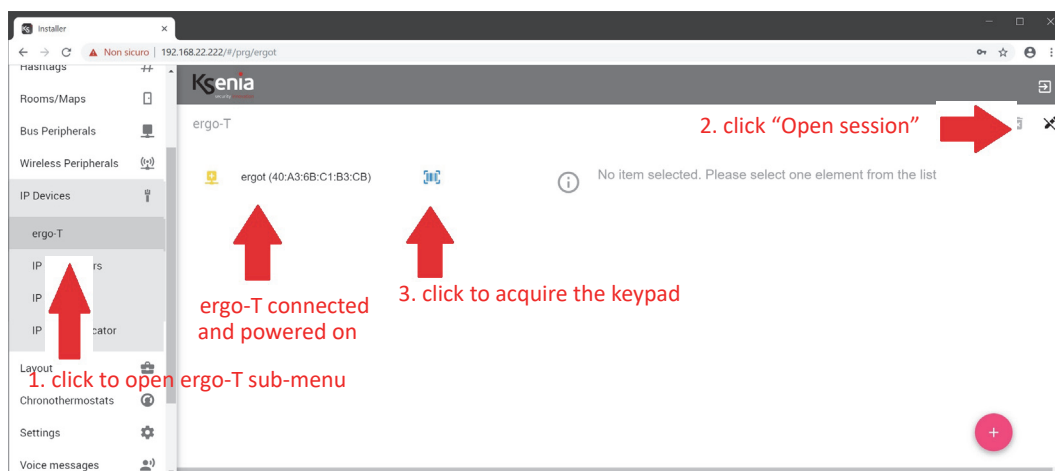
### 3.8.1 Automatic IP Devices acquisition

The IP devices connected via LAN, are shown on the left side of the configuration page under sub-menus: "ergo-T", "IP supervisor", "IP Cameras", "IP Communicator".

To acquire a connected and powered on peripheral device, click on “Open session”  icon (if not already open).

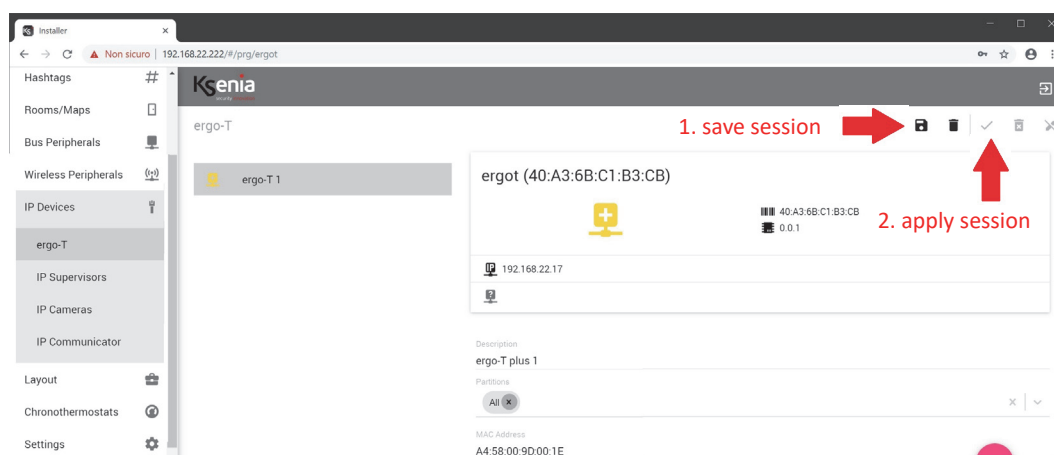
#### 3.8.1.1 Acquiring an ergo-T keypad - Example

1. Open IP Devices -> ergo-T

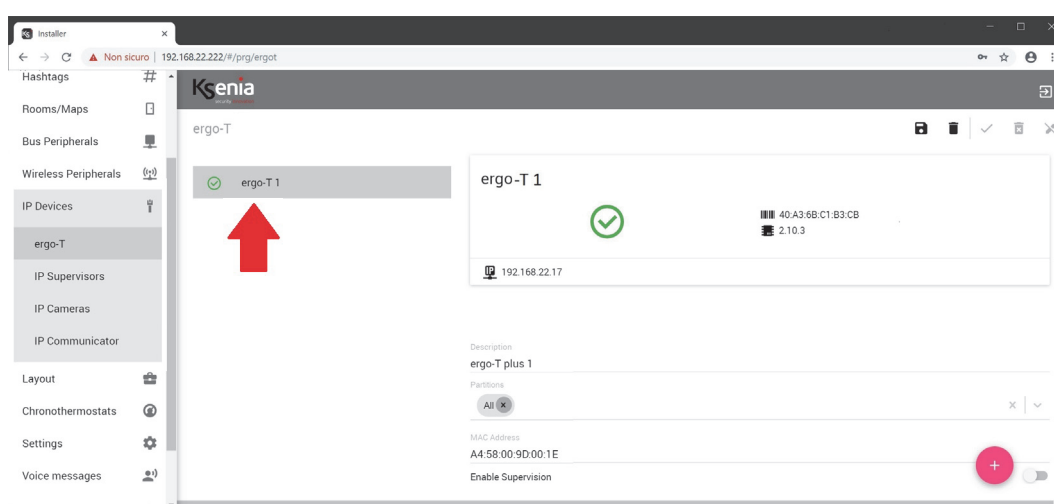


If the device does not appear, may be it has not been connected correctly or it is not powered on or it does not communicate with the mother board.

2. An immediate acquisition occurs and soon after the page appears as shown in the next image. Now it is necessary save and apply the session.



3. The configuration will be sent to the central panel, at the end of the loading the page changes as shown in the image below.

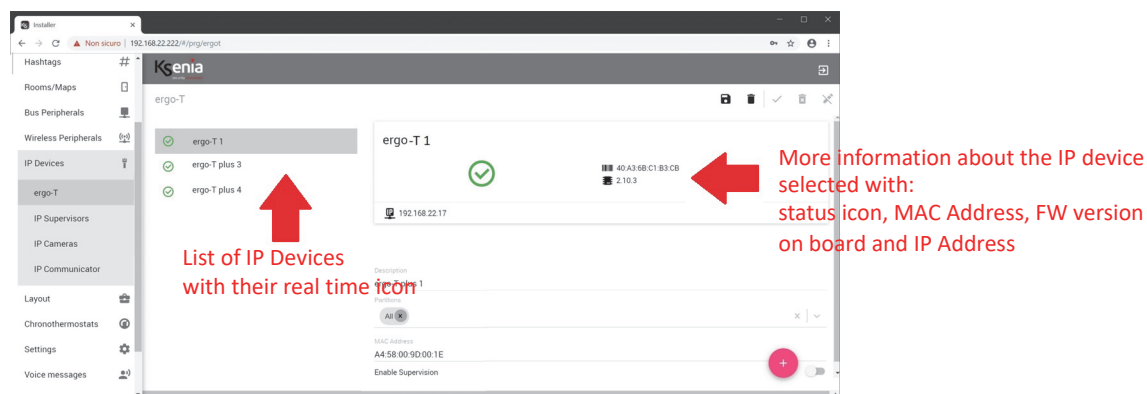


### 3.8.2 Read the status of IP Devices in real time






The following image shows the list of “ergo-T” and their relative real time icon. In the following tables the possible status are described.

To view more information about the real time, click on a name, as shown in the following image.

The status icons may change as follows:



The status icons may change as follows:

example: ergo-T	 <p>ergo-T</p> <p>D5:05:05:05:05:05 2.00.0</p> <p>192.XXX.XXX.XXX</p>	<p>GREEN ICON: Device connected and working correctly. If available, also the Firmware Update icon will be displayed</p> 
	 <p>ergo-T plus</p> <p>192.168.22.76</p>	<p>BLUE ICON: Initializing or upgrading device (temporary state).</p>
	 <p>porta 4.0 (A4:58:0F:92:00:0D)</p> <p>A4:58:0F:92:00:0D 1.2.9</p> <p>192.168.22.103</p>	<p>YELLOW ICON: Tampering device/Device present but not configured.</p>
	 <p>ergo-T plus 1</p> <p>A4:58:00:9D:00:C7</p> <p>NA</p>	<p>GREY ICON: device no longer detected by the network or addressing phase. It appears when the device is no longer detected by the network or in addressing phase.</p>



### 3.8.3 Programming IP Devices

See below the description of the configuration parameters available, they are different according to the type of peripheral module.

#### 3.8.3.1 ergo-T

List of keypads programmable:

- **ergo-T, ergo-T plus**

The configuration parameters available of ergo-T keypads are the following:

<b>Description</b>	Give a name to the device (i.e. entering keypad, box keypad, etc.))
<b>Partitions</b> (see <a href="#">"Partition menu" page 22</a> )	Click on the arrow next to the field to open the menu with the list of partitions previously programmed. It is possible to associate one or more partition to the same device.
<b>MAC Address</b>	Enter the MAC address printed on the label of the device
<b>Ignore</b>	If enabled, it allows the configuration without setting the Mac Address. (see also <a href="#">"Programming IP peripherals without configuring the Mac Address" page 57</a> )
<b>Enable supervision</b>	Enable/disable the supervision of the keypad

#### 3.8.3.2 IP Supervisors

The configuration parameters available of third parties devices compatible with the control panel (i.e.: Control 4 supervisor) are the following:

<b>Description</b>	Give a name to the third party device (i.e. Control 4 supervisor)
<b>Partitions</b> (see <a href="#">"Partition menu" page 22</a> )	Click on the arrow next to the field to open the menu with the list of partitions previously programmed. It is possible to associate one or more partition to the same device.
<b>MAC Address</b>	Enter the MAC address printed on the label of the device
<b>Ignore</b>	If enabled, it allows the configuration without setting the Mac Address. (see also <a href="#">"Programming IP peripherals without configuring the Mac Address" page 57</a> )

### 3.8.3.3 IP Cameras

Depending on the version of the control panel, a certain number of IP cameras can be set, see the list below:

- lares 4.0 - 16 / lares 4.0-16WLS: 4 IP cameras
- lares 4.0 - 40 / lares 4.0-40WLS: 12 IP cameras
- lares 4.0 - 140 WLS: 20 IP cameras
- lares 4.0 - 644 WLS: 30 IP cameras

The configuration parameters available for IP cameras are the following:

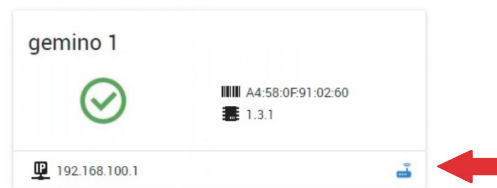
<b>Description</b>	Give a name to the device (i.e. street side camera, front garden camera, etc.).
<b>Partitions</b> (see <a href="#">"Partition menu" page 22</a> )	Click on the arrow next to the field to open the menu with the list of partitions previously programmed. It is possible to associate one or more partition to the same device.
<b>IP Address</b>	Enter IPAddress (local) of IP camera.
<b>Rooms</b> (see <a href="#">"Rooms / Maps menu" page 23</a> )	Click on the arrow next to the field to open the menu with the list of Rooms/Maps previously programmed. It is possible to associate one or more rooms to the IP Camera, in such a way it can be managed directly from "Floor Plans" menu.
<b>Brand</b>	Click on the arrow next to the field to open the drop down list and select a name. In this case the " <b>instant url</b> " parameter is pre-set; otherwise you need to select " <b>Custom</b> " and contact the technical assistance of the camera manufacturer, for customizing the IP parameters.
<b>Snapshot Url</b>	The string (URL) to send to the camera, in order to receive a "snapshot", that is a jpg image. If the camera is selected from the "brand" menu, this parameter will be configured automatically. In some cases it will have to be configured manually (contact the manufacturer's assistance).
<b>Internal port</b>	Internal port inside the LAN on which the camera is located.
<b>External port</b>	External port outside the LAN network.
<b>Authentication type</b>	Enable/disable Basic authentication. If the Basic authentication is enabled, the camera ask you to enter a <b>username</b> and a <b>password</b> in order to allow the visualization of the images: remember to enter your credentials to log in.

### 3.8.3.4 gemino IoT

gemino IoT can be used in normal mode or as a router.

The router function can be manually set up by pressing a switch key on the device and it is signaled by means a little blue router icon in the real time section, if not present, gemino IoT works in normal mode.

**When the gemino IoT functions as router, it ignores the IP address and DHCP parameters that may be present in the configuration and it uses the static IP address 192.168.100.1**, subnet mask 255.255.255.0. The DHCP server implemented by gemino IoT when it works as a router, assigns IP addresses from a reserved dynamic range [from 192.168.100.2 to 192.168.100.100] while a reserved static range [from 192.168.100.101 to 192.168.100.254] are available to connect a device with an IP address belonging to this static range, subnet mask 255.255.255.0, and default gateway 192.168.100.1. Lease time is fixed to 12 hours.



For further information, see the gemino IoT Installation manual.

The configuration parameters available for gemino IoT are the following:

<b>Description</b>	Give a name to the device.
<b>MAC Address</b>	Enter the MAC address printed on the label of the device.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Mac Address. (see also <a href="#">“Programming IP peripherals without configuring the Mac Address” page 57</a> )
<b>DHCP</b>	Enable/disable DHCP on gemino IoT. If the local network to which the control panel is connected supports DHCP, you have to enable DHCP on gemino IoT and the IP address will be automatically assigned to it. If the local network to which the control panel is connected does not support DHCP, you have to disable DHCP and enter a static IP address. gemino IoT uses the subnet mask and the default GW of the control panel. Default: enabled.
<b>IP address</b>	Enter a static IP address. The field is editable only if the above field is disabled. The default IP address of gemino IoT is <b>192.168.2.98</b> in normal mode.
<b>Enable supervision</b>	Enable/disable the supervision of the IP communicator.
<b>Select antenna</b>	Indicates the antenna that will be used by the communicator (internal or external).
<b>Mobile data</b>	Enable/Disable mobile data.
<b>APN</b>	Indicates the APN (Access Point Name) for access to the data network.
<b>Authentication type</b>	Type of authentication to be performed to the phone operator before starting to use the data channel (if requested by the phone operator).
<b>User</b>	User name to access the data network (if requested by the phone operator).
<b>Password</b>	Password to access the data network (if requested by the phone operator).

### 3.8.3.5 Gateway

Configuration of a gateway device connected to the local network that allows the communication between the control panel and third-party devices:

- porta 4.0 is a Konnex gateway used as an interface towards the Konnex BUS and vice-versa;
  - porta IoT is a http/s gateway used as an interface between the control panel and third-party devices, thanks to this protocol it is possible to manage requests and command actions when certain events take place.
- lares 4.0 supports just one gateway device.

The service is linked to the MAC Address of the device and cannot be transferred to another device.

The configuration parameters for porta 4.0 are the following:

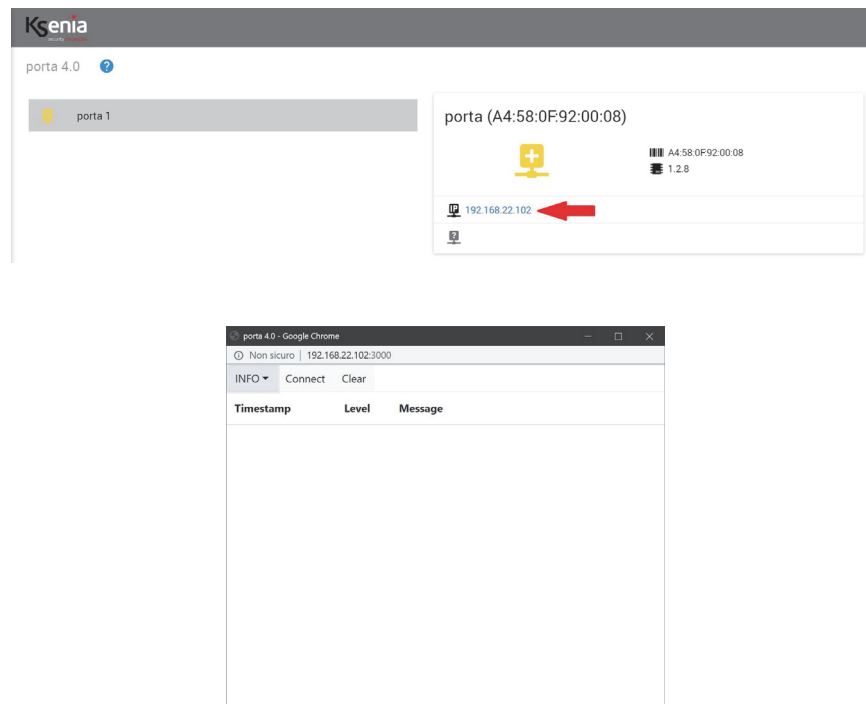
<b>Description</b>	<p>Give a name to the device (e.g. port 4.0). Note:</p> <ul style="list-style-type: none"> <li>• porta 4.0: following open Services -&gt; Konnex to configure the datagrams exchanged between lares 4.0 and KNX devices.</li> <li>• porta IoT: following, open Services -&gt; Gateway http to program the outgoing API (devices and actions) in the Services -&gt; Gateway http menu; the endpoints of porta IoT, relating to the possible actions, are displayed directly in the Layout-&gt;Zones/Outputs/Partitions and Scenarios menus.</li> </ul>
<b>MAC Address</b>	Enter the MAC address printed on the label of the device.
<b>Ignore</b>	If enabled, it allows the configuration without setting the Mac Address. (see also <a href="#">"Programming IP peripherals without configuring the Mac Address" page 57</a> )
<b>Enable action with PIN</b>	By enabling this option, the configured Konnex datagrams will be allowed to perform PIN-protected actions (scenarios, outputs activation, etc.).
<b>Enable Supervision</b>	Enable/disable the supervision of the device by the control panel.
<b>DHCP</b>	<p>Enable/disable DHCP on porta 4.0. If the local network to which the control panel is connected supports DHCP, you have to enable DHCP on porta 4.0 and the IP address will be automatically assigned to it. If the local network to which the control panel is connected does not support DHCP, you have to disable DHCP and enter a static IP address. porta 4.0 uses the same subnet mask and the default gateway of the control panel. Default: enabled</p>
<b>IP Address</b>	<p>Enter a static IP address. The field is editable only if the above field is disabled. The default IP address of porta 4.0 is <b>192.168.2.99</b>.</p>

#### AVAILABLE ONLY IN LOCAL CONNECTION:

possibility to view the **logs of communication activity** between the lares 4.0 control panel and KNX devices (receive commands / send status changes) **and set the debug levels**.

Remember that the configuration of the datagrams exchanged between the lares 4.0 control panel and KNX devices is necessary: open ["Konnex" page 103](#) configuration page to configure them.

Click on the IP address of the device, present in the "real time" section, as shown in the following images.



### 3.8.4 Programming IP peripherals without configuring the Mac Address

It is possible to add a IP peripheral configuration without setting its Mac Address, by enabling the <Ignore> button. Also, the saving data is allowed, it is indicated by yellow warnings as well as the peripherals name and related menu items are coloured in yellow. The outputs and zones configuration associated to these peripherals is allowed too, but they won't be displayed on the real time page.





The real peripheral association by typing the Mac Addresses previously ignored, can be performed later.






Quick association can be made by clicking on the barcode button: if some peripherals of the same type with Mac Address not associated are present, a list of them will appear so you just have to choose one from it.

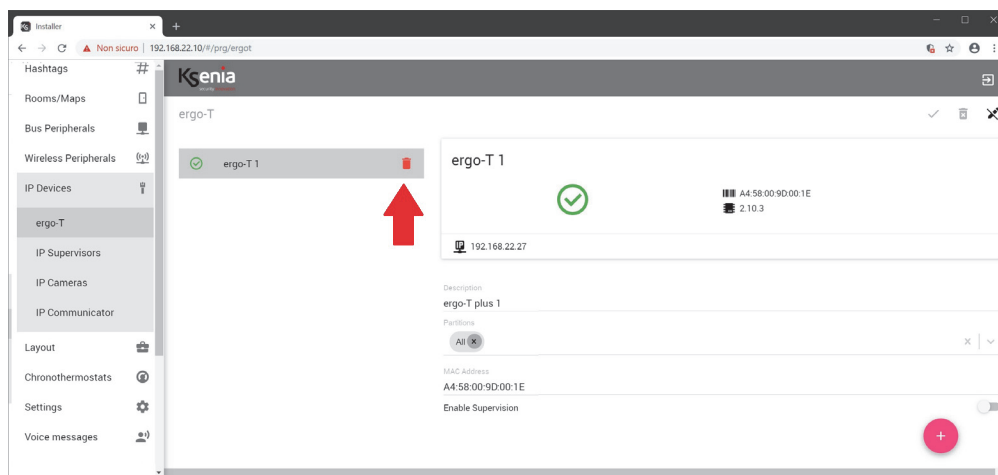
### 3.8.5 Add / cancel IP devices

In addition to the IP devices acquisition (described in the paragraph [“Automatic IP Devices acquisition” page 50](#)), it is possible to add an IP device manually.

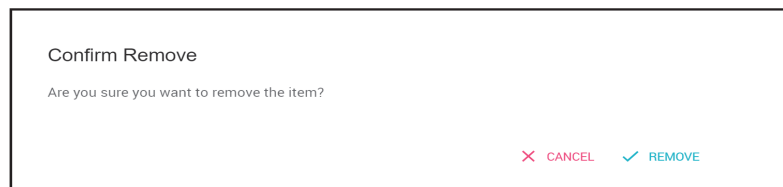
- **To add manually** the devices, it is necessary to open the menu related to the type of IP device to be configured:

1. Click on “Open session”  icon (if not already open)
2. Click on  <+> red icon to add a new peripheral
3. Click on the  <+> blue icon relative to the device chosen (among the list of devices proposed)
4. Type the serial number printed on the device label
5. To add a new one device and you are in the same session, click again on  <+> red icon
6. Complete or modify the configuration parameters available

7. Click on  Save session icon (until now, still the changes can be discarded by clicking on  cancel changes icon). Click on “Apply session”  icon to make the new configuration effective.
- **To cancel an IP device**, enter the sub-menu of interest, click on “Open session”  icon (if not already open), click on the peripheral name to cancel and click on  (red bin) icon next to it.



“Confirm Remove” is required: press <Remove> to confirm or <Cancel> to reject.



## 3.9 Layout

### 3.9.1 Arming modes

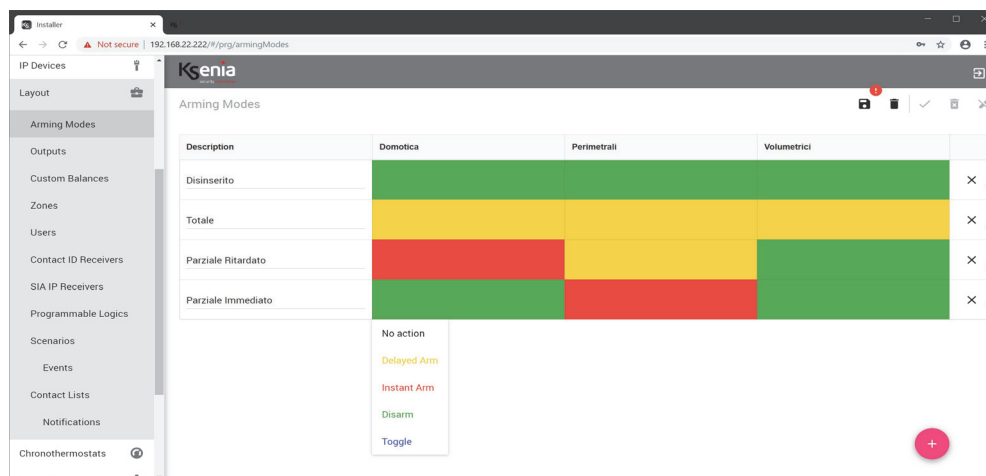
In this section you will be able to create the entries of partitions that will be assigned to scenarios later, then the **scenarios** will be associated to some **events**.

The meaning of the colors is the following:

- **White:** no action. The partition status doesn't change.
- **Yellow:** delayed arm. The partition is armed but entry and exit timer are still valid (only for zones of those partitions also delayed).
- **Green:** disarm. The partition is disarmed.
- **Red:** instant arm. The partition is armed and both entry and exit timer are reset.
- **Blue:** toggle. If the partition is armed, it will be disarmed and vice versa.



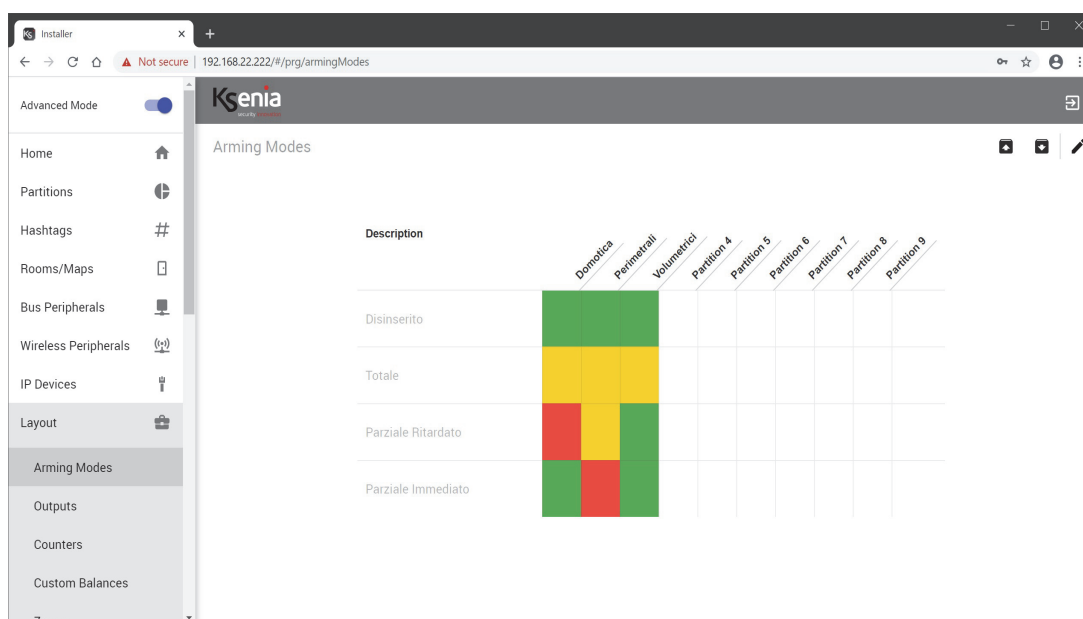
Note: the "switch" type arming mode can be used several times: it is possible to carry out arming and disarming of the partition with only one scenario (insert -> disarm -> insert -> disarm etc.). If the partition is programmed with delay it will be inserted only with delay (it is not possible to toggle to an instant arm).



The image above shows:

- Entry 1: partitions 1 and 4 inserted with delays. Partitions 2 and 3 inserted instantly.
- Entry 2: partitions 1 and 4 inserted instantly. The status of partitions 2 and 3 remains unchanged (if they were previously inserted they will remain inserted, if they were disarmed they will keep this state).
- Entry 3: all partitions are disarmed.
- Entry 4: partitions 2 and 3 inserted instantly. Partition 4 does not change status. Partition 1 if it was disarmed is now inserted and vice versa.

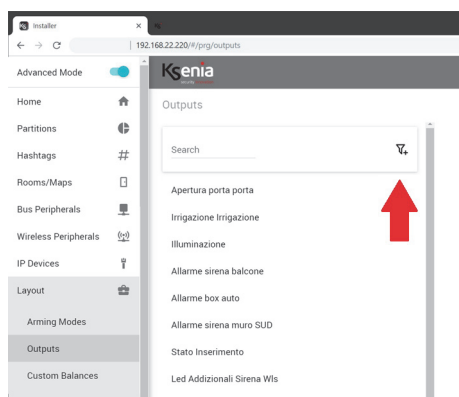
If the partitions are equal to or greater than 7, the display of the entries changes as shown in the following image:



### 3.9.2 Outputs

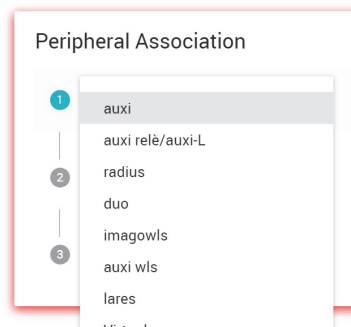
It is possible to program the outputs of the system (from 16 to 644, it depends on the size of the control panel).

The **filter** tool (by description, by partition, by peripheral) makes easier the search of the outputs programmed.







The configuration parameters available for Outputs are the following:

<b>Description</b>	Give a name to the outputs (i.e. boiler, living room light, box automation, etc.)
<b>Hashtags</b> (see <a href="#">“Hashtags menu” page 23</a> )	Click on the arrow next to the field to open the menu with the list of hashtags previously programmed. It is possible to associate one or more hashtags to the same output.
<b>Partitions</b> (see <a href="#">“Partition menu” page 22</a> )	Associate the output with the partitions. Useful, for example, when you want to limit the management of the output by users (i.e. layout available for two-family house).
<b>Rooms</b> (see <a href="#">“Rooms / Maps menu” page 23</a> )	Click on the arrow next to the field to open the menu with the list of Rooms/ Maps previously programmed. It is possible to associate one or more rooms to the output, in such a way it can be managed directly from “Floor Plans” menu.
<b>Peripheral Association</b>	<p>In this section the outputs are associated with the terminals of the main board or to one of the peripherals previously programmed in the BUS peripheral sections or wireless peripherals.</p> <ul style="list-style-type: none"> <li>It is necessary to program: <ol style="list-style-type: none"> <li>the type of peripheral module to which the outputs will be associated;</li> <li>the description of the selected peripheral module;</li> <li>the single connection terminal to which the output is associated.</li> </ol> </li> </ul> <ol style="list-style-type: none"> <li><b>Choose the type of peripheral.</b> Select one of the devices previously configured in the system, the list is dynamic and displays only the configured peripherals, excluding those already associated:</li> </ol>  <ol style="list-style-type: none"> <li><b>Select the description of the selected peripheral module.</b> Select an item from the list. <b>Example:</b> you are configuring an output associated to the terminal “m1” of auxi peripheral (i.e. auxi box). Of course you have already configured the auxi peripheral (see <a href="#">“BUS peripherals menu” page 24</a> ), so select auxi, as described at point 1. and then select “auxi box” from the drop down list.</li> <li><b>Select the single connection terminal to which the output will be associated.</b> Only the available single connection terminals will be shown in the list.</li> </ol>

	<p><u>List of single connection terminals available for each peripheral module:</u></p> <ul style="list-style-type: none"> <li>• <b>lares:</b> "m1" and "m2" terminals of lares 4.0;</li> <li>• <b>auxi:</b> all the terminals of expansion module. Unavailable for auxi10!</li> <li>• <b>auxi-HT/auxi-HL:</b> all the terminals of auxi-H.</li> <li>• <b>auxi relè/auxi-L:</b> all the terminals of auxi relè.</li> <li>• <b>ergo-rev.0/ergo:</b> "m1" and "m2" terminals of ergo keypads. Unavailable for ergoS and ergoM.</li> <li>• <b>duo:</b> "m1" and "m2" terminals of duo transceiver/repeater. Unavailable if duo is programmed as repeater.</li> <li>• <b>radius:</b> it is possible to associate the output to the Led and to the buzzer, or just to the Led.</li> <li>• <b>imago:</b> it is possible to associate the output to the main LED and to the buzzer, or only to the main LED or only to the additional LEDs (generally used to indicate the status of the system).</li> <li>• <b>auxi wls:</b> "o1" and "o2" terminals of auxi wireless.</li> <li>• <b>imago wls:</b> it is possible to associate the output to the main LED and to the buzzer, or only to the main LED or only to the additional LEDs (generally used to indicate the status of the system).</li> </ul> <p><b>energia:</b> it is possible to associate the 4 outputs relays provided both to drive external relays for overloaded circuits disconnection and as generic outputs of the control panel.</p>
	<p>!</p> <p><b>Note:</b> If <b>imago wls</b> is powered by connecting a non-rechargeable battery (KSI7207580.000) the outputs will be managed regardless of the configuration made:</p> <ul style="list-style-type: none"> <li>• <b>Alarm Output:</b> monostable with ON time equal to the maximum alarm time established in the phase of programming (default: 3 min.);</li> <li>• <b>Power LED Output:</b> monostable with maximum ON time equal to 30 seconds;</li> <li>• <b>Aux LED Output:</b> monostable with maximum ON time equal to 30 seconds; this operating mode is used to save the battery life. If the wireless imago is powered by a 12Vdc external power supply and a rechargeable Pb battery, the outputs are managed as instructed in their programming.</li> <li>• <b>Virtual:</b> with respect to the traditional lares platform, software timers are no longer present, but these have been replaced by virtual outputs, combined with "output activation" and "output deactivation" events. A virtual output is not associated with any device.</li> </ul>

<b>Mode</b>	<p>Configuration of the outputs arming mode. Configuration parameters are the following:</p> <ul style="list-style-type: none"> <li>• <b>Monostable:</b> it is an output that is activated for a time programmed (ON time) when the event occurs and then automatically returns to the resting status.</li> <li>• <b>Bistable:</b> it is an output that follows the status of the corresponding event or that can be activated by an event and deactivated by another.</li> <li>• <b>Arming state:</b> it follows the arming state of the partition (or partitions) to which it is associated. If the partition is armed, the output activates and vice versa.</li> <li>• <b>Alarm:</b> it is activated when the partition (or the partitions) associated with it generates an alarm. The ON time duration is set in "Partitions cycle" (min).</li> <li>• <b>Tamper:</b> it is activated when the partition (or the partitions) associated with it, generates an event of tamper. (The ON time duration is equal to the alarm cycle time of the partition).</li> <li>• <b>Alarm and tamper:</b> it is activated when the partition (or the partitions) associated with it generates an alarm and tamper event and it is equal to the alarm cycle time of the partition.</li> <li>• <b>Fault:</b> it is activated when a fault occurs (i.e. fault control panel battery). It is deactivated when the fault condition is restored.</li> <li>• <b>Roller blind:</b> the output configured with this mode is preparatory to the configuration of the "Roller blind outputs" scenario, see <a href="#">"Scenarios" page 81</a>.</li> <li>• <b>Thermoregulation:</b> the output configured with this mode is preparatory to the configuration of the chronothermostat, see <a href="#">"Chronothermostats" page 101</a>.</li> <li>• <b>Ready to arm:</b> the output configured with this mode allows you to signal when all the zones of the partitions associated with it are on idle.</li> <li>• <b>Analog:</b> this mode is assigned if the polarity is equal to analog.</li> </ul>
<b>Closing time (sec.)</b>	(only available for auxi-HT) Possibility to program the closing time of "Roller blind" in steps of 0.1 seconds.
<b>Opening time (sec.)</b>	(only available for auxi-HT) Possibility to program the opening time of "Roller blind" in steps of 0.1 seconds.

<b>APP management</b>	<p>Configuration of APP and Webserver management mode. Configuration parameters are the following:</p> <ul style="list-style-type: none"> <li>• <b>Hidden:</b> if this option is selected, the output will not be displayed in the APP and Web server in the page of real-time output.</li> <li>• <b>With PIN (local) - With PIN (remote):</b> in this case, the output will be managed locally with PIN and it will be managed through the APP in the same way.</li> <li>• <b>With PIN (local) - Not managed (remote):</b> in this case, the output will be managed locally by PIN but it will not be possible to manage it through the APP (even if displayed).</li> <li>• <b>Without PIN (local) - Without PIN (remote):</b> in this case, the output will be managed locally without PIN and it will be managed through the APP in the same way.</li> <li>• <b>Without PIN (local) - Not managed (remote):</b> in this case, the output will be managed locally without PIN but it will not be possible to manage it through the APP (even if displayed).</li> <li>• <b>Without PIN (local) - With PIN (remote):</b> in this case the output will be managed locally without PIN but it will be required to enter a code to manage it through the APP.</li> <li>• <b>Not managed (local) - Not managed (remote):</b> in this case, it will not be possible to manage it through the APP (even if displayed).</li> </ul>
<b>Polarity</b>	<p>The configuration parameters are the following:</p> <ul style="list-style-type: none"> <li>• <b>Normally open:</b> select this option if you want an O.C. (open collector) output in resting state to be open and closes to the ground when it is activated (negative to give) or if you want the relay contact (i.e. relay auxi) to be open.</li> <li>• <b>Normally closed:</b> select this option if you want an O.C. output in the resting state to be closed to ground and opens when it is activated (negative to miss) or if you want the relay contact (i.e. auxi relay) to be closed.</li> <li>• <b>Analog:</b> (only for M5 terminal of auxi peripheral module) select this option if M5 terminal of auxi to manage the voltage at 0-10V.</li> </ul>
<b>Time ON</b>	<p>Time expressed in seconds, for which an output programmed as monostable remains active when an event occurs.</p> <p>! _____ Note: this option only appears if you set a monostable output.</p>
<b>Reactivation inhibition (sec.)</b>	<p>Time expressed in seconds, when exceeded, an output programmed as monostable is reactivated for the time configured in the previous field "Time ON", when an event occurs.</p> <p>! _____ Note: this option only appears if you set a monostable output.</p>

<b>Active only if the control panel is armed</b>	<p>The output is activated only if the partition (or partitions) associated with it is armed.</p> <p> _____</p> <p><b>Note:</b> This option is available only if you set the "tamper" or "alarm and tamper" mode.</p> <p> <b>Note:</b> an output must be created that is activated when a fault event occurs in accordance with the standard EN 50131.</p>
<b>Category</b>	<p>Default value "Generic".</p> <p>If configured, in the "Smart Home" page of the APP lares 4.0 for user, the output being configured will be displayed in the category programmed in this field. (i.e. the output called "irrigation" with category = "Irrigation" will be displayed on the Smart Home page -&gt; "Irrigation" category of the Lares 4.0 App).</p>
<b>Http endpoints on Gateway</b>	<p>This section displays the endpoints exposed by Ksenia device, Gateway Http service enabled, applicable to the OUTPUTS.</p> <p>"Read status GET" and "Edit status using PUT/GET method" APIs, display URL and body (JSON) with which the third-party device communicates with the device Ksenia. Copy and paste the messages to the connected device and edit the suggested values.</p>

### 3.9.3 Counters

In this section the configuration of "Counters" is possible, they can be increased, decreased or set to zero, depending on the personalized actions that can be performed directly from the Scenarios.

Programming a maximum threshold generates events and sends notifications to the lares 4.0 APP or to ergo-T/ergo-T plus keypads, in order to inform the Customer.

Each counter can also be associated with one or more partitions and with one or more rooms/maps to be directly managed by the graphic maps.

According to the configuration, the "Counters" function applies in different scenarios, for example:

- can provide the number of people present in a place, measuring entries and exits in real time and generating events such as blocking the entrances;
- can be used to count the flow of people who daily frequent a shop, to be used for example to analyze performances (for example, it is possible to analyse the difference between the number of people who entered and the number of people who actually bought, data easily detectable by the number of tax receipts issued);
- by means of a Tag supplied to the customer, it can be used to allow the entrances in gyms, cinemas, etc., up to the number of entrances paid (threshold) before renewing the subscription.


<b>Description</b>	Enter a description to identified the role of the counter. (i.e. People present)
<b>Partitions</b> (see <a href="#">"Partition menu" page 22</a> )	Click on the arrow next to the field to open the menu with the list of partitions previously programmed. It is possible to associate one or more partition to the same counter.
<b>Rooms</b> (see <a href="#">"Rooms / Maps menu" page 23</a> )	Click on the arrow next to the field to open the menu with the list of rooms previously programmed, to be associated with the counter. It is possible to associate one or more rooms to the same counter. The Rooms / Maps association allows the counter to be managed directly from the graphical Map.

<b>Threshold</b>	Enter a threshold limit value, upon reaching which the "reached-threshold" event will be generated and when it decreases, upon reaching the first value below the threshold, the "under-threshold" event will be generated. Possible values: 1...60000. Default values: 60000.
<b>Counter mode</b>	Configure how the counter must increase, related to the value set in "Threshold" field (default value: Continuous increase): <ul style="list-style-type: none"> <li>Continuous = the counter increases beyond the threshold, up to the maximum possible value of it (60000). Upon reaching the threshold, the "threshold-reached" event will be generated, when it decreases and reaches the first value below the threshold, the "sub-threshold" event will be generated.</li> <li>Stop = the counter increases up to the threshold; upon reaching the threshold, the event of "reached-threshold" will be generated, when it first decreases, the "sub-threshold" event will be generated.</li> <li>Reset = the counter increases up to the threshold; upon reaching the threshold, the "reached-threshold" event will be generated, at the first increase after the threshold is reached, the counter restarts from 1 and the "sub-threshold" event will be generated. If the threshold has been reached and a decrease occurs, the "sub-threshold" event will be generated.</li> </ul>

### 3.9.4 Custom Balances

In this section, custom configurations can be created for the end-of-line resistors to be associated then with the zones.

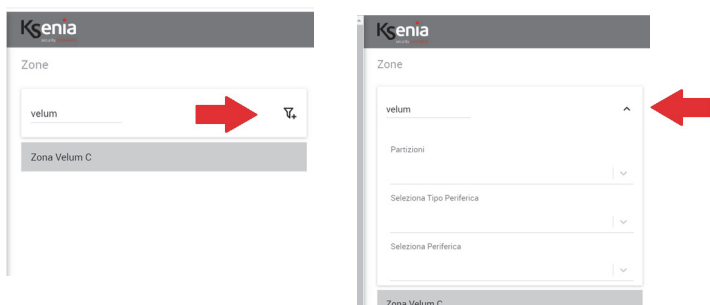
It is possible to modify the intervention thresholds and the behaviour of the input (short, resting, alarm, masking/fault, tamper), starting from the basic configuration of the standard balancing.

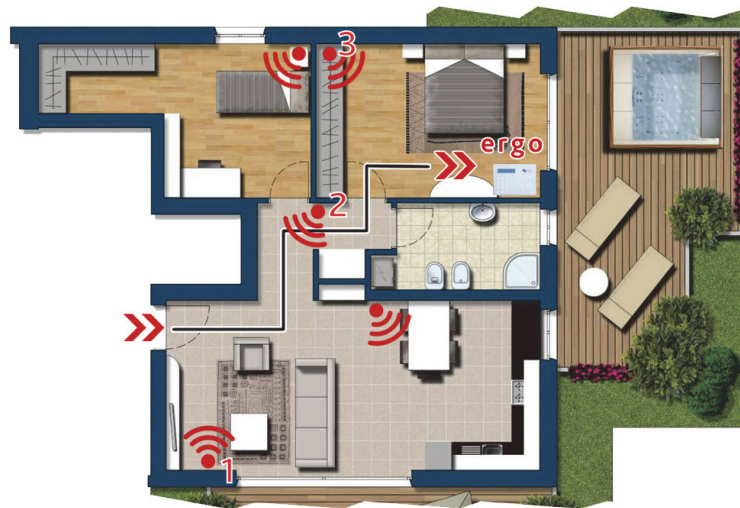
In this page, next to the session management buttons, the following button appears this icon:  . By clicking on it, you can open an Excel spreadsheet that allows to easily determine the thresholds to be applied according to the end-of-line resistors installed.

### 3.9.5 Zones

It is possible to program the zones of the system (from 16 to 644, it depends on the size of the control panel).

The **filter** tool (by description, by partition, by peripheral) makes easier the search of the zones programmed.





The figure shows a hypothetical situation of entrance into a house where the control panel of the system can be reached only after having intercepted some areas. Specifically, the volumetric sensor marked with ( 1 ) must be the first to be violated so as not to generate an alarm. Then, the number (2) and the number (3) will follow.

The configuration parameters of zones are the following:

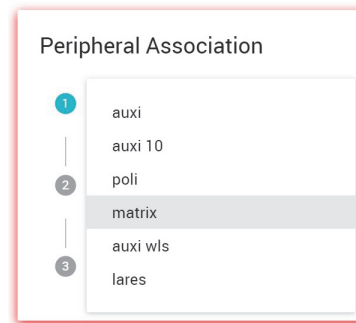
<b>Description</b>	Give a name to the zone (i.e. entrance door contact, living room volumetric sensor, etc.)
<b>Hashtags</b> (see <a href="#">“Hashtags menu” page 23</a> )	Click on the arrow next to the field to open the menu with the list of hashtags previously programmed. It is possible to associate one or more hashtags to the same zone.
<b>Partitions</b>	These are the areas associated with the zone. If the zone is associated with multiple partitions, it will generate an alarm only when it is violated and all the partitions to which it belongs are inserted, otherwise no alarm will be generated.
<b>Rooms</b> (see <a href="#">“Rooms / Maps menu” page 23</a> )	Click on the arrow next to the field to open the menu with the list of Rooms/ Maps previously programmed. It is possible to associate one or more rooms to the zone, in such a way it can be managed directly from “Floor Plans” menu.
<b>IP camera</b>	Selects the camera that will send the email with the snapshot. The same snapshots will also be saved in the event log under "Image" item.
<b>Camera Trigger</b>	Select the event related to the zone that will send the snapshots. Three events are available, and multiple choices can be made: <ul style="list-style-type: none"> <li>- Zone alarm event.</li> <li>- Zone tamper event.</li> <li>- Zone masking event.</li> <li>- Zone real time event.</li> <li>- Zone pre-alarm event.</li> <li>- Zone by-pass event.</li> </ul>

## Peripheral association

In this section the zones are associated with the terminals of the main board or to one of the peripherals previously programmed in the BUS peripheral sections or wireless peripherals.

It is necessary to program:


1. the type of peripheral module to which the zones will be associated;
2. the description of the selected peripheral module;
3. the single connection terminal to which the zone is associated.






	<ol style="list-style-type: none"> <li><b>1. Choose the type of peripheral.</b> Select one of the devices previously configured in the system, the list is dynamic and displays only the configured peripherals, excluding those already associated:</li> <li><b>2. Select the description of the selected peripheral module.</b> Select an item from the list. <b>Example:</b> you are configuring an output associated to the terminal "m1" of auxi peripheral (i.e. auxi box). Of course you have already configured the auxi peripheral (<a href="#">see "BUS peripherals menu" page 24</a>), so select auxi, as described at point 1. and then select "auxi box" from the drop down list.</li> <li><b>3. Select the single connection terminal to which the zone will be associated.</b> Only the available single connection terminals will be shown in the list.</li> </ol> <p><u>List of single connection terminals available for each peripheral module:</u></p> <ul style="list-style-type: none"> <li>• <b>lares:</b> all the terminals of lares 4.0.</li> <li>• <b>auxi/auxi 10in:</b> all the terminals of expansion module.</li> <li>• <b>ergo-rev.0/ergo:</b> "m1" and "m2" terminals of ergo keypads. Unavailable for ergoS and ergoM.</li> <li>• <b>duo:</b> "m1" and "m2" terminals of duo transceiver/repeater. Unavailable if duo is programmed as repeater.</li> <li>• <b>poli:</b> the internal reed contact or one of the auxiliary inputs on the "m1" and "m2" terminals.</li> <li>• <b>nanus:</b> internal reed contact.</li> <li>• <b>velum.</b></li> <li>• <b>nebula.</b></li> <li>• <b>auxi wls:</b> i1 and i2 terminals of the wireless auxi.</li> <li>• <b>matrix / matrix BUS:</b> for matrix -&gt; universal: generic output, for matrix -&gt; Optex BXS, WXI and WXS generic output / right / left, for matrix -&gt; Optex VXS and QXI generic output.</li> <li>• <b>IP:</b> IP zones are not supposed to have physical terminals, typically an IP Zone is represented by an IP device that can generate an HTTP GET request (e.g. IP camera).</li> <li>• <b>IP (Gateway Http):</b> same function as IP zone, but this Zone can be associated to the device with the Gateway http service active, giving the possibility to configure the supervision parameters: URL or IP address of the device to be supervised and supervision timer.</li> </ul>
--	--

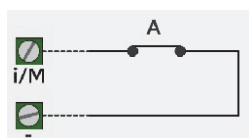
<b>Processing mode</b>	<p>After having associated the zone with the device, the type of analysis of the signal required to generate an alarm is determined.</p> <p>Note: some modes may not be usable depending on the type of device selected (i.e. on the lares 4.0 board, only the standard and command modes will be available)!</p> <p>For convenience, all available configurations will be described:</p> <ol style="list-style-type: none"> <li>1. <b>Standard:</b> to be combined with contacts, detectors, etc. <b>Note: not available for unum WLS, velum WLS, nebula WLS, auxi WLS.</b></li> <li>2. <b>Command:</b> this zone does not generate alarms, but is only used to activate scenarios. To program a command zone, associate to the zone the partitions that will arm/disarm. Subsequently, in the "Events" page, associate the real-time zone (alarm) with the scenario which must be activated. If all the partitions managed by that scenario are not associated, only the selected partitions will be armed/disarmed. If this option is activated, it is possible to directly manage an output (or a group of outputs using a Hashtag) without creating a scenario. In this case, the following additional configurations are displayed: <ol style="list-style-type: none"> <li>a. <b>Command output:</b> in this menu, it is possible to select the output (or the group of outputs via Hashtag) that you want to be managed by the command zone</li> <li>b. <b>Action type:</b> in this menu, it is possible to select the type of action to be performed on the output: activation, deactivation, switching (with respect to the current status), dimmer output (when an analog command output has been selected).</li> <li>c. <b>Command mode:</b> in this menu, it is possible to select the type of command between the button (the action on the output will be carried out only when the zone is opened) and the switch (the action is performed both at the opening and closure of the zone). <b>Note: this additional configuration is not available for unum WLS, velum WLS, nebula WLS, auxi WLS.</b></li> </ol> </li> <li>3. <b>Inertial/Glass break:</b> to be combined with seismic, glass break detectors etc. <b>Not available for lares, ergo, duo, auxi WLS.</b></li> <li>4. <b>Roller blind:</b> to be combined with detectors for roller blind (i.e. ropes contacts, etc.). <b>Not available for lares, ergo, duo, auxi WLS.</b></li> <li>5. <b>Test:</b> if this option is selected, only events in the event log will be traced without generating an alarm.</li> </ol>
<b>Category</b>	<p>Default value "Generic".</p> <p>If configured, in the "Security" page of the APP lares 4.0 for user, the zone being configured will be displayed in the category programmed in this field. (i.e. the zone called "nanus zone" with category = "Rubbery" will be displayed on the Security page -&gt; Sensors-&gt;"Rubbery -&gt; nanus zone" of the Lares 4.0 App).</p>
<b>Entry delay</b>	<p>The entry delay is the time that passes between the violation of the zone in an armed system and the alarm event: it is the time available to disarm the system when the zone is violated.</p> <p>Enable it if you want that the violation of the zone starts the entry time. The entry delay of the zone is possible if the partition to which it belongs is armed in delayed mode.</p> <ul style="list-style-type: none"> <li>•</li> </ul>
<b>Path</b>	<p>This field can be edited only if "Entry delay" field is enabled.</p> <p>Select the path (up to five paths are available) to which the zone with entry delay must be included.</p> <p>Zones belonging to the same path do not need to belong to the same partition. If no path is selected, the alarm will start when the entry timer expires.</p> <p>Default: No Path. Possible values: No Path, Path 1, ..., Path 5.</p>

<b>Level</b>	<p>This field can be edited only if "Path" field is different from "No Path".</p> <p>The level is the zone progressive number with respect to the entry path that you are configuring; if within the path, the zones will be violated in a different order than the numerical sequence assigned to the level, the alarm will be triggered.</p> <p>Default: 1. Possible values: 1...250.</p>
<b>Exit logic</b>	<p>In this section, the operating logic of the zone is set during the output time.</p> <p>There are three modes:</p> <ul style="list-style-type: none"> <li>- <b>Immediate</b>: if violated during the exit time, the zone will generate an alarm.</li> <li>- <b>Delayed</b>: Select this option if you want the zone to generate no alarms during the exit time.</li> <li>- <b>Last exit</b>: It is the last zone of the exit path, when it is breached and then restored during the exit time, it automatically resets the exit time. Always referring to figure a (Page 33), the zones marked with 1, 2 and 3 must be marked as exit delay and number 1 as "last exit".</li> </ul>
<b>Always active</b>	<p>If this option is enabled, when the zone is breached, an alarm will be generated regardless of the partitions associated to the zone (i.e. 24h zone).</p>
<b>Enable pre-alarm</b>	<p>Enable/disable the pre-alarm confirmation function of the zone, before triggering the alarm. Default value: disabled.</p> <p>This functionality is mutually exclusive with respect to "Always active", "Emergency exit" and "Test".</p> <p>Furthermore, although it is compatible with the Entry Delay, it is exclusive with respect to the "Path Management".</p> <p>This enabling depends on the values configured in the "Options -&gt; General-&gt; Management of pre-alarm zone" page.</p>
<b>Emergency Exit</b>	<p>If this option is enabled, the zone will always generate "events" as if it were armed while notifications will be sent only if the partitions, with which it is associated, are armed.</p> <p>Mutually exclusive, with respect to "Always active" option.</p>
<b>Test</b>	<p>If this option is enabled, the zone will never be armed and all the events occurred will be traced in the event log (both in arm and disarm mode).</p>
<b>Chime</b>	<p>If this option is enabled, when the zone is breached with the partitions disarmed, an audible signal will be generated on the keypads having "bell sound signal" enabled and associated to the same partitions of the same zone.</p> <div data-bbox="555 1391 660 1447">  </div> <p><b>Note:</b> "Always active" and "Chime" is not IMQ-SECURITY SYSTEMS certified.</p>

<b>Bypass</b>	<p>It is possible to manage the exclusion of the zone with four different modes:</p> <ol style="list-style-type: none"> <li>1. <b>Not bypassable:</b> if this option is selected, the zone cannot be excluded by the user.</li> <li>2. <b>Bypassable:</b> if this option is selected, the zone can be excluded by the user. An excluded zone does not signal alarms. Tamperers and faults/masks will continue to be signaled unless the option "also exclude zone tamper" is enabled.</li> <li>3. <b>Auto-bypassable:</b> if this option is selected, the zone is automatically excluded if it is breached at the time of arming. The self-exclusion never excludes tamperers and maskings unless the option "also exclude tamper zones" is enabled. The zone is automatically rearmed in the next disarming.</li> </ol>  <p><b>Note:</b> "Auto-bypassable" option is not IMQ-SECURITY SYSTEMS certified.</p> <ol style="list-style-type: none"> <li>4. <b>Auto-unbypass:</b> if this option is selected, the zone is automatically excluded. If it is breached at the time of arming, as soon as it returns to the resting status, it will be automatically rearmed.</li> </ol>
<b>Balance</b>	<p>Each control panel board has 8 inputs and 2 programmable I/O terminals that can be configured as inputs or outputs (so, on the control panel board, we already have 10 inputs). Both on the control panel and aux module, each input can be programmed into eight different types of balancing.</p>

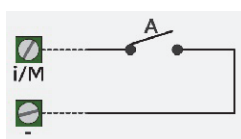
The following table shows how Iares 4.0 control panel interprets the resistance values for different balancing configurations and their associable conditions:

### 1. Normally closed:



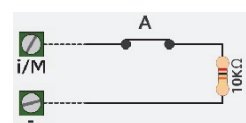
Band 0	Band 1	Band 2	Band 3	Band 4
0-1,8K $\wedge$	2,2-4,1K $\wedge$	4,2-6,8K $\wedge$	7,2-14K $\wedge$	(open)
Riposo	Alarm			

### 2. Normally open:



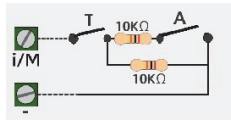
Band 0	Band 1	Band 2	Band 3	Band 4
0-1,8K $\wedge$	2,2-4,1K $\wedge$	4,2-6,8K $\wedge$	7,2-14K $\wedge$	(open)
Alarm				Idle

### 3. Balanced (10K):



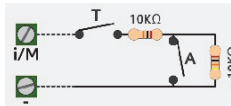
Band 0	Band 1	Band 2	Band 3	Band 4
0-0,1K $\wedge$	0,1-0,9K $\wedge$	0,9-6,2K $\wedge$	6,2-14,5K $\wedge$	(open)
Tamper			Idle	Alarm

#### 4. Double balancing in parallel (2 x 10K):



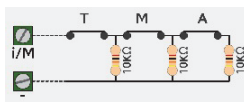
Band 0	Band 1	Band 2	Band 3	Band 4
0-0,5K $\wedge$	0,5-6,6K $\wedge$	6,6-12K $\wedge$	12-17K $\wedge$	(open)
Tamper	Idle		Alarm	Tamper

#### 5. Double balancing in serial (2 x 10K):



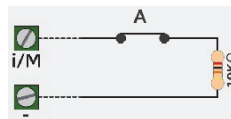
Band 0	Band 1	Band 2	Band 3	Band 4
0-1K $\wedge$	1-13K $\wedge$	13-24K $\wedge$	24-30K $\wedge$	(open)
Tamper	Idle	Alarm	Tamper	

#### 6. Triple balancing in parallel (3 x 10K):



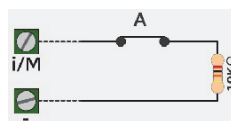
Band 0	Band 1	Band 2	Band 3	Band 4
0-0,5K $\wedge$	0,5-4,2K $\wedge$	4,2-7,6K $\wedge$	7,6-15K $\wedge$	(open)
Tamper	Idle	Alarm	Mask*	Tamper

#### 7. Balanced fault (10K):



Band 0	Band 1	Band 2	Band 3	Band 4
0-1,8K $\wedge$	2,2-4,1K $\wedge$	4,2-6,8K $\wedge$	7,2-14K $\wedge$	(open)
Fault			Idle	Fault

#### 8. Balanced tamper (10K):




Band 0	Band 1	Band 2	Band 3	Band 4
0-1,8K $\wedge$	2,2-4,1K $\wedge$	4,2-6,8K $\wedge$	7,2-14K $\wedge$	(open)
Tamper			Idle	Tamper

#### 9. Custom balancing:

When this setting is selected, a submenu that allows to associate one of custom balancing defined in the previous section to the zone, is enabled.



**Note:** All those parameters that disable the tampering are not IMQ - SECURITY SYSTEM certified. In particular, all the zones programmed as NC, NA.

<b>Pulse number</b>	It is the number of pulses necessary before the zone alarm is generated. They are standard pulses in the case of 'Standard' or 'Command' zone, and fast pulses in the case of 'Roller blind' or 'Inertial' zone.
<b>Alarm window (sec.)</b>	Time window within which the number of programmed pulses must occur so that an alarm is generated.
<b>Pulse lenght (msec.)</b>	<p>It is the duration of the single alarm pulse (expressed in ms.). This value determines the time for which the zone must be breached before the generation of a valid pulse, and is valid for all processing modes. For example, if we program a zone as 'Shutter', the alarm will be generated in case a programmed number of fast pulses occurs (shutter movement) or if the contact remains open for the time programmed in this window (wire cut protection). In the case of a zone programmed as 'Shutter' setting this time to 0, only the fast pulse analysis is carried out, without generating an alarm if the contact remains open.</p> <div style="display: flex; align-items: center;">  <div style="margin-left: 10px;"> <p><b>Note:</b> to "Pulse length" option, you must associate a pulse length of 400ms for intrusion and tampering signals in accordance with the standard EN 50131.</p> </div> </div>
<b>Alarm cycle</b>	It is the maximum number of alarms that can be generated by the zone: after exceeding the cycles set, the zone will no longer generate an alarm even if it is breached. The alarm cycles are reset each time the zone is armed. If set to 0, the zone can generate endless alarms when the partition to which it is assigned is armed.
<b>Inactivity (min.)</b>	<p>With the zone disarmed, if the zone itself has never been breached for the programmed time (expressed in minutes), the zone masking event will be generated (passive control of the masking).</p> <p>Minimum time 10 minutes, maximum time 2500 minutes (approximately 41 hours).</p>
<b>IP Zone:</b>  <b>Auto restore</b>	<p>If enabled, the control panel sends the restore command, the url address that the IP device must send for "alarm" signaling, will be displayed. Click on Copy button and paste it in the IP device.</p> <p>If disabled, the url addresses that the IP device must send for "alarm" and "restore" signalings, will be displayed. Click on Copy button and paste them in the IP device.</p> <p>Default value: enabled.</p>
<b>IP Supervision</b>	Enable/disable supervision of the IP (GW http) Zone.
<b>Masking notification time (min.)</b>	<p>Enter the supervision interval (expressed in minutes). The supervision consists of periodic communications between the control panel and the device with IP address/URL configured in the next field. The control panel checks the persistence of the connection, when it fails the IP zone masking will be generated; when the connection goes back to work the masking restore event will be generated.</p> <p>Possible values 1... 10. Default: 5.</p>
<b>IP address</b>	Enter the URL or IP address of the device to be supervised.

<b>HTTP endpoints on gateway</b>	<p>This section displays the endpoints exposed by Ksenia device, Gateway Http service enabled, applicable to the ZONES.</p> <p>"Read status GET", "Edit status using PUT/GET method" and " Bypass/Unbypass using PUT/GET method" APIs, display URL and body (JSON) with which the third-party device communicates with the device Ksenia. Copy and paste the messages to the connected device and edit the suggested values.</p>
----------------------------------	--


### 3.9.6 Users




This page contains all the users who will use the platform, their personal data (telephone, email, permissions, etc.) and the access levels assigned.

The configuration parameters of users are the following:

<b>Description</b>	Give a name to the user you are configuring.
<b>Access level</b>	<p>It establishes the access level to the lares 4.0 configuration menu. The following list of types are provided: Administrator, Master, Standard, Guest, Patrol, Arming mode Only and Key Only.</p> <ul style="list-style-type: none"> <li>• <b>Administrator:</b> can manage all the partitions and users of the system and the other administrators if present.</li> <li>• <b>Master:</b> can manage only the associated partitions of the system and other users (of lower level), clear alarm cycles/memory, faults and clear the communications which are both active and queued. This user can also create and modify the scheduler timers and can also create and modify the chronothermostats.</li> <li>• <b>Standard:</b> can manage the system as a master user, but can only see the present scheduler timers, edit the chronothermostats and enable/disable the access options his own user (key, remote and pin).</li> <li>• <b>Guest:</b> can only use the system locally, either via the user interfaces or a 'lares 4.0' App on a device in the same network of the panel. The user cannot access the system via cloud service and change the user's access options.</li> <li>• <b>Patrol:</b> if this option is selected, the code, the key or the remote control associated with it will be able to perform the disarming operations, but the partitions will be automatically rearmed at the end of the patrol time programmed in the 'Partitions' page. It is possible to 'force' the arming without waiting for the end of the patrol time. Keypads and readers must be enabled when disarming.</li> <li>• <b>Only Arming:</b> if this option is selected, the code, the key or the remote control associated with it will not be able to carry on the disarming operations.</li> <li>• <b>Key Only/No Action:</b> If this option is selected, when the code is entered, or the key is approached to the reader, only the scenario corresponding to the recognized code and/or recognized key event (programmed in the 'Events' page) is activated, without allowing the activation of the scenarios associated with the keypad or reader or accessing the menu (if approached to the ergo keypad). This option is very useful if you want to use the code to do only one action (e.g. the activation of an exit to open a door or a particular scenario).</li> </ul>
<b>Phone</b>	The telephone number (fixed or mobile) that will be called by the control panel.
<b>Email</b>	The e-mail address to which the event emails will be sent.
<b>Partitions</b>	Associate the partitions that can be managed to the user. In this way, it is possible to create a multi-user access on the APP (e.g. a semi-detached villa managed by a single central panel: user A can manage only his/her apartment but cannot manage the partitions associated with user B).
<b>Hashtags</b>	The group to which the user belongs (e.g. employees). It is possible to create a scenario that enables or disables all users with the hashtag employees




<b>Priority channel</b>	For each number, it is possible to program which communication channel must be used first. The non-priority channel, if any, will be used automatically as a backup vector. For example, if GSM is selected, the calls will be forwarded via GSM module. In case of anomalies on the mobile network, the calls will be sent via PSTN (if any).
<b>Call</b>	Enable/disable the feature for sending the voice call (via GSM or PSTN) to the user.
<b>SMS</b>	Enable/disable the feature for sending the SMS message.
<b>Email</b>	Enable/disable the feature for sending the email.
<b>Pin</b>	Enter the user code.
<b>Tag ID</b>	On each Rfid Tag, a unique code is saved. When the key is learned from the system, this code will appear in this field.
<b>Enable PIN</b>	Enable/disable the use of the code on the keypad and APP. If this option is disabled and the code is entered on the keypad, the message 'Wrong pin!' will appear; if you type on the APP, the message 'Login failed' will appear.
<b>Enable key</b>	Enable/disables the use of the key.
<b>Enable remote control</b>	Enable/disable the use of the remote control.  Note: In accordance with the standard EN 50131, the access levels are: Level 1: Access by any person; Level 2: Access by user; Level 3: Access by installer; Level 4: Access by the manufacturer.
<b>Duress code user</b>	Enable/disable duress code for user. The Event and Notification of Duress code can be found in the category System, subtype Duress Code (the entity is Panel).

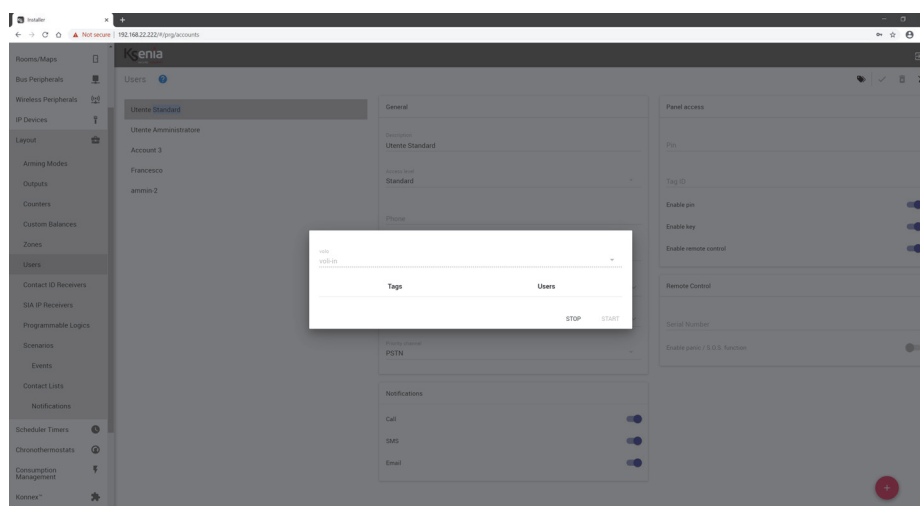
<p><b>Serial number</b></p>	<p>In this field, the serial number specified on the remote control label must be entered. Once the serial number is entered, the following options will appear:</p> <p>Confirm with vibration Long pressing the (i) key Long press ins. button Total Long press the disarming key Long press ins. button Partial</p> <ul style="list-style-type: none"> <li>• <b>Confirm with vibration:</b> activate/deactivate the vibration of the device to confirm the execution of the command sent.</li> <li>• <b>Long press info button:</b> enable/disable the functions associated with the long press of the key (i), the association with the actions is carried out on the "Events" page.</li> <li>• <b>Long press Away Arm button</b> (  ): enable/disable the functions associated with the long press of the Total Arm key, the association with the actions is carried out on the "Events" page.</li> <li>• <b>Long press Disarm button</b> (  ): enable/disable the functions associated with the long press of the Disarm key, the association with the actions is carried out on the "Events" page.</li> <li>• <b>Long press Stay Arm button</b> (  ): enable/disable the functions associated with the long press of the Partial key, the association with the actions is carried out on the "Events" page.</li> <li>• <b>Enable panic / S.O.S. function:</b> enable/disable Panic/S.O.S. function when any key of the remote control will be pressed, the association with the actions is carried out on the "Events -&gt; Remote Control -&gt; Press Panic/SOS button" page. This function is available only for remote controls with serial number higher than 100000.</li> </ul>
-----------------------------	---

### 3.9.6.1 Start enroll tags



Press the "Start enroll tags" icon  on the status bar for starting the tag recognition procedure (you must have installed the "volo-in" device/s) and a new page open, then select "volo-in" device and click on <START> button.

Put the tag close to the proximity reader "volo-in" and wait a few seconds until you'll see the number code displayed; at this point, associate a user from the Users list and click on STOP button to end the procedure.



### 3.9.7 Contact ID Receivers

The configuration parameters are the following:

<b>Description</b>	Give a name to the Contact ID receiver.
<b>Main phone number</b>	The telephone number of the Contact ID receiver to which the control panel is connected.
<b>Main code</b>	The 4-digit code that identifies the user. It is provided by the surveillance institute.
<b>Backup phone number</b>	The backup telephone number of the Contact ID receiver to which the control panel is connected.
<b>Backup code</b>	The 4-digit backup code that identifies the user. It is provided by the surveillance institute.

### 3.9.8 SIA IP Receivers

For each receiver, a possible backup receiver, on which the signals are sent in case of communication failure with the main receiver, is also created. Then enter the various parameters:

<b>Description</b>	Give a name to the SIA-IP receiver
<b>Enable Eth/GPRS supervision</b>	By selecting this option, in case of availability of both Ethernet connection and GPRS, supervisory packets are sent to the receiver using both the available communication channels alternately.
<b>Transmit over TCP</b>	Selecting this option sets the use of TCP instead of UDP protocol to send signals
<b>Use Timestamp</b>	If selected, this option sets the presence of information related to date and hour on the data packet.
<b>Communication timeout</b>	Waiting time in seconds necessary to receive confirmation of the signal sent to the receiver before the control panel makes a further attempt (default 5, maximum 60)
<b>Ethernet port</b>	Local port on which the control panel is listening when the message is sent via Ethernet
<b>Ethernet supervision interval (sec.)</b>	The time interval in seconds between a supervisory package and the other via the Ethernet channel.
<b>GPRS supervision interval</b>	The time interval in seconds between a supervisory package and the other via the GPRS channel.
<b>Supervision mode</b>	Select which receivers should be supervised (Select the 'Only one' option if you want to supervise only the main receiver, and 'All' if you want to supervise both)
<b>Protocol</b>	Application protocol used to format the data field of the transporting protocol SIAIP DC09 (SiaLevel3, KS-PROT for compatibility with the Vigilo receiver).
<b>Application Status ID</b>	ID of the control panel's application protocol used with the current receiver.
<b>Transporting Layer ID</b>	SIA-IP DC09 ID of the control panel used with the current receiver, maximum 12 hexadecimal digits.

The device allows sending signals to a primary receiver, and possibly to an optional secondary backup. The following data is valid for both receivers, but only mandatory for the primary receiver.

#### RICEIVER AND BACKUP RECEIVER

Ethernet IP	The IP address of the receiver to be used when a message is sent via Ethernet
Ethernet port	The remote port through which the receiver listens when a signal is sent via Ethernet
GPRS IP	The IP address of the receiver to be used when a message is sent via GPRS
GPRS port	The remote port through which the receiver listens when a message is sent via GPRS
Receiver ID	SIA-IP DC09 identifier of the receiver, maximum 6 hexadecimal digits

### 3.9.9 Programmable logics

The programmable logics allow to add to the standard events provided by the system the most advanced events that take into account certain conditions. When the conditions set are met, an event will be generated that can be used to run a scenario or send notifications.

The configuration parameters are the following:

<b>Description</b>	It is possible to set the programmable logic description that will be shown in the events log and notifications.
<b>Trigger</b>	In this field you can set the events that start checking the conditions listed below. By setting more than one event in this field they will always be in OR.
<b>Conditions</b>	In this field you can set the conditions to be verified in order to generate the event related to the programmable logic. The conditions could be set in AND or OR. In case you want to set a time window, use the virtual outputs (timer) to be set on the conditions.

### 3.9.10 Scenarios

Depending on the control panel model, up to 512 scenarios can be configured, all of which can be managed remotely. The scenarios are a set of up to 16 actions, which can freely manage outputs (activation, deactivation, switching), zones (exclusion, inclusion, switching), users (enabling, disabling), insertion mode, counters (increase, decrease, reset).

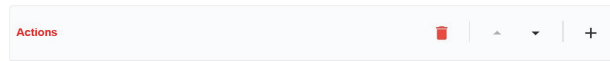
The configuration parameters are the following:

<b>Description</b>	Give a name to the scenario you are configuring (e.g. alarm and outdoors lights)
<b>Partitions</b>	The scenario can manage outputs, users, insertion mode, etc. associated to a partition.
<b>Rooms</b> (see <a href="#">“Rooms / Maps menu” page 23</a> )	Click on the arrow next to the field to open the menu with the list of Rooms/ Maps previously programmed. The association Rooms / Maps and Scenarios allows the device to be managed directly from the Map.

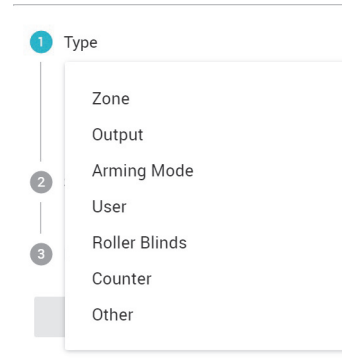
<p><b>APP management</b></p>	<p>Configuration of APP and Webserver management mode. Configuration parameters are the following:</p> <ul style="list-style-type: none"> <li>• <b>Hidden:</b> if this option is selected, the output will not be displayed in the APP and Web server in the page of real-time output.</li> <li>• <b>With PIN (local) - With PIN (remote):</b> in this case, the output will be managed locally with PIN and it will be managed through the APP in the same way.</li> <li>• <b>With PIN (local) - Not managed (remote):</b> in this case, the output will be managed locally by PIN but it will not be possible to manage it through the APP (even if displayed).</li> <li>• <b>Without PIN (local) - Without PIN (remote):</b> in this case, the output will be managed locally without PIN and it will be managed through the APP in the same way.</li> <li>• <b>Without PIN (local) - Not managed (remote):</b> in this case, the output will be managed locally without PIN but it will not be possible to manage it through the APP (even if displayed).</li> <li>• <b>Without PIN (local) - With PIN (remote):</b> in this case the output will be managed locally without PIN but it will be required to enter a code to manage it through the APP.</li> <li>• <b>Not managed (local) - Not managed (remote):</b> in this case, it will not be possible to manage it through the APP (even if displayed).</li> </ul>
------------------------------	---

## Actions

In this section the actions are associated with the scenario. When a new scenario is created the actions are not programmed, the programming section appears as follows:



To add new "Action" click on <+> and configure the following three fields:



- **Type:** identifies the group that will be managed (i.e. zone, partition, output etc.).
- **Subtype:** the action that will take effect on the above parameter (Type) (i.e. Type: Zone -> Subtype: bypass zone).
- **Entity:** detail of the zone, the partition, the device, the user, Counters, etc. that will be managed.

To add the new action click on <ADD> button.

### Type: **Zone**

The subtypes available are:


- **Bypass zone:** a previously included zone is excluded.
- **Unbypass zone:** a previously excluded zone is included.
- **Toggle zone:** if this option is enabled, a previously excluded zone is included and vice versa.

Note: this subtype has no effect on zones with the "unbypass" attribute.

### Type: **Output**

The subtypes available are:

- **Output on:** the output is activated.
  - **Output off:** the output is deactivated.
  - **Toggle output:** a previously activated output is deactivated and vice versa.
- Note: this subtype also affects outputs with the "unmanaged (local)" and "unmanaged (remote)" attributes. If an output is programmed with the "with PIN (local)" or "with PIN (remote)" attribute, it will be managed by the scenario without requiring a PIN.

	<p>Type: <b>Arming mode</b> The subtypes available are:</p> <ul style="list-style-type: none"> <li>  <b>Compliance EN50131:</b> if the system is not ready, it will not be armed and a "Failure to insert" event will be generated.  <b>Note:</b> if there is an open zone with the "bypass" and "unbypass" attributes, at the time of arming mode it will be shown open on the keypad, but it cannot be excluded. As a result, the system cannot be inserted.  Zones with the "self-exclusion" attribute, if opened during arming mode, will be excluded and will not generate alarms even if they return on idle: they will be reincluded when they will be disarmed.  Zones with the "with reinclusion" attribute, if opened during arming mode, will be excluded and will not generate alarms. If they go back in idle, they will be reincluded and therefore will be ready to generate an alarm. </li> <li> <b>Manual bypass:</b> if the system is not ready, the list of open zones will be shown with the possibility of manual exclusion.  <b>Note:</b> if, upon arming mode, there is an open area with an "unbypass" attribute, it will be shown on the keypad but it cannot be excluded.  Zones with the "self-exclusion" attribute, if opened during arming mode, will be excluded and will not generate alarms even if they return to rest: they will be reincluded when they are switched off.  Zones with the "with reinclusion" attribute, if opened during arming mode, will be excluded and will not generate alarms. If they go back they will be reincluded and will, therefore, be ready to generate an alarm.  Zones with the "exclusion" attribute, at the time of arming mode, are shown on the keypad and cannot be excluded. </li> <li> <b>Forced arm with alarm:</b> if the system is not ready, it will be armed and an alarm will generate.  <b>Note:</b> if there is an open area with the "unbypass" attribute at the time of arming mode, this zone will not be excluded and an alarm will be generated. The same applies to areas with the "bypass" attribute (however, these areas will not be self-excluded).  Zones with the "self-exclusion" attribute, if open during arming mode, will be excluded and will not generate alarms even if they return to rest: they will be reincluded when they are switched off.  Zones with the "with reinclusion" attribute, if opened during arming mode, will be excluded and will not generate alarms. If they go back they will be reincluded and will, therefore, be ready to generate an alarm. </li> </ul>
--	---







	<ul style="list-style-type: none"> <li>• <b>Forced arm with auto-bypass:</b> if the system is not ready, it will be armed with forced exclusion of any open areas.</li> </ul> <p><b>Note:</b> if there is an open area with the "unbypass" attribute, at the time of arming mode, this zone will not be excluded and an alarm will be generated. Zones with the "exclusion" and "self-exclusion" attributes, if open during arming mode, will be excluded and will not generate alarms even if they return to rest: they will be reincluded when they are switched off. Zones with the "with reinclusion" attribute, if opened during arming mode, will be excluded and will not generate alarms. If they go back they will be reincluded and will, therefore, be ready to generate an alarm.</p> <p>Type: <b>Users</b> The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Enable user:</b> the user's account (including the code, key or remote control), if inactive, is now activated.</li> <li>• <b>Disable user:</b> the user's account (including the code, key or remote control) is deactivated.</li> </ul> <p>Type: <b>Roller blinds</b> The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Open:</b> the blind is opened</li> <li>• <b>Close:</b> the blind is closed</li> <li>• <b>Stop:</b> the blind is stopped</li> </ul> <p>Type: <b>Counter</b> The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Increase:</b> increase the number counted.</li> <li>• <b>Decrease:</b> decrease the number counted.</li> <li>• <b>Reset:</b> reset the number counted.</li> </ul> <p>Type: <b>Other</b> The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Call queue reset:</b> cancel calls in progress.</li> <li>• <b>Alarm reset:</b> all outputs associated with an alarm or tamper event are stopped.</li> </ul>
<b>Http endpoint on gateway</b>	<p>This section displays the endpoints exposed by Ksenia device, Gateway Http service enabled, applicable to the SCENARIOS.</p> <p>"Scenario execution using POST/GET method" display URL with which the third-party device communicates with the device Ksenia. Copy and paste the messages to the connected device</p>

After having entered the three parameters described above, click on (  ) to confirm.

To add more actions, click on <+> (plus).

See below an example with three programming actions.

When the scenario occurs, zone 1 is excluded, the green led output is activated and account 2 is enabled (if previously enabled nothing will change).

Actions		   
Bypass zone	IN 1	
Unbypass zone	green led	
Enable user	Account 2	

To cancel a single action (i.e. "Bypass zone" 1), click on the action desired and then click on  icon.

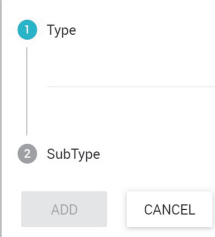


To move a single action from top to bottom and vice versa, click on the little arrows near the  icon.

### 3.9.11 Events

This page links events (alarm, tamper, etc.) with the scenarios programmed.

For creating events for which you want to perform a single action you can associate the action to the event directly, to add an action to the event, just perform the same configuration to add an action to the scenario; however, the possibility to create a scenario, associate one or more actions to it and, at last, associate the scenario with the event, remains.

To program the "Events", that is the executions/actions of the scenarios (arming, activation of outputs, etc.) already programmed, the following parameters must be configured:

<b>Type</b>	It identifies the group that generates an event (i.e. zone, partition, output etc.).
<b>Subtype</b>	<p>This is the action related to the previous parameter (i.e. Type: Zone -&gt; Subtype: zone alarm). You can make a multiple choice with up to 15 items.</p>  <p>After having configured the previously described two parameters, click on  (  ). At this point it is necessary to set two other parameters:</p> <ul style="list-style-type: none"> <li>• <b>Entities:</b> enter the zone, the partition, the device, the user, etc., that generates the event.</li> <li>• <b>Scenario:</b> enter the previously programmed scenario, which will be activated when the event generated by the selected entity occurs.</li> </ul> <p>The notification types are listed below the "Subtypes".</p> <p><b>Type: Zone</b> The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Alarm:</b> the scenario runs when the zone generates an alarm.</li> <li>• <b>Restore:</b> the scenario runs when the zone is restored after an alarm.</li> <li>• <b>Pre-alarm:</b> the scenario runs when the zone generates a pre-alarm.</li> <li>• <b>Tamper:</b> the scenario runs when the zone generates a tamper alarm.</li> <li>• <b>Tamper restore:</b> the scenario runs when a tamper is restored.</li> <li>• <b>Bypass:</b> the scenario runs when the zone is excluded.</li> <li>• <b>Unbypass:</b> the scenario runs when the zone is included.</li> <li>• <b>Mask:</b> the scenario runs when the detector generates a masking alarm.</li> <li>• <b>Mask restore:</b> the scenario runs when the detector's masking condition is restored.</li> <li>• <b>Real time - Alarm:</b> the scenario runs when the zone is alarmed, even with the partition switched off.</li> <li>• <b>Real time - Restore:</b> the scenario runs when the previous condition will be restored.</li> </ul>

	<p>Type: <b>Partition</b></p> <p>The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Alarm</b>: the scenario runs when the partition generates an alarm event.</li> <li>• <b>Arm</b>: the scenario runs when the partition is armed.</li> <li>• <b>Tamper</b>: the scenario runs when the partition generates a tamper alarm.</li> <li>• <b>Disarm</b>: the scenario runs when the partition is disarmed.</li> <li>• <b>Chime</b>: the scenario runs when the chime is activated.</li> <li>• <b>End chime</b>: the scenario runs when the chime is deactivated.</li> <li>• <b>Patrol</b>: the scenario runs when, following switch-off, the patrol has begun.</li> <li>• <b>End patrol</b>: the scenario runs when the patrol ends.</li> <li>• <b>Entry delay</b>: the entry delay starts when the partition is armed.</li> <li>• <b>Entry delay end</b>: the scenario runs when, after activation, the entry time ends.</li> <li>• <b>Exit delay</b>: the exit delay begins when the system is armed.</li> <li>• <b>Exit delay end</b>: the scenario runs when the exit time ends and the system is armed.</li> <li>• <b>Negligence</b>: the scenario runs when the negligence time ends (if programmed in the "Partitions") page</li> <li>• <b>Missed arming mode</b>: the scenario runs when the control panel aborts the entry (e.g. area open during arming mode and the scenario that manages the entry has the EN5013 compatible or manual exclusion attribute).</li> </ul> <p>Type: <b>Output</b></p> <p>The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Output ON</b>: the scenario runs when the output is activated (command by APP or following an event).</li> <li>• <b>Output OFF</b>: the scenario runs when the output is deactivated (command by APP or following an event).</li> <li>• <b>Reconnect load output</b>: (to be used in case of load outputs) the scenario runs when the output is activated.</li> <li>• <b>Disconnect load output</b>: (to be used in case of load outputs) the scenario runs when the output is deactivated.</li> </ul>
--	---

	<p>Type: <b>Peripheral</b></p> <p>The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Tamper (BUS):</b> the scenario runs when a BUS device generates a tamper alarm (i.e. opening of an ergo keypad).</li> <li>• <b>Tamper restore (BUS):</b> the scenario runs when tamper on the BUS device is restored.</li> <li>• <b>Tamper (wls):</b> the scenario runs when a wireless device generates a tamper alarm (i.e. opening of the poli lid)</li> <li>• <b>Tamper restore (wls):</b> the scenario runs when the tamper on a wireless device is restored.</li> <li>• <b>Missing (BUS):</b> the scenario runs when a BUS device is no longer detected by the control panel (i.e. cable cut or peripheral fault).</li> <li>• <b>Missing restore (BUS):</b> the scenario runs when the device returns and is detected by the control panel (i.e. device operation reset or BUS wiring reset).</li> <li>• <b>Missing (wls):</b> the scenario runs when the control panel no longer receives periodic communication from some wireless devices.</li> <li>• <b>Missing restore (wls):</b> the scenario runs when the control panel returns to receive the periodic communication of a previously lost wireless device.</li> <li>• <b>Tamper (IP):</b> the scenario runs when an IP device generates a tamper alarm.</li> <li>• <b>Tamper restore (IP):</b> the scenario runs when tamper on the IP device is restored.</li> <li>• <b>Missing (IP):</b> the scenario runs when an IP device is no longer detected by the control panel.</li> <li>• <b>Missing restore (IP):</b> the scenario runs when the IP device returns and is detected by the control panel.</li> </ul> <p>Type: <b>Keypad / Keypad wireless</b></p> <p>The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Key 0:</b> the scenario runs when the (0) key on the keypad is pressed.</li> <li>• <b>Key 1:</b> the scenario runs when the (1) key on the keypad is pressed.</li> <li>• <b>Key 2:</b> the scenario runs when the (2) key on the keypad is pressed</li> <li>• <b>Key 3:</b> the scenario runs when the (3) key on the keypad is pressed</li> <li>• <b>Key 4:</b> the scenario runs when the (4) key on the keypad is pressed</li> <li>• <b>Key 5:</b> the scenario runs when the (5) key on the keypad is pressed</li> <li>• <b>Key 6:</b> the scenario runs when the (6) key on the keypad is pressed</li> <li>• <b>Key 7:</b> the scenario runs when the (7) key on the keypad is pressed</li> <li>• <b>Key 8:</b> the scenario runs when the (8) key on the keypad is pressed</li> <li>• <b>Key 9:</b> the scenario runs when the (9) key on the keypad is pressed</li> </ul> <p>Type: <b>Proximity reader</b></p> <p>The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Green Led:</b> the scenario runs when the green LED on the reader is selected.</li> <li>• <b>Red Led:</b> the scenario runs when the red LED on the reader is selected.</li> <li>• <b>White Led:</b> the scenario runs when the white LED on the reader is selected.</li> <li>• <b>Blue Led:</b> the scenario runs when the blue LED on the reader is selected.</li> <li>• <b>Yellow Led:</b> the scenario runs when the yellow LED on the reader is selected.</li> </ul>
--	--

	<p>Type: <b>Communication</b></p> <p>The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Start:</b> the scenario runs when the control panel initiates a PSTN/GSM/E.mail call, etc.</li> <li>• <b>Fail:</b> the scenario runs when the control panel fails a PSTN/GSM/E.mail call, etc.</li> <li>• <b>Incoming call:</b> the scenario runs when the control panel receives a call</li> <li>• <b>Contact-ID done:</b> the scenario runs when the control panel makes a call using the Contact-ID protocol.</li> <li>• <b>Contact-ID failed:</b> the scenario runs when a call made using the Contact-ID protocol was unsuccessful.</li> <li>• <b>SIA done:</b> the scenario runs when the control panel makes a call using the SIA protocol.</li> <li>• <b>SIA failed:</b> the scenario runs when the call made using the SIA protocol was unsuccessful.</li> </ul> <p>Type: <b>Power management</b></p> <p>The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Main fault:</b> the scenario runs when power is lost on the "Iares 4.0" panel, the wireless duo repeater or the "opis" power supply station.</li> <li>• <b>Mains restore:</b> the scenario runs when power supply is restored to the "Iares 4.0" panel, the wireless duo repeater or the "opis" power supply station.</li> <li>• <b>Low battery:</b> the scenario runs when the battery voltage drops below the threshold (&lt;11V) (in the absence of the network)</li> <li>• <b>Restored low battery:</b> the scenario runs when the battery voltage is restored following the recovery of the 230V voltage.</li> <li>• <b>Battery fault:</b> the scenario runs when the "Iares 4.0" control panel, the imago siren, a wireless device and the "opis" power supply station fail the battery test.</li> <li>• <b>Low power output:</b> the scenario runs when the voltage supplied by the "Iares 4.0" control panel falls below the threshold (&lt;14.4V), or when the "opis" power supply station falls below the threshold (&lt;13.1V)</li> </ul>
--	---

	<ul style="list-style-type: none"> <li>• <b>Restored low power output:</b> the scenario runs when the voltage supplied by the "lares 4.0" control panel is restored above the threshold (&gt; 14.4V) or when the voltage supplied by the "opis" power supply station is reset above the threshold (&gt; 13.1V)</li> <li>• <b>Battery charger fault:</b> the scenario runs when the "lares 4.0" control panel or the "opis" power supply station fails to supply the necessary current to the system.</li> <li>• <b>Restored battery charger:</b> the scenario runs when the power supply of "lares 4.0" or the "opis" power supply station returns to normal operation or it is replaced.</li> <li>• <b>Fuse fault:</b> the scenario runs when the fuse on the "lares 4.0" control panel or the "opis" power supply station goes into operation (e.g. due to a short circuit).</li> <li>• <b>Restored fuse:</b> the scenario runs when the fuse on the "lares 4.0" control panel or the "opis" power supply station resets its fuse operating condition.</li> </ul> <p>Note: if the CPU window appears in the entity window, the events that generate the communication refer to the "lares 4.0" panel.</p> <p>Type: <b>Remote control</b> The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Disarm button:</b> the scenario runs by pressing the disarm button on the remote control (short pressing).</li> <li>• <b>Stay arm button:</b> the scenario runs by pressing the partial button on the remote control (short pressing).</li> <li>• <b>Away arm button:</b> the scenario runs by pressing the Total button on the remote control (short pressing).</li> <li>• <b>Long press disarm button:</b> the scenario runs by pressing the switch-off button on the remote control (long pressing).</li> <li>• <b>Long press stay arm button:</b> the scenario runs by pressing the Partial button on the remote control (long pressing).</li> <li>• <b>Long press away arm button:</b> the scenario runs by pressing the Total button on the remote control (long pressing).</li> <li>• <b>Long press info button:</b> the scenario runs by pressing the (i) button on the remote control (long pressing).</li> <li>• <b>Press Panic/SOS button:</b> the scenario runs when any key of the remote control will be pressed.</li> </ul> <p>Type: <b>User</b> The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Recognized PIN code:</b> the scenario runs when a code is recognized. Valid option for codes entered on the keypad or APP.</li> <li>• <b>Recognized tag:</b> the scenario runs approaching a Key enabled to the reader (keypad or volo/volo-IN).</li> </ul>
--	--

	<p>Type: <b>System</b></p> <p>The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Tamper:</b> the scenario runs when a tamper condition occurs in the metal box of the control panel (opening and/or detachment from the wall) detected through the switches connected to the T connector of the "lares" card.</li> <li>• <b>Tamper restore:</b> the scenario runs when the tamper condition of the control panel box is reset</li> <li>• <b>Start maintenance:</b> the scenario runs when a new configuration is applied.</li> <li>• <b>End maintenance:</b> the scenario runs when parameter programming, via portal or installer app, is completed</li> <li>• <b>Periodic report:</b> the scenario runs based on a scheduled periodic event (test event).</li> <li>• <b>Wrong PIN:</b> the scenario runs after three incorrect codes have been entered on the keypad. After four incorrect codes, the keypad is blocked for (90s.).</li> <li>• <b>Recognized installer PIN:</b> the scenario runs when the installer PIN code is recognized.</li> <li>• <b>Panel shutdown:</b> the scenario runs when a system shutdown event occurs (230V power is off and the battery is discharged). In this case we should preserve the battery from total discharge.</li> <li>• <b>Panel reset:</b> the scenario runs when the control panel has restarted because the power has been lost and subsequently restored or due to a system fault or due to a firmware update.</li> <li>• <b>Lost ethernet connection:</b> the scenario runs when the Ethernet cable is disconnected (or when the router/switch is turned off).</li> <li>• <b>Restore ethernet connection:</b> the scenario runs when the Ethernet cable is reconnected (or when the router/switch is turned on).</li> <li>• <b>PSTN fault:</b> the scenario runs when the telephone line is removed from the PSTN module (cable cut or line failure).</li> <li>• <b>Restore PSTN:</b> the scenario runs when the telephone line on the PSTN module is restored.</li> <li>• <b>GSM network fault:</b> the scenario runs when the GSM network is missing (no signal, GSM repeater malfunctioned or switched off for maintenance, SIM disabled and no longer registered on the network of the mobile operator).</li> <li>• <b>GSM network restore:</b> the scenario runs when the GSM network is restored.</li> <li>• <b>Remote supervision fault:</b> the scenario runs when the IP receiver fails to send supervision.</li> <li>• <b>Restored supervision:</b> the scenario runs when the IP receiver responds to supervision packets.</li> <li>• <b>Jamming wireless:</b> the scenario runs when the wireless receiver of the panel or one of the two-way transceivers detect a disturbance on the 868Mhz frequency.</li> <li>• <b>Restore jamming wireless:</b> the scenario runs when the noise on the 868MHz frequency, detected by the wireless receiver of the control panel or one of the two-way transceivers, ceases to exist.</li> <li>• <b>Network from LAN to Mobile:</b> the scenario runs when a data transfer from LAN to Mobile takes place.</li> <li>• <b>Network from Mobile to LAN:</b> the scenario runs when a data transfer from Mobile to LAN takes place.</li> <li>• <b>Missing Internet:</b> the scenario runs when the Internet network is missed</li> <li>• <b>Restore Internet:</b> the scenario runs when the internet network is restored.</li> <li>• <b>Duress code:</b> the scenario runs when a duress code is recognised.</li> </ul>
--	--

	<p>Type: <b>Programmable logic</b> The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Programmable:</b> the scenario runs when the programmable logic is realized.</li> </ul> <p>Type: <b>Smart Home</b> The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Lux sensor activation:</b> the scenario runs when the twilight threshold, configured for the domus multifunction sensor, exceeds (more or less) (the event generation will consider a hysteresis equal to 5%).</li> <li>• <b>Lux sensor deactivation:</b> the scenario runs when the brightness values detected by the domus are within the configured twilight threshold.</li> <li>• <b>Wet environment:</b> the scenario runs when the Wet threshold, configured for the domus multifunction sensor, exceeds (more or less) (the event generation will consider a hysteresis equal to 2%).</li> <li>• <b>Dry environment:</b> the scenario runs when the dry values detected by the domus are within the configured dry threshold.</li> </ul> <p>Type: <b>Counter</b> The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Counter sub-threshold</b> = the scenario runs at the first increase after the threshold is reached.</li> <li>• <b>Counter reached-threshold</b> = the scenario runs upon reaching the threshold.</li> <li>• <b>Counter reset</b> = the counter increases up to the threshold; upon reaching the threshold, the "reached-threshold" event will be generated, at the first increase after the threshold is reached, the counter restarts from 1 and the "sub-threshold" event will be generated. If the threshold has been reached and a decrease occurs, the "sub-threshold" event will be generated.</li> </ul> <p>Type: <b>Load management</b> The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Excess power consumption:</b> the event will be generated upon exceeding the "Consumption threshold" configured in "Consumption management".</li> <li>• <b>Normal power consumption:</b> the event will be generated when the consumption falls below the thresholds configured in "Consumption management".</li> <li>• <b>Load disconnection risk:</b> the event will be generated upon exceeding the "Disconnection threshold" configured in "Consumption management".</li> <li>• <b>End risk of load disconnection:</b> the event will be generated when the disconnection risk falls below the "Disconnection threshold" configured in "Consumption management".</li> </ul>
--	---

### 3.9.12 Contact lists

It is possible to program the user groups that will receive the communications (calls, SMS, e-mail, etc.).

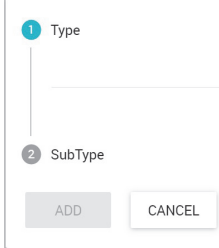


<b>Description</b>	Give a name to the group of contacts (i.e. employees).
<b>Options</b>	Select the type of communication to send for a particular list of contacts. It is possible to make a multiple choice: <ul style="list-style-type: none"><li>- <b>Voice call</b>: sends the voice call via GSM or PSTN.</li><li>- <b>SMS</b>: sends the SMS generated automatically by the control panel</li><li>- <b>E-mail</b>: sends the detailed email of the event.</li><li>- <b>Contact-ID</b>: sends a message via Contact-ID protocol.</li><li>- <b>SIA IP</b>: sends a message via SIA-IP protocol.</li></ul>
<b>Contacts</b>	Select users (previously programmed) that will receive communications.
<b>Contact-ID</b>	Select Contact-ID receivers (previously programmed) that will receive communications.
<b>SIA IP</b>	Select SIA IP receivers (previously programmed) that will receive communications.

### 3.9.13 Notifications

This page links the notifications (calls, SMS, etc.) with various events.

To program the "Notifications" the following parameters must be configured:

<b>Type</b>	It identifies the group generating notification (i.e. zone, partition, output, etc.).
<b>Subtype</b>	<p>This is the event related to the previous parameter (i.e. Type: Zone -&gt; Subtype: zone alarm). You can make a multiple choice with up to 15 items.</p>  <p>After having configured the previously described two parameters, click on ( <b>ADD</b> ). At this point it is necessary to set two other parameters:</p> <ul style="list-style-type: none"> <li>• <b>Entities:</b> enter the zone, the partition, the device, the user, etc., that generates the notification.</li> <li>• <b>Contact list:</b> enter a previously programmed contact list, which will receive calls, text messages, e-mails, and the contact ID message</li> </ul> <p>The notification types are listed below the "Subtypes".</p> <p>Type: <b>Zone</b> The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Alarm:</b> send a message when the zone generates an alarm.</li> <li>• <b>Restore:</b> send a message when the zone is restored after an alarm.</li> <li>• <b>Pre-alarm:</b> send a message when the zone generates a pre-alarm.</li> <li>• <b>Tamper:</b> send a message when the zone generates a tamper alarm.</li> <li>• <b>Tamper restore:</b> send a message when a tamper is restored.</li> <li>• <b>Bypass:</b> send a message when the zone is excluded.</li> <li>• <b>Unbypass:</b> send a message when the zone is included.</li> <li>• <b>Mask:</b> send a message when the detector generates a masking alarm.</li> <li>• <b>Mask restore:</b> send a message when the detector's masking condition is restored.</li> <li>• <b>Real time - Alarm:</b> send a message when the zone is alarmed, even with the partition switched off.</li> <li>• <b>Real time - Restore:</b> send a message when the previous condition will be restored.</li> </ul>

	<p>Type: <b>Partition</b></p> <p>The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Alarm</b>: send a message when the partition generates an alarm event.</li> <li>• <b>Arm</b>: send a message when the partition is armed.</li> <li>• <b>Tamper</b>: send a message when the partition generates a tamper alarm.</li> <li>• <b>Disarm</b>: send a message when the partition is disarmed.</li> <li>• <b>Chime</b>: send a message when the chime is activated.</li> <li>• <b>End chime</b>: send a message when the chime is deactivated.</li> <li>• <b>Patrol</b>: send a message when, following switch-off, the patrol has begun.</li> <li>• <b>End patrol</b>: send a message when the patrol ends.</li> <li>• <b>Entry delay</b>: the entry delay starts when the partition is armed.</li> <li>• <b>Entry delay end</b>: send a message when, after activation, the entry time ends.</li> <li>• <b>Exit delay</b>: the exit delay begins when the system is armed.</li> <li>• <b>Exit delay end</b>: send a message when the exit time ends and the system is armed.</li> <li>• <b>Negligence</b>: send a message when the negligence time ends (if programmed in the "Partitions") page</li> <li>• <b>Missed arming mode</b>: send a message when the control panel aborts the entry (e.g. area open during arming mode and the scenario that manages the entry has the EN5013 compatible or manual exclusion attribute).</li> </ul> <p>Type: <b>Output</b></p> <p>The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Output ON</b>: send a message when the output is activated (command by APP or following an event).</li> <li>• <b>Output OFF</b>: send a message when the output is deactivated (command by APP or following an event).</li> </ul>
--	--

	<p>Type: <b>Peripheral</b></p> <p>The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Tamper (BUS):</b> send a message when a BUS device generates a tamper alarm (i.e. opening of an ergo keypad).</li> <li>• <b>Tamper restore (BUS):</b> send a message when tamper on the BUS device is restored.</li> <li>• <b>Tamper (wls):</b> send a message when a wireless device generates a tamper alarm (i.e. opening of the poli lid)</li> <li>• <b>Tamper restore (wls):</b> send a message when the tamper on a wireless device is restored.</li> <li>• <b>Missing (BUS):</b> send a message when a BUS device is no longer detected by the control panel (i.e. cable cut or peripheral fault).</li> <li>• <b>Missing restore (BUS):</b> send a message when the device returns and is detected by the control panel (i.e. device operation reset or BUS wiring reset).</li> <li>• <b>Missing (wls):</b> send a message when the control panel no longer receives periodic communication from some wireless devices.</li> <li>• <b>Missing restore (wls):</b> send a message when the control panel returns to receive the periodic communication of a previously lost wireless device.</li> <li>• <b>Tamper (IP):</b> send a message when an IP device generates a tamper alarm.</li> <li>• <b>Tamper restore (IP):</b> send a message when tamper on the IP device is restored.</li> <li>• <b>Missing (IP):</b> send a message when an IP device is no longer detected by the control panel.</li> <li>• <b>Missing restore (IP):</b> send a message when the IP device returns and is detected by the control panel.</li> </ul> <p>Type: <b>Keypad / Keypad wireless</b></p> <p>The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Key 0:</b> send a message when the (0) key on the keypad is pressed.</li> <li>• <b>Key 1:</b> send a message when the (1) key on the keypad is pressed.</li> <li>• <b>Key 2:</b> send a message when the (2) key on the keypad is pressed</li> <li>• <b>Key 3:</b> send a message when the (3) key on the keypad is pressed</li> <li>• <b>Key 4:</b> send a message when the (4) key on the keypad is pressed</li> <li>• <b>Key 5:</b> send a message when the (5) key on the keypad is pressed</li> <li>• <b>Key 6:</b> send a message when the (6) key on the keypad is pressed</li> <li>• <b>Key 7:</b> send a message when the (7) key on the keypad is pressed</li> <li>• <b>Key 8:</b> send a message when the (8) key on the keypad is pressed</li> <li>• <b>Key 9:</b> send a message when the (9) key on the keypad is pressed</li> </ul> <p>Type: <b>Proximity reader</b></p> <p>The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Green Led:</b> send a message when the green LED on the reader is selected.</li> <li>• <b>Red Led:</b> send a message when the red LED on the reader is selected.</li> <li>• <b>White Led:</b> send a message when the white LED on the reader is selected.</li> <li>• <b>Blue Led:</b> send a message when the blue LED on the reader is selected.</li> <li>• <b>Yellow Led:</b> send a message when the yellow LED on the reader is selected.</li> </ul>
--	---

	<p>Type: <b>Communication</b></p> <p>The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Start:</b> send a message when the control panel initiates a PSTN/GSM/E.mail call, etc.</li> <li>• <b>Fail:</b> send a message when the control panel fails a PSTN/GSM/E.mail call, etc.</li> <li>• <b>Incoming call:</b> send a message when the control panel receives a call</li> <li>• <b>Contact-ID done:</b> send a message when the control panel makes a call using the Contact-ID protocol.</li> <li>• <b>Contact-ID failed:</b> send a message when a call made using the Contact-ID protocol was unsuccessful.</li> <li>• <b>SIA done:</b> send a message when the control panel makes a call using the SIA protocol.</li> <li>• <b>SIA failed:</b> send a message when the call made using the SIA protocol was unsuccessful.</li> </ul> <p>Type: <b>Power management</b></p> <p>The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Main fault:</b> send a message when power is lost on the "Iares 4.0" panel, the wireless duo repeater or the "opis" power supply station.</li> <li>• <b>Mains restore:</b> send a message when power supply is restored to the "Iares 4.0" panel, the wireless duo repeater or the "opis" power supply station.</li> <li>• <b>Low battery:</b> send a message when the battery voltage drops below the threshold (&lt;11V) (in the absence of the network)</li> <li>• <b>Restored low battery:</b> send a message when the battery voltage is restored following the recovery of the 230V voltage.</li> <li>• <b>Battery fault:</b> send a message when the "Iares 4.0" control panel, the imago siren, a wireless device and the "opis" power supply station fail the battery test.</li> <li>• <b>Low power output:</b> send a message when the voltage supplied by the "Iares 4.0" control panel falls below the threshold (&lt;14.4V), or when the "opis" power supply station falls below the threshold (&lt;13.1V)</li> </ul>
--	--

	<ul style="list-style-type: none"> <li>• <b>Restored low power output:</b> send a message when the voltage supplied by the "Iares 4.0" control panel is restored above the threshold (&gt; 14.4V) or when the voltage supplied by the "Opis" power supply station is reset above the threshold (&gt; 13.1V)</li> <li>• <b>Battery charger fault:</b> send a message when the "Iares 4.0" control panel or the "Opis" power supply station fails to supply the necessary current to the system.</li> <li>• <b>Restored battery charger:</b> send a message when the power supply of "Iares 4.0" or the "Opis" power supply station returns to normal operation or it is replaced.</li> <li>• <b>Fuse fault:</b> send a message when the fuse on the "Iares 4.0" control panel or the "Opis" power supply station goes into operation (e.g. due to a short circuit).</li> <li>• <b>Restored fuse:</b> send a message when the fuse on the "Iares 4.0" control panel or the "Opis" power supply station resets its fuse operating condition.</li> </ul> <p>Note: if the CPU window appears in the entity window, the events that generate the communication refer to the "Iares 4.0" panel.</p> <p>Type: <b>Remote control</b> The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Disarm button:</b> send a message by pressing the disarm button on the remote control (short pressing).</li> <li>• <b>Stay arm button:</b> send a message by pressing the partial button on the remote control (short pressing).</li> <li>• <b>Away arm button:</b> send a message by pressing the Total button on the remote control (short pressing).</li> <li>• <b>Long press disarm button:</b> send a message by pressing the switch-off button on the remote control (long pressing).</li> <li>• <b>Long press stay arm button:</b> send a message by pressing the Partial button on the remote control (long pressing).</li> <li>• <b>Long press away arm button:</b> send a message by pressing the Total button on the remote control (long pressing).</li> <li>• <b>Long press info button:</b> send a message by pressing the (i) button on the remote control (long pressing).</li> <li>• <b>Press Panic/SOS button:</b> send a message when any key of the remote control will be pressed.</li> </ul> <p>Type: <b>User</b> The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Recognized PIN code:</b> send a message when a code is recognized. Valid option for codes entered on the keypad or APP.</li> <li>• <b>Recognized tag:</b> send a message approaching a Key enabled to the reader (keypad or volo/volo-IN).</li> </ul>
--	---

	<p>Type: <b>System</b></p> <p>The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Tamper</b>: send a message when a tamper condition occurs in the metal box of the control panel (opening and/or detachment from the wall) detected through the switches connected to the T connector of the "lares" card.</li> <li>• <b>Tamper restore</b>: send a message when the tamper condition of the control panel box is reset</li> <li>• <b>Start maintenance</b>: send a message when a new configuration is applied.</li> <li>• <b>End maintenance</b>: send a message when parameter programming, via portal or installer app, is completed</li> <li>• <b>Periodic report</b>: send a message based on a scheduled periodic event (test event).</li> <li>• <b>Wrong PIN</b>: send a message after three incorrect codes have been entered on the keypad. After four incorrect codes, the keypad is blocked for (90s.).</li> <li>• <b>Recognized installer PIN</b>: send a message when the installer PIN code is recognized.</li> <li>• <b>Panel shutdown</b>: send a message when a system shutdown event occurs (230V power is off and the battery is discharged). In this case we should preserve the battery from total discharge.</li> <li>• <b>Panel reset</b>: send a message when the control panel has restarted because the power has been lost and subsequently restored or due to a system fault or due to a firmware update.</li> <li>• <b>Lost ethernet connection</b>: send a message when the Ethernet cable is disconnected (or when the router/switch is turned off).</li> <li>• <b>Restore ethernet connection</b>: send a message when the Ethernet cable is reconnected (or when the router/switch is turned on).</li> <li>• <b>PSTN fault</b>: send a message when the telephone line is removed from the PSTN module (cable cut or line failure).</li> <li>• <b>Restore PSTN</b>: send a message when the telephone line on the PSTN module is restored.</li> <li>• <b>GSM network fault</b>: send a message when the GSM network is missing (no signal, GSM repeater malfunctioned or switched off for maintenance, SIM disabled and no longer registered on the network of the mobile operator).</li> <li>• <b>GSM network restore</b>: send a message when the GSM network is restored.</li> <li>• <b>Remote supervision fault</b>: send a message when the IP receiver fails to send supervision.</li> <li>• <b>Restored supervision</b>: send a message when the IP receiver responds to supervision packets.</li> <li>• <b>Jamming wireless</b>: send a message when the wireless receiver of the panel or one of the two-way transceivers detect a disturbance on the 868Mhz frequency.</li> <li>• <b>Restore jamming wireless</b>: send a message when the noise on the 868MHz frequency, detected by the wireless receiver of the control panel or one of the two-way transceivers, ceases to exist.</li> <li>• <b>Network from LAN to Mobile</b>: send a message when a data transfer from LAN to Mobile takes place.</li> <li>• <b>Network from Mobile to LAN</b>: send a message when a data transfer from Mobile to LAN takes place.</li> <li>• <b>Missing Internet</b>: send a message when the Internet network is missed</li> <li>• <b>Restore Internet</b>: send a message when the Internet network is restored.</li> <li>• <b>Duress code</b>: send a message when a duress code is recognised.</li> </ul>
--	--

	<p>Type: <b>Programmable logic</b> The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Programmable:</b> send a message when the programmable logic is realized.</li> </ul> <p>Type: <b>Smart Home</b> The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Lux sensor activation:</b> send a message when the twilight threshold, configured for the domus multifunction sensor, exceeds (more or less) (the event generation will consider a hysteresis equal to 5%).</li> <li>• <b>Lux sensor deactivation:</b> send a message when the brightness values detected by the domus are within the configured twilight threshold.</li> <li>• <b>Wet environment:</b> send a message when the Wet threshold, configured for the domus multifunction sensor, exceeds (more or less) (the event generation will consider a hysteresis equal to 2%).</li> <li>• <b>Dry environment:</b> send a message when the dry values detected by the domus are within the configured dry threshold.</li> </ul> <p>Type: <b>Load management</b> The subtypes available are:</p> <ul style="list-style-type: none"> <li>• <b>Excess power consumption:</b> send a message upon exceeding the "Consumption threshold" configured in "Consumption management".</li> <li>• <b>Normal power consumption:</b> send a message when the consumption falls below the thresholds configured in "Consumption management".</li> <li>• <b>Load disconnection risk:</b> send a message upon exceeding the "Disconnection threshold" configured in "Consumption management".</li> <li>• <b>End risk of load disconnection:</b> send a message when the disconnection risk falls below the "Disconnection threshold" configured in "Consumption management".</li> </ul>
--	--



### 3.10 Scheduler timers

The Time Scheduler allows the planning of automatic processes, represented by pre-programmed scenarios, which can be executed according to scheduled timetable and weekdays. The weekdays can be distinguished from the holidays so that, a disarm time scheduler programmed every day at 07:00am (for example) will not take place if a holiday falls on a weekday. The maximum configuration number of Time Schedulers depends on the Iares 4.0 control panel models.

<b>Enable</b>	Enable/disable the Time scheduler.
<b>Description</b>	Give a name to the Time scheduler.
<b>Partitions</b>	From the list, select one or more partitions previously programmed.
<b>Scenarios</b>	From the list, select a scenario to start, among those previously programmed.
<b>Type of start time</b>	Select one of the options offered, mutually exclusive: - <b>Time</b> : in the next field, enter hour and minutes to start the time scheduler. - <b>Sunrise</b> : the time scheduler will start at sunrise, according to the values configured in the Options-> General menu. - <b>Sunset</b> : the time scheduler will start at sunset, according to the values configured in in the Options-> General menu.
<b>Hour</b>	The field is visible if "Type of start time" = Time Click the icon to program hour and minutes to start the Time scheduler.
<b>MON...SUN</b>	Choose the weekdays to repeat the scenario.
<b>Exclude holiday</b>	Exclude/include the holidays calendar. Click the icon to open the list of holidays of the country in which the control panel is installed. The Country must be configured in the page <Settings -> General options-> Section Holidays>.

### 3.11 Chronothermostats

In this page the "heating" and "cooling" outputs of the domus multifunction sensor are customized. This configuration will allow the user, via the APP Iares 4.0, to be able to configure his own chronothermostat (heating, air conditioning, schedules, weekly programs, etc.).

<b>Description</b>	Give a name to the chronothermostat.
<b>Select peripheral</b>	Link the chronothermostat to the domus sensor, previously programmed.
<b>Heating output</b>	Outputs available are: <ul style="list-style-type: none"> <li>• <b>Thermoregulation</b></li> <li>• <b>Test</b></li> <li>• <b>Heating</b></li> <li>• <b>Conditioning</b></li> </ul>

<b>Cooling output</b>	Outputs available are: <ul style="list-style-type: none"> <li>• <b>Thermoregulation</b></li> <li>• <b>Test</b></li> <li>• <b>Heating</b></li> <li>• <b>Conditioning</b></li> </ul>
<b>Hysteresis</b>	Thermal hysteresis: (min 0.1, max 1.0, step 0.1)°C (default 0.3°C)

### 3.12 Consumption management

Once **energia** peripheral BUS has been configured, the configuration of the "meters" is required to control the power in real time, resulting from the difference between the power produced and the power absorbed measured by even multiple **energia** devices. The meter is associated with partitions and rooms for a correct display on the user APP and on the graphic maps.

The value of the power in real time is displayed for each meter with the following dynamic icons:



green = no consumption or positive value between power produced (i.e. photovoltaic) and absorbed.



blue = consumption below the programmed consumption and disconnection thresholds



orange = power consumption threshold exceeded



dark red = disconnection threshold exceeded, load disconnection risk

The same value is visible even in the lares 4.0 user APP, section Smart Home -> Consumption Management or in the room associated with the device.

<b>Description</b>	Give a name to the meter.
<b>Partitions</b>	Click on the arrow next to the field to open the menu with the list of partitions previously programmed, to be associated with the meter. It is possible to associate one or more partitions to the same meter.
<b>Rooms</b>	Click on the arrow next to the field to open the menu with the list of rooms previously programmed, to be associated with the meter. It is possible to associate one or more rooms to the same meter.
<b>Power absorbed</b>	Click on the arrow next to the field to open the menu with the list of measure lines, made available by previously programmed energia devices. Their total power value will be subtracted from the produced power value. Multiple measure lines can be configured.

<b>Power produced</b>	Click on the arrow next to the field to open the menu with the list of measure lines, made available by previously programmed energia devices. Their total power value will be added to the absorbed power value. Multiple measure lines can be configured.
<b>Loads management</b>	
<b>Consumption threshold</b>	Threshold limit value of power consumption expressed in Watts, beyond this value an alert is generated (default 3000 Watt)
<b>Disconnection management</b>	Enables/disables the loads disconnection management, the procedure according to which, upon exceeding the consumption threshold limit value, the loads disconnection starts according to the configuration of the following fields.
<b>Disconnection threshold</b>	Threshold limit value of power consumption expressed in Watts (greater than "Consumption threshold"), beyond this value the loads disconnection starts (default 3300 Watt)
<b>Disconnection delay timer</b>	Loads disconnection delay timer, expressed in minutes. Possible values: 1...60 min. (default 2 min.)
<b>Outputs list</b>	Enter the "Manageable load" outputs to be considered in the disconnection sequence, according to the control panel model, the maximum number of outputs changes.

### 3.13 Services

#### 3.13.1 Konnex

porta 4.0 KNX gateway is an IP interface placed between KNX devices world and lares 4.0 control panel, for integrate its functionalities.

It is required the configuration of:

- datagrams that come from the KNX world through port 4.0, against which to execute commands towards the lares 4.0 control panel;
- datagrams that come from lares 4.0 control panel towards the KNX world, through port 4.0, due to status changes.

From porta 4.0 towards lares 4.0, it is possible to manage the following commands:

- arming/disarming partitions;
- activation scenarios;
- bypass/unbypass zones;
- turn on/turn off outputs.

<b>Konnex Address</b>	Enter the porta 4.0 address on Konnex BUS
<b>Partition</b>	Choose a partition from the list
<b>Commands:</b>	You can configure datagrams to execute commands for the selected partition

Instant Arm	<p>Enter the group address (which represents all the KNX devices involved in this function), the format is: x/y/z (e.g. 1/1/1). Possible values (3-level structure): main(x)= 0..31, middle(y)= 0..7, sub(z)= 0..255. Press &lt;Enter&gt; to confirm.</p> <p>Button 1 enabled (default) = the command received is executed with value 1 (ON); Button 0 enabled = the command received is executed with value 0 (OFF).</p> <p>Check the box preceding the group address and click on the red bin, to delete it.</p> <p>Possibility to configure up to 5 group addresses each partition.</p>
Delayed Arm	<p>Enter the group address (which represents all the KNX devices involved in this function), the format is: x/y/z (e.g. 1/1/1). Possible values (3-level structure): main(x)= 0..31, middle(y)= 0..7, sub(z)= 0..255. Press &lt;Enter&gt; to confirm.</p> <p>Button 1 enabled (default) = the command received is executed with value 1(ON); Button 0 enabled = the command received is executed with value 0 (OFF).</p> <p>Check the box preceding the group address and click on the red bin, to delete it.</p> <p>Possibility to configure up to 5 group addresses each partition.</p>
Disarm	<p>Enter the group address (which represents all the KNX devices involved in this function), the format is: x/y/z (e.g. 1/1/1). Possible values (3-level structure): main(x)= 0..31, middle(y)= 0..7, sub(z)= 0..255. Press &lt;Enter&gt; to confirm.</p> <p>Button 1 enabled (default) = the command received is executed with value 1 (ON); Button 0 enabled = the command received is executed with value 0 (OFF).</p> <p>Check the box preceding the group address and click on the red bin, to delete it.</p> <p>Possibility to configure up to 5 group addresses each partition.</p>
<b>Status:</b>	<p>You can define which datagrams will be sent, following the status changes for the selected partition.</p>

Armed delayed	<p>Enter the group address (which represents all the KNX devices involved in this function), the format is: x/y/z (e.g. 1/1/1). Possible values (3-level structure): main(x)= 0..31, middle(y)= 0..7, sub(z)= 0..255.</p> <p>Invert = OFF (default) the status change is sent with a non-inverted value, with respect to the programmed one; Invert = ON the status change is sent with an inverted value, with respect to the programmed one.</p> <p>Notes: a) At armed delayed, together with the "armed delayed" status, also the "armed instant" status is sent, but with an inverted value, with respect to the programmed one. b) At disarming, the "armed delayed" status and the "armed instant" status are sent with an inverted value, with respect to the programmed one.</p>
Armed Instant	<p>Enter the group address (which represents all the KNX devices involved in this function), the format is: x/y/z (e.g. 1/1/1). Possible values (3-level structure): main(x)= 0..31, middle(y)= 0..7, sub(z)= 0..255.</p> <p>Invert = OFF (default) the status change is sent with a non-inverted value, with respect to the programmed one; Invert = ON the status change is sent with an inverted value, with respect to the programmed one.</p> <p>Notes: a) At armed instant, together with the "armed instant", also the "armed delayed" status is sent, but with an inverted value, with respect to the programmed one. b) At disarming, the "armed instant" status and the "armed delayed" status are sent with an inverted value, with respect to the programmed one.</p>
Alarm	<p>Enter the group address (which represents all the KNX devices involved in this function), the format is: x/y/z (e.g. 1/1/1). Possible values (3-level structure): main(x)= 0..31, middle(y)= 0..7, sub(z)= 0..255.</p> <p>Invert = OFF (default) the status change is sent with a non-inverted value, with respect to the programmed one; Invert = ON the status change is sent with an inverted value, with respect to the programmed one.</p> <p>Note: When the partition returns to rest, the datagram will be sent with an inverted value, with respect to the programmed one.</p>

<p>Tamper</p>	<p>Enter the group address (which represents all the KNX devices involved in this function), the format is: x/y/z (e.g. 1/1/1). Possible values (3-level structure): main(x)= 0..31, middle(y)= 0..7, sub(z)= 0..255.</p> <p>Invert = OFF (default) the status change is sent with a non-inverted value, with respect to the programmed one; Invert = ON the status change is sent with an inverted value, with respect to the programmed one.</p> <p><b>Note:</b> When the partition returns to rest, the datagram will be sent with an inverted value, with respect to the programmed one.</p>
---------------	--

<p><b>Scenario</b></p>	<p>Select a scenario from the list.</p>
<p><b>Commands:</b></p>	<p>You can configure datagrams to execute the selected scenario.</p>
<p>Execute</p>	<p>Enter the group address (which represents all the KNX devices involved in this function), the format is: x/y/z (e.g. 1/1/1). Possible values (3-level structure): main(x)= 0..31, middle(y)= 0..7, sub(z)= 0..255. Press &lt;Enter&gt; to confirm.</p> <p>Button 1 enabled (default) = the command received is executed with value 1 (ON); Button 0 enabled = the command received is executed with value 0 (OFF).</p> <p>Check the box preceding the group address and click on the red bin, to delete it.</p> <p>Possibility to configure up to 5 group addresses each scenario.</p>

<b>Zone</b>	Select a zone from the list.
<b>Commands:</b>	You can configure datagrams to execute commands for bypass or include the selected zone.
Bypass/Unbypass	<p>Enter the group address (which represents all the KNX devices involved in this function), the format is: x/y/z (e.g. 1/1/1). Possible values (3-level structure): main(x)= 0..31, middle(y)= 0..7, sub(z)= 0..255. Press &lt;Enter&gt; to confirm.</p> <p>Invert = OFF (default) the command received is executed with a non-inverted value: upon receipt of value 1 it commands "bypass", upon receipt of value 0 it commands "unbypass"; Invert = ON the command received is executed with an inverted value: upon receipt of value 1 it commands "unbypass", upon receipt of value 0 it commands "bypass".</p> <p>Check the box preceding the group address and click on the red bin, to delete it.</p> <p>Possibility to configure up to 5 group addresses each scenario.</p>
<b>Status:</b>	You can define which datagrams will be sent following the status change for the selected zone.
Real time	<p>Enter the group address (which represents all the KNX devices involved in this function), the format is: x/y/z (e.g. 1/1/1). Possible values (3-level structure): main(x)= 0..31, middle(y)= 0..7, sub(z)= 0..255.</p> <p>Invert = OFF (default) the status change is sent with a non-inverted value; Invert = ON the status change is sent with an inverted value.</p> <p>Note: The programmed datagram is sent when the "real time" status changes, whether the zone is in alarm or not. When the zone returns to rest, the "real time" status is sent with an inverted value, with respect to the programmed one.</p>
Alarm cycle	<p>Enter the group address (which represents all the KNX devices involved in this function), the format is: x/y/z (e.g. 1/1/1). Possible values (3-level structure): main(x)= 0..31, middle(y)= 0..7, sub(z)= 0..255.</p> <p>Invert = OFF (default) the status change is sent with a non-inverted value; Invert = ON the status change is sent with an inverted value.</p> <p>Note: The programmed datagram is sent when the "alarm cycle" status changes. When the alarm cycle stops, the programmed datagram is sent inverted.</p>

<b>Output</b>	Select an output from the list.
<b>Commands:</b>	You can configure datagrams to execute commands to turn on or turn off the selected output.
On/Off	<p>Enter the group address (which represents all the KNX devices involved in this function), the format is: x/y/z (e.g. 1/1/1). Possible values (3-level structure): main(x)= 0..31, middle(y)= 0..7, sub(z)= 0..255. Press &lt;Enter&gt; to confirm</p> <p>Invert = OFF (default) the command received is executed with a non-inverted value: upon receipt of value 1, it commands "ON", upon receipt of value 0, it commands "OFF"; Invert = ON the command received is executed with an inverted value: upon receipt of value 1, it commands "OFF", upon receipt of value 0, it commands "ON".</p> <p>Check the box preceding the group address and click on the red bin, to delete it.</p> <p>Possibility to configure up to 5 group addresses each scenario.</p>
<b>Status:</b>	You can define which datagrams will be sent following the status change for the selected output.
Real time	<p>Enter the group address (which represents all the KNX devices involved in this function), the format is: x/y/z (e.g. 1/1/1). Possible values (3-level structure): main(x)= 0..31, middle(y)= 0..7, sub(z)= 0..255.</p> <p>Invert = OFF (default) the status change is sent with a non-inverted value: if the output turns ON, "1" is sent, otherwise "0" is sent; Invert = ON the status change is sent with an inverted value: if the output turns on, "0" is sent, otherwise "1" is sent.</p>



---

### 3.13.2 Gateway HTTP

---

Gateway http service consists of the Http/s messages configuration that lares 4.0 and third party devices connected, exchange through the configured device (porta IoT, porta 4.0).

Gateway http service requirements:

- register control panel on Ksenia SecureWeb cloud;
- launch Installer from Ksenia SecureWeb;
- the first time you enter the page, activate Gateway http service by clicking on <PURCHASE THE SERVICE> button.

Follow the steps described below for programming Gateway http service:

1. enter the authentication data of the configured device (e.g. porta IoT) toward the devices connected, as: enable/disable secure connection, a specific token for the APIs, to be copied into the device for its integration security;
2. add the devices (IP cameras, IoT devices, PC, etc.), their IP address and the type of authentication, click on Add icon ("+" red button);
3. add actions/requests (GET, POST, PUT, DELETE method), the URL (URLs are how you identify the things that you want to operate on) and the body (JSON) when required, to be sent to each device, as required by the device itself to be controlled, which follow the actions of event/scenario programmed in the control panel. Click on '+' blue button to add more actions.




---

### 3.14 Settings

---

The "Options" submenus allow you to configure some basic features regarding the **General** data of the lares 4.0 control panel (date, time, language, etc.), related data to the **Network** and the **GSM / PSTN Communicator**.



### 3.14.1 General options

<b>Session System language</b>	
<b>Language used by panel</b>	Allows you to change the language in the control panel, select a language from those included in the drop-down menu.
<b>Session Wireless</b>	
<b>On-board transceiver</b>	Enable/disable the on-board wireless receiver. (Not available on lares 4.0 - 16 and lares 4.0 - 40 that need the DUO transceiver).
<b>Jamming threshold (dBm)</b>	Noise power threshold present on the radio channel beyond which a sabotage attempt is made.
<b>Session Arming</b> In this section you can select how to manage the arming and possibly prevent them in the event of a failure. Alarm and fault signals are also managed.	
<b>Tamper time cycle (min)</b>	Time (expressed in minutes) that determines the maximum duration of the sabotage cycle.
<b>Throw alarms each zone cycle</b>	By default, the control panel generates the 'Zone alarm' event and the associated associated actions (i.e. SMS, phone calls, etc.) whenever a zone is violated. Selecting this option, if the zone event is repeated several times during the same alarm cycle, the relative actions are performed only the first time.
<b>Bypass also zone tamper</b>	When a zone is excluded if it is tampered with and if this option is enabled, no tampering reports will be generated. Tampering will not be recorded in the event log and will not be displayed on the keyboard or web server.  <b>Note:</b> if the "Bypass also zone tamper" option is enabled, the IMQ-SECURITY SYSTEMS certification is no longer valid.
<b>Allow system arm on fault condition</b>	By default the control panel DOES NOT allow the system to be inserted in the presence of faults and / or sabotages. Selecting this option it will be possible to insert the partitions in the presence of faults in progress.  <b>Note:</b> if the "Allow system arm on fault condition" option is enabled, the IMQ-SECURITY SYSTEMS certification is no longer valid.
<b>Delete alarm memory when arming</b>	When an entry occurs, the alarm memories will be deleted, that is they will no longer be displayed on the keypads.
<b>Clear tamper memory with user code</b>	Selecting this option it will be possible to use the user code to cancel the sabotage memories displayed on the keyboard (main menu / Reset alarms).
<b>Manage missing peripheral as fault</b>	If a BUS or wireless device no longer communicates with the control panel, because it is faulty or disconnected, the related fault event will be generated.  <b>Note:</b> if the "Manage missing peripheral as fault" option is enabled, the IMQ-SECURITY SYSTEMS certification is no longer valid.
<b>Limit log event number per event</b>	If enabled, the recording of the same event is limited to 8. The counter resets on arming / disarming.

<b>Session System</b>	
<b>Voice menu via GSM</b>	Enable/disable the voice menu playback on GSM network
<b>Voice menu via PSTN</b>	Enable/disable the voice menu playback on PSTN network
<b>Hide calls</b>	Enable/disable the "Call in progress" message on ergo, ergo S and ergo M keypads display, with an alarm in progress (default: disable).
<b>Session Date and time</b>	
<b>Time shift</b>	Setting of the daylight saving time or the standard time (read only).
<b>Date format</b>	Change the format used to display the time on the keypads (not on the ergo T).
<b>Time format</b>	Change the time format in 24h or 12h.
<b>Time zone</b>	Allows to set the time zone to 15, 30 and 45 minutes in addition to the whole hour.
<b>Offset sunrise</b>	Enter the minutes (+/- 30) to add/subtract from sunrise time, in order to balance a particular position where the control panel is installed, with respect to the horizon (e.g. presence of mountains). The sunrise time calculation is based on the geographical coordinates of the control panel, received from cloud after Ksenia PRO registration or entered manually in the Ksenia SecureWeb platform. The field is editable if the control unit coordinates are different from 0°, 0°, therefore received from cloud.
<b>Offset sunset</b>	Enter the minutes (+/- 30) to add/subtract from sunset time, in order to balance a particular position where the control panel is installed, with respect to the horizon (e.g. presence of mountains). The sunset time calculation is based on the geographical coordinates of the control panel, received from cloud after Ksenia PRO registration or entered manually in the Ksenia SecureWeb platform. The field is editable if the control unit coordinates are different from 0°, 0°, therefore received from cloud.
<b>Holidays</b>	
<b>Country</b>	To load the holidays calendar (valid until 2039) of the country in which the control panel is installed, select the country of interest from the drop down menu. To know more details about the holidays, click the icon to open the popover with date and description (e.g. Easter - 04/04/2021).
<b>Session Voice messages</b>	
<b>Header</b>	Enter the header of the system in this field (i.e. Smith Family, address ...). This message will be generated by the speech synthesis, it will identify the system and will be the first to be reproduced (i.e. header/alarm zone/zone 1).
<b>Session Account</b>	
<b>Weak PIN</b>	Select this option to disable the control about the robustness of the PINs by the control panel, to prevent the insertion of easily identifiable PINs (i.e. birth dates, etc.).
<b>Confirm scenario execution</b>	Enable to confirm every time the scenario chosen from the keypad, by entering your PIN.

<b>Session Faults</b>	
In this section it is possible to select which faults must be ignored by the control panel if there are permanent fault conditions that you do not wish to display (example: Ethernet connection missing). They are all enabled by default.	
<b>Fault memory</b>	By selecting this option, the control panel will show on the keypad display that a fault has been reset ("Fault Memory"). This memory will be deleted only after a check in the "Failure status" section, by an authorized user.
<b>Mains fault</b>	It signals a power supply fault to the control panel or to the "opis" power station.
<b>Low power supply voltage</b>	It signals a low power supply voltage.
<b>Battery charger</b>	It signals when the power supply fails and fails to supply the necessary current to the system.
<b>Fuse</b>	It signals that one of the fuses (i.e. short circuit) has blown on the mother board or on board of the "opis" power station.
<b>Low battery</b>	It occurs when the voltage of the battery and wireless devices drops below the minimum operating threshold.
<b>Battery fault</b>	It occurs when the control panel, the external/internal sirens, the "opis" power station fail the dynamic battery test. For wireless devices it occurs when their batteries are running out.
<b>Missing BUS peripheral</b>	The fault event will be generated when one or more peripherals are no longer in communication with the BUS.
<b>Missing wireless peripheral</b>	The fault event will be generated when wireless devices are not communicating with the control panel, once the supervision time has elapsed.
<b>Zone fault</b>	It occurs when an balanced detector generates the masking event. This event will also be generated when the partition assigned to the zone has been disarmed and the zone itself has never been violated for any programmed period of inactivity (expressed in minutes).
<b>Ethernet connection missing</b>	It signals the disconnection of the ethernet cable from the router/switch. The connection with the "DNS" or "Cloud" server may still be active (GPRS connection).
<b>Internet connection missing</b>	This signals a lack of Internet connectivity, despite the integrity of the wiring and the functioning of the Ethernet connection.
<b>PSTN fault</b>	It signals that the PSTN module cannot detect the telephone line any more.
<b>GSM fault/Missing signal</b>	It signals that the SIM card is not functioning correctly (SIM has expired and been disabled) or the GSM signal is not present.
<b>Communication fault</b>	It signals that the call has been unsuccessful.
<b>SIA IP supervision fault</b>	It occurs when the control panel no longer communicates with the SIA IP server.
<b>System fault</b>	It occurs when a system error forces the control panel to be reset.


Pre-alarms management	
<b>Number of pre-alarms</b>	Maximum number of pre-alarms before triggering an alarm. Default value: 2, Possible value: 2...5.
<b>Timer for alarm confirmation</b>	Timer for alarm confirmation within which a number of pre-alarms equal to the one set in previous field ("Number of pre-alarms") are verified. If the number of pre-alarms is reached within the expiration of this timer an alarm will occur, otherwise not. Default value: 30 sec., Possible values: 1..300 sec.
<b>Same partition</b>	- If enabled and a zone on partition X is in pre-alarm, the counter will be increased only by pre-alarms from zones that belong to the same partition X; - if disabled (default) and a zone on partition X is in pre-alarm, a further pre-alarm from any zone on any partition will help to increase the counter.
<b>Confirmation from different zones only</b>	Indicate if incrementing the number of pre-alarms within the timer for alarm confirmation only if the pre-alarms come from different zones or from the same zone too. Default value: disabled (pre-alarms can also come from the same zone). If enabled, the pre-alarms must necessarily come from other zones than those already in pre-alarm.


Session Power supply	
<b>Mains fault delay (min.)</b>	This is the time (expressed in minutes) which identifies the delay for which the reports will be sent once this event occurs "220V network is missing". The fault message will appear immediately if set to zero.  <b>Note:</b> In order to maintain compatibility with the EN-50131 standard this value should be set to 1 minute.
<b>Max charge supply battery (mA)</b>	Maximum current supplied by the control panel to charge the battery. In case of under-sizing of the power supply it is possible to reduce the charging current, extending the recharge time of the battery.  <b>Note:</b> In order to maintain compatibility with the EN-50131 standard this value can not be less than 200mA for 2Ah batteries, 400mA for 7Ah batteries, 800mA for 17Ah batteries.
Session Periodic test	
<b>Enable</b>	Enable/disable the periodic test (it is possible to associate the "periodic test" to an event and subsequently to a "notification").
<b>Start date and time</b>	Date and time test start. Format: DD / MM / YYYY hh mm
<b>Periodicity</b>	Possible values: from 1 to 400. Choose the unit of measure in the next field (minutes, hours or days).
<b>Unit of measure</b>	Select from the drop-down menu: Minutes, Hours or Days

### 3.14.2 Network

Network setting of lares 4.0 control panel.

Session Ethernet	
<b>DHCP</b>	If enabled, it allows the control panel to connect to a local network to automatically configure the necessary parameters. If it is not enabled, all the network parameters must be entered manually.

Session Web Server	
<b>Protocol</b>	Enable / disable the encryption protocol (TLS) used to connect to the control panel via webserver.
<b>Port</b>	Set the listening port (443 = TLS active / 80 = TLS inactive).
 <p>Unless strictly necessary, it is recommended not to change these parameters. In this case, contact your network administrator.</p>	

Session NTP	
<b>Enabled</b>	<p>Enable or disable the connection to the NTP (Network Time Protocol) server. Allows you to keep the system clock automatically updated. By enabling this option it will be possible to modify the parameters, if necessary:</p> <ol style="list-style-type: none"> <li>1. <b>Server name:</b> it is the server used by the control panel to synchronize the time.</li> <li>2. <b>Port:</b> the port on which the NTP protocol data are transmitted</li> <li>3. <b>Request interval (sec):</b> it is the time interval that elapses between one communication and the other (control panel &lt;-&gt; NTP server)</li> <li>4. <b>Request interval after an error:</b> it is the time interval between a communication and the next one in case of error</li> </ol> <p> Unless strictly necessary, it is recommended not to change these parameters.</p>

**Session SMTP**

Enable the SMTP server configuration that allows the control panel to send e-mails.

The parameters required for sending e-mails are the following.

**(Those that appear by default are not valid!)**


The lares 4.0 platform can also manage e-mail addresses using SSL or TLS protocols (i.e. gmail).

Otherwise, you can create a host on [www.kseniadns.com](http://www.kseniadns.com) and use the same settings.


<b>Sender</b>	In this section the name of the sender must be programmed (example: Alarm panel). However, some servers may require you to enter a valid e-mail address (servers that do not require authentication). If "Kseniadns" server settings are used, the sender will for example be: (xxxxxx@kseniadns.com).
<b>Protocol</b>	Select SSL or TLS or none. Refer to the parameters of the server used. (SSL if kseniadns is used).
<b>Port</b>	Protocol communication port. Refer to the parameters of the server used. (465 if kseniadns is used).
<b>Username</b>	Username used for the SMTP service. For server settings "Kseniadns" : if the hostname is mariorossi.kseniadns.com, the username will be mariorossi@kseniadns.com).
<b>Password</b>	Password used for the SMTP service. For server settings "Kseniadns": it is the password chosen during host creation (default 123456).
<b>Mail subject</b>	Description of the subject that must appear in the emails to be sent.

**Session DDNS**

<b>Enabled</b>	Enable or disable synchronization with a DDNS server to resolve a dynamic public IP address.
<b>DynDns server name or address</b>	kseniadns.com or Porta DynDns: 80
<b>Host nome</b>	username.kseniadns.com (example: mariorossi.kseniadns.com)
<b>Username</b>	configure username of DDNS account DDNS (example: mariorossi)
<b>Password</b>	configure password of DDNS account
<b>CheckIP server name or address</b>	checkip.kseniadns.com
<b>CheckIP port</b>	80
It is also possible to use a third-party DDNS server by properly configuring the fields listed above.	

<b>Session SecureWeb</b>	
<b>Enabled</b>	Enable/disable the connection to the SecureWeb server.
 <p>By disabling this option, it will no longer be possible to connect to the control panel via the APP (SecureWeb) and via the configuration portal! Only the local peer to peer or remote connection will be possible via public IP address or DDNS and it will be necessary to map the ports on the router to the control panel and any IP cameras connected to the system. It will be possible to use the APP Iares 4.0 only in local or remote connection (via public IP or DDNS) but the possibility of receiving PUSH notifications will be excluded.</p>	

### 3.14.3 GSM/GPRS/PSTN Communicator

<b>Session General</b>	
<b>Numbers of attempts</b>	It represents the number of call attempts that the device makes on each configured number before the failed communication event is generated (even if the confirmation is not received).
<b>Number of message repetition</b>	It indicates the number of repetitions of a voice message during the same call.
<b>Confirm request</b>	If enabled, it will be necessary to confirm receipt of the call by pressing the button (*) on the receiving telephone. Otherwise the device will consider the call as failed and proceed with the next number among those configured.
<b>Call all numbers</b>	If enabled, the voice messages will be sent to all the configured numbers. The call sequence will stop only when all the numbers in the list will answer the call. If disabled, the telephone queue will be interrupted and canceled following the first confirmation by any of the users.
 <p>Answers from any answering machines/fax/etc. will be considered also valid.</p>	

<b>Session GSM</b>	
<b>Mobile data</b>	Enable/disable data traffic on GSM/GPRS. Used to manage the system in case of absence of ADSL/Fiber line. It can also be used as an automatic fixed line backup.
<b>APN</b>	Access Point Name for connecting the central panel to GPRS/3G/4G network.
<b>User</b>	If required, enter the user name to connect to the APN.
<b>Password</b>	If required, enter the password to connect to the APN.






**For GPRS / 3G / 4G parameters, contact your mobile service provider.**



**Note:** Classification according to EN50136-2, SP2 - SP4. Environmental class II.  
The device can be programmed to send the following communications: pre-recorded voice messages, SMS, contact ID with SIA-DC03 protocol, signaling via GPRS with SIA-DC03 protocol with encryption.

Session PSTN	
<b>Rings</b>	Enter the number of rings
<b>Disable tone check</b>	Disable the search for telephone tones (free, busy, congestion, etc.)
<b>Bypass answering machine</b>	Bypass the answering machines.
 <b>Note:</b> Classification according to EN50136-2, SP2. Environmental class II. The device can be programmed to send the following communications: pre-recorded voice messages, SMS, contact ID with SIA-DC03 protocol, signaling via GPRS with SIA-DC03 protocol with encryption.	

### 3.15 Voice messages

From the Web Server installer 1.5.1 version it is possible to generate voice messages even in local connection with the control panel, which is not feasible with the previous versions that required Online connection with the Secureweb portal.

If you already have a Loquendo USB key, just add some files by downloading them from the reserved area in compressed format (Update Loquendo\_lares4.zip).

Once the file has been downloaded, it must be decompressed on the main root of the USB key: at this point the key is ready for use with Lares 4.0 and this operation must not be repeated again.

#### 3.15.1 Play

The main window displays the voice messages generated and subdivided into sub-categories (events, zones, partitions, etc.).



= voice message available for download.



= voice message downloaded and ready to be listened to.

### 3.15.2 Generate

- To generate voice messages via an online connection through the Secureweb portal, you must have an activated Loquendo license, provided on a scratch card (purchased separately "one-off").
- To generate voice messages in the peer-to-peer mode with the control panel, you must perform the following steps instead:
  1. Access the control panel with a local connection (refer to the manual supplied with the product), in the unencrypted mode (so in http instead of https). To change the default setting, you need to access the control panel configuration, and in Section "Options" "Network" then in section "Web Server" and under "Protocol" select the "None" Mode (port 80).
  2. Exit the internet browser.
  3. Connect the USB key to the PC, turning off the firewall that may prevent communication with the USB key
  4. Open the file folder on the USB key and previously extracted from the .zip file. Manually start the server by double-clicking the executable lares-4-win in Windows or lares-4- mac on MAC.
  5. Log in to the control panel with a local connection again.
  6. In the voice messages section there is the menu section for voice message generation.
  7. At the end of the voice messages generation, if desired, it is possible to restore the connection to the encrypted mode.

The system header is set to "Options" "Voice Messages".

At this point we can find two states:



The programming could be changed, regenerate the messages.

The message above appears when the messages have been created or previously created but in the meantime configuration has been changed.

To generate voice messages:

1. select a voice (requires a Loquendo license).




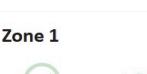
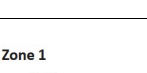

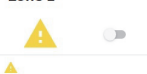

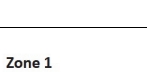
2. click on (  )





The message "Congratulations, all the voice messages are aligned" appears when all the messages will has been generated correctly. You cannot generate them again unless you make some configuration changes (zones, partitions, etc.)



### 3.16 Real time

Possibility to display in real time the status of the zones, outputs and partitions programmed in the system, by means of easy-to-understand icons. The following table lists and describes the icons that appear in relation to the possible states that can be controlled by the control panel.






If necessary, the statuses can be modified using the command key highlighted in the table.

Real time submenu	Icon	Description	Commands
Zones		Zone in idle and included	 = excluded  = included
		Zone excluded (the status icon becomes transparent)	
		Zone alarmed	
		Zone in tamper and tamper alarm in progress	
		Zone in tamper and tamper alarm memory.	
		Zone fault (i.e. masking) and fault alarm in progress.	
		Zone in idle and fault memory	

Outputs	<div>Output 1</div> <div> </div>	Output ON
	<div>Output 1</div> <div> </div>	Output OFF

 = ON  
 = OFF

**Note:** if the output has been programmed with the "not visible" attribute or "not managed (local)" attribute, it will not be possible to activate or deactivate it.

Partitions		Partition disarmed	
		Partition arming in progress and exit delay timer countdown	
		Partition arming in progress and entry delay timer countdown	
		Partition armed (after exit delay timer or immediately)	
		Partition armed and alarm in progress	

### 3.17 Event log

The page displays the event logs of the control panel in a variable number, as programmed in "Events to show" field, with the possibility of filter them by "event description" and then download the events displayed to a \*.csv file.



**Note:** The events are stored on a non-volatile memory (Flash) with 100,000 write cycles and a minimum of 10 years of data retention.


- **Filter by:** The field allows you to edit the name of the log to be searched, making a filter on the list that appears on the screen (i.e. if you type the word "session", the events that will be displayed will all contain the word "session").

**Events to show:** enter the number of events to be shown and click on (  ) icon.

The event log contains the following data:


1. **Description:** a brief description of the event, preceded by an icon that classifies the event itself, as described below:



(  ) Access event:

- User code recognised
- Installer PIN recognised
- Scenario execution



(  ) Generic event:


- This opens/closes the programming session
- This starts/ends the configuration
- Periodic report
- Com. code deleted (communication reset)



(  ) Events:


- Incorrect code
- Low battery/battery reset
- 220 Vac failure/reset
- Zonal masking/failure
- Fault/masking reset
- Wireless device has disappeared



(  ) Events:


- Inclusion/exclusion of zone
- Scenario execution
- Activate/deactivate partition



(  ) Events:

- Zone reset/alert
- Partition alarm
- Partition input time
- End of partition input time
- Partition output time
- End of partition output time



(  ) Events:

- Tamper/zonal tamper reset
- Tamper/zonal partition tamper reset

2. Date: this displays the date and time when the event occurred.
3. Info: this shows details of the event (the user, the device which generated it, etc.).
4. Image: This shows the images which have been saved against the event being described. Clicking on the icon will show the images.

---

### 3.18 Installer

---

The Installer menu has two submenus: "Maintenance" and "Change PIN".

From **Maintenance** page it is possible to send the following commands to the control panel:

- NO BLOCK = Unblock the control panel if it is in ALARM LOCK and / or BLOCKED ACTION;
- ALARMS BLOCK = It blocks the alarms in the control panel (use in maintenance);
- BLOCKS ACTION = Blocks the actions in the control panel (use in maintenance);
- RESET ALARMS (and sabotage) = send command to delete alarm memory and sabotage;
- COMMUNICATION RESET = send reset command of all communications, even those in progress;
- FAULT RESET = send fault memory cancellation command.

From **CHANGE PIN** page you can change the installer PIN.

---

### 3.19 Floor plans

---

The menu is visible only in local connection to the central panel.

The end user can interact with the different functions configured on his control panel, having at his disposal a logical organization for rooms.

In fact, each element configured on the control panel (sensors, outputs, scenarios, camera, etc.) can be associated with one or more rooms.

The user, through the App Iares 4.0, using the visualization in rooms in the Smart Home section, will be able to see each element configured in that room and have control over it.

The images that reproduce the real space (living room, kitchen, bedroom, etc.) and used as the background of the configured elements, are visible only by connecting from a PC.

## 4. FUNCTIONALITIES AND CONFIGURATIONS DESCRIPTION

In this chapter, the main functionalities offered by lares 4.0 IoT platform and their step-by-step configuration are described, in tabular form. In fact, each table provides information about: the step and the why you have to do it, the menu to open and the fields to configure. The description of the fields and the expected values are described in the relevant chapters in this document. It is sufficient to search for the menu name and the fields (for example: to search for the "Number of pre-alarms" field, search (Ctrl + F) for "Menu Settings" and then "Number of pre-alarms").

### 4.1 Scheduler timers

The Time Scheduler allows the planning of automatic processes, represented by pre-programmed scenarios, which can be executed according to scheduled timetable (hour/sunrise/sunset) and weekdays. The weekdays can be distinguished from the holidays so that, a disarm time scheduler programmed every day at 07:00am (for example) will take place or not if a holiday falls on a weekday.

To load the holidays calendar (valid until 2039), you must select the country where the control panel is installed. Sunrise and sunset are calculated according to the geographic position (latitude and longitude configured) and the time zone where the lares 4.0 control panel is installed. More, you can enter the minutes (+/- 30) to add/subtract from sunrise/sunset time, in order to balance a particular position where the control panel is installed, with respect to the horizon (e.g. presence of mountains). The sunrise time calculation is based on the geographical coordinates of the control panel, received from cloud after Ksenia PRO registration or entered manually in the Ksenia SecureWeb platform.

The maximum configuration number of Time Schedulers depends on the lares 4.0 control panel models.

STEP	DESCRIPTION	MENU	FIELD
1	Enable the holidays calendar		
		Settings-> General options, section Holidays	Country
2	Configure the offsets		
		Settings-> General options, section Date and Time	Sunrise offset Sunset offset
3	Configure the scheduler timers		
		Scheduler timers	Enable Description Partitions Scenario Type of start time Hour MON...SUN Exclude holidays

### 4.2 Path management

It is possible to assign to a zone with "Entry delay" enabled, a "Path" (up to) and a "Level" (1...250). The level is the zone progressive number with respect to the entry path that you are configuring; if within the path, the zones will be violated in a different order than the numerical sequence assigned to the level, the alarm will be triggered.

The violation time is equal to the minimum entry time between all partitions involved in that path.

Zones belonging to the same path do not need to belong to the same partition.

**WARNING!** After the upgrade, the panel will convert automatically the system as follows:

- a zone with "Entry delay" enabled, after the conversion will be assigned "Path 1" and the previous levels will be preserved;
- a zone with "Entry delay" not enabled, after the conversion will be assigned "No path" and Level 0 (not editable until "Entry delay" will be enabled).

STEP	DESCRIPTION	MENU	FIELD
1	<b>Functionnality configuration</b>		
		Zones	Entry delay
			Path
			Level

### 4.3 Pre-alarms management

When the control panel is armed, it can distinguish whether a violated zone should generate an alarm immediately or it can wait for a further alarm signal, within a certain time interval, before triggering the alarm.

This functionality is an alarm confirmation for alarms coming from one or more zones enabled to the pre-alarm functionality.

When one of these zones will be violated, a pre-configured maximum number of pre-alarms must be received before triggering the alarm, within the expiration of timer for alarm confirmation.

If the timer expires before having received the maximum number of pre-alarms, the alarm will not be generated.

It is possible to indicate whether the alarm confirmation must come from different zones or even from the same zone.

It is possible to point out whether the pre-alarmed zones, which help increase the maximum number of pre-alarms, must belong to the same partition or to different partitions:

- if enabled and partition X is in alarm, then any pre-alarm coming from partition X will be considered an alarm;
- if disabled (default) and any partition is in alarm, then any pre-alarm will be considered an alarm.

It is possible to configure Scenarios to be run when the zone generates a pre-alarm (with sub-type Pre-alarm),

Events to be associated with those scenarios, Programmable logics to add customized and more advanced events compared to the standard events provided by the system and finally the Notifications (calls, SMS, e-mail, etc.) to be sent.

Finally, it is possible to receive snapshots from cameras zones with also "zone real-time event", "zone pre-alarm event", "zone by-pass event" enabled.

The functionality is mutually exclusive with respect to the "Path management".

STEP	DESCRIPTION	MENU	FIELD
1	<b>Functionnality configuration</b>		
		Settings-> General options, section <Pre-alarms management>	Number of pre-alarms
			Timer for alarm confirmation
			Same partition
			Confirmation from different zones only
2	<b>Enabling the pre-alarm zone</b>		
		Zones	Enable pre-alarm
3	<b>Pre-alarm zone management</b>		
		Events	Type == Zone
			Subtype == Pre-alarm
		Notifications	Type == Zone
			Subtype == Pre-alarm
4	<b>Select the event related to the zone that will send the snapshots (a camera typically)</b>		
		Zones	Camera trigger



## 4.4 Dimmer

One terminal (M5) of **auxi** expansion module of the lares 4.0 control panel, can be programmed as an analog output 0-10V to adjust the output voltage.

The analog output can be connected to actuators with standard input 0-10V, for detecting the voltage variations (e.g. generic dimmers, fan coils, etc.).

Programming the analog output of the auxi BUS peripheral as an Intensity regulator (DIMMER) to increase/decrease the luminous intensity of a lamp, besides turn it on and off. Configuring a Zone as follows: "Command" processing mode and "Output Dimmer" action type.

The intensity regulator can be managed by the end user from lares 4.0 App and ergo-T/ergo-T plus touchscreen keypads, besides the graphic maps, and monitoring it in real time too.

The end user can adjust the luminous intensity with a slide bar, also the colour intensity varies according to the selected percentage value: from 5 to 100% (step = 0.5V). The icon changes as the setting of the category programmed for the device changes.

STEP	DESCRIPTION	MENU	FIELD
1	Add an analog output		
		Layout->Outputs	Peripheral association (auxi, M5 terminal)
			Polarity (analog)
2	Add a command analog zone		
		Layout->Zones	Peripheral association (any free terminal)
			Processing mode (Command)
			Command output (description assigned to the analog output)
			Action type (Output Dimmer)
			Command mode (Button)

## 4.5 Services on Ksenia Secureweb

---

### 4.5.1 Automatic Backup

---

The Automatic Backup service is an online service offered by Ksenia.

The service consists in the execution of automatic copies of the system configuration data (including images of rooms/maps) with the possibility of restoring them, if necessary.

The maximum number of automatic savings is 3 for each system, when this number is exceeded, the overwriting of copies begins, starting with the oldest one. It is possible to prevent, and therefore preserve from overwriting, a maximum of 2 copies that can be saved by adding a description to identify them; however, 1 copy will always remain overwritable.

After the first activation, the automatic backup is always active and transparent to the installer, both in case of local connection and from Ksenia Secureweb; while the Backup page that allows you to view the backups, enter a description to block them and restore the configuration, is visible only by launching Installer from Ksenia SecureWeb.

#### How the service works

When the installer logs out (and no other installer login is active) a 5-minutes timer starts, after which the backup file is created (locally on the control panel). If the installer logs in again before the timer expires, this will be stopped and the backup will be cancelled. The timer starts again when the installer logs out.

In a completely transparent way to the installer, the backup file with all the configuration data and images of the rooms/maps is saved locally (file name: "filename".ksa) and then uploaded to the cloud. In case of unavailability of the connection, the control panel carries out all the necessary attempts until the upload takes place.

#### Requirements:

1. the control panel must be registered on the Ksenia SecureWeb cloud;
2. the Installer must be launched from Ksenia SecureWeb;
3. the Backup service must be activated by clicking on <ACTIVATE THE SERVICE> button, just the first time;
4. the "green little cloud" icon next to the file name indicates that the backup is synchronized, otherwise a "red barred cloud" appears;
5. the "empty pushpin" icon next to the file name indicates that the backup is not locked and, therefore, could be overwritten, click on the icon if you want to lock the file from being overwritten by entering a free description; when saving, the "pushpin" icon will appear full.

#### Management of backup restore on the same control panel:

Select a file name and then click on "Restore backup" button. After confirmation, the backup restore starts and you will be disconnected; the control panel will restart and then you will be able to log in again.

#### Management of backup restore on different control panels:

Open the list of control panels on cloud by clicking on the "little cloud with lens" icon, once chosen, select the backup file you want to restore and then start the restore.

The compatibility constraints are the following:

FROM TO	lares 16	lares 40	lares 40 wls	lares 96 wls	lares 140 wls	lares 644 wls+*
lares 16	✓	✗	✗	✗	✗	✗
lares 40	✓	✓	✗	✗	✗	✗
lares 40 wls	✓	✓	✓	✗	✗	✗
lares 96 wls	✗	✗	✗	✓	✗	✗
lares 140 wls	✓	✓	✓	✓	✓	✗
lares 644 wls	✓	✓	✓	✓	✓	✓



## 5. APPENDIX

### 5.1 Programming summary

This section summarizes the programming options that guarantee the correct operation of the control panel based on the parameters defined by the IMQ - SAFETY SYSTEMS certified standards. If these options are changed, the control panel will NOT comply anymore the aforementioned regulations.

#### PROGRAMMING ALARMS, TAMPER AND FAULT EVENTS

EVENT	PROGRAMMING OUTPUTS SESSIONS	PROGRAMMING DESTINATION SESSION
Zone alarm Partition alarm		Select a list of contacts almost
Jamming wireless Sabotage area Partition sabotage Central panel sabotage Peripheral sabotage Peripheral missing Wireless Device Sabotage Wireless Device Missing Wireless Jamming	Create an output programmed in "alarm and sabotage" mode, enable the "active only if system armed" option and associate it with the "lamp and buzzer" terminal of an imago siren device.	Select a list of contacts almost
Zone Masking / Fault Low Battery Battery failure Low mains power Low output power Battery failure fault Faulty fuse Central reset Lack of ethernet network Lack of PSTN network Lack of GSM network	The activation of any acoustic signaling device is not permitted.	Select a list of contacts almost

If a list of contacts for zone alarm events is associated, it will not be necessary to associate them with the partition alarm events, and vice versa. The same is also true for Zone Sabotage and Partition Sabotage events.

## ARM AND DISARM OPERATIONS ALLOWED

All the options that allow to arm and disarm the system without the use of an adequate level of access are not compliant. In particular, it is not possible to associate entry methods to zones programmed as 'Command' or to keys on the keypad where the 'Without PIN' option is enabled.

### TRANSMISSION OF ALARMS

#### GRADE 3

The events must be transmitted to the alarm reception center exclusively via GPRS network (via add-on 2G / 3G) or Ethernet with communication protocol SIA DC-09. An SIA IP receiver (previously programmed) can be added to the contact list associated with the alarm, sabotage and fault events. The SIA IP receiver must have the "enable supervision" option enabled.

### TRANSMISSION OF ALARMS

#### GRADE 2

The use of the PSTN card and communication in vocal synthesis is permitted.

It is necessary to activate a supervision by programming a recipient on the "Periodic test" event. The periodicity for the periodic test, to be set on the general settings page, must be less than 25 hours. In any case, the option "Request confirmation" (present in the options relating to the GSM / PSTN communicator) must always be enabled.

### OTHER CONSTRAINTS ON PROGRAMMING

- The maximum programmable input time on the partition page must not exceed 45 seconds.
- For each ergo series keypad programmed in the system the options "Sound feedback entry time" and "" Sound feedback exit time "must be enabled while the options" View entry status "and" View zone status "must NEVER be enabled
- Regarding the balance of the alarm zones, the options "Normally closed" and "Normally open" must NOT be selected.
- The exclusion option "Auto-exclusion" or "With reinclusion" must NOT be selected
- The "Pulse length" option must be greater than 400 ms.
- The faults on the options page must all be enabled.
- In the general options page, the option "Exclude also zone sabotage" must be disabled.
- In the general options page, the option "Allow entry with faults" must be disabled.
- In the general options page, the option "Erasing the sabotage memory from the user" must be disabled.
- In the general options page, the option "Processing of peripheral disappearance as a fault" must be disabled.
- In the general options page, the option "Restrict registration of the same event" must be enabled.
- In the scenario page, regarding the programming of insertion actions, select the sub-type "EN50131 compatible".
- The 'BUS control' option of the imago siren must be enabled.
- All scenarios that perform disarming actions must be programmed in order to also cancel the telephone queue.
- The supervision interval of wireless devices must be programmed equal to:  
1 for GRADE 3 or up to 15 for GRADE 2.

## 5.2 Correspondence table of PUSH notification and Events

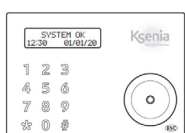
Push category	Event on Iares 4.0
ZONE ALARM	Alarm Zone
ZONES	Tamper Zone Restore Tamper Zone Bypass Zone Unbypass Zone Mask Zone Restore Mask Zone
PARTITION ALARM	Partition alarm
ARMING	Partition arming Partition disarming Partition arming missed Partition negligence
PATROL	Start Patrol End Patrol
PERIPHERALS	Peripheral tamper* Peripheral tamper restore* Peripheral missed* Peripheral missed restore* (* = valid for all BUS, WIRELESS and IP peripherals)
POWER SUPPLY	All the events related to the power supply, for example: Low battery or Battery charger fault
ACCESS CONTROL	Recognized PIN code Recognized tag Incorrect code Recognized installer PIN code
MAINTENANCE	Start maintenance End maintenance
COMMUNICATION	Internet KO Internet OK PSTN KO PSTN OK GSM KO GSM OK
SYSTEM FAULT	Panel shutdown Panel reset Ethernet connection KO Ethernet connection restore Switch LAN – MOBILE network Switch MOBILE – LAN network Supervision SIA fault Supervision SIA restore Jamming wireless Jamming wireless restore
TAMPER PANEL	Partition tamper Panel tamper Panel tamper restore
SCENARIOS	All keys of keypad All keys of wireless keypad All macros of proximity readers (volo) Scenario execution Scenario execution from time scheduler

Load management	Power consumption exceed Normal power consumption Load disconnection risk End risk of load disconnection
OTHER	All the other missing events belonging to other categories.

## 5.3 Customization forms

Downloadable forms from [www.kseniasecurity.com](http://www.kseniasecurity.com) site in \Reserved area\Manuals.

### 5.3.1 Keypad Keys Customization form




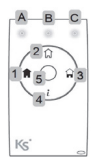
KEYPAD



KEY	Scenario name	PIN
1		
2		
3		
4		
5		
6		
7		
8		
9		
0		
#	View partitions status, then use the round scroll or the arrows to navigate.	
*	View zones status, then use the round scroll or the arrows to navigate.	





### 5.3.2 opera Remote Control Keys Customization form

**OPERA  
REMOTE CONTROL**

Key	Operation	Function	Scenario name
1	Short press	Set scenario 1	
	3 sec. at least	Set scenario 2	
2	Short press	Set scenario 3	
	3 sec. at least	Set scenario 4	
3	Short press	Set scenario 5	
	3 sec. at least	Set scenario 6	
4	Short press	View control panel status	Light on LED A (ARMED) Light on LED B (DISARMED) Light on LED C (PARTIAL)
	3 sec. at least	Set scenario 7	
5	Short press	Battery level	3 Leds steady ON: HIGH 2 Leds steady ON: MEDIUM 1 Led steady ON: LOW Red led blinking: REPLACE
Any key	Short press	Panic/S.O.S. (only with serial number higher than 100000)	Panic/S.O.S

### 5.3.3 volo Customization form

**PROXIMITY READER: volo**

**How to activate a scenario:** approaching a valid Tag to the Proxy Reader, the LED will switch on in the colour associated to the possible scenario (example if DISARMED it will switch on ARMED). To activate the desired scenario, take the Tag away when the LED is lit of the colour related to that scenario: as acknowledgement, the LED will remain ON with the same colour for other 3 seconds. In the idle state the LED colour is:

- Red > if all partitions will be enabled\*
- Blue > if only some partitions will be enabled\*.

\* It depends on the proximity reader configuration.

LED colour	Scenario name
GREEN	
RED	
WHITE	
BLUE	
YELLOW	

If alarm or tamper conditions are present, the LED blinks yellow every 3 seconds.

### 5.3.4 volo-in Customization form



#### PROXIMITY READER: volo-in

**How to activate a scenario:** approaching a valid Tag to the Proxy Reader, the LED will switch on in the colour associated to the possible scenario (example If DISARMED it will switch on ARMED). To activate the desired scenario, take the Tag away when the LED is lit of the colour related to that scenario: as acknowledgement, the LED will remain ON with the same colour for other 3 seconds. In the idle state the LED colour is:

- Red > if all partitions will be enabled\*
- Blue > if only some partitions will be enabled\*.

\* It depends on the proximity reader configuration.

LED colour	Buzzer (if enabled)	Scenario name
GREEN	1 bip	
RED	1 bop	
WHITE	1 bip + 1 bip	
BLUE	1 bop + 1 bop	
YELLOW	1 bip + 1 bop	

If buzzer is enabled, it sounds 3 bips to confirm the operation, 1 long bop to signal "no operation".

If alarm or tamper conditions are present, the LED blinks yellow every 3 seconds.

