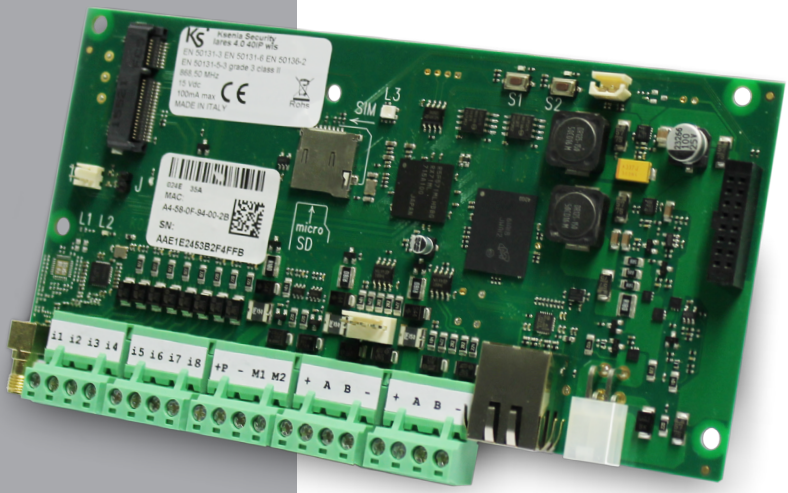
lares 4.0

The most innovative IoT Solution
for Security and
Home & Building Automation

INSTALLATION AND USE MANUAL



Ksenia
SecureWeb

Ksenia
security innovation

INDEX

EN

NOTE

Technical Specifications, appearance, functionality and other product characteristics may change without notice.

lares 4.0 represent by far the most advanced and reliable Solution in the Digital Revolution (**IoT**) for what concern both the Security (Intrusion, Video-surveillance, Access Control) and the Home & Building Automation. The lares 4.0 Platform has been developed and manufactured with unprecedented characteristics of power, calculation speed and capacity of memory calculation.

lares 4.0 HARDWARE - SOFTWARE CHARACTERISTICS

	lares 4.0 - 40	lares 4.0 - 40 wls	lares 4.0 - 140 wls	lares 4.0 - 644 wls
Generali				
Number of zones (of which radio)	40 (40)	40 (40)	140 (64)	644 (64)
Number of outputs (of which radio)	40 (40)	40 (40)	140 (128)	644 (128)
Number of arming modes	32	32	64	128
#Hashtag number	12	12	20	64
Number of partitions	12	12	20	30
Number of IP Cameras	12	12	20	30
Motherboard				
Programmable inputs / outputs	2	2	2	2
Inputs	8	8	8	8
868 MHz radio interface	/	●	●	●
On Board Bus	1	2	2	2
BUS				
User Interfaces (**ergo** keyboards, **ergo S**, **ergo M volo** e **volo-in**)	24	24	40	64
Expansion Module (auxi, auxi relay, auxi 10in, auxi-L)	24	24	64	250
opis / divide	12	12	20	64
duo BUS (64 peripherals)	2	2 *	2 *	2 *
Sirens (indoor and outdoor)	24	24	40	64
Wireless				
Wireless sensor (**poli, nanus, unum, velum, nebula**)	40	40	64	64
imago wireless Siren	3	3	5	5
opera Remote control	64	64	64	64
duo repeater	2	2	2	2
auxi wireless I / O	20	20	64	64
User Management (Codes + Keys)				
Number of manageable users	64	128	512	1024
Events LOG				
Number of stored events	1.500	5.000	10.000	10.000
Scenarios				
Number of programmable scenarios	32	32	128	512
Events groupings				
Number of events groupings to which associate the scenarios	64	64	256	1024
Notifications Management				
Number of contact lists	8	8	16	32
Number of contacts for each list	8	8	8	8
Number of events grouping to which associate a list of contacts	32	32	64	128
Hardware				
Stabilized Switching Power Supplies	15 Vdc - 50 W			
Power Supply voltage	15 Vdc ± 1%			
Control Panel Power Consumption (max)	100 mA			
BOX Weight without battery and Power Supply	4,2 Kg			
Temperature range	5 °C / + 40 °C 23 °F / 131 °F			
Degree of protection IP	IP34			

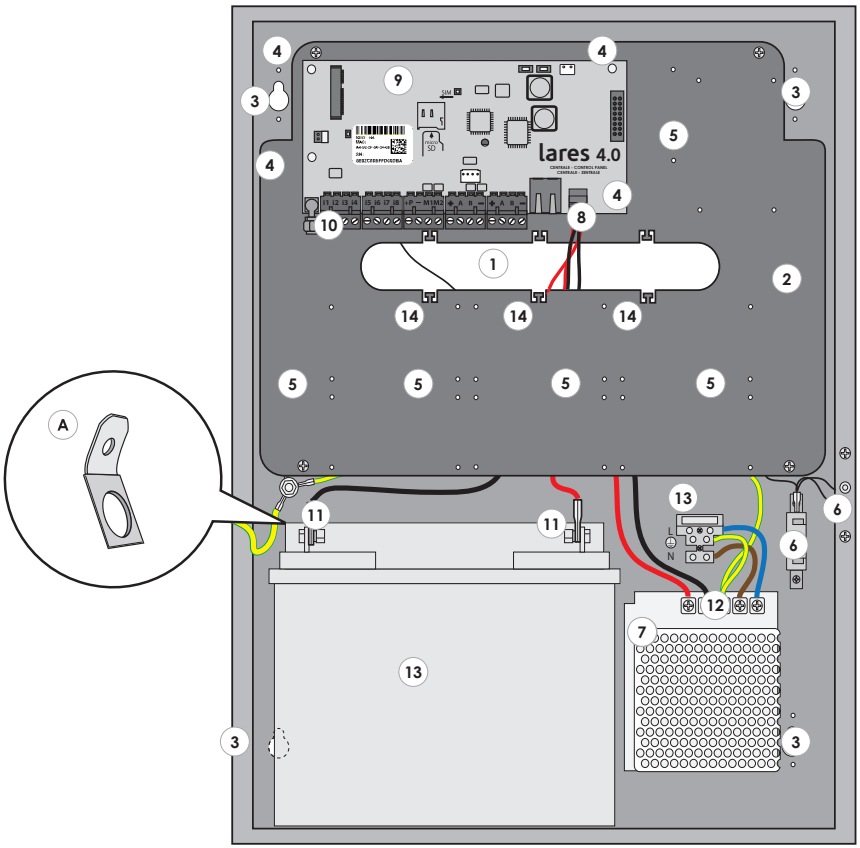
***** If the Mother Board is already having the wls 'onboard', n. 1 '**duo BUS**' can be added.

PARTS IDENTIFICATION

Hereafter, shows the main parts composing the **lares 4.0** system. The picture also shows the Power Supply connections in detail: pay attention to the protection ground connection. The large buttonhole on the Box bottom provide an wide passage of cables for wiring the peripheral devices also in the case of quite large systems.

1. Large buttonhole for passing cables	11. Battery terminals. If necessary use the included Faston adapters (A)
2. Removable metal plate	
3. Bottom fixing holes	12. Power Supply unit terminals
4. Support for Motherboard	13. 2A Fuse
5. Support for Motherboard expansion modules	14. Holes for cables fixing
6. Tamper micro-switch	15. Holes for front cover fixing. Use the included 4 screws.
7. 18Ah Battery	
8. Power Supply cable*	16. Metal box fixing holes If necessary use the included 5 shims. (B)
9. Motherboard Control Panel	
10. Connection terminals	17. Tamper micro-switch.

***** Included for connecting the Power Supply and the Battery. The **clean** two Terminals are for the Power Supply (**15Vdc**), the two Terminals with **Faston** are for the Battery **12V**.

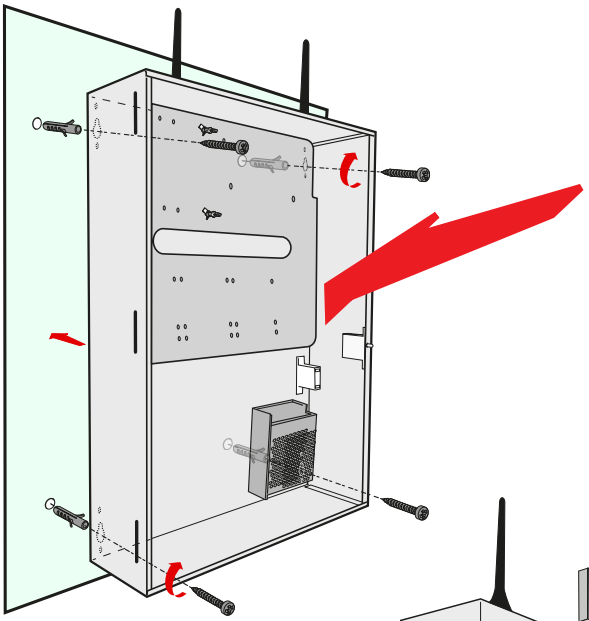


WALL MOUNTING INSTRUCTION

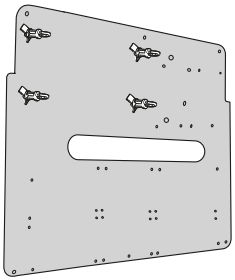
In order to correctly install the metal cabinet and the components inside it, please follow the instructions here below:

1. Fix the metal box on the wall, using screws Ø6mm (**included**)
2. Wire the cables as shown in picture.
3. Ensure the cables to the fixing holes (N°14 page. 24) using plastic clamps (**Not included**).

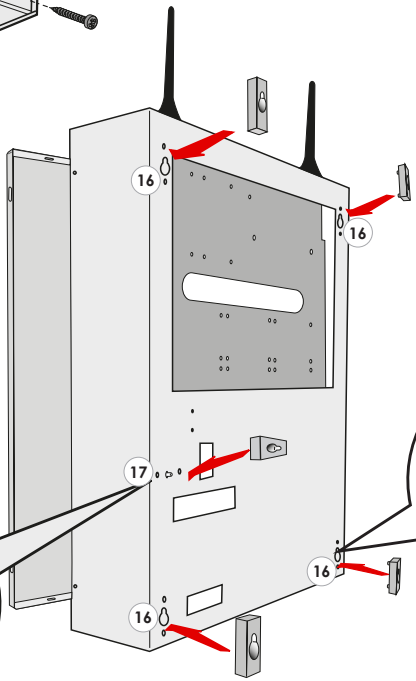
Wall fixing of the Metal Box.



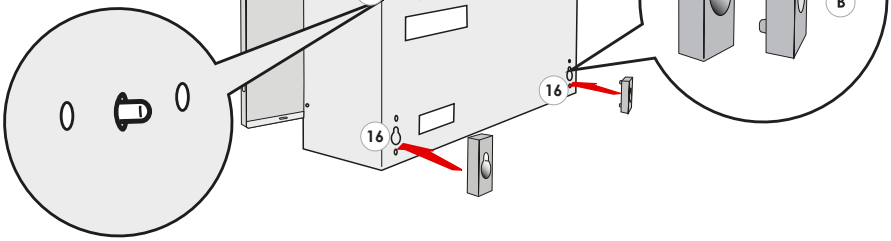
Removable metal part.

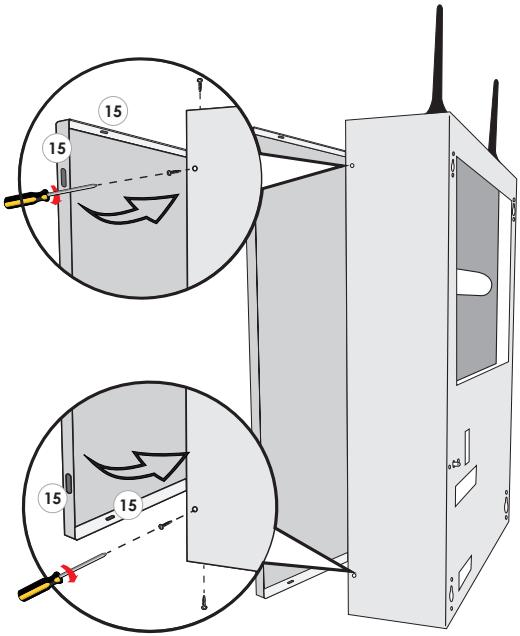


Before fixing the Metal Box to the wall, check if it is necessary to use the included shims.



Tamper micro-switch.





Fixing the front cover of the metal box of Control Panel:
After closing the cover of the metal box, fix with the included screws at the indicated points: (15)

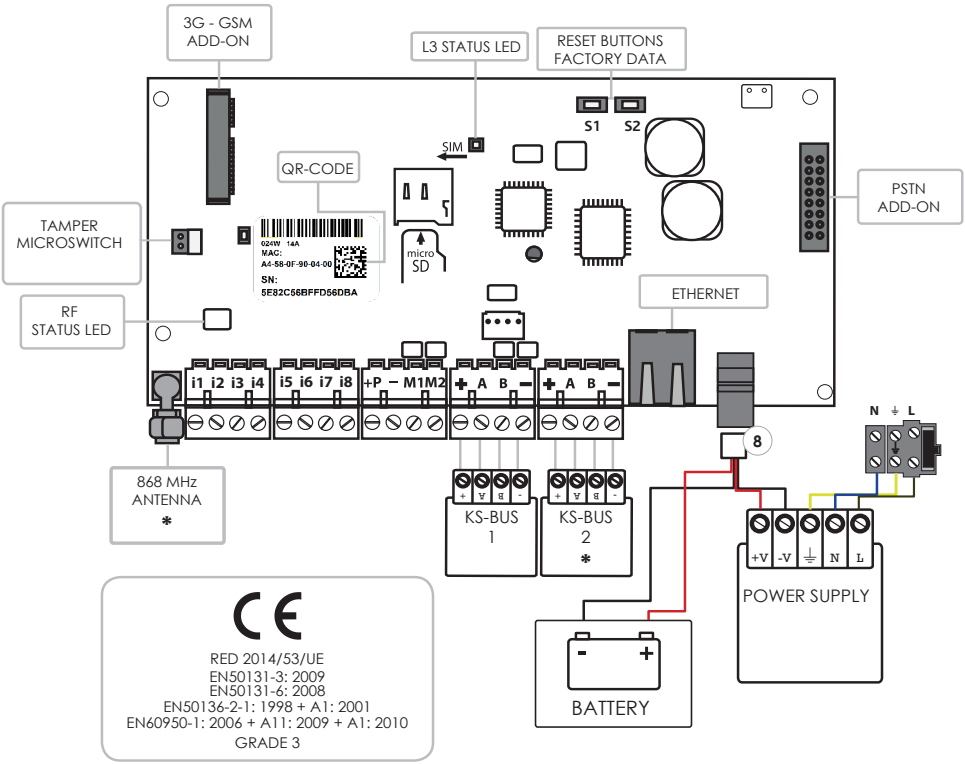
- Arrange outside the Panel an isolating device (es. Circuit Breaker Device 16A Curve C).
- The Power Supply has an internal fuse (50W - F3.15AL).
  In case should fail, its replacement requires the opening of the Power Supply and must therefore be carried out by authorized personnel.
- Wire the protection ground connection directly on the Power Supply unit.
- The Power Supply conductors must be 0,6 inch.² minimum section
- Depending on the installed Control Panel, check the relative box in the label using a petroleum solvent resistant pen, outside the metal cabinet.

Ksenia
security innovation

230V ~ +10% -15% 50 Hz
EN50131-1 grado 3 classe II

☐ lares 4.0 - 40
☐ lares 4.0 - 40 wls
☐ lares 4.0 - 140 wls
☐ lares 4.0 - 644 wls
☐ opis

CE



*** lares 4.0 - 40:** this Control Panel model does not have an RF transceiver and a second BUS.

Note: Power Supply cable **(8) included** for connecting the Power Supply and the Battery is **composed of four Terminals,** two Terminals are for the Power Supply (**15Vdc**), the two Terminals with **Faston** are for the Battery **12V**.

To install **lares 4.0** on metal boxes **KSI 7402117.010** or **KSI 7403130.010** adjust the Power Supply to **15V.**

i1, i2, i3, i4, i5,i6, i7, i8 • Input Terminals.
M1,M2 • Input / Output Terminals (OC 500mA max).
SENSORS: ianitor, unum, velum, magnetic contacts, etc.
+P • Positive Terminal of Power Supply (1.5A max).
- • Negative Terminal of Power Supply.

+	KS-BUS Serial BUS of communication	Positive Terminal of BUS supply (15V 1,5 A Max).
A		Data
B		Data
-		Negative Terminal of BUS supply .

STATUS LED RD - L2
This LED blinks every time the Control Panel receives a valid radio packet.
STATUS LED - L3
The Control Panel has an RGB LED (**L3**) which, depending on the status, indicates the different information.
GREEN flashing: normal operation.
WHITE flashing: initialization phase.
PURPLE flashing: **NOR** memory formatting.
RED flashing: firmware update in progress.
YELLOW flashing: data factory restore.
BLU flashing: reload backup of the configuration, following a firmware update with database replacement.
fixed **Yellow**: **NOR** memory access problems. execute Control Panel formatting.
fixed **RED**: firmware problems. Contact Ksenia Security technical assistance.

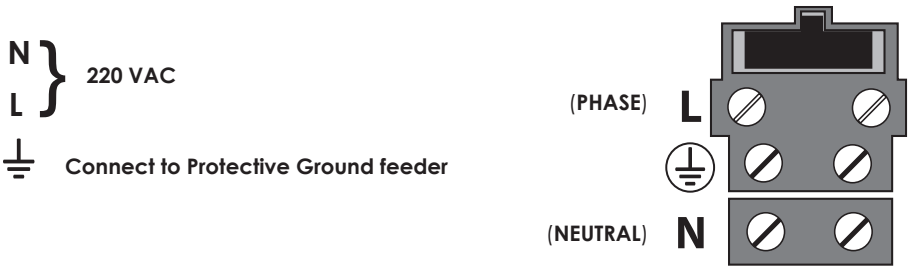
EN

Factory data restore: press the **S1** button for 4 seconds, The status LED **L3** will start flashing **RED-GREEN** color. When the LED **L3** turns fixed **RED**, release the button.

De-entry from SecureWeb: press the **S2** button, The status LED **L3** will start flashing **GREEN / BLU**. When the LED **L3** turns fixed **BLU** the procedure is completed.

Complete formatting of the Control Panel: press **S1** and **S2** at the same time, LED **L3** flashes **RED / BLUE** alternately. After 4 seconds, when **L3** becomes fixed purple, the necessary pressure time to control factory data and the deregistration to the **SecureWeb** has been reached, if you keep pressing the buttons for another 10 seconds the LED will start to flash **PURPLE** and starts the complete formatting.
WARNING - carry out this procedure only if the **L3** LED is on in fixed **YELLOW.**

CONTROL PANEL POWER TERMINALS



Before powering and switching on the Panel, make sure that all necessary wirings have been executed.
• in presence of GSM Module, verify its connections to the Control Panel board, that the micro SIM has been inserted and that the GSM Antenna has been linked by means of its SMA connector.

• in presence of PSTN Module, verify the connections with the Panel board. Insert the RJ11 connector both for incoming and outcoming line.

• Verify that the connection of RF 868 Antenna has been linked by means of its SMA connector
• If present, verify the connection of the integrated Keypad with the BUS terminals
• In the presence of an Internet Network, wire the Ethernet cable to its connector.
• If required, execute all wired inputs cablings.
• If required, execute all wired outputs cablings
• Make all wirings for the Mains
• Connect the Battery using the provided cables.

For all details on how to realize all connections, please refer to the next paragraphs.

GSM / 3G

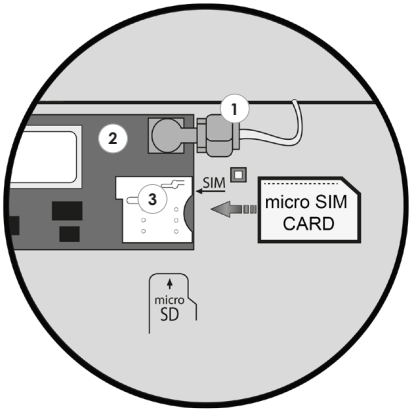
GSM / GPRS COMMUNICATOR (Optional Add-on Module)

KSI4102000.300

3G COMMUNICATOR Optional Add-on Module)

KSI4103000.300

1. GSM / 3G Antenna
2. GSM / 3G Module
3. Slot SIM Card (micro SIM).



- Voice Messages and / or SMS Transmission.
- Separate SMS distinct for each Sensor.
- 'Calls Stop' when System disarmed.
- Voice Dialer with possibility to personalize the messages
- Voice message Recorder by KP or Text-to-Speach (different Voices and Languages with 'loquendo' license)
- High Quality Digital Audio
- GSM Jamming detection.
- Contact ID Transmission

IMPORTANT: before inserting the micro SIM inside the GSM module, be sure to DE-ACTIVATE the PIN code request by using a mobile phone

NOTES:

• please pay attention to the correct insertion direction of the SIM card as illustrated (not included)

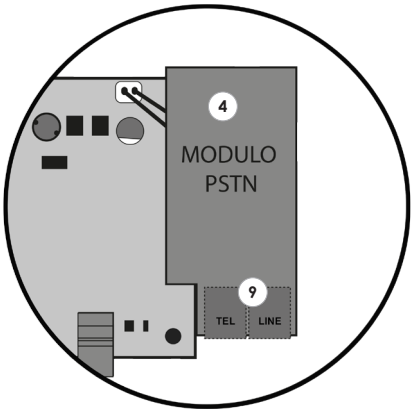
• the device is not compatible with Providers who support the UMTS networks only (e.g. 3 Italy)

PSTN

PSTN Communicator (Optional Add-on Module)

KSI4200001.300

4. PSTN Communication Module.
9. LINE / TEL: Terminals for wiring to the phone line.



TEL

terminal for wiring of phones, fax or other Devices wich use the tel. **PSTN** line

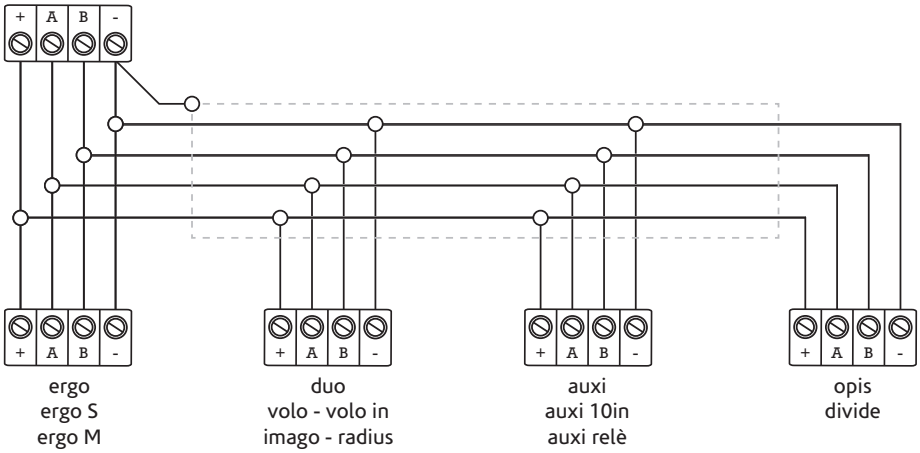
LINE

terminal for wiring to the tel. Line

- Voice Messages Transmission.
- 'Calls Stop' when System disarmed.
- Voice Dialer with possibility to personalize the messages
- Voice message Recorder by KP or Text-to-Speach (different Voices and Languages with 'loquendo'license)
- Contact ID Transmission.

KS-BUS CONNECTION DIAGRAM (RS485)

Peripheral units of the Ksenia system are connected through the fast KS-BUS. It is recommended not to exceed, for each wiring branch (e.g. Control Panel - device), the maximum length of 500 m (1400 feet), and the complete wiring should not be longer than 1000m (2800 feet). Always use a shielded cable with one end of the shield connected to the Control Panel's ground and the other end free. Figure below is an example.



COMPATIBLE BUS DEVICES

DEVICE	**auxi** **auxi 10in** **auxi relè** expansion module	**ergo** **ergo S** **ergo M** LCD keypad	**imago** outdoor siren on BUS	**radius** indoor siren on BUS	**volo** **volo-in** proximity readers	**divide** BUS isolator/ repeater	**duo** BUS wireless receiver	**opis** Supervised Power Supply station
COMPLIANT EN50131	✓	✓	✓	✓	✓	✓	✓	✓
CONSUMPTION	20mA P terminal and outputs excluded	15mA stand-by 100 mA max	20mA stand-by 250mA max	20mA stand-by 250mA max	40mA	20mA	50mA max	50mA

NOTE: not compatible device (pontis, gemino BUS, duo 16)

WIRELESS PERIPHERALS

The Control Panel is compatible with the following 868 MHz bidirectional wireless devices:

poli, nanus	Wireless detectors
velum wls, unum wls, unum wls PI	Motion detectors
nebula	Optical smoke detector
auxi wls	Wireless control module
imago wls	Outdoor siren
duo	Radio repeater
opera	Wireless Bidirectional Remote control

CONTROL PANEL CONFIGURATION

When delivered, the '**lares 4.0**' Control Panels has to be programmed on purpose.

The configuration can be done choosing one of the following modes:

1. remotely, thanks to the **APP Ksenia PRO** available for iOS and Android.
2. remotely, through the portal: **www.kseniasecureweb.com.**
3. through **webserver**, accessing in local mode or peer-to-peer to the Panel.

In general, all configurations can be carried out using any of the methods described above; the few exceptions are reported in the following sections.

NOTE:
- **the default Installer PIN to access the configuration is 123456**
- **the access to 'Technical Menu' of configuration is NOT possible if the System is armed stay or away, or if it has specifically been blocked by the User**.

EN

1. REMOTE APP CONFIGURATION: download the APP named 'SecureWeb' for any mobile device available on AppStore or PlayStore. Login to the APP using the same credentials used to get access to our 'Reserved Area' on the site **www.kseniasecurity.com**, in case of Installers not yet registered, you must then register on the above site.
The registration is strictly personal and allows to configure an unlimited number of Panels.
Once the APP is opened, it is sufficient to enter into the Tab called 'Devices', here all Panels are listed and in communication with you.
To configure a new Control Panel, press on + (top-right) , scan the QR-code present on the Motherboard label
or insert manually the 16 digits serial number.

2. REMOTE PORTAL CONFIGURATION: It uses the service Ksenia **SecureWeb**, through the portal: **www.kseniasecureweb.com**, reserved to the Selected Ksenia Installers. The access is allowed by using the same credentials used to get access to our 'Reserved Area' on the site **www.kseniasecurity.com**, in case of Installers not yet registered, you can then register directly on the Portal.
The registration is strictly personal and allows the configuration of an unlimited numbers of Panels.
Once logged on the portal, it is sufficient to enter into the section 'Devices' and you find the list of all Panels already in communication with you. To configure a new Panel, insert 16 digits serial number that you'll find on the Motherboard label and click 'Register new panel'.

3. WEB SERVER CONFIGURATION: Locally accessing the webserver configurator. The Panel starts by default with enabled DHCP, then there are 2 possibilities to find out the IP Address:
by the Keypad, entering the dedicated 'technical menu' or using the server named:
https://KS-BOARD-xx-yy-zz (replacing the **xx-yy-zz** with the last 6 digits of the MAC Address printed on the label). In case the network programmed will not support the DHCP, the default address is **https://192.168.2.97.**

Note: in the default status, the Control Panel only communicates in safe mode (https) on port 443

INSTALLER MENU (BUS KEYPAD)

In this section the keypad installer available operations are described.
To access the installer menu the installer code (DEFAULT **123456**) is required.

The installer menu can be navigated using the following keys:
- **ENTER**: to enter the lower level menu.
- **ESC:** to go back at the previous menu.
- **UP ARROW**, **CLOCKWISE SCROLL**, **DOWN ARROW**, **COUNTER CLOCKWISE SCROLL** to scroll in the same level items.

This is the menu items tree:
- **System management:** System management items
  - **Reset alarm:** all the alarms will be stopped, tamper and alarm memories will be cleared
  - **Stop calls:** all the running and queued communications (SMS, phone calls, emails, etc.) will be deleted
  - **Freeze system:** here one on three operating modes can be selected:
    - No freeze: normal operating mode
    - Freeze alarm: no action related to alarms will be done
    - Freeze actions: the panel will do no actions at all
- **User management:** here RF-ID tags can be assigned to users.
- **Event logger:** memory of all the panel events, with possible details
- **Trouble list:** active troubles list
- **Zone status:** list the status of configured zones
- **Zone test:** this section is useful during system installation. In this menu all the zones that alway had been resting for the beginning of test are listed.
- **Installer data:** this menu contains the following items, all related to installer data:
  - **Change PIN:** here the installer change its PIN
  - **Description:** typically used for installer name
  - **Number:** phone number of installer
- **Update:** the panel firmware will be update, using the file in the SD card
- **Program. Backup**:
  - **Create New:** programming data will be backed up in the SD card
  - **Restored:** programming data will be read from SD card and loaded in the panel
- **Networking:** network configuration menus, for reading or changing the network parameters:
  - **IP address**
  - **Subnet mask**
  - **Gateway**
  - **DHCP server:** this item is available only if the panel has a static IP address, and its purpose is to enable the DHCP server.
- **Language:** here the keypad language can be selected in a list.

The **lares 4.0** platform includes countless innovations, in this section are highlighted the more important variations compared to the lares platform, in order to help installers that habitually installed lares to migrate to the new platform.

This section can also be used as a quick guide to quickly access to the configuration.
From the hardware point of view, referring to the motherboard, the main differences are:
• There are 8 inputs (and not 6)
• There are 2 configurable input / output terminals (and not 4)
• Onboard inputs and I / O terminals on board, if configured as a zone, can not handle directly glass break / inertial sensors and roller blind
• The supply voltage of the board is 15Vdc (and not 14.2V)
• The board can host two add-on modules, one for the PSTN connection, the other for the mobile one (therefore 2G, 3G and in the future 4G)
• The versions **lares 4.0 - 40 wls**, **lares 4.0 - 140 wls**, **lares 4.0 - 644 wls** have two Buses on board, completely independent
• lares versions **lares 4.0 - 40 wls**, **lares 4.0 - 140 wls**, **lares 4.0 - 644 wls** already integrate the 868 MHz radio interface on board, this acts as an alternative main receiver to one of the receivers on the BUS. It is possible to deactivate the receiver on board to connect two receivers on the BUS. The control panel supports always two repeaters.
• The motherboard has a slot onboard to insert an SD card, which is currently used for back up the configuration, to restore a saved configuration, for firmware update.

From the BUS point of view, all the peripherals are compatible, with the exception of gemino BUS, pontis, duo 16.

From the software point of view, the lares 4.0 platform can not be programmed by the basis software. The programming installer interface is realized by webserver, and therefore the configuration can be done via **Ksenia PRO** APP, from the portal **www.kseniasecureweb.com** or by connecting directly to the control panel via a network cable.
In the case of a direct connection, the default setting of the control panel is in safe mode, therefore the address must be specified preceded by **https: //**
Even if we check our software with different Internet browsers, our suggestion is to preferably use Google Chrome.
When you access the control panel configuration, you can see the configuration of the control panel currently in use.
In order to modify a configuration, you need to open a session by pressing the pen icon in the upper right corner.
In this phase you can make all the changes to the programming, if there are any partial or incorrect information, these are indicated by a red colored exclamation point above the save icon, and prevents data from being saved until these anomalies are resolved.
When you save a configuration, the new data are not used immediately by the control panel, but for actually apply the programming, it is necessary to press on the V icon.

Regarding the configuration, the main differences are:
• There is a new grouping, called Hashtags, which can be applied to zones, outputs, users and user interfaces (keypads and proximity readers). From the scenarios it is possible, for example, activate two outputs individually (example light1 and light2), but if I have associated them with a Hashtag #lights, activating the outputs with #lights, with a single command the panel will turn them both on.
• BUS and wireless devices are grouped by type, and then individually identified so the panel can appropriately manage even the slightest differences between them. For example while on **lares / basis** there is only one model of keypad, on the lares 4.0 there are the **ergo** (and **ergo-rev.0**, the hardware version of the ergo keypad produced until May 2017) - **ergo S** - **ergo M**.
• The zone association (output) to the relevant terminal is done directly in the configuration of the zone (output), associating it with the available peripherals and terminals
• The outputs have operating modes dedicated to anti-intrusion management, therefore it is not necessary to configure a scenario to activate alarm outputs.

• Software timers are no longer present, but these have been replaced by virtual outputs, combined with the Output Activation and Output Deactivation events.
• For each output it is also possible to select different operating modes in the local or remote management via APP, allowing for example, an activation on local network without PIN and remote with PIN.
• Address book configurations, codes, keys and remote controls are grouped into a new structure, called Users. For each User, you can select the type of notification you can receive, you can assign a PIN, a key, and a remote control (only in this last case limited to one maximum of 64 users).
• Depending on the panel size, up to 512 scenarios can be configured, all of which can also be managed remotely (thus exceeding the limit of 10 on the lares platform).
The scenarios are a list of maximum 16 actions, which can freely manage outputs (activation, deactivation, toggle), zones (exclusion, inclusion, toggle), users (enabling, disabling), partition arming/disarming.

• Arming modes can be activated with 4 forcing levels: Compatible EN50131 (in system case not ready, it is not inserted and the Event of Failed Entry is generated);
Manual Bypass (if the system is not ready, the list of open zones is shown with the possibility of manual bypass), Forced arm with alarm (in case of system not ready, it is armed and it generates the alarm); Forced with arm with auto-bypass (in case of system not ready, it is armed with forced bypass of open zones).
• For each scenario it is also possible to select different operating modes in the local or remote management via APP, allowing for example, an activation on local network without PIN and remote with PIN.
• The scenarios are then assigned to the events to be activated, grouped by category.
• To send different notifications (SMS, voice calls, email, etc), the contact lists must be created, then associated in the section Notifications to events that must be sent.
•The generation of voice messages can be done via **text-to-speech Loquendo**, only from the portal **www.kseniasecureweb.com**, having purchased a license (one for installer) with the scratch-card.

From the LCD keypad management, any configurations can not be made.
Entering on the Technical menu with installer code, the control panel does stop the normal operation.
To block the operation of the control panel, it is necessary to select the Freeze Alarm or Freeze Action in the Sys. Configuration menu.

CONFIGURATION OF CONTROL PANEL FROM INSTALLER INTERFACE

The same configuration interface is available from the portal **www.kseniasecureweb.com**, via the **Ksenia PRO** mobile APP, or with direct connection.
It automatically adapts to the resolution and screen size, It can be PC / MAC, tablet or smartphone.

This section explains the main pages of the configuration menu, while for the detail refer to the programming manual.

- **Home**: It is the home page of the configuration, it includes the real time information of the system, information about the versions, the last 10 events of the panel log.
- **Settings:** Includes two sub-pages:
  - **General options:** Includes configuration options that affect the system in general.
  - **Network:** Includes all the options concerning the connectivity of the control panel.

- **Events Log:** This page shows the panel's event log.
- **Hashtags:** allows the definition of hashtags, to be combined with zones, outputs, user interfaces and users.
- **Partitions:** This page includes the partition configuration.
- **Bus Peripherals:** Includes 5 sub-pages, for configuring devices connected to the KS-BUS:
  - **Expansion Modules:** It allows configuration of auxi, auxi 10, auxi relays / auxi-L.
  - **Isolators:** It allows the configuration of opis and divide.
  - **Receivers:** It allows the configuration of the duo.
  - **User interfaces:** It allows the configuration of ergo keypads (rev.0), ergo S, ergo M, ergo, volo, volo-in.
  - **Sirens:** allows the configuration of the BUS sirens: imago BUS and radius BUS.

- **Wireless Peripherals:** Includes 4 sub-pages, for configuring 868 MHz wireless devices:
  - **Wireless sirens:** It allows the configuration of sirens imago wls.
  - **Wireless Repeaters:** allows configuration of the duo (set as repeaters).
  - **Wireless I / O modules:** allows configuration of the auxi wls.
  - **Wireless sensors:** It allows the configuration of the magnetic contacts, (poli and nanus), of the sensors unum wls and velum wls, of the nebula wls smoke detectors.
- **IP Cameras:** It allows the configuration of IP cameras.
- **Layout:** Includes 8 sub-pages, for system configuration:
  - **Arming Modes:** configuration of the different arming modes to be associate to the partitions.
  - **Zones:** zone configuration (inputs).
  - **Outputs:** configuration of outputs (also virtual - Timers).
  - **Users:** configuration of system users (address book, codes, tags, remote controls).
  - **Scenarios:** configuration of scenarios (list of actions).
  - **Events:** configuration of events, to which the scenarios are associated.
  - **Contact lists:** lists of users who receive notifications.
  - **Notifications:** configuration of events, to which are associated the contact list to which transmit the voice alarms, sms, e-mails, etc.

- **Real time:** real time windows for system status analysis.
- **Voice messages:** pages for generation (not available with direct connection) and listening of voice messages.

In this section the operation available using the ergo LCD KEYPAD are described

KEYPAD OPERATIONS
Please, see the ergo LCD KEYPAD manual for keys and scroll usage.

STAND-BY DISPLAY – UPPER DISPLAY ROW
When in stand-by, in the upper display row the system status is shown. The available informations are (in priority order):

- **CONFIGURATION:** the panel is applying a new configuration data set.
- **PERIPHERAL LOST:** one or more BUS peripheral is not communicating with the panel.
- **ACTION BLOCKED:** the installer blocked the panel actions (see Installer menu-System management-Freeze system).
- **ALARM BLOCKED:** the installer blocked the panel alarm actions (see Installer menu-System management-Freeze system).
- **TAMPER:** at least one of the partitions on which the keypad is enabled is in tamper.
- **ALARM!:** at least one of the partitions on which the keypad is enabled is in alarm.
- **TAMPER MEMORY:** at least one of the partitions on which the keypad is enabled has a tamper memory.
- **ALARM MEMORY:** at least one of the partitions on which the keypad is enabled has an alarm memory.
- **FAULTS IN PROGR. :** at least a fault is running in the system.
- **MEMORIA GUASTI (TBV):** at least one fault arose and disappeared.
- **ENTER TIME:** at least one of the partitions on which the keypad is enabled is running the entry time.
- **EXIT TIME:** at least one of the partitions on which the keypad is enabled is running the exit time.
- **PREARMING:** at least one of the partitions on which the keypad is enabled is running the pre-arming time.
- **CALL RUNNING:** the communication system is running a call.
- **BYP / TEST ZONE:** at least one zone is in test mode, or is manually bypassed.
- **SYSTEM OK:** the system is working, no anomalies, no intrusions.
- **INFOS AVAILABLE:** this information is visible only if the panel was programmed to be EN50131 grade 3 compliant. In this case the system status can't be displayed, so this information means that there is something to check in the system.

STAND-BY DISPLAY – LOWER DISPLAY ROW
The stand-by information on the ergo LCD KEYPAD display upper row can be disabled by the installer. If this is the case, to show these information a valid user **PIN** or a valid tag must be used.
In the upper row the text "**Ksenia Security**" if everything is ok, or "**INFOS AVAILABLE**" in other cases will be shown.
Otherwise, if system is disarmed, always "**Ksenia Security**" will be displayed.
The information set on the lower row can be customized on a keypad-by-keypad basis. These infos are:

- Time and date.
- Arming status (active scenery).
- External temperature (at least one external siren imago BUS must be present in the system).
- Interior temperature (at least one interior siren radius BUS or temperature sensing keypad must be present in the system).
- GSM provider.
- Real time open zones.

NOTE: When in a user menu, the keypad will return to stand-by if no key will be used for 30 seconds.

STAND-BY OPERATIONS
From the stand-by state, 6 different actions can be done using keys:

- **ENTER key**: will show deeper information about the system status (upper row), that can be scrolled using arrows or scroll.
- **#** key: partitions status, that can be scrolled using arrows or scroll.
- ***** key: zones status, that can be scrolled using arrows or scroll.
- **0-9** keys (for at least 3 seconds): will activate the corresponding macro action (if programmed and enabled).
- **0-9** keys: PIN code input (default: **000001**).
- **ESC** key (for at least 3 seconds): will freeze the keypad for cleaning purpose.

If the keypad is not enabled in the system, the display will show only "**SYSTEM OK**", and the user PINs are disabled. The installer PIN is always enabled.

USER PIN ACTIONS / SCENARIOS
The user PIN is always 6 figures long.
After user PIN input the user can choose in a list of scenarios (starting from the most used one, based on enabled functions programmed) or the main menu.
For example:
two scenarios are enabled, key **0** ('**Disarm**') and key **1** ('**Arm**'); the keypad will prompt the more used of these. If no key will be pressed within 3 second, the prompted scenario will be executed, and the keypad will return to idle state.

FAST KEYS: For a faster use, the user can also input the PIN followed by the figure of the wanted scenario, or by the **#** (**Pound**) key to enter the user menu.

EXECUTING MORE SCENARIOS IN SEQUENCE
After PIN code input, a digit can be input followed by the **ENTER** key. The key corresponding scenario will be executed, and now is possible to input another digit, followed by the **ENTER** key.
The new scenario will be executed as well, and so on. Using the **ENTER** key allow the user to execute more scenarios with a single PIN code input.
It is also possible to use the scroll for choosing a scenario and execute it using the **ENTER** key.

MAIN MENU

To select an item in the list the ENTER key must be used.

- **Reset alarm:** running alarms will be stopped, and alarm memories cleared.
- **Partition status:** partitions arming status will be displayed.
- **Zone status:** the zones real time status will be displayed; furthermore, using the ENTER key again, the zones will toggle its bypass status.
- **Change PIN:** selecting this option the user PIN can be changed.
- **ergo options:** selecting this option, the ergo keypad operating parameters can be changed.
  - **Backlight**: the backlight level can be chosen from normal, maximum, eco.
  - **Volume:** the volume level can be chosen from normal, high, maximum, low, off.
  - **Chime:** chime function can be enabled or disabled.
  - **Touch sens. :** the sensitivity of touch keys can be chosen from low, medium, high.
- **Advanced options:** see the related following list.
- **Trouble list:** the list of troubles will be displayed.
- **Stop calls:** this action will stop and reset all the running or queued communications from the panel (phone calls, SMS and e-mails).

ADVANCED OPTIONS MENU

This menu can be reached only using a master user code.

- **Event Logger:** the events logger will be displayed, starting from the newest one. Using the ENTER key again the display will show deeper info on event.
- **Enable Mainten. :** this option will enable / disable the installer to enter maintenance.
- **Test event:** this option will generate promptly a Periodic Test Event. The running test event timer will not be modified.
- **Date time manag. :** this option can be used to set the time and date of the system.
- **Networking:** this option will show the IP communications parameters:
  - **IP address.**
  - **Address mask**.
  - **Gateway address.**
- **User management:** this option allows the master user to manage lower levels users parameters.
  - **Description:** user description can be changed.
  - **Manage codes:**
    - Enable code: enable / disable the chosen user code.
    - Change PIN: change the PIN for the selected user.
  - **Enable tags:** user tags can only be enabled or disabled.
  - **Remote control:** remote controls can only be enabled or disabled.
- **WLS alarm led:** this option will enable the red LED on every wireless device to light every time the device communicates successfully with the panel. This is very useful in order to verify the wireless network and sensors. This option will last for 10 minutes.
- **Replace LEXAN**: this option allows the user to open the ergo keypad without generating a tamper, in order to replace the LEXAN inside it. Please, refer to the ergo manual for opening and closing the keypad.

RFID TAGS OPERATIONS

The **RFID** tags behave exactly as a user PIN does: the user just needs to approach the RFID tag to the keypad reading.

Information for users: Disposal (RAEE Directive)

Warning! Do not use an ordinary dustbin to dispose of this equipment.
Used electrical and electronic equipment must be treated separately, in accordance with the relative legislation which requires the proper treatment, recovery and recycling of used electrical and electronic equipment.
Following the implementation of directives in member states, private households within the EU may return their used electrical and electronic equipment to designated collection facilities free of charge. Local retailers may also accept used products free of charge if a similar product is purchased from them.*
If used electrical or electronic equipment has batteries or accumulators, these must be disposed of separately according to local provisions.
Correct disposal of this product guarantees it undergoes the necessary treatment, recovery and recycling. This prevents any potential negative effects on both the environment and public health which may arise through the inappropriate handling of waste.

** Please contact your local authority for further details.*

Installation of these systems must be carried out strictly in accordance with the instructions described in this manual, and in compliance with the local laws and bylaws in force. this product have been designed and made with the highest standards of quality and performance adopted by Ksenia Security. Is recommended that the installed system should be completely tested at least once a month. Test procedures depends on the system configuration. Ask to the installer for the procedures to be followed. Ksenia Security srl shall not be responsible for damage arising from improper installation or maintenance by unauthorized personnel. The content of this guide can change without prior notice from KSENIA SECURITY.

ANNOTAZIONI - NOTES

DICHIARAZIONE DI CONFORMITÀ UE
UE DECLARATION OF CONFORMITY
DÉCLARATION DE CONFORMITÉ UE

Ksenia Security Srl, Strada Provinciale Valtesino, 44 – 63065 Ripatransone AP - Italia
Dichiara che / Declares that / Déclare que:

lares 4.0

KSI1400040.300 centrale lares 4.0 - 40 / Control Panel lares 4.0 - 40 / centrale d'alarme lares 4.0 - 40

è conforme ai requisiti essenziali di sicurezza delle seguenti direttive
complies with the essential safety requirements of the following CE Directives
est conforme aux exigences essentielles de sécurité des directives CE suivantes

2014/30/UE
2014/35/UE
2011/65/EU

è quindi conforme a quanto previsto dalle seguenti norme armonizzate
and therefore complies with the following harmonised standards
elle est donc conforme aux norms harmonisées suivantes

EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013; EN 50130-4:2011; EN 61000-6-3:2007+A1:2011; EN 50581:2012

Ripatransone, 15/11/2017

L'amministratore delegato
Raffaele Di Crosta

DICHIARAZIONE DI CONFORMITÀ UE
UE DECLARATION OF CONFORMITY
DÉCLARATION DE CONFORMITÉ UE

Ksenia Security Srl, Strada Provinciale Valtesino, 44 – 63065 Ripatransone AP - Italia
Dichiara che / Declares that / Déclare que:

lares 4.0 wls

KSI1410040.300	centrale lares 4.0 - 40wls / Control Panel lares 4.0 - 40wls / centrale d'alarme lares 4.0 - 40wls
KSI1410140.300	centrale lares 4.0 - 140wls / Control Panel lares 4.0 - 140wls / centrale d'alarme lares 4.0 - 140wls
KSI1410644.300	centrale lares 4.0 - 644wls / Control Panel lares 4.0 - 644wls / centrale d'alarme lares 4.0 - 644wls

è conforme ai requisiti essenziali di sicurezza delle seguenti direttive
complies with the essential safety requirements of the following CE Directives
est conforme aux exigences essentielles de sécurité des directives CE suivantes

2014/53/UE
2011/65/EU

è quindi conforme a quanto previsto dalle seguenti norme armonizzate
and therefore complies with the following harmonised standards
elle est donc conforme aux norms harmonisées suivantes

EN 60950-1:2006 + A11:2009 + A1:2010 + A12:2011 + A2:2013; EN 50130-4:2011; EN 61000-6-3:2007+A1:2011; EN 301 489-1 v2.1.1; EN 301 489-3 v1.6.1; EN 301 489-7 v1.3.1; EN 301 511 v9.0.2; EN 300 220-2 v3.1.1; EN 50581:2012

Ripatransone, 15/11/2017

L'amministratore delegato
Raffaele Di Crosta

ENVIROMENTAL CARE

lares 4.0 is designed and manufactured with the following features to reduce its environmental impact:

- No PVC
- Halogen-free laminates and lead-free PCBA
- Low consumption
- Packaging realized mainly with recycled fibers and materials

Designed and Produced in Italy

29 / 01 / 2018
RMX0300046.000
Rev.01

Ksenia
security innovation

www.kseniasecurity.com