vigilo

KSI7810050.000 • KSI7810500.000
KSI7810050.001 • KSI7810500.001

ALARM RECEIVING AND CENTRALIZING SOFTWARE
PROGRAMMATION MANUAL

INDEX

INTRODUCTION

vigilo is alarm receiving and centralizing software by Ksenia Security.
Thanks to the enormous opportunities offered by their **lares IP** Panels that connect directly to the network without need for additional transmission devices, or to **gemino** GSM/GPRS Communicator series, the next logical step is to allow, for example, General Headquarters of a credit institute to centralize contemporarily a very significant number of security systems as well as to allow selected Ksenia installers to offer new and important value-added services to its customers (*for example maintenance contracts with planned intervention or depending of system operating conditions*).
vigilo provides three access levels (*Installer, operator, customer*) and doesn't need any application: just open an internet browser and connect to the IP address of the machine on which it is installed to display the systems status, so it works with all operating systems and also with tablet Android or MAC-OS. The **vigilo** SW (*not to be confused with the supervisory SW*) is designed to be very simple, self-explanatory but still able to receive any events from connected systems. The number of such systems is limited to 50 in the case of the basic version and can reach up to 500 in **vigilo pro** version (*Professional*).

TECHNICAL DATA

CPU / Intel® Atom™ D525 1.8GHz
CPU Cache / 1024 KB
RAM / 2048 MB DDR3-800 So-DIMM
Mass storage / Hard Disk 320 GB SATA 2.5''
Graphic board / 512 MB NVIDIA® ION™ 2
LAN / Built-in Ethernet board with 10/100/1000 Mbps support
Wi-Fi / Built-in Wi-Fi board with IEEE 802.11 b/g/n support
I/O / VGA - HDMI - RJ45 - 4 USB 2.0 input - Audio input - Line-Out output
Power Supply / AC 100 ~ 240V 50/60Hz - 19v ~ 3,42A 65W
Monitor / supplied separately
Keyboard/Mouse / supplied separately
Dimensions / 19,3 x 14,8 x 2,2 cm (W x H x D)
Weight / 530 g.

Technical specifications, appearance, functions and other product characteristics may change without notice.

ASSISTANCE ON VIGILO SOFTWARE

For assistance regarding the software please send an e-mail to the following address:

vigilo@kseniasecurity.com

An answer will be sent within 24 hours.
The body of the email must contains the serial number of the hardware in which the vigilo software is installed. You can find the serial number on the label mounted on device.

FIRST POWER UP

1. Turn on the PC

2. The machine is supplied with the following network settings:
   IP Address:.....192.168.2.93
   Subnet Mask:.....255.255.255.0
   Gateway:.....192.168.2.1
   Dns1:.....8.8.8.8
   Dns2:.....8.8.4.4

3. Configure your network settings. This allows to use a cable (not necessarily a crossover cable) to exactly connect to the machine.

4. Do a test of the machine by running a ping 192.168.2.93 on a command shell.

5. Open a browser and type the following url on the address bar: **http://192.168.2.93**

6. The following screen is shown, as software activation screen

7. After the software activation, it access to the login page.

IMPORTANT:
To change the network settings, in order to use the vigilo in pre-existing network, please use the '**Utility menu**' (*see following pages*)

Connect your own PC to the same Net as the **vigilo**, configuring the proper settings.
Type the following url on the address bar: **http://192.168.2.93/csr**
The following page is shown:

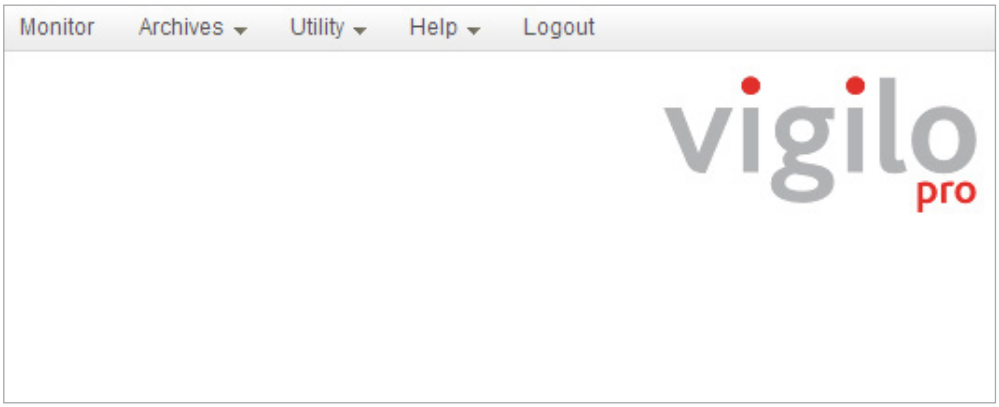
This is the login page. You can the software language and the kind of user.

At the first start just one admin user is pre-configured: **admin/admin**
For safety reasons, at the first start it is highly recommended to create a new 'Installer' user and then delete the default one.

No customer and no operator users are pre-configured at the first start.

Please insert the following parameters to login:
language: english
UserName: admin
Password: admin

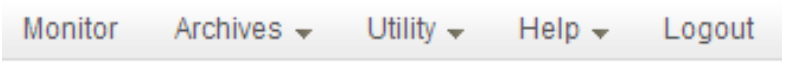
After login, the following page is shown:



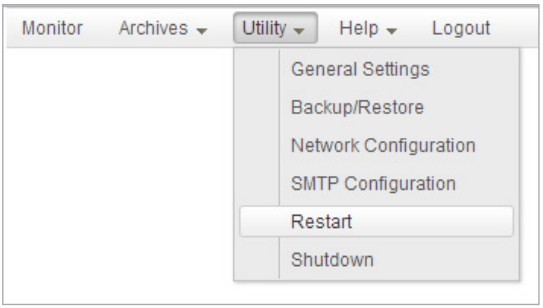
SOFTWARE

vigilo has 3 user levels: **INSTALLER | OPERATOR | CUSTOMER**

CUSTOMER and OPERATOR levels have less rights and less menu voices than the INSTALLER level, so from here in advance the full options will be presented (*INSTALLER level*).

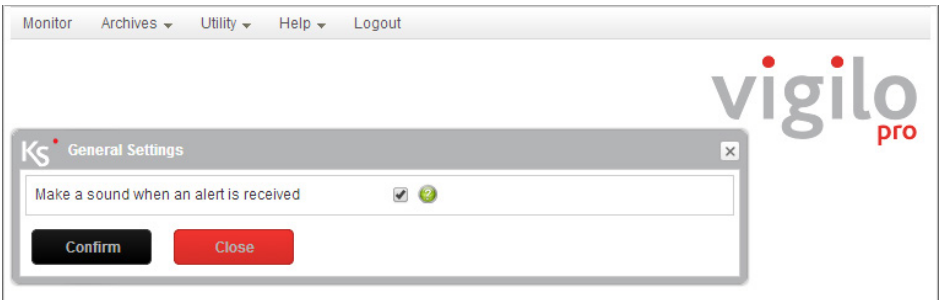


UTILITY MENU



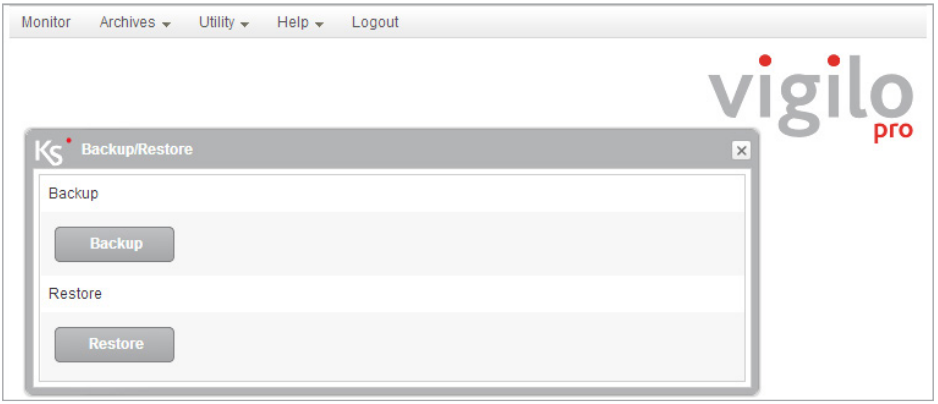
In this section there are utilities for interacting with the vigilo hardware

MAIN SETTINGS



By enabling this option, the PC connected on software monitor issues an acoustic alert when an alert event occurs (*enabled by default*).

BACKUP / RESTORE

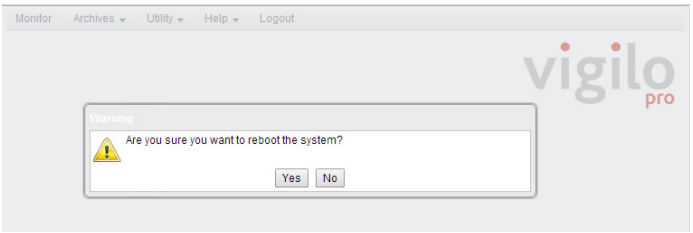


It is possible to backup the database, using the first key. The file created will be named:

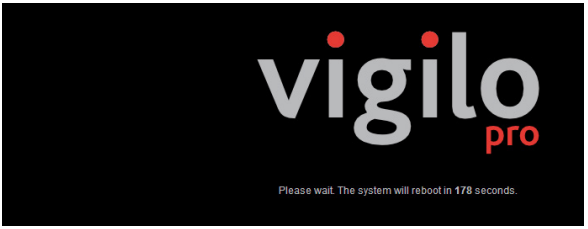
vigilo_dateHour.bak

Using the second key it it possible to restore a backup previously created.

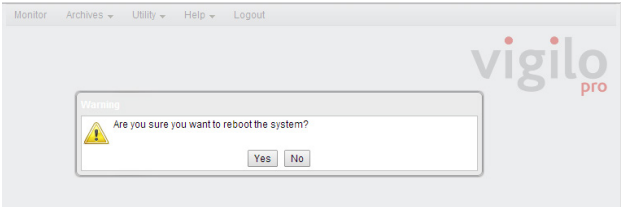
RESTART
This command will prompt the following page and then will re-boot the PC.



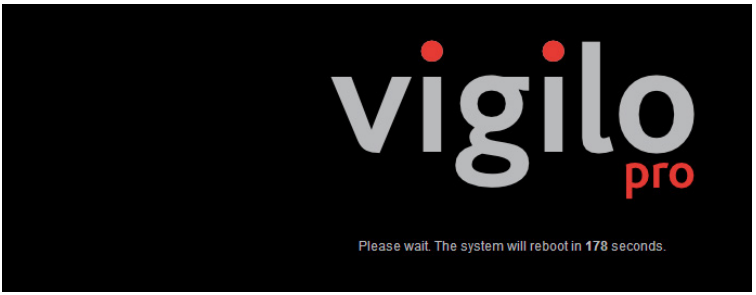
After answering '**Yes**' the following screen will be shown, and the PC will re-boot.



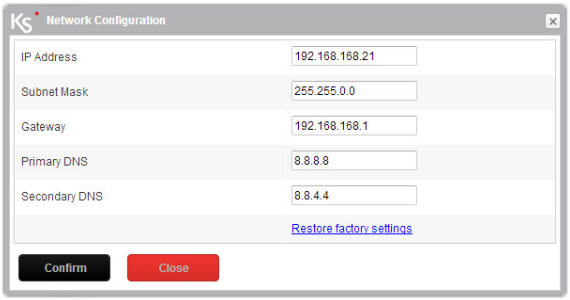
SHUTDOWN
This command will switch off the PC. The following question will be prompted:



After answering '**Yes**' the following screen will be shown, and the PC will switch off.

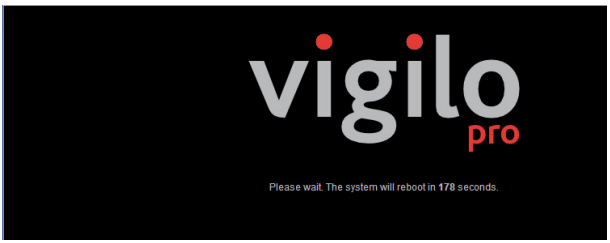


NETWORK CONFIGURATION
Here the network setting of the host PC can be configured. This is the configuration prompt:



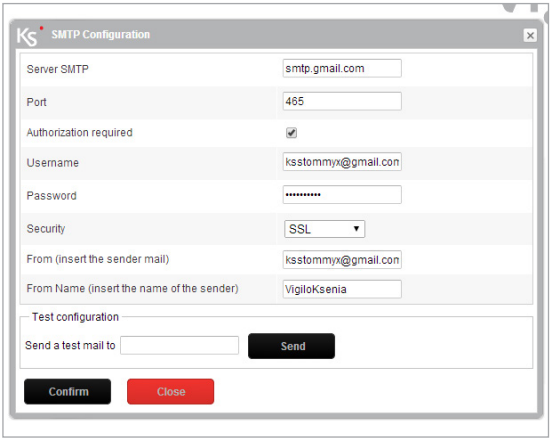
IMPORTANT
By selecting '**Restore factory data**' the default network configurations will be restored (*see page 3*)

After checking '**Confirm**' the following page with a progress timer will be shown, and the host PC will re-boot.



When the timer expires, the browser will be re-directed to the new network address.

SMTP SETTINGS

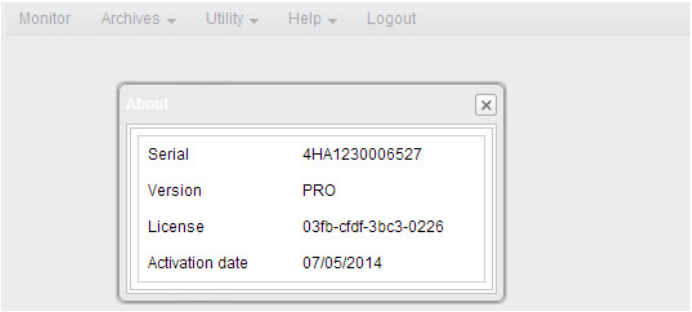


SMTP Server / server from which **vigilo** will send e-mails
Port / SMTP server port
Authorization required / selecting this option it needs user/psw to send e-mails
Username / username used by **vigilo** to send e-mails
Password / account password used by **vigilo** to send e-mails
Security / kind of security used to send e-mails
From / insert the sender mail address.
From Name / name displayed to the receiver.

Note: there is a test section on which it is possible to set a test receiver to check if configurations are correct

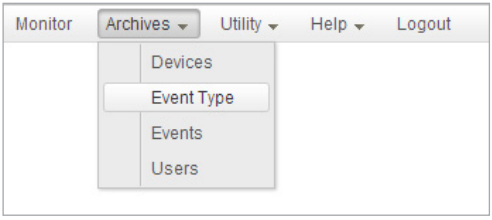
HELP MENU

INFORMATIONS



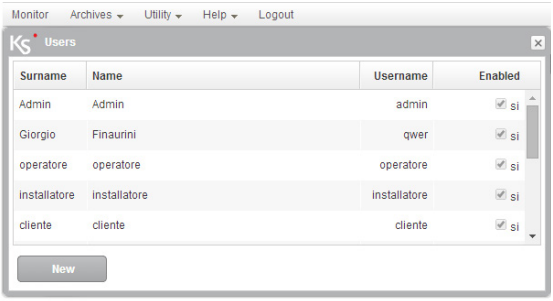
On this section, the following informations are available:
Serial / serial number of the PC on which **vigilo** is installed.
Version / Pro or Standard (*that is 500 or 50 devices*).
Licence / Software licence code.
Activation date / date of the first login, start of warranty and assistance

ARCHIVES MENU



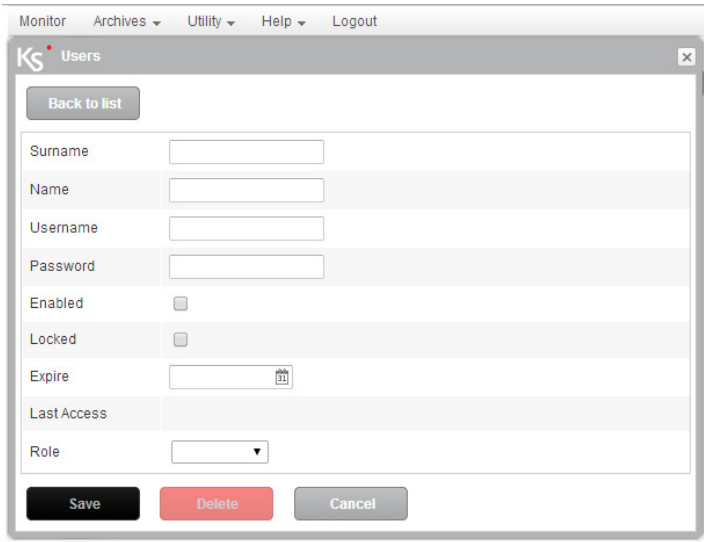
USER MANAGEMENT

By checking 'Users' the following page is shown:



NEW USER

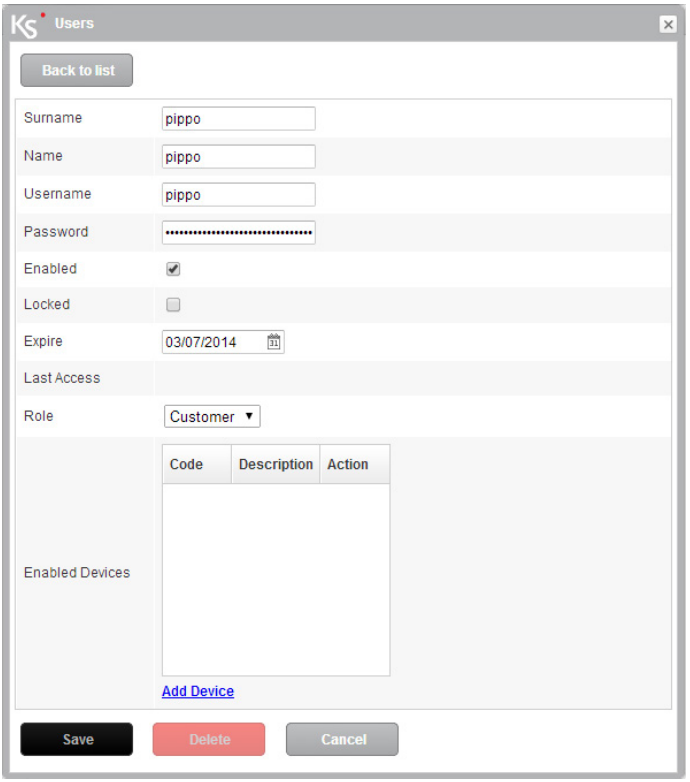
In order to create a brand new user, check '**New**'. The following page is shown:



Enabled: Enables user
Locked: Blocks user
Expire: insert a date after which this user will be locked
Role: **Installer** / this user can manage system sensible data, that is to manage 'Archives' section. Moreover, it can check/acquire all alerts/events from all panels in system.

Operator / this user can check/acquire all alerts/events from all panels in system
Customer / this user can only check/acquire alerts/events from the panels connected to him

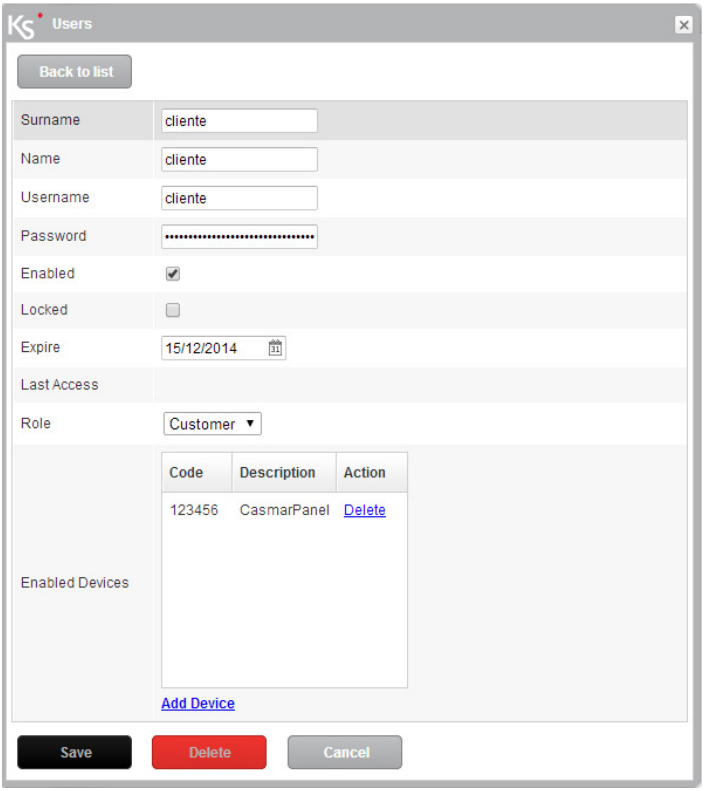
'CUSTOMER' USER



In addition to the data for all other users, there is the '**Enabled Devices**' section, on which it is possible to insert all the Panels connected to this user.

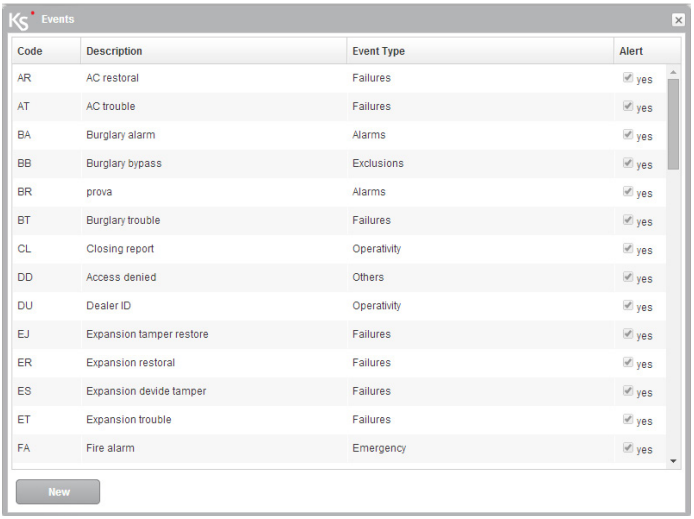
EDIT USER

In order to edit one of the users, just click on its row on table. The following page is shown:



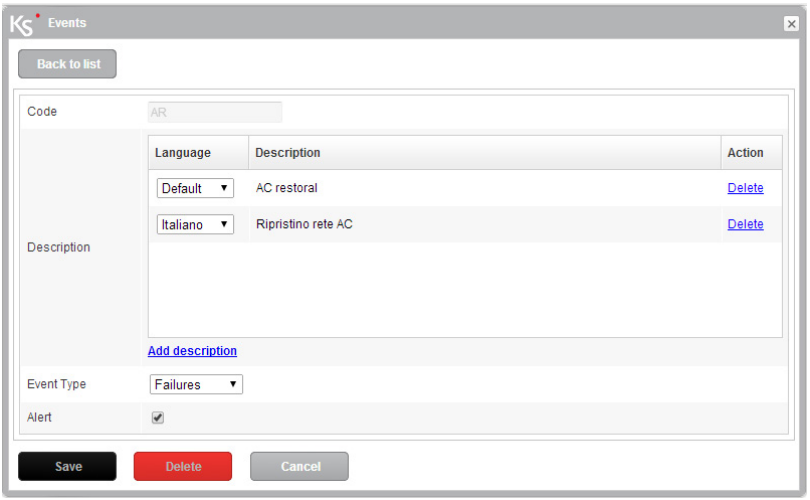
EVENTS MANAGEMENT

In order to manage events, click on **'Events'**. The following page is show:



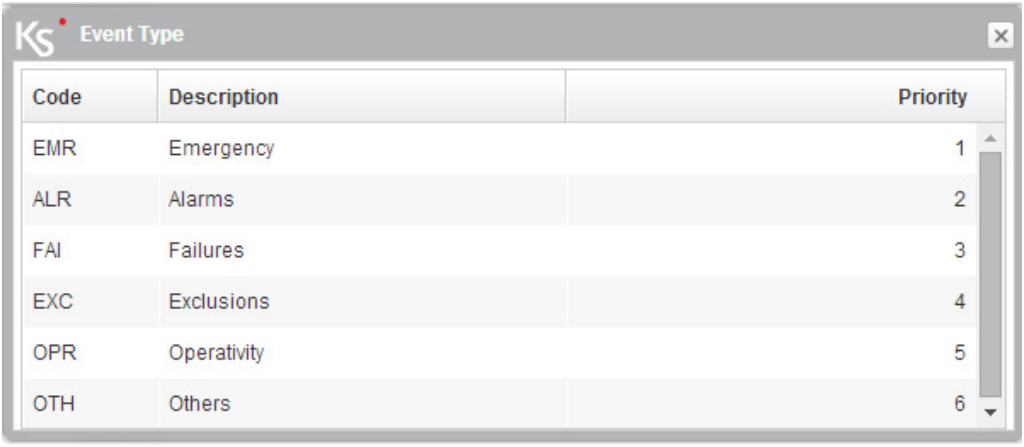
On this page, all the events generated by Ksenia Panels by default are displayed. It is possible to modify single events or to create new ones. Obviously, new events are needed only if custom events are programmed on **lares** panels.

Regardless the kind of events, the following page is shown:

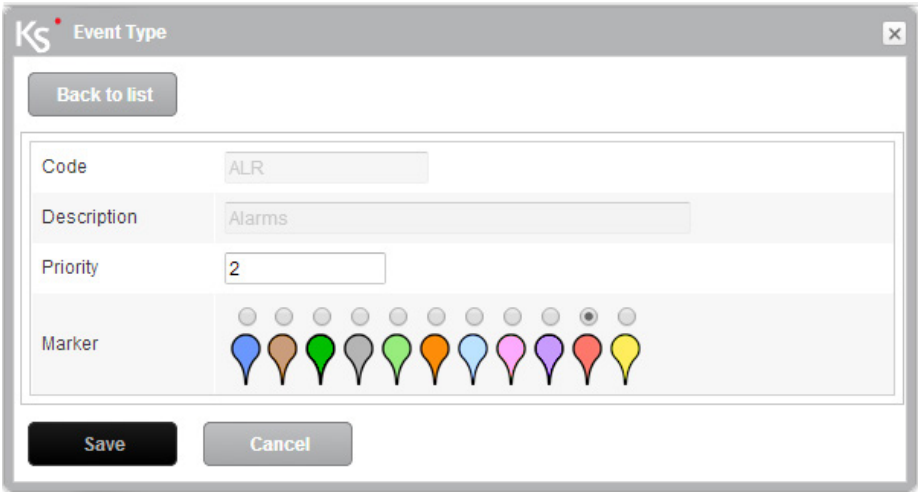


Code / event code.
Description / event description
Event Type / select a kind of event (*the different available events are displayed on the following 'Kind of Events' section*)
Alert / this flag allows the event to be displayed on '**Alert**' section and on the log map

EVENTS CLASS MANAGEMENT
Select '**Event Type**' to manage it. The following page is shown:

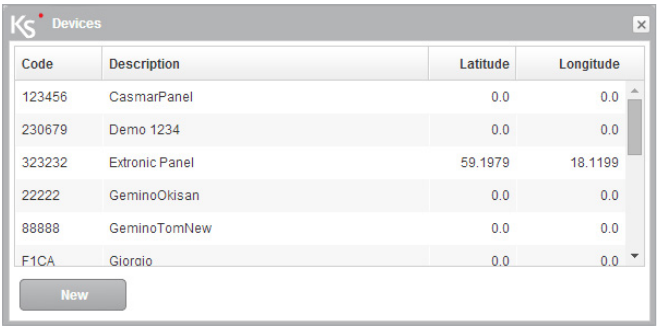


In this case, the types of events are only editable. Once pressing on a row, the following page is shown:



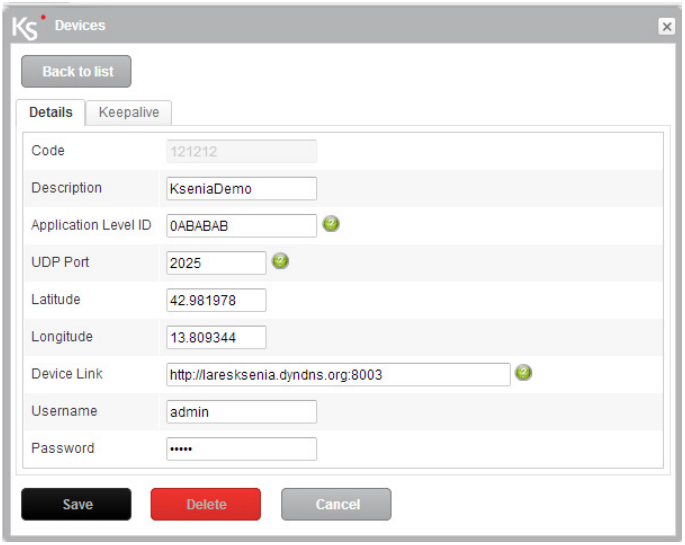
Priority / numeric value associated with a tipe of events. It is used to manage the order of appaerence of marker on '**Map Log**' section.
Marker / marker displayed on '**Map Log**' section at the occourring of an event that belongs to a specific type

DEVICE MANAGEMENT
Select '**Devices**' to manage it. The following page is shown:



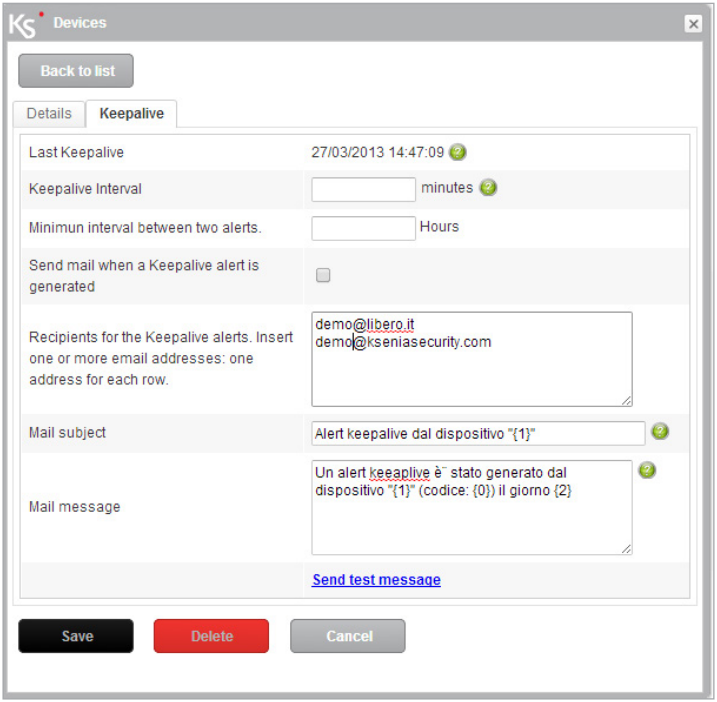
On this page, the devices present on system are displayed (*Panels and Communicators*). It is possible to modify the present devices or create new ones. In both cases, the following page is displayed:

DETAIL SECTION



Code / this code identifies the Panel in an univocal way on system.
Application Level ID / this code identifies the Panel in an univocal way on application layer
UDP Port / indicates the UDP port in which the devices receives the ACK message. If empty, **vigilo** sends the answer to the port from wich the data packet is arrived.
Device Link / link to the Panel web server.
Username/Password / credits to access the web server

KEEPALIVE SECTION



Last Keepalive / This indicates the date/hour on which the last Keepalive signal is received

Keepalive Interval / This indicates the maximum interval that has to intervene between a Keepalive signal and another. If more than this interval intervenes, a 'Missing Keepalive' signal is generated. This event is repetitively generated until a new Keepalive signal is received. To disable this check, leave the empty field.

Send mail when a Keepalive event is generated / this enables to send mails when the supervision fails

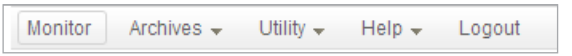
Minimum interval between two alerts / minimum time that has to lapse before a new KAE (*KeepAliveEvent*) is generated by vigilo.

Recipient for the Keepalive alerts / receivers of the alert mails about failed supervision from the selected device. Please insert only one receiver per row.

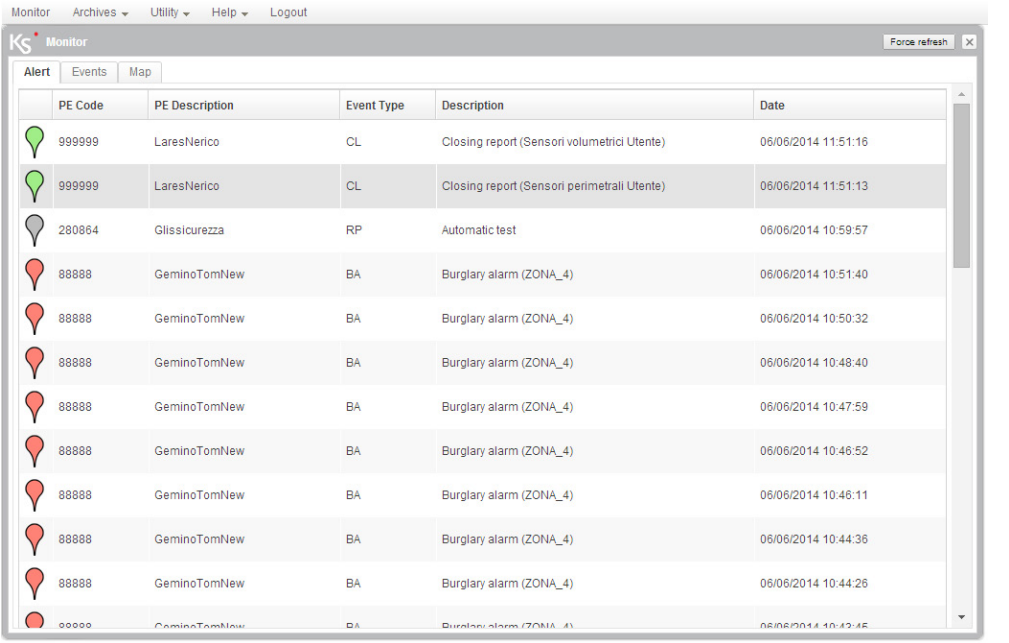
Mail subject / this text will be the mail 'Object'. It possible to use the following placeholder: {0} for device code, {1} for device description, {2} for date/hour of event

Mail Message / this text will be the 'body' of the mail. It possible to use the following placeholder: {0} for device code, {1} for device description, {2} for date/hour of event

By clicking on '**Send test message**' is forced the sending of a mail that simulates a failed supervision.

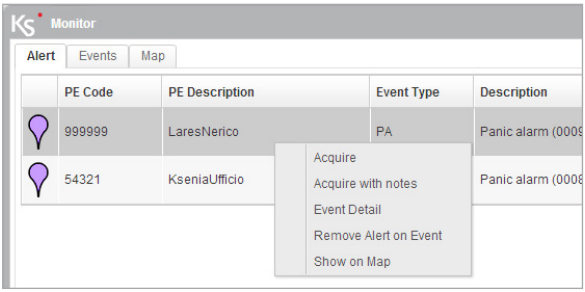


By selecting this option, the following page is shown:



On this page, there are 3 tabs. Let's see in detail: **Alert** | **Events** | **Map**

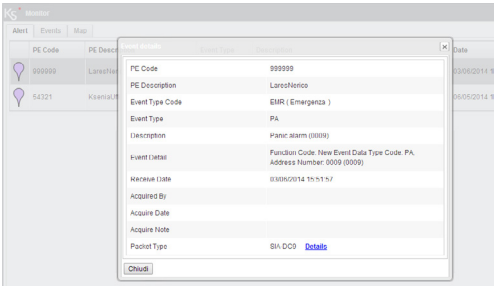
ALERT
On Alert page, all the alerts generated by monitored Panels are reported. All the events that have the '**Alert**' flag ON are reported in here (*see events detail*).



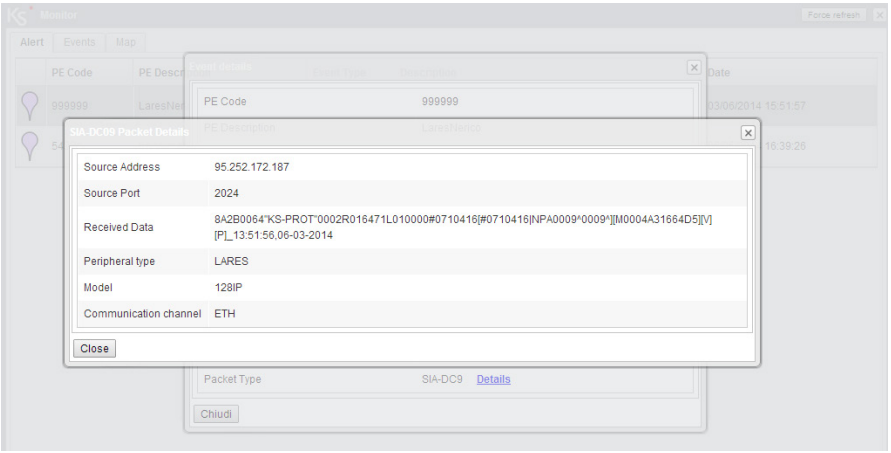
As shown over here, by right-clicking on a selected alert, it appears a window that shows the performable actions.

Acquire/Acquire with notes / This option moves the selected alert in the events page. Moreover, by 'Acquire with notes' it appears a window on which write acquiring notes.

Event detail / it appears a window on wich event details are reported. An example of this window is shown here below:



By selecting 'Details' it appears the window here below, regarding the received packet



The following informations are available on this section:

Source Address / IP address from which arrives the data packet.
Source Port / UDP port from which the data packet is sent.
Received Data / packet launched from the source device.
Peripheral Type / that identifies the device that sent the signalisation. It could be:
• lares
• gemino

Model / device version. It could be: 16 / 16IP / 48 / 48IP / 128IP / in case of **lares**.
expandable / 4 inputs / in case of **gemino**.

Communication channel / the channel used to send signalisations from the device. It could be:

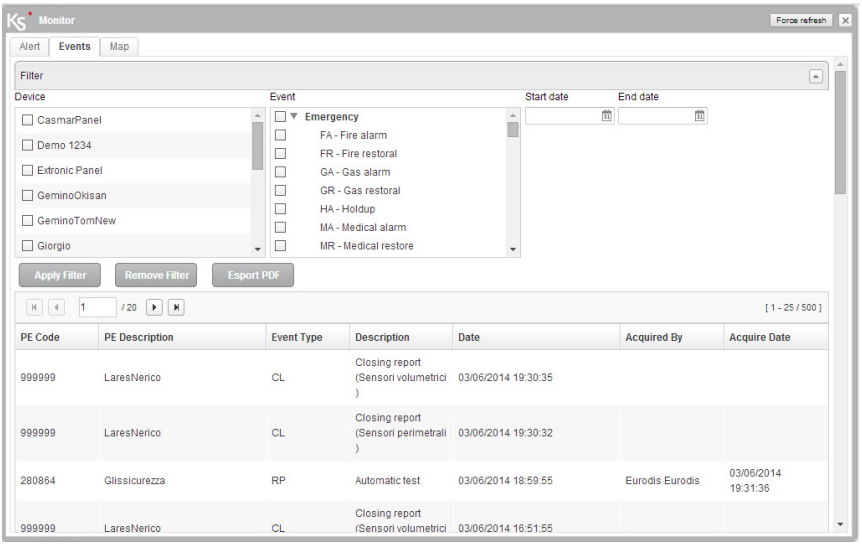
lares 16 / 48	GPRS (*using gemino BUS*)
lares 16IP / 48IP / 128IP	GPRS / Ethernet
gemino exp. / gemino4	GPRS only

EVENTS

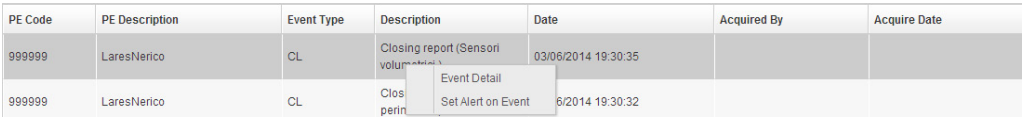
On this page, all the events of all the Panels on system are reported. It is possible to filter events by:

Device | **Event** | **Time interval**

and their combinations.



Once applied the filter, it is possible to create a .pdf file on which the results of filtering are reported. Considering a single event, it is possible to proceed as follow:



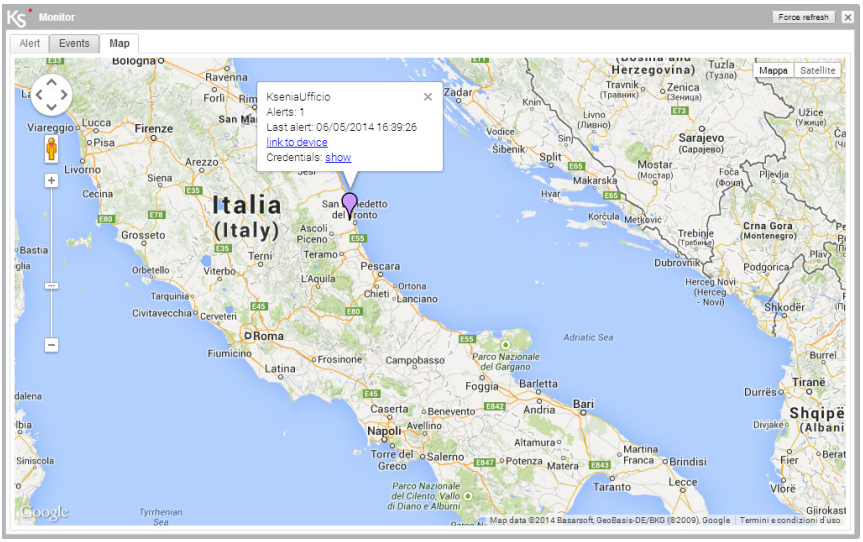
so:
Event detail / It appears a window on which is reported the details of event, as the alerts.

Set alert on event / it allows to enable the 'Alert' flag on the selected event, both for the current Panel and for them all.

MONITOR MENU

MAP

On this page all alerts from all Panels on system are reported.

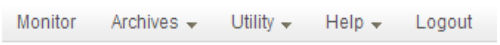


By clicking on markers on map, the following informations are available:

1. Panel description
2. Number of occurred events
3. Date/Hour of the last event
4. Link to the web server of the Panel

It is also possible to reach this page through the event page by clicking on '**Show on map**' option

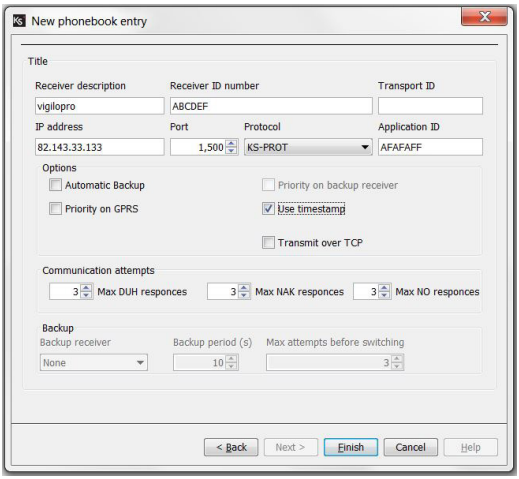
LOGOUT MENU



To correctly logout.

CREATE AN IP RECEIVER

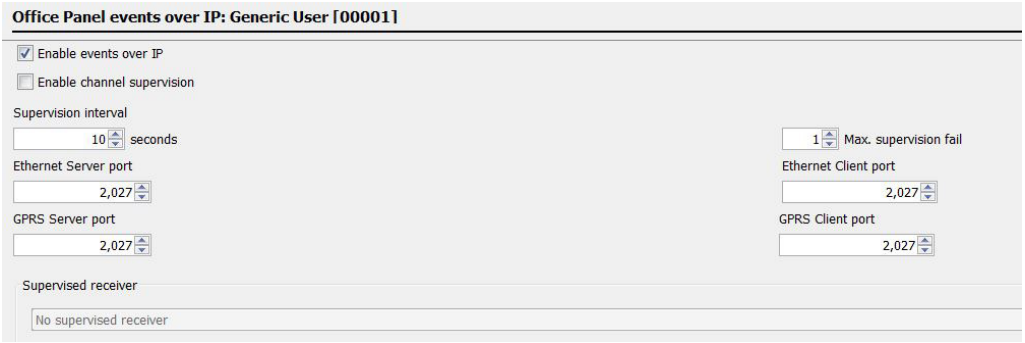
In order to create a new receiver, browse toward the phonebook and create an '**IP receiver**' contact.



Receiver description / the description of receiver
Receiver ID number / this identifies the receiver (*optional, not used by **vigilo***).
Transport ID / this identifies the Panel on Transport level (*optional, not used by **vigilo***).
IP address / address of public server on which **vigilo** is installed.
Port / port on which the receiver is listening - **fixed value: 1500**
In this particular case it been done a portmapping on router on which **vigilo** is installed. All UDP traffic on 1500 external port of router is re-direct toward the 1500 internal port of IP address 192.168.x.x that has to be the sub-net address on which **vigilo** sw is installed.
Protocol / KS-PROT - Ksenia propretary protocol, applicative level, incapsulated in the SIA-DC09 trasport protocol
Application ID / this identifies the protocol incapsulated in the DC-SIA09
(*this value is provided by the **vigilo** provider*)
Options / Automatic Backup: this activates the backup of receiver. In order to interface it with **vigilo** receivers, please flag 'Use timestamp'
Proirity on backup receiver / the backup receiver is prioritary than the selected one
Proirity on GPRS / This enables priority on GPRS channel.
Use timestamp / This enables to send data and hour in milliseconds
Transmit over TCP / This enables TCP communication protocol towards the receiver
Communication attemps / Max DUH responces / number of attempts after DUH reply from receiver
Max NAK responces / number of attempts after NAK reply from receiver
Max NO responces / attempts after NO responces from receiver

BackUp / Backup receiver / description of backup receiver
Backup periond (s) / period during which the backup receiver is used
Max attemps before switching / communication attempts towards the main receiver before sending signals to the backup receiver

EVENTS OVER IP



Enable events over IP / This enables signalisations over IP (*to flag*)

Enable supervision / This enables the supervision toward the supervision receiver

Supervision interval / The interval between a supervision signalisation and another.

Max supervision fail / number of failed supervision after which the Panel generates the 'Failed Supervision' event

Ethernet server port / port used by the Panel **to receive** answers from receivers on Ethernet channel

Ethernet client port / port used by the Panel **to send** answers from receivers on Ethernet channel

These ports are set with the same value, to make it easier. In this specific case this value is 2027. In case these are different, it is necessary to make a portmapping on the LAN router on which **vigilo** is installed: all the UDP traffic arriving on the 2027 external port has to be re-direct toward the 2027 internal port of 192.168.x.x IP address that has to be the sub-net address of **lares**

In the same way, using **gemino BUS** for sending signalisations, it is necessary to assign a value to the client/server GPRS ports that should be (*at least the server one*) the same as the Ethernet ports.

GPRS server port / this port is used by the Panel **to receive** answers from receiver on GPRS channel.

GPRS client port / this port is used by the Panel **to send** answers from receiver on GPRS channel.

Supervised receiver / This identifies the receiver toward which it sends supervision signalisations

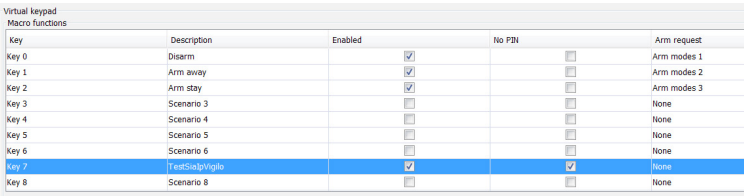
INSERT A PANEL ON VIGILO DATABASE

The main parameters are described here below:

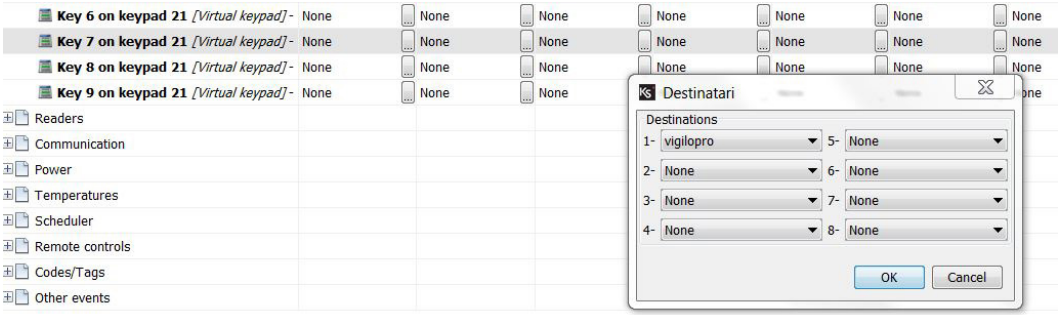
- Application level ID / the configured ID previously used to create the IP receiver on **lares** phonebook
- UDP port: port toward which **vigilo** sends send the answer to the received signalisation. This value has to be the same as the one configured on '**Ethernet server port**' (*or, respectively, on 'GPRS server port'*)

- EXAMPLE - CONFIGURATION TO SEND A TEST EVENT

How to insert a scenario on the virtual keyboard in order to test the sending of signalisation to **vigilo**



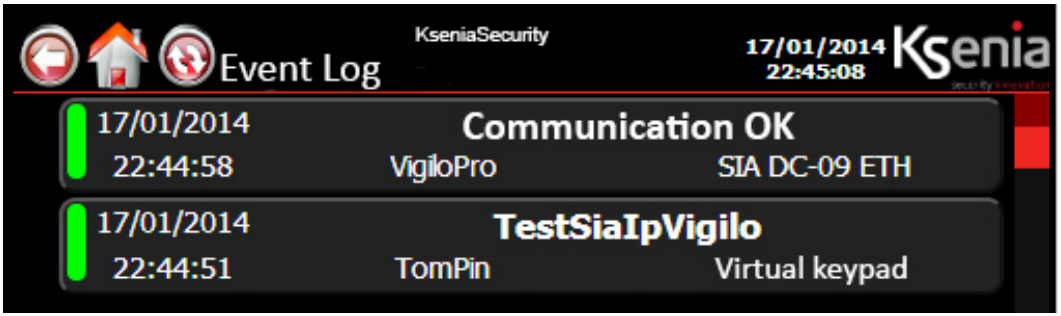
1. Enables the key 7 (*for example*) on virtual keyboard without PIN and arming modes.
2. On scenarios page, add **vigilo** as recipient to the 'Key on virtual keyboard' event



3. Send the variations to the Panel

4. At Panel restart, access to the web server, go to the scenarios section and run the '**TestSiaIpVigilo**' scenario.

5. On 'Events' section the test result is shown



NETWORK CONFIGURATIONS

VIGILO HARDWARE CONFIGURATION
In order to reach the **vigilo** hardware is necessary to:
1. Externally associate the machine to a static IP address
2. Perform the following portmapping / port re-directing

Supposing that **vigilo** has 192.168.1.156 address:

Description	Internal Address	Internal Port	External port	Protocol
VigiloWeb	192.168.1.156	80	8080	TCP
VigiloUdp	192.168.1.156	1500	1500	UDP
VigiloAssRem	192.168.1.156	22	2222	TCP

Obviously these configurations on router could be different depending on different devices

PANEL CONFIGURATION
In order to obtain the answers from **vigilo** sw, the following portmapping / port re-directing are necessary on Panel:

Supposing that **vigilo** has 192.168.1.200 address
and is expecting answers on 2027 port:

Description	Internal Address	Internal Port	External port	Protocol
LaresVigiloUdp	192.168.1.200	2027	2027	UDP

Obviously these configurations on router could be different depending on different devices

RESET NETWORK CONFIGURATIONS

In order to reset the network configurations, please proceed as follow:
1. Turn OFF the PC
2. Connect the **ergo** keypad
3. Connect the monitor
4. Wait until the following screen appears, doing nothing:
   'Press 's' to restore default network settings...'
5. A countdown will starts, displayed after the dots. Press 's' before it expires.
   Note: in case the countdown is expired, press Ctrl+C to restart it
6. By pressing 's' it will appear the following message:
   'Configuration restored, wait 60 seconds while system applies configuration'

CERTIFICATIONS

The complete Declaration of Conformity for each Device can be found at: www.kseniasecurity.com

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 device has 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.

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.

05 / 06 / 2014
RMX0300018.001