Phoenix-4

Operating Manual

ORTUS Group

Table of contents

1. General information

Nowadays, security has become an integral part of the functioning of institutions and organizations with a variety of activities, including enterprises with private property. The main purpose of safety provision is to prevent both intentional and unintentional acts and accidents, disturbing its operation, or to reduce the damage caused by them.

The security is provided by the security services: either those on the staff of institutions or organizations, or those providing their services on a paid basis.

Requirements to the level of security constantly grow, which obviously determines the need for extensive use of automation equipment, integrating the organizational and technical resources to address these problems.

The monitoring of objects using the remote central monitoring station is an important part of ensuring the security of protected objects. This station may include "Orlan" modules connected to the computer to receive message via GSM channel. The computer is "Phoenix-4" software-based.

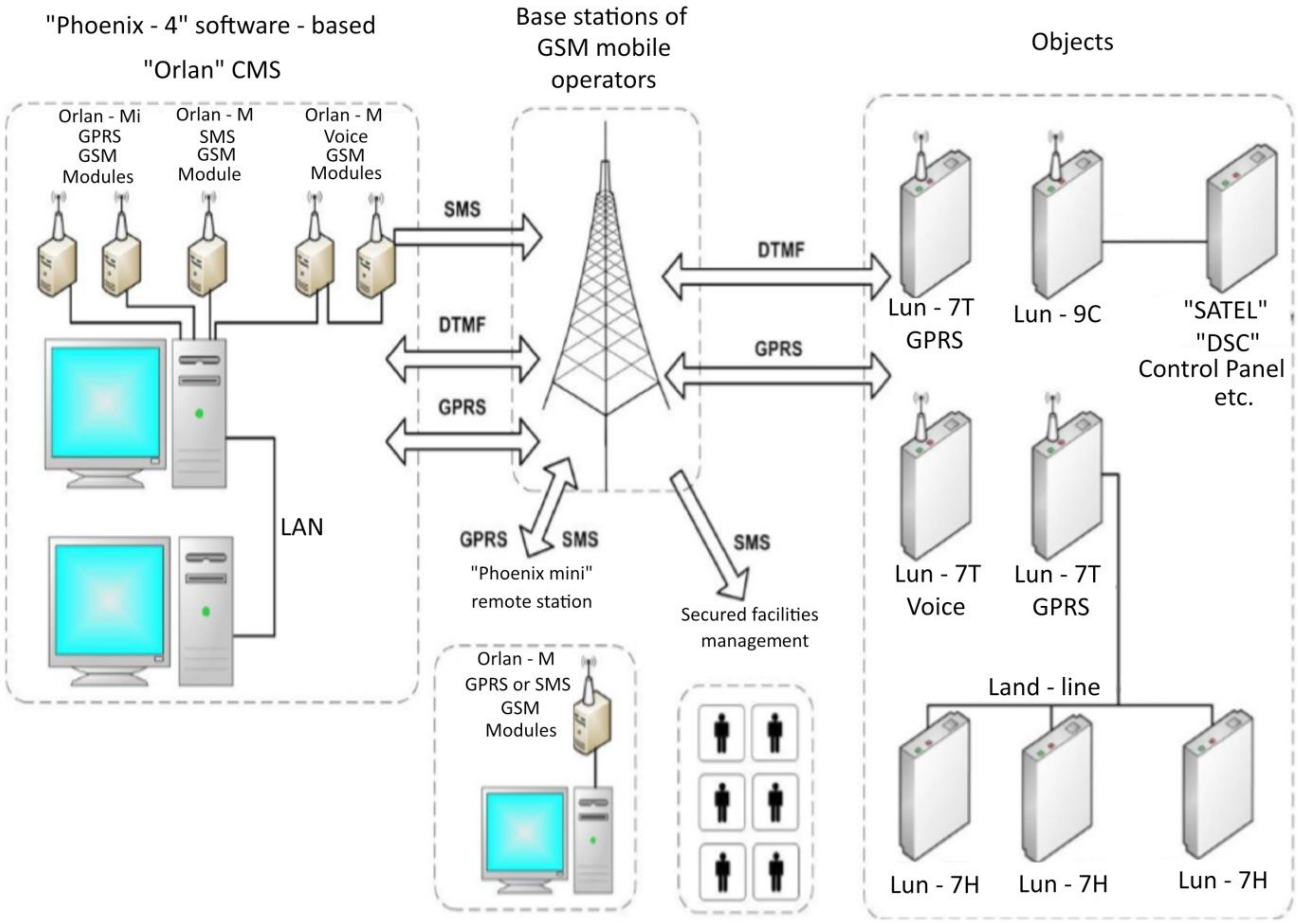


Figure 1. "Orlan" CMS structure diagram

"Phoenix-4" software is of new generation of the software for central monitoring stations. The structure diagram of central monitoring station is given in Figure above. "Phoenix 4" is constantly improving, and its can be downloaded at our website.

1.1. "Phoenix 4" brief description

- Message reception from external sources with accompanying sound and visual tracking, interpretation and processing.
- The Microsoft SQL Server 2012 SP3 database is used. It provides a client-server software architecture with extreme flexibility of central monitoring station maintenance.
- Received messages filing.
- Monitoring of the object status, instant change of their status on the reception of a message from the object, which is a good monitoring tool for remote operators.
- Storage and display of driveways and layout of objects, different schemes.
- Storage of information in the form of text description of objects, numbers of access codes, events and their decryption, zone descriptions.
- Possibility of splitting of an object into groups and tracking of information separately for each group of the object, possibility of setting the schedule for each of the groups and control over opening of the groups in accordance with this schedule.
- Printing of objects databases, event archives.
- Display of a list of armed and disarmed objects, of objects with arming schedule violated for some reason, objects with testing schedule violated, as well as a list of objects for which you shall change the batteries in case of using of wireless sensors.
- Archive search by various criteria: number of object, event code, protocol, date and time, etc.
- Possibility to make an object (or a zone) as a temporary or permanent stand (indicating the time interval), in which all coming events are auto-restoring, that is accepted without an operator.
- Logging of time of arrival of the response team to the object upon alarm.
- Special mention should go to the extreme flexibility of system configuration. For example, it is possible to physically connect the receivers to one computer, at the same time, the program runs for operators on another computer, while the database itself can be on the third one. However, that is not all, the station engineer can use the fourth computer and database editor can use the fifth one. In addition to workability, it also leads to the high fail safety of the whole system.
- Monitoring of the test mode of object protection devices. You can specify the test interval for each security device, and the program will monitor them strictly at the specified time interval. If the device was not tested within this interval, the relevant information goes to "Not tested in time" list, and an event of testing time violation is generated.
- Operators registration.
- Automatic unattended backup of the database with the provision of an operation report to the operator.
- Export of an archive to MS-Excel format.
- Analysis and construction of charts and reports on the monthly operation of station.
- Backing-up of all events from the object to a mobile phone of the owner in the form of SMS, as well as to the application for Android and iOS-based mobile phones.
- Smart "Alarm Analysis" – for tracking of false alarms, restarts, connection quality. It is a table with a list of objects and events for the whole month, for each day that allows you to visualize the problematic objects, which give false alarms, or those with the poor quality of connection, etc.

The basic computer specification to operate with "Phoenix 4" software see in the table below.

Parameter	Minimum value	Recommended value
Processor	Intel Core i3 (2 cores)	Intel Core i5 (4 cores or more)
RAM capacity, GB	8	16 or more
HDD free space, GB	64	128
Monitor	1600x900	1600x900 or more
Operation system	MS Windows 7 Pro, Windows 8.1, Windows 10, Windows Server 2008R2 SP1	MS Windows 7 Pro, Windows 8.1, Windows 10, Windows Server 2008R2 SP1
Network card	Ethernet 100Mbit	Ethernet 100Mbit
USB ports, minimum	USB 2.0 compliant, 6 pcs	USB 2.0 compliant, 6 pcs

1.2. Structure of “Phoenix-4” software

"Phoenix 4" consists of multiple programs that intercommunicate (see Figure 2):

- "**DB Administrator**" – program for creation and editing of the station database.
- "**Control Center**" – driver for all CMS receivers, as well as the processing centre of all other CMS software commands. It shall always run to ensure the operation of the whole complex of programs. After running, the program icon appears at the bottom of the task panel as  .
- "**Duty Operator**" – program that provides the reception and processing of events from object devices. Using this program, the operator can remotely control the object devices.
- "**Configurator**" – program for configuring of “Lun” Control Panels. It can be installed on any computer by copying from the disk.
- "**Configurator 11**" – program for configuring of "Lun-11" series Control Panels.

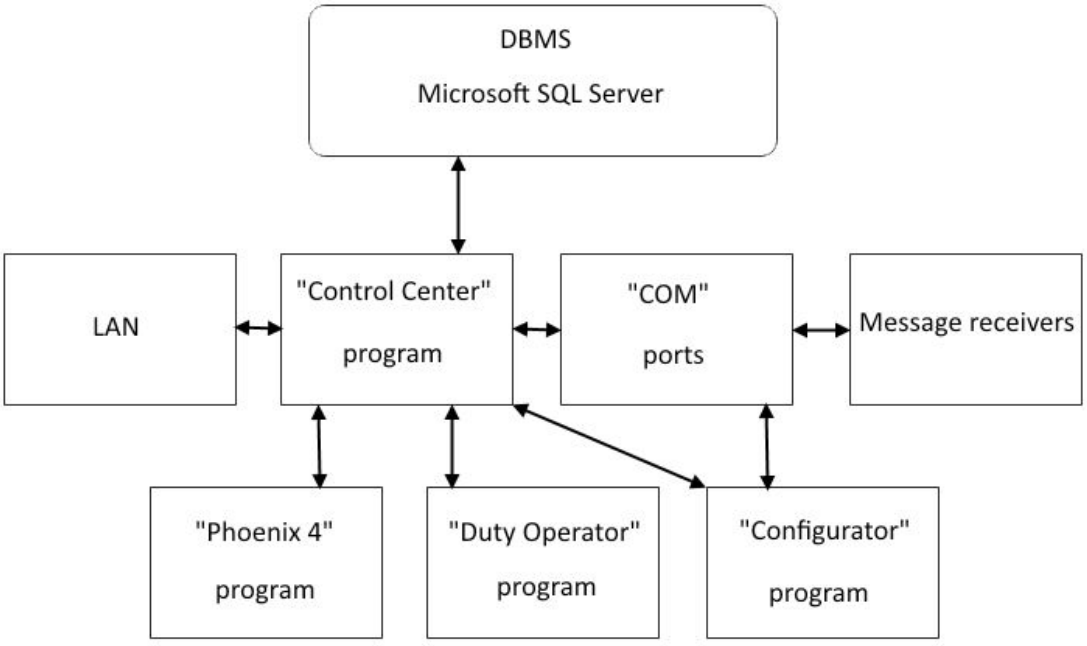


Figure 2."Phoenix-4" software structure

Next programs is used for configuring of the station and object equipment:

- "**GPRS connection configuration**" – to make an Internet connection configuration (installed on the station computer by default).

- "**DB Backup**" – to configure an automatic database backup (installed on the station computer by default).
- "**DB Recovery**" – to recovery the database from backup archive (installed on the station computer by default).
- "**Archive Data Deletion**" – to delete old database backups.
- "**Creating of DB for Android**" – to create a database for “Phoenix Mobile 4” Android application.
- "**FM4Server**" – it provides data exchange with “Phoenix Mobile 4” Android application. "Control Center" does not directly support tablets, but uses this program to communicate with tablets. This program should be running if the “Phoenix Mobile 4” application is used.

All programs you can find in the **Start** menu as shown in the Figure 3.

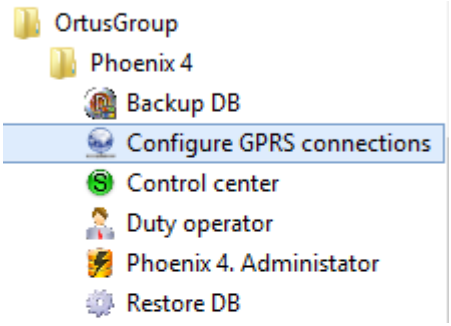


Figure 3. "Phoenix-4" software in the Start menu

"Control Center" program permanently exchanges data with “Orlan” modules and auto-redials receiving stations. In case the modules have received an event, it is read, decoded, archived and put in a new events buffer, after which it informs "Duty Operator" program of it under using TCP/IP protocol, that is why TCP/IP protocol shall be enabled on computers with Phoenix 4 (in Windows 2000 / XP and above it is enabled by default). In addition, "Control Center" program provides the operation of "Configurator" program in the mode of remote configuration of "Lun" GPRS object devices of the seventh and ninth series.

The database is stored on a computer with Microsoft SQL Server 2008 Database Management System (DBMS), which is reliable and fast, that is why "Phoenix 4" software has a network client-server architecture. In other words, it is possible to access to the entire database from any computer in the network. For example, the database is installed on a computer, which is also a computer working station of CMS operator.

The database can be edited from another computer connected to the first one over the network; it is very convenient, as in this case, the monitoring station operators are not distracted. Moreover, to facilitate the work of CMS operator when a large number of objects are secured, it is advisable to connect one more computer to the receiver over the network to offload the first computer in this way. Moreover, “Orlan” modules and auto redial call-receiving stations can be connected to a computer other than that, where the database and “Duty Operator” program are installed.

2. Receiving equipment – installation and configuration

"Orlan" CMS consists of “Orlan-M11” board-based "Orlan-M" modules (with batteries connected) that support voice operation mode, "Orlan-Mi” modules that support GPRS operation mode, and "Orlan SMS” modules that support SMS sending and receiving mode.

An integral part of "Orlan" CMS is a computer with "Phoenix 4” software package, which provides the registration, storage and processing of the coded messages. "Orlan" CMS is divided into packages: basic and upgrade.

"Orlan" CMS basic package. The basic package of "Orlan" CMS consists of two "Orlan-M" modules (with batteries connected) that support voice operation mode, 2 Nokia AC-6E power source with micro USB connectors, a set of cables (see Passport) and "Phoenix-4" software package. The basic package of "Orlan" CMS can operate with 300 to 350 "Lun" object devices.

2.1. “Orlan-M” voice modules

“Orlan” CMS voice upgrade package” consists of two "Orlan-M" modules that support the voice operation mode, and “Phoenix 4”Service Pack. The technical characteristics, installation procedure and connection of the modules fully comply with the characteristics of the "Basic “Orlan” CMS package”.

“Orlan” CMS voice upgrade package” (each) can operate with 300 to 350 "Lun" object devices in addition to the existing ones.

2.1.1. Structure of modules

The receiving part of "Orlan" CMS consists of two separate "Orlan-M" wall modules with GSM modems as shown in Figure 4. "Orlan-M" module has the “Orlan-M11” or “Orlan-15” PCB with a power supply connector, connectors for inter-module connections and PC interfacing (through the special USB cable adapter), remote antenna connector and the configuration connector as shown in Figure 4. The module connection diagrams shown in Figure 5.

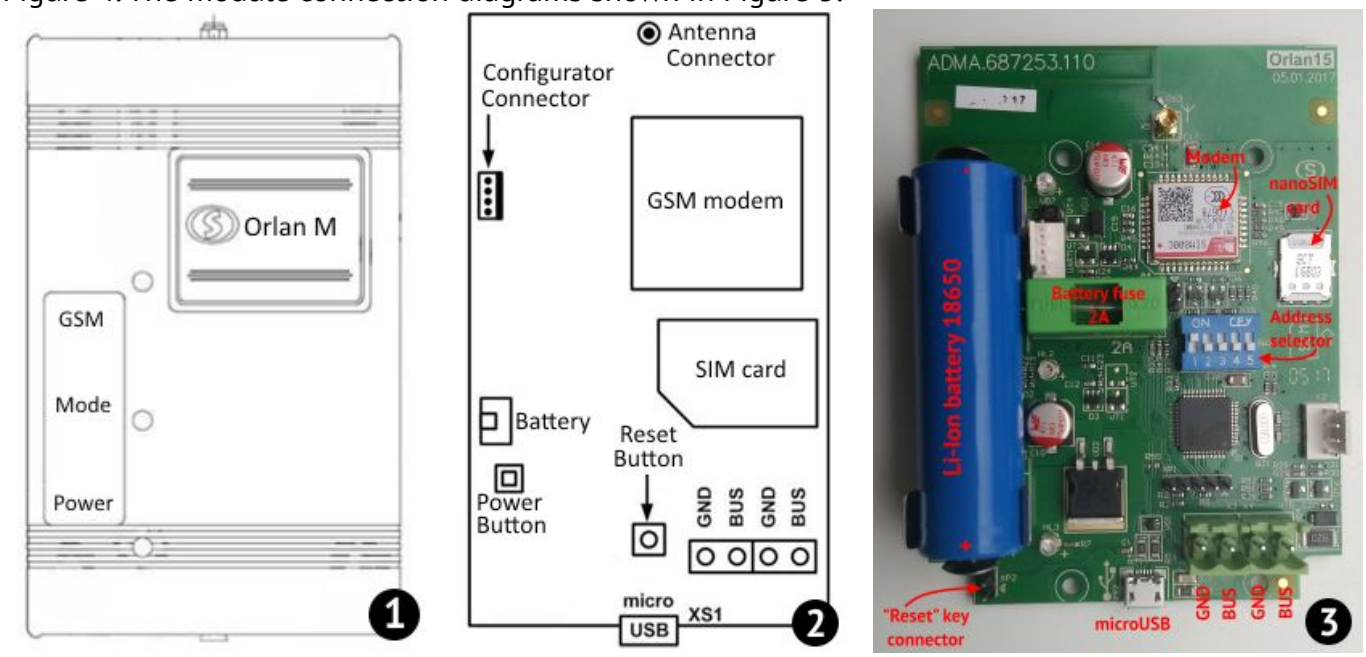


Figure 4. “Orlan-M” module (1) and its “Orlan-M11” (2) or “Orlan-15” (3) PCBs

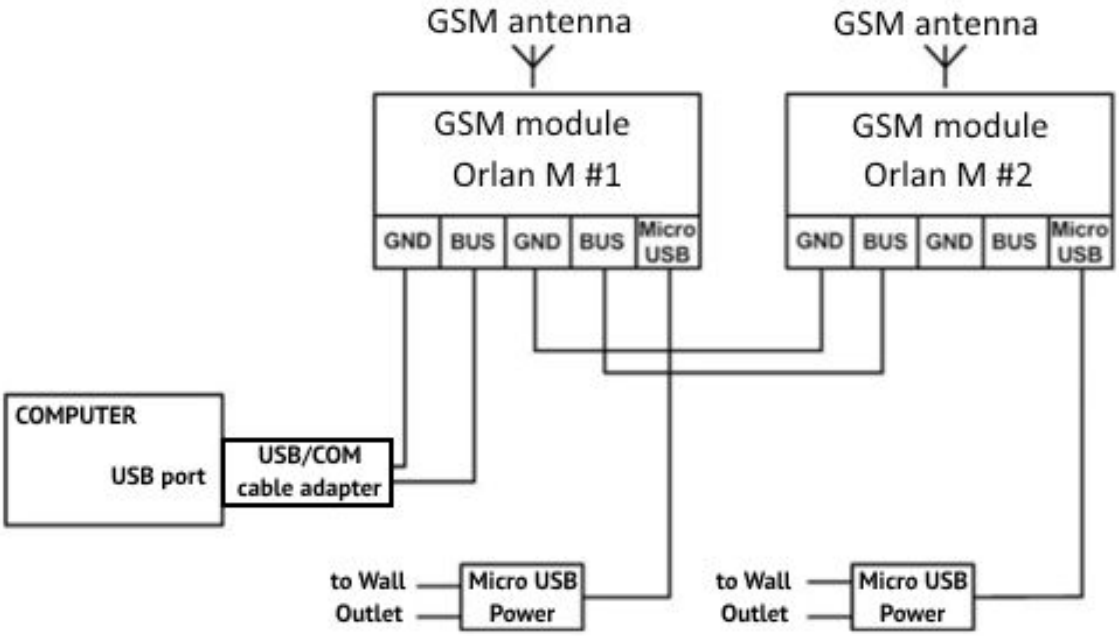


Figure 5. "Orlan-M" module connection diagram

2.1.2. Technical characteristics

The technical characteristics of "Orlan-M" module are given in Table 1:

Table 1. "Orlan-M" technical characteristics

Characteristic	Value
Power consumption, max, W	5
Capacity of received events memory buffer of "Orlan-M" module (each)	310
DC power voltage (with pulsation of no more than 50 mV), V	5.0 – 6.5
Communication session duration, max, s	6
Time of message transmission from "Lun" Control Panel (voice mode), max, s	30
Dimensions of "Orlan-M" module with GSM module mounted, mm	92x44x148

2.1.3. Installation procedure and connection of "Orlan-M" modules

Prior to installing of "Orlan-M" modules, they shall be configured:

- To configure the "Orlan-M" module **based on "Orlan-M11" PCB**, the "Configurator" software shall be used as follows:
  1. Disconnect the operating battery;
  2. Connect the operating charger with the micro USB connector to "Orlan-M" module. The module shall be in the open position;
  3. Connect 4-wire Orlan-SMS USB cable to the computer. "Orlan-M" module shall be configured using this cable;
  4. Start the "Configurator" program and select the corresponding COM-port;
  5. Press the "**Select device manually**" button and select "**Orlan-M**";
  6. Connect the Orlan-SMS USB cable to the configuration connector of "Orlan-M" module (see. Figure 4, "Orlan-M11" PCB). The module shall be in the open position;
  7. Allow the charger power supply with **SW2** button;
  8. Wait until **red LED** lights up continuously. If this does not happen within 10 seconds, hold

down **Reset** button (see. Figure 4) for 2 seconds;

9. The red LED on “Orlan-M11” PCB is continuously lit that means the module is in the configuration mode and the green label “**Connected**” shows in "Configurator" software;
10. Set the required address of the device on the bus in the appropriate field and click "**Write data**";
11. Exit the program, disconnect the cable from the module. Configuration is completed.

■ To configure the "Orlan-M" module **based on “Orlan-15” PCB**, the hardware address selector is used. The required address of the device on the bus should be set in binary code in accordance the Table 1 while the module’s **power is off** (see Figure 4, “Orlan-15” PCB)**.**

After configuring the module, it is necessary to evaluate the signal strength of the base station at the place of installation of the remote antenna of the module. The connection here shall be steady; voice during a conversation on the phone shall be with no echo and distortion. The antenna feeder antenna shall be completely pulled out of the module housing. When installing multiple modules, the remote antennae of module shall be at a distance of at least 0.5 m from one another. It is not recommended to put the antenna cable into the same cable duct (box) with wires of power supply and computer communication. Do not install the antenna on a metal surface.

The connection shall be carried out as follows:

- Connect the communication cables to the computer and install the drivers of communication cable according to software Operating Manual (see "Initialization of USB cables of devices" section);
- Connect HASP key to the computer;
- Insert SIM cards in the modules;
- Connect the antenna;
- Connect the computer communication cables to the computer and the second module to the terminals of the module;
- Connect the power supply adapter's microUSB cable to the module, then connect adapter to the wall outlet;
- Allow the charger power supply with SW2 button;
- Apply power to the modules by pressing the Power button (see. Figure 4);
- If within 5 seconds no indication of the module operation appears, hold down the Reset button for 5 seconds. The operating indication mode is as follows: red and blue LEDs flash, green LED is constantly lit;
- Configure "Phoenix-4" software package according to its Operating Manual (see “Configuration of “Phoenix-4” software” section).

2.1.4. “Orlan-M” LEDs indication

The board of "Orlan-M" module has three LEDs: red, green and blue (see. Figure 4).

Red LED – “**Mode**” – is an indicator of the system status and has 4 modes of operation:

- Short flashes – Module is in standby mode;
- Long flashes – Module memory contains the events not transmitted to CMS;
- Is not lit and not flashing – Incorrect operation of the module; there are some faults;
- Continuously lit – Module event memory is full or the module is in configuration mode.

Blue LED – “**GSM network**” – is an indicator of the modem status and has 4 modes of operation:

- Short flashes with a short interval – GSM modem is being registered on GSM network;
- Short flashes with a long interval – GSM modem has been successfully registered on GSM network and operates in the normal mode;

- Continuously lit– GSM modem failed to register on GSM network;
- Not lit and not flashing – GSM modem is faulty or not powered.

Green LED – "**External power supply**" – is an indicator of the connection of charging voltage and has two modes of operation:

- Continuously lit– external power supply is switched on;
- Not lit and not flashing– no external power supply is switched on.

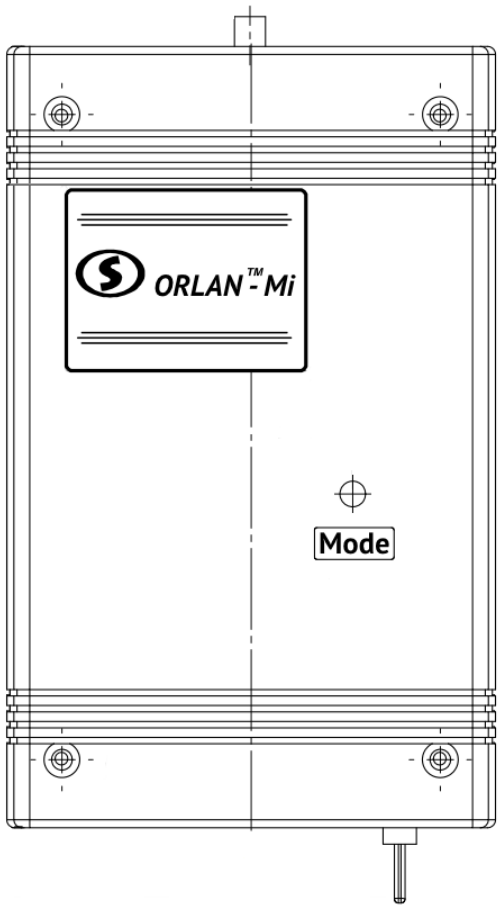


Figure 6."Orlan-Mi" module

2.2. "Orlan-Mi" modules

"Orlan GPRS" CMS package consists of two "Orlan-Mi" modules (Figure 6) supporting GPRS with addresses 1 and 2 and "Phoenix 4" software. The modules are powered via computer communication cable. "Orlan GPRS" supports operation with up to 2000 "Lun" object devices in addition to the existing ones.

The connection shall be carried out as follows:

- Create your own Virtual Private Network (VPN) with the static IP-addressing based on local GSM mobile operator service (without Internet access and without any mobile operator's equipment);
- Connect the communication cables to the computer and install the drivers of communication cable;
- Connect the antenna;
- Insert SIM card;
- Apply power to the modules via the switch on the module housing;

2.2.1. "Orlan-Mi" module LED indicator

"Orlan-Mi" module has one green LED, which is the "**Modem status indicator**" and has 4 modes of operation:

- Short flashes with a short interval – GSM modem is being registered on GSM network;
- Short flashes with a long interval – GSM modem has been successfully registered on GSM network and operates in the normal mode;
- Continuously lit – GSM modem failed to register on GSM network;
- Not lit and not flashing – GSM modem is faulty or not energized.

3. "Phoenix-4" software installation

Installation of the software has several stages:

- Installation of Microsoft SQL Server Database Management System (DBMS);
- Installation of driver for HASP hardware dongle key;
- Installation of “Phoenix” software;
- Installation of driver for USB-cable;
- Installation of a new configurator for Lun-11;
- Installation of FTP server.

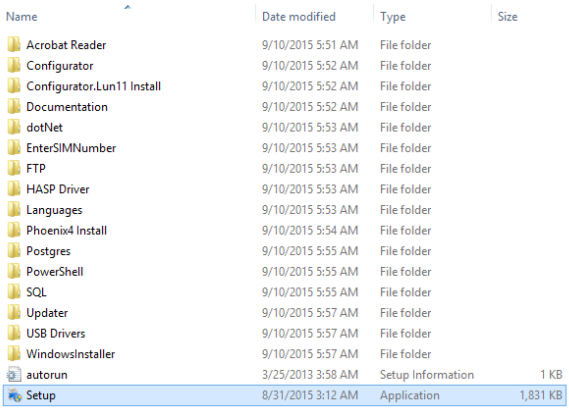
The installation program analyses your system and, if necessary, installs the required components. It can be Microsoft.Net Framework platform, language pack, Microsoft IIS, Windows PowerShell, and other. In case any additional splash windows appear, you cannot refuse to install the suggested components. This will lead to incorrect operation of "Phoenix 4".

All installation stages are automated and require minimum user's actions. Before installing the software, you shall close all the programs, since upon completion of the installation the computer will be automatically rebooted. Below you can find the description of all the stages.

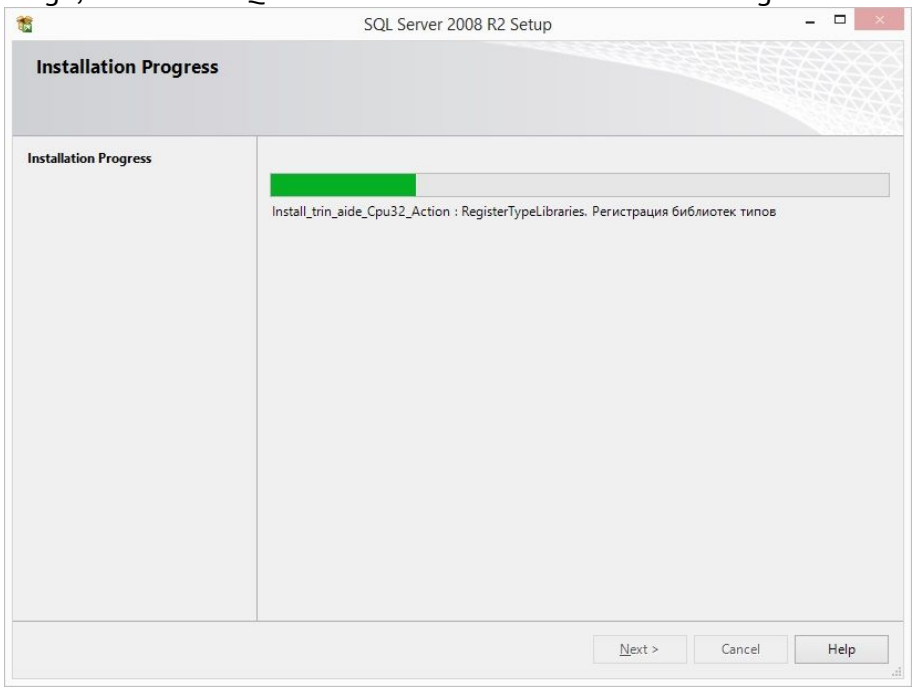
Starting of the installation is performed automatically when you insert CD with the software in the drive. Upon autorun, the monitor screen displays the message shown in the figure below.

Click "Install".

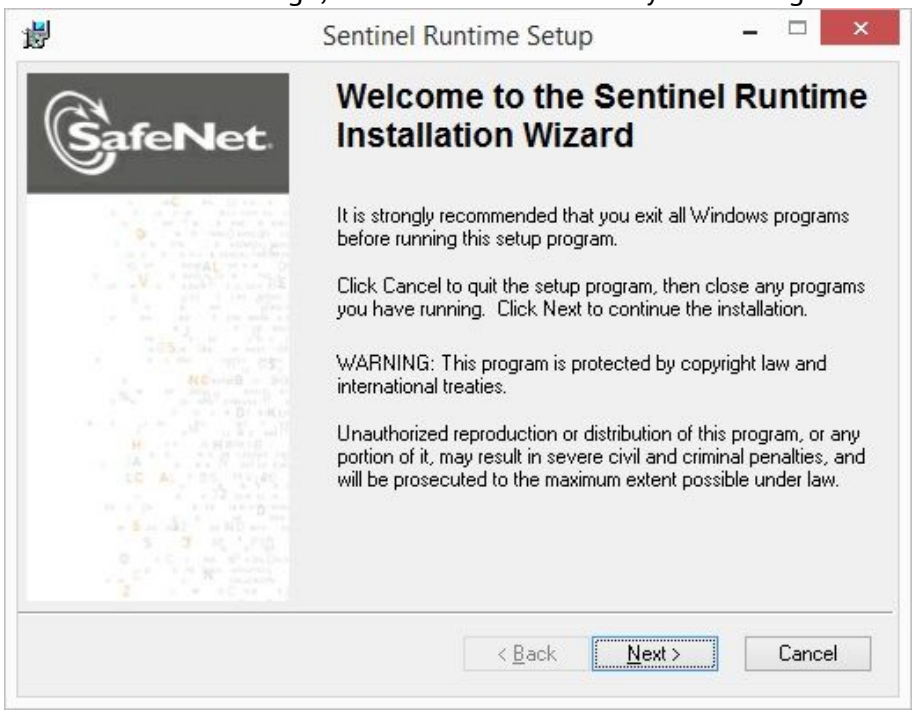
In case there was no autorun, you shall open the disk with “Phoenix-4” software using the “Explorer”, find “Setup.exe” file and run it by double-clicking the left mouse button:



At the first stage, Microsoft SQL Server DBMS is installed and configured.



Upon completion of the first stage, installation of HASP key driver begins.



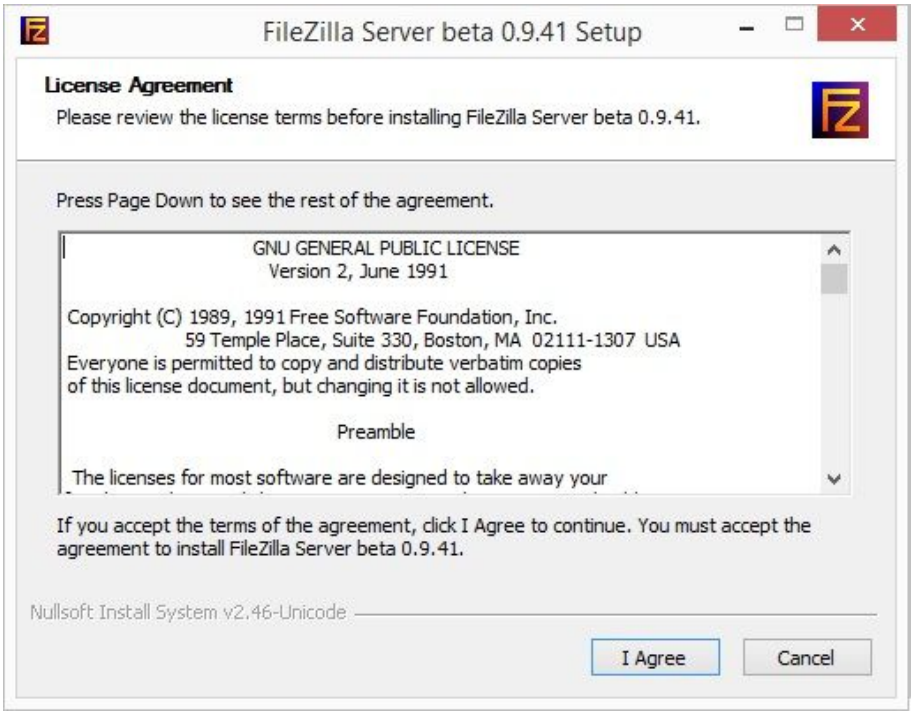
After that, installation of “Phoenix-4” software begins; it suggests you to accept the provisions

of Software License Agreement with Ortus.

Upon completion of “Phoenix-4” software installation, installation of drivers for USB cables manufactured by Ortus begins.

In case you set the “**Install FTP Server**” checkbox at the initial stage, it will be installed.

FTP server is required to support the configuration of “Lun-11” Control Panel and the “black box” of “Alet” device. In case you did not set “**Install FTP Server**” checkbox at the initial stage of installation, you can install it any moment by running the installation program once more and set of the “**Install FTP Server**” checkbox.



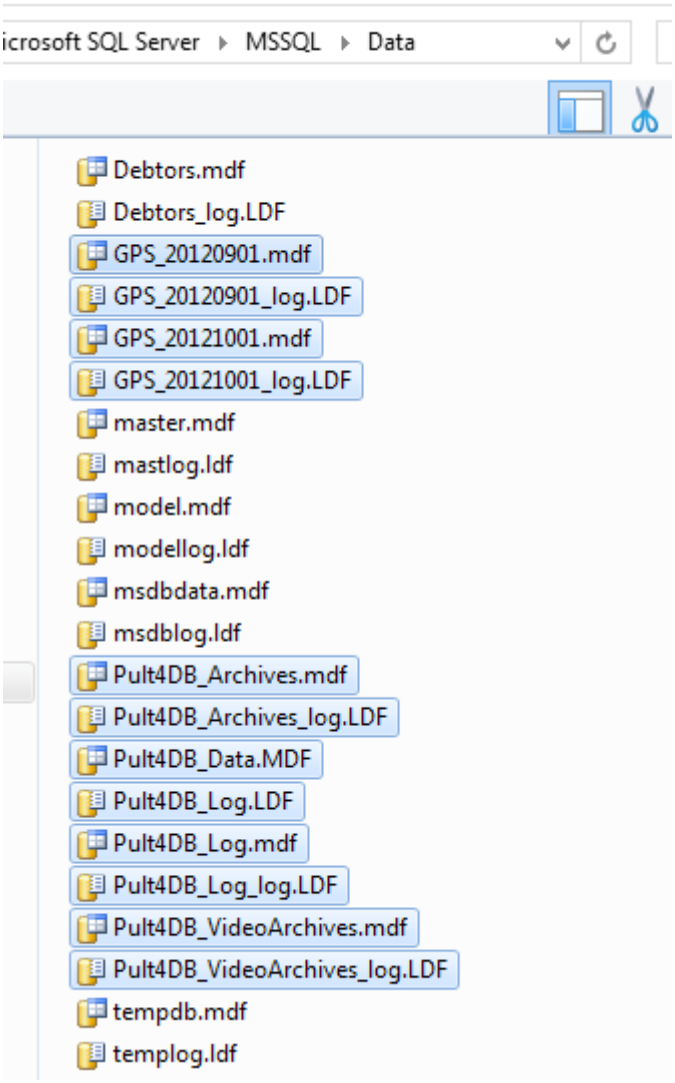
At the next stage, “Configurator 11” software is installed.

Upon completion of this stage, a window will appear and suggest you to press **Done** to reboot the computer and complete the installation of SQL server.

After the reboot is complete, “Duty Operator”, “Control Center”, and “DB Administrator” program shortcuts will appear on the desktop.

“Phoenix-4” objects database files will appear in

C:\Program Files\Microsoft SQL Server\MSSQL\Data folder:



"Phoenix 4" stores information in different databases (DB):

Pult4DB – major BD where all information about the s, devices, as well as guides are stored.

Pult4Db_Log – sub-database; used for debugging; all bugs are logged in it.

Pult4DB_Archives – DB of archives of messages received from any devices.

Pult4DB_VideoArchives – DB of archives of images received from "Dozor" modules.

GPS_<yyymm01> – DB of coordinates (tracks) received from "Alet-9" devices; every month a new DB is created, named as follows: <GPS_yearmonth01>

Attention! All the above-mentioned DBs are closely related, therefore, if you archive a DB manually, do not forget to archive all the databases, and not just the major one.

Consequently, when recovering DBs, do not forget to recover ALL the databases, and not just the major one.

3.1. Initialization of USB cables of devices

Attention! Prior to connecting of "Orlan" modules to a computer, be sure to install the cable drivers (make sure they are installed).

Upon installation of "Phoenix 4" software and restarting of the computer, USB cables of the devices that will operate with this computer shall be initialized. During the initialization, OS “Windows” will assign the numbers of “COM” ports to the relevant devices.

Attention! In the future, the information on assignment of "COM" ports to the relevant devices will be needed when configuring “Phoenix 4” software.

The following USB cables can be included:

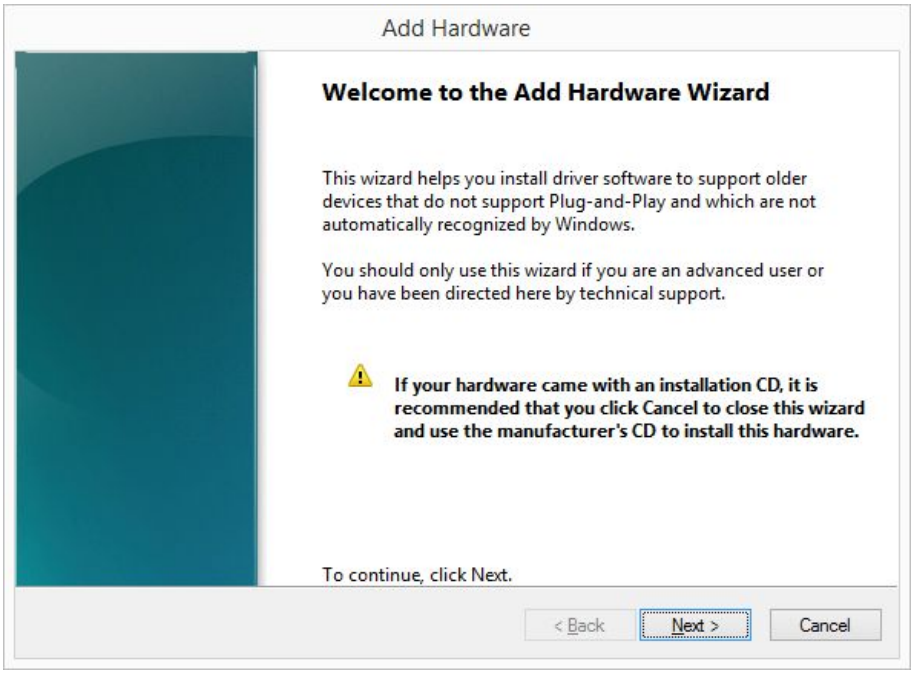
- Orlan-M USB –voice cables for connection of "Orlan-M" modules;
- Orlan GPRS_1 – cable for connection of the first "Orlan-Mi" GPRS module;
- Orlan GPRS_2 – cable for connection of the second "Orlan-Mi" GPRS module;
- Orlan SMS – cable for connection of "Orlan-SMS" module;
- Lun Config– connection cable for configuring of "Lun" object devices before mounting.

Attention! "Lun Config" cable can be connected to any other computer based on which a workplace for configuring of "Lun" object devices will be arranged. To arrange an individual workplace for configuring of object devices, use the instructions to "Configurator".

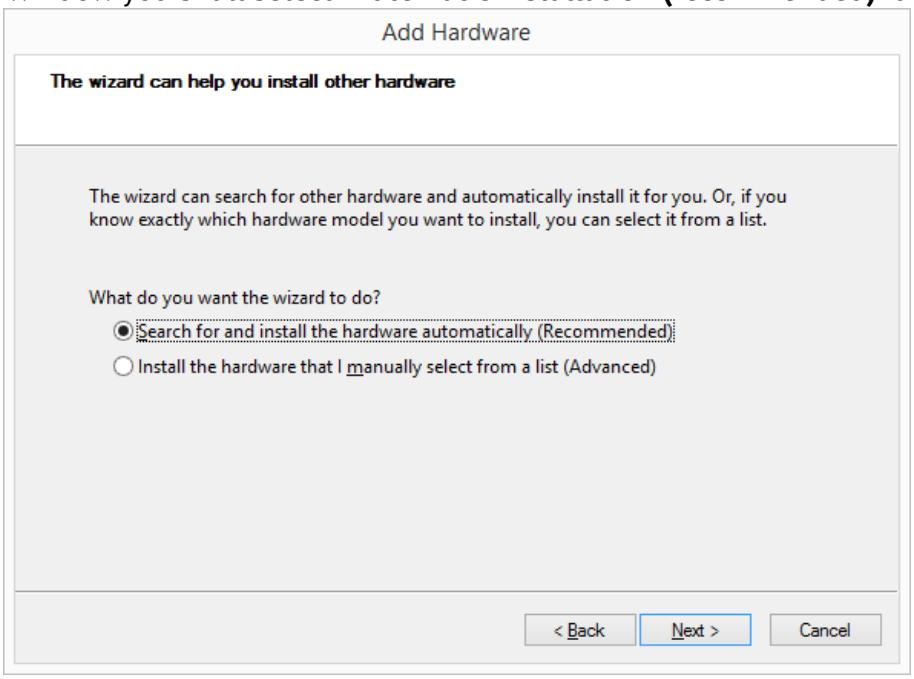
To initialize USB cables, connect the device cables one by one to the computer:

After USB cable is connected to the computer, OS Windows will find a new hardware.

The driver will be suggested to be installed. You shall take the following steps:
Select “**No, not this time**” in the window that appeared and press “**Next**”.



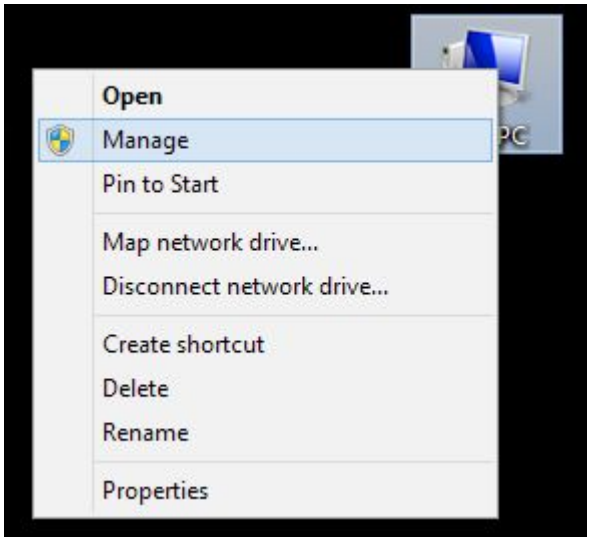
In the next window you shall select "**Automatic installation (recommended)**" and press "**Next**".



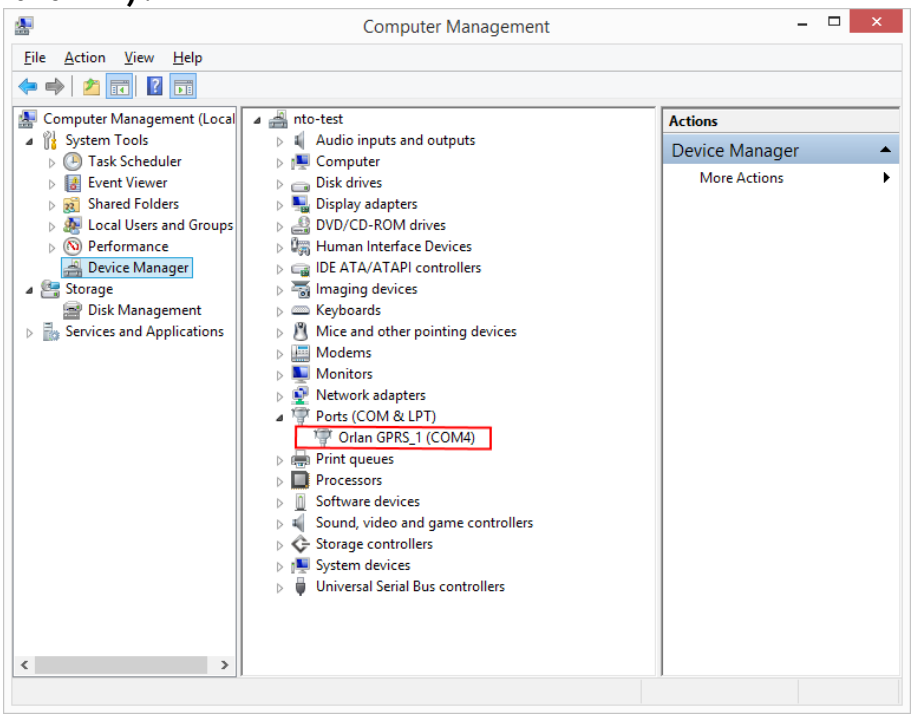
After that, the alert box will appear informing you that the software has not been tested for Windows compatibility. You shall press "**Continue anyway**".

After that, a successful installation message will appear.

Upon the successful installation of drivers of USB cables, a record with the name of device and its assignment to a specific COM port shall appear in the device manager. To get to know which COM is assigned to a device, right-click on "**My Computer**" and select "**Management**" (see below).



"**Computer Management**" window will open, in which you shall select "**Device Manager**" and then "**Ports (COM and LPT)**".

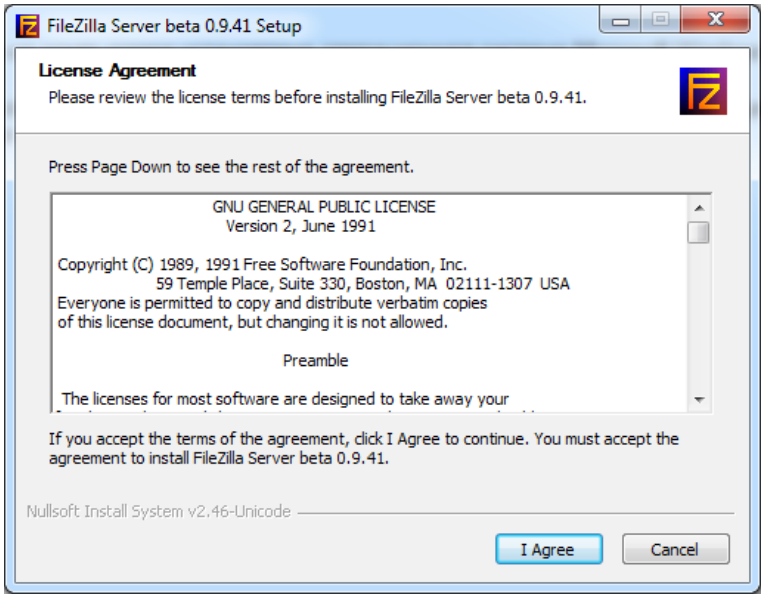


In this window you can see that at this moment "Orlan GPRS" cable is connected to the computer, and **COM** port No. **4** is assigned to it. The initialization procedure shall be carried out for each type of cables.

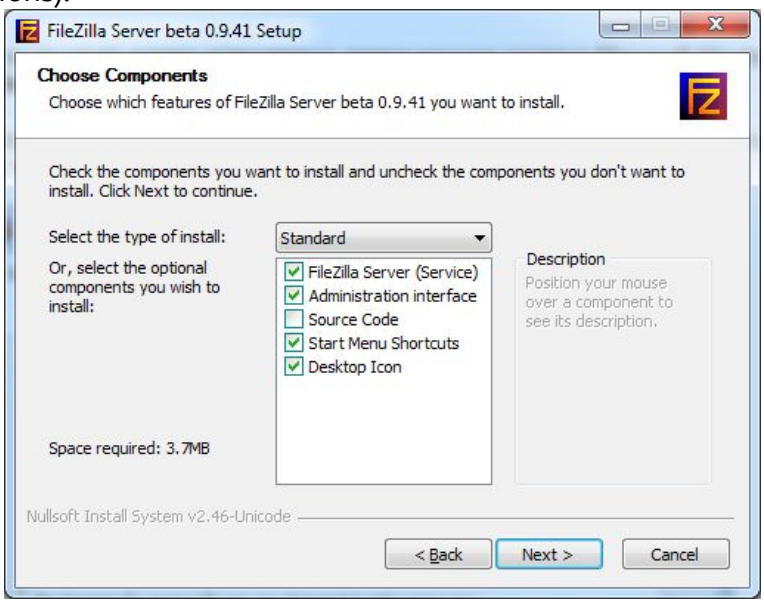
3.2. Installation of FileZilla FTP server

Attention! FTP server shall be installed on the same computer, to which "Orlan-GPRS" modules are connected.

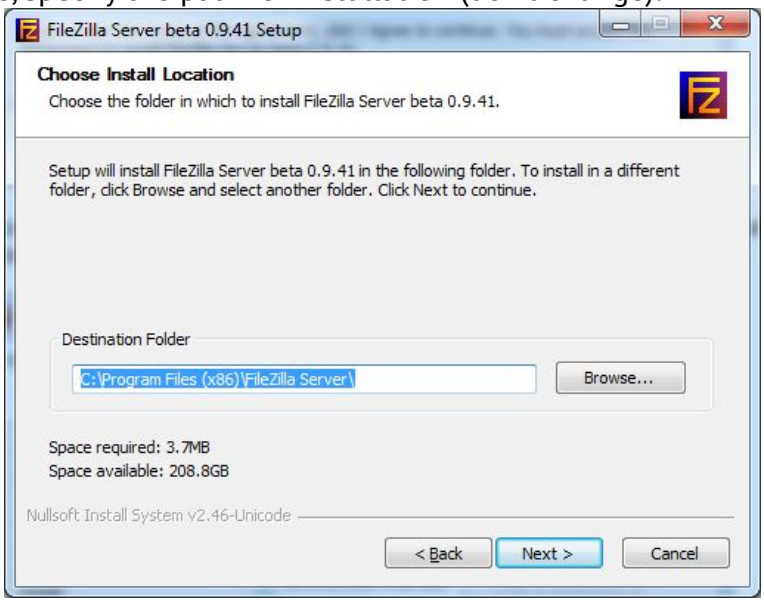
Set the "**Install FTP server**" checkbox in the update program or installer of "Phoenix-4", then FTP server Installer will be launched.



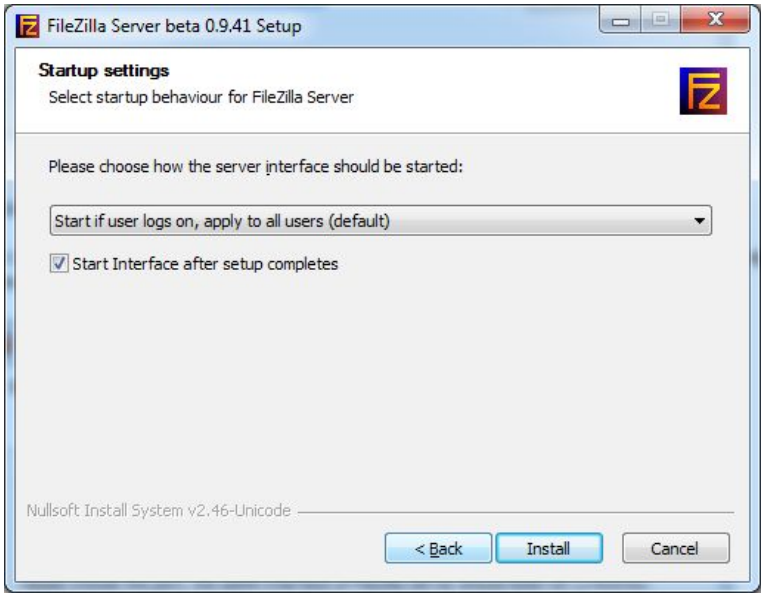
To continue installation, accept the terms of License Agreement. At the next stage, press **Next** (don't change any options).



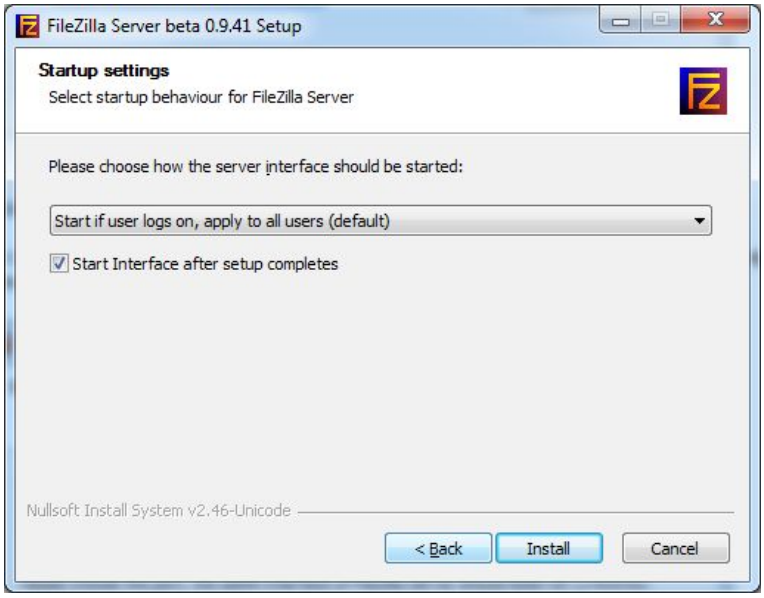
At the next stage, specify the path for installation (don't change):



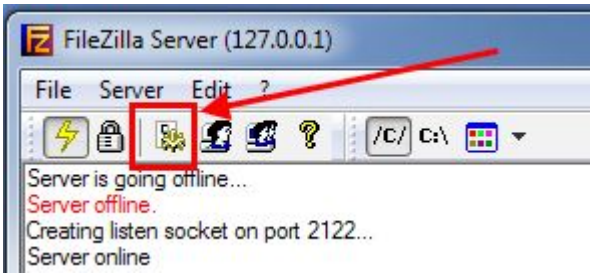
In the next window leave the default values and press **Install**:



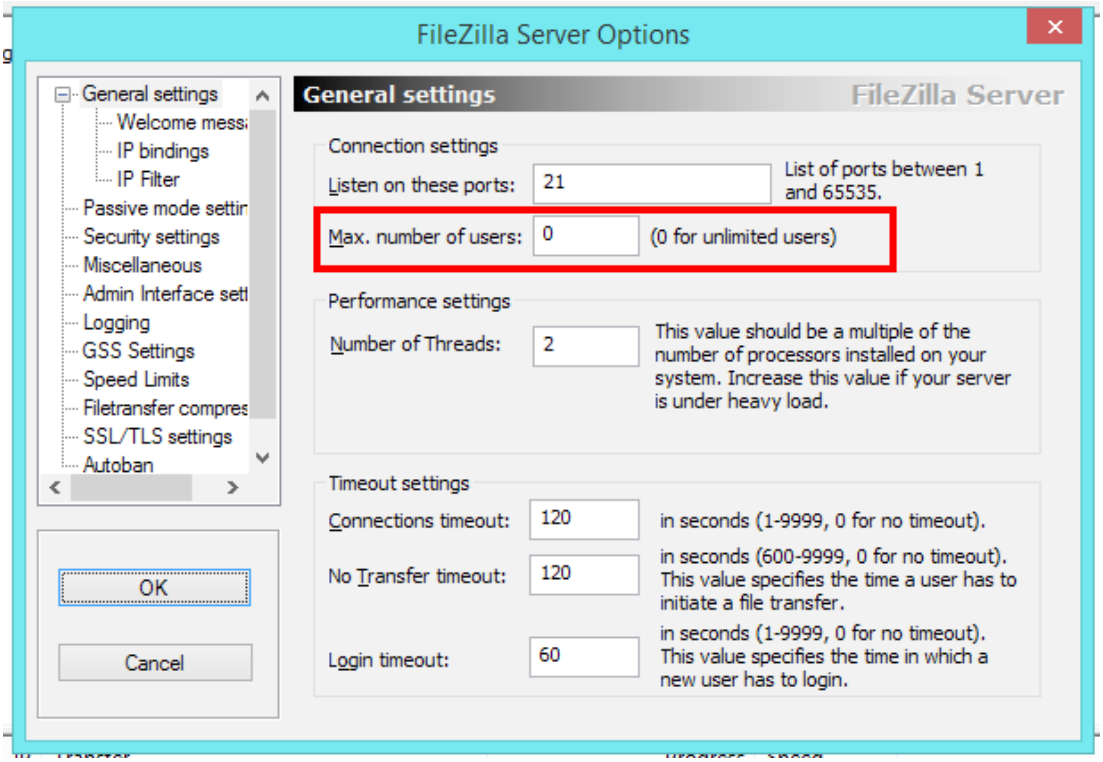
In the next window leave the default values as well and press **Install**:



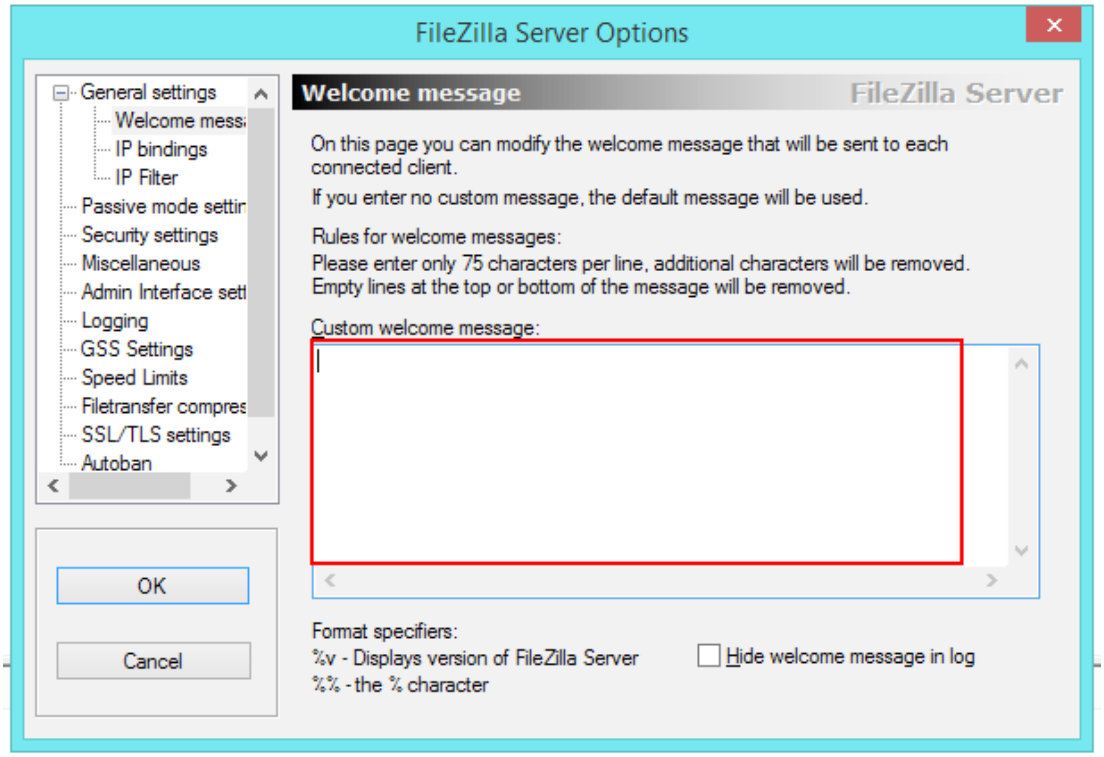
Then server shall be configured using the administration console. Press **Settings**:



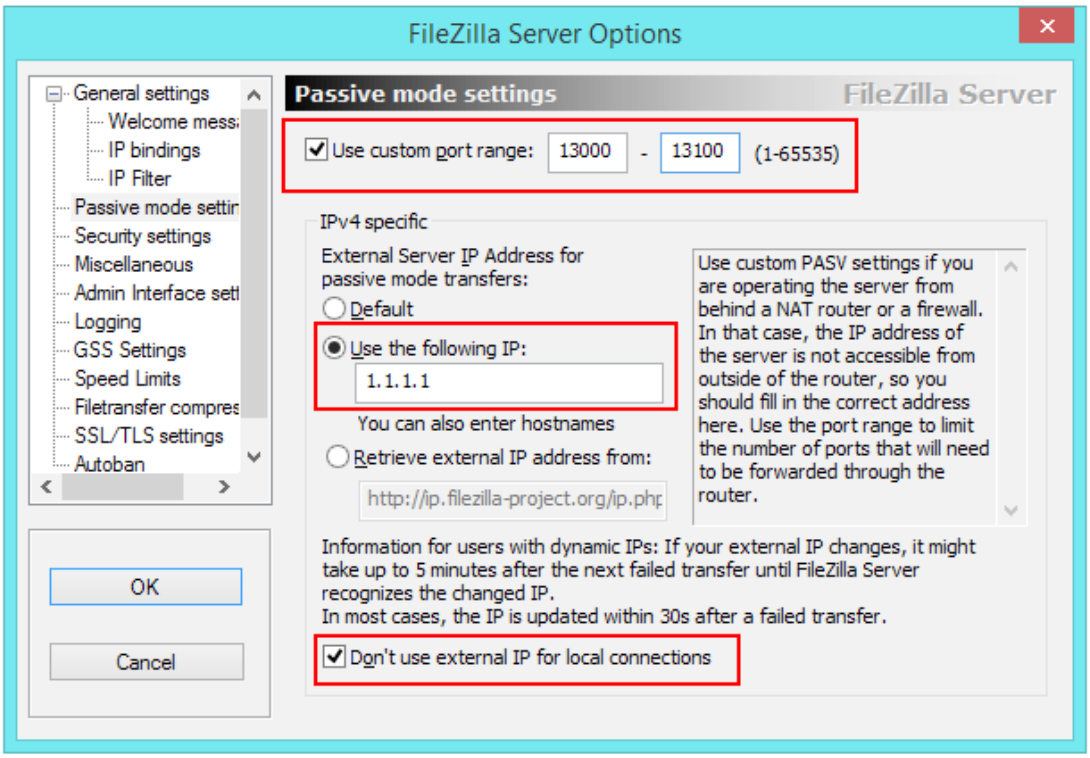
Go to "**General Settings**". Specify the management port (e.g., 2121). A non-standard port significantly decreases the number of attempts to hack into the server. The same port shall be forwarded from the external IP address, in case FTP server is NAT-based. You can also limit the number of concurrent connections to complicate such attacks as DDoS:



"**Welcome message**" section (optional). You can preset a welcome message:



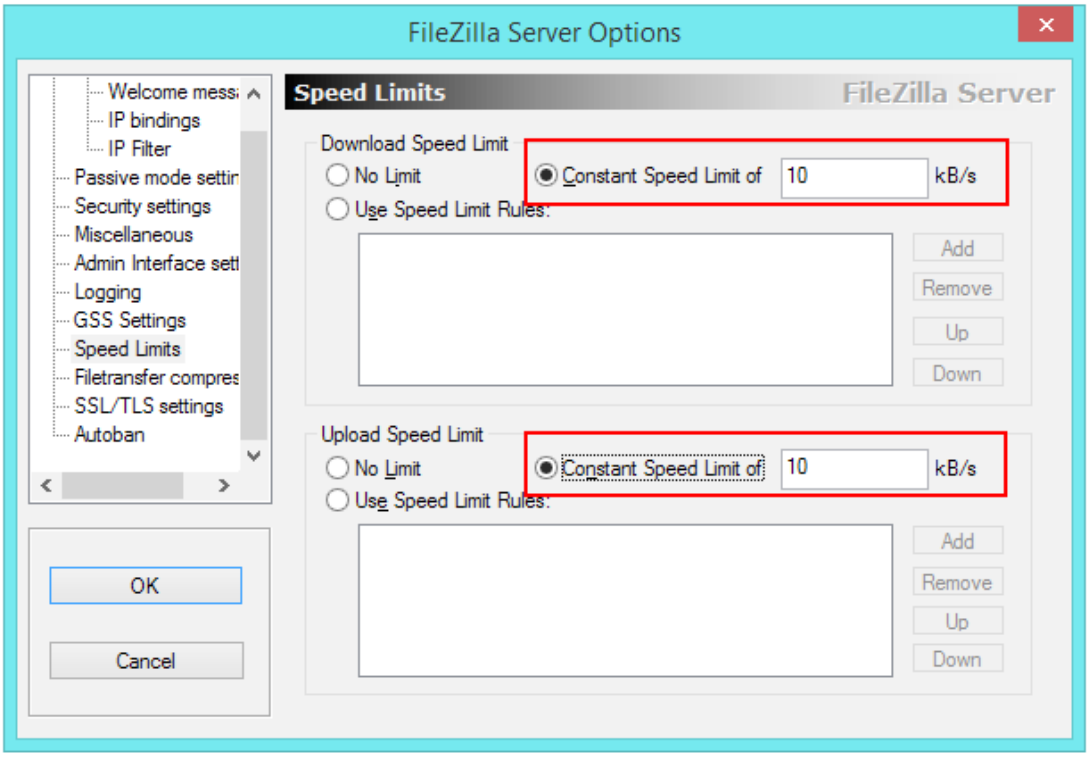
"**Passive mode settings**" section. In this section, the passive mode settings are configured:



Specify the range of ports to transmit data (e.g., 13000-13100). The same ports shall be forwarded from the external IP address, if the server is NAT-based. It is recommended to specify the range starting from the port number of no less than 1024. The number of ports is determined by the intended maximum load on FTP server (on the basis of one data port for one device; in other words, as many ports are provided, as many devices can be served by the server at the same time).

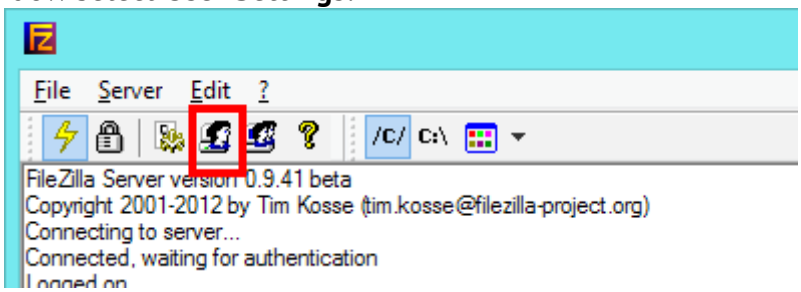
Specify the external IP (if the server is NAT-based) and select the "**Don't use external IP for local connections**" (as shown by the 3rd pointer), if there are any local clients (e.g., "Lun" devices via "Orlan" modules).

"**Speed Limits**" section. You can preset the speed limits for FTP server:

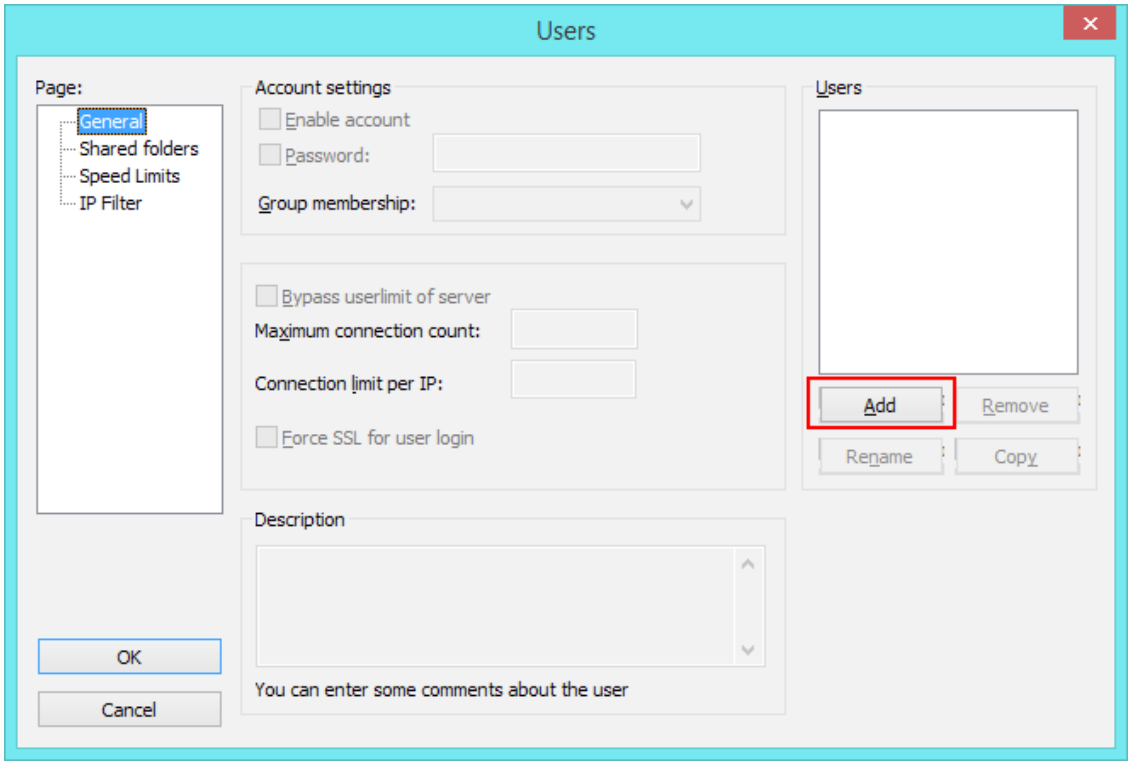


This limitation is another parameter of protection that will complicate large files transfer for hackers. Press **OK** and go to **User Settings**.

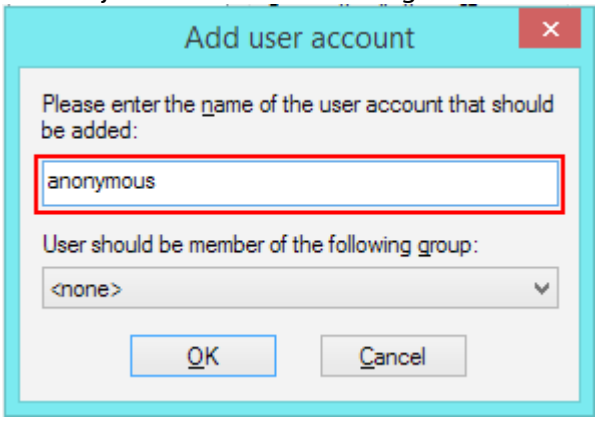
In the main window select **User Settings**:



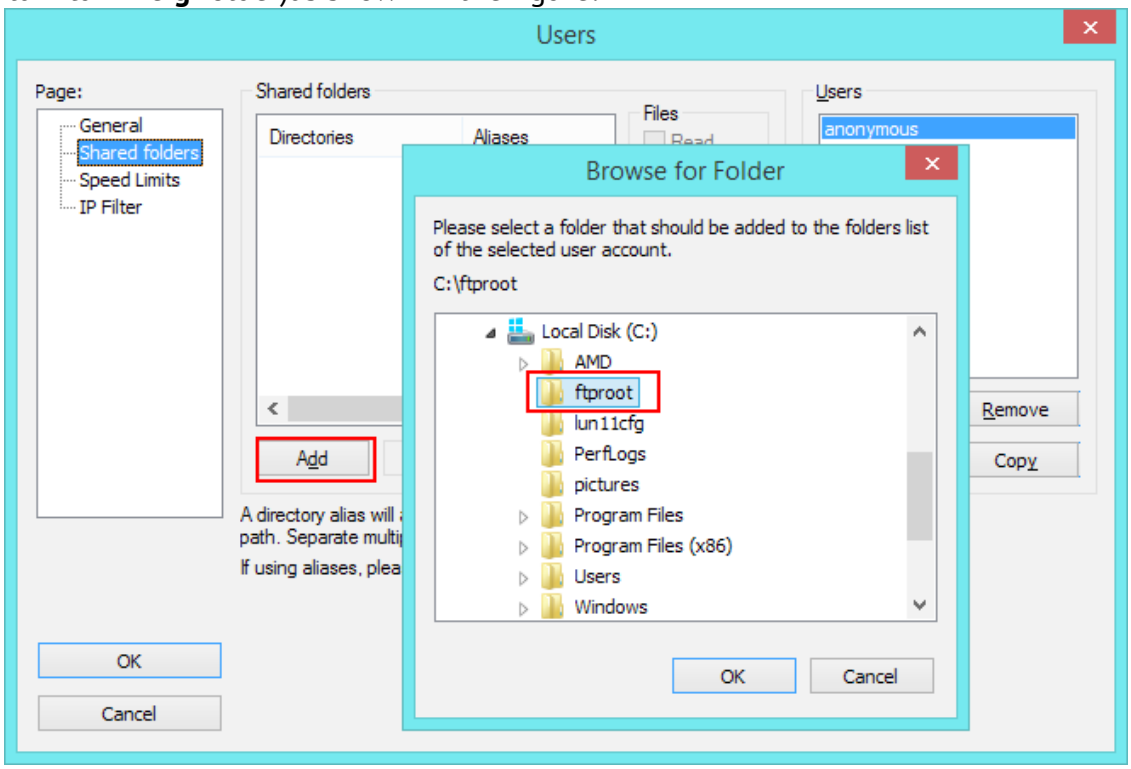
In "**General**" section click "**Add**":



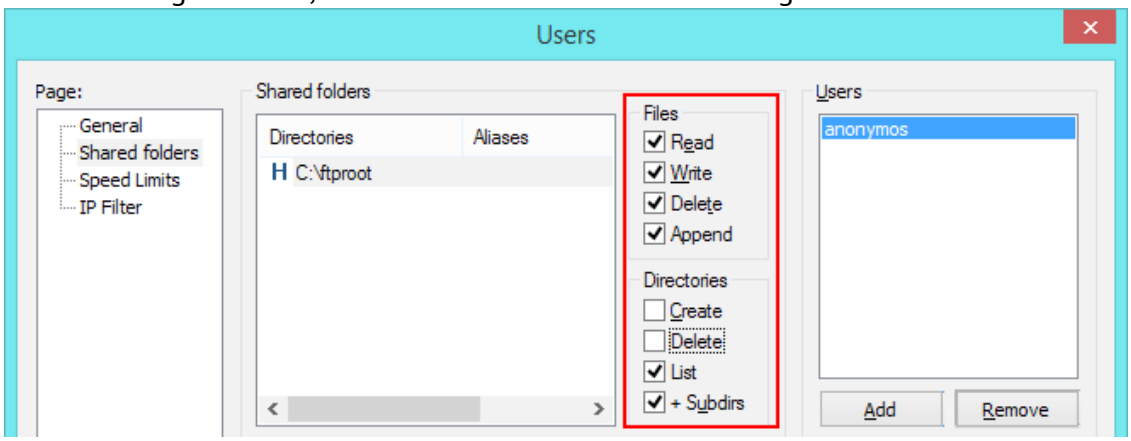
And create "**Anonymous**" user just as shown in the figure below:



"**Shared folders**" section. Click **Add** and select the pre-created folder for FTP server (this folder shall contain **lun11cfg** folder)as shown in the figure:

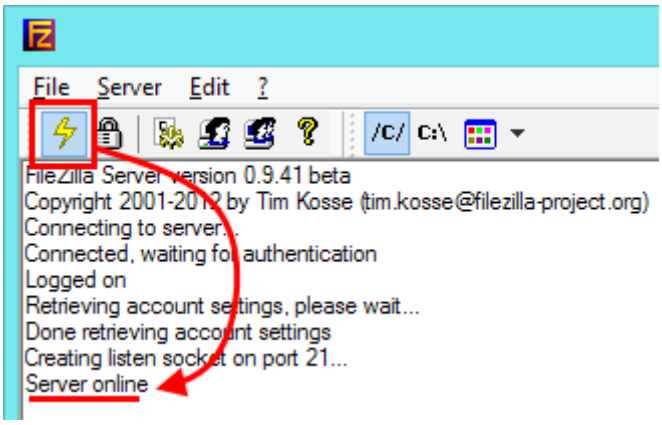


The folder being selected, set checkboxes as shown in the figure below:



Click **OK**. The configuration of user is completed.

Run the FTP server:

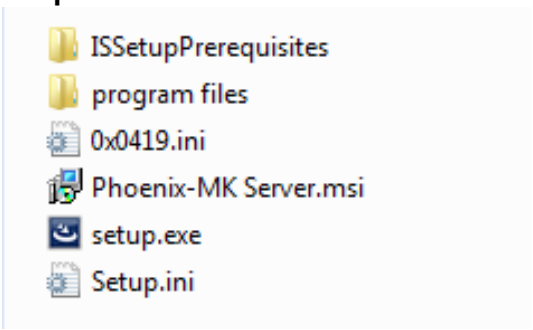


The configuration is completed.

3.3. Phoenix-MK server installation

Phoenix-MK server supports “Phoenix-MK” mobile application (mobile keypad) on the part of CMS. It can be installed either on CMS computer (on which ‘Phoenix-4” software is installed), or on any other computer.

To install the server, run **setup.exe** file:

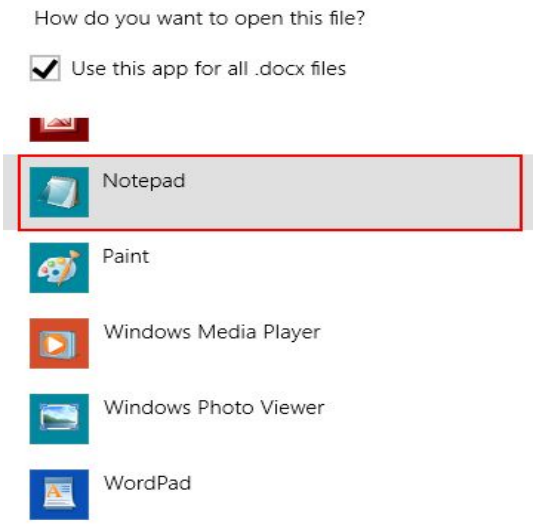


After the application is launched, click “**Install**”. During the installation the program will install the additional components depending on the system. During this process, console windows can appear that will suggest you to press any key to continue the installation; you must do that.

In the process of installation, a restart might be required – you must restart the computer then. Server is a Windows Service. The Startup Options can be viewed and changed in the system window of the Service (Control Panel – Administration – Services).

After installation of the server, in Start menu of Windows the relevant section will be added. Prior to starting the server, it shall be configured. To do this, open “**config.properties**” file via **Notepad**. A shortcut for this file will be created in “**Settings**” menu. After you click it, the following window will open.

You shall select the “**Select program from the list of installed programs**” option and click **OK**; the following window will open:



In this window select Notepad and make sure that the “**Use the selected program for all files of this type**” option was selected, and click **OK**. After that a text configuration file will open.

Two parameters shall be set:

Phoenix-4 **“Control Center”** (CC) **connection address** – IP address and port of the computer with CC that is responsible for joint operation with this server (i.e., CC with the configured “**Mobile keypad**” section), are to be set.

CC_WS_URL=ws://192.168.x.x(local PC IP):3050

Port based on which WAMP server for the Mobile keypad will operate (given server). You shall set the port that users will specify in the settings of Phoenix-MK mobile application.

MK_SERVER_PORT=8282

Do not change other parameters not having consulted with the technical support first.

After you changed the parameters, save the configuration file (close **Notepad** with all changes saved).

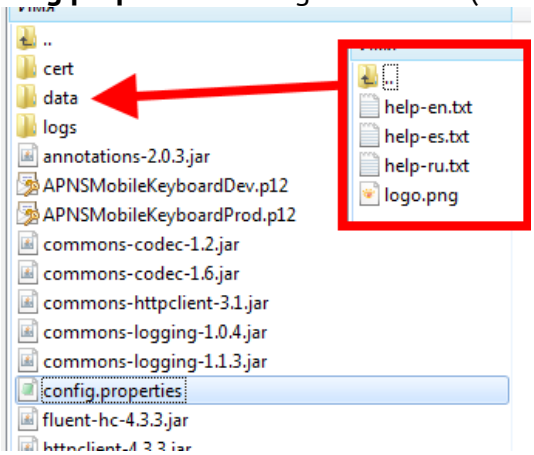
To start the server (Windows Server), click the "**Start Phoenix-MK Server**" shortcut, to stop the server, click the "**Stop Phoenix-MK Server**" shortcut.

After the first start the server will be started automatically when Windows is started.

A company that uses the server can install its own logo and help files that will be displayed in the Mobile Keyboard application.

For this you need:

1. Your logo file in PNG format, 120*120 pixels with a transparent background.
2. A new help file or correct an existing one in text format. The file name must match the pattern: **help-ru.txt**
   The part of the name "**-ru**" must correspond to the system language used in the user's mobile phone (in this example the Russian system language is used). A separate help file should be created for each system language, for example, **help-en.txt** – for English, or **help-es.txt** – for Spanish.
   The text format is UTF-8; you can use HTML codes for formatting, for example:
   ** ** – indent from the beginning of the line (it will look like a regular tab);
   &#8226 – list marker (it will look like a dot at the beginning of a line •);
   &#8227 – list marker (it will look like an arrow to the right ‣).
   You can specify the security company phone numbers, so user can make a call by touching the number placed in the text. A space character and double brackets are allowed in the phone number. Use international format for phone number (start with "+" and country code), for example:
   +38 (067) 123-45-67
3. The created files (logo and help) should be placed in the **data** folder located along the same path as the "**config.properties**" configuration file (see description above):



A working server automatically updates data files every 60 minutes. If immediate changes are required, then restart the server.

4. Configuration of “Phoenix-4” software

The software configuration can be divided into several stages:

1. Registration.
2. “Control Center” configuration.
3. “DB Administrator” configuration.
4. “Duty Operator” configuration.

Attention! Upon completion of editing of the database, log out of the system (LogOff) to prevent any accidental or unauthorized change of the database. The default password of “Administrator” account is

510eb93

The factory password is also specified on CD. Do not lose it!

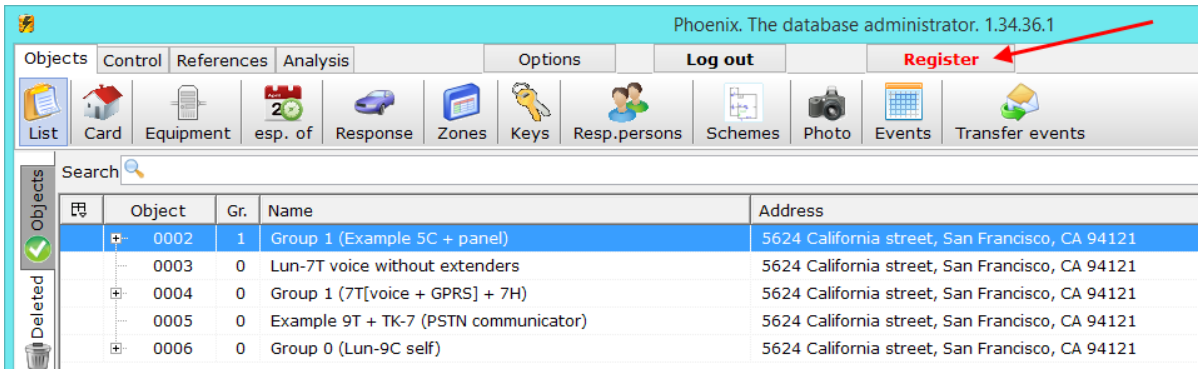
The “Phoenix-4” software uses the following network ports while operating:

Control Center – 5050, 5055, 7015
DB Administrator – 5052
Duty Operator – 5051
Phoenix-GPS – 5053
Application Engineers – 5054

4.1. Software registration

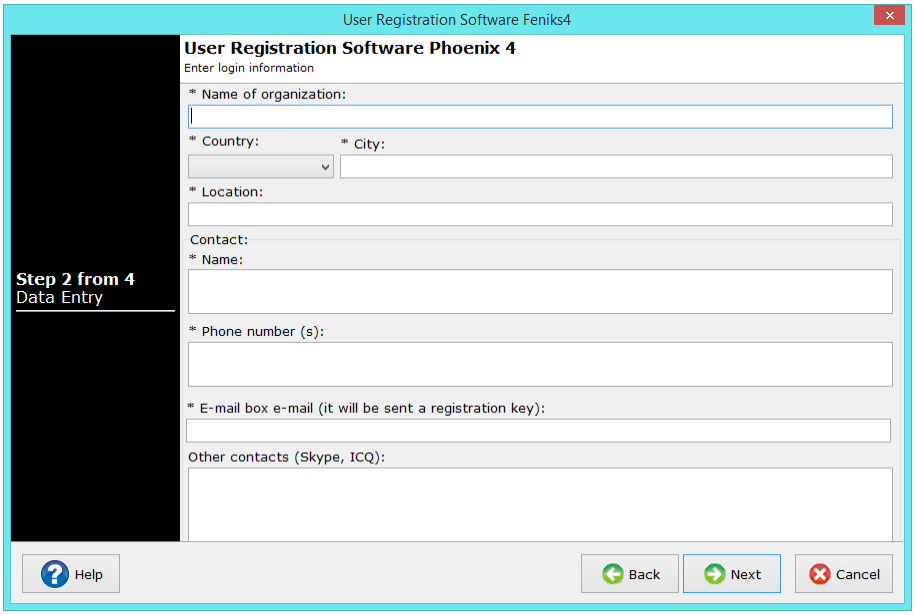
Attention! The programs of “Phoenix-4” software package can be started only when HASP key is connected.

Each copy of “Phoenix-4” software shall be registered. To register the software, run “**DB Administrator**” (Phoenix4.exe), and click “**Registration**” button:

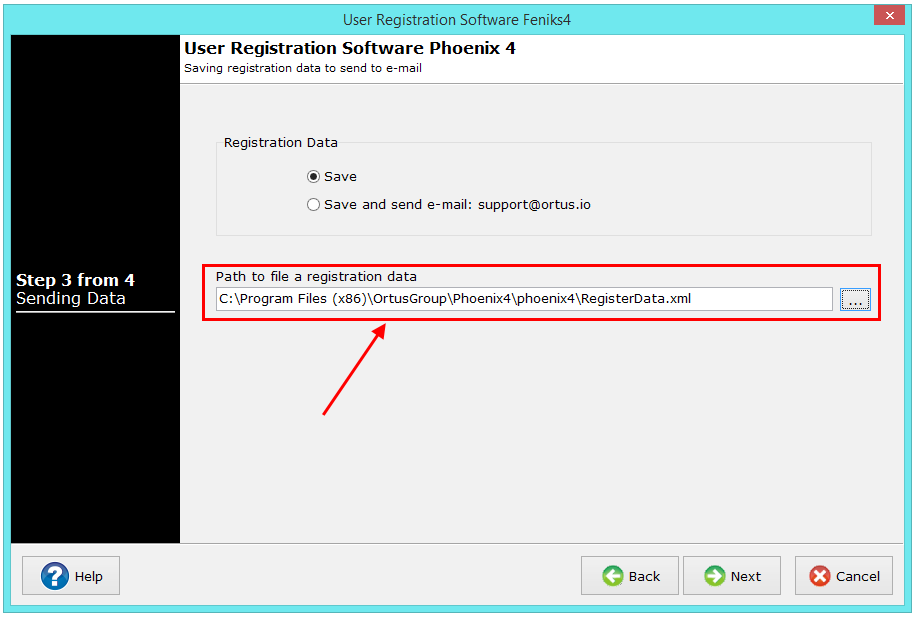


The Registration window will open.

Select "**Yes, I want to register now**" and click "**Next**", to open registration data form:



Upon completing the form and clicking **Next** a file will be created that you shall send to the email specified. The file path is specified in the program window.

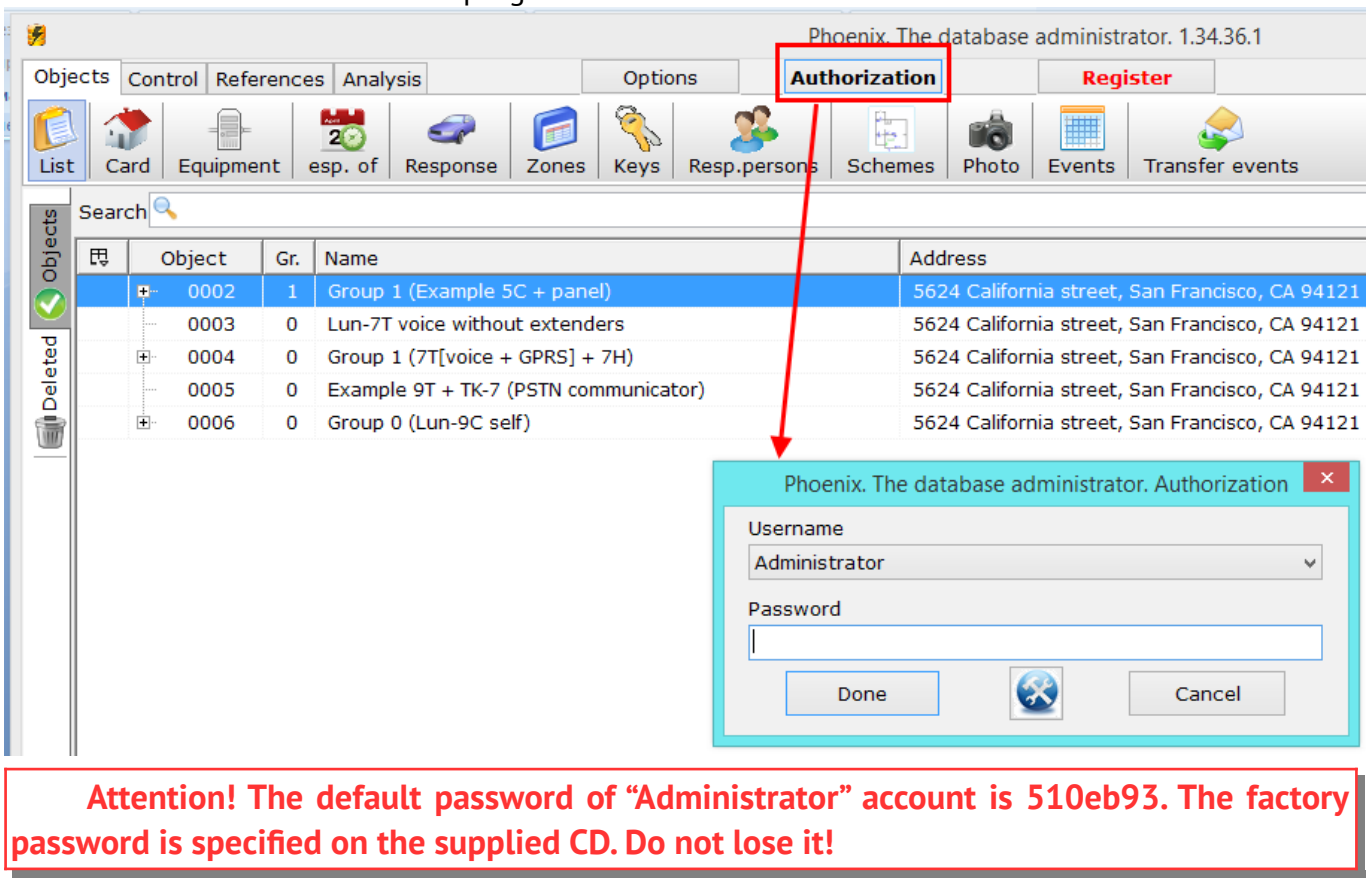


You will get a **registration code** (key) in reply.

Upon getting of the registration key, you shall launch "**Registration Wizard**" in the main window of "**DB Administrator**" (click "**Registration**"), select "**Enter registration key**" and enter the received code.

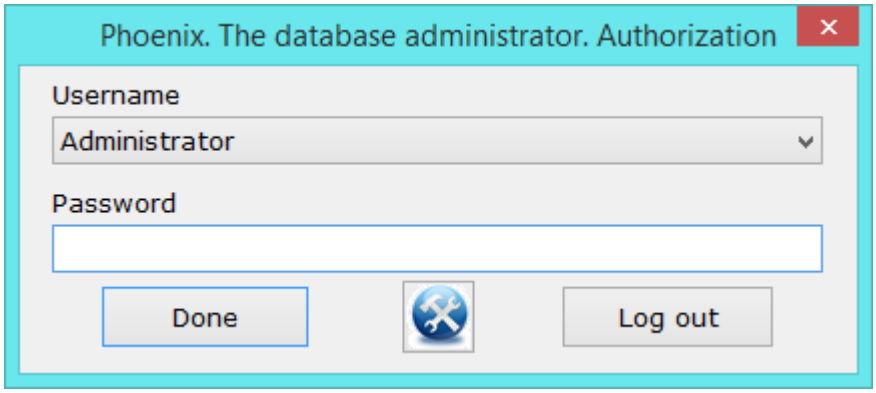
4.2. "DB Administrator" configuration

To start the configuration, "**Control Center**" and then "**DB Administrator**" shall be launched. Select "**Authorization**" button in the program main window.



Attention! The default password of "Administrator" account is 510eb93. The factory password is specified on the supplied CD. Do not lose it!

In case your software is configured for "**Zero access level with password**", you can log in when starting the program:

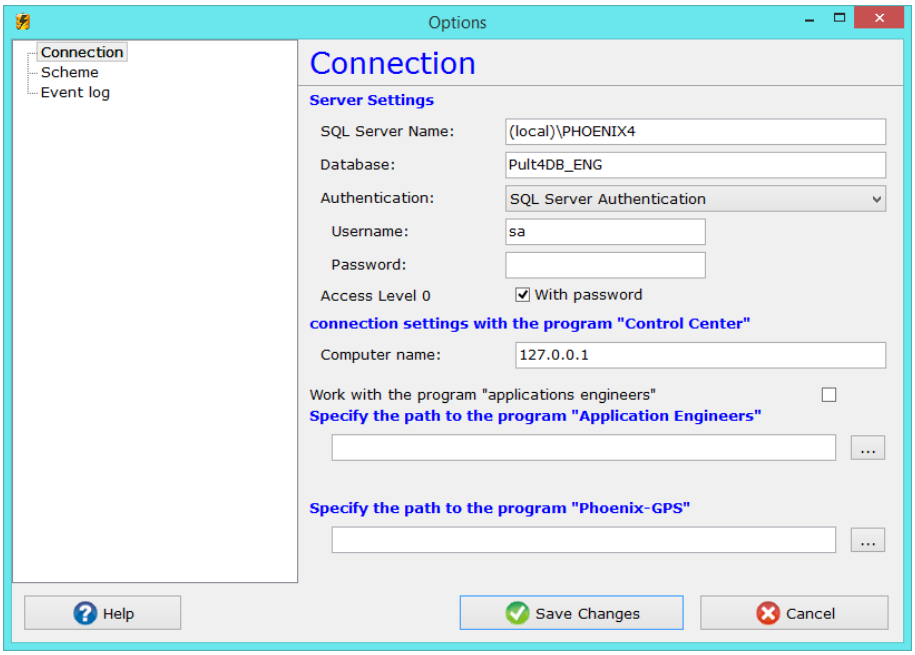


In this window you can also change the parameters of DBSM connection by clicking the relevant "**Settings**" button  . It may be useful, for example, when changing over for another SQL Server in case of emergency.

After logging in, click "**Settings**":

In the opened window select the "**Connection**" tab. In this tab you shall set the DBMS connection options, as well as networking options.

Attention! If you are not the System Administrator and do not clearly understand what these MS SQL Server Settings options are for, do not change them!



1. **Connection**. This group of parameters is the same for "**DB Administrator**" and "**Duty Operator**".

"**SQL Server name**" – network name of the computer is specified, where MS SQL Server DBMS is installed with the database (default local computer).

"**Database**" – database name (default name – Pult4DB).

"**Authentication**", "**User Name**", "**Password**" – configuring of MS SQL Server connection.

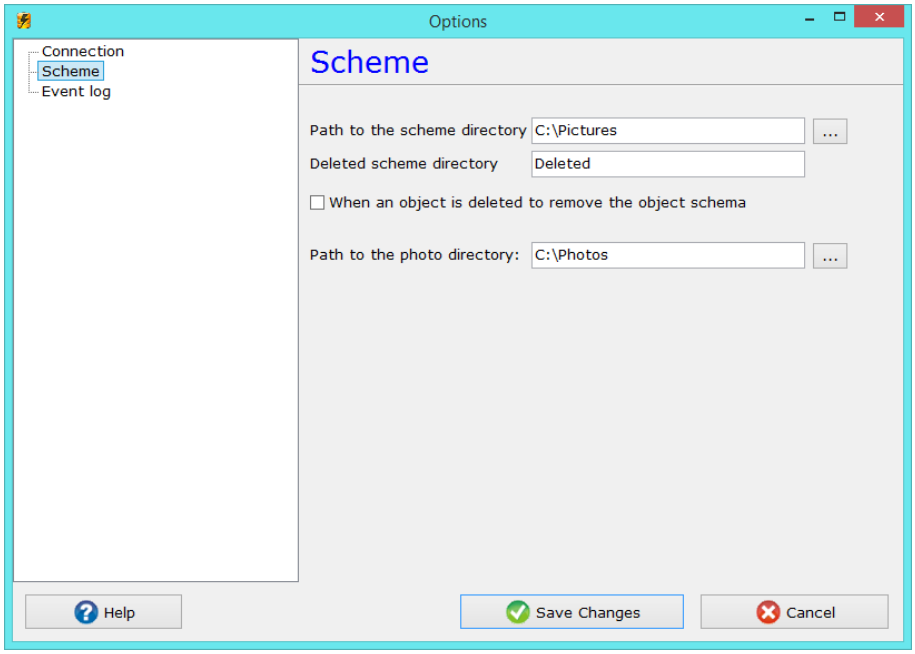
"**Zero access level with password**" option is required to limit the access to the software for the unauthorized personnel. Zero access level (without logging in) allows to view any information about the s and events. If this option is set, prior to running of "DB Administrator, log in to the system as a user; in case this option is not set, the program will start automatically with zero access level. "Duty Operator" has the same option in its settings.

In "**connection settings with the program "Control Center**" enter IP address of the computer, where "Control Center" is installed.

To provide the collaboration of Phoenix-4 and "**Application Engineers**" program, fill the corresponding checkbox and specify the path to the folder when "**Application Engineers**" program installed.

If your "Phoenix-4" software contains a "**Phoenix-GPS**" program, you should specify the path to this program in the correspondent field.

2. Scheme



The view of program window in “Settings. Scheme” tab.

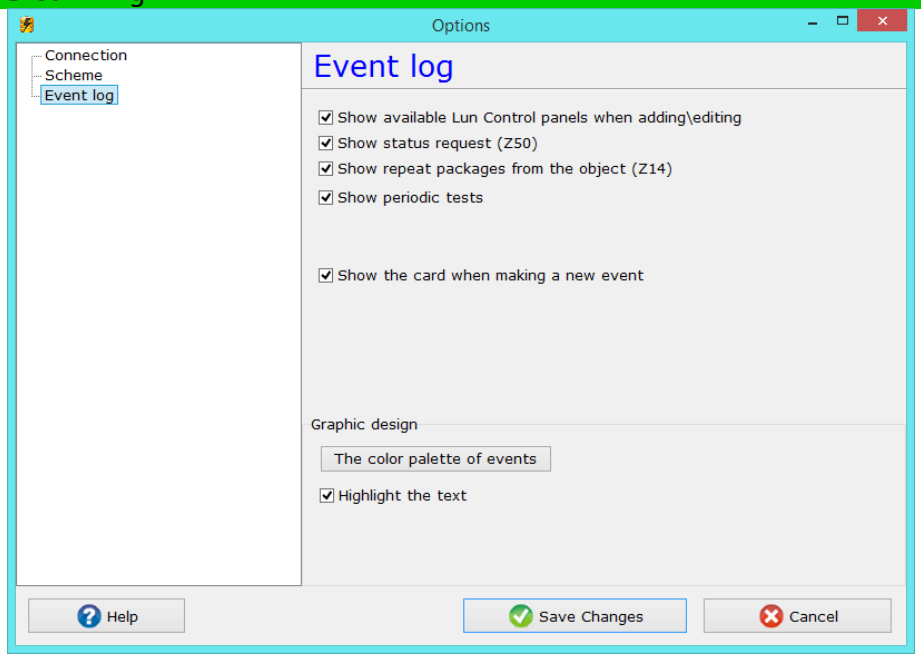
In the “Scheme” tab, specify the paths to the folders, where diagrams of objects, deleted diagrams (“Bucket”), and photos of the objects will be stored. The “When an object is deleted to remove the object scheme” checkbox determines whether the “Bucket” will be used or not.

3. Event log

In the “Event View” tab allow required event review options.

In the “Graphic Design” sub menu choose the event colour scheme. In the program archive they will be displayed as follows:

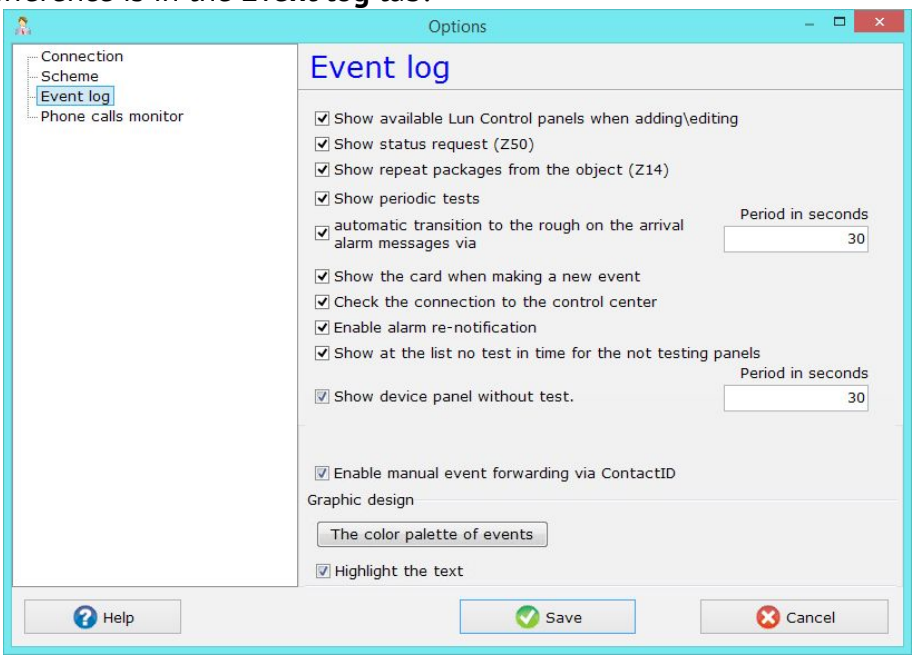
O03	Alarm
O11	Normal
O21	Arming
O39	Disarming



4.3. “Duty Operator” configuration

“Duty Operator” is configured in the same way as “DB Administrator”.

The only difference is in the **Event log** tab:



“**Automatic transition to the rough on the arrival alarm messages via period in ... seconds**” parameter. In case you are in any tab other than the “**Unprocessed**” tab, in a given time you will automatically go to this window after CMS receives an alarm message.

“**Show the card when making a new event**” parameter. In case this option has been selected, each time an alarm message is received for processing, the object’s card will be displayed.

“**Check the connection to the Control Center**” parameter. In case this option has been selected, Duty Operator will control the Control Center connection. In case any connection failures are found, a siren will be heard and connection failure information will be displayed in the bottom of the program.

“**Enable alarm re-notification**” parameter. In case this option has been selected, when a repeated alarm is transmitted from the object, an alarm will be sounded, even if the previous event is already being processed by the operator.

“**Show at the list no test in time for the not testing panels**” parameter. If this checkbox is set, then non-testing devices will be shown in the common test failed objects list.

“**Show device panel without test**” parameter. If this checkbox is set, then the new window for test failed panels will be displayed.

“**Enable manual event forwarding via ContactID**” parameter. If this checkbox is set, then the “**Send event via ContactID**” button will be displayed for unprocessed events.

4.4. “Control Center” configuration

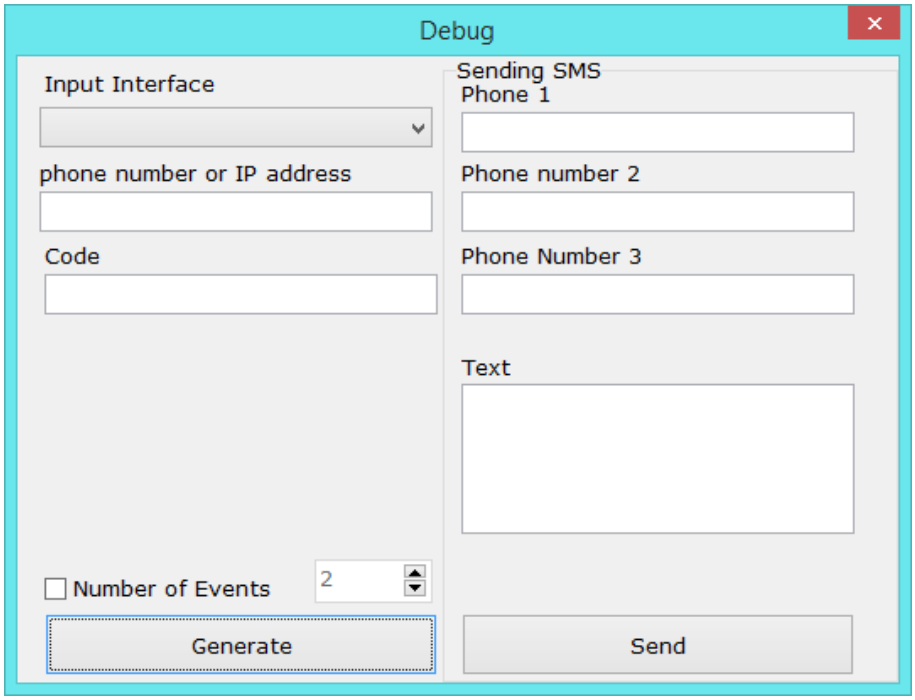
“Control Center” is a sort of driver for all the devices of “Orlan” series, auto dial receiving stations, and other receivers operating with COM ports. In addition, this program is also a center of commands processing of other programs of “Phoenix-4” software package. It shall always be running to provide the operation of all the package.

There can be several Control Centers, one Control Center for each computer with receiving equipment. However, only one of them can be the “major” Center. All others are “auxiliary”. For all auxiliary Control Centers the relevant option shall be selected in the settings (see the configuration details below).

Upon running of the program, a program icon appears in the task tray 

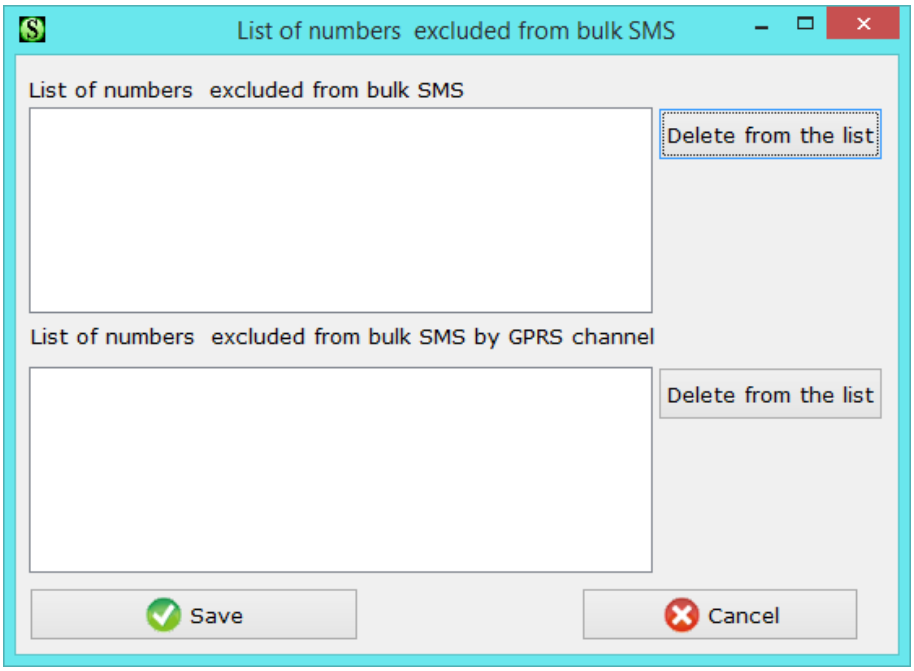
When right-clicking this icon, a menu appears with the following entries:

- **Exit** allows to terminate the program. You cannot exit the program during the restart or GPRS connection setup, therefore, Exit is not always available.
- **Settings** allows to set the program parameters. See the details below.
- **Debugging** allows to debug the system. You can generate any event for any object, and check the operability of all the object. It is designed by the Ortus Technical Support Service to diagnose issues.



Connection Restart allow to restart all Orlan devices in the case of its connection lost.

Numbers Removed from Delivery List allows to view the numbers removed from the SMS delivery list, as well as IP addresses removed from the list of addresses to be sent to remote stations.



Stop SMS delivery allows to discontinue SMS delivery. This entry is available if the subsystem is configured and enabled. The delivery will be discontinued until another manual clicking on this entry. The Control Center will remind from time to time that you have disabled the delivery by gen-

erating the code. The interval of reminders is specified in the Settings of Control Center (see below).

Program Settings

All the Settings are arranged into several categories:

Connection

In this category an operation mode is selected (local or distributed). It is critical when making CMS of several workplaces. Database connection parameters are also set.

Clients

This category provides allocation of message receipt responsibilities for operators.

Event sources

This category of parameters allows for configuring of event reception channels. The details of configuration of each reception channel are given in individual sections. To configure a channel, the corresponding category shall be determined. Each subcategory allows for adding of event sources using the "Add event source" button. Each source can be enabled (use a device) or disabled selecting the relevant option.

SMS subsystem

This category provides the configuration of connection of "Orlan-SMS" module.

Advanced

This category has the additional service options (automatic actions, remote configuration settings, FTP repository path).

Orlans check

This category provides the configuration of parameters of check of "Orlan-M" Voice Channel modules.

Backup

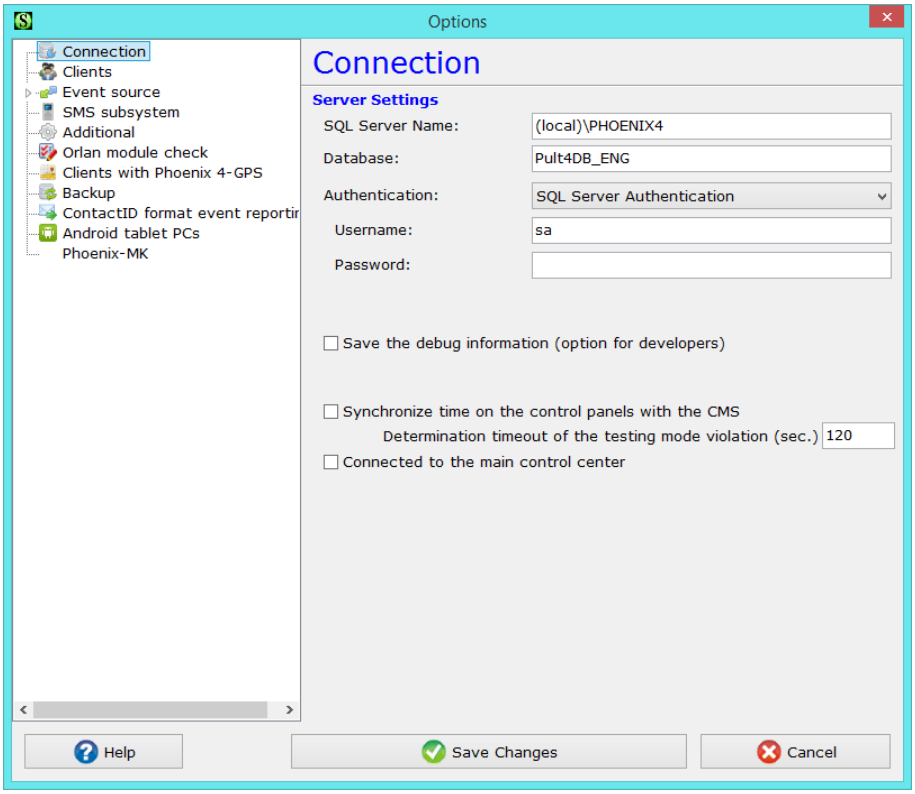
This category provides the configuration of backup.

ContactID event transmission

This category allows for configuring of ContactID event transmission to the third-party CMS software.

When checking a category (subcategory) in the left corner, the configurable parameters appear in the right corner of the window.

4.4.1. Connection



"**Synchronize time on the control panels with CMS**" option. When this option is selected, CMS time will be synchronized with the real-time clock of object Control Panels. Synchronization is carried out once in two days only via GPRS channel (VPN network or Internet). In case a device is not configured to operate via this channel, it cannot be synchronized. For any device the clock zone can be moved with respect to the time of CMS clock (specified when configuring the devices using Configurator 11). This function is available ONLY for "Lun-11", "Lun-19", "LanCom" and "Lun-23" devices.

"**Determination timeout of the testing mode violation**" parameter (in seconds).Control Center monitors the self-testing of devices. The value of this parameter is always added to the testing period set when configuring "Lun" Control Panels. The minimum value is 30 seconds.

"**Connected to main Control Center**" option shall be selected for all auxiliary Control Centers, and the name of computer on which the major Control Center is installed shall be specified.

"**SQL Server Name**" – network name of the computer with MS SQL DBMS and database (default local computer) installed shall be specified. Named instances of SQL Server are also supported.

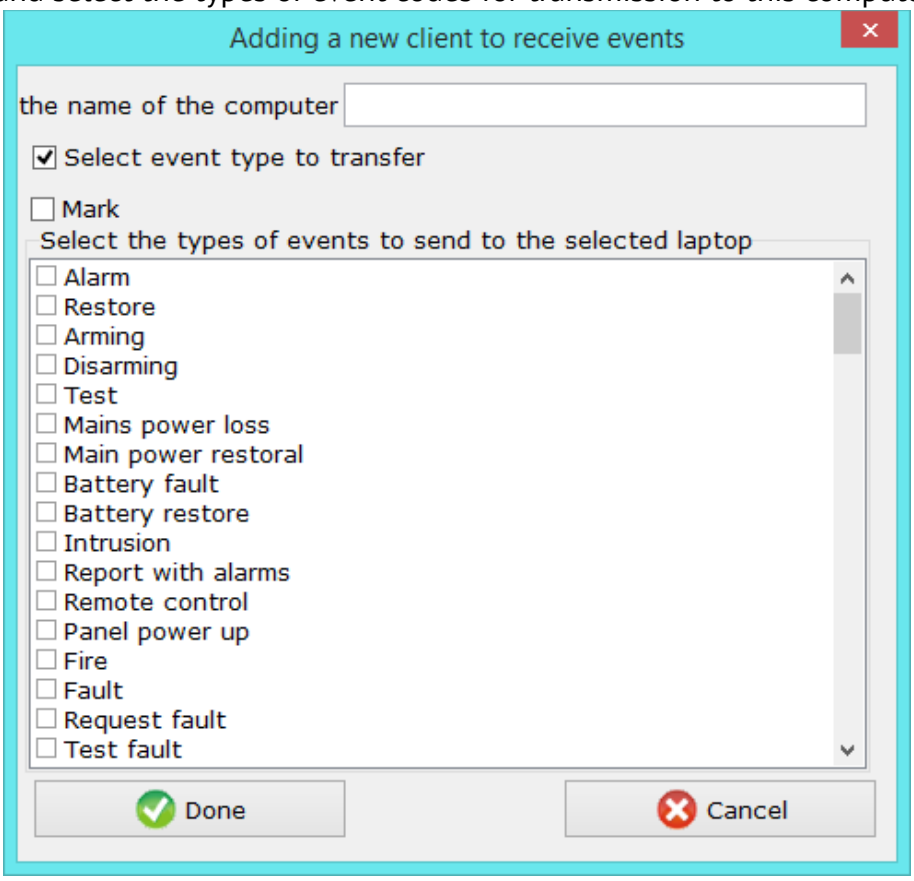
"**Database**" – database name (default name – Pult4DB), "**Authentication**", "**Username**", "**Password**" provide the configuration of connection to MS SQL Server.

Attention! If you are not the System Administrator and do not clearly understand what these MS SQL Server Settings options are for, do not change them!

4.4.2. Clients

This category allows for setting of network parameters for operators' workplaces. In other words, you specify the names of computers in LAN, where "Duty Operator" is installed and runs.

In addition, when you press "**Add**", a window opens, where you shall specify the name of operator's computer and select the types of event codes for transmission to this computer.



In this window, you can specify which codes and to which computer with "Duty Operator" will be transmitted. Therefore, you can allocate the operators' responsibilities.

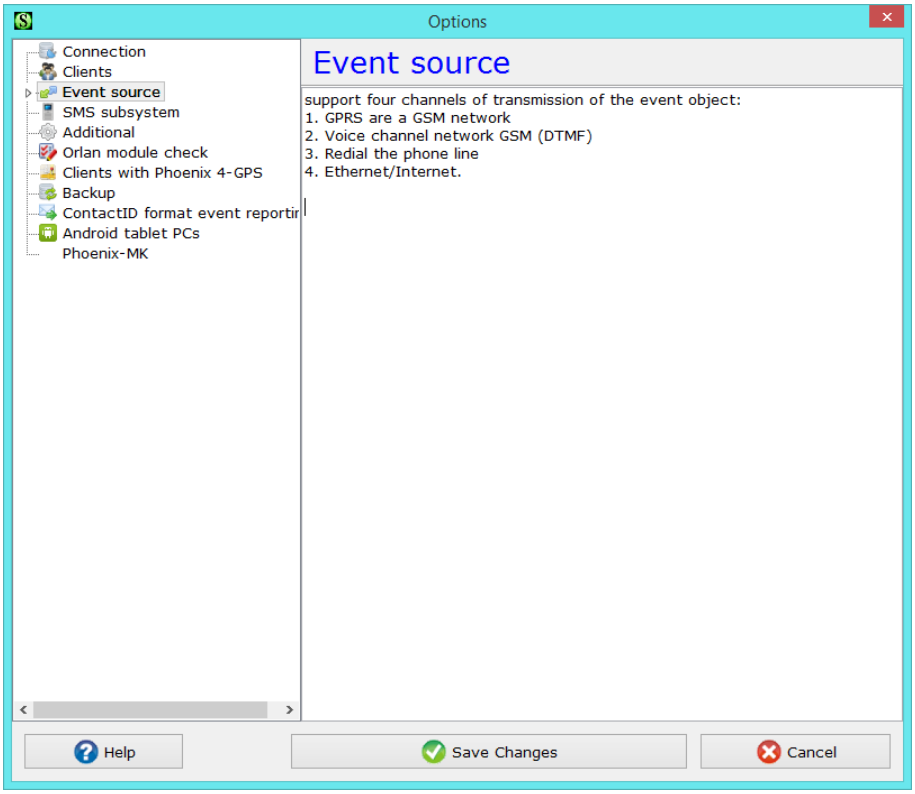
To distribute events among different computers you shall do the following: specify the computer's name and specify required code types for each computer.

Attention! If you need a computer that will receive ALL types of events, you STILL shall select the "Select event types for transmission" option and select ALL event types on the list. In other case, distribution between the computers by the event types will not be active!

In case you always need to add clients without any filters, i.e., clients to which all the events will be transmitted, you do not need to select all the types; you shall only enter the computer's name (or its IP address) and click **Done**.

"Duty Operator" has the "**Show all**" option in the "**Unprocessed**" window. In case this option is deselected, the filtration will be carried out according to the clients' settings, if this option is selected, clients will NOT be filtered.

4.4.3. Event source

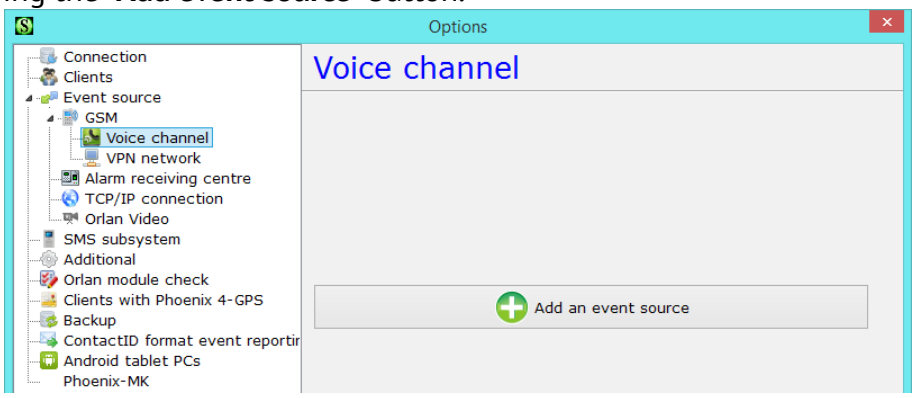


This category of parameters allows for the configuration of event reception channels.

Four event reception channels are supported:

- Voice channel;
- VPN network;
- Auto dial stations;
- Ethernet/Internet channel.

The details of configuration of each channel are given in an individual section. To configure a channel, the corresponding category shall be determined. Each subcategory allows for adding of event sources using the "**Add event source**" button.

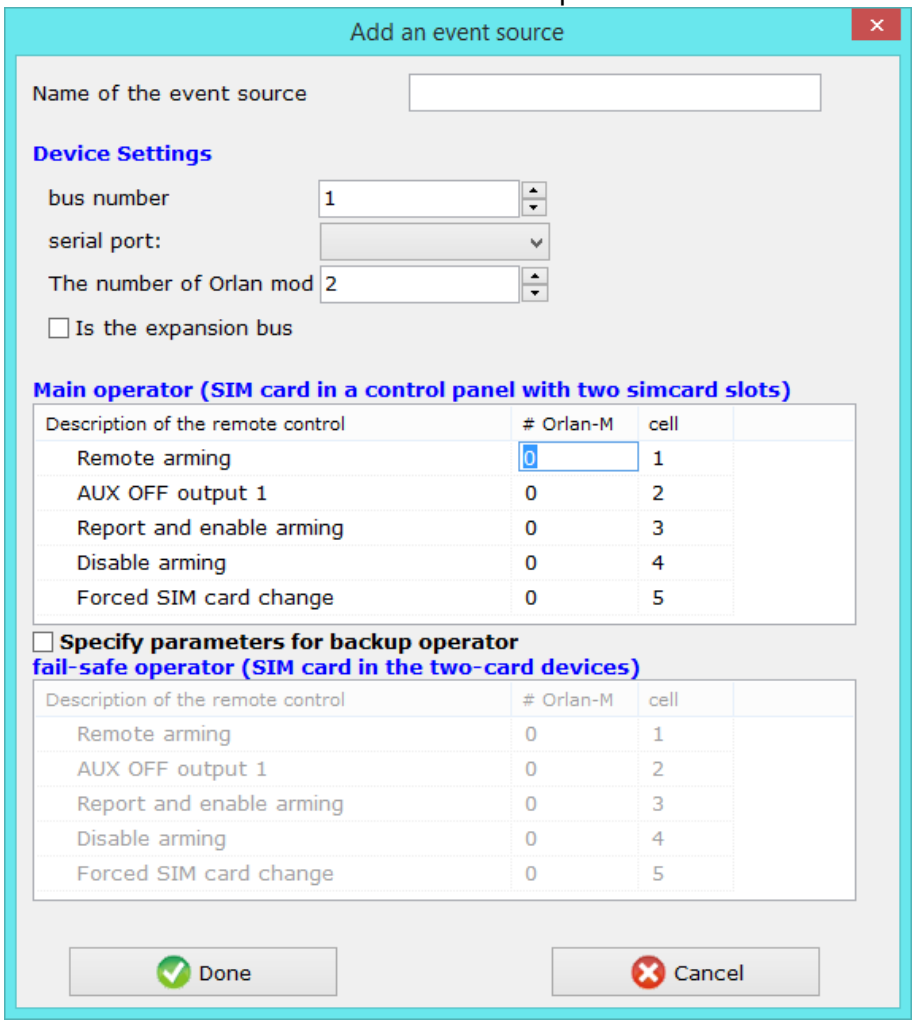


Each source can be enabled (use a device) or disabled selecting the relevant option.

4.4.4. Voice/CSD channel

Attention! Voice Channel event source also provides the reception of events via CSD channel. No additional configuration of Control Center is required (see below).

To configure the voice channel event source, select the "**Voice Channel**" connection option, and then click "**Add new event source**" button in the window opened.



After that, enter "**Name Event Source**" (as you prefer).

Then, specify "**Bus Number**".

Attention! When messages are received via the voice channel, in the "Channel" field of "Duty Operator" a channel number will be displayed. In this number the first digit is a number of bus and two last digits are a number (address) of "Orlan-M" module, which received the message, e.g. 112 – bus No. 1, 12 – "Orlan-M" modules number (address).

After that, specify the "**Serial port**" number (see the device manager) that will be connected to this bus, and "**The number of Orlan modules**" (longest "Orlan" address on the bus).

To configure the remote control via the voice channel, you shall set the parameters for the main operator and the backup one (if any).

"**# Orlan-M**" is a sequence number (address) of "Orlan-M" module connected to this bus.

Important Note! In case your CMS is equipped with a new "Orlan-M11" module, this very module must be in the third position of "Report and enable arming". Otherwise, the remote control over "Lun-11" devices will not be available neither via the voice channel, nor via CSD channel.

To change any parameter, left-click the number of parameter to be changed and set the required value.

"**Is the expansion bus**" option allows to specify that this bus is additional in relation to the one on this or any other computer. This option is enabled if the number of Orlan-M voice modules is above 32.

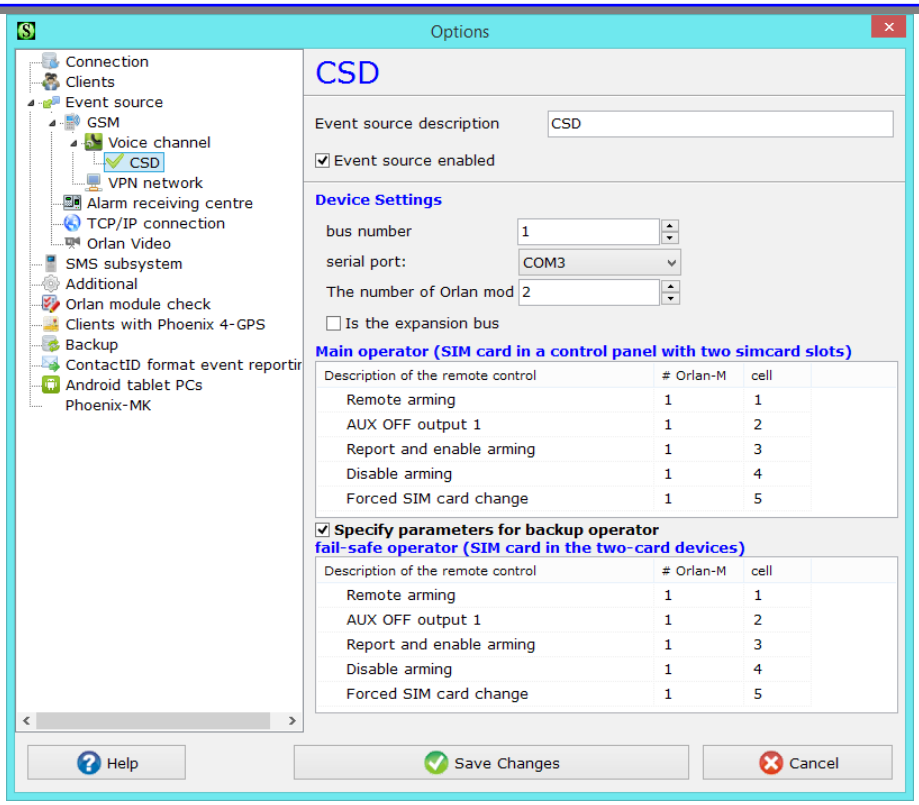
The remote control over object's Control Panels is carries out using "Duty Operator".

Upon entering of all the data, enable "**Event Source Enabled**" option and click "**Save Changes**".

In case there are any event sources of "Voice channel" operating on other bus, the procedure shall be repeated setting the required parameters.

Upon completion of creation of the voice channel event sources, go to "Orlan-M" modules check configuration.

"Phoenix-4" support CSD event transmission channel. Only "Orlan-M11" modules support this channel; the only difference is that only one module can provide the remote control over all the function, e.g., as shown in the Figure below:



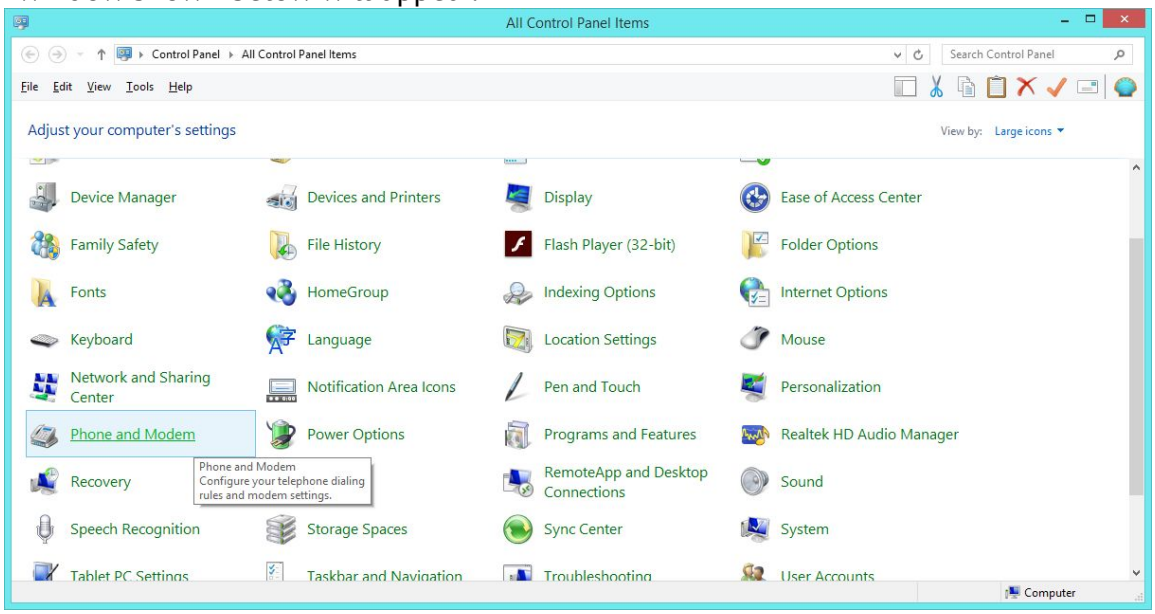
4.4.5. GPRS channel

To configure GPRS channel, the following is required:

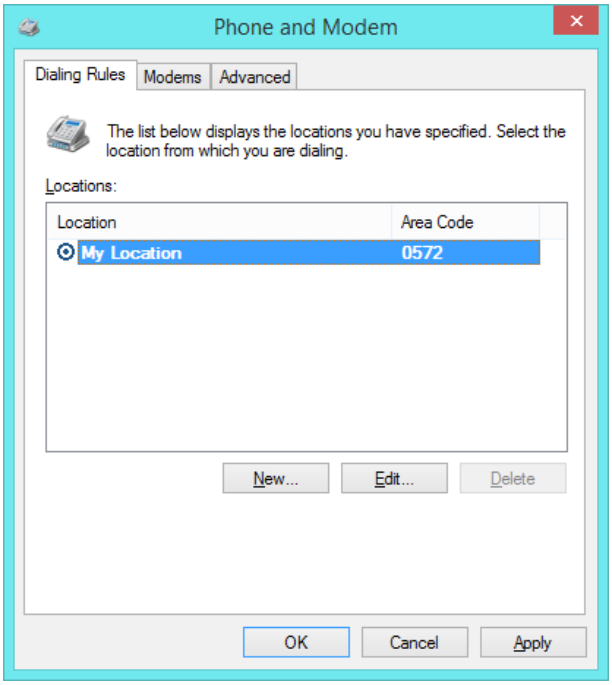
1. "Orlan-Mi" receiving modules.
2. Virtual sub-network provided by the mobile operator, with APN, login, password, and phone number.
3. Two SIM-cards of the mobile operator with IP-addresses of the provided network.

Attention! As GPRS is an Internet connection, you shall add modems to Windows OS and create network links (according to the number of "Orlan-Mi" modules).

To add a modem to the system, click Windows button **START**, select "**Settings**", and "**Control Panel**". A window shown below will appear.

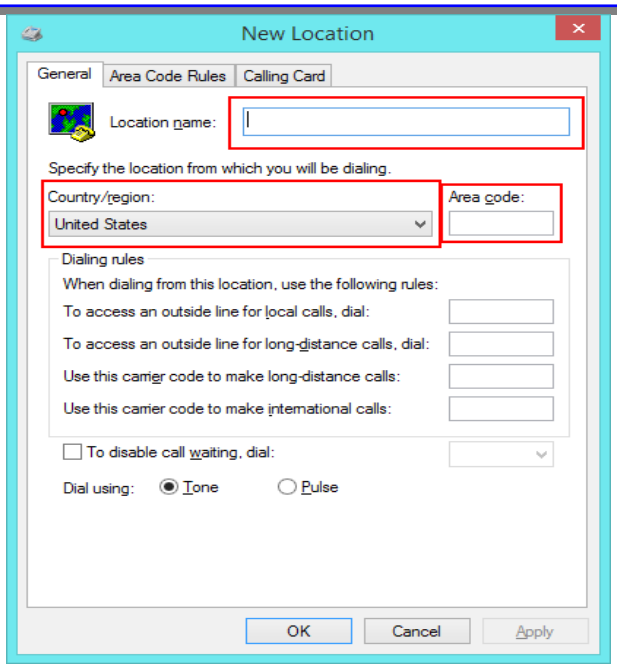


Double-click the "**Phone and modem**" icon. A window with the same name will appear.

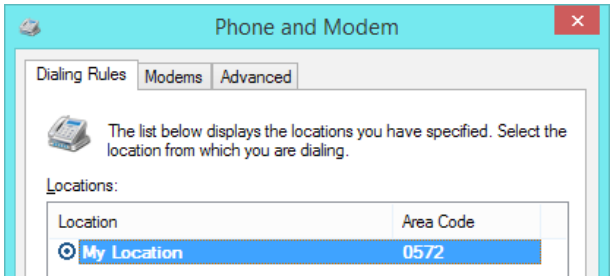


If the list is empty, click "**Create**", in the "**New location**" window fill in the parameters "**Location Name**", "**City Code**" and select your region from the "**Country and region**" drop-list.

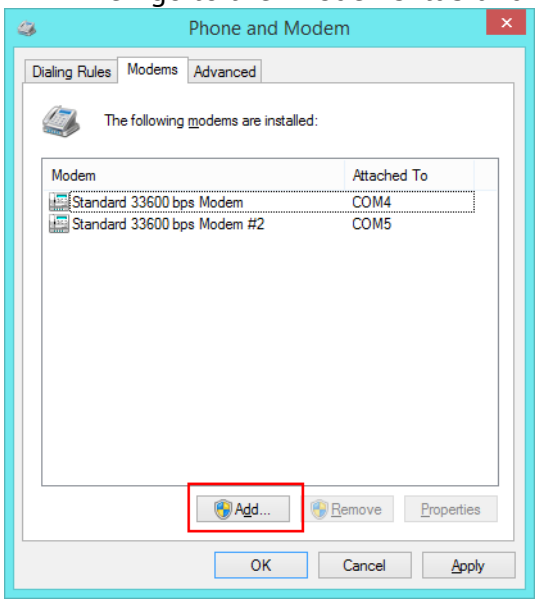
Attention! In the "New Location" window only the above-mentioned parameters shall be filled in and only once if there are no entries in the "Dial-up" tab of "Phone and modem". These parameters have no relation to CMS, thus, any values will do (for example, those shown in the Figure).

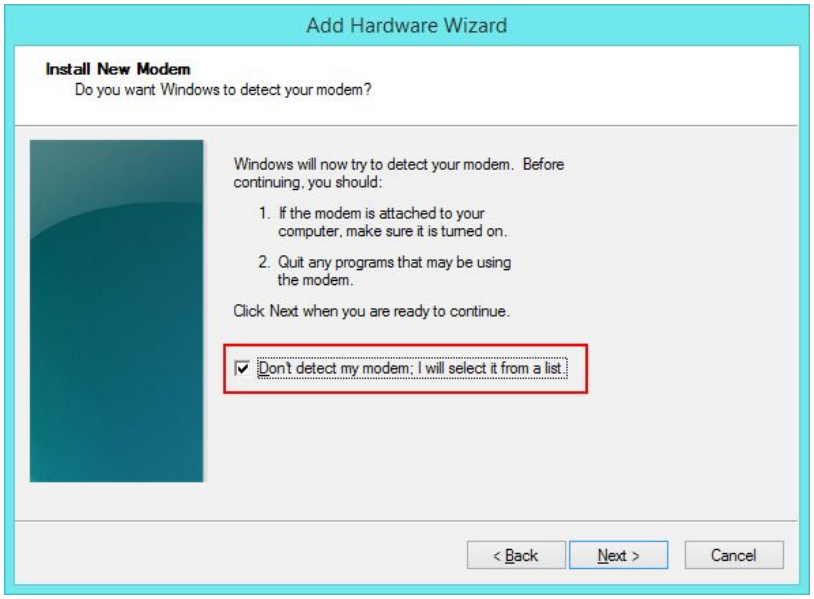


The window will look as follows:

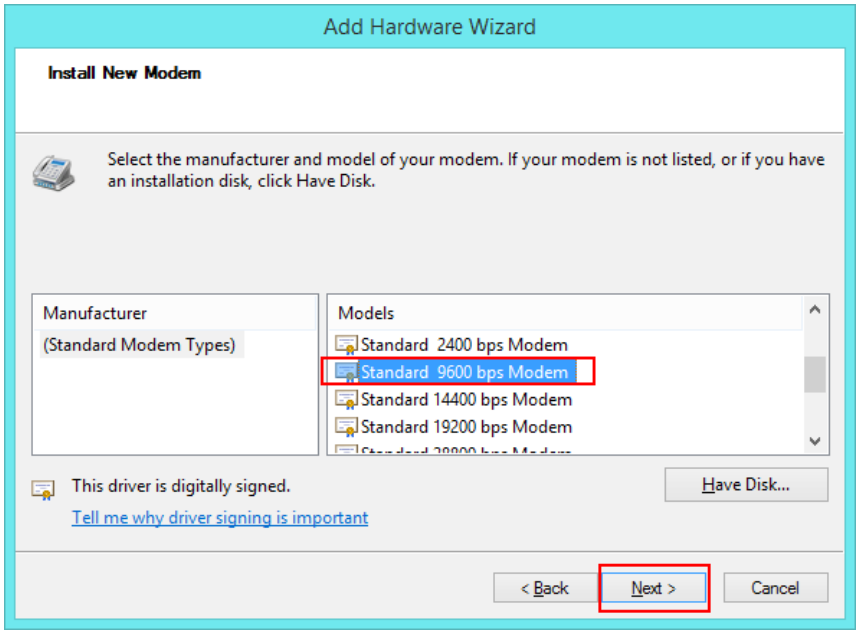


Then go to the "**Modems**" tab and click "**Add**":





In this window select the "**Don't detect my modem**" option and click **Next**.

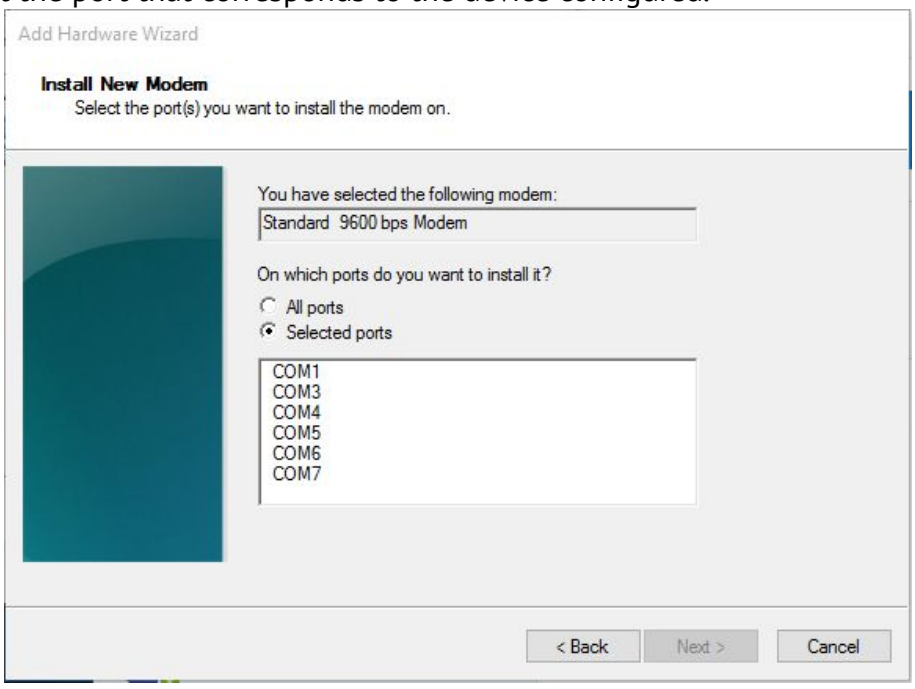


Attention! The speed of the created modem depends on the type of GSM module mounted on "Orlan-Mi" board. In case the model of the mounted GSM module is "Quectel M72"

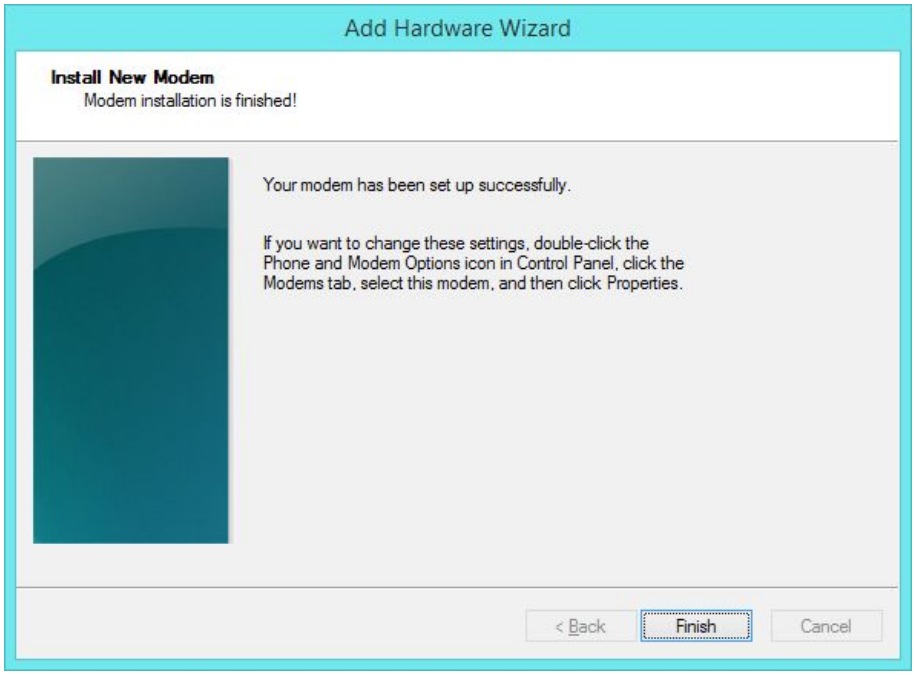
Select **Manufacturer** –> **Standard modem types**, and **Model** –> **Standard modem 9600 bps** or **Standard modem 33600 bps**.

Attention! The type of Orlan module "33600 bps" is marked on the module. If there is no marking on the module, you shall select "Standard modem 9600 bps".

Click **Next** and in the next window enable the "**Selected ports**" option. In the list of available COM ports select the port that corresponds to the device configured.



Click **Next**.



A message of successful modem installation will appear, and an entry with the name of modem and COM port to which it is connected will appear in the list of modems.

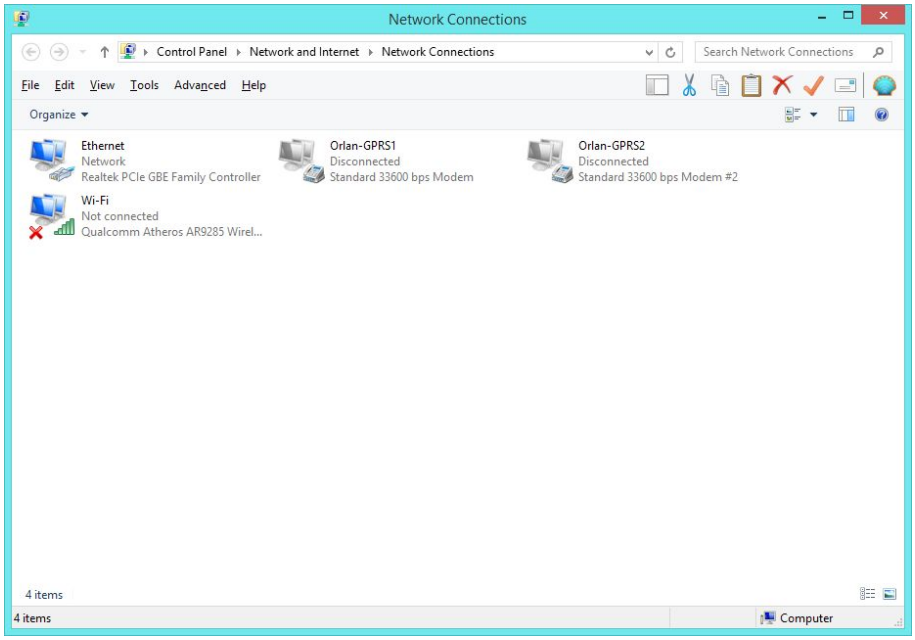
Other modems are added in the same way.

At the next stage, network connections are created. This stage of configuration is controlled by the "**Configure GPRS Connections**" program. The program is launched from the Windows **Start** menu from "Phoenix4" software package.

Attention! Network connections shall be created with all USB cables of "Orlan-Mi" modules connected.

Upon launching, a work window of the program appears. In this window you shall enter the data provided by your mobile operator, and click **Create**. After that, error messages can appear (see GPRS channel configuration errors).

The program will configure the modems, create and configure the network connections that will be seen in the "**Network Connection**" windows.

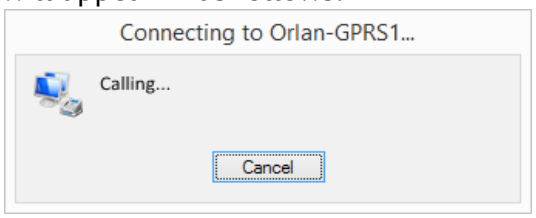


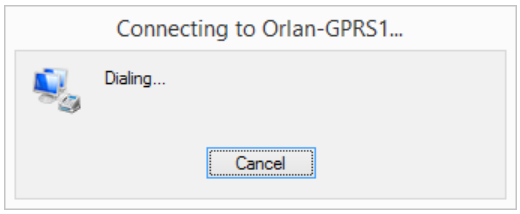
Attention! At the end of this stage, it is recommended to restart the computer.

Attention! After the computer is restarted and prior to the first launch and configuring of the "Monitor" program, check the performance of the connections created.

When checking the performance of the connections you can see IP addresses of SIM-cards inserted in "Orlan" modules.

To do this, double-left-click the "Orlan – GPRS 1" connection icon in the "Network Connections" window, and wait until the connection is established. In the process of connection the following messages will appear in as follows:

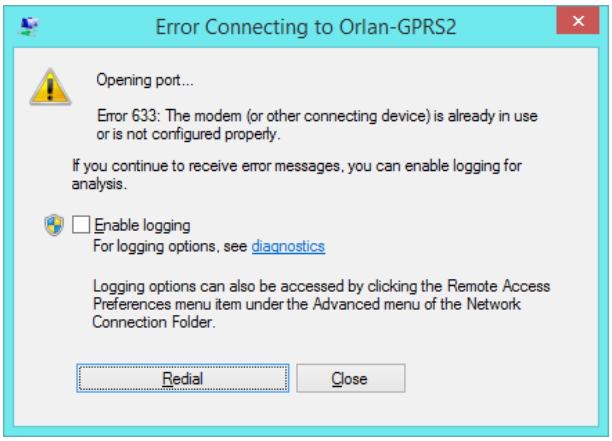




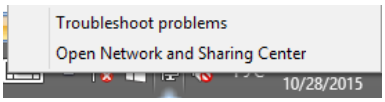
If the connection is normal, a successful connection message will appear in the right bottom corner of the monitor.

Launch and check the "Orlan – GPRS 2" connection in the same way.

In case a "**Connection error**" message appears (see the Figure below), click **Cancel** and see "**GPRS channel connection errors**".



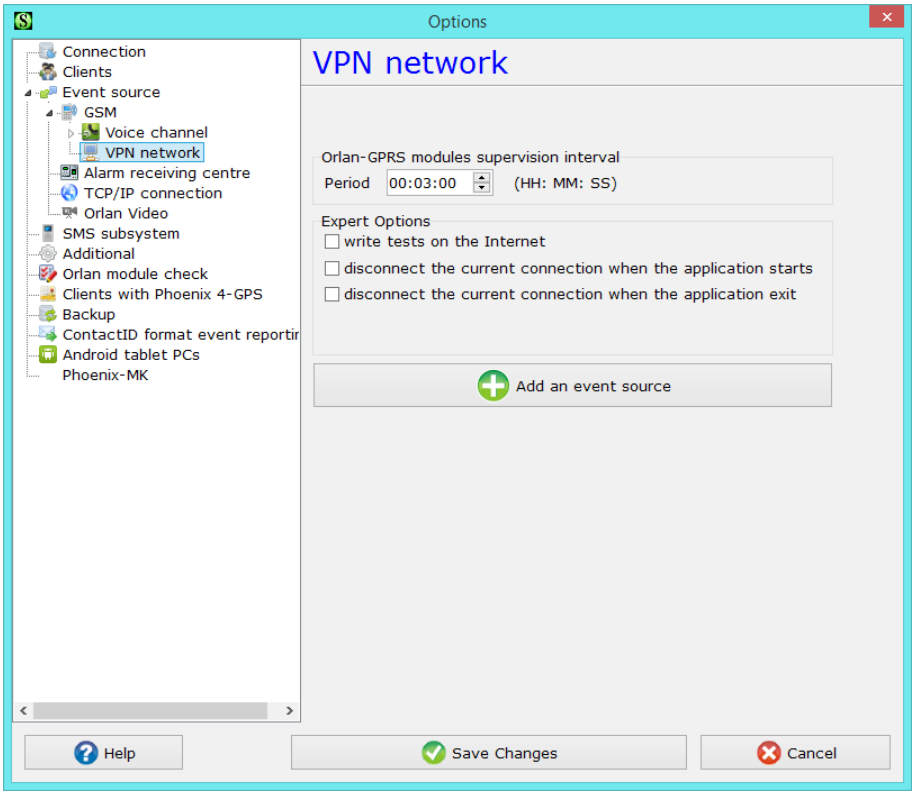
To learn IP-addresses of SIM cards of "Orlan" modules, right-click the icon near the clock on the monitor as shown in the Figure below:



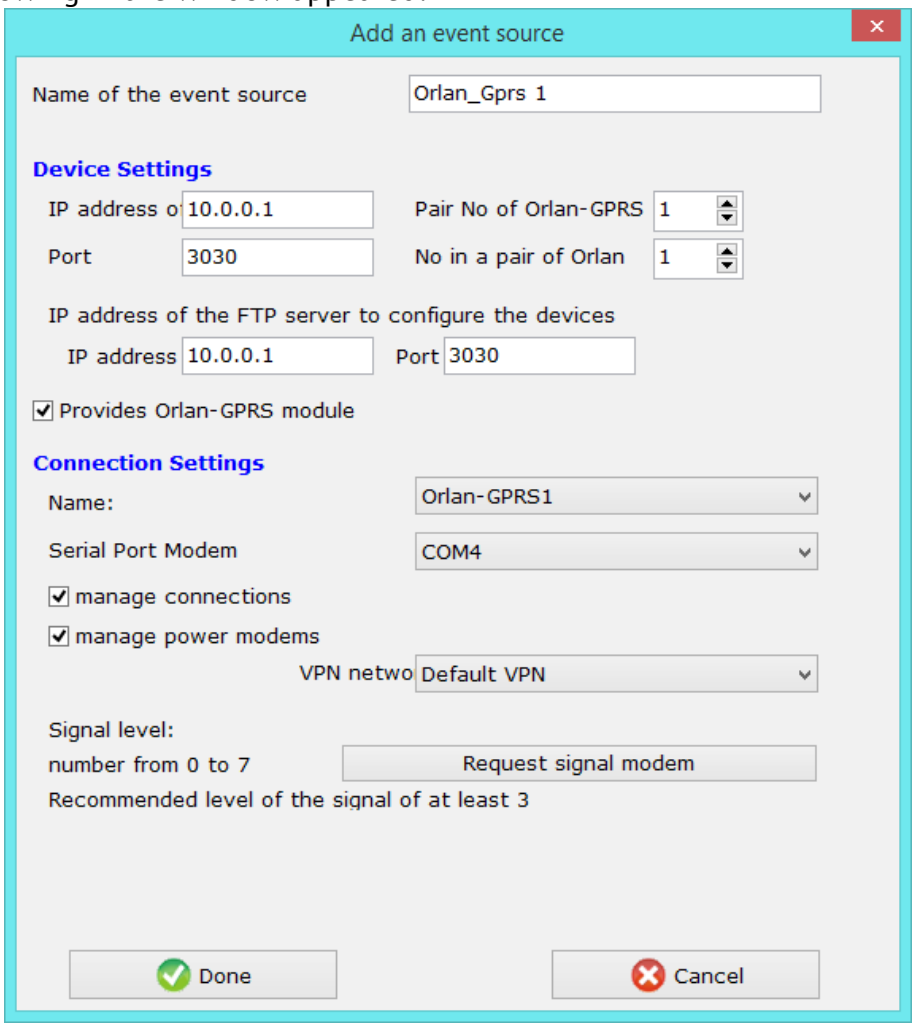
In the pop-down context menu select the "**Status**" option. In the appeared "**OrlanGPRS1 Status**" window, select the "**General**" tab. The view of OrlanGPRS1 status window with active "**Data**".

In case both the connection have successfully connected, disconnect them and proceed to creating of event sources in the "Control Center" program.

To do this, go to "**VPN**" and click "**Add new event source**".



Do the following in the window appeared:



1. Enter the **event source name** (at you choice).
2. Enter **IP address** of SIM-card used for this event source.

3. Enter the number of TCP **port** via which events will be received (default value is 3030).
4. **Address** and **port** of **FTP server to configure devices** is an external IP address of the computer on which FTP server is installed to configure "Lun-11" Control Panel.

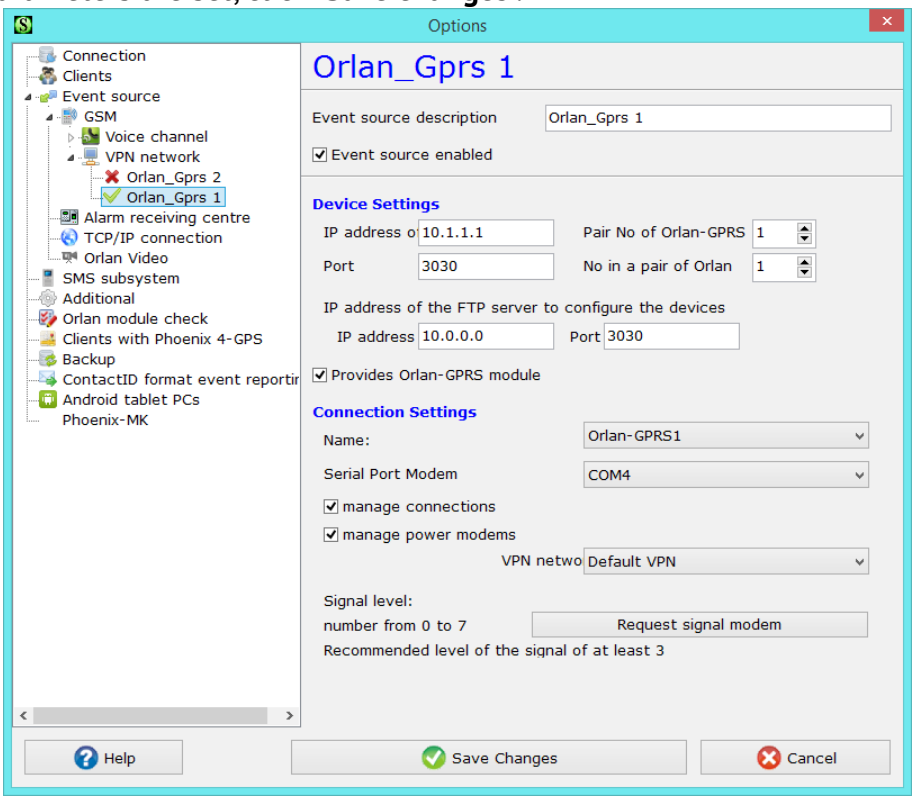
Attention! "Lun-11" devices are configured remotely using FTP server. To provide the correct operation of these devices, FTP server shall be installed and the above-mentioned parameters shall be set correctly.

5. Select the network connection name in the list as it is displayed in the "**Network Connections**" window.
6. Select **Modem serial port** on which the connection was created.
7. Enable the "**manage connections**" and "**manage power modems**" options.
8. Select **VPN name**, if there some of them.

Attention! This parameter shall not be changed. It is used ONLY when there are several VPNs in CMS.

This parameter is strongly related to the remote control and check of Orlan-GPRS modules. GPRS settings of the Control Panel have the same parameter; VPN name shall be the same for all the Control Panels connected to this Orlan-GPRS module.

After the parameters are set, click "**Save changes**".

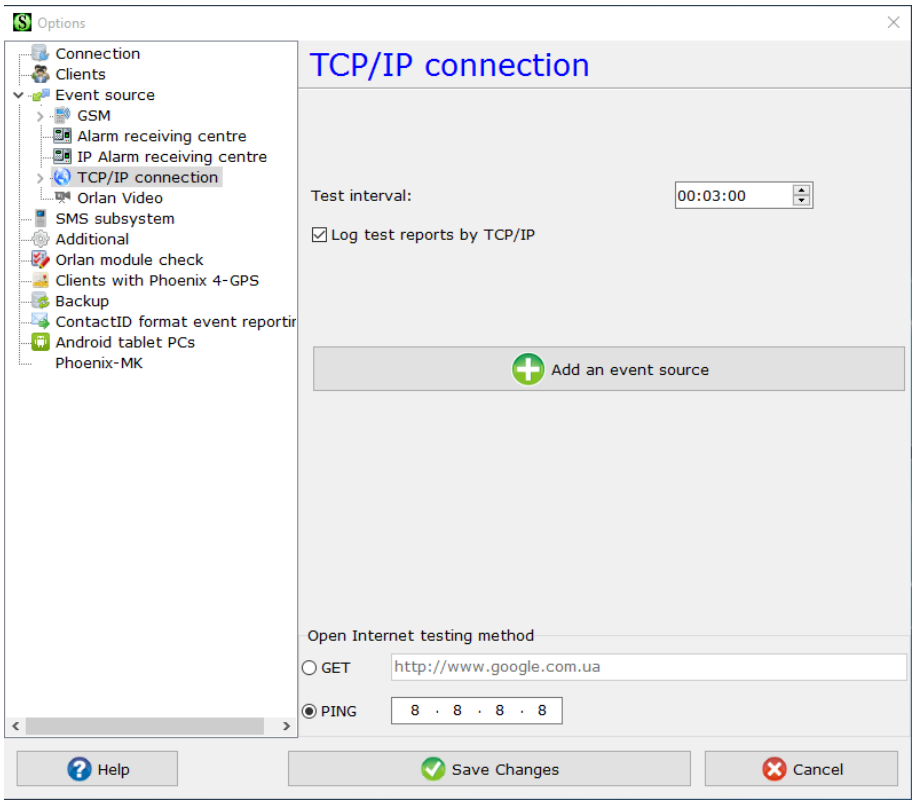


After the "**Request signal modem**" is clicked, a number in the range of 0 to 31 will appear that shows the signal level of "Orlan-Mi" module. Larger value corresponds to a higher quality signal.

If any other program is using COM port, close it. If this connection is not established, disconnect it. If any internal modem error occurred in the process of determination of signal level, an error message will be shown.

4.4.6. Open Internet (TCP/IP connection)

Select **TCP/IP connection** tab:



Test interval – is used for test Control Center TCP/IP connection for ensure the events from all control panels can be received. Set interval as Hours:Minutes:Seconds format.

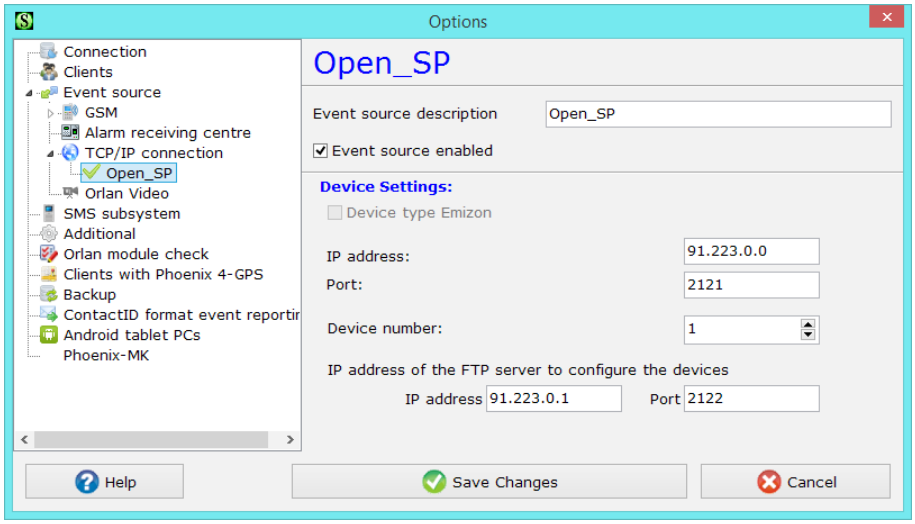
Log test reports by TCP/IP – set to enable logging tests from control panels to database.

Open Internet testing method – select one method to testing internet connection:

GET – using get http query to selected internet host;

PING – using ping query to selected IP-address.

Click **Add an event source** button:



This event source is used to receive events via Internet channel (TCP/IP, not VPN).

To add a new source, specify the following:

- Event **source name** (information field);
- **IP address** – IP address of the computer that will receive events transmitted by the object devices through the open Internet;

- **Port** – port through which events will be transmitted;
- **Device number** – every TCP/IP source should have the unique number.
- **IP address and port of the FTP server to configure devices** – external IP address of the computer, on which FTP server is installed to configure "Lun-11" Control Panel;

Attention! "Lun-11" devices are configured remotely using FTP server. To provide the correct operation of these devices, you shall install FTP server and set the above parameters correctly.

4.4.7. Configuration of auto dial channel

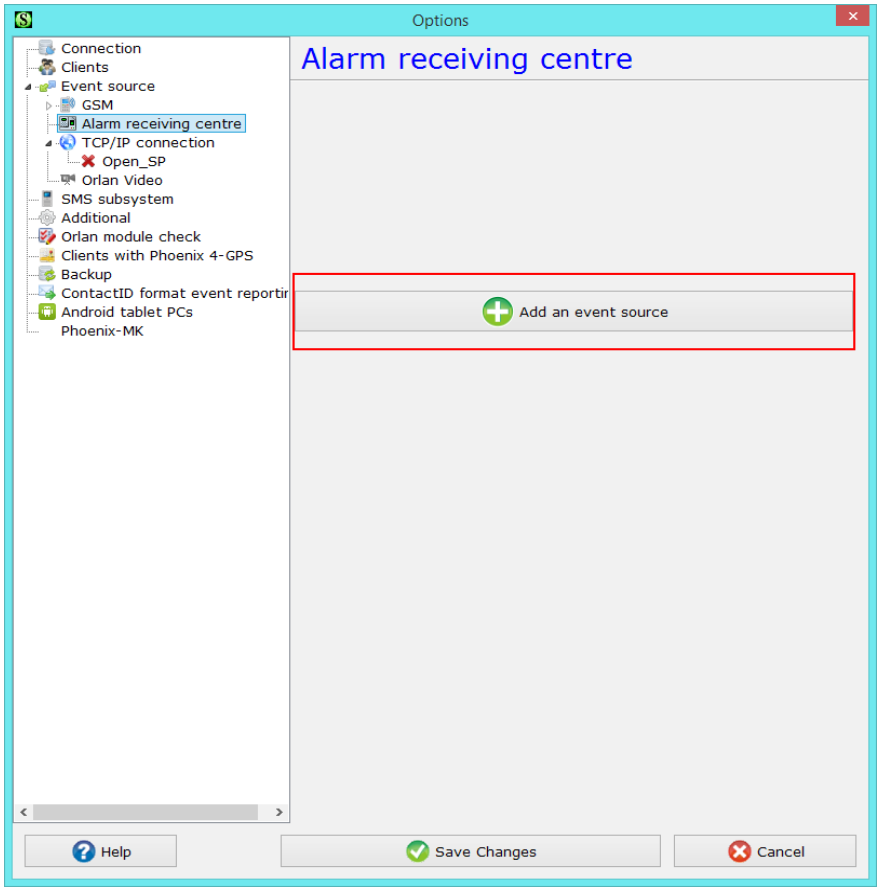
The auto dial channel can have various receiving stations as events sources, which support various protocols: pulse 4+2, contact ID, SIA (Level 1, 2, 3), Ademco685, SilenKnight Express, and other protocols.

These protocols are supported with base receiving stations connected via RS-232 or USB ports (through virtual COM port).

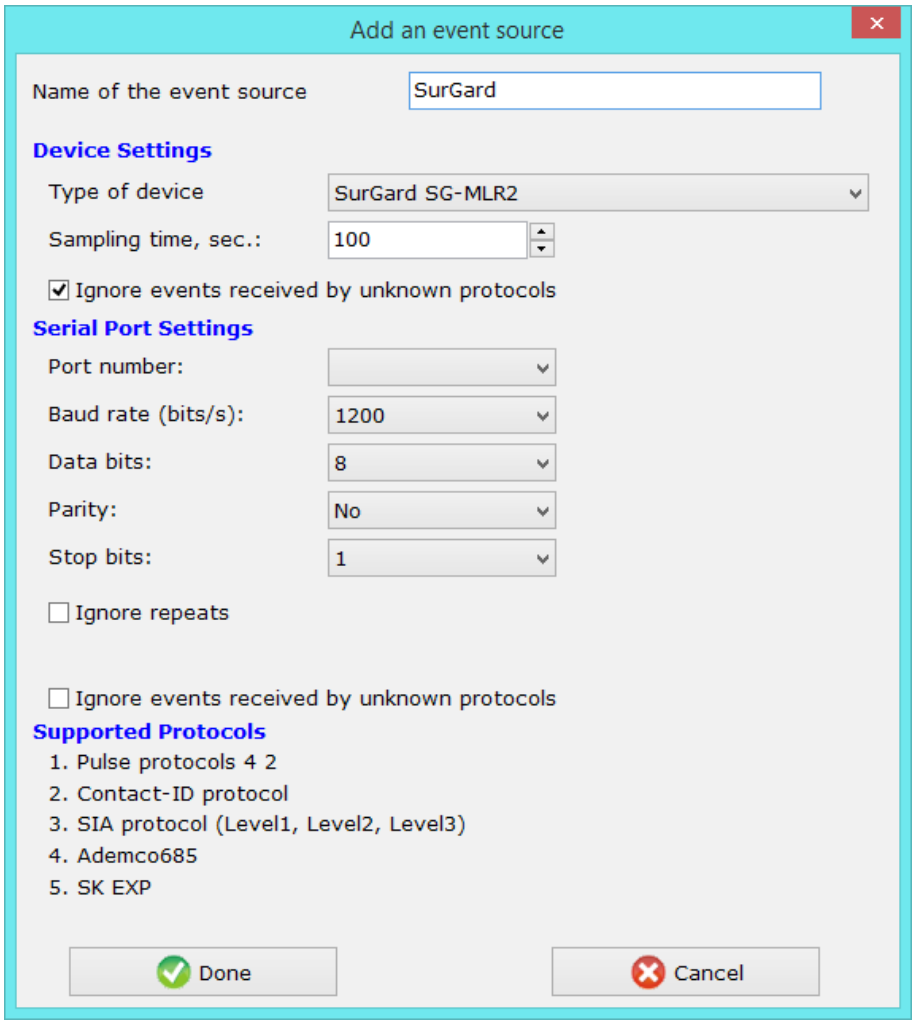
The following receiving stations are supported:

- SurGard SG-MLR2;
- SurGard PC-LC2;
- SurGardSG System III;
- ADT "Pakt-2", "Pakt-2P";
- "Contact" by Rhythm;
- "Virial-RFM";
- "Blits";
- SilentKnight SK9500;
- "Barier SB";
- "Megaluks" Protocol Station;
- "Akkord" Protocol Station.

In case one of the above stations is connected, there is no need to set any additional settings of COM port, the required settings will be set automatically. You will only need to select the "**Device type**" from the drop-down list after you enter the information in the "**Name of the event source**" field.



In case any other device is used, which is not on the list, you shall select the "**Other receiving device**" option in the "**Type of device**" drop-down list.



Ignore repeats within, sec (default value – 10). This option is required only for radio protocols to correctly recognize new events. Within the time specified, repeated events will be ignored.

Save all events in BlitsLog.txt. This option is used only by "Blits" receiving station. If selected, all repeated events will be saved in a text file for further analysis.

Attention! The "Ignore events received by unknown protocols" option shall be enabled only if you cannot switch off the protocols that are not on the "Supported protocols list", when configuring the receiving station.

Enabling of this option allows to avoid the situation when "Control Center" cannot recognize a message and, thus, does not give a receipt, thereby, blocking receipt of further messages. Such messages are cleared with the following code generated:

FZ3 Attention! Message received in unknown protocol through telephone line

Example. Configuration of **Sur-Card SG-DRL2**

To provide the correct interaction between the computer and Sur-Gard SG-DRL2, you shall configure the latter correctly.

To view/change the settings, switch to the mode of configuring of the general settings, pressing **Escape**.

The default password is "**CAFÉ**".

Navigation is provided by "**Tx**" and "**Rx**" buttons.

Select option "**05: Com1 Config**".

To enter an option, press "**ACK**".

The following parameters shall be set:

Br (BitRate) = 12

Bits per byte = 8

Pa (parity) = 2

After the parameters are set, go to option "**06: Com1 Format**" and set the current format – **4** (Sur-Gard SG-DRL2 – to – COM port communication protocol).

To exit the configuration mode, press **Escape**.

Be sure to connect the computer to COM1 of Sur-Gard SG-DRL2 only!

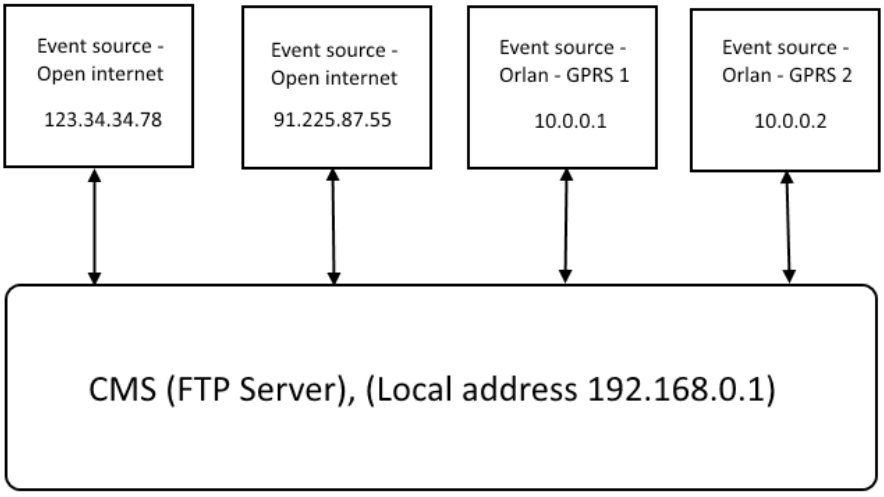
Example. The required settings of "**SilentKnight SK9500/9800**" receiver:

1. Operating mode – **Automatic** (see details in SK9500 Manual, section 7.1.1);
2. Port functions – COM1 = **Automation** (sect. 7.1.3.1);
3. COM1 port settings – **speed=38400, D=8, S=1, P=No, PortMon=Yes, F=None** (sect. 7.1.3.2);
4. Protocol – **SK EXP** (sect. 7.1.3.5);
5. IMPORTANT! (sect. 7.1.2) CID parameter = **Code** (see details in SK9500 Manual, pages 5-10);
6. Correct date and time.

4.4.8. FTP protocol remote configuration

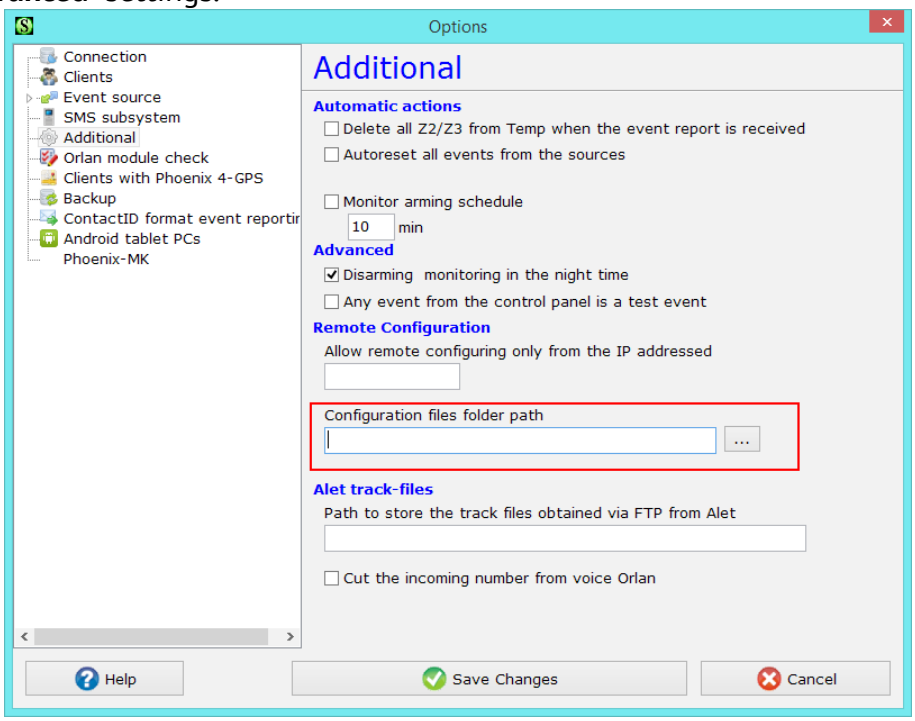
This section has the details of unrolling of FTP server (servers) for remote configuration of devices, and the required settings of the Control Center and operation procedure.

The remote configuration of "Lun-11" device is carried out via FTP protocol. FTP server shall be installed in CMS (can be find on "Phoenix 4" software disc). For each event source, whether it is the open Internet or Orlan-GPRS modules (VPN), you shall specify the address, through which you can connect to FTP server form the outside.



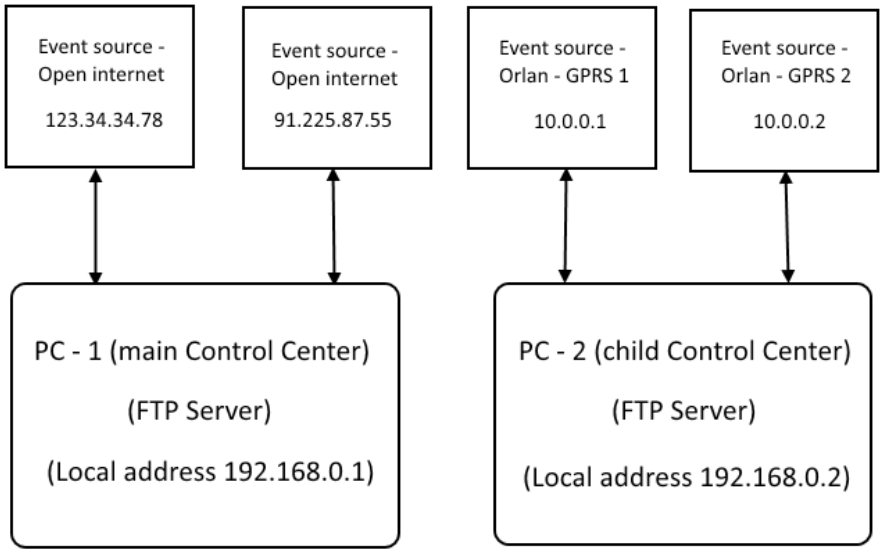
In this example, you can see **four** event sources created in CMS – two event sources via open Internet and other two via VPN using oral-GPRS modules. For each event source, its IP address (source address) and not CMS local address will be FTP server address.

"**FTP server address**" will differ from "**Event source address**" only when FTP server is installed on the computer with no Control Center or event sources, for example, on the server provided. In this configuration, the "FTP server" parameter will be an external IP address of the computer with FTP server. In this case, the repository of FTP server shall have the shared access and shall be specified in the "**Advanced**" settings.



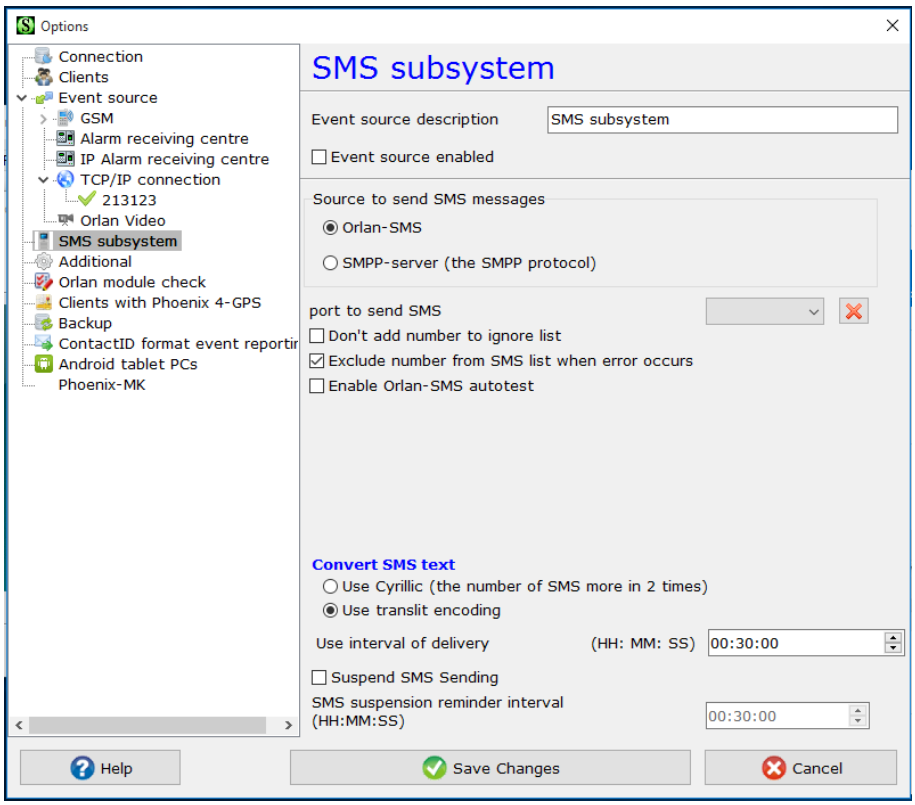
In any case, the repository path shall be specified, regardless of whether FTP server is installed locally or not.

Let us consider the variant with two computers for CMS, to one of them two Orlan-GPRS modules are connected, and on the other one two event sources have been created via the open Internet. The easiest way would be to install two FTP servers (on each computer) and set the settings for each computer locally (as for two independent CMSs):



Attention! "Open Internet" event sources shall be ONLY on the computer with the main Control Center.

4.4.9. Configuration of SMS subsystem



There are two ways of sending SMS: via "Orlan-M (SMS)" module or specific service of the provider using SMPP protocol.

You shall choose SMS sending source:

- Orlan-SMS (specify the port via which SMS will be sent);
- WEB server (via SMPP protocol).

In case SMS are sent via "Orlan-M (SMS)" module:

Select **COM port**, to which Orlan-SMS module is connected. To clear the port, click .

The selected "**Exclude number from SMS list when error occurs**" option provides deletion of a mobile number from the messaging list in case any error occurs. The following errors can occur:

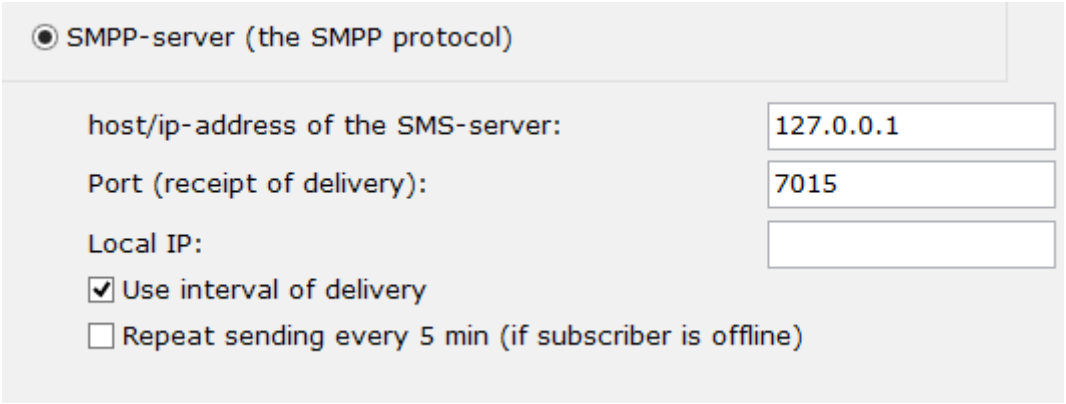
wrong number, number does not exist, or number not serviced. The deleted numbers list shall be available in the menu of "Control Center". The deleted numbers will save their status until Control Center is restarted or manual deletion of numbers form that list.

The "**Enable Orlan-SMS autotest**" option enables the self-testing function. In case this option is selected, the module will send SMS to itself with the interval specified. In case SMS sending or SMS receipt fails, a corresponding message will be generated. The number shall be specified in the international format.

Attention! You must remember that the less the testing interval is, the more SMS will be sent, therefore, the more funds will be deducted from this SIM card balance.

In case of sending SMS via specific service of the provider using SMPP protocol:

The specific parameters shall be set:



Host/IP address of the SMS server – IP address of the computer with SMPP server software running (manufactured by "Protection and Security")

Port (receipt of delivery) – port, via which the delivery confirmation is sent (SMS delivery)

Local IP (to deliver SMS changes) – local IP address of the computer.

Use interval of delivery – option that allows to set the "Delivery Wait On Interval" (see below).

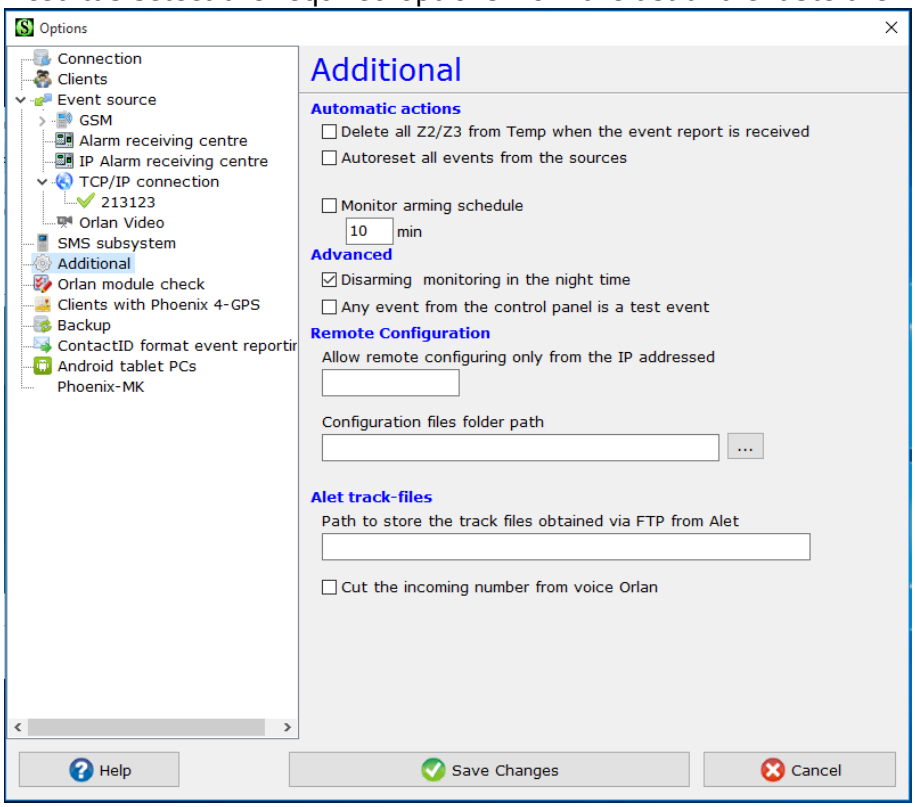
Then select the **text conversion** before sending: **Cyrillic** or **Latin** (transliteration).

In addition, "**Use interval of deleivery**" shall be specified. In case there is no delivery confirmation within the time specified, a "**SMS was not sent in time**" message will be generated.

Sending of SMS can be paused through the main menu of the program that has this option.

4.4.10. Additional Tab

In the Advanced tab select the required options from the list and enable them:



"**Delete all Z2/Z3 from Temp when the event report is received**" – if selected, when CMS receives the confirmation code, all Z2 (no test in time) and Z3 (faulty OFF code not confirmed) codes will be deleted from the unprocessed.

"**Autoreset all events from the sources**" – if selected, Phoenix 4 software automatically processes all alarm messages of all the object devices without operator (events are archived at once). Another option becomes available – "**Including moving objects**", which, if selected, provides processing of mobile objects as well ("Alet", mobile applications).

"**Monitor arming shedule**". In case you need to control the closing of s with the appropriate schedule, if you select this option, Phoenix-4 will generate alarm, if the object shall already be closed according to the schedule (armed), but remains open (not armed). The object closing timeout (in minutes) shall be set in the "**Alarm sending timeout**" parameter. In addition, do not forget to set the operation control parameters for each object, where necessary, and select the "**Scheduled opening control**" checkbox in particular – "**Operation features**" in "DB Administrator".

"**Disarming monitoring in the night time**" – makes the program switch on the siren upon receipt of opening message form any object between 10 p.m. and 5 a.m., i.e. set the response as for an alarm message. If this parameters is not set, the alarm opening will be carried out outside the working hours, individually for each object.

"**Any event from the control panel is a test event**" – if selected, every event received is considered as a test.

"**Allow remote configuring only from the IP address**". Enter **IP address** of the network, from which the remote configuration will be allowed. If the field is empty, the remote configuration is available from any IP address.

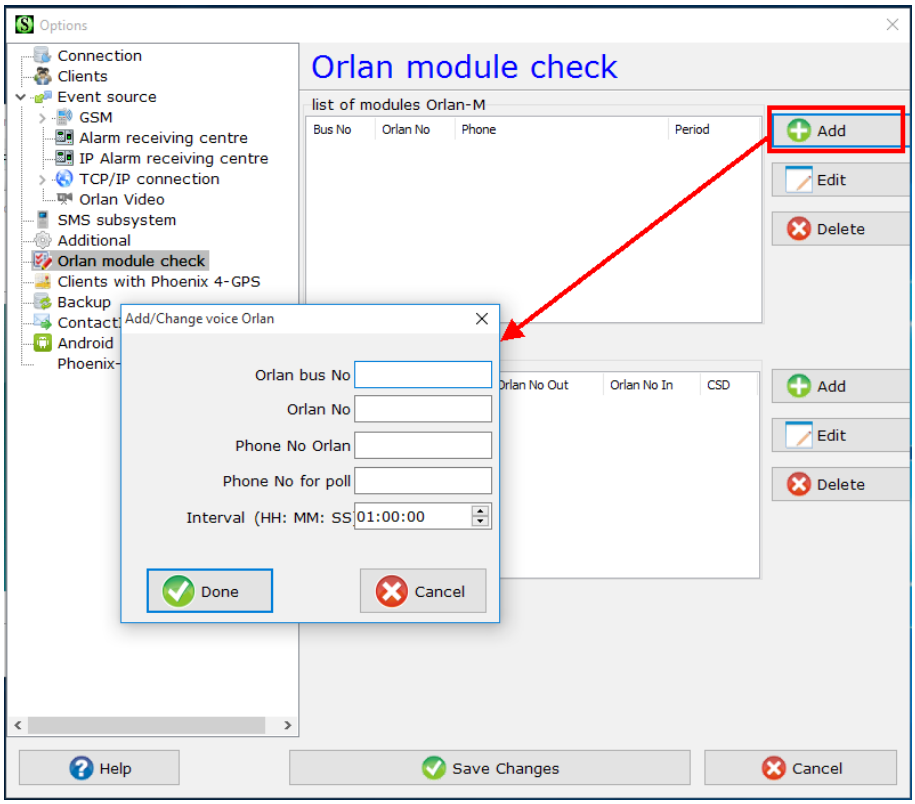
Attention! The parameters given below apply only to "Lun-11" devices. "Lun-11" devices are configured remotely via FTP server. To provide the correct operation of these devices, you shall set the following parameters correctly:

“**Configuration files folder path**” – FTP repository path. It is set when FTP server is installed manually. In this folder (repository) “lun11cfg” sub-folder will be created with the configuration files of “Lun-11” devices.

“**Path to store the track files obtained via FTP from Alet**” – mobile devices “Alet” can save its tracks (coordinates) to internal files while no GPRS connection, then upload it to CMS FTP server when GPRS connection established.

“**Cut the incoming number from voice Orlan**” – set when the incoming number is not contain the country code, so it is shorter than system expected.

4.4.11. “Orlan-M” check configuration



Go to the “**Orlan module check”** section, and click **Add** in the “Orlan-M modules list”.

In the opened window enter the **bus number** and “Orlan-M” **module number** (address).

Then enter the phone number of SIM card set in the module in the “**Orlan phone No.**” field in the format as it is recognized when received (example for Ukraine 38067...), enter the phone number of SIM card set in the module in the “**Poll phone No.**” field in the dialing format (example for Ukraine 067...).

Set the required checking **interval** and click **Done**.

Attention! The countdown of checking period restarts, when any new event is received from “Lun” device or “Orlan” module.

This procedure shall be repeated for all “Orlan-M” modules on all buses. Then set the sequence of dialing up of “Orlan-M” modules. To do this, click Add in the “Orlan-M mutual check” window.

In the opened window set which module and to which “Orlan-M” module shall call after the checking period.

High attention! There are two major approaches to configuration of “Orlan-M” modules calls:

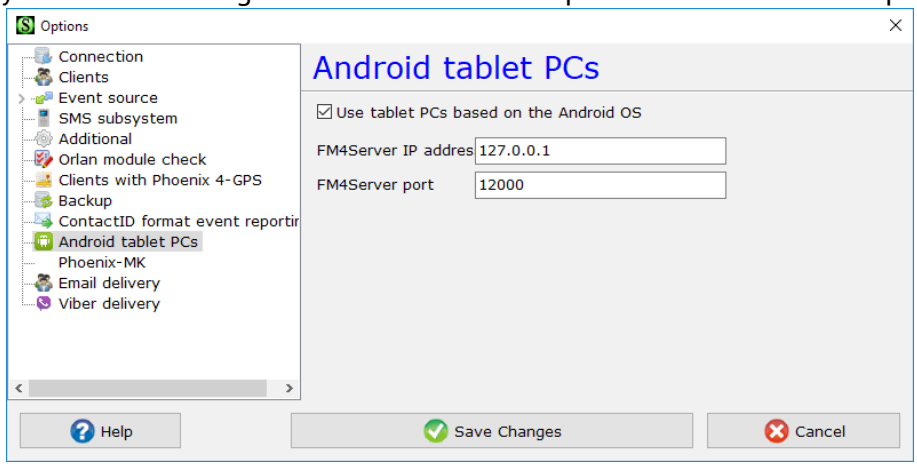
1. **One Orlan calls all the others. This approach is recommended when readdressing is not enabled.**
2. **All other Orlans call one Orlan, for which readdressing is enabled. In case of readdressing, the self-check will be available ONLY with this approach.**

Readdressing of SIM cards on Orlan modules allows to “unload” the lines in case of non uniform load on the line pairs. You shall be more attentive when configuring it though.

4.4.12. Android Tablet PCs

"Phoenix-4" supports the use of tablets with the Android operating system in conjunction with Phoenix-Mobile 4.

To do this, you need to configure the IP address and port of the FM4-Server program:

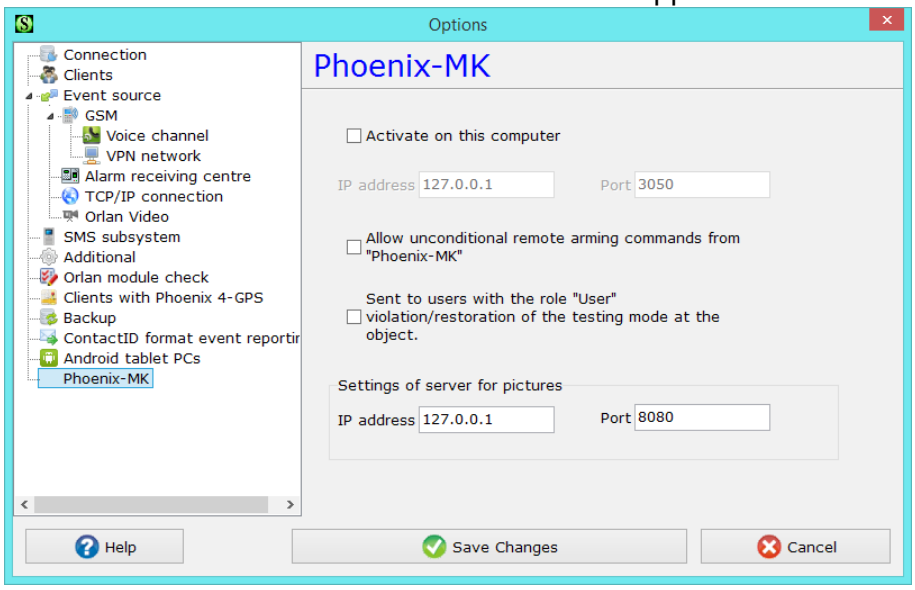


“**Use tablet PCs based on the Android OS**” – if checked the Android tablets is enabled.

“**FM4Server IP address**” – enter the IP address of the computer where the FM4Server software is installed. Don’t use IP address 127.0.0.1 for current computer – enter the real local network IP address, for example 192.168.0.120. If your CMS consists of several Control Centers (main and slaves) then you should enter this parameter on every Control Center computer.

4.4.13. Phoenix-MK (Mobile keypad)

The parameters in this tab are used for the “Phoenix-MK” application.



In the “**IP address**” field, an actual address of the computer in LAN with the installed MOBIS server is specified, as well as “**Port**” that it uses.

“**Allow unconditional remote arming commands from “Phoenix-MK”** – allows to arm the group/object without checking of the status of zones. In this case, the violated zones generate alarm with the related message transmitted to CMS.

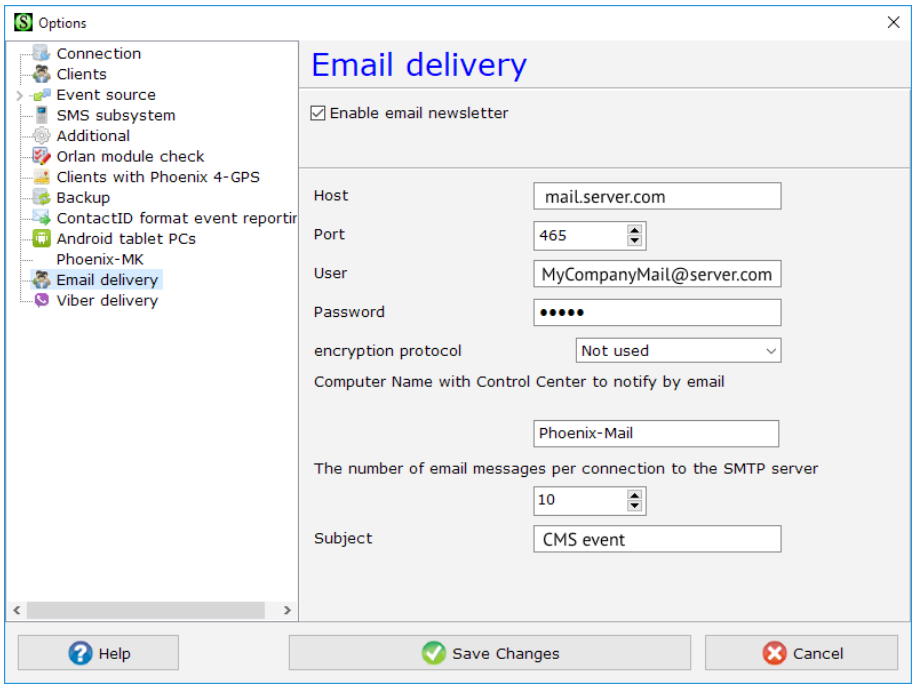
“**Send to user with the role “User” violation/restoration of the testing mode at the object**” includes the users in the object testing messaging list.

To send images to the “Phoenix-MK” application users, specify **IP address** of the image server and **Port** that it uses.

Attention! You shall specify the actual network address of the computer in the “IP address” fields. If the required server is on the currently used computer, you cannot use 127.0.0.1 value as the actual LAN address must be specified, for example, 192.168.0.100.

4.4.14. Email delivery

Parameters located on this tab are used to send events that occur on the objects to their owners by email.



The checkbox "**Enable email newsletter**" allows to use the automated mailing to owners about events that occurred on their objects. If it is checked, the following options are available:

Host – the email server name;

Port – port of the email server;

User – email address is used for mail send;

Password – password to log into the mailbox for mail send;

Encryption protocol – select the protocol used by the server;

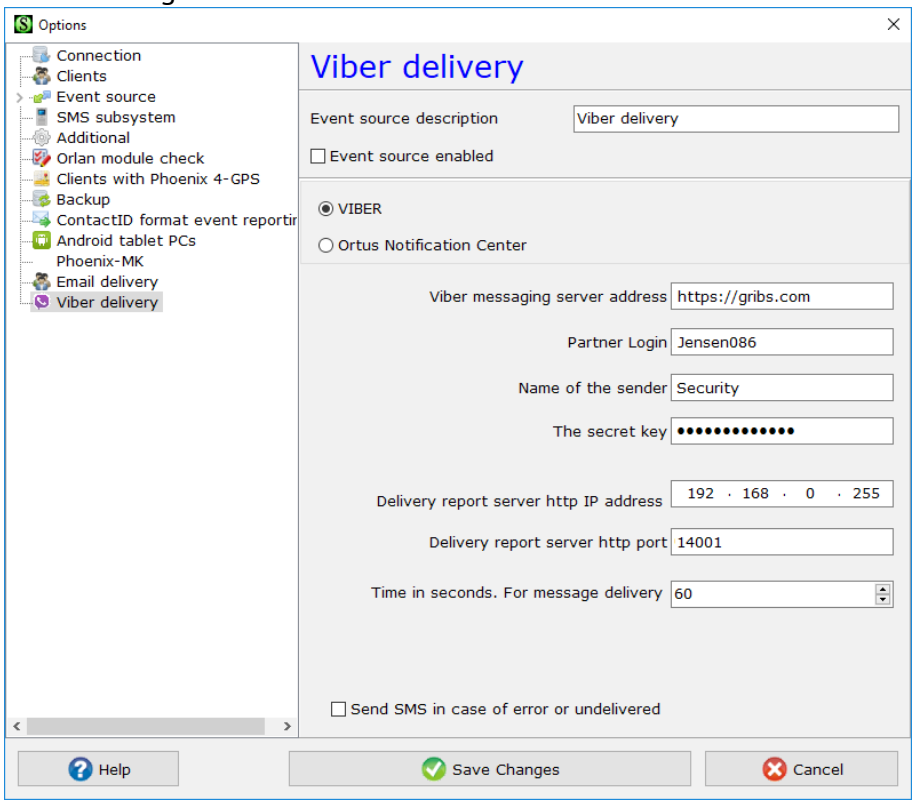
Computer Name with Control Center to notify by email – if only one Control Center (main) is used in the CMS, then you should specify this computer name; if several Control Centers are used (main and slaves), then you should specify only one computer with the "Control Center" software;

Number of email messages per connection to the SMTP server – if a public mail server is used, it is recommended to specify up to 10 messages in order to prevent the mailbox blocking by the anti-spam server. If the own server is used, then number of messages is limited by the server and network productivity;

Subject – text will be used as the header for each email sent.

4.4.15. Viber delivery

Parameters located on this tab are used to send events that occur on the objects to their owners via Viber instant messenger.

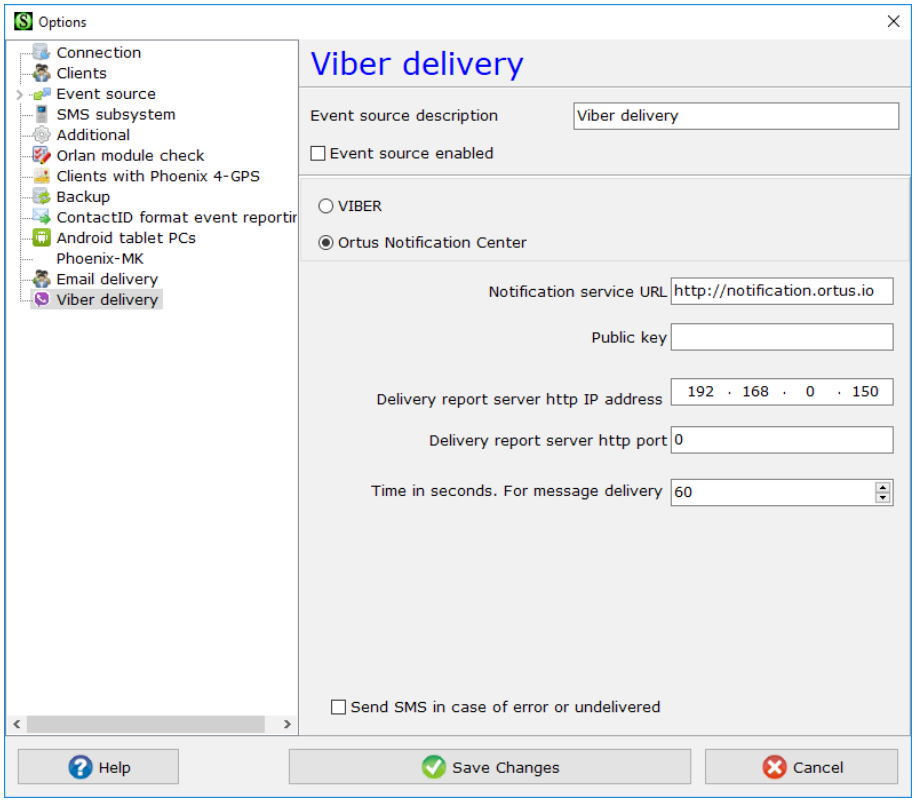


The server and software of one of the partners of Viber Media S.a r.l. is used. (if the **Viber** option is selected). This partner provides data for filling in the fields in the form above:

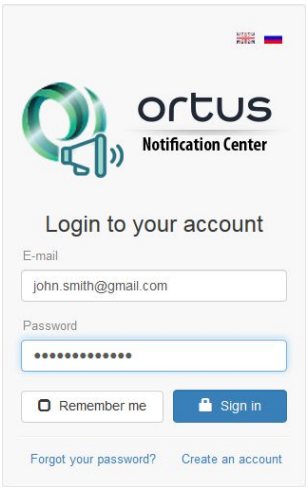
Viber messaging server address – partner Internet IP-address;

Partner Login, **Name of the sender**, **The secret key** – required to deleivery access.

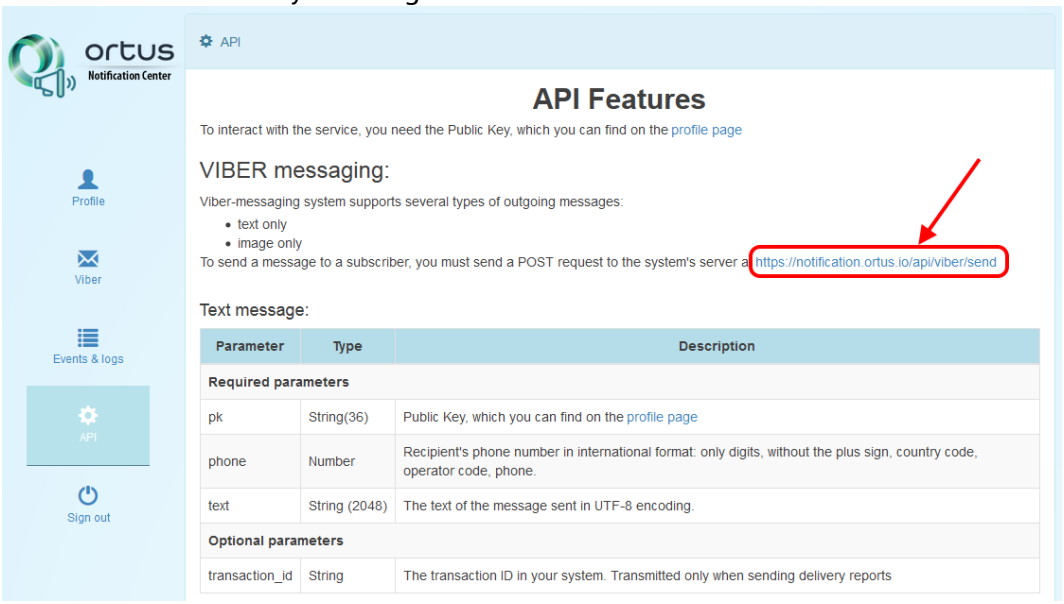
You can use the **ORTUS Group** company messaging service (choose the **ORTUS Notification Center** option):



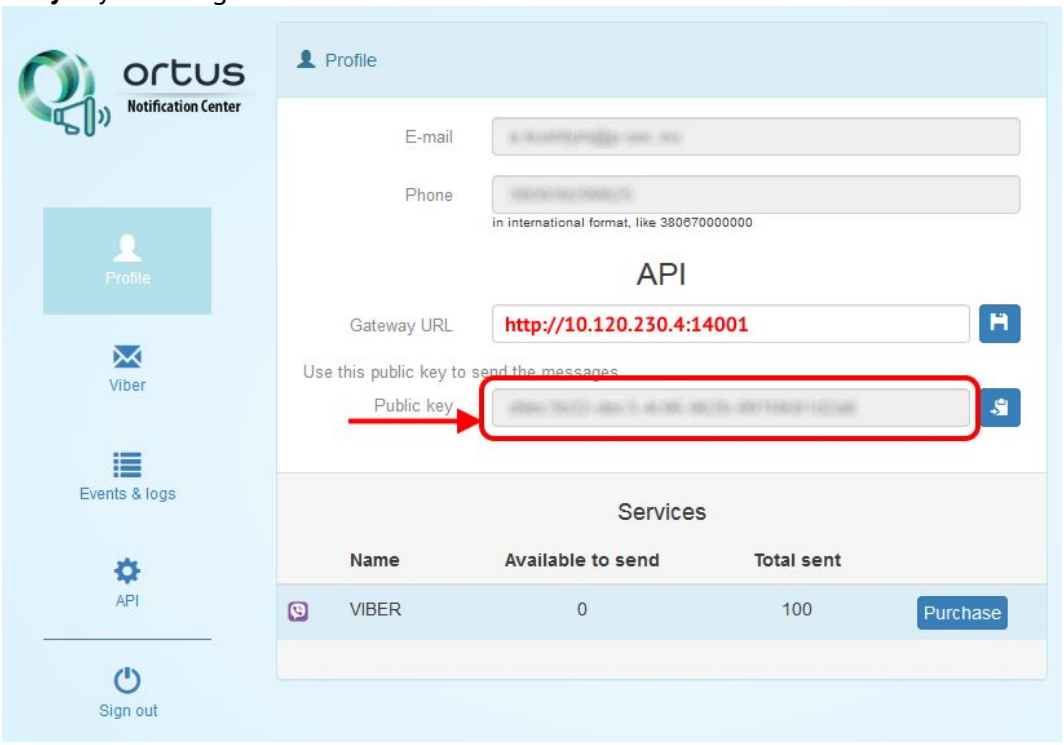
Parameters for accessing this service you can get on the site https://notification.ortus.io (registration required):



Notification Service URL – you can get it on **API** tab:



Public key – you can get it on **Profile** tab:



Gateway URL – Internet network address of the computer (for example 10.120.230.4) and port (for example 14001), where the service sends a delivery report. Write as format:

http://10.120.230.4:14001

The next general options should be set by your local network administrator:

Delivery report server IP address, Delivery report server port – local network address of the CMS computer and its port (it must be accessible from the Internet), where the delivery reports from the partner receives;

Message delivery time, seconds – the time while the message is stored on the partner's server, if it can not be delivered to the recipient;

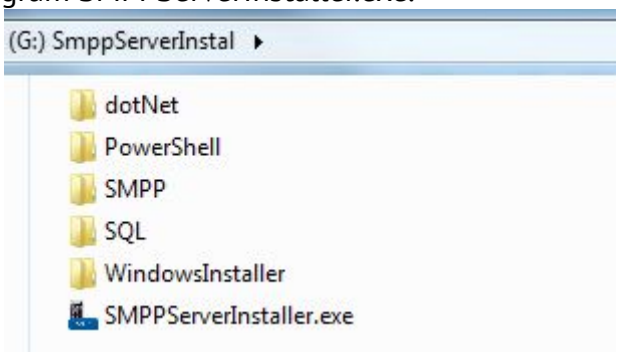
Resend undelivered message as SMS – allows to automatically send a duplicate normal SMS message if an error occurred while trying to send via Viber.

4.4.16. SMPP server configuration

Short message peer-to-peer protocol (SMPP) is protocol that describes interaction of an end user with SMS server (SMSS). It is used to transmit SMS and USSD messages.

SMPP server is a special software produced by 'Protection and Security" that supports this protocol to provide connection between the operator and SMS server on the one hand, and supports operation with "Phoenix-4" software on the other hand. Therefore, SMPP server is an interim server that receives requests from "Phoenix-4", translates them into SMPP protocol, and transmits them to the provider (mobile operator). It also send "Phoenix-4" SMS delivery confirmation or non-confirmation. This software shall be always running and have network access both to "outside" and "inside" of the network.

This software is an additional component to send SMS; it is supplied on a separate disc and has its own installation program SMPPServerInstaller.exe.



When launched, this Installer analyzes your system and determines the system components missing, and then installs SMPP server program.

Attention! SMPP server software is compatible with Microsoft SQL Server 2008 DBMS version or higher only. MS SQL Server 2000/2005 is NOT supported.

This MS SQL Server 2008 Express DBMS will be installed on the computer if necessary, moreover, the named version "**SQL2008**" will be installed. In case SQL 2008 is already installed, DBMS will not be installed, and you shall specify the correct parameters in SMPP Server Settings.

After installation, the program will create an empty database. This program must always be running, you can add it to autorun by copying the shortcut.

In the main window the current activity of server is displayed (current SMS). "**Settings**" button allows for configuring of this program.

The settings of this program are divided into two categories: SMPP settings and SQL Server connection settings.

All the parameters for configuration of SMPP protocol are provided by the mobile operator.

Let's consider the database connection parameters more closely.

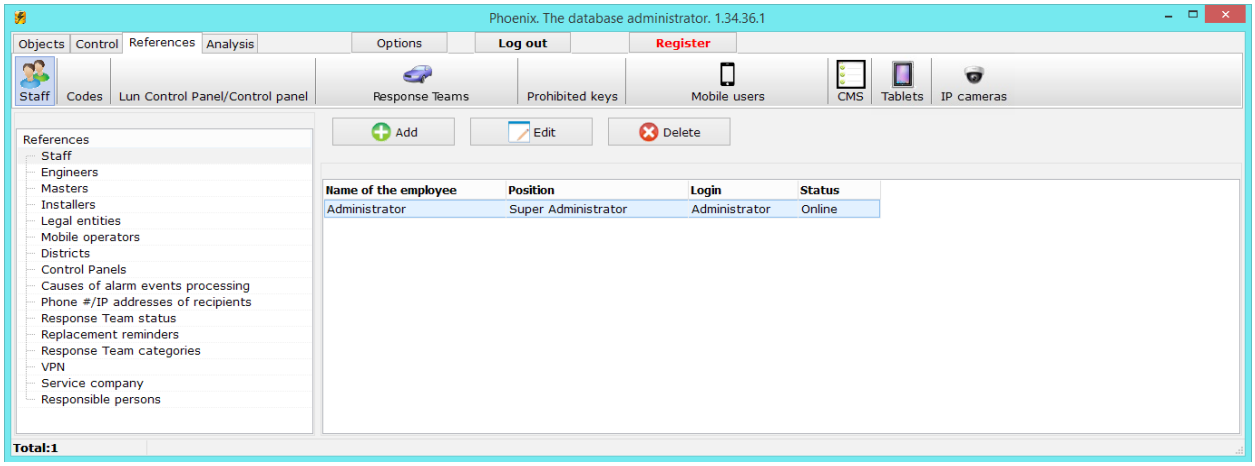
“**SQL server name**” – network name of the computer with MS SQL Server 2008 DBMS and database is specified. As the Installer installs the named instance of this DBMS (specified with “\”), the default parameter value is “\SQL2008” – it means that DBMS named “SQL2008” is installed on the local computer (“.”). if your default instance (unnamed) is SQL 2008, you shall specify the computer name only or its IP address in the settings.

Database – database name (default value is SMPPServer, it cannot be changed).

“**Verification**”, “**Login**”, “**Password**” – used to configure MS SQL connection. It is not recommended to change these parameters.

5. Database creation

When you create “Phoenix-4” database, you shall create references first. To create/edit references, go to “**DB Administrator**” and log in. Then create all the necessary references using the menu window.



The “**References**” tab has the following tabs:

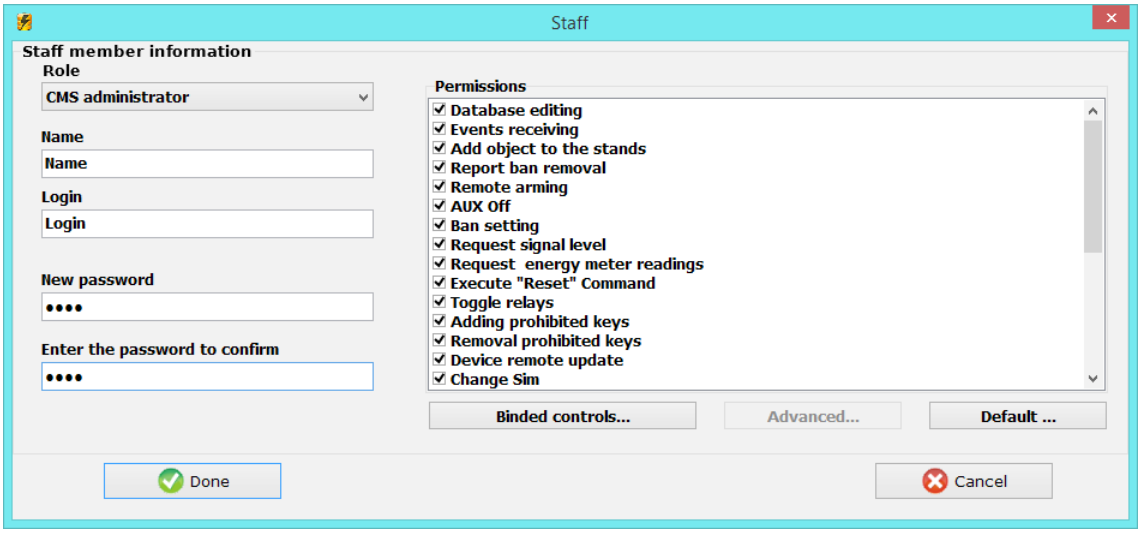
- Staff;
- Codes;
- Lun Control Panel;
- Response Teams;
- Prohibited Keys;
- Mobile users;
- CMS;
- Tablets;
- IP-cameras.

5.1. Staff

Filling in of all the fields of references with the information will much simplify and regulate using of “Phoenix-4” software.

In the **Staff** tab you enter all the information about personnel.

1. To enter the information about personnel that works with “Phoenix-4” software, select the **Staff** branch in the **References** tree and click **Add** button:



“**Role**” – new staff member role;

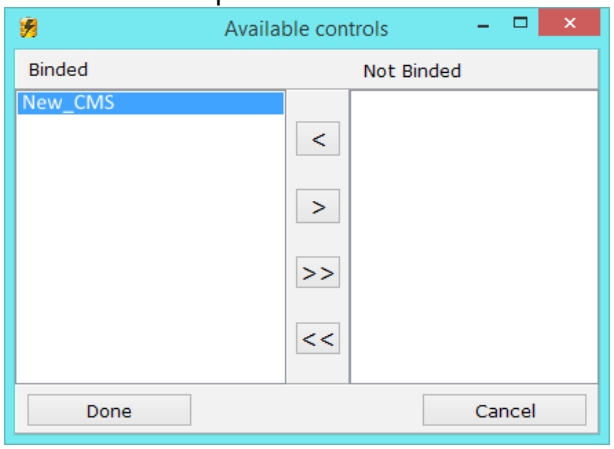
“**Name**” – new staff member name;

"**Login**" – user's name in the system. Together with a **password** it allows to identify the user.

To set a password, select the appropriate option and enter a **password**.

You shall also select **Permissions** – actions allowed for this user. We recommend to set the **Default permissions** with the appropriate button, but you can also set any other permissions.

To set access to the objects of some certain stations you shall use the "**Binded controls...**" button. After clicking it, you shall select the required stations from the list.

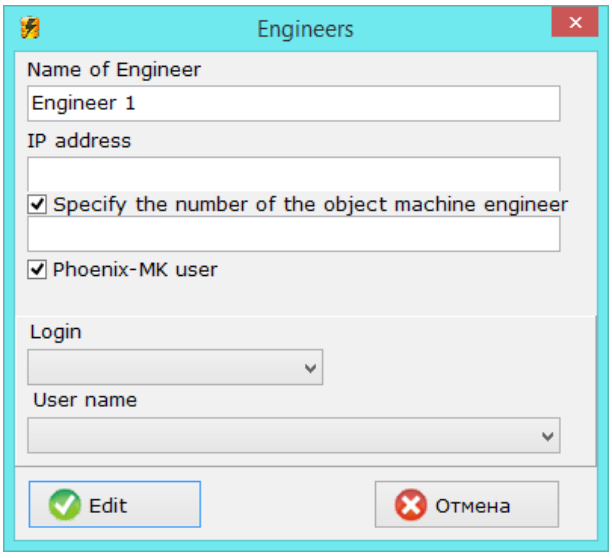


After the stations are assigned to the personnel, the latter will be able to work only with the objects that are assigned to these stations, as well as with the objects that are not assigned to any station.

This limitations apply to any personnel in such programs as "DB Administrator" and "Duty Operator".

Only the user with the embedded account role of "**SuperAdministrator**" can assign personnel to stations.

2. To add a new engineer, select the "**Staff**" branch in the "**References**" tree and click **Add** button:



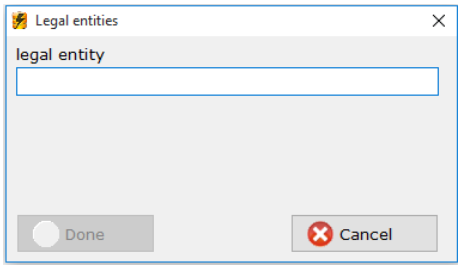
In the opened window you shall enter the following:

- **Engineer's name;**
- Engineer's computer **IP address**, where "**Phoenix-Technic**" and "**Application Engineers**" software installed;
- **Login and user name** of "Phoenix-MK" mobile application user. This application allows to view events by the s remotely and control them. See the details of creation of mobile users.

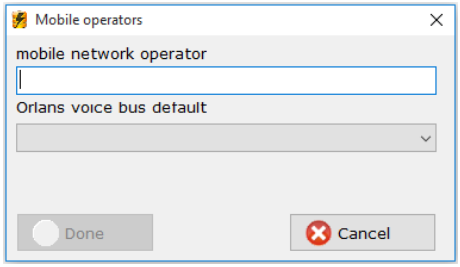
3. The "**Masters**" and "**Installers**" categories are filled in the same way.
4. "**Legal Entities**" category shall be filled in by all the legal entities of the station company.

When creating objects, you can select with which legal entity the contract was concluded.

In the "**Legal Entity**" field you shall enter the company names with which the manager concludes the Security Service Agreements.

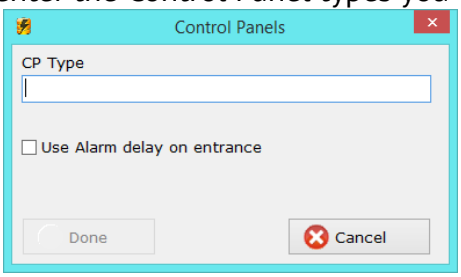


5. **Mobile operators**:

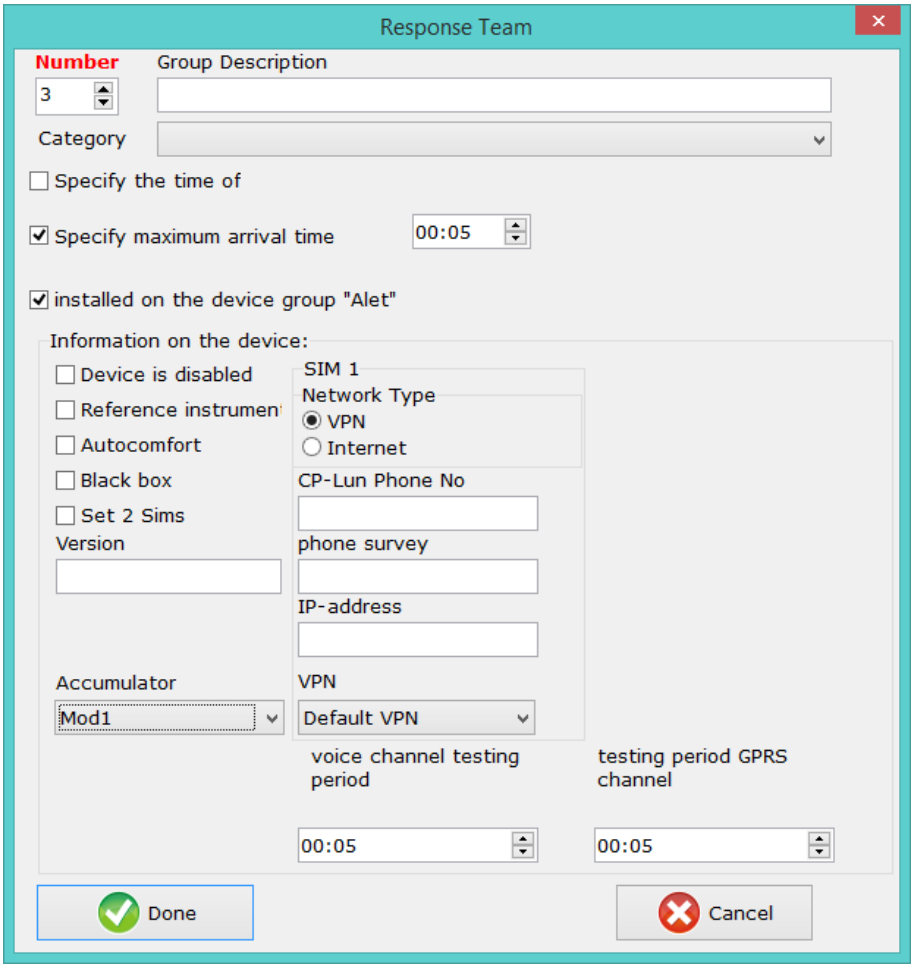


Specify the mobile operators you will work with and Orlan-M bus number for it. The same mobile operators Orlan-M modules in pair configure to the same bus recommend.

6. **Districts** – enter the city districts (in the same way), where the control panels are located.
7. **Control Panel** – you shall enter the Control Panel types you will use



8. **Response Team**



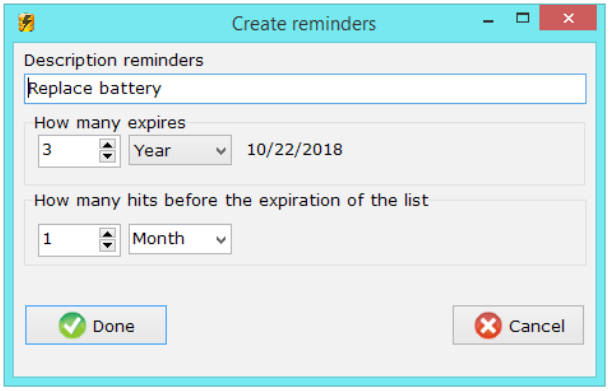
In this window you create the response teams.

To create a response group, enter its number and name.

If necessary, you can specify the working hours of the team.

If an "Alet" device is installed for this group's car, select the "**Alet installed for group**" option and set the required settings about "Alet" device.

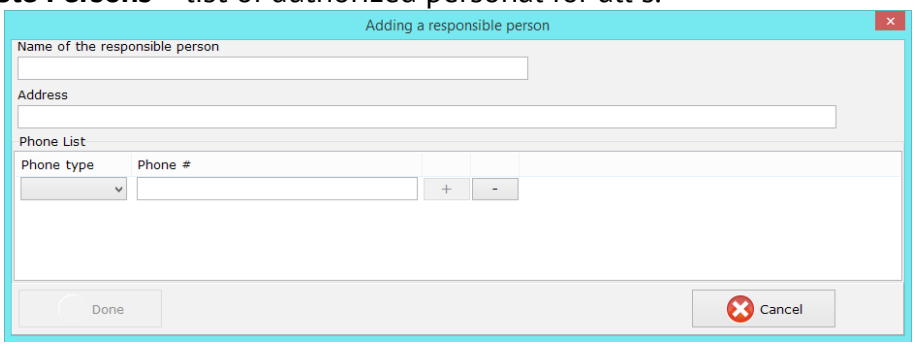
9. **Causes of alarm events processing** – the list of reasons for processing of alarm messages can be edited here.
10. **Phone No. / IP addresses of message receivers** – Clients' phone numbers, to which SMS will be sent in case of alarm or IP-addresses of remote CMS can be store there.
11. **Responce team status** – list of available statuses stored here.
12. **Replacement reminder** – list of reminders for replacement of spare parts.



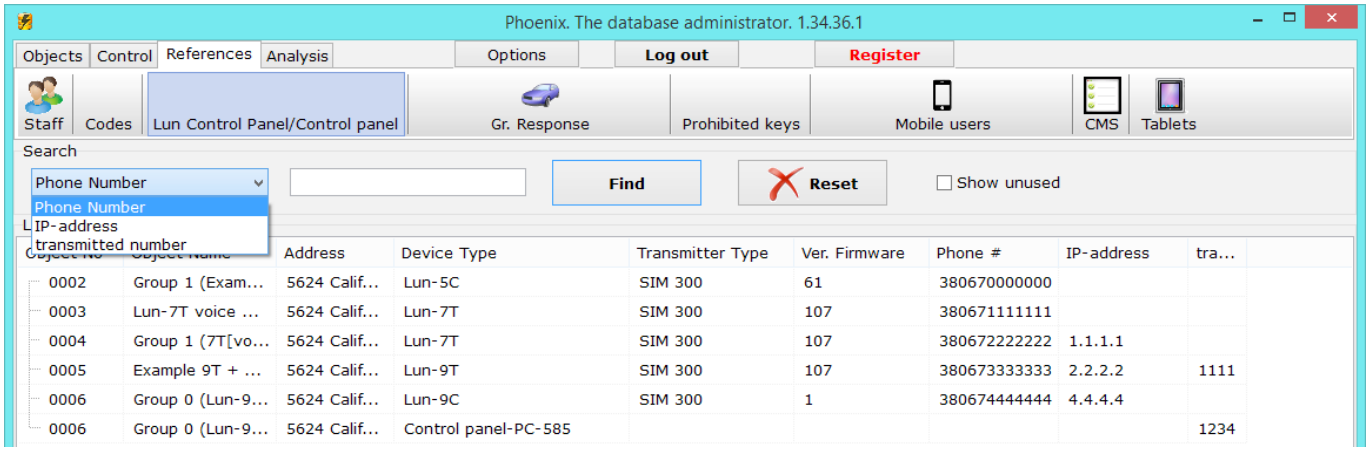
13. **VPN** – It used to create VPNs list that the object Control panels will operate with through GPRS channel.

You shall specify these networks when creating a Control Panel and configuring the Control Center (event sources via GPRS channel).

14. **Service Company** – an organization that performs maintenance of fire protection s. When you create objects, you must specify the fire service company. In general, the CMS and the service company may be different.
15. **Responsible Persons** – list of authorized personal for all s.



5.2. Lun Control Panel / Control Panel



In this tab you can see the list of all “Lun Control Panels” and other Control Panel (external panels) and their major characteristics:

- Control Panel type;
- Transmitter type;
- Firmware version;
- Phone number;
- IP address;
- Transmitted number.

You can also control panel search by:

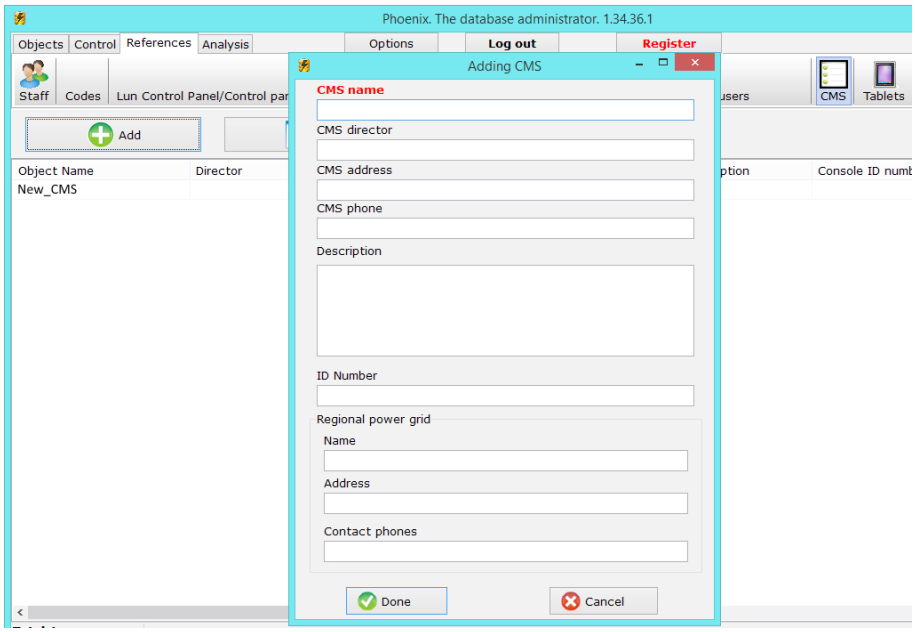
- Phone number;
- IP address;
- Transmitted number.

If you want to show the unused object devices (those not installed in any object), select the appropriate option “**Show unused**”.

5.3. CMS

“Phoenix-4” supports the matter of a “central monitoring station” (“CMS”). In this context, “CMS” is a matter that allows to distribute the object visibility between the operators. Let’s consider an example, in case you have affiliates or any other subdivisions, or you transmit events, or let other persons to view an archive (remote CMS), this mechanism allows to demark the field of vision. You cre-

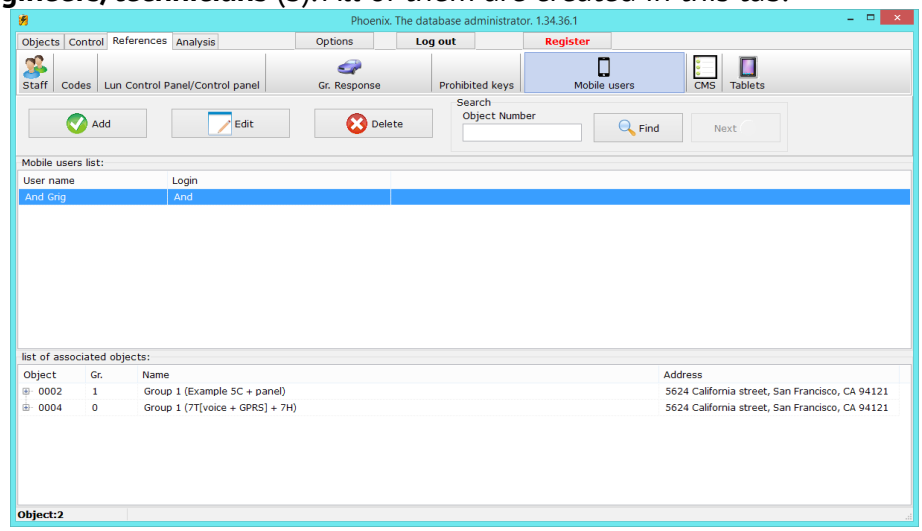
ate as many “CMS” as you need. After that, you assign the required s to the “CMS”. Then you specify which operator/administrator/personnel has access to which “CMS” (it can be done only using the SuperAdministrator account). After doing this, the personnel will have access to the objects of the stations they are assigned to (it is completely clear to the personnel, as if there are no other objects).



5.4. Mobile users

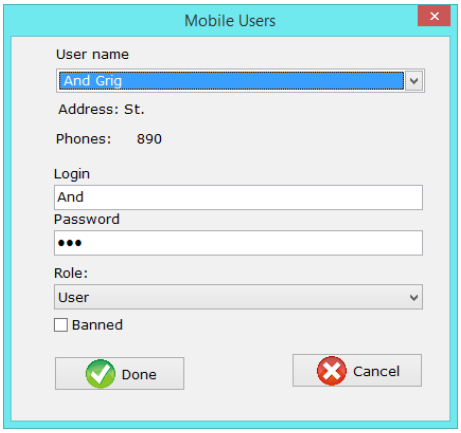
This tab is used to create users of “Phoenix-MK” application (Mobile Keypad), that allows to view the information and events on the objects, as well as to query the object status remotely and execute some other commands.

There are two scenarios of the “Mobile Keypad” use – by object **users/owners** (a) and object maintenance **engineers/technicians** (b). All of them are created in this tab.



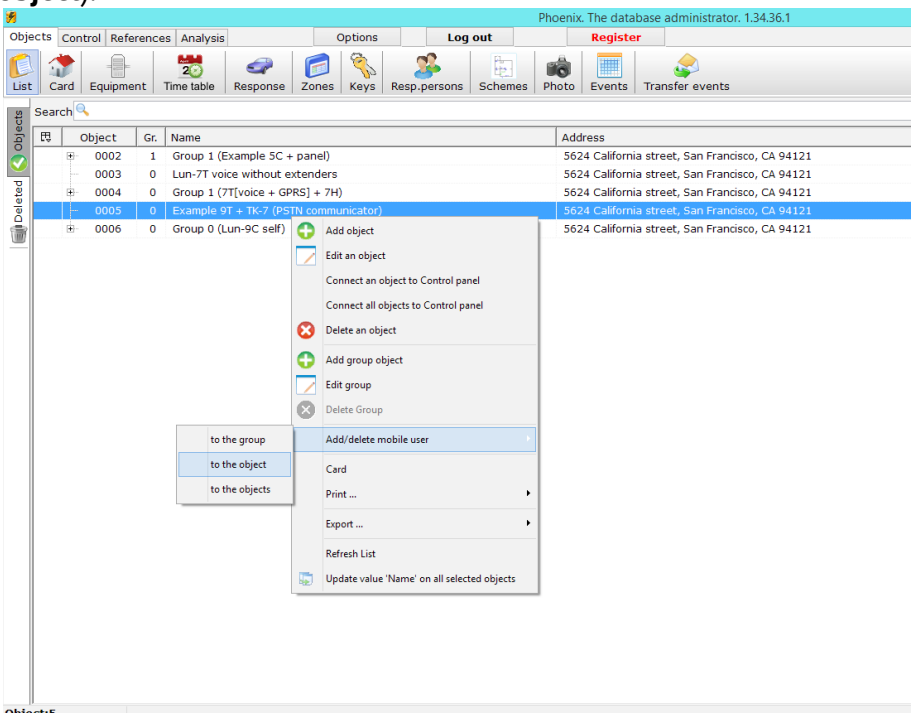
To create a user, click “**Add**” and in the opened window specify the required parameters: name, login, and password. Login and password shall be entered in the application itself.

You shall also specify the users “Role”: **User** or **Engineer**. The difference between the roles is that the User has access to the actual events of the object only, but the Engineer has access to all events, including generated by “Phoenix-4” software itself (these special codes start with “Z”).

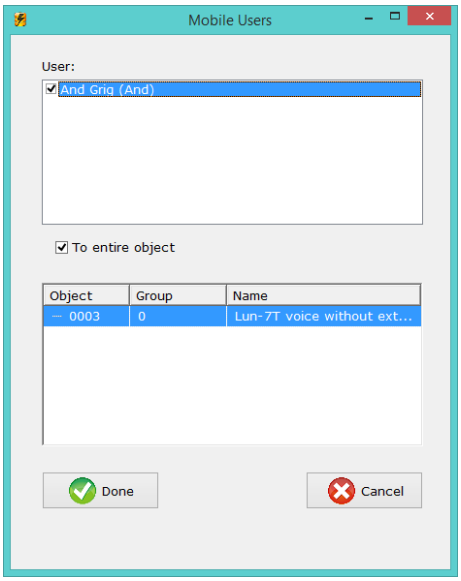


In case you need to block a user, you need to select the "**Banned**" option. The banned users cannot access or control with the s.

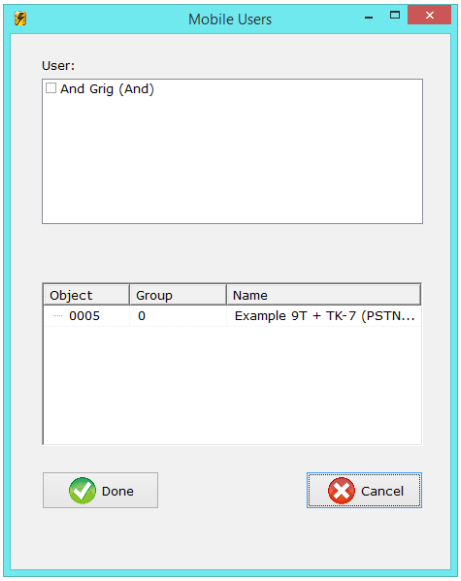
After the user is created, you shall assign the s to it. You can also assign only a group (one or several) to the user. It is done in the object list via the context menu of the right mouse button. To assign s, right-click the required object and select "**Add mobile user**" (two variants will be available: **to group** and **to object**).



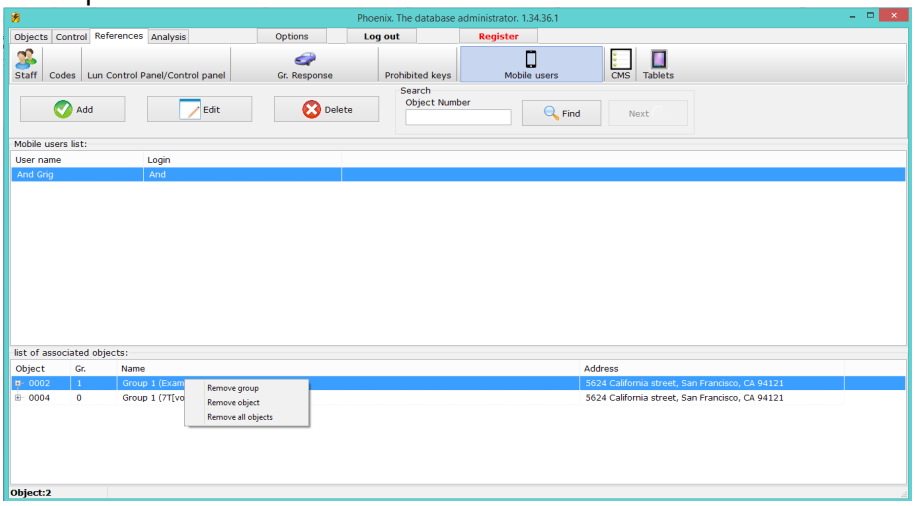
After you click "**Add mobile user**", select a user in the "**User**" list for the object and click "**Done**".



If you need to assign a group, select the group in the object and click "**Add mobile user**" "**to group**" in the context menu.



To delete the assignment of an object to a mobile user, right-click in the list of assigned objects and select the required action:



5.5. Online users

This tab is used to create online user list, that allows to view the events of the objects in the Web-browser – without the "Phoenix-4" software at all.

The most settings and working order to add/edit/delete the online user to the database and to assign a user to the object/group – is the same to Mobile users section.

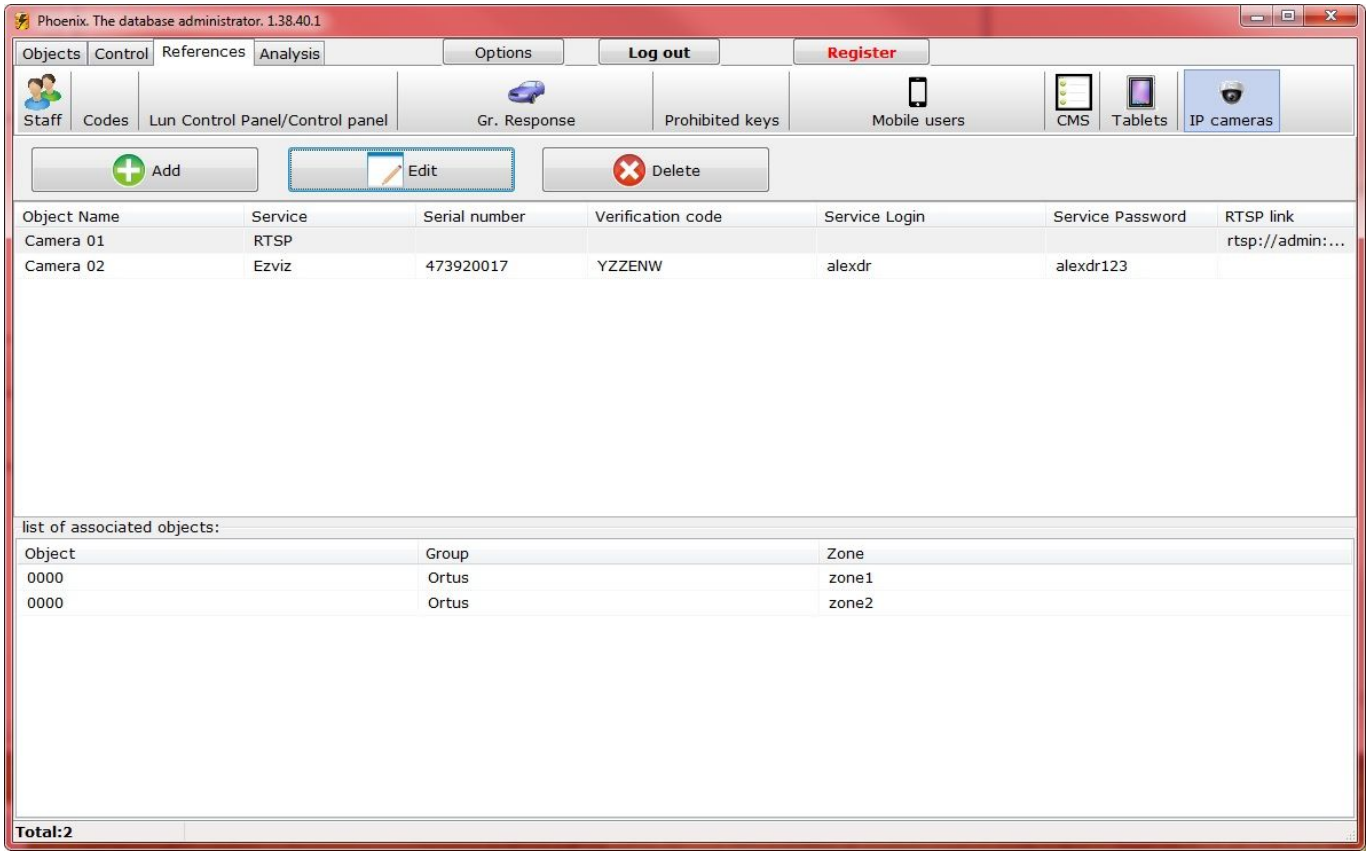
As the users assigning to some objects/groups, the user can view selected object's event types in web-browser – the special "events web site" uses.

To create this "events web site" you should use the "*Event Site Deployment Guide*" is placed on the www.ortus.io.

Login and password required to access to "events web site". After login user can select the object/group and events types he want, so the filtered events will be displayed.

5.6. IP-cameras

Here you can declare all IP-cameras, used in the system for the subsequent binding to any zone of a specific object. General requirements for the equipment are set out in end of this section.



The top half of the window displays a list of all IP-cameras in the system. In this list, you can add a new camera, change it or delete the camera with the corresponding buttons.

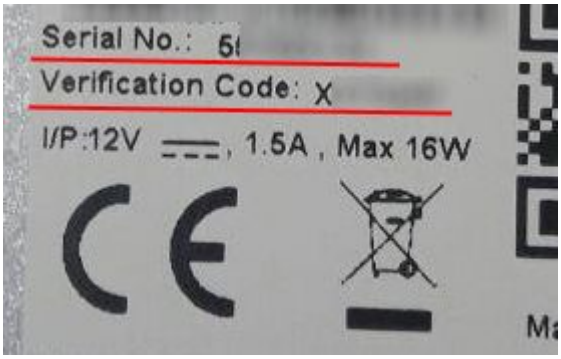
When adding/changing an IP camera, you need to correctly set its connection parameters, depending of the used service/protocol – see the pictures below.

Service – the type of service/protocol used for receiving/managing/storing data from the camera:

- Service **Ezviz** – to view archive records on the events, which took place after at least 10 minutes;
- Protocol **RTSP** – to view the video stream online – at the time of the appearance of a new event.

Name – the name of the current camera, is used to indicate it in the DB Administrator.

Serial number and **Verification code** – indicated on the camera label when it is manufactured:



Login and **password** – get it after registration on the service web site http://www.ezvizlife.-com/

Common requirements for the equipment:

Supports IP-cameras produced by HIKVISION. Additionally, you can use DVR (Digital Video Recorder). If you use DVR, video from IP-cameras can be saved locally, otherwise it uses cloud storage. IP-cameras should have unique network addresses, also high-quality high-speed Internet channel for transferring video stream to network storage is needed.

Detailed recommendations for setting up HIKVISION equipment and solving various technical issues can be found on the website http://www.hikvision.com.

6. “DB Administrator” software

“DB Administrator” software is used to administer “Phoenix-4” system: add, change, delete information of the secured s, users, devices, response teams, etc.

To edit DB, you need to enter the system. For this purpose, the “**Enter**” button is placed in the upper panel. There is the default fully authorized “**Administrator**” account. The “Administrator” password is “**510eb93**”. You can change the password of this account any time.

6.1. Icons

In the “Duty Operator” and ‘DB Administrator” programs, graphic “icons” are used to display additional information on s or events. The icons are displayed in the leftmost column of the event or object list.

The definition of the icons are as follows:

“**no icon**” – standard secured object or event;

– “fire” on object (in this object a fire alarm system is installed, for example, “Lun-9R”);

– permanent stand (from this object all events are translated into unalarmed and archived without the operator’s processing, for example, during the repairs at the object);

– technician (maintenance engineer) works at the object;

– object is disconnected;

– “disable arming” object (only for “Lun” Control Panels);

– “No test in time” list has the comments of the operator (with or without effective term other than the current date);

– “No test in time” list has the comments of the operator and term until the end of which this comment is valid, which is the current date.

In addition, there are following icons for the zones:

– zone is in the normal state;

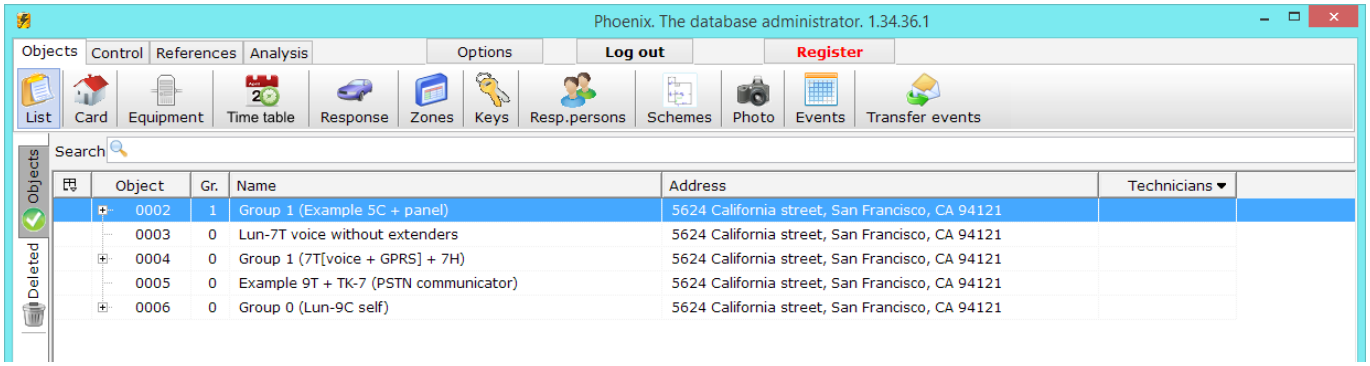
– zone is alarmed;

– fire alarm for zone;

– faulty zone;

– zone is OFF.

6.2. Program main window

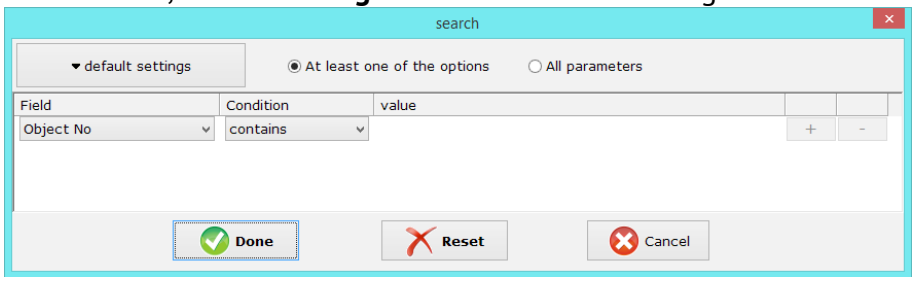


The main window of the program has the following tabs:

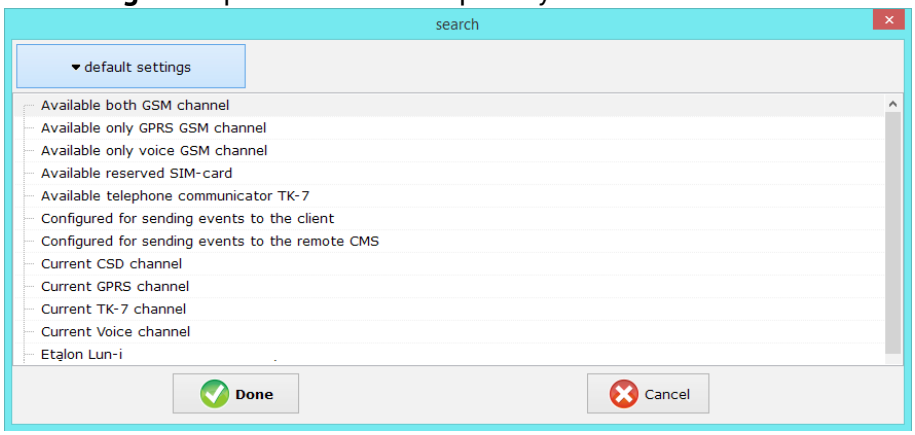
- **Objects**;
- **Control**;
- **References** (see “Creation of References”);

- **Analysis**.

In the "**Search**" field you can enter a line according to which the search will be executed (object, Name, Address). After this, press **Enter**. All matches will be shown. See the details in the next section. For advanced search, click the "**Magnifier**" icon. The following window will open:

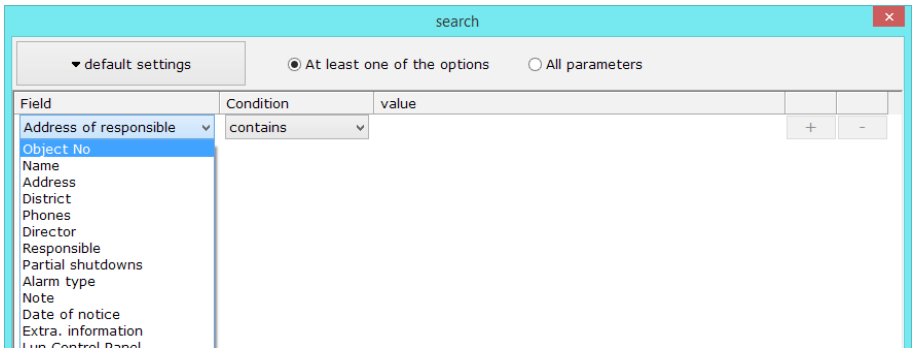


Click "**Default settings**" to open the most frequently used search criteria.



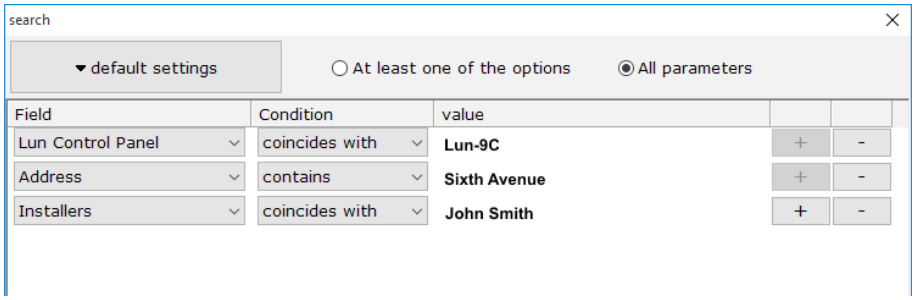
To apply the default search settings, select the required criteria and click **Done**. The list will be filtered.

If you want to set the filter yourself, specify the field, by which the search will be executed, condition and set its value.



You can specify several criteria, they are added by clicking "**+**".

Example: you need to select all s, type of the object is "*Shop*" with "*Lun-9T*" installed and located in "*Sixth Avenue*", street, with the installer in charge "*John Smith*". The advanced search shall be as follows:



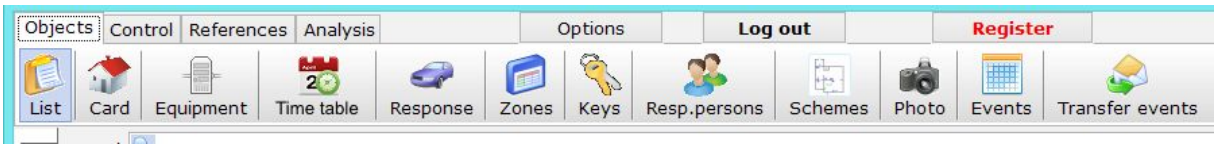
After you click **Done**, the list will be filtered according to the criterion set.

To clear the advanced search criteria, click the button in the **Search** bar.

Activity of Disconnected criteria allows to find the objects that were temporarily disconnected

(with the 'Disconnected" option), but which were "Armed/Disarmed" from the data you enter until the present.

6.3. Objects tab

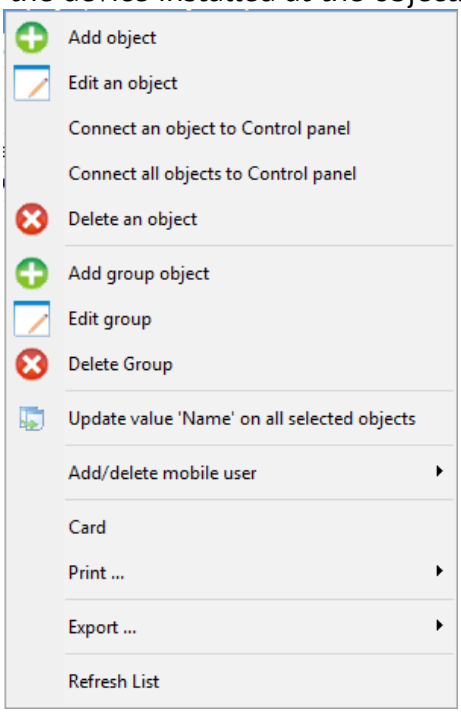


This panel has the following sections:

- List;
- Card;
- Equipment;
- Time table;
- Response;
- Zones;
- Keys;
- Responsible persons;
- Schemes;
- Photo;
- Events;
- Transfer events.

6.3.1. Context menu

To call the context menu, right-click the highlighted object. The menu will open depending on the rights of the current user and the device installed at the object.

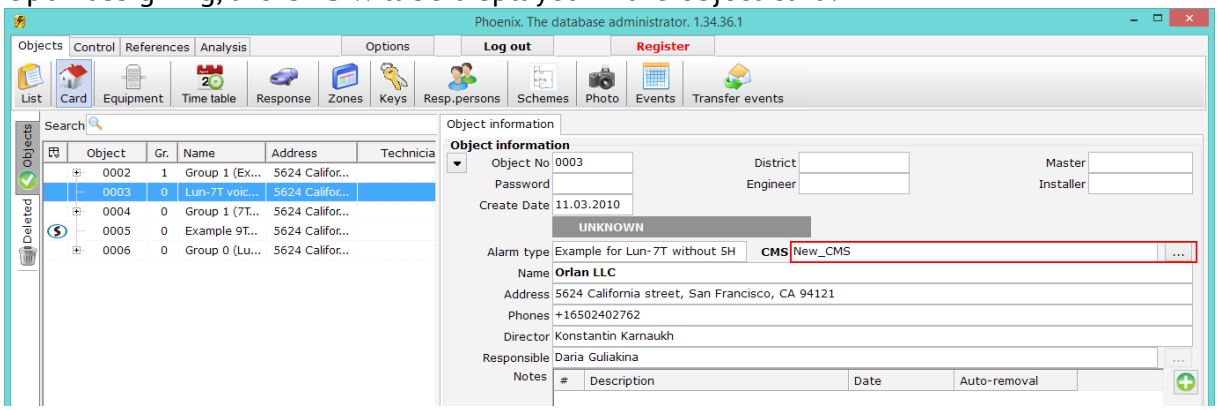


The purpose of the most of menu items are intuitively clear (Add object, Delete object), the specific menu items are described below.

Assign object to CMS option is used to assign the highlighted object to the CMS matter; the assigned objects are shown only to the operators that have access to this CMS. See the details in Stations section.

After that, select the CMS to which the object will be assigned.

Upon assigning, the CMS will be displayed in the object card:



Assign all objects to CMS option is used to assign all the displayed objects to one CMS. See the details in **CMS** section. You can filter the required objects using the search bar, then assign all the objects by one command by clicking this menu option.

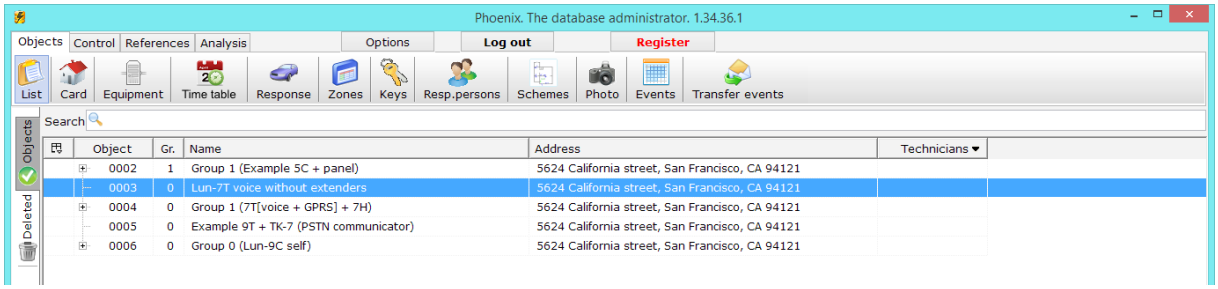
Card option is used to open the object "card" (all information) in a separate window.

Print option is a drop-down list with the following sub-items:

- **Object card** – printing of object cards (legal information)
- **Object data sheet** – printing of technical information (device and zones data)
- **The entire list of objects** – printing of the object list
- **Passport of object** – printing of the object card and the list of responsible persons for all the groups of object

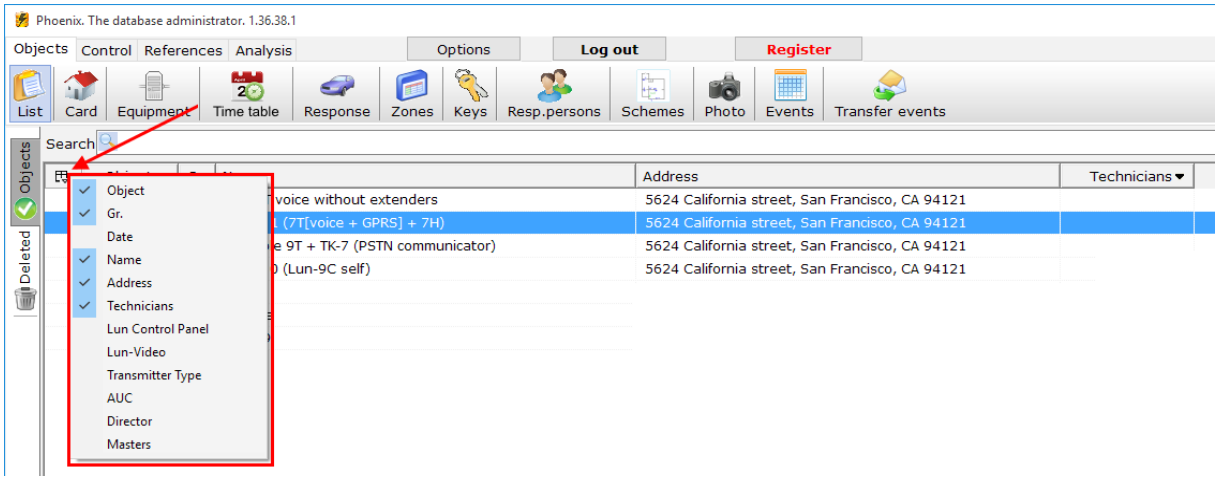
Export list to Excel – exporting of the current object list to MS Excel® table.

6.3.2. List section

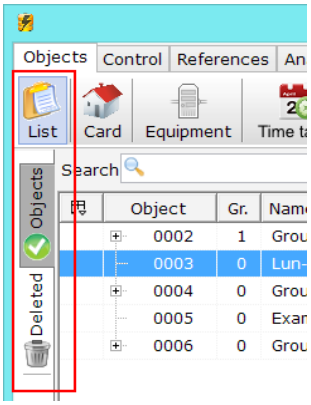


This section has a list of all the secured objects (their numbers, names, addresses), etc.

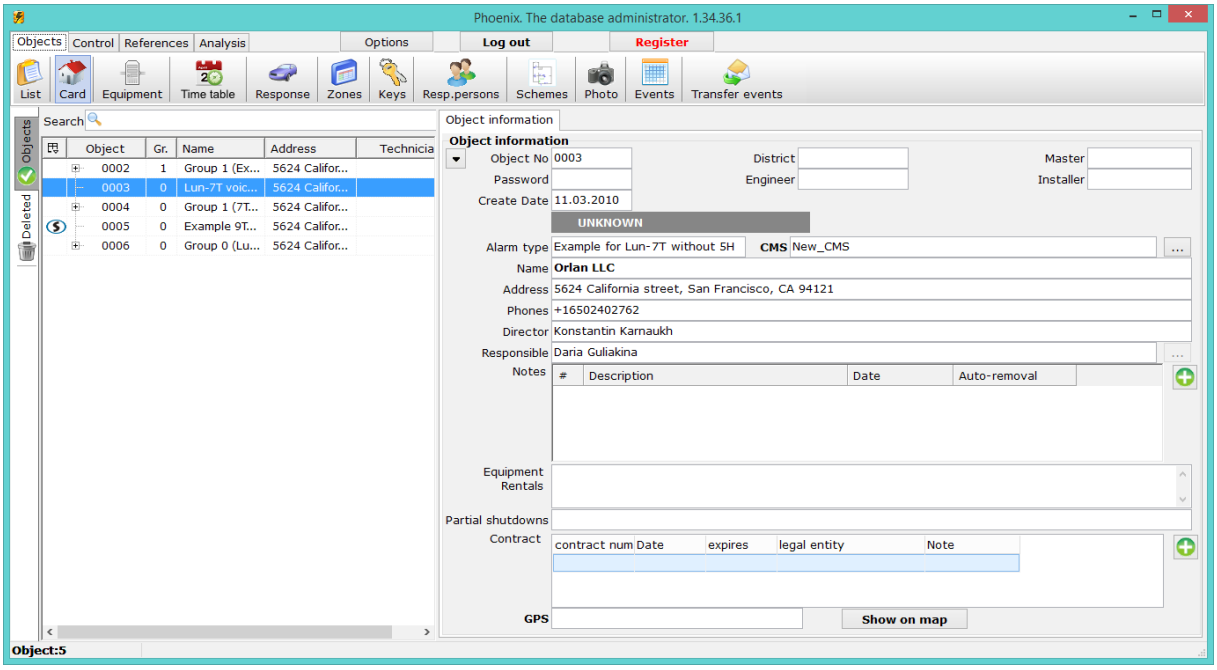
By pressing  , you can select the list of columns displayed.



The "**Objects**" section shows the active objects, and the "**Deleted**" tab shows the objects that were deleted to the basket, but can be restored.



6.3.3. Card section



This section has the information of the object as card: number, name, rented equipment, notes, address, and other key parameters required by operators, administrators, and technicians of the company.

There is an option of “mass” editing of the objects, the most often of corporate objects.

For example, you need to change the “Responsible person” field for all the objects. It is done as follows:

- **filter** the objects for which the change should be made;
- right-click the “**Responsible person**” field and select the “**Refresh filed <> for all selected objects**”.
- click **OK** in the opened window.
- The next window will inform you of the successful mass editing.

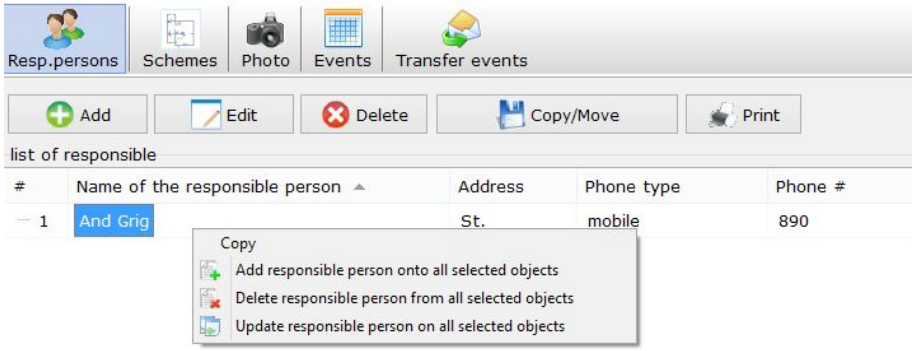
After this, the value of the “**Responsible person**” field of the highlighted object will be applied to all the objects displayed in the object list at this moment.

The fields that can be mass edited are as follows:

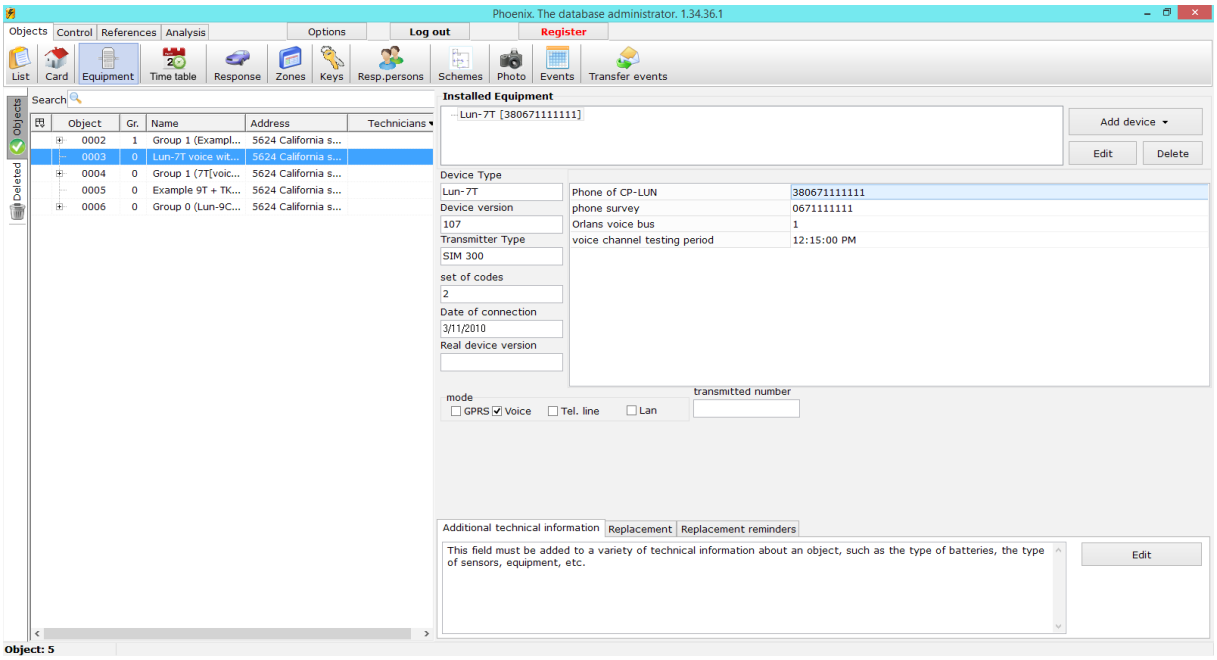
- Object name;
- Director;
- Responsible person;

- Notes (you need to click the note itself), for each note;
- And in the "**Responsible persons**" window for each responsible person.

The last two fields (**Notes** and **Responsible persons**) provide the following functional: **Add**, **Delete**, and **Refresh** these fields for all objects.

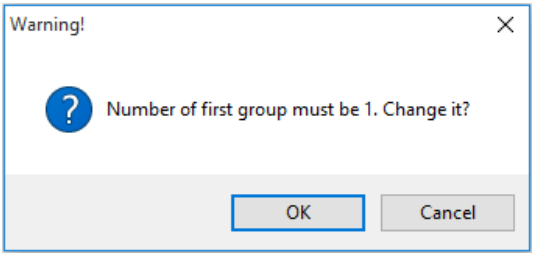


6.3.4. Equipment section



This section shows the information about the equipment installed at the objects: Control Panel, additional technical information (sensors, power supply units, etc.), replacements made at this objects, and next replacements reminders.

In case of change of the Control Panel type, the program generates a reminder of the correct numeration of the objects groups, depending on the Control Panel type. For example, if "Lun-7T" is installed at the object, for this device the numeration of groups starts with zero. When this device is changed to "Lun-11", the following message will be shown.

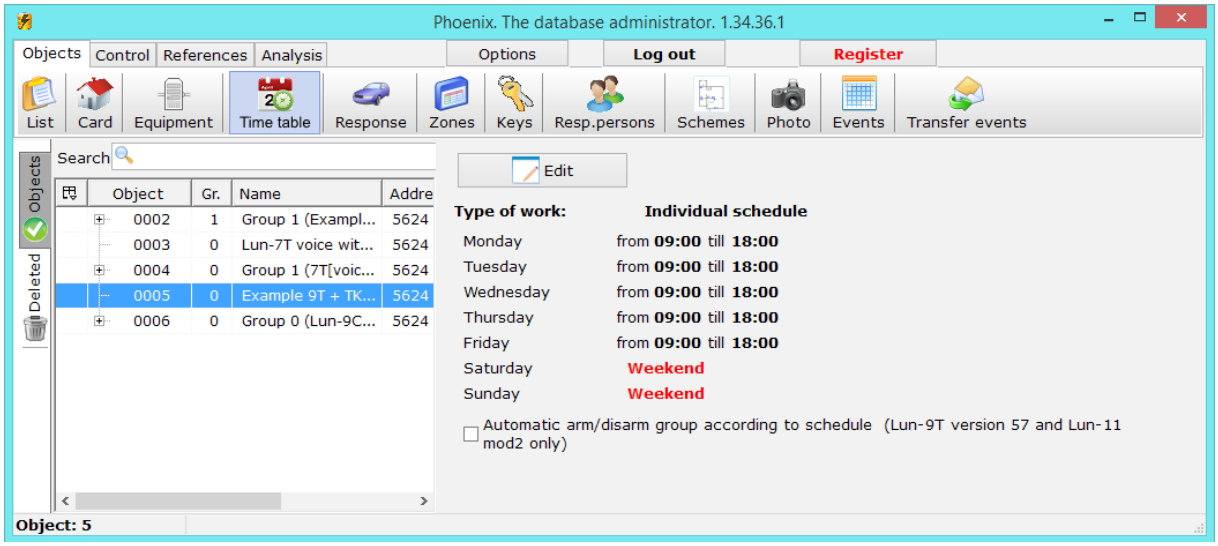


In case you click **OK**, the program will automatically change the group number form 0 to 1. If group 1 already exists, there will be no change, and the program will warn you that you must make the change manually.

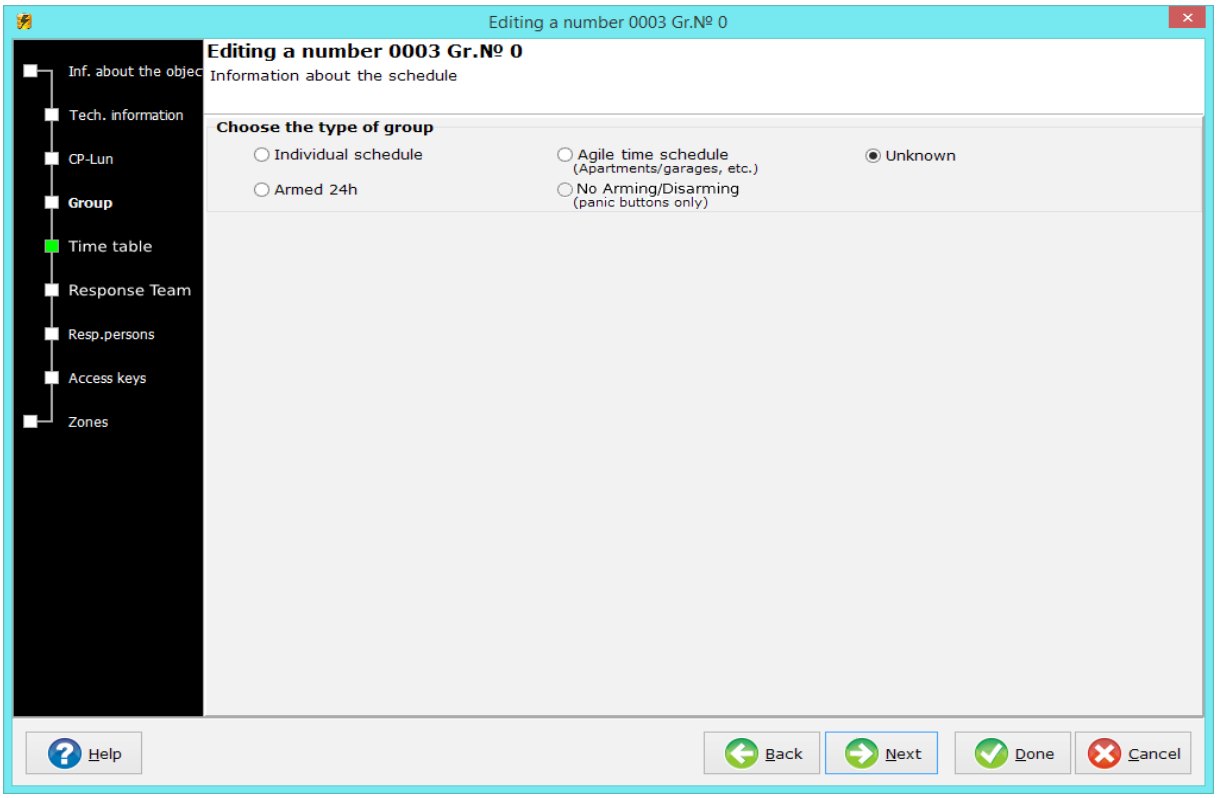
Attention! After changing of the group numeration either automatically or manually, do not forget to change the name of the diagram files for each group, they are not changed automatically by the program! You shall change the names of diagram files by yourself.

The rule of diagram files naming: <objects number>_<group number>_<a..f>.jpg

6.3.5. Time table section

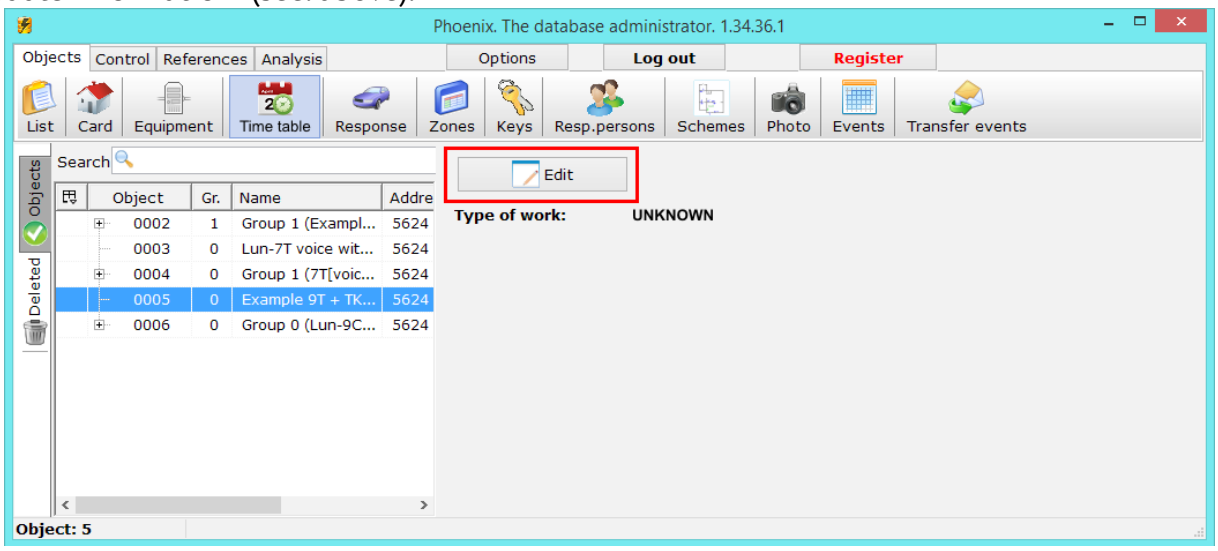


"**Time table**" reflects the object's group schedule and additional options. This section can be filled both at the moment of object group creation and during operation. In the first case (clicking the desired object/group with the right mouse button and selecting "**Add Group to object**" or "**Edit Group**") you will see a new "**Group Information**" window. If you click "**Next**", you will switch to "**Schedule Information**" screen.



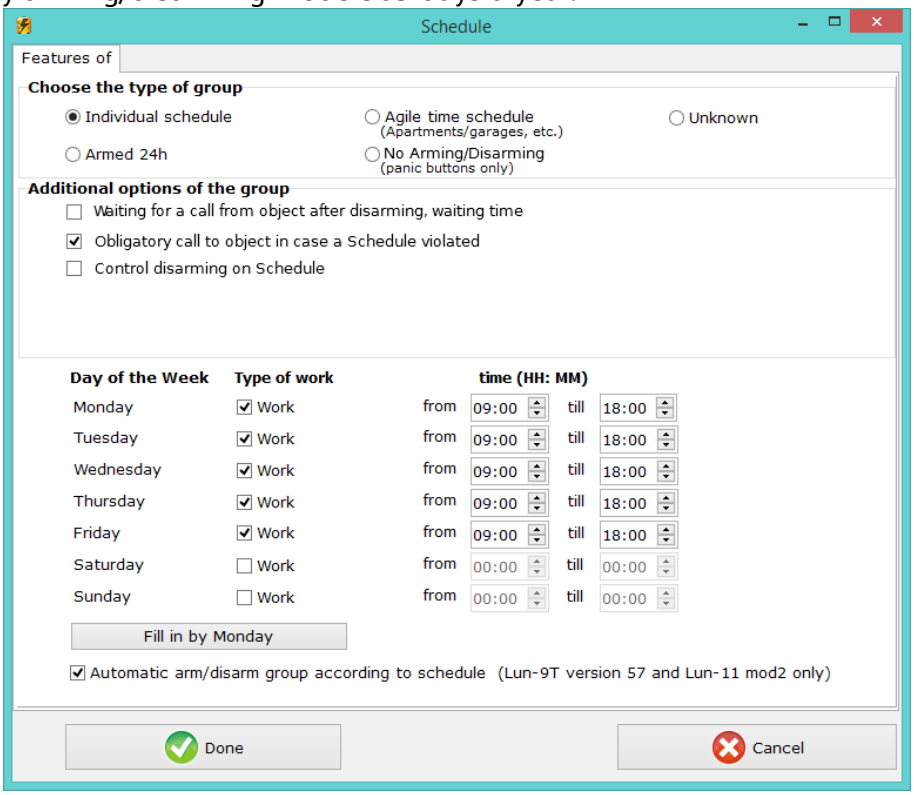
In the second case, it is convenient to select "**Time table**" from the main menu and click on the desired object's group.

Current operation mode can be changed by clicking "**Edit**". You will see a window similar to "**Schedule Information**" (see. above).



There are the following variants of object's group operation.

"**Individual Schedule**" -you can specify individual time schedule according to which the object group will be armed or disarmed. The schedule is arranged by days of the week, and is suitable for s with regular daily arming/disarming mode 365 days a year.



To enable a schedule for the specific day, you must check the "**Work**" box in the line of corresponding day and set the time – hours and minutes to arm (**from**) and disarm (**till**). If the schedule is constant for the entire week (or most week days), it will be convenient to fill the time for Monday only, and click "**Fill in by Monday**". Arming and disarming time will then be updated for every day (check boxes must be set manually).

"**Automatic Arm/Disarm group according to schedule**" checkbox allows operating according to a pre-filled schedule and without the participation of users/owners.

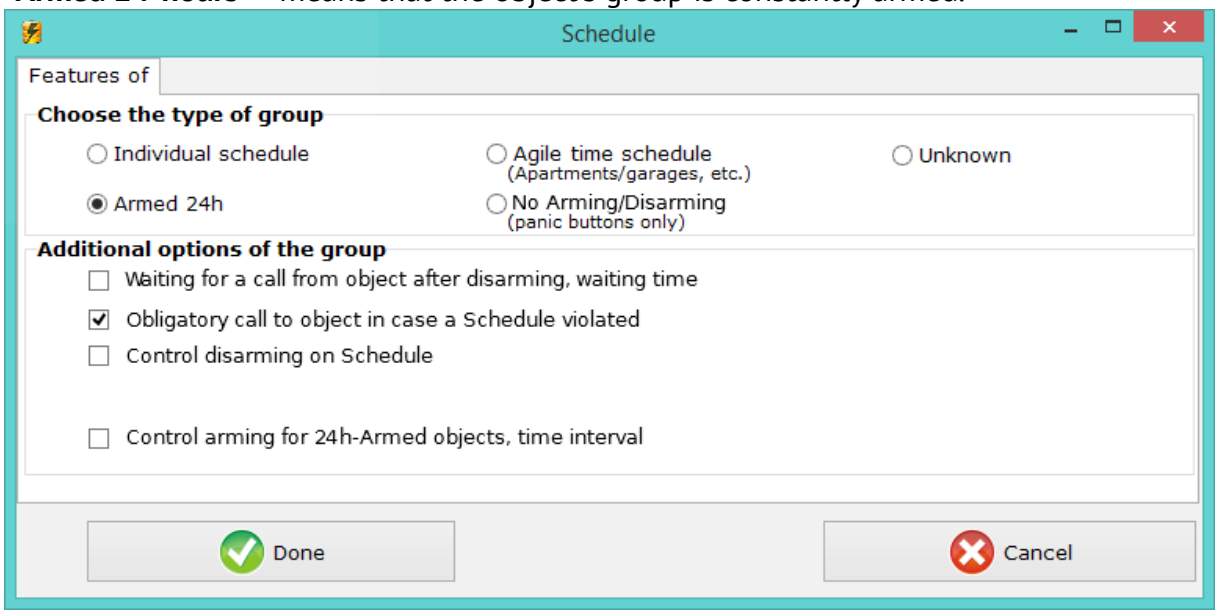
Attention! Automatic arming/disarming is only available for"Lun-9T" and "Lun-11" Control Panels.

Additional group options "**Waiting for a call from the object at the opening, during XX:XX hours:minutes**" - sends a reminder to CMS operator as soon as the specified time expires (event "**Check for a call from the object**" in the "**Unprocessed**" tab of "Duty Operator" software, and in "**Object Card**" of "DB Administrator") to confirm the legality of disarming.

"**Required ring in violation of the work**" - sends a reminder to CMS operator (event "**Check for a call from the site**" in the "**Unprocessed**" tab of "Duty Operator" software) in case the established schedule has been violated.

"**Scheduled Opening Control**" - sends a reminder to CMS operator (event "**Disarming on schedule! Send Response Team**", which is displayed in the "**Unprocessed**" tab) if the opening is not on schedule.

"**Armed 24-hours**" – means that the object's group is constantly armed.



In addition to these options, you can also choose "**Control-night closures of objects, the interval XX:XX**" – sends a reminder to CMS operator (event "**Full-Time object Has Not Been Closed on Time**" in the "**Unprocessed**" tab of "Duty Operator" software) in case if the time before object closing exceeds the specified time interval.

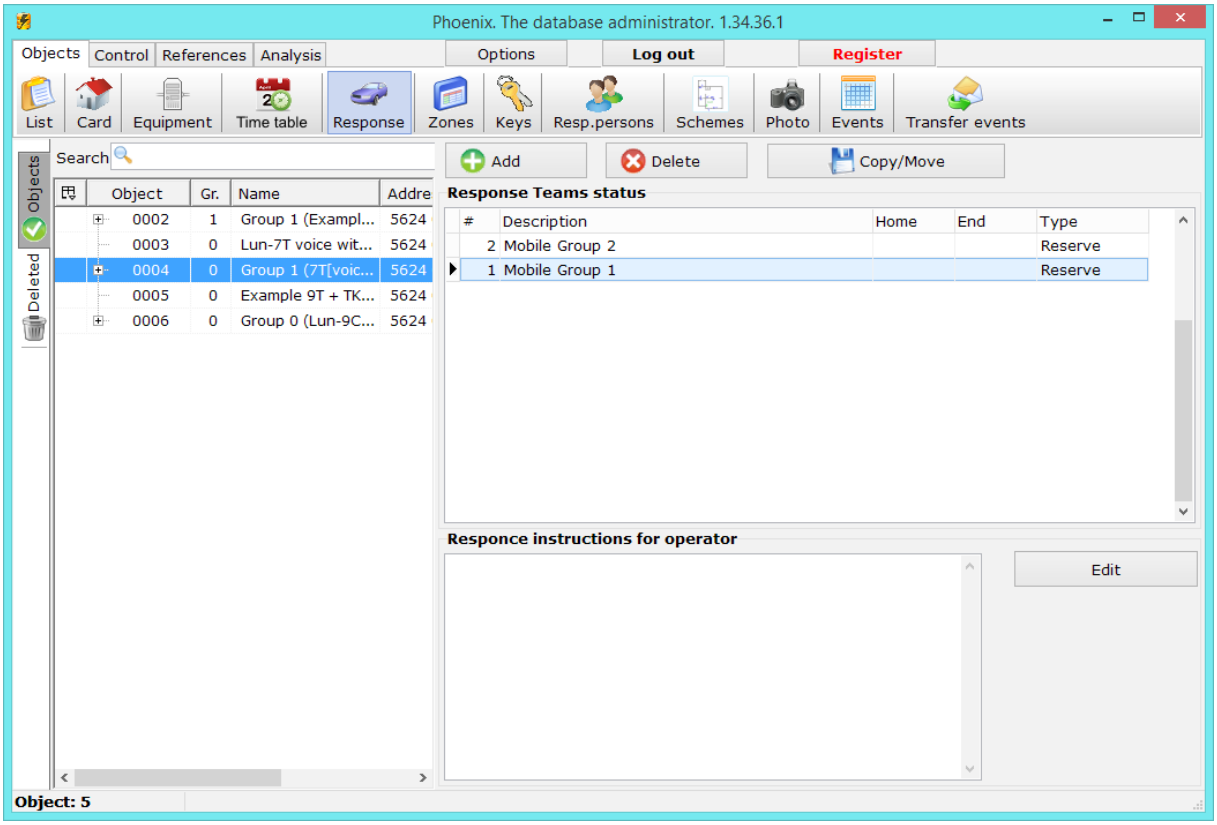
"**Agile time schedule**" – suitable for private apartments, garages and other s where it is impossible to foresee any work schedule.

"**No Arming/Disarming**" – used for round-the-clock sites. In this mode, only the panic button is monitored.

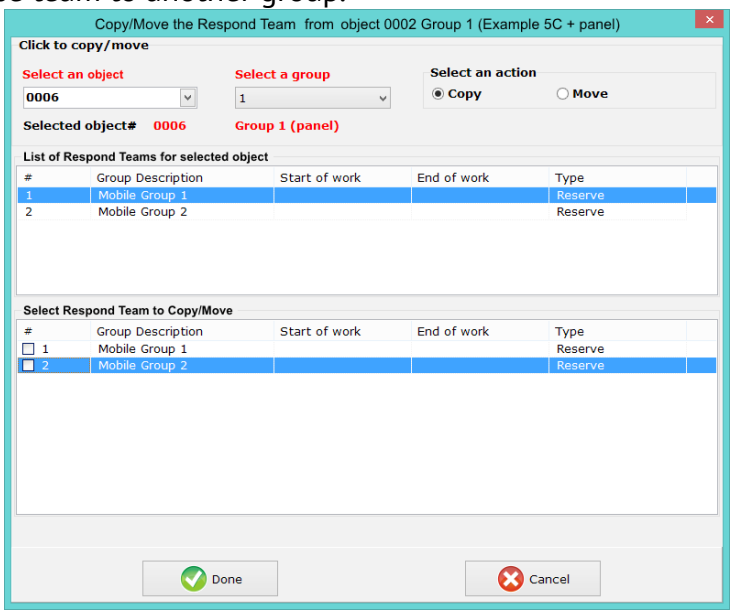
"**Unknown**" – used by default when creating a new object group.

Attention! Control Center responding to "Time table" of all objects is dependent on the settings of "Advanced" page of "Control Center" program.

6.3.6. Response Teams section

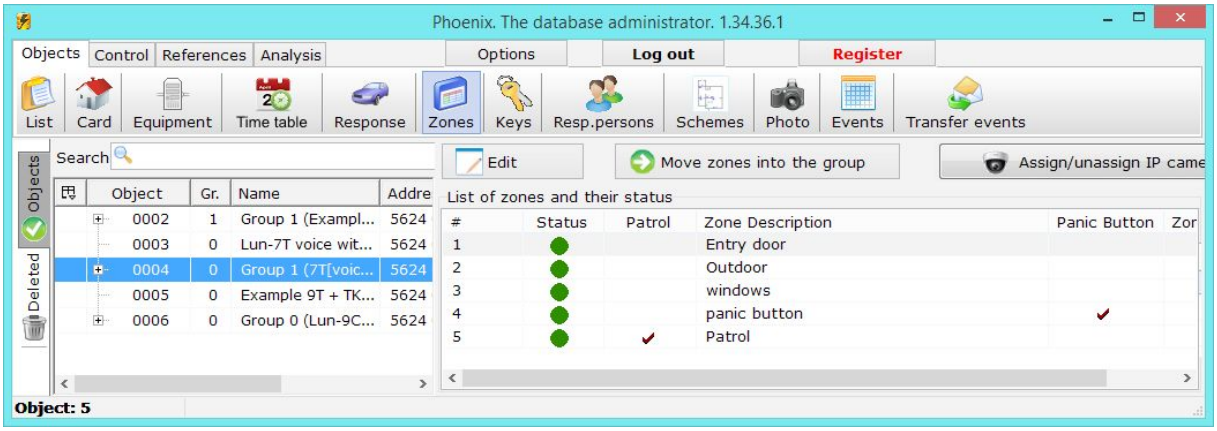


"**Response**" section displays the information about response teams assigned to a particular object's group, as well as the operator's response instructions. "**Copy/move**" button opens a window to move/copy a response team to another group.



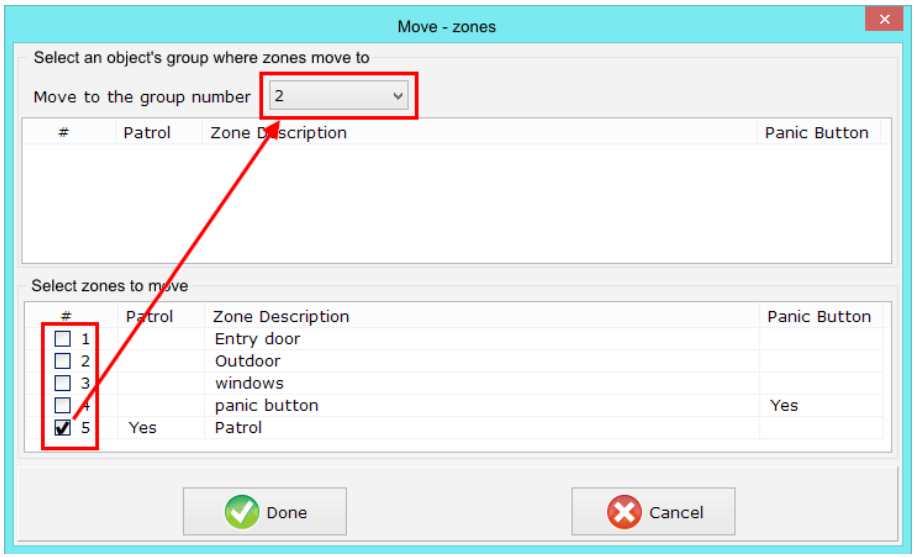
In the "**Select an object**" field select the object you want to transfer a response team. In the "**Select a Team**" field select the object's group to transfer the response team. "**Select Action**" switch indicates how to transfer a team ("copy" or "move-and-delete"). In the "**Select Response Team to be Copied/Transferred**" you can mark the response team switch will be moved or copied to the selected object's group.

6.3.7. Zones section



"**Zones**" section displays the information about the zones of object's group.

If the object contains several groups, you can move a zone from the current group to another one by "**Move zones into the group**" button (window is shown below).



In the list on the bottom of the window you can select zones to be moved to the group, which you can select at the top of the window.

"**Patrol**" field is used to control the arrival time of the response team to the object. To set the loop as "Patrol", you must first set the name of this loop as "***Patrol***". Only after that it will be possible to change the type of loop in the "**Patrol**" field (value "***Yes***").

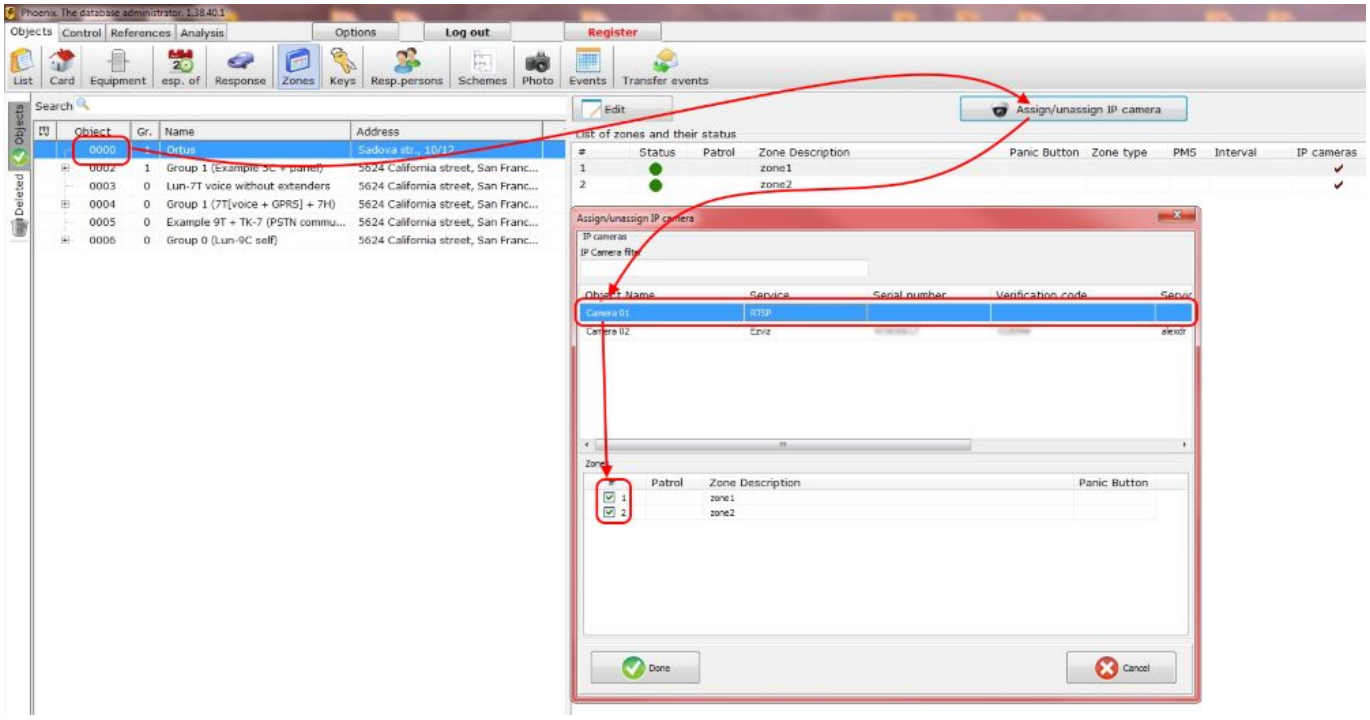
Button "**Assign/unassign IP camera**" allows you to match events on the selected zone of the object with one or more IP cameras for later viewing the video stream from the camera in real time or from the archive of records (depending on the service used (see Section 5.6).

To do this, first select the desired object, then press the button "**Assign/unassign IP camera**", and in the opened window select an available camera, and then check the boxes, those zones that need to be connected to the selected camera (see picture below).

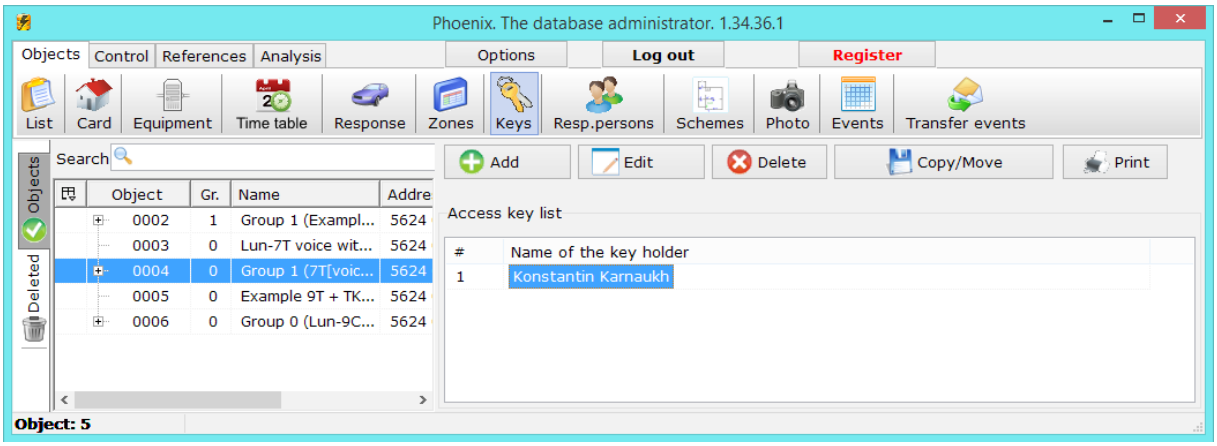
After clicking the "**Finish**" button, the IP camera will be tied to the device zone. You can repeat this operation to link another IP camera to the same device/zone.

The values of any combinations of IP cameras, devices and their zones are allowed.

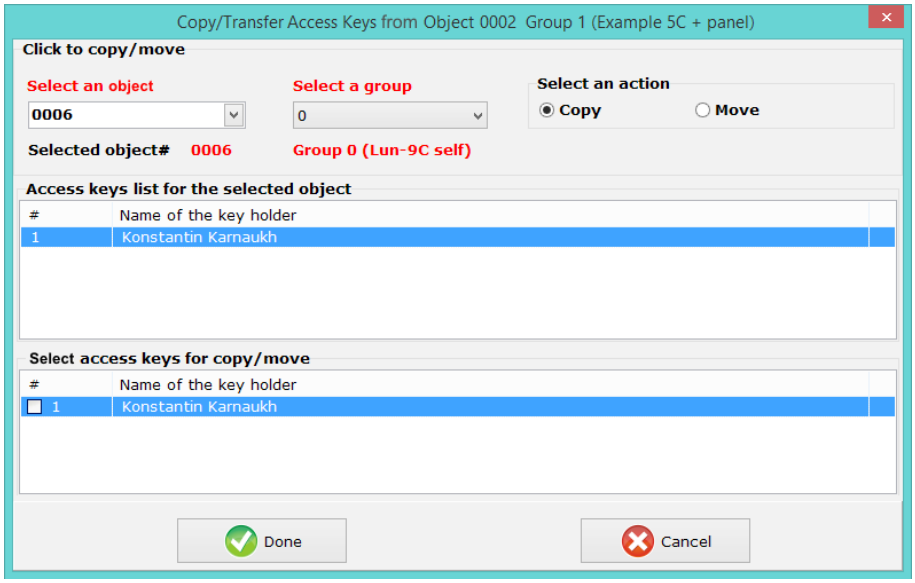
In order to unbind the IP camera from the zone, you need to repeat the above steps and uncheck checkbox next to the required device zone.



6.3.8. Keys section

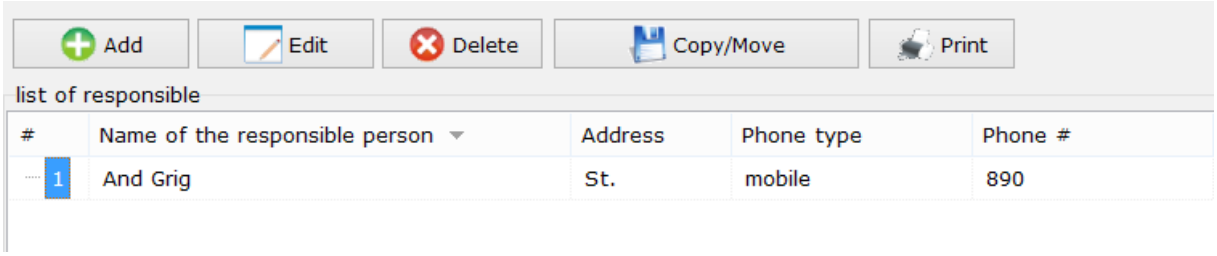


"**Keys**" section displays the information about the object owners access keys. You can add, edit, delete, and copy/move the keys:

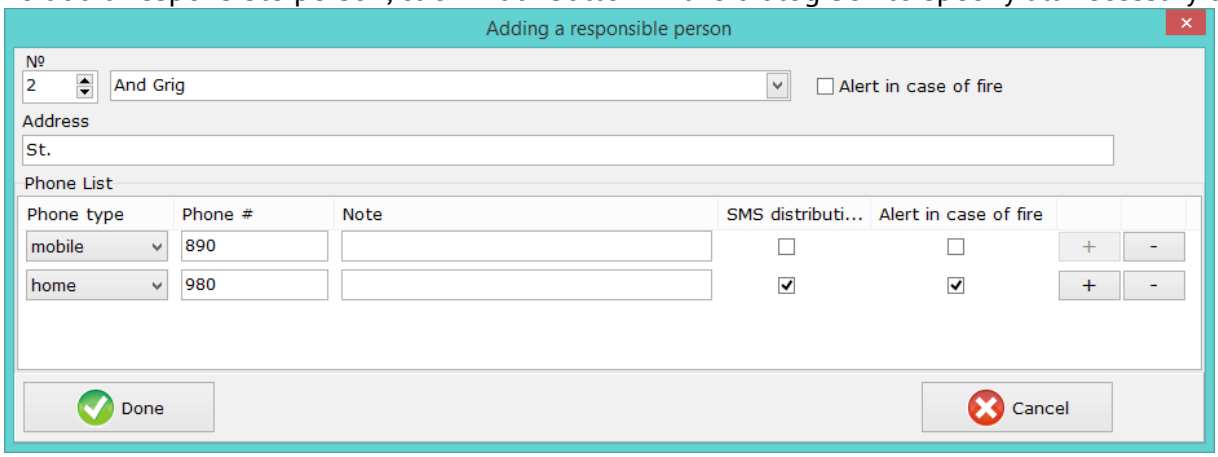


6.3.9. Responsible persons section

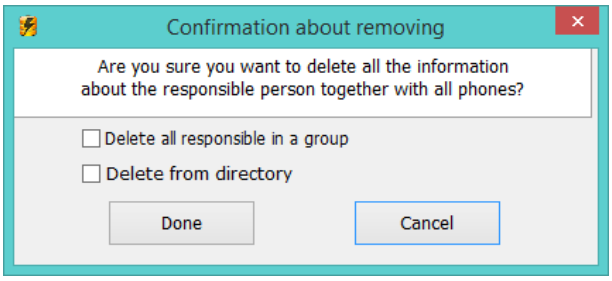
"**Responsible persons**" section shows the information about the persons that must be contacted in different cases, for example, in case of alarm, re-closing etc.



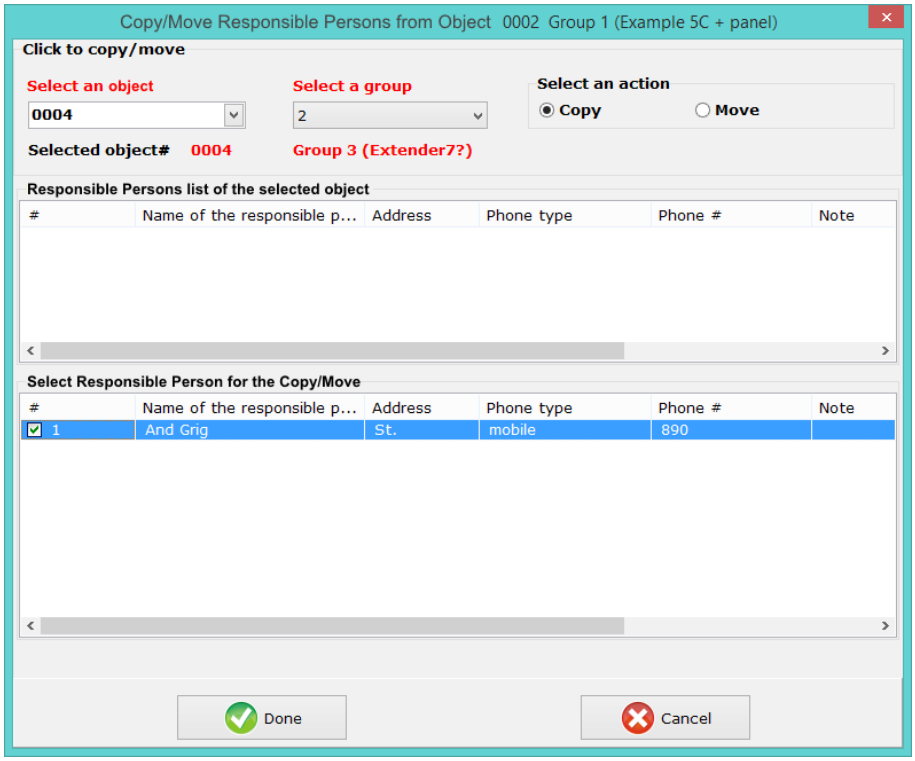
To add a responsible person, click "**Add**" button in the dialog box to specify all necessary data:



You can remove all the responsible persons at a time by setting the appropriate checkbox in the window and clicking "**Delete**":

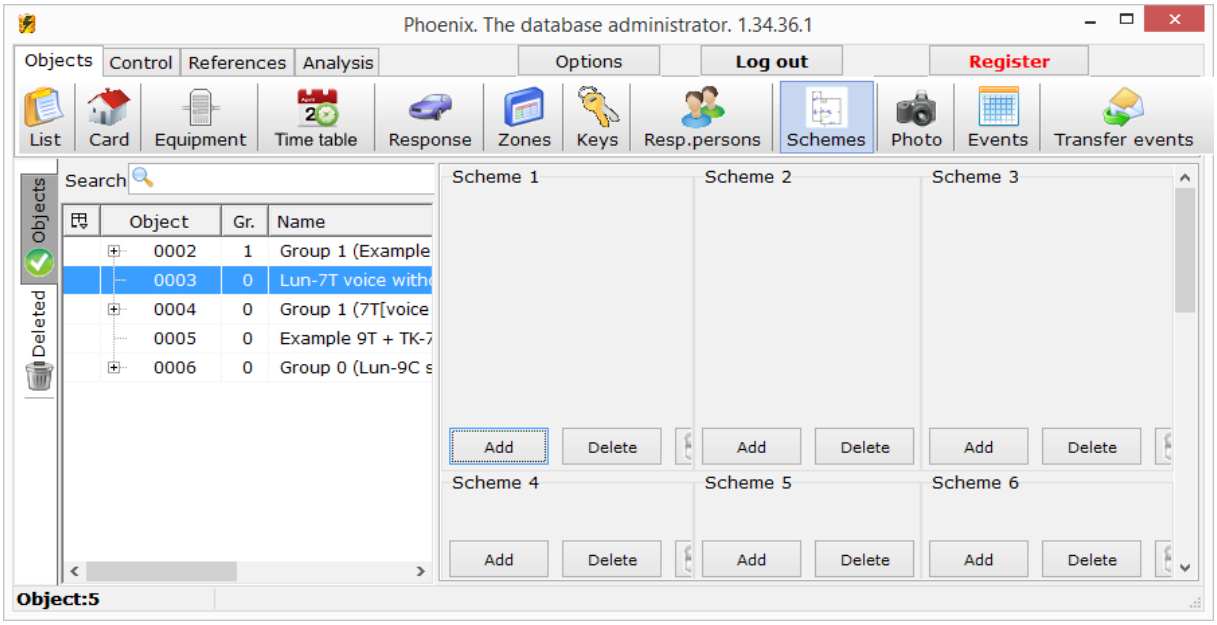


You can also copy or move s sand groups between the responsible persons with the help of "**Copy/Move**" button:



At the top of the window you need to choose where to copy/move the responsible persons: object and group (you can copy all groups by selecting "**All**"), as well as the action itself – copying or moving. In the middle of the window you can see the existing responsible persons. At the bottom you can select responsible persons then click "**Done**".

6.3.10. Schemes section



"**Schemes**" section shows the diagrams for each object group. These diagrams may include object access diagrams, burglar alarm diagram, etc. Diagrams are common graphic files that display any information about the object. The system supports a maximum of 27 graphic diagrams. Graphic diagram can be created in any graphic editor that supports saving of files in JPEG (*.jpg extension). These files are automatically copied to the chart folder that contains program settings by pressing "**Add**". When copied, a new name is assigned to the file as follows:

<object_number> _ <group_number> _ <a..z or &>. jpg

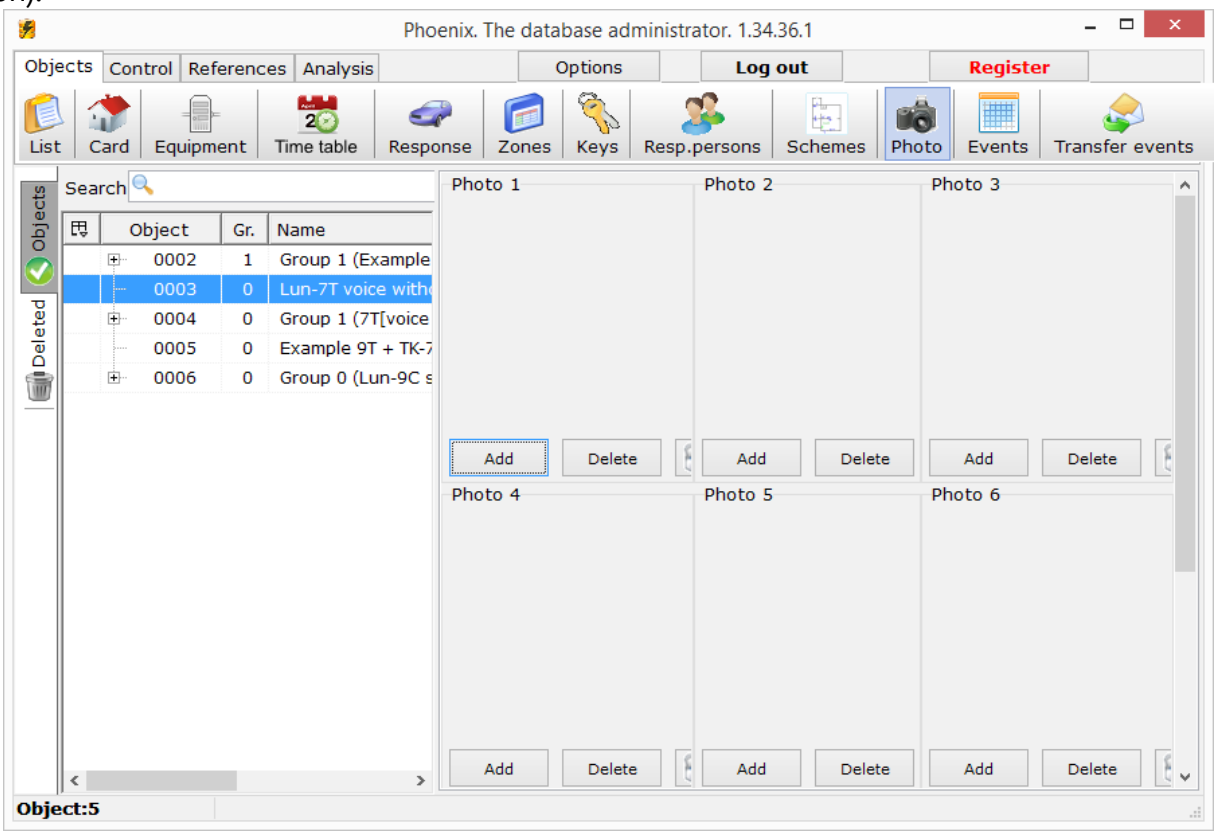
Example 1: **1011_1_a.jpg** – Object **1011**, group **1**, Scheme No. **1**.

Example 2: **2344_2_b.jpg** – Object **2344**, group **2**, Scheme No. **2**.

Example 3: **2345_7_&.jpg** – Object **2345**, Group **7**, Scheme No. **27**.

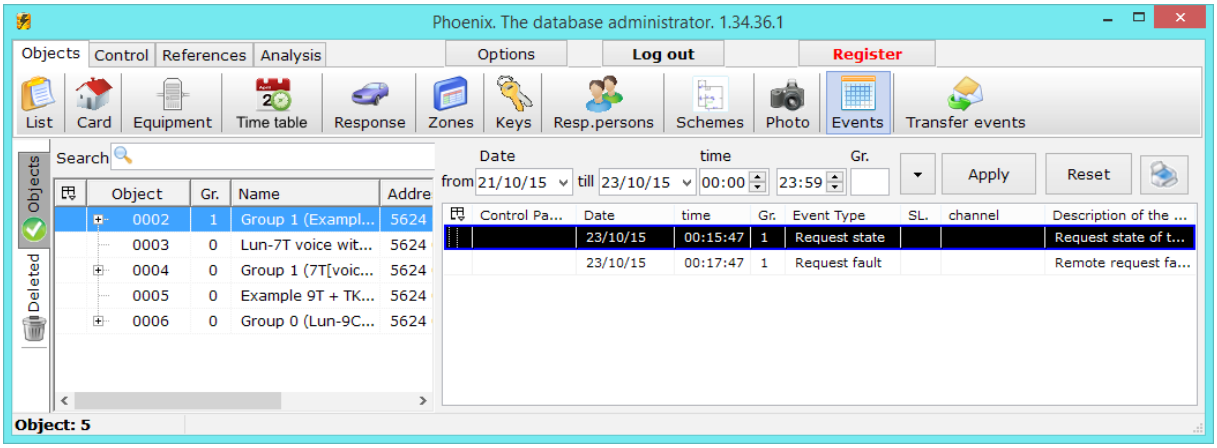
6.3.11. Photo section

This section is used to specify and display object's photos. You can specify up to 9 photos for each object. Photo storage path is indicated in the program settings (see "DB Administrator" configuration).

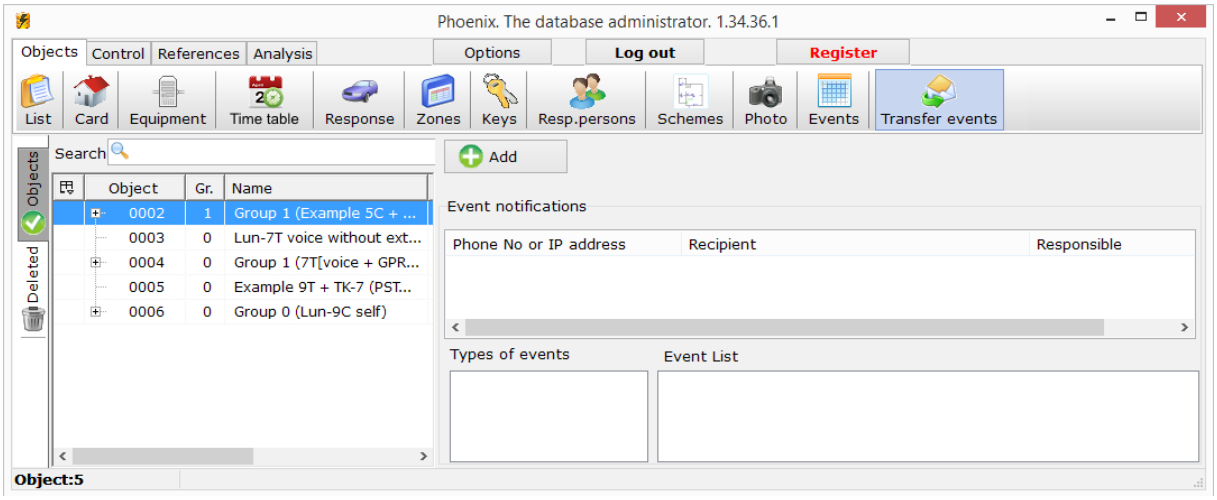


6.3.12. Events section

"**Events**" section displays the information about events sent to CMS from the object's group.



6.3.13. Event Transmission section

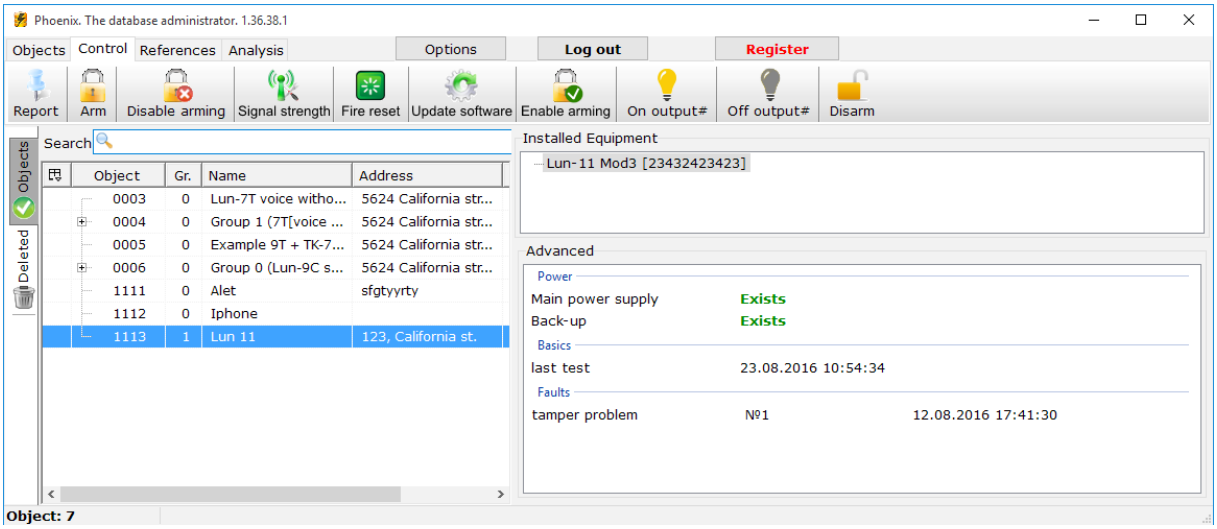


"**Event Transmission**" section displays a list of message recipients from CMS. These can be SMS notifications, event transfer to a remote CMS or events that will be sent to this recipient.

SMS from the disconnected objects will not be sent.

When you add an existing object, the program remind if the other groups of this object are already configured to transmit events.

6.4. Control tab



It shows the ability to remotely control the status of the object and its instruments (main and backup power, signal strength, GSM-module temperature, final test and other instrument parameters). Panel view (a list of available buttons) depends of the selected object, installed Control Panel type, user permissions and involved communication channels.

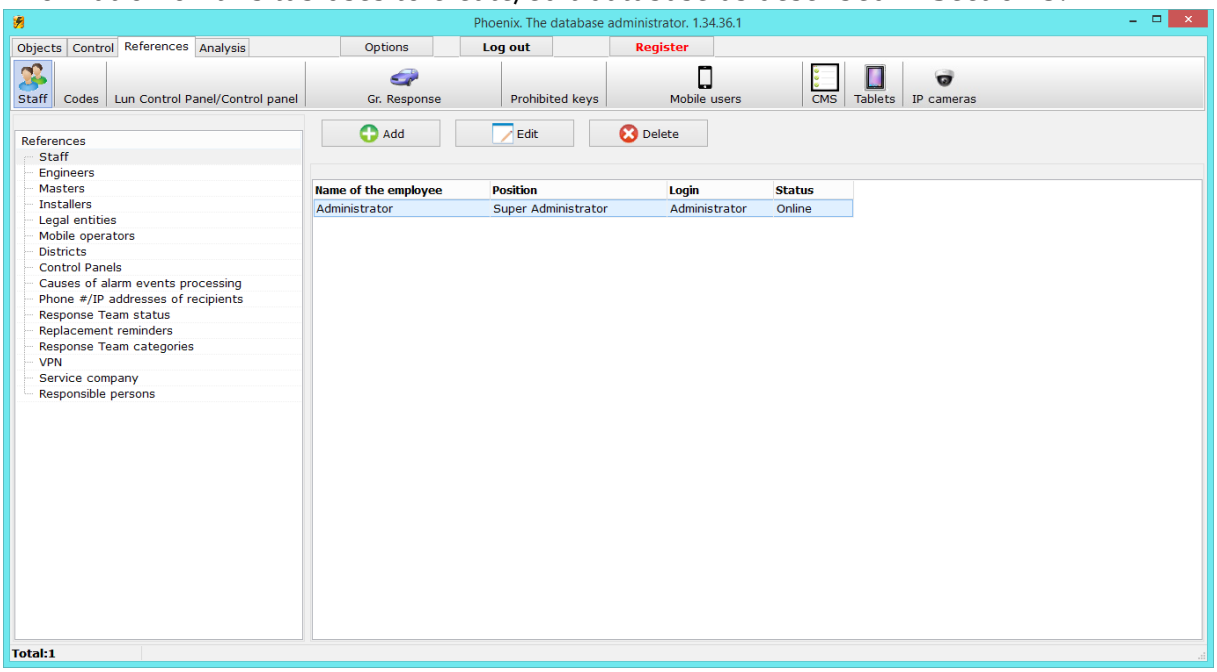
For example, "Lun-11" Control Panel supports the following remote control functions (functions marked as bold correspond to buttons on figure above):

- **Report**;
- **Arm** (forced, with alarm for violated zones);
- Conditional arming (if violated zones cannot armed);
- **Disable arming** (for one group);
- **Enable arming** (for one group);
- **Signal strength** (only for GPRS-channels);
- **Output control** (on and off);
- **Reset** fire subsystem;

- **Update** embedded **software**;
- Time synchronization (setting the device time in accordance with the time of CMS);
- **Disarming** (if enabled in device configurations);
- Conditional arming mode "Stay Home";
- Get photos from camera (for any of the cameras if enabled in device configurations).

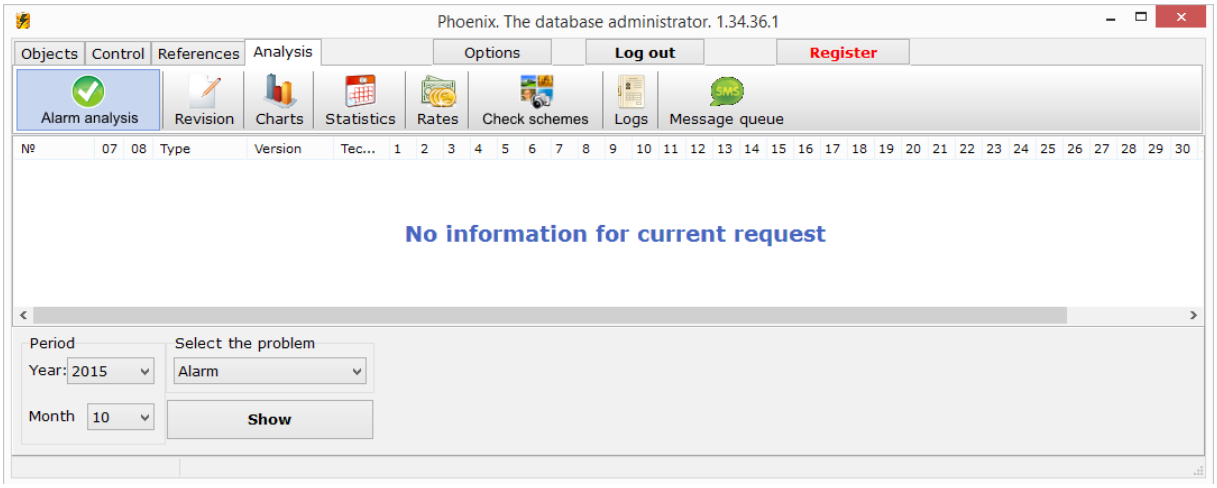
6.5. References tab

Information on this tab uses to create/edit database as described in Section 5.



6.6. Analysis tab

The information in this tab is used for analysis of the security system and the object status in time, display of statistics providing security services according to different criteria and other information.



6.6.1. Alarm Analysis section

"**Alarm Analysis**" section allows analysing of the quality of object operation, cable installation and antenna location (see figure above).

This analysis should be carried out for the previous month (to be specified in the parameters "**Period**").

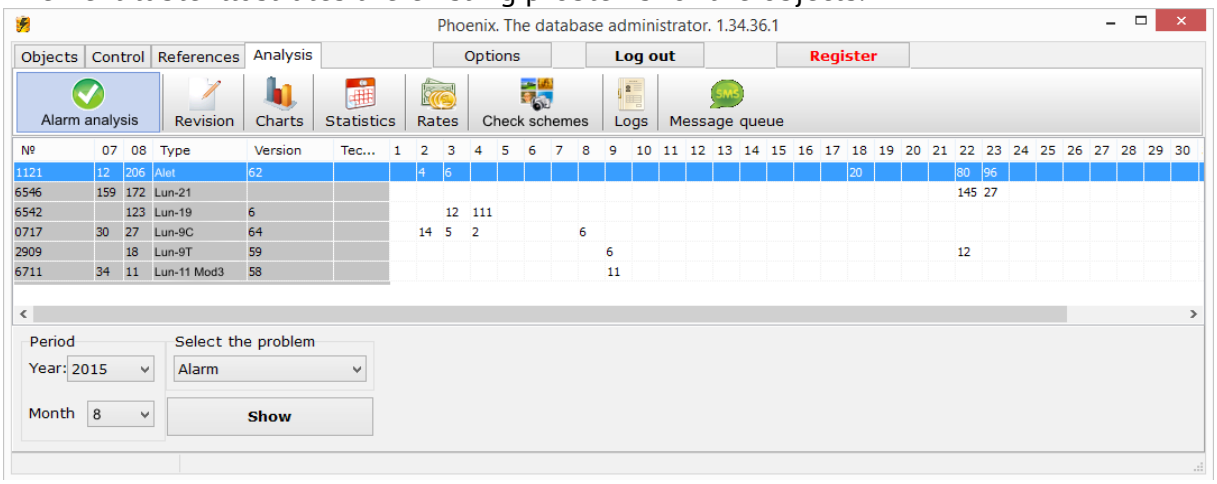
You can choose one of the next event types:

- Alarms;
- Restarts;
- Statistics by OFF, Z3, OD3, Z14 special codes;
- Coordinates are not true (for "Alet" device);
- Main and backup power supply troubles;
- Shock sensor and motion sensor alarms (for "Alet" device).

You can also specify how to sort the entire list and filter criteria in the appropriate fields.

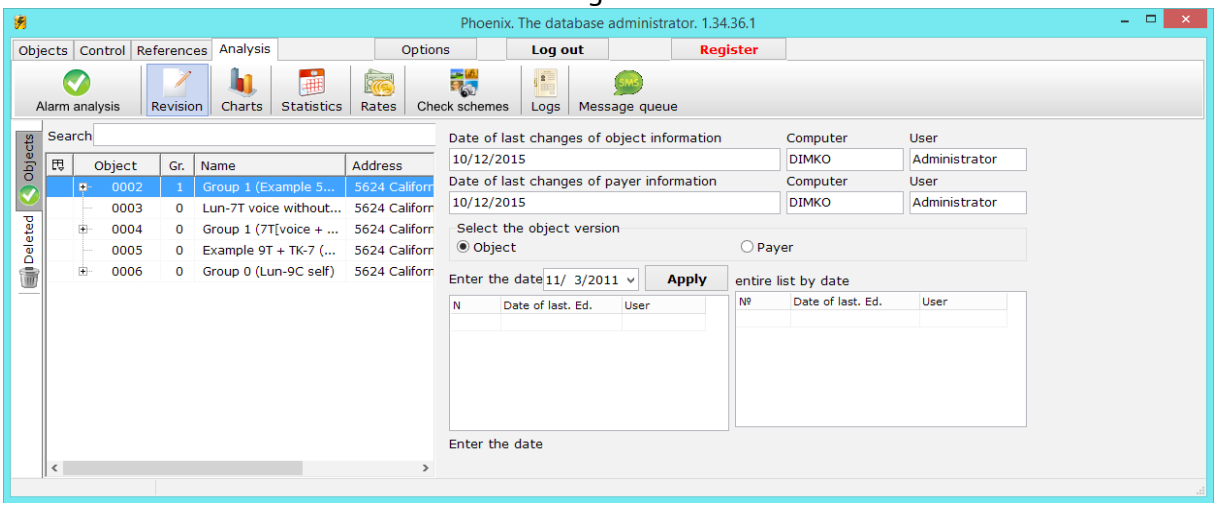
All information display as table where days of the month placed horizontally, while the number of events for the specified day placed vertically.

The next table illustrates the existing problems for the objects.

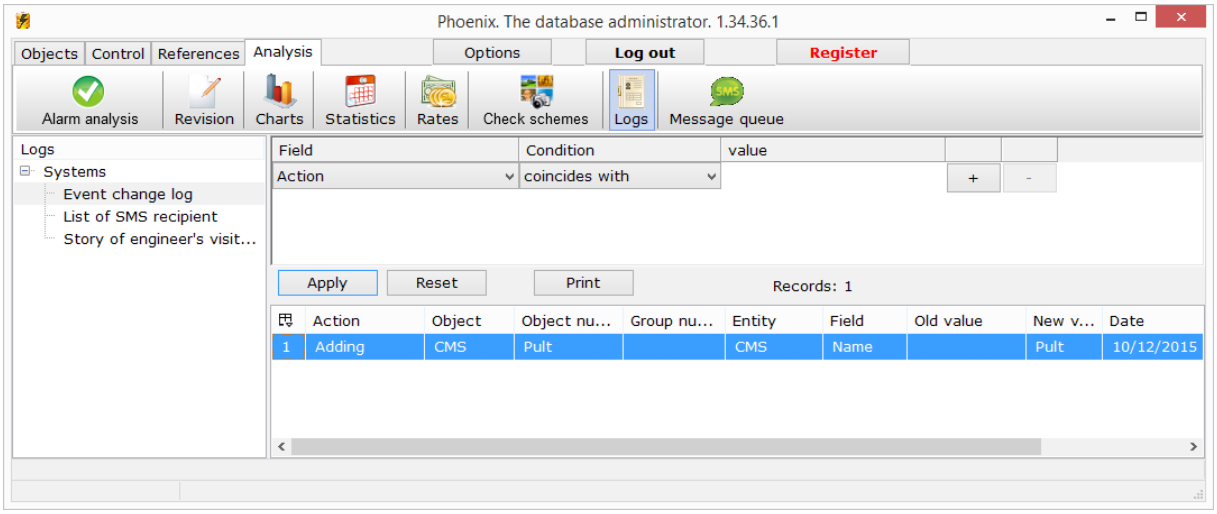


6.6.2. Revision section

"**Revision**" section shows the date of the last information modification, as well as the computer name and user name where and who changed it.



6.6.3. Logs section

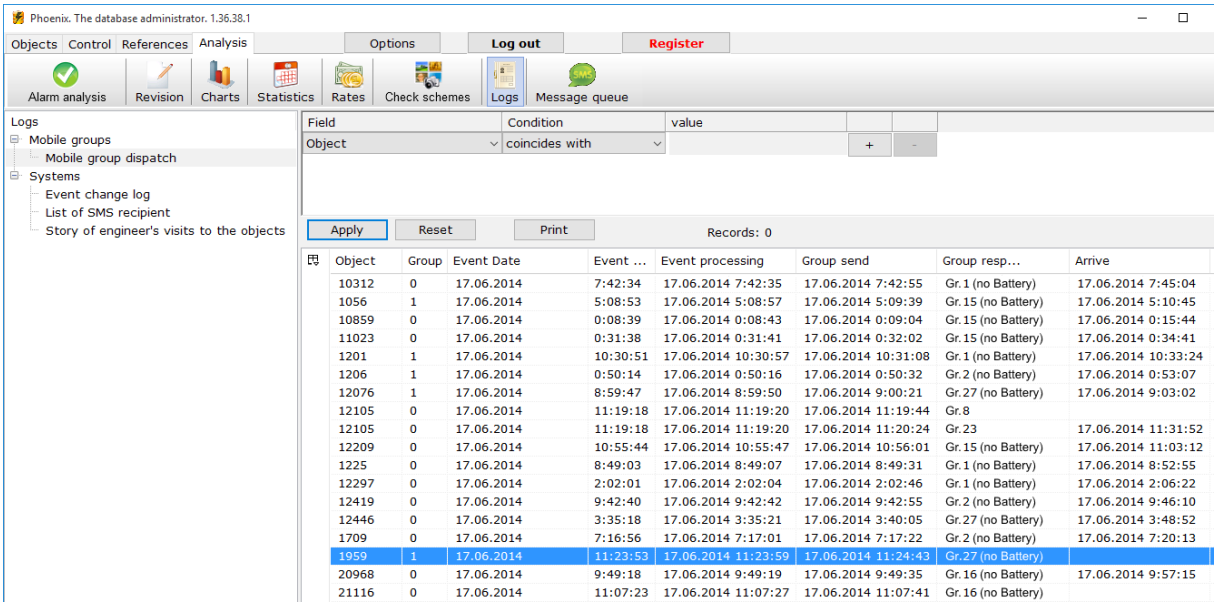


This section displays various logs grouped in the list. You can select a category of logs, then a particular log itself. Log types:

- Response Teams log:
  - Response team visits;
  - Temporarily unsupported objects;
  - Unsupported objects.
- System log:
  - History of object changes;
  - List of SMS recipient;
  - Story of engineer's visits to the objects.

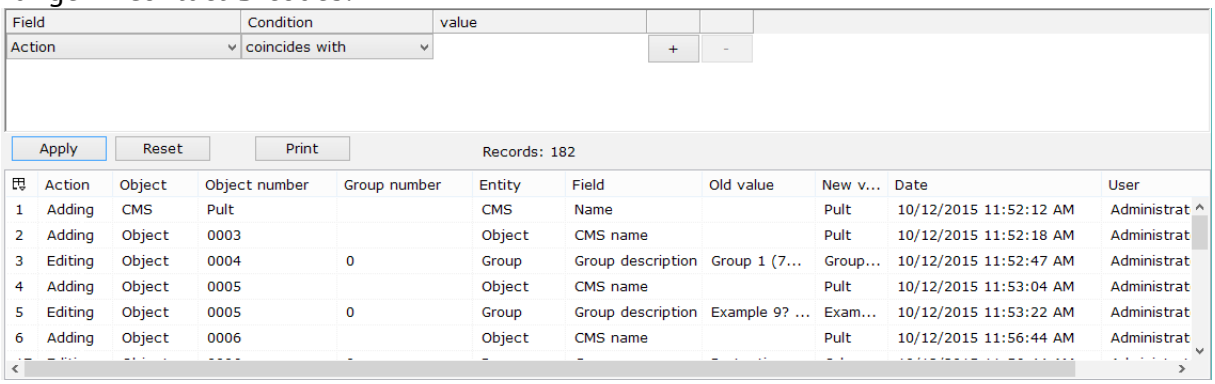
Response team visits log displays all visits of response teams. The log can be filtered by:

- Object;
- Group;
- Event time;
- Acceptance for processing;
- Response team sent date/time;
- Response team number;
- Arrivals;
- Result.



History of object changes log is used to display the object changes (all information), as well as

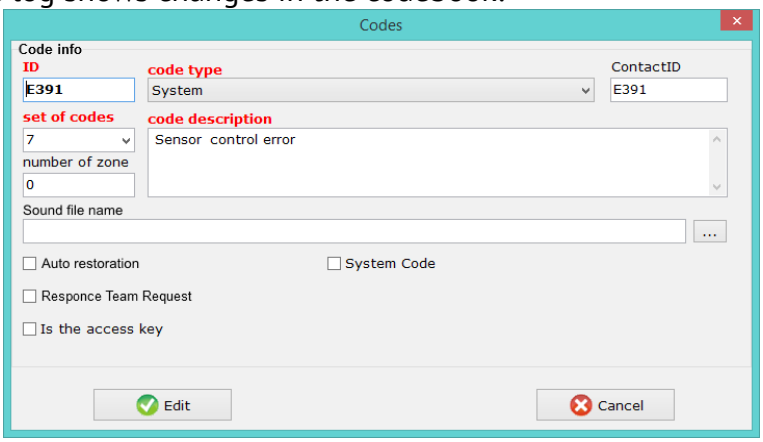
any change in ContactID codes:



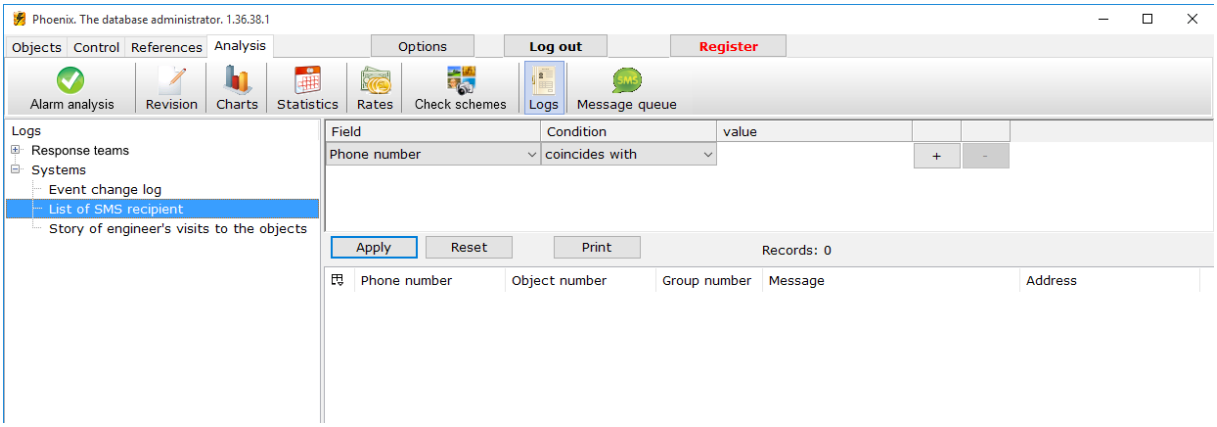
You can filter by all the fields, namely:

- Action;
- Logged object (object, personnel, engineers);
- Object number (name);
- Group number;
- Entity (what was edited);
- Old and New value;
- Date and Time;
- User name (for Phoenix-4);
- Computer (used for editing).

The same log shows changes in the codebook:

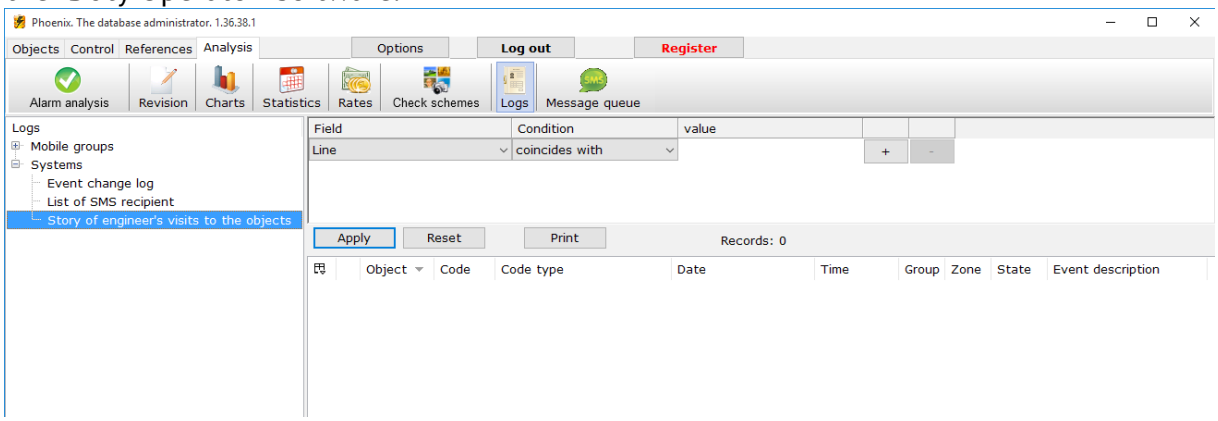


List of SMS recipient log displays the list of persons receiving SMS about the events on objects.



The list can be filtered by phone number, object number, group number, object name and address. If no search criteria is specified, after clicking "**Apply**", you will see all the recipients of SMS-messaging (their phone numbers). In addition, you can print the list by pressing the "**Print**" button.

Story of engineer's visits to the objects log used to display information about the visits of maintenance engineers (technicians). In order to do this, operators must use appropriate functionality in the "Duty Operator" software.



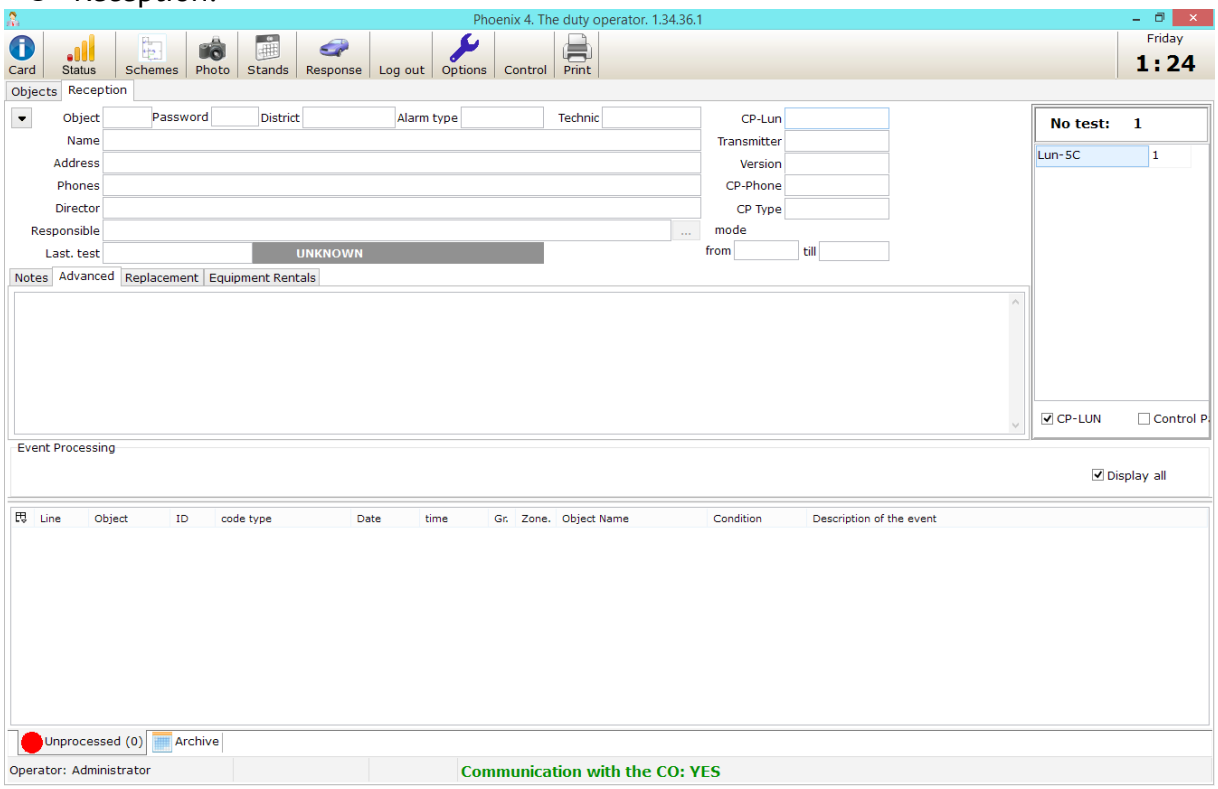
7. “Duty Operator” software

7.1. Main window

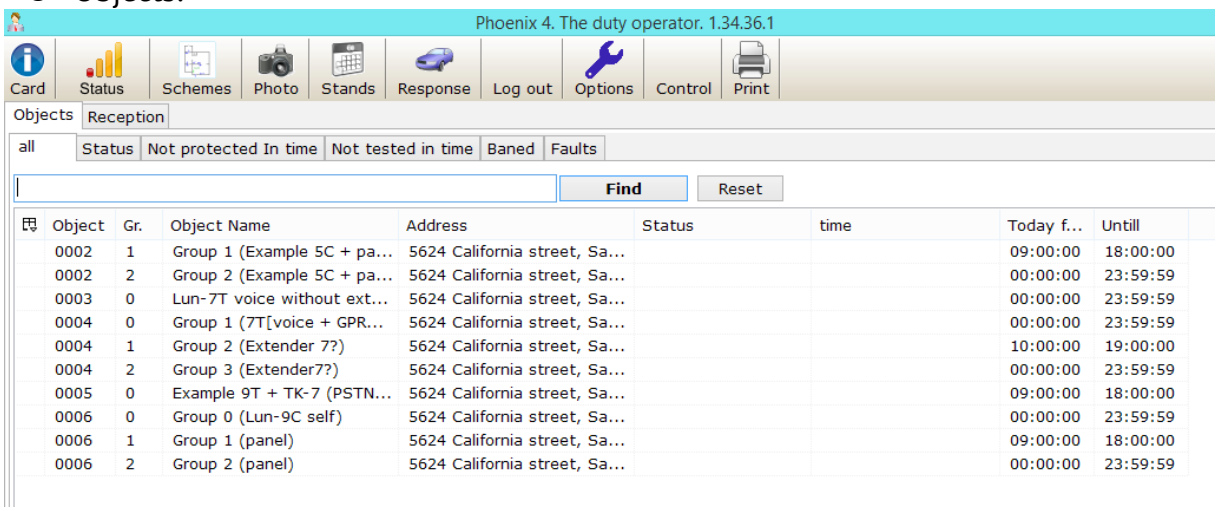
Duty Operator is used to receive and process alarms, send response teams and track the object status. This is the main program of CMS operator.

Main window contains of toolbar and tabs:

- Reception:



- Objects:



In the **Search bar**, on the **Objects** tab you can search all objects by

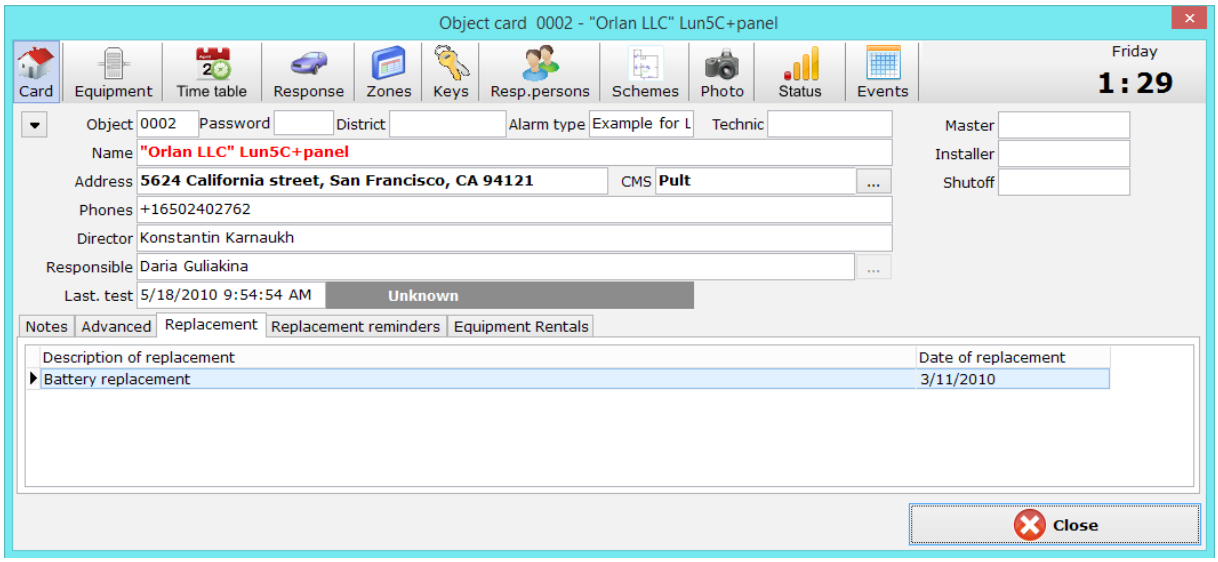
- Number;
- Name;
- Address;
- Sim-card number/ IP-address.

7.2. Toolbar

Toolbar is on the top of the window:

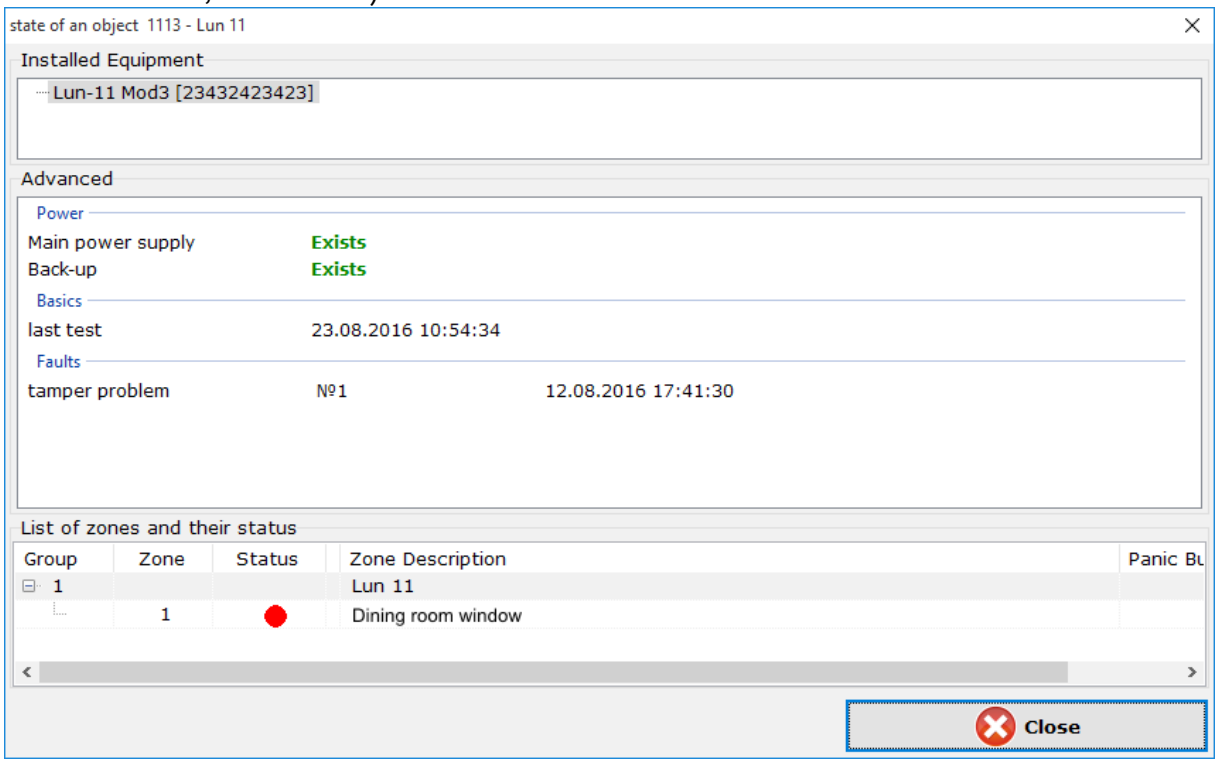
7.2.1. Card button

Card shows the complete card of the group selected in "**Objects**" or "**Reception**" tabs. At the top you will see a card navigation bar; in each section you can see the necessary information, just as in "DB Administrator" software.



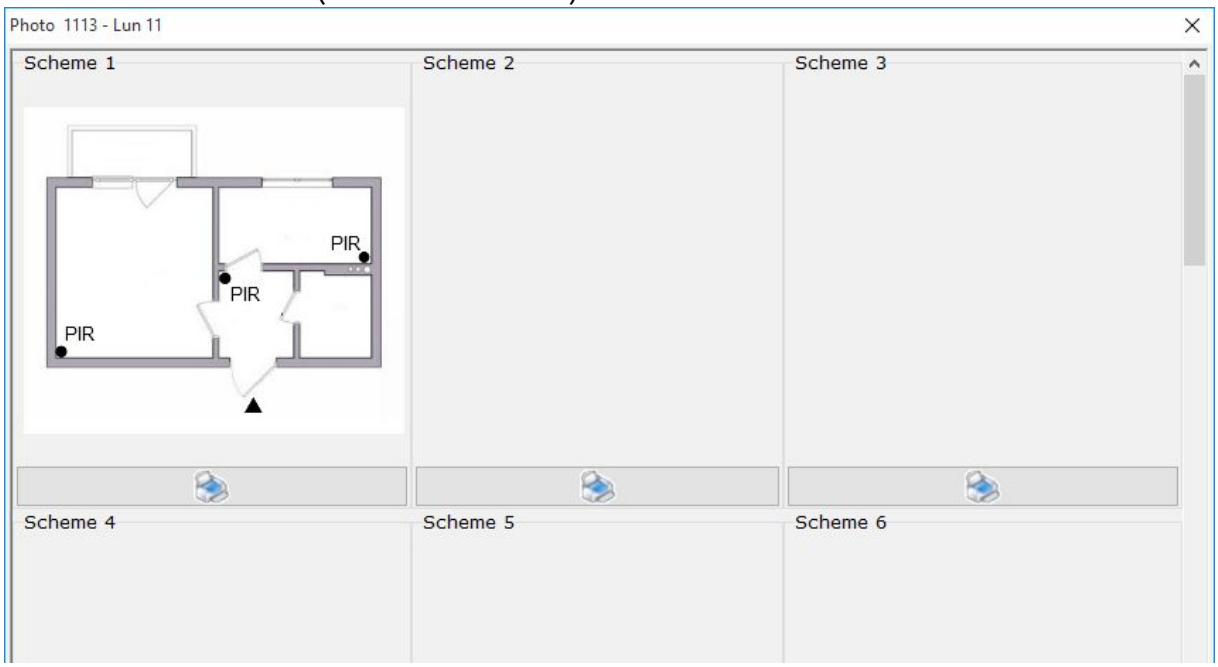
7.2.2. Status button

Status button shows the object's Control Panel system status (main and backup power source, basic info and faults, zones state):



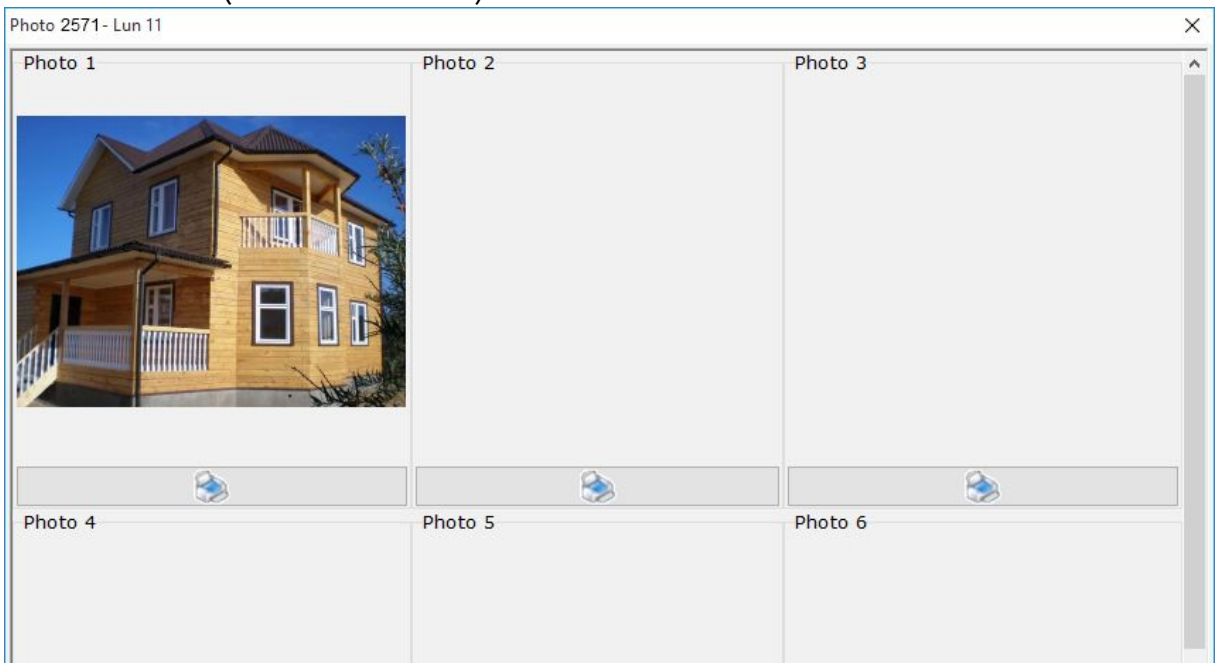
7.2.3. Schemes button

Schemes button shows all object's schemes that have been created and added to object in “DB Administrator” software (see section 6.3.10).



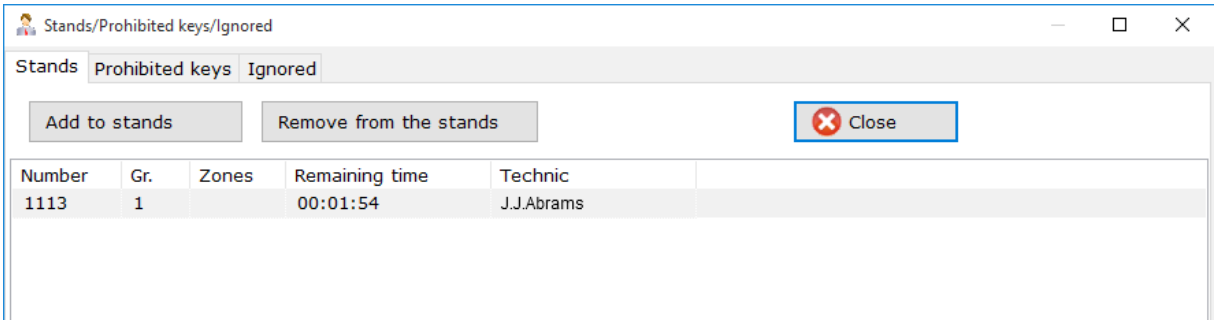
7.2.4. Photo button

Photo button shows all object's photos that have been created and added to object in “DB Administrator” software (see section 6.3.11).

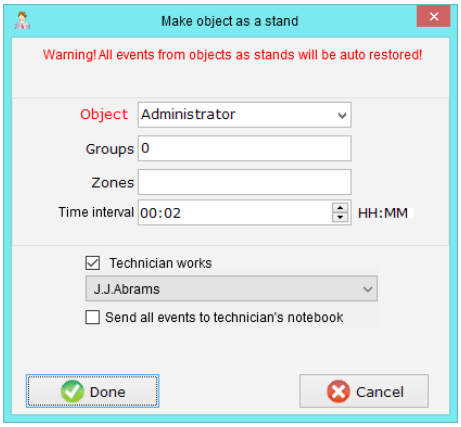


7.2.5. Stands button

Stands button shows the objects where security system repairs and the time until the end of them. For these objects, all events are auto-recovery. If any engineer present at the object, its name appears in the "**Technician**" column.



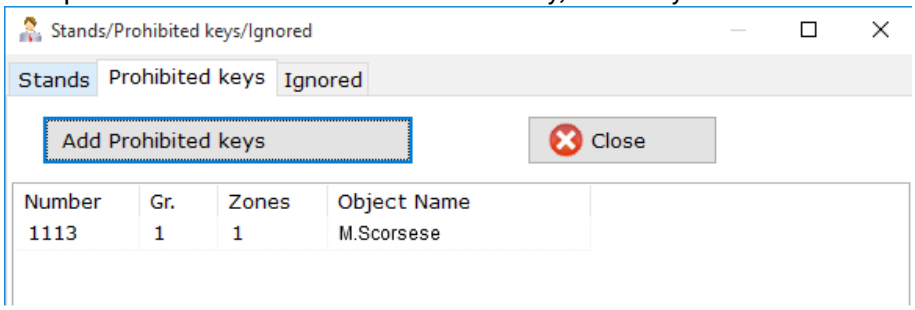
From this window you can make an object as a stand by clicking the appropriate button. Then you will see the following window:



You can specify the object number, groups, zones (separated by commas) and the time interval while it will be as stand. You can also specify that a technician works at the object at this time. If the technician use the "Phoenix Tech" software on personal laptop, all object's events can be send to technician's laptop by "**Send all events to Technician**" option.

After the object made as a stand (or vice versa), this action is saved in the event log.

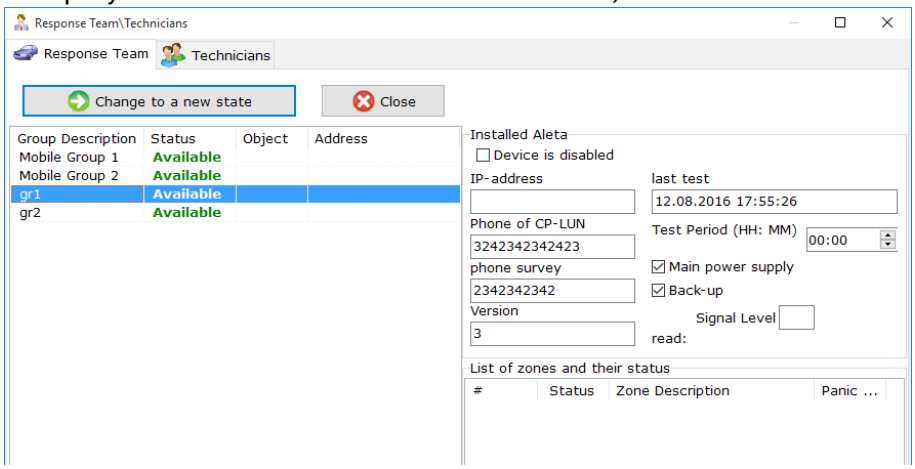
Unauthorized keys tab displays the keys that have been banned in CMS (lost or stolen), so any arming/disarming with these keys will come with alarm and "**Arming/Disarming with unauthorized key**" message. CMS operator can add an unauthorized key, but only administrator can remove it.



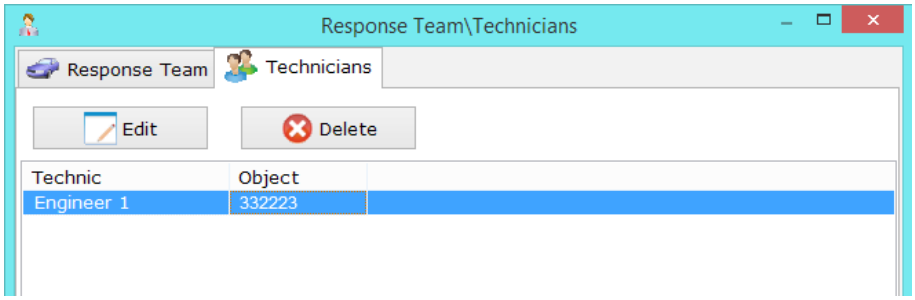
On the **Ignored** tab, you can add objects, groups, or zones, then all their events will be ignored and not be saved to the archive database, though the device will send these events to the CMS.

7.2.6. Response team/Technicians button

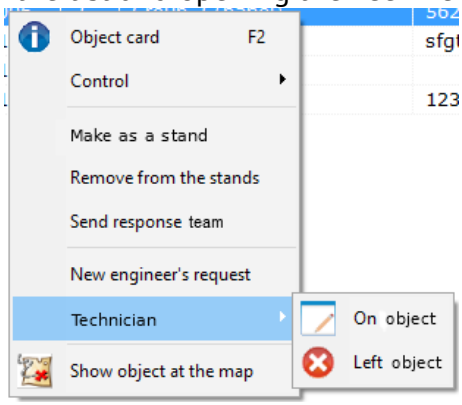
Response button shows response teams (on the corresponding tab), as well as their location and status. It also displays information on the "Alet-9" devices, which are set on the team's cars.



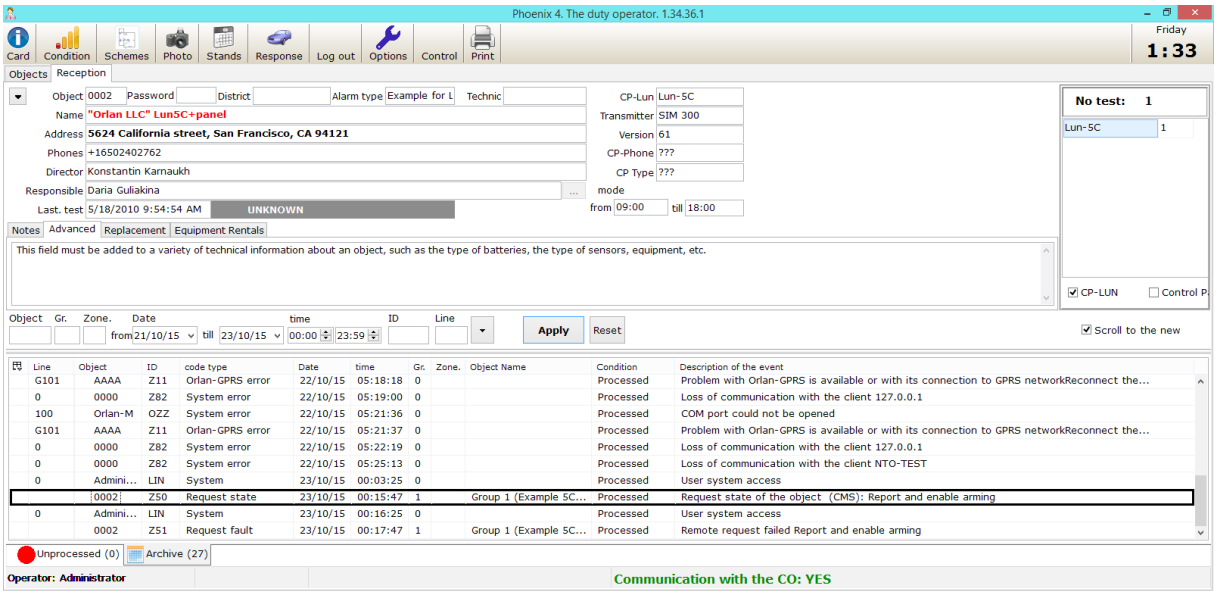
In **Technicians** tab you can see a list of technicians/engineers and objects where they are currently located.



To change the object number, where technician is currently located, click **Edit**. To specify that the technician left the object, click **Delete**. These actions can also be performed using the context menu by selecting an object from the list and opening the **Technician** field:



7.3. Reception tab

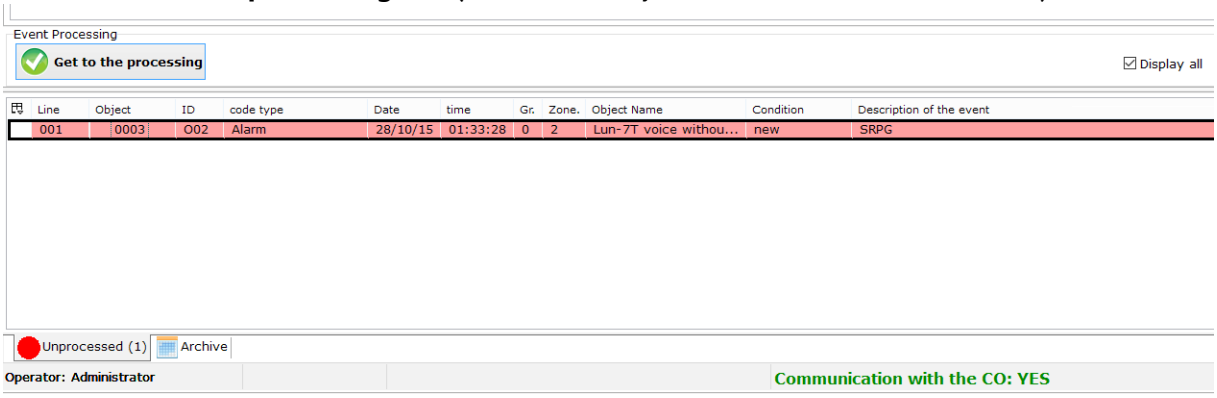


Window content is divided into two parts. At the window's bottom part you can select some object's event, then in the window's upper part you will show the information about selected object.

The window's lower part shows lists of events in **Unprocessed** and **Archive** tabs.

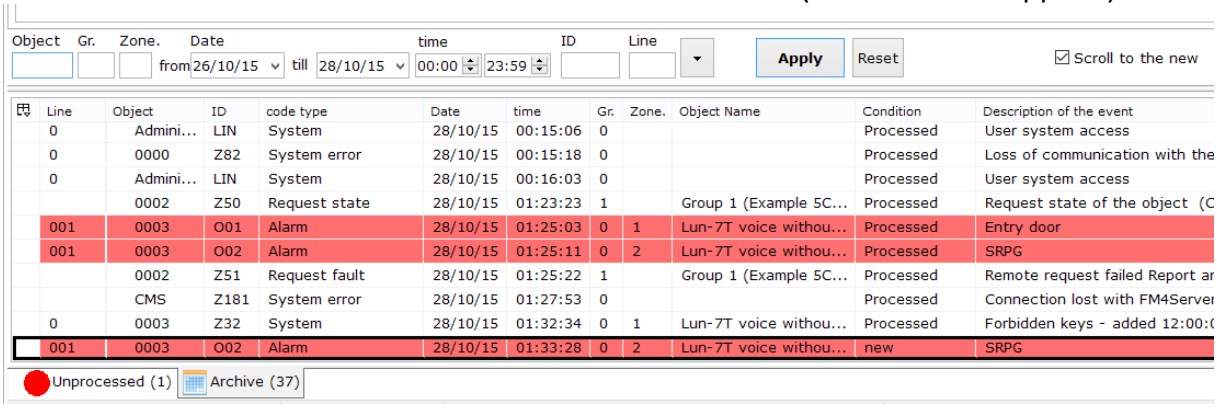
7.3.1. Unprocessed

There are all events that require operator's assistance. Events colour is corresponding to "DB Administrator" software (see Section 4.2). After the operator selected event, then click **Get to the processing** button and finished processing with some action (in the associated window) – this event will be deleted from **Unprocessing** tab (but it is always stored to **Archive** database).



7.3.2. Archive

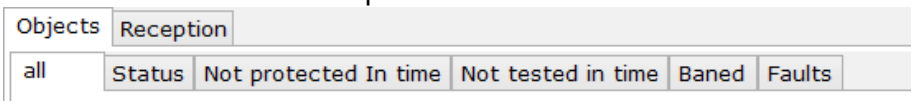
As usual it shows last 50 events was received to Database (with no filters applied).



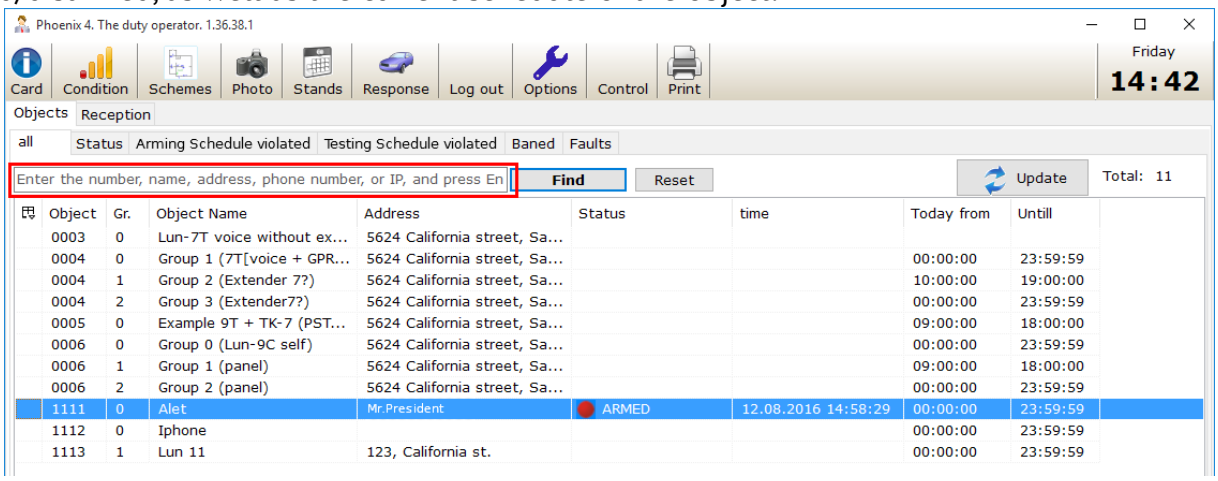
Scroll to the New checkbox allows to follow CMS receiving events and show their according with applied filters by **Object**, **Group**, **Zone**, Code (**ID**) and communication **Line**. If no filter applied, it show all events that CMS received. To set a filter, you should fill in the required values and click **Apply**. To reset filters, click the **Reset** button.

7.4. Objects tab

Objects tab contains 5 sub-tabs as a specific filters:

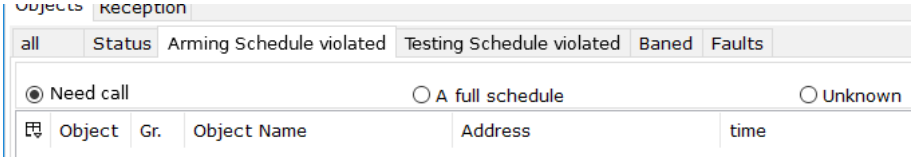


All tab displays all the CMS registered objects. In the **Search** bar you can search for objects by number, name and address. **Esc** key clears the filter. **Update** button updates the objects status. The **Status** column displays the status of the object: **Armed** or **Disarmed** and time since which it is armed/disarmed, as well as the current schedule of the object.



Status tab divides objects into 2 categories: **Armed** and **Disarmed.**

Arming Schedule violated tab displays the objects that haven't been armed with schedule violated, and includes 3 switches:

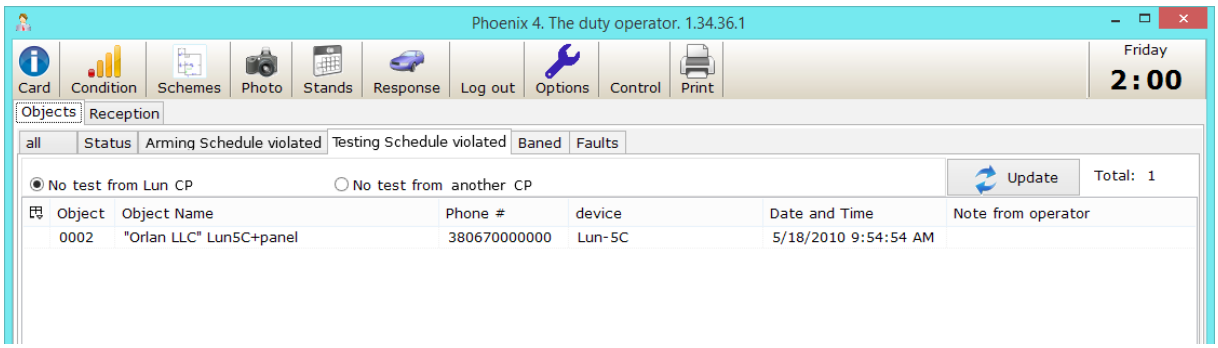


Need call – objects, where **Obligatory Call to object in case Schedule violated** option is set in the object's **Time Table** section (see Section 6.3.5). These objects must be called by operator to know when the object will be armed, and why they haven't been armed yet.

A full schedule – objects that have an arming schedule, and according to this schedule, they should already be armed.

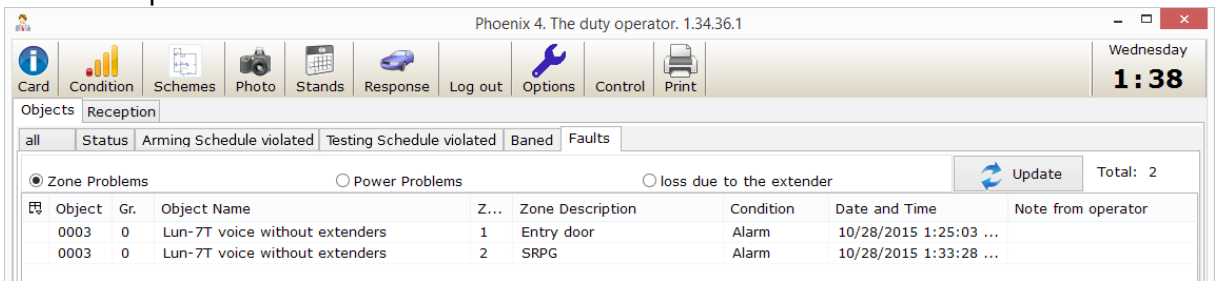
Unknown – unknown schedule, only for connected objects or objects with unknown schedule.

Testing Schedule violated displays the objects, where the test was lost at the time specified in **Date and Time** column.

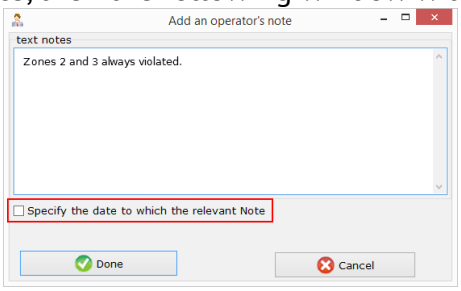


Baned tab shows the objects with disable arming for some reasons.

Faults tab contains 3 switches. **Zone Problems** displays the objects with zone violated, which means that the service required. **Power Problems** displays a list of objects where the main and/or backup power is lost. They should draw the attention of operators, so the Control Panels at these objects were not left completely without power. **Loss due to the Extender** shows the objects with communication problems between the Control Panel and zones extender module.

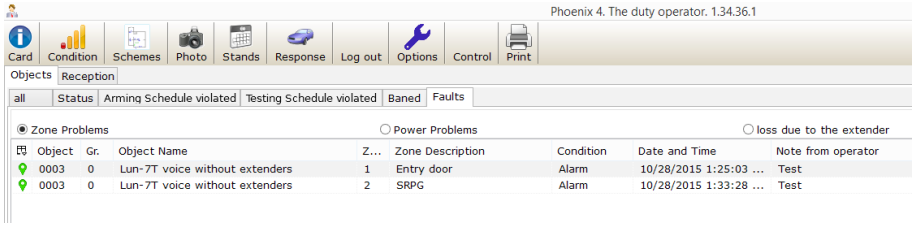


Operator can leave their own notes in these windows. To do this, right-click on the object and choose **Note: Operator** -> **Add Note**, then the following window will appear.



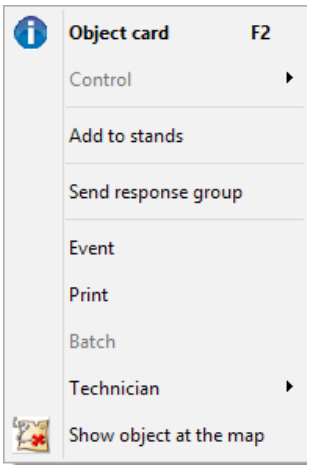
Operator can add a note regarding the trouble and the date to which this note is valid.

The trouble will be marked green if the note date has not expired, or red when the date is expired, and the operator must pay attention why this trouble has not been eliminated:

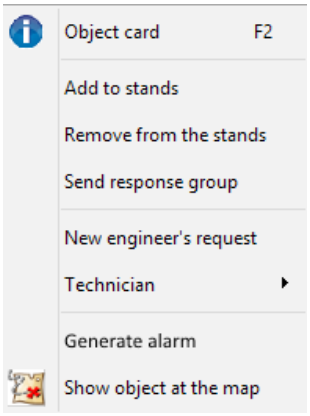


7.5. Context menu

All searches provide a context menu opened with the right button:



For the objects that do not contain any equipment, you can use another context menu item **Generate Alarm**, but **Control** menu item will be unavailable for them:

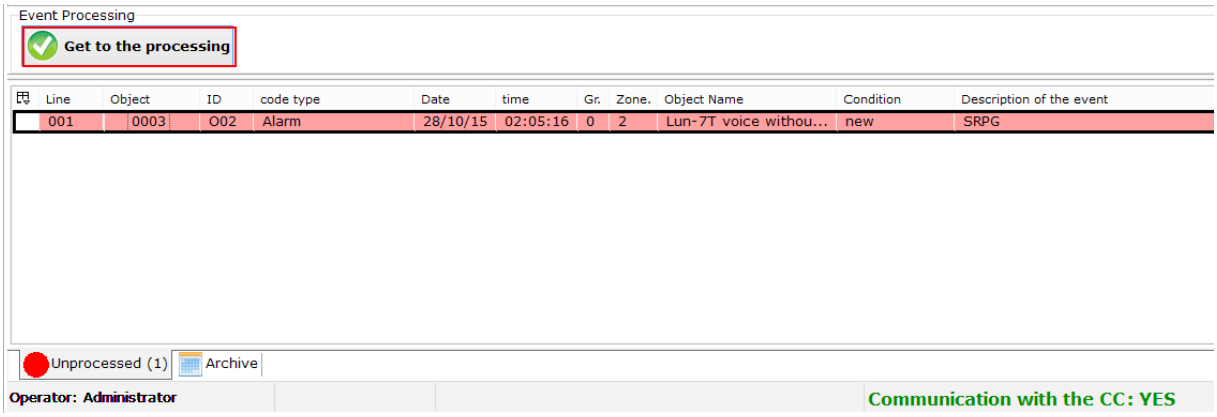


By clicking **Generate Alarm**, you will generate an artificial Zone 1 alarm.

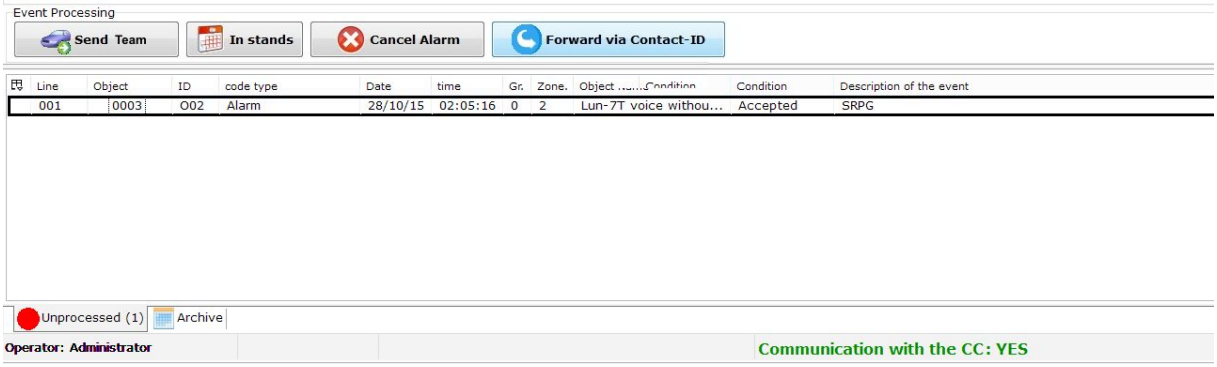
7.6. Event Processing by CMS Operator

As soon as a new event is received, it goes to the **Unprocessed** tab, and a siren is activated. If operator was in any other tab, within 30 seconds he will be automatically switched to the **Unprocessed** tab with activated **Get to the Processing** button. In the list below you will see the first unprocessed event, and in the top of the screen – the object's card will be displayed. In the event status column you will see **New**.

Show All option is used to display all unprocessed events intended for all computers (clients), not only for the current one. This option is directly related to the user settings of “Control Center” software.



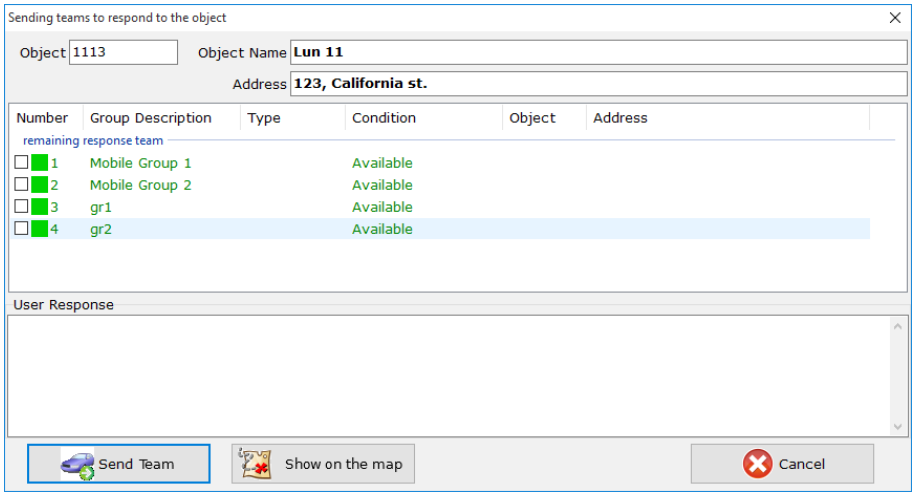
After clicking the **Get to the Processing** button, you will see the object's card, the siren will be turned off, event background will turn white and the available operations for events will be displayed: **Send Team**, **As Stands**, **Cancel Alarm**. Event status will change to **Accepted**.



The operator can forward this event to third party CMS software via ContactID by clicking the **Forward via ContactID** button.

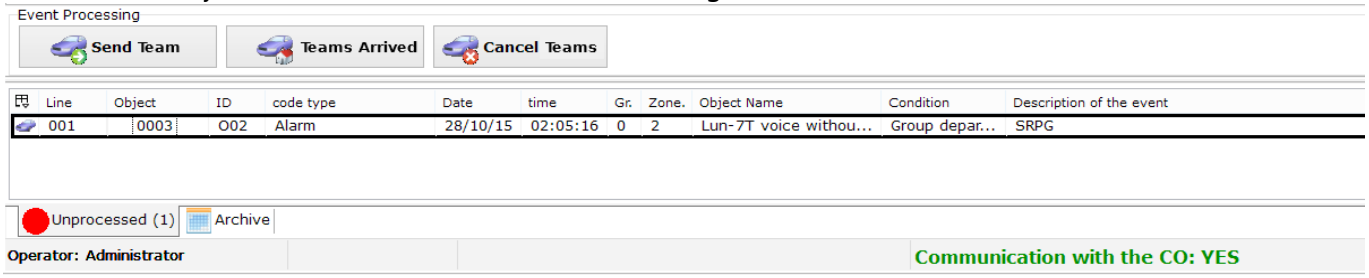
The operator can make the specified object's group as a stand by clicking **As Stand**, and cancels the alarm by clicking **Cancel Alarm**.

By clicking **Send Team**, the operator can send a Response Team to the object. In this case, you will see a window displaying information about the object, the list of teams and their status, as well as the operator’s response guide.

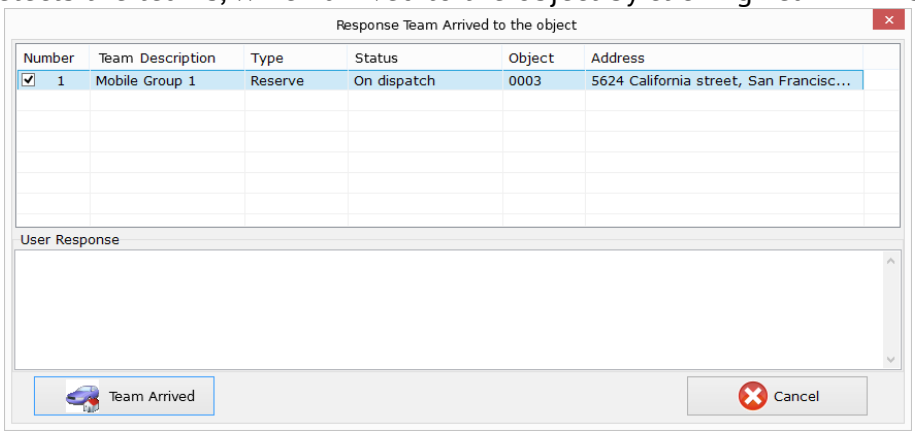


Operator can choose one or more teams to send to the object from the list of response teams.

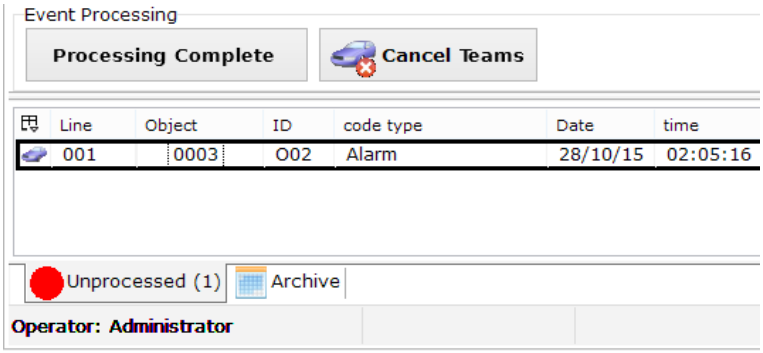
In order to immediately send a team, click **Send Team**. To show the alarmed object on the map, click **Show on the map**. Event status will be changed to **Team Sent**, and you will see the following options **Send Teams** – send another team to the object, **Teams Arrived** – to mark the teams that arrived to the object, **Cancel Teams** – to cancel sending teams.



Operator selects the teams, which arrived to the object by clicking **Team Arrived**.

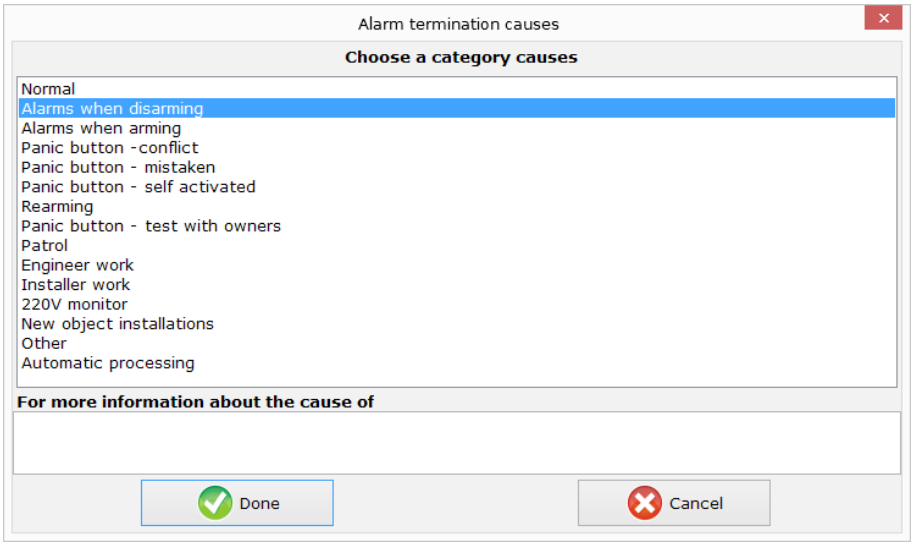


Event status will be changed to **Group at Object**. The available action – **Processing Complete** – processing completion and alarm reasons display, **Cancel Teams** – if one of the arrived teams needs to move to another location or return to the CMS.

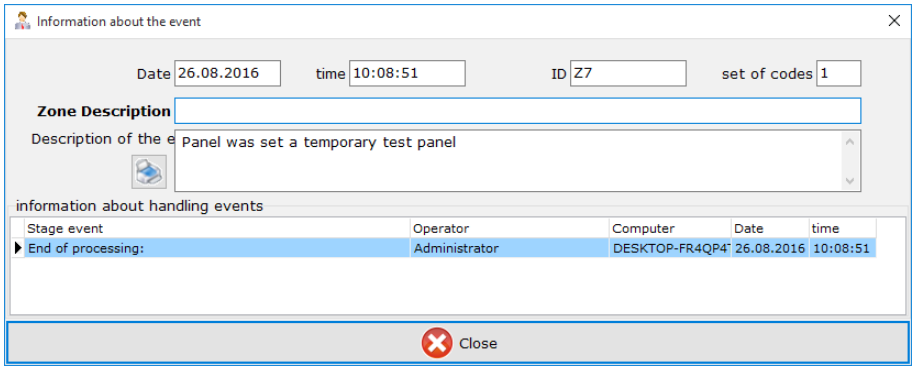


When the operator clicking **Processing Complete**, the alarm reason must be selected.

The list of alarm reasons can be edited in the **References** tab of "DB Administrator" software:



After clicking **Done**, the event state will be changed to "processed" and will be removed from the **Unprocessed** tab. The **Available** status will be assigned to all the teams sent to the object. In order to view information of event processing, you can right-click on an event in the **Unprocessed** or **Archive** tabs and select **Event** command.



If an alarm event was generated in the "Panic button" application, the button on the smartphone screen is pressed and locked. After the processing of this event is completed by the CMS operator, the Control Center software automatically sends the **Z50** "**Transfer of the tracker to normal mode**" request. The application will unlock and release the panic button on the smartphone screen by this request, so the user will be able to press it again.

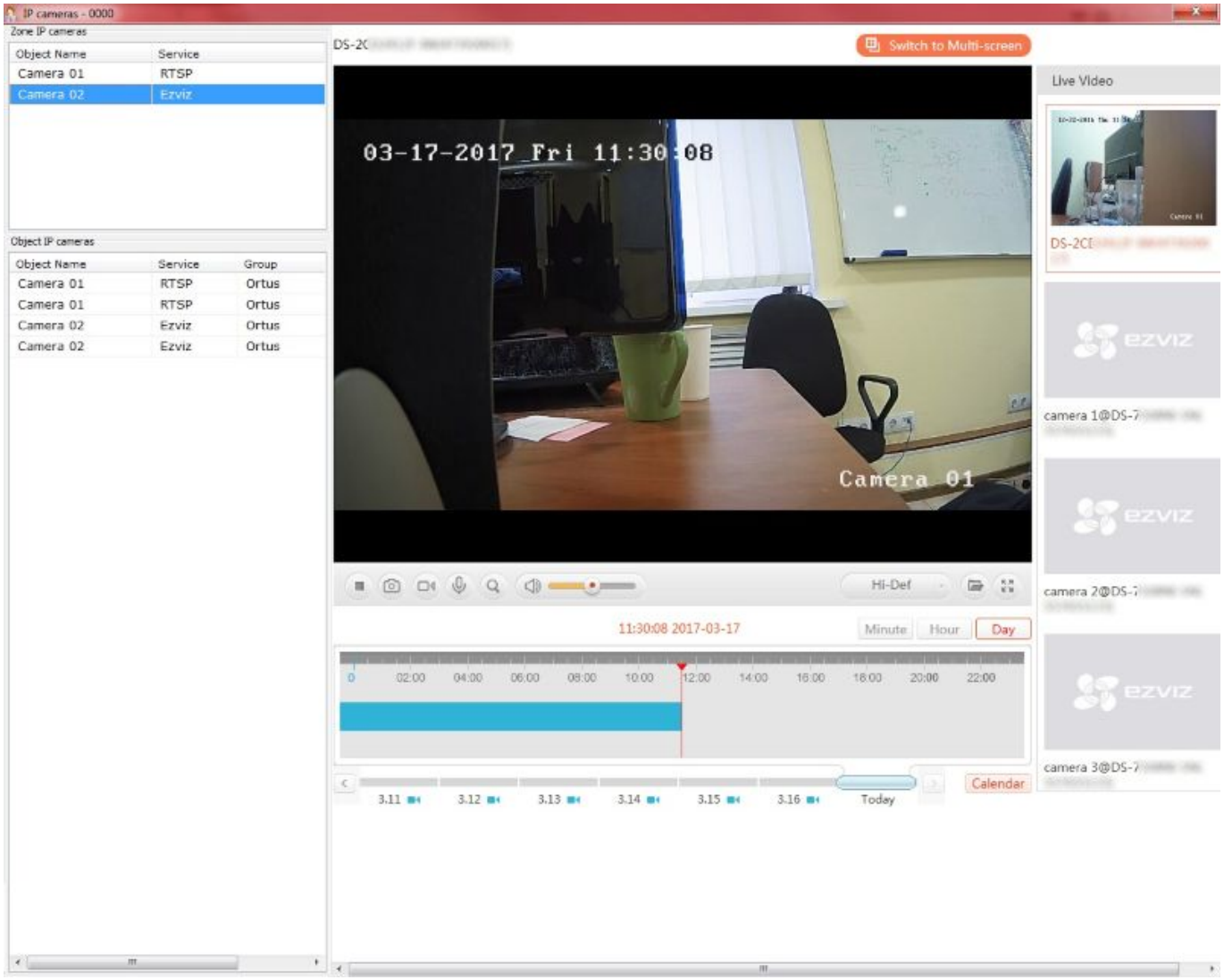
7.6.1. IP-cameras video view

If an IP-cameras are assigned to the Control Panel's zone, and an alarm occurs on this zone, operator can watch the video from the corresponding camera. The presence of an assigned IP-camera is displayed in the object card as a camera icon.

The camera is accessed from the context menu of the alarm event (it is called by right-clicking on the event), the "**Show video from IP cameras**" item.

If no IP-camera is attached to the current alarm event, a message about the absence of cameras will appear instead of the video.

Video from the IP-camera opens in a separate window, on the left side of which a list of IP-cameras of the object is displayed. The right part is occupied by the interface of the IP camera, which is determined by the used service:



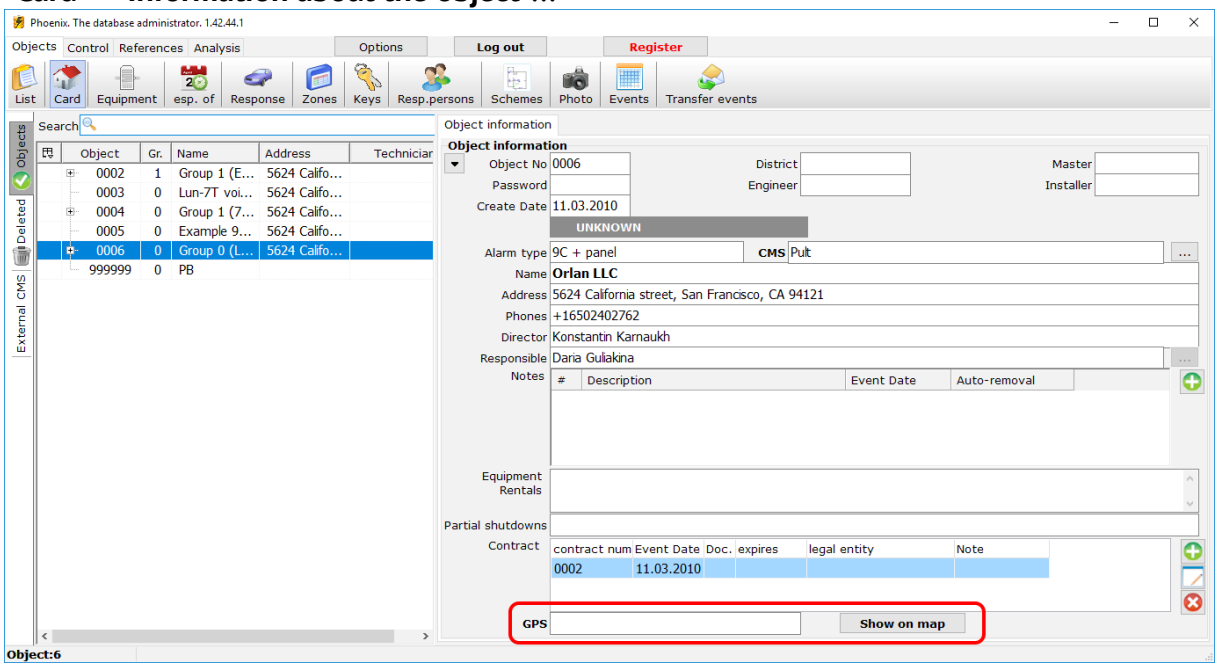
The assigning of IP-cameras to devices zones is described in Section 6.3.7. More information about the settings of IP-cameras can be found on the website http://hikvision.com.

The operator can save the viewed video or individual frames to a local disk. By default, the entry is made in the **Hicloud** folder of the current user. You can view the contents of this folder by pressing the button in the IP-camera interface.

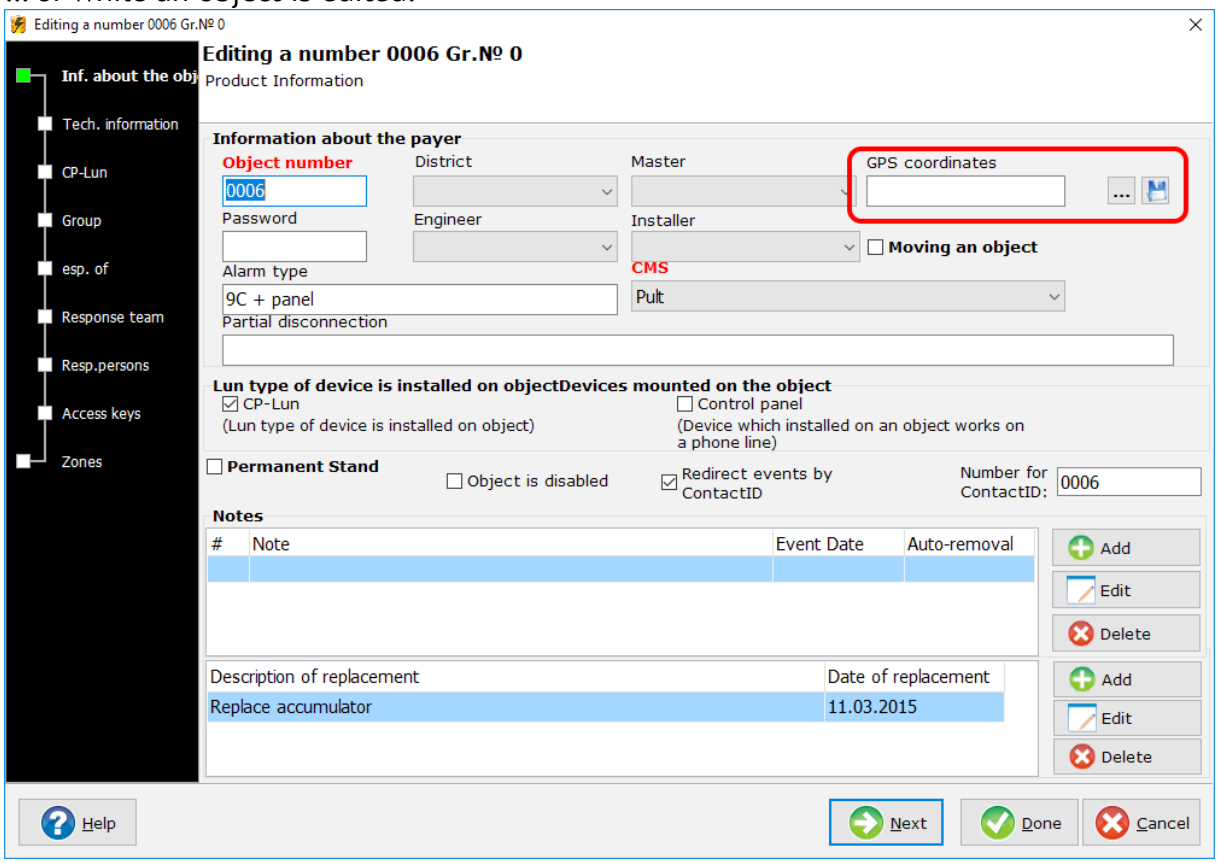
7.6.2. Show object on the map

If the "Phoenix-GPS" software is installed, then you can display the object on the map where the alarm occurred. This function works only for objects where the coordinates are set.

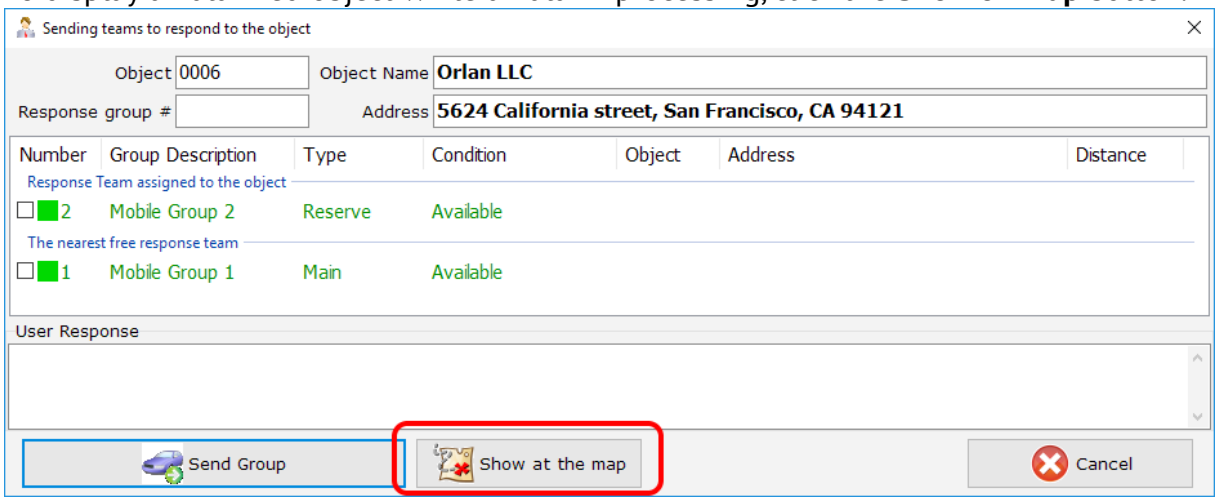
You must specify the coordinates in the “Database Administrator” software, on the “**Objects**” tab – “**Card**” – “**Information about the object**”...



... or while an object is edited:

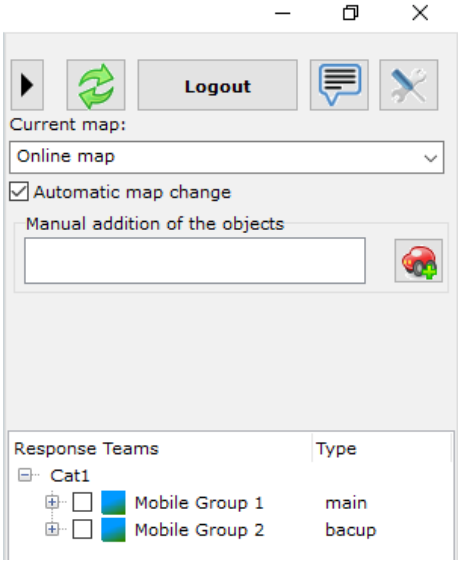


To display an alarmed object while an alarm processing, click the **Show on Map** button:



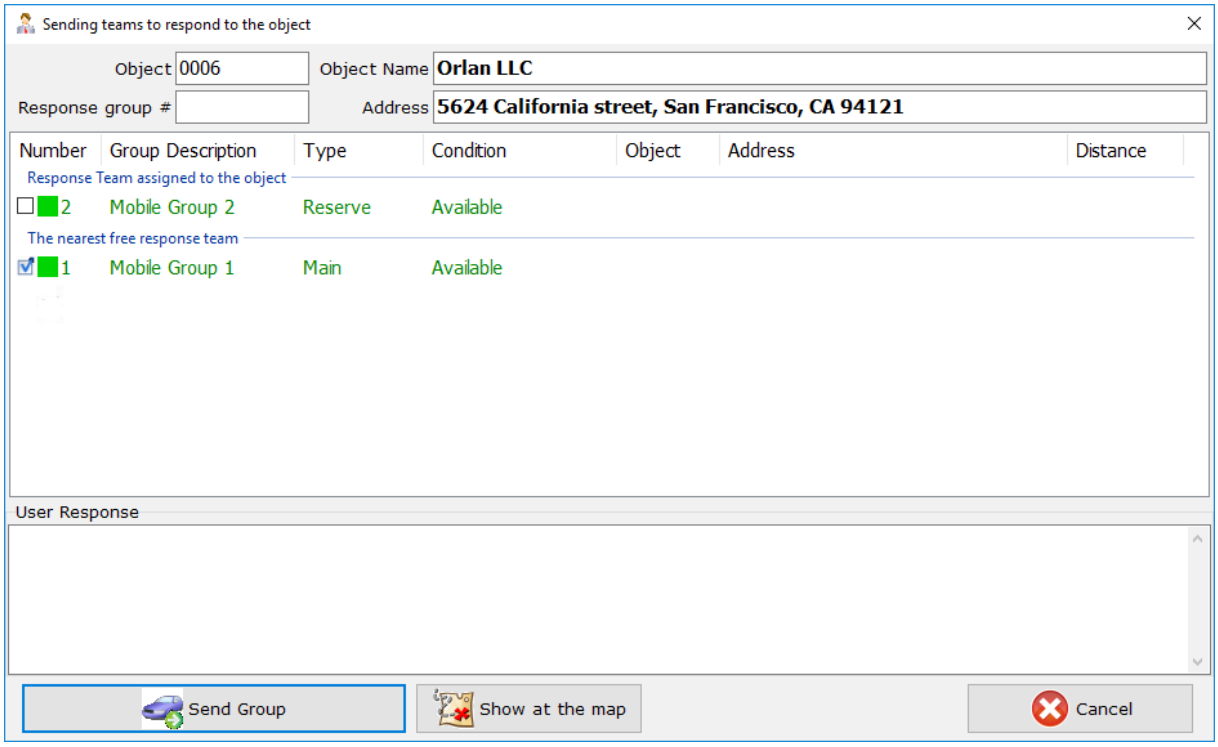
The "Phoenix-GPS" program window will open and the alarmed object (object number is 0004 in the screen-shot) shows on the map:

Then, select a free response group and mark it in the list of response groups:



Click "**Send response groups**" button.

Then the "Duty Operator" software window will open, the response group you selected before will be marked.



Click “**Send groups**” button, then the response group will be sent and the "Phoenix-GPS" confirm it by short message.

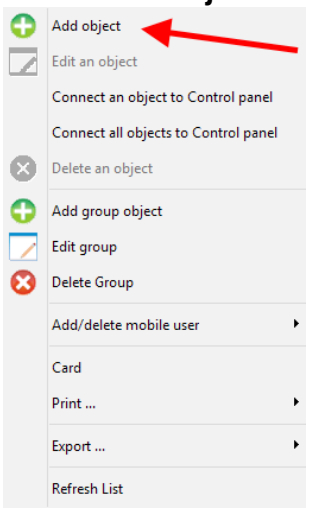
Further actions are doing as described in the Event Processing by CMS Operator Section.

8. Fixed object creation

8.1. Simple fixed object creation

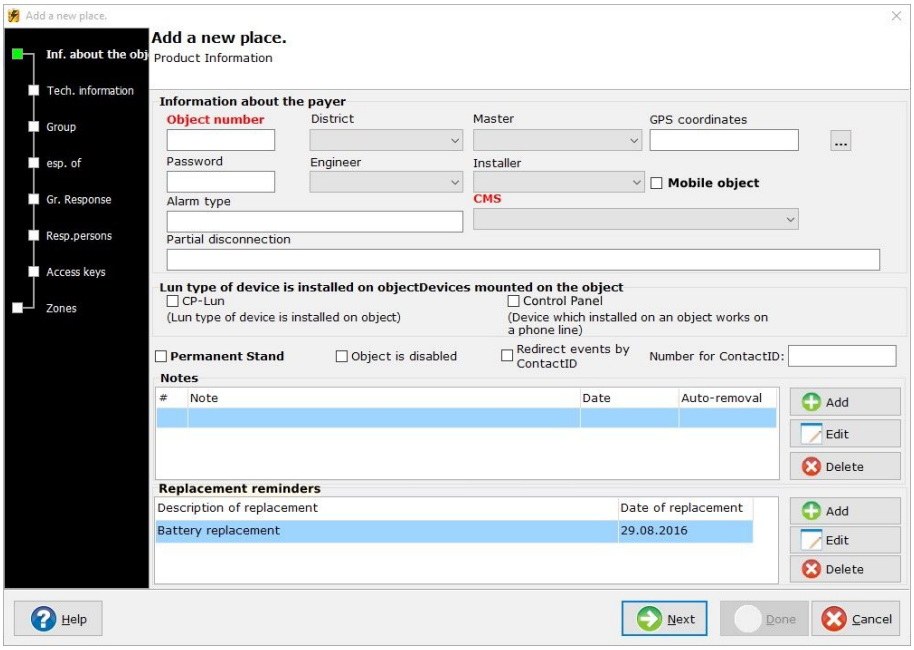
Fixed objects can be created using the "DB Administrator" software. You can run the program using the desktop icon or from the list of all programs in the "Start" menu.

You will see the main application window. Log in and click **Objects** -> **List**. Right-click the objects list to open the context menu, and select **Add object**:



You will see a wizard to create new object with several steps.

1. Object information.



Enter the payer's information:

Object # – select object number you are creating;

District – district where a new object will be placed;

Master – person (security service provider), representing the interests of the security company. As a rule, he is authorized to manage the service agreement;

Password – a secret word that the consumer must tell to CMS operator;

Engineer – service engineer, whom a particular object is assigned to;

Installer – person, who install Control Panel at the object;

Alarm type – brief description of alarm type installed at the object;

Partial Disconnection – this field describes all disabled features of the Control Panel (if this

features exists while a new object creating).

Mobile object – set if the object needs a fire monitoring. This option is used to cooperate with the firemen of "**Orlan-P**" CMS.

CMS – you must select one of the registered CMS assigned to the created object.

The next information describes the Control Panel installed at the object:

CP-Lun – set checkbox if a "Lun" Control Panel is installed at the object.

Control Panel – set checkbox if the Control Panel installed at the object uses the wired phone line.

Permanent Stand – set this checkbox, if the object you create will be as a stand.

Object is disabled – you need to check this box, if you want to disable the object.

Redirect events by ContactID – set this checkbox, if you want to transmit events via ContactID protocol to a third-party CMS software. If you select this option, you must also specify the following parameter.

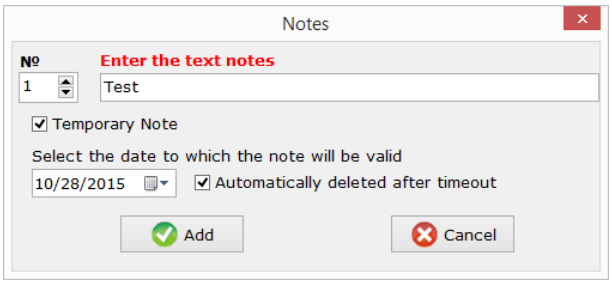
Number for ContactID – object number, this value will be transmitted to the third-party CMS software. In general, these numbers can be different.

Notes – this field contains additional information about the new object.

Replacement Reminders. In this field you can enter information about the spare parts replacements on the object (for example, battery replacement).

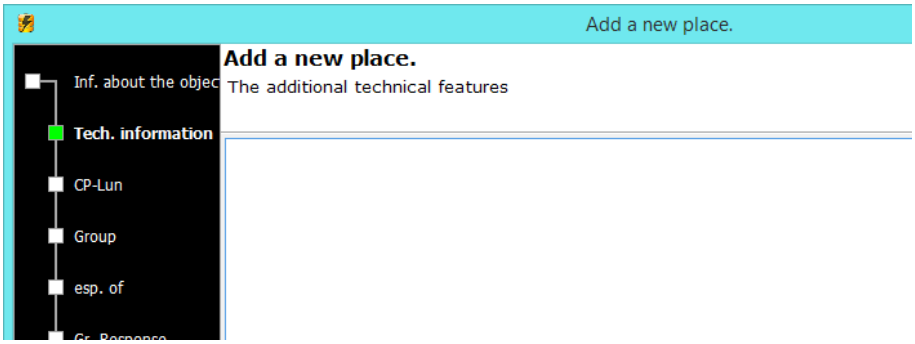
Notes and **Replacement Reminders** fields are filled and edited using the buttons located to the right.

Notes may be temporary (valid until a certain date), and can be automatically self-deleted after that date:



To continue, click **Next**.

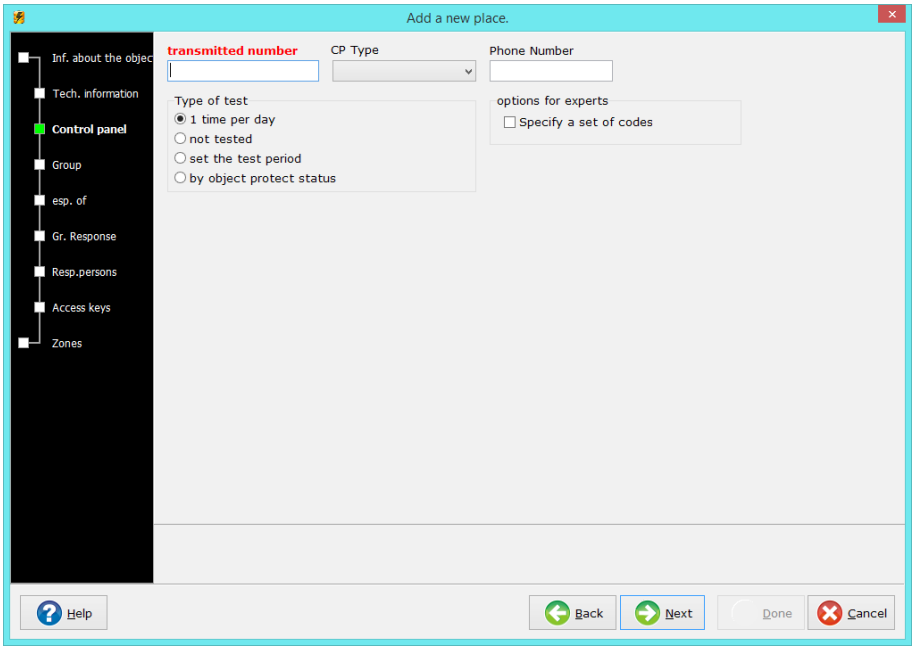
2. You will see the **Technical information** window:



Technical information window contains the information about the object's technical features.

To continue, click **Next**.

3. You will see the Control Panel window:



Transmitted Number – number of the object created, be use for object identification;

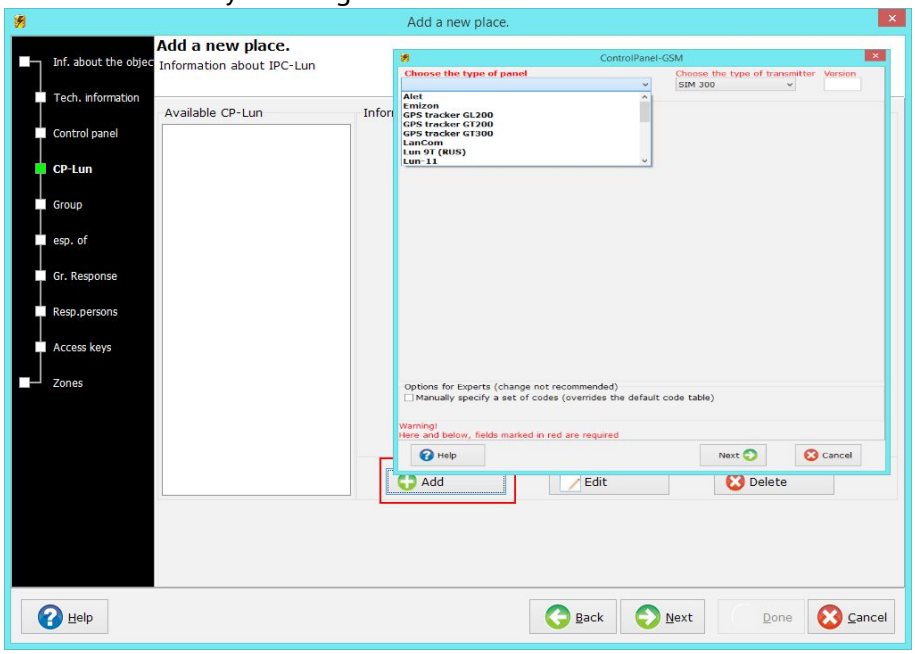
CP Type – type of device operating via a telephone line (PSTN number);

Phone Number – CP phone number;

Type of test – set the testing messages period from the Control Panel;

Specify a set of codes – this option is for experts only and uses for specify a non-standard codes set for events from Control Panel.

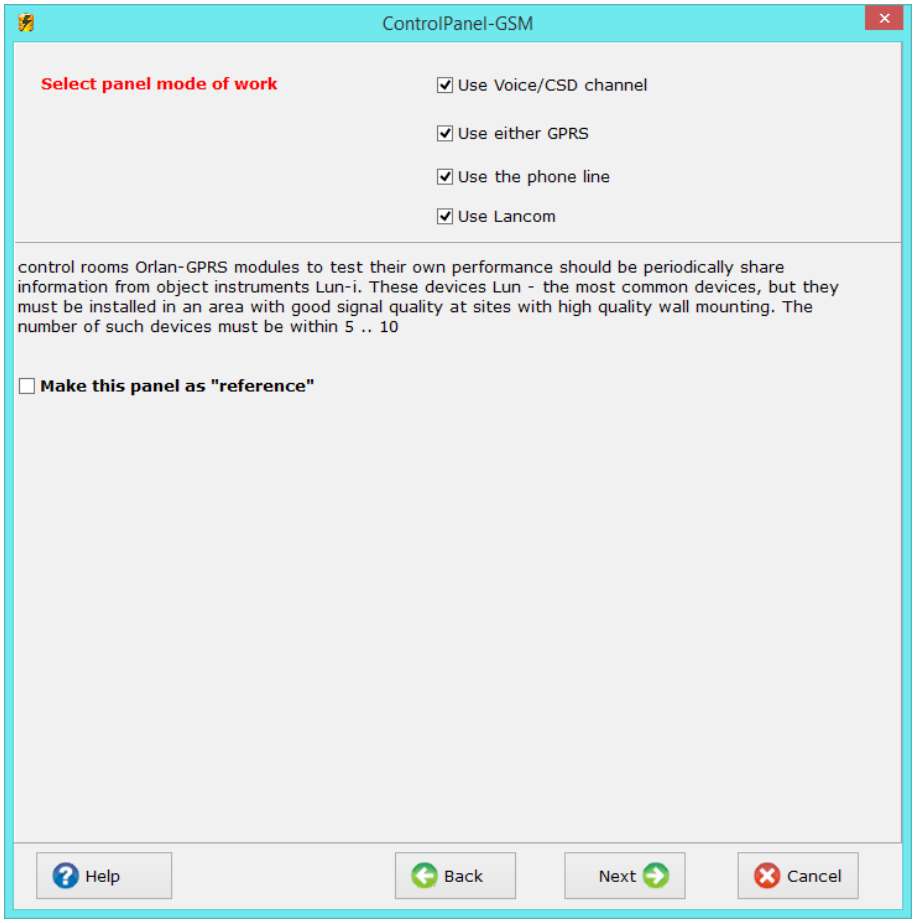
4. Then specify Lun Control Panel parameters. You can either select Lun Control Panel type from the list or create it by clicking **Add**:



You will see another master to create a **Lun** Control Panel.

In the first box select the Lun Control Panel type, its transmitter type and embedded software version value, then click **Next**.

In the next step specify the communicate channels to connect to the CMS:

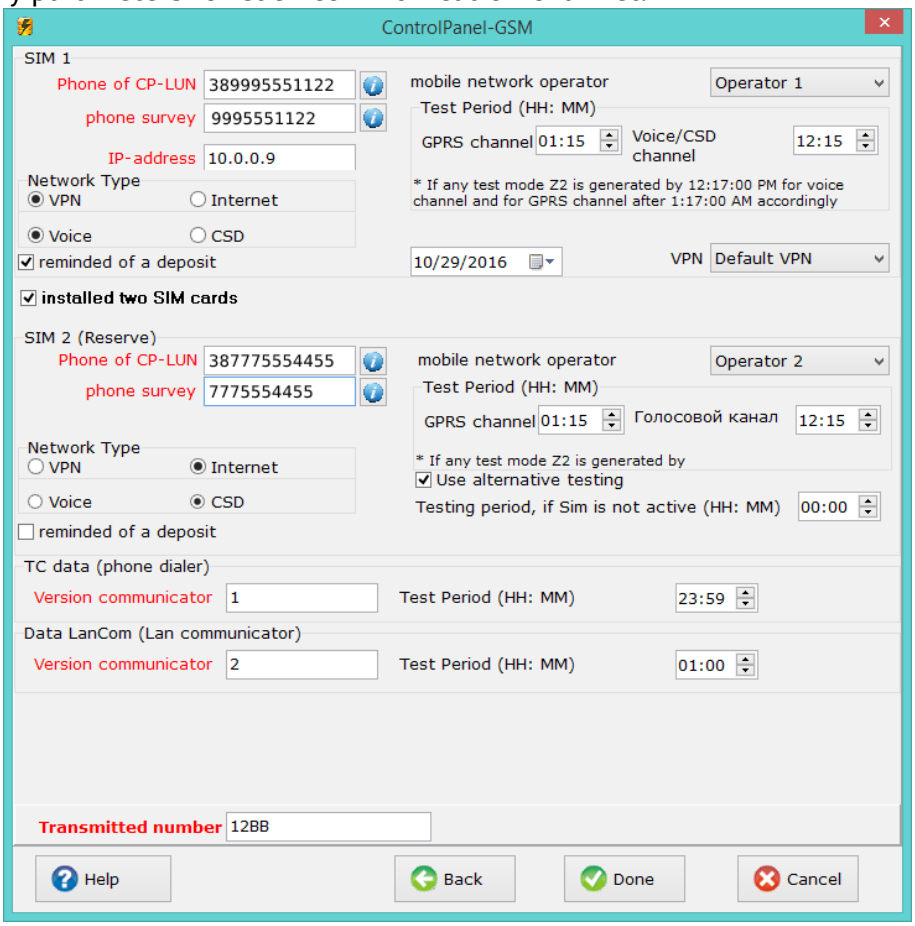


If you select GPRS/3G channel, it is possible to make the Control Panel as "**reference**".

"**Reference**" means that the Control Panel serves as a "gauge" for "Orlan-GPRS" modules – every "Orlan-GPRS" module periodically try to connect with the reference Control Panel. If this connection is not established then it's mean the "Orlan-GPRS" module need to restart, so Phoenix-4 software will restart this module then reconnect it.

Attention! The more Control Panels make as references ones, the less false restarts of "Orlan-GPRS" modules will be made and, correspondingly, the higher the system fault-tolerance will be. We recommend 5 to 10 Control Panels make as "reference". This Control Panels should be the devices with the best operating conditions, such as consistently high signal level, stable power supply, and reliable cable installation.

Then specify parameters for each communication channel:



SIM 1 parameters.

Phone of CP Lun – Control Panel's SIM1 phone number in the international format (without "+" sign).

Phone survey – the same phone number, but in the dialing format.

IP address – it displayed in case of "**VPN**" mode in GPRS/3G-network. In case of "**Internet**" mode, you must specify "**Transmitted Number**" instead of this parameter.

Network Type – select network to operate via GPRS: **VPN** or **Internet**.

Test Period for GPRS and voice channels – time interval for testing messages from Control Panel; the appropriate parameters shall be set when configuring the device.

SIM2 parameters.

This parameters need be set if the SIM2 (as reserved card) is used.

Use alternative testing – this parameter is used for Lun-11 Control Panel based objects only. It switch testing messaging algorithm creation in accordance to Control Panel settings. More details see in the Lun-11 Control Panel Operation Manual.

TC Data (phone dialer) parameters.

Set the Phone Communicator embedded **software version, testing period** and **transmitted number** (its field placed at the bottom of the window).

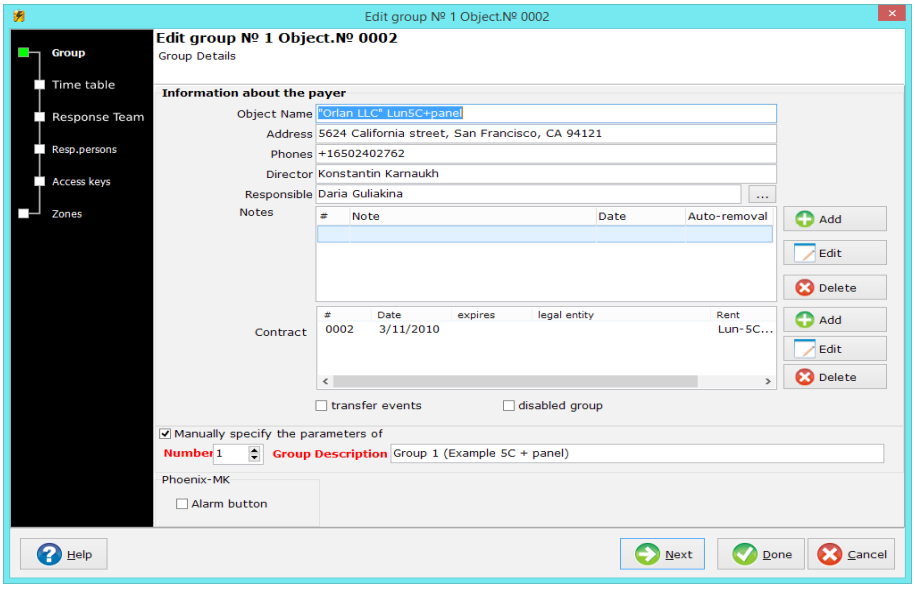
LanCom Communicator Data parameters.

Set the LanCom (Ethernet-communicator) embedded **software version, testing period** and **transmitted number** (its field placed at the bottom of the window).

Attention! You can't use Internet mode (by SIM or LanCom) and Phone Communicator for Lun-73T simultaniously.

Transmitted Number – used for Control Panel identification by LanCom (Ethernet Communicator), TK-17 (Phone Communicator), GPRS (on SIM-card) via Internet mode.

Group window:



Group shall contain all the necessary payer's information; make sure you filled in all the fields.

If you want to configure e-mail messages in case of activation, set the appropriate option in the **Transfer Events**, and a **Send Messages** step will be added to the wizard. See below.

Another important option is **Disabled Group**. If set, all alarm events will be transferred to non-alarmed, i.e., will be archived without processing.

Alarm Button specify the "**mobile alarm button**" be used in "Phoenix-MK" mobile application. When you click this button, the application will receive an "alarm button" alarm from this particular group. For more details, please, see "Phoenix-MK" manual.

Connected to Lun CP checkbox is available only for the objects where "Lun-7T" CP installed. After you set this checkbox, you must also select the extender type (Lun-5A, Lun-5N, Lun-7N) for this group.

In the **Time Table** window you should set the object's operation schedule.

In this window you must select one of the following types of operation:

- individual schedule (typical for offices or shops);
- 24-hours protection (for example, ATMs, substations of communication providers);
- free schedule (private homes, cottages, apartments);
- no arming and disarming (alarm buttons at box offices);

- unknown (possible to specify in the future).

In addition to the type of operation, you can specify the additional options:

Waiting for a call from object after disarming – after this time interval, the device will generate an event for the operator: "**Check for a call from the object**"

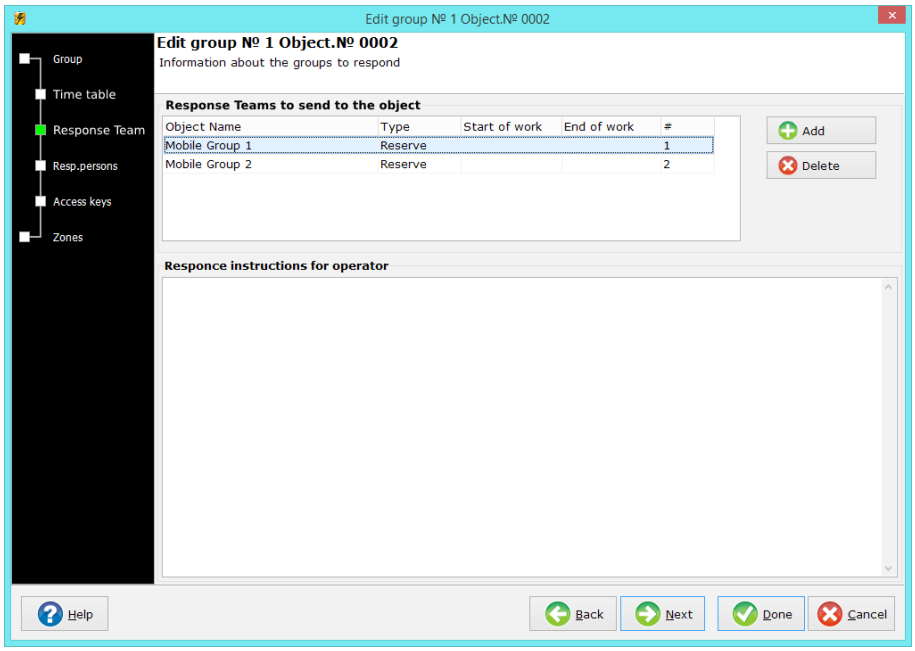
Obligatory call to object in case a Schedule violation – objects with this option set go to a special list "**To be Called**" of the "**Arming Schedule violated**" tab of "Duty Operator" software.

Control disarming on Schedule – when this option is set, operator will receive alarms upon opening (disarming) of the object. Otherwise, usual events will be archived at once.

Armed 24-hour objects (this option is available only for full-time armed objects) – after the specified time interval, Phoenix-4 software will generate a reminder.

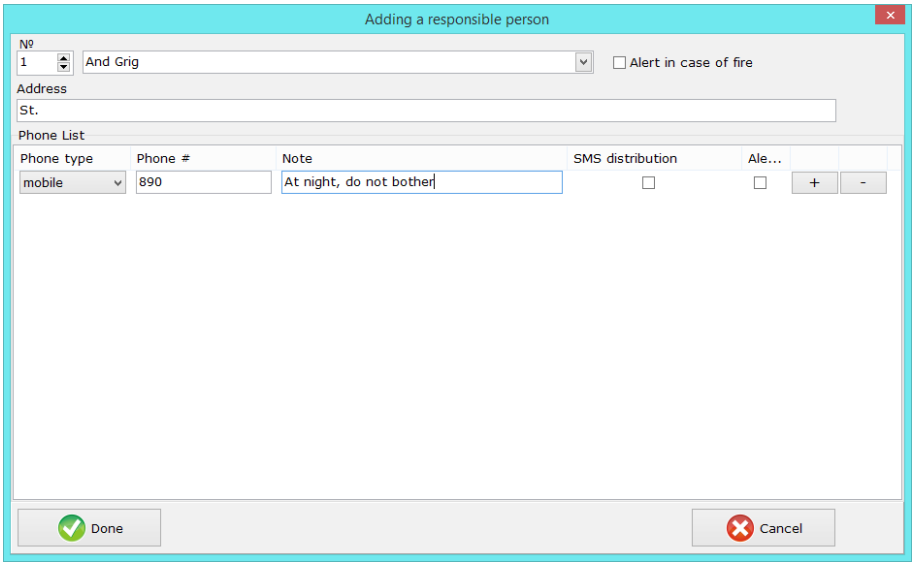
Attention! Automatic Arm/Disarm group according to schedule option allows to arm and disarm objects according to the specified schedule. This option is available for "Lun-11" Control Panel only.

Response Team window:



In the **Response Team** window you must select a team that visit the object if necessary. In the **Response Instructions for operator** field you should specify the additional information about the CMS operator's actions in case of alarm activated.

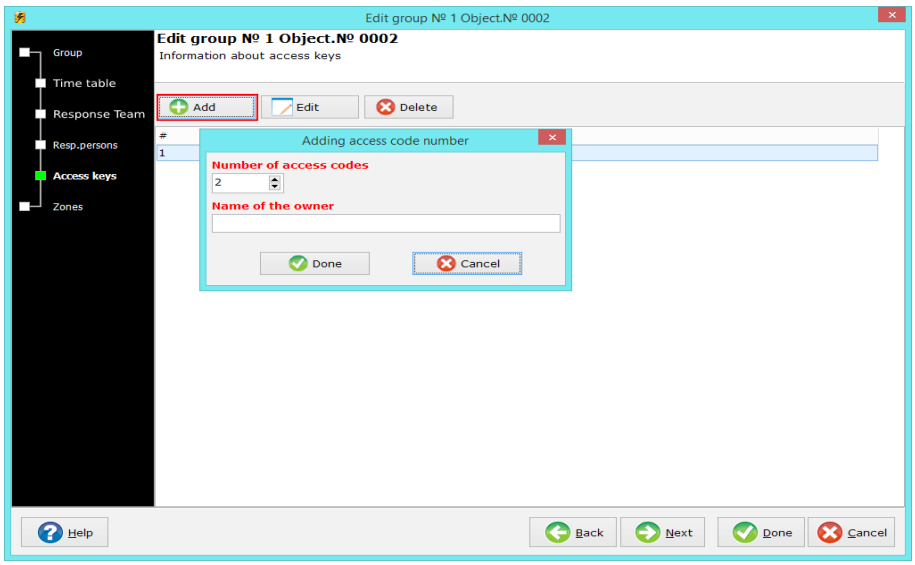
Responsible Persons window:



In the **Responsible Persons** window you must specify the information about responsible persons using the **Add** button:

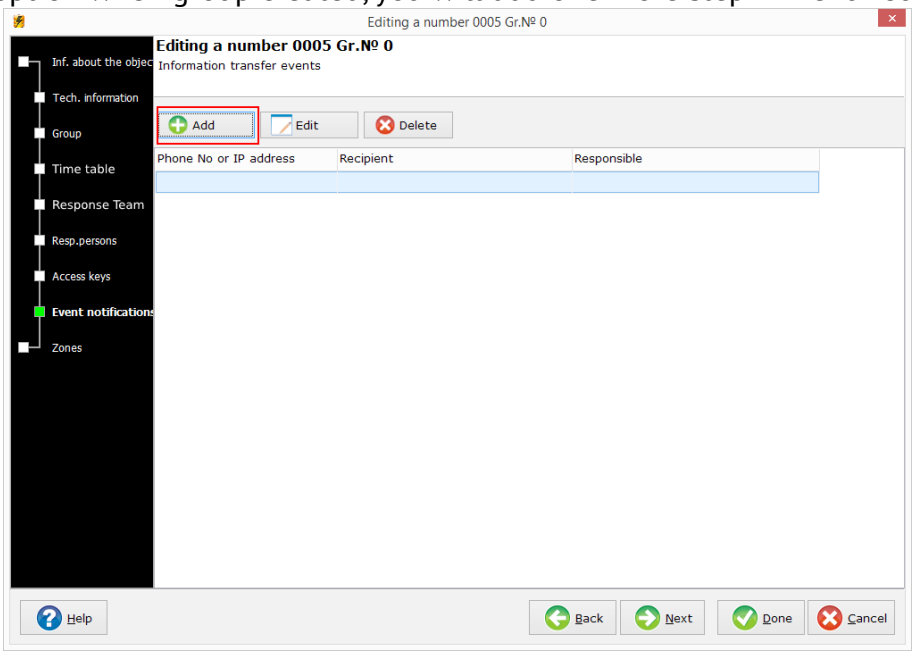
- phone type;
- phone number;
- text notes.

Access Keys window:



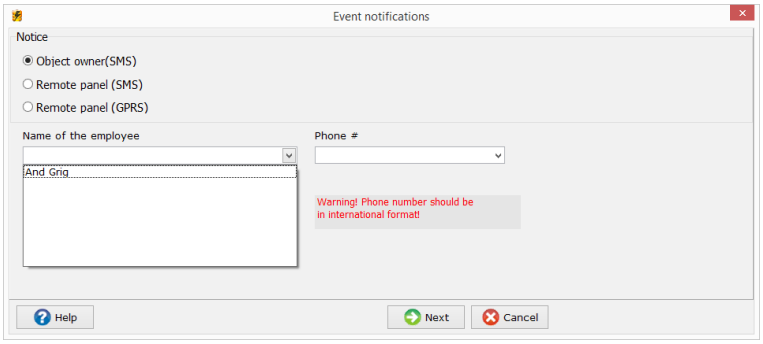
In the **Access Keys** window you must enter the access codes using the **Add** button.

In the window that opens, enter the access code number and the owner's data. If you set the **Transfer events** option when group created, you will add one more step – **Event notifications**.



In this window you can see a list of event recipients. You can **add**, **change** or **delete** recipients with the menu buttons.

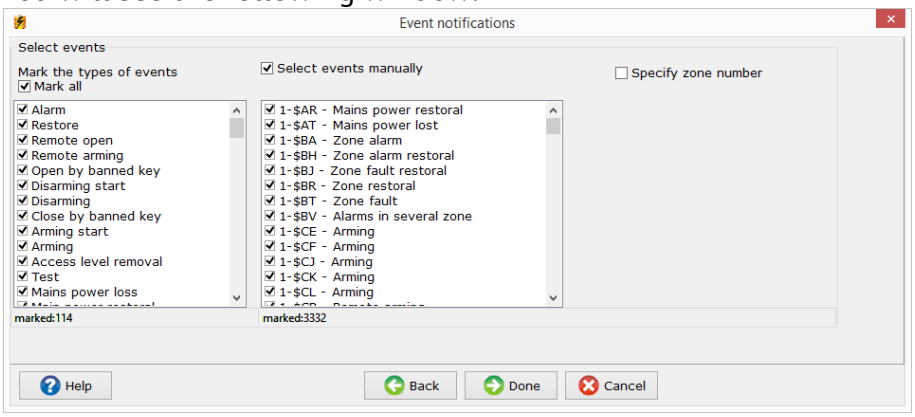
Click **Add** if you want to add an event recipient. You will then see the following window:



Notice – specify persons to be notified.

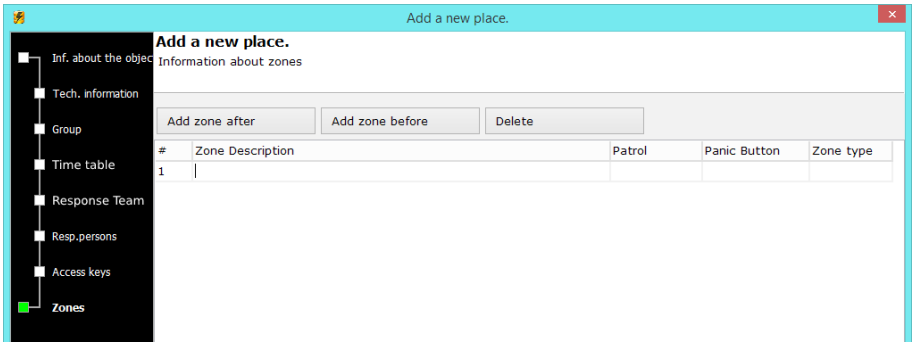
Enter the phone number to send the message to. When entering of numbers, the device automatically searches from the existing numbers. If the number is not on the list, you can create it by clicking "**New Number/IP address**".

Click **Next**. You will see the following window:



In the left list select the events type set to be sent. In the right list you can select the specific events to be sent.

Zones window:



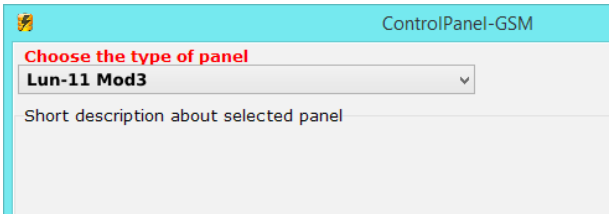
In **Zones** window you must add zone's descriptions. If a zone is an "**Alarm Button**" or a "**Patrol**" sensor, you need to set the appropriate option.

"**Patrol**" – 24-hour zone used to control the arrivals of teams to the object. It is a sensor of "reed" type installed, for example, in the door box. A response team presses a magnet to the "patrol" sensor, and as a result, CMS receives a "patrol event" message, thereby confirming that the response team arrived to the object.

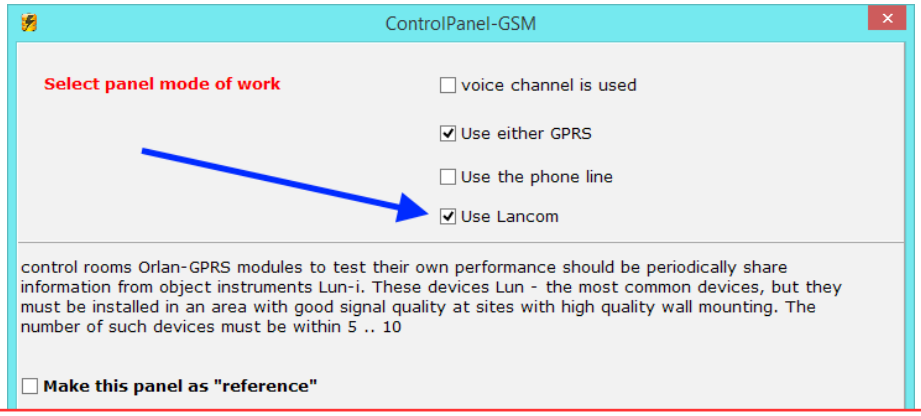
8.2. Fixed object with Ethernet Communicator creation

8.2.1. Lun Control Panel with LanCom as Communicator

You must create the new object based on the selected Control Panel (Lun-7T, Lun-11).



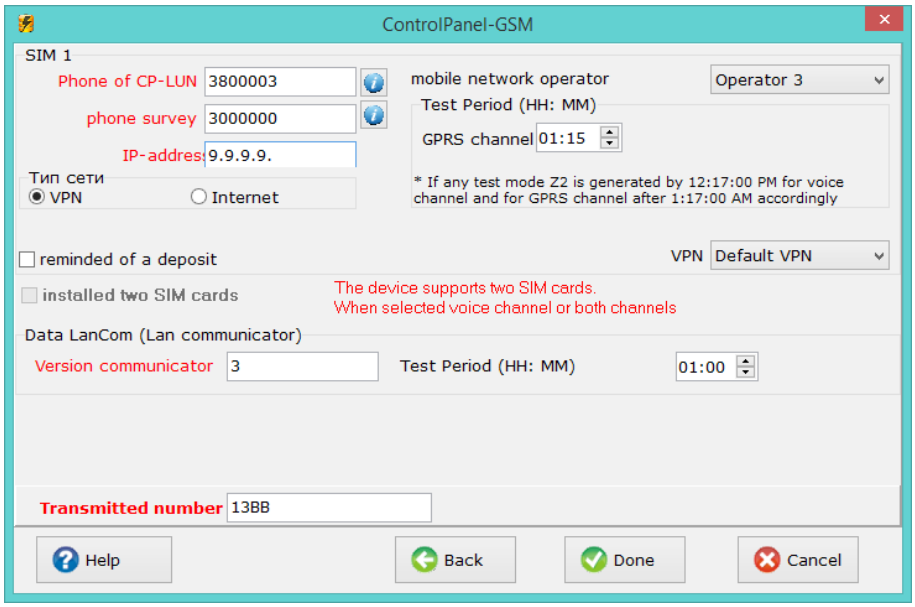
The first steps for object creation are the same to simple fixed object creation. The differences begins from the **Lun-CP** window:



Attention! When a LanCom device used, you mustn't use the Internet mode via GPRS channel, only VPN is allowed.

Click **Next**.

Fill all the necessary fields. Pay attention to the **Transmitted Number** field; this number used for events via LanCom identification.

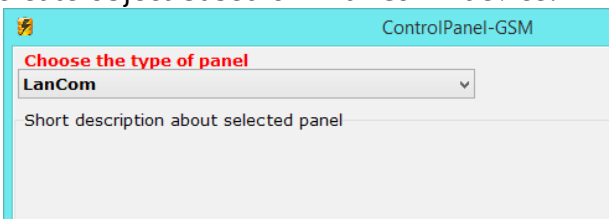


Click **Done**.

Attention! If you connect LanCom Communicator to "Lun-73T", you must create group "0" (the Control Panel main group) and group "30" (use the “Manually Specify Group Parameters” option) – this group will transmit events from the communicator.

8.2.2. LanCom as Control Panel

In this case you must create object based on «LanCom» device:



Fill in all required fields and click Finish. Pay attention to the **Transmitted Number** field; this number used for events via LanCom identification.

9. Software Update

Attention! It is recommended to update the software from time to time (if any new version is available at the web-site). The update is available at Ortus website: www.ortus.io, as well as on the supplied CD (current version). "Orlan" CMS software has three main programs:

"Duty Operator" (Ph4Operator.exe) – a program which receives and processes events from the objects. With this program operators can remotely control the object Control Panels.

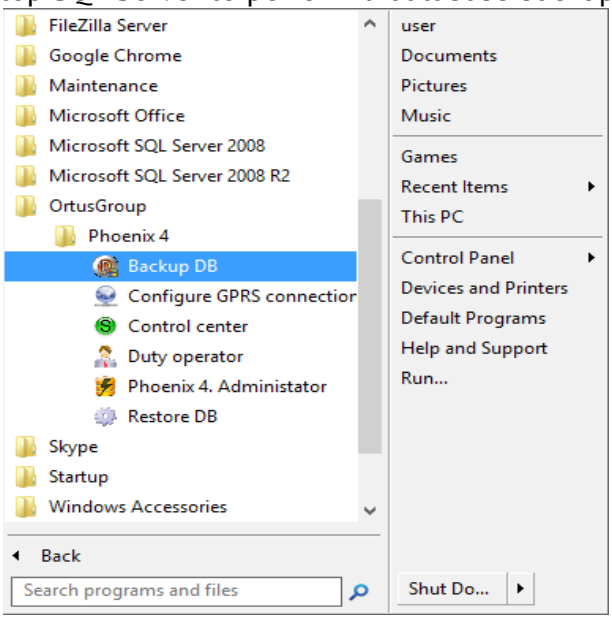
"DB Administrator" (Phoenix4.exe) – a program to create and edit the CMS database.

"Control Center" (ControlCenter.exe) – driver of all CMS receivers, as well as a processing centre for all CMS commands.

Update procedure:

1. **Be sure to make a backup copy of the database, it is important!**

Use the "**Backup DB**" from the main program menu. Select the "**Make copy right now**". In this case, it is not necessary to stop SQL Server to perform a database backup.



2. **Make sure to create a backup copy of "Phoenix 4", it is important!**

Default folder – **C:\Program Files\OrtusGroup\Phoenix4**.

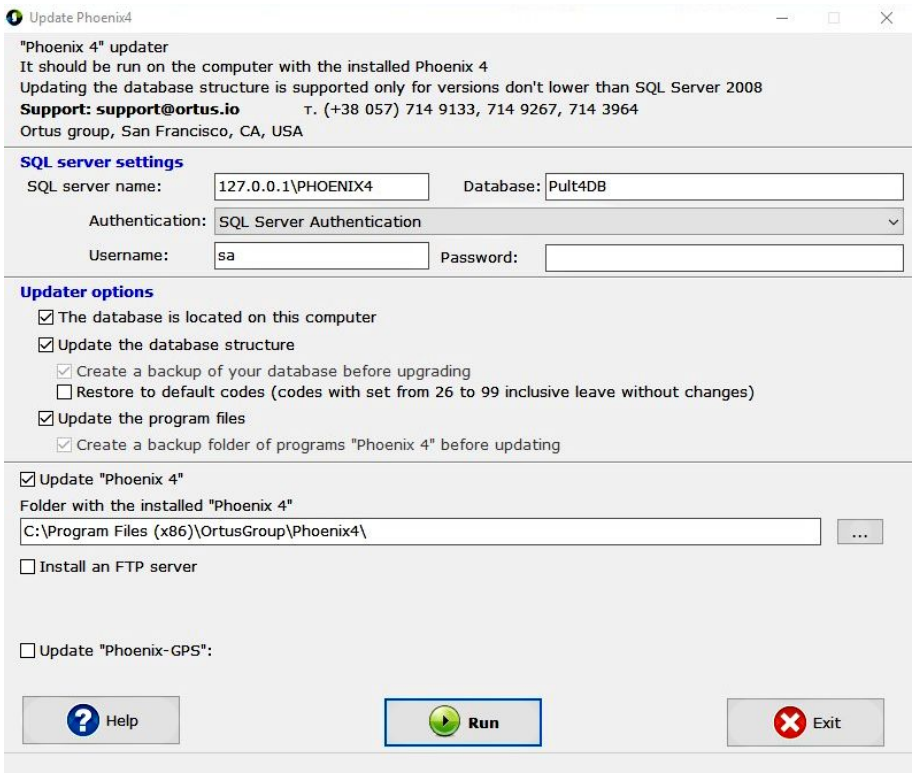
Note. Backup copies of the database and folders can be created independently by "Updater" program.

3. When necessary, update HASP protection driver. The update is available at http://ortus.io
4. Unzip and Run the "**Updater**" program.

Do not run this program from the archive – it leads to incorrect operation.

Remember! After the update is complete, it will be impossible to return to the previous version if you do not perform steps 1 and 2.

Attention! "Updater" must be installed on the local computer with SQL-server and CMS database installed.

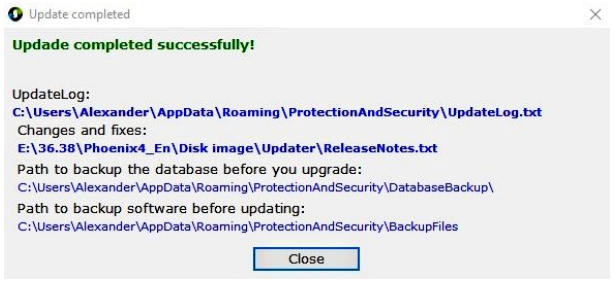


"Updater" does the following:

- Changes the database structure;
- Records new codes;
- Replaces program files with new versions (overwriting the previous);
- Sets FTP-server, if checked;
- Updates Phoenix-GPS software, if this option is set;
- Restores the original code, if this option is set.

Attention! Information about the objects is not changed!

The program always creates a new backup of all databases (objects, archives, tracks) before updating. If there is not enough space on a disk, the earliest copy will be erased. The path to the backups will be listed in the summary window at the end of update.



Attention! If the Phoenix-4 software installed on the some computers, you must update it all , so that software and the remote database versions matched.

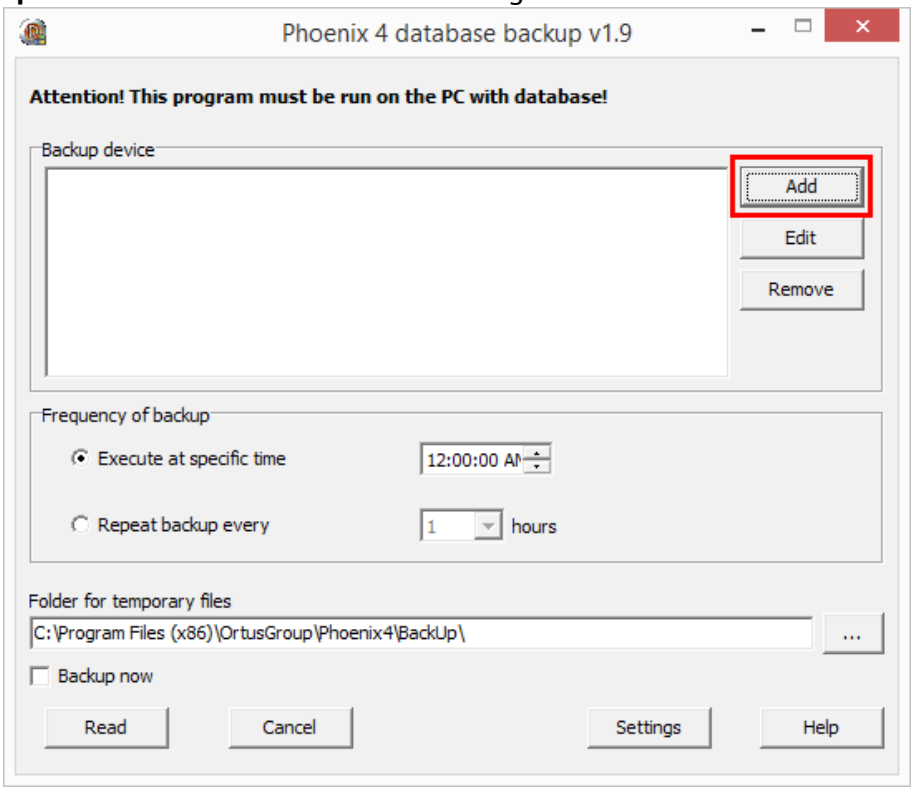
Attention! If the new version does not run, does not work or malfunctions, you should downgrade to the previous version.

10. Automatic Backup

Database backup algorithm consists of two steps. During the first step, a database backup is created, while during the second step it is copied. This process is automated, and you need to specify how often the database should be copied and where.

Attention! To backup the database using "Backup DB", you will not need to stop SQL-server.

To configure automatic DB backup and copy, you must use "**Programs**–**OrtusGroup**–**Phoenix 4**–**Backup DB**". You will then see the following window:



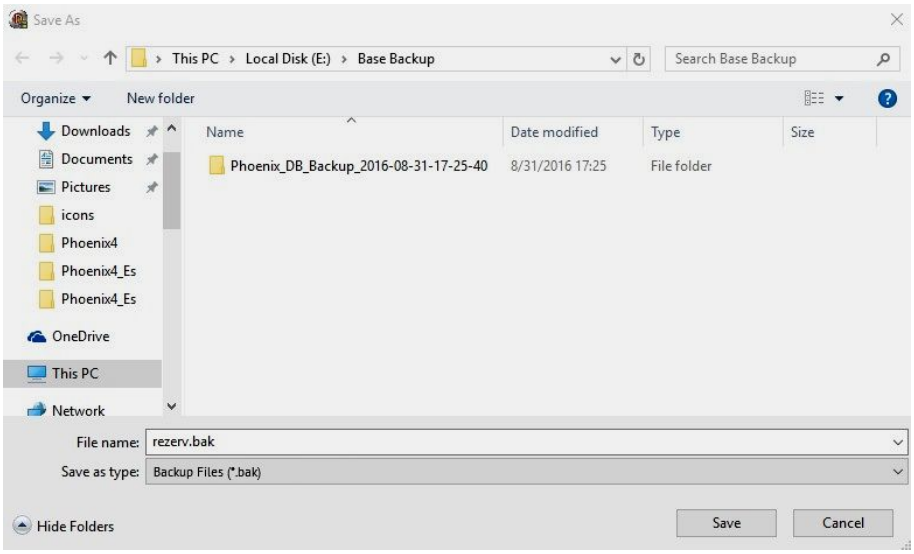
In this window, you must select how often database copy shall be created. It can be done either at the specified time every day or periodically at the specified time interval. In addition, there is an option to back up the database manually at the time of configuration, by selecting of the "**Back Up Now**" option.

"**Temporary Files**" folder sets the path when the database will temporarily store while backup process. In case of multiple users on a single workstation, it is necessary to grant full access to all users.

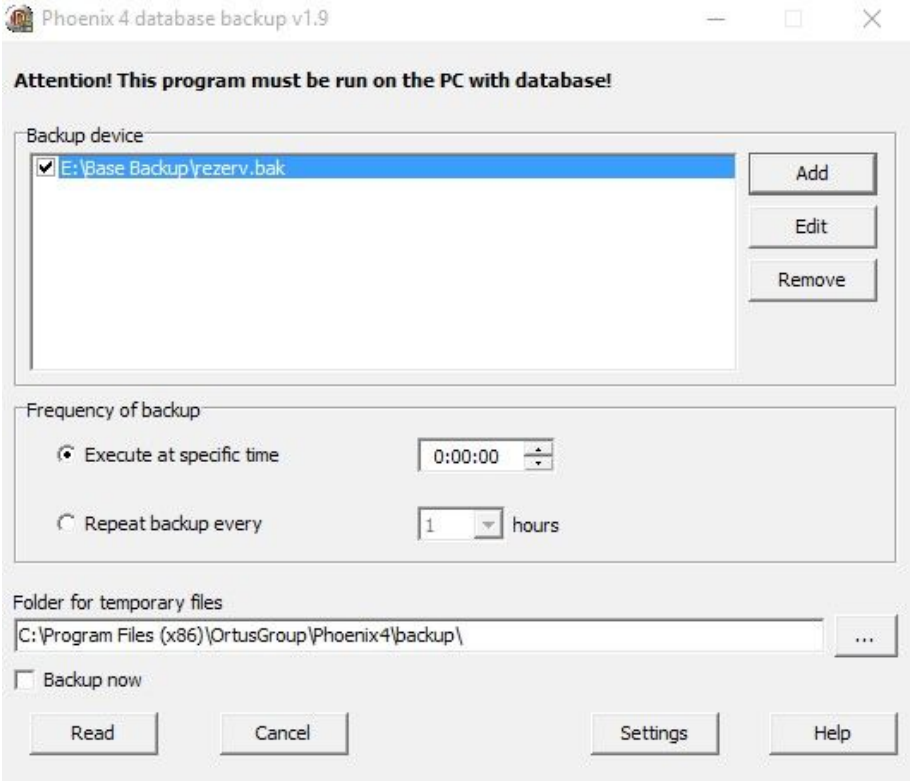
Attention! If access to this folder is granted only to one user in multiple user computer, creating of backup in the automatic mode is not possible.

You can copy the database to any media connected to computer (CD, DVD, removable hard disk, flash memory card) with memory enough. In addition, you can back up the database on a network drive.

Select where you would like to copy the database by clicking **Add**.



In this window, select the location and file name as mask “XXXXXX.bak", where "XXXXXX" is the file name you choose. (for example, *rezerv.bak* or *03_11_08.bak*). Click **Save**.



You will return to previous window, where a new record with the selected path to keep the database will show. Mark this record with a checkbox, and select the frequency of backups. Activate the **Back Up Now** option and click **OK**.

After the backup is completed, you will see a message notification and a new backup file will be created. This file will be updated according to a schedule that you choose.

Settings button is used to specify of SQL-server access parameters and is intended for system administrators only. It uses in cases when SQL-server is installed on separate computer or if a named instance of the server is installed.

11. Downgrade to previous version

1. Database Recovery

If you make a backup using "**Backup DB**", database recovery is performed using the "**Restore DB**" program. You can don't stop SQL-server.

2. Recovery section.

Restore Phoenix folder copied before the update procedure. To do this:

Close "Duty Operator", "DB Administrator" and "Control Center" programs;

Copy the whole folder back.

3. Run the software.

"**Updater**" makes a backup copy of the database and all program files before updating the software. If the update is unsuccessful or you just want to restore a previous version, you can find database backup at the location indicated by "**Updater**" program after the update or update failure.

In case of update failure, database is not upgraded, and you can try to run the program. If you see "**Application is not compatible with database**" error, you can copy the files from the backup file according to the path, where "Phoenix 4" software installed

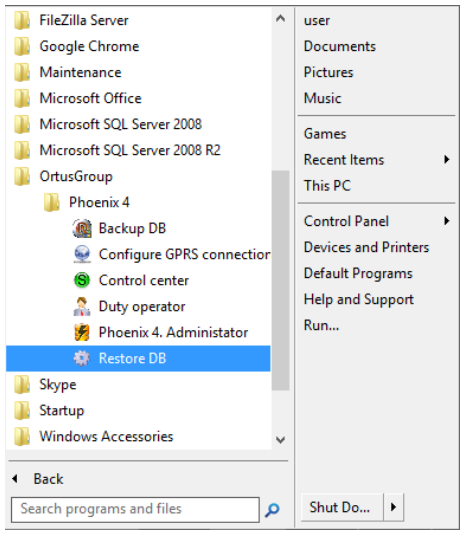
(default path: **C:\Program Files\Ortus Group\Phoenix4**).

12. Database Recovery

To restore CMS database, you should use the "**Restore Database**" program installed automatically when you install "Phoenix-4".

Attention! You can don't stop the SQL-Server while restore the database by "Restore Database" program.

Run the program from the "**Start**" menu.



You will see "**Database Recovery**" window, where you must specify the path to the database backups and the path where you want to restore the database by clicking the "**Browse**" button.

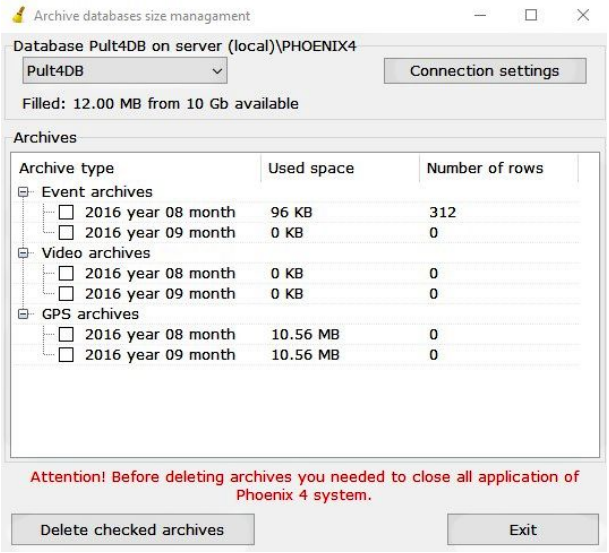
You can also specify the path to the database file storage (this is an optional parameter) (default path: **C:\Program Files\Microsoft SQL Server\MSSQL\Data**).

To change connection settings for SQL-Server database, click "**Connection Settings**" and specify connection parameters – server name, authentication method, login and password. It is recommended to leave the default settings.

Click "**Restore**" to start the recovery process. After the process completed, you will see a notification message.

Attention! Recovery may take a long time (depends of database size), do not interrupt the program running during the recovery!

13. Uninstalling of Archive Data



This program is used to clear the database from files that, for one reason or another, are unnecessary. This can ensure free space for new archives in the database. Depending on the database version of Microsoft SQL Server, the maximum database size can vary between 2GB and up to the total volume of the hard disk. The program displays the filled and available space and shows the size of each file. The drop-down list of databases is required for an overall assessment of the database capacity and size.

14. Appendix 1. Binary code for address selection

Table 2. Binary code for address selection

Address	DIP-switches settings (1=ON; 0=OFF) 				
	1	**2**	**3**	**4**	**5**
1	1	0	0	0	0
2	0	1	0	0	0
3	1	1	0	0	0
4	0	0	1	0	0
5	1	0	1	0	0
6	0	1	1	0	0
7	1	1	1	0	0
8	0	0	0	1	0
9	1	0	0	1	0
10	0	1	0	1	0
11	1	1	0	1	0
12	0	0	1	1	0
13	1	0	1	1	0
14	0	1	1	1	0
15	1	1	1	1	0
16	0	0	0	0	1
17	1	0	0	0	1
18	0	1	0	0	1
19	1	1	0	0	1
20	0	0	1	0	1
21	1	0	1	0	1
22	0	1	1	0	1
23	1	1	1	0	1
24	0	0	0	1	1
25	1	0	0	1	1
26	0	1	0	1	1
27	1	1	0	1	1
28	0	0	1	1	1
29	1	0	1	1	1
30	0	1	1	1	1
31	1	1	1	1	1

15. Appendix 2. GPRS Connection Errors

Error 619: *Port is not opened – there was a temporary glitch with the phone (modem) or PC.*

Shut down and restart the "Orlan" module, or restart the computer.

Error 633: *The modem or other connection device is already in use or not configured – Network Remote Access tries to use the COM-port that is used by the active network connection or another program (fax, telephone or HyperTerminal program). Modem driver is not installed or is installed incorrectly.*

Close all programs that can use COM-port and remove them from the startup. Restart the computer.

Error 678: *Remote computer is not responding – connection process freezes on a set of numbers, then an error message appears. This error occurs when subscriber's account doesn't have enough funds (the balance is zero or negative).*

It is necessary to refill the account balance and restart “Orlan” module.

Error 692: *A hardware error occurred – modem initialization line or access point to the phone menu are filled incorrectly, wrong module selected in the properties of remote connection (for example, PCI-modem) or the modem is configured incorrectly, the cable is defective. Incorrect driver of the cable or modem is installed.*

It is recommended to reconnect the phone and cable, turn off and restart the phone, restart PC, check the modem initialization line (AT + CGDCONT = 1, "IP", "internet.provider.ru"), replace the cable or update the driver of the modem or cable. Make sure you closed all the programs that may use the port used by the modem.

Error 711: *Failed to connect with this phone book element – this occurs, if some services are disabled.*

Open the Control Panel, Administrative Tools, Services and start (or restarted if already running) Plug and Play service (enabled, auto), Remote Access Connection Manager (enabled, manually) and Remote Auto-Connection Manager (enabled, auto).

Error 718: *TCP/IP protocol reports an error – “Orlan” module crashed or insufficient mobile signal.*

Move "Orlan" module to another location and try to reconnect to the Internet.

Error 734: *PPP-connection Control Protocol was interrupted – may occur in case of insufficient network signal, incorrect login or password, incorrect modem initialization line or incorrect security settings. In addition, error 734 (along with error 777) can occur due to non-activated GPRS-access for the phone number. Furthermore, error 734 may occur in case of insufficient amount of funds at subscriber's account, or in a situation where the balance during the last 24-48 hours (usually no more than a day) has been zero or negative.*

You must move the phone to another location (if possible, closer to the window), check your login and password and double-check the modem initialization line (AT + CGDCONT = 1, "IP", "internet.provider.ru"). Make sure that GPRS-access services are active on your phone number.

Refill your account balance or wait until access to GPRS is resumed (for the changes to take effect, please restart the "Orlan" module).

Error 777: *Connection attempt failed because the modem or other communication device assigned to remote computer is out if service – usually occurs in a situation where you try to connect to the Internet without being connected to GPRS services.*

You must make a request for service enabling.

Error 797: *Failed to connect because the modem was not found or busy – no communication with the modem.*

Reboot "Orlan" module and/or restart PC.