

PR MASTER USER MANUAL

PRM Version 4.5.26

Rev. P

Contents

I. Introduction	5
Chapter 1. Preparing system to work.....	7
1.1. PR Master Installation.....	7
1.1.1. Roger ACS 4.5 application group content.....	11
1.2. Starting the software.....	12
1.3. List of PR Master parameters	13
1.4. Quick Start	14
Chapter 2. The System in use	16
2.1. Initial operations	16
2.1.1. Defining password for the ADMIN user	16
2.1.2. Defining program operators.....	16
2.1.3. Defining INSTALLER user	16
2.1.4. Planning of backup schedule.....	17
2.1.5. Planning of system configuration update schedule	17
2.1.6. Planning of reading event buffers schedule.....	17
2.2. Advanced maintenance operations	18
2.2.1. Setting up the Anti-passback mechanism.....	18
2.2.2. Defining attendance areas	18
2.2.3. Defining alarm zones.....	18
2.2.4. Defining facility plans	18
2.3. Day to day system operation	19
2.3.1. User management.....	19
2.3.2. Making system backups.....	19
2.3.3. System monitoring	20
Chapter 3. PR Master functionality	21
3.1. File Menu.....	21
3.1.1. New system... command	21
3.1.2. Import system settings from file	22
3.1.3. Export system settings to file	24
3.1.4. Exit	26
3.2. System menu.....	26
3.2.1. Installer.....	26
3.2.2. Holidays	27
3.2.3. Users	28
3.2.4. Guests.....	36
3.2.5. Groups	38
3.2.6. Schedules.....	43
3.2.7. Access zones	49
3.2.8. Networks.....	54
3.2.9. Attendance areas	68
3.2.10. APB Zones	71
3.2.11. Alarm Zones	73
3.2.12. Fingerprint readers.....	76
3.2.13. Card Box	79
3.2.14. Facility plans.....	83
3.2.15. CCTV devices.....	89
3.3. Reports menu	91
3.3.1. Groups	91
3.3.2. Users	91
3.3.3. Access zones	91
3.3.4. Networks.....	91
3.3.5. Controllers.....	92
3.3.6. Access rights	92
3.3.7. Event history	92
3.3.8. Attendance.....	100

3.3.9. User modifications	104
3.4. Commands menu	105
3.4.1. Read event buffers now	105
3.4.2. Read event buffers later	106
3.4.3. Clear event buffers now	106
3.4.4. Update system now	106
3.4.5. Update system later	107
3.4.6. Set system clocks.....	108
3.5. Tools Menu.....	109
3.5.1. Online monitoring	109
3.5.2. Quick user update.....	110
3.5.3. Access map	111
3.5.4. Users' attendance in Access Zones	112
3.5.5. T&A modes.....	112
3.5.6. Inputs	114
3.5.7. Alarm Events	116
3.5.8. Program operators	117
3.5.9. Change Password	119
3.5.10. Lock program	120
3.5.11. Options	120
3.5.12. Backup configuration.....	134
3.5.13 Identify user	136
Chapter 4. Online monitoring	137
4.1. View menu	137
4.1.1. Clear EVENTS window	138
4.1.2. EVENTS window columns	138
4.1.3. Reverse event order.....	139
4.1.4. ALARMS window	139
4.1.5. Clear ALARMS window.....	139
4.1.6. ALARMS window columns.....	139
4.1.7. Acoustic signal on alarm event.....	140
4.1.8. Monitoring filter	140
4.1.9. Alert monitor	141
4.1.10. Users last logins.....	142
4.1.11. Evacuation Monitor.....	143
4.1.12. Access Point Monitor	143
4.1.13. Controller status.....	144
4.1.14. View map	145
4.1.15. Access map	147
4.1.16. Users' attendance in Access Zones	147
4.1.17. Integra status monitor.....	147
4.1.18. Connected Remote Monitors	147
4.1.19. Exit	147
4.2. Commands menu	148
4.2.1. Controllers command submenu	148
4.2.2 Alarm Zone commands.....	149
4.2.3. System commands submenu	150
4.2.4. Clear all alarms.....	151
4.2.5. Set system clocks.....	151
4.3. Tools Menu.....	151
4.3.1. Quick user update.....	151
4.3.2. Online reports.....	152
4.3.3. Email configuration	153
4.3.4. Authorised access	153
4.4. Hide window.....	155
4.5. Play CCTV record and Real Time monitoring buttons	155
4.5.1. Play CCTV record button	155

- 4.5.2. Real-time monitoring button155
- Chapter 5. Remote Monitor software157
 - 5.1. Starting the software.....157
 - 5.2. View menu159
 - 5.3. Commands menu160
 - 5.4. Tools menu.....160

I. INTRODUCTION

PR Master is used for configuration and management of RACS 4 system (**Roger Access Control System**). RACS 4 is an Access Control System based on PRxx1 and PRxx2 series controllers, PRT series readers, UT and RCI series communication interfaces as well as CPR32-SE and CPR32-NET network controllers manufactured by Roger.

PR Master is an application for 32-bit Windows XP and newer 32-bit systems as well as 64-bit Windows Vista and newer 64-bit systems.

Licensing system was introduced for PR Master 4.5.4 and newer. The integration with alarm panels of INTEGRA (SATEL) series and wireless door locks of APERIO (ASSA ABLOY) system requires license key which is managed by PR Master software but it is generated individually for each CPR32-NET network controller. Default, free of charge license key for PR Master software allows to use all functionalities described in this manual. There are only following limitations:

- ◆ Maximum two alarm zones of INTEGRA (SATEL) alarm panel per CPR32-NET
- ◆ Maximum two door locks of APERIO (ASSA ABLOY) system per CPR32-NET

The maximum number of controlled INTEGRA alarm zones in the whole system is 32 while the maximum number of APERIO locks per CPR32-NET is 16.

Additionally some language versions of PR Master can also be governed by license excluding Polish and English versions.

PR Master is used by:

- ◆ **installers** — who conduct basic software configuration and prepare it to work;
- ◆ **end users (owners)** — who perform day to day program maintenance, prepare reports, make backups, manage users, create APB zones, attendance areas, and so on.

Such division is in line with Access Control System life cycle. First, installation company installs the system, attaches all the devices, configures the system, and then hands it over to the end user who is responsible for its day-to-day maintenance.

The PR Master application should be installed by the installer from company deploying the ACS after physical installation of all the system components (including controllers, CPR network controllers, readers and interfaces) and after making all the connections. Then the application should be handed over to the final system's user and put into use. From then on, end users will utilize the application on day-to-day basis.

The purpose of this manual is to present functionalities of PR Master software, taking into account tasks performed by the installer and end users. Of course the allotment of tasks is not strict. It may happen that after computer crash, replacement, backup loss or similar situations, end user will make an attempt to set up an application single-handedly. In such case it is advised to read carefully chapter 1. "Preparing the system to work" and to perform all the steps described there. A specific case of preparing the system to work is PR Master upgrade from older into newer version. In such a case it is necessary to take all the steps needed for preserving data from previous version.

Remote Monitor is an additional software, which can be used in RACS 4 system. The software can be installed on multiple workstations and it can connect with PR Master software in order to enable user enrollment, user monitoring, etc. Therefore, Remote Monitor enables RACS 4 to be operated from multiple workstations with some functional limitations.

The Manual is divided into 5 chapters.

In **Chapter 1.** "Preparing System to Work" an installation process and its initial setup is described.

In **Chapter 2** „Day to Day Maintenance“, typical tasks performed on daily basis are discussed. They include such tasks as defining system's users and groups, schedules, alarm zones, events monitoring, preparing reports, and so on.

In **Chapter 3.** "PR Master Functionality", synthetic summary of all the program's menu and commands is presented. The chapter describes all the menus, dialog boxes and alternative ways of invoking different functions.

In **Chapter 4** „Monitoring“, monitoring mode of PR Master is described.

In **Chapter 5** „Remote Monitor software“, additional software for RACS 4 system is described.

The present manual is supplemented with installation guides for particular controllers and such manuals as **Functional description of PRxx2 series controllers** and **Functional description of PRxx1 series controllers**. All available integrations of RACS 4 system are described in dedicated manuals.

CHAPTER 1.

PREPARING SYSTEM TO WORK

1.1. PR MASTER INSTALLATION

In order to install PR Master, the archive with setup program should be first downloaded from the Roger's website (<http://www.roger.pl/>). The archive can be found in file called **PRMaster 4.x.x.xxxx setup.exe**. After the file is downloaded it should be executed, which results in displaying an initial installation screen (Figure 1.1).

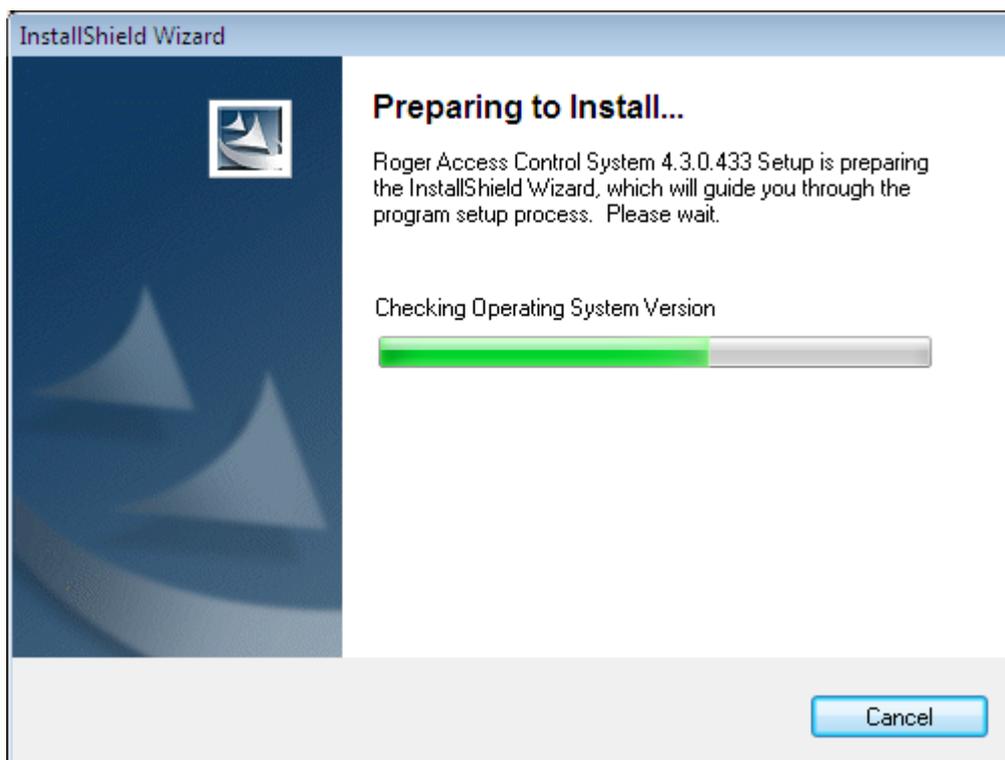


Figure 1.1. *Installation screen*

Then an initial RACS 4 installation wizard screen displays (Figure 1.2).

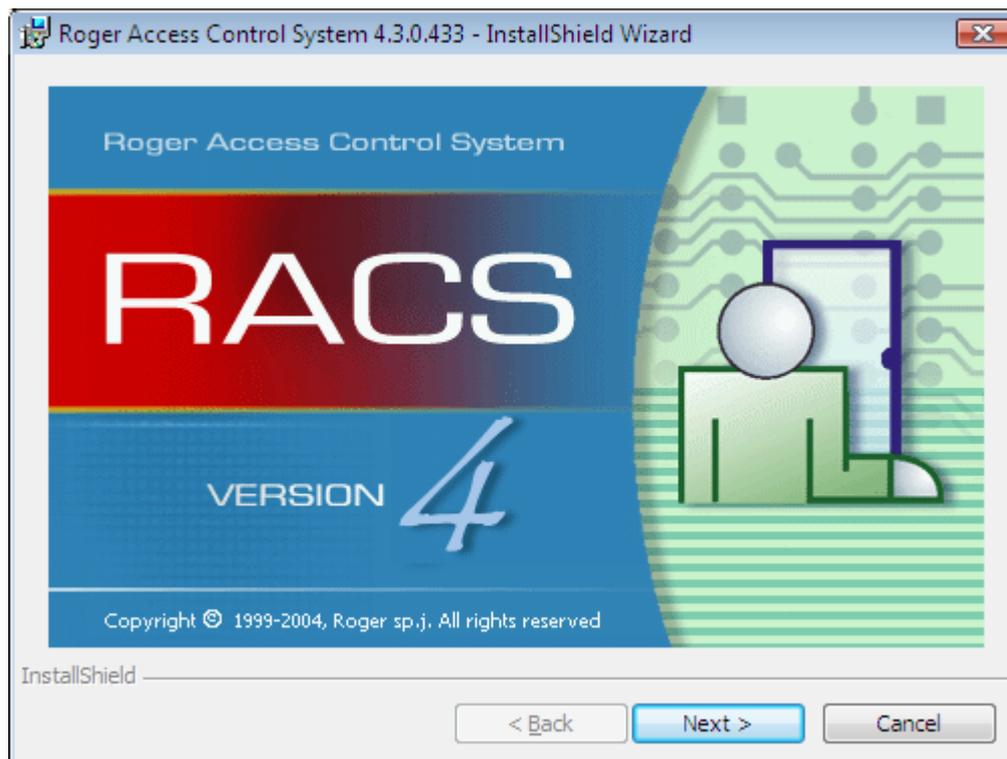


Figure 1.2. RACS 4 installation wizard — step 1

In this window you should click **Next**. The second dialog box displays — a welcome screen containing copyright information. In this window you should also click **Next**.

The next wizard's window is a screen containing license agreement. You should read it carefully, and place a check next to the **I accept the terms in the license agreement** option. If you don't select this option, the **Next** button will be disabled, and you will be unable to continue the installation. Once you familiarize with the license agreement, you can click **Next** and proceed with the installation. In the next wizard's screen you can find the **README** file. You should read it carefully and then click **Next**.

The next wizard's window displays (Figure 1.3). You should enter user's first and last names (the **User Name** field) as well as its organization (the **Organization** field). As for most Windows applications you can also indicate if the application should be available only for the current user (the **Only for me** option) or for all users of the computer (**Anyone who uses this computer (all users)**).

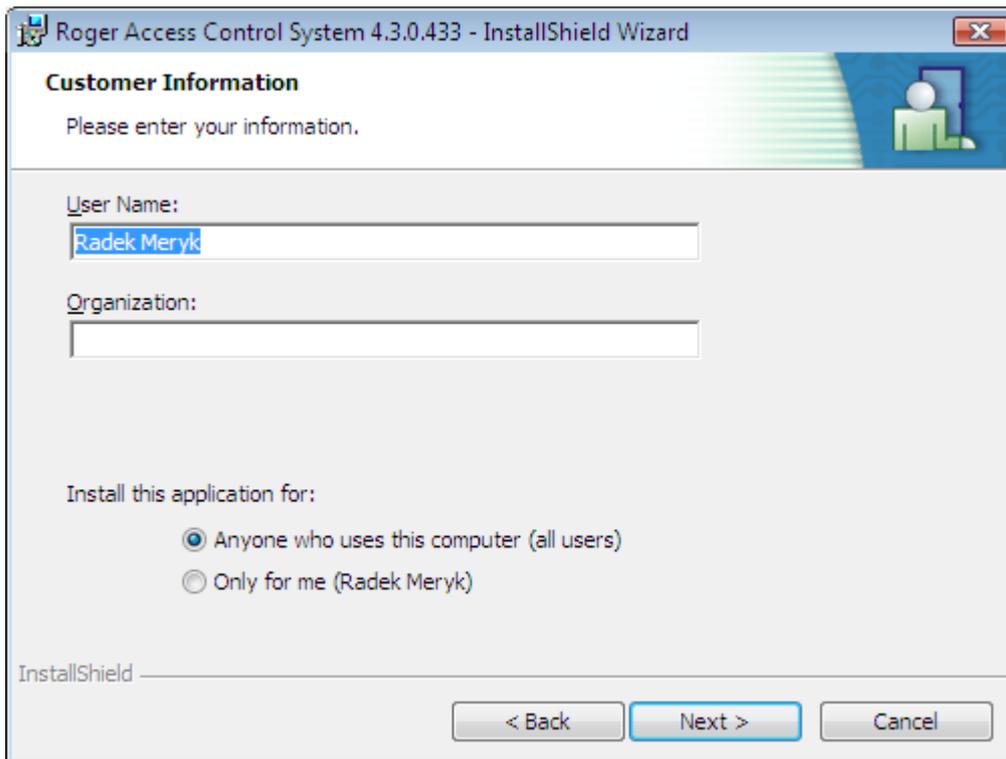


Figure 1.3. RACS 4 installation wizard — user's data

Upon entering this data, you should click **Next**. The destination folder selection window displays (Figure 1.4).

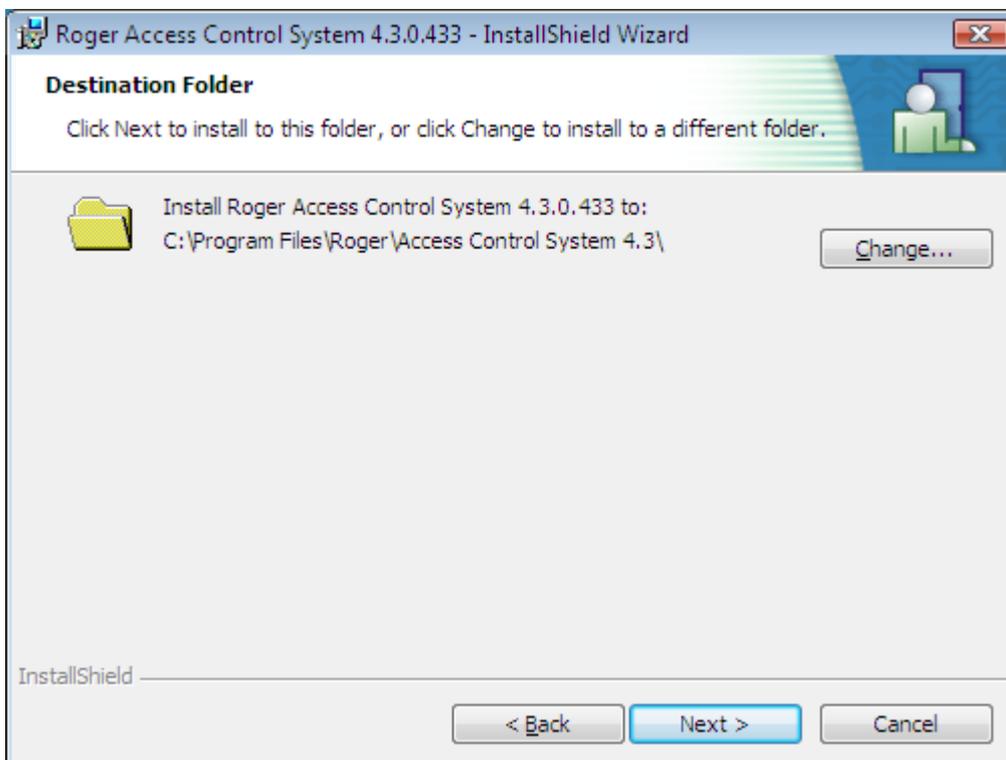


Figure 1.4. RACS 4 installation wizard — destination folder selection

By default, the PR Master application installs in the **C:\Roger\Access Control System 4.5** folder. If you want to change this location, you can use the **Change** button.

After the installation destination folder has been entered, you should click **Next**. The file copying process starts. Upon its completion, the system will validate the installation (Figure 1.5).

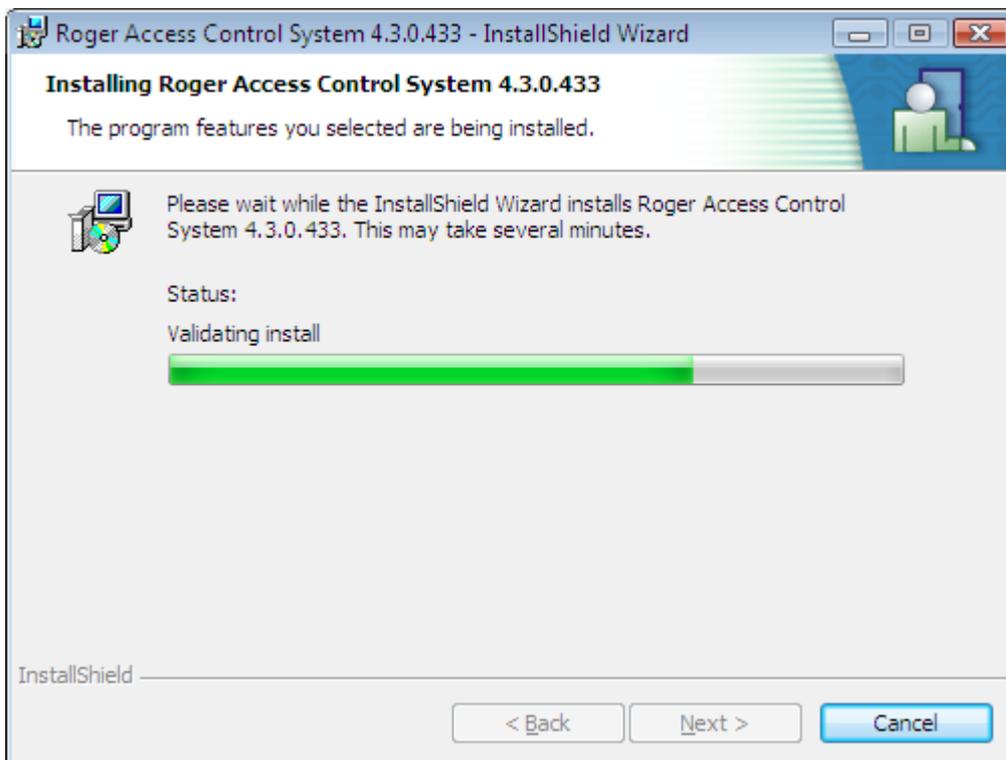


Figure 1.5. RACS 4 installation wizard — copying files and validating install

After this process is completed, if everything is done correctly, the system will display the window with an information that the installation is successful (Figure 1.6).



Figure 1.6. RACS 4 installation wizard — the application has been successfully installed

1.1.1. Roger ACS 4.5 application group content

When you install the PR Master application, the **Roger ACS 4.5** application group will be created. Its content is shown in Figure 1.7.

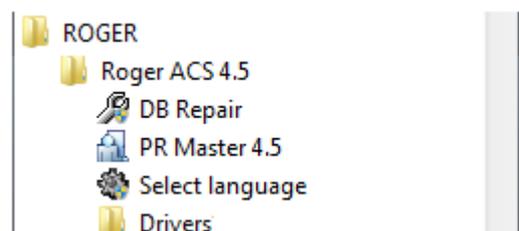


Figure 1.7. The Roger ACS 4.5 Application Group Content

The **Roger ACS 4.5** application group contains the following elements:

- ◆ **PR Master 4.5** — link to PR Master executable file.
- ◆ **Repair database indexes** — a tool for repairing database's indexes.
- ◆ **Select language** — a tool for selection of PR Master language version. Some language versions might require license. Polish and English versions can be used without any limitations.
- ◆ **Drivers** — group contains drivers for USB-RS485 communication interfaces



If the PR Master application was previously used in the computer where you install the system, then before running the setup program but after application uninstall, the best thing is to manually delete the folder where the application was installed. Most often the path to this folder is **C:\Program Files\Roger\Access Control System 4.5** or **C:\Roger\Access Control System 4.5**

If you remove all the files from the previous installation you will be certain, that the copy of the program is „clean“.

1.2. STARTING THE SOFTWARE

When you start PR Master for the first time after the installation, the language selector windows is displayed (Figure 1.8).

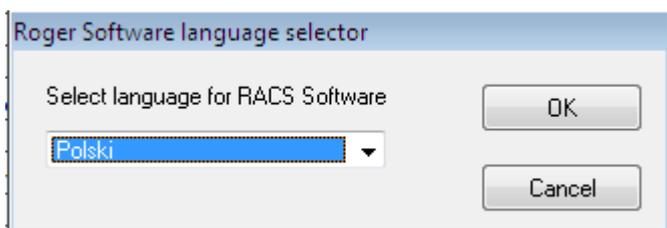


Figure 1.8. Language selection for the PR Master

In this dialog box you should select the user interface language, and then click **OK**. The confirmation dialog box displays, where you should click on the **OK** button if you want to confirm the selection or on the **Cancel** button if you want to resign. Then an information dialog box displays, containing list of system’s components and selected language version. In this window you should click **OK** once again. Only then an initial PR Master login screen appears (Figure 1.9).

Default password for the ADMIN user is empty. So, you should click **OK**.

The PR Master can communicate with other programs through network. Because of that, depending on Windows firewall settings, the program may display a warning window similar to the one shown in Figure 1.11.

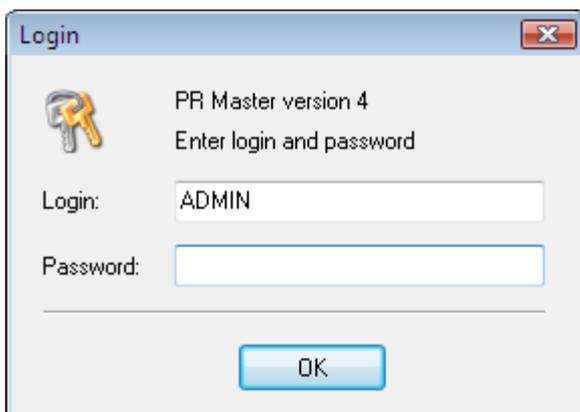


Figure 1.9. PR Master logon screen

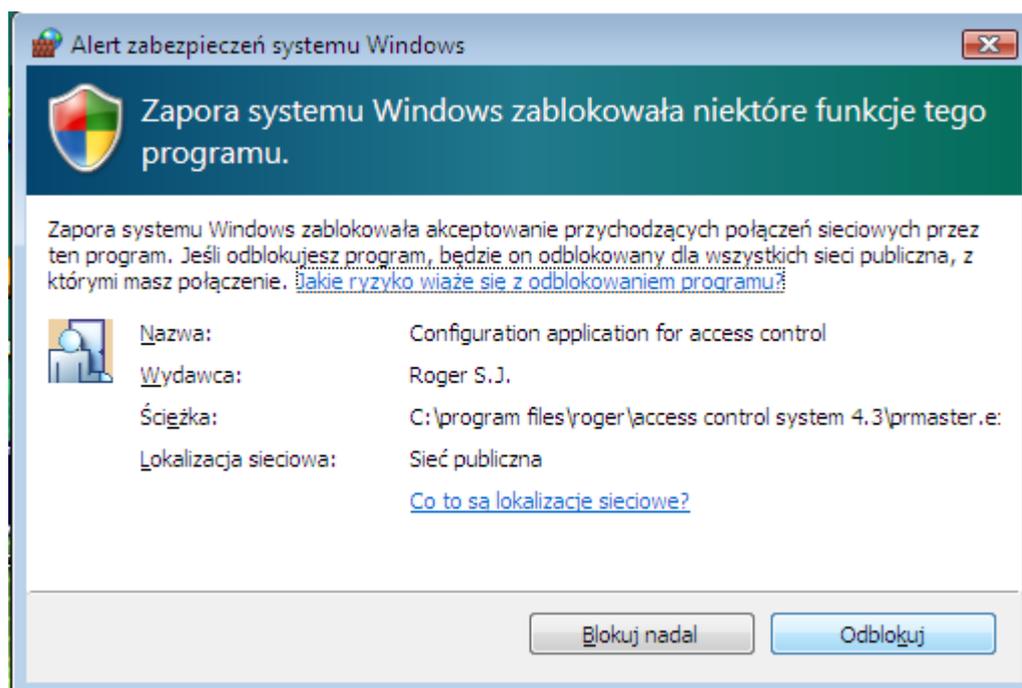


Figure 1.11. Windows firewall informs that network connections to the PR Master application are blocked

If you want to remotely connect to the PR Master, you should click on the **Unlock** button. Now the PR Master can start without further problems.

1.3. LIST OF PR MASTER PARAMETERS

PR Master software can be started with various parameters which offer additional non-standard functionalities or allow to use the software in non-standard way. List of available parameters:

/NOEVDL – when **Update system now** command is selected – see **section 3.4.4**, then the program does not collect events from the system at all and starts configuration update immediately

/MONITOR – when PR Master is started then it enters Online monitoring automatically - see **Chapter 4**. When operator's login and password are defined in [Autologin] section of config.ini file then login window is skipped.

/AUTOEVENT – the program is started only for events collection and storing into database - see **section 3.4.1** and then it closes automatically.

/EVLIMIT=x – the parameter enables to increase the maximal number of events processed by the program from default 300 thousand events to x events - see **section 3.3.7**.

/CPRNETPORT=x – the parameter enables configuration of default and normally unconfigurable UDP port for communication of the program with CPR32-NET devices.

/USE_CPR_PORT – the parameter enables the program to distinguish CPR32-NET devices not only by the IP address but also by their port. This can be used when multiple CPR32-NET devices are available behind router with port forwarding.

1.4. QUICK START

When you start the PR Master, the main PR Master window is displayed (Figure 1.12).

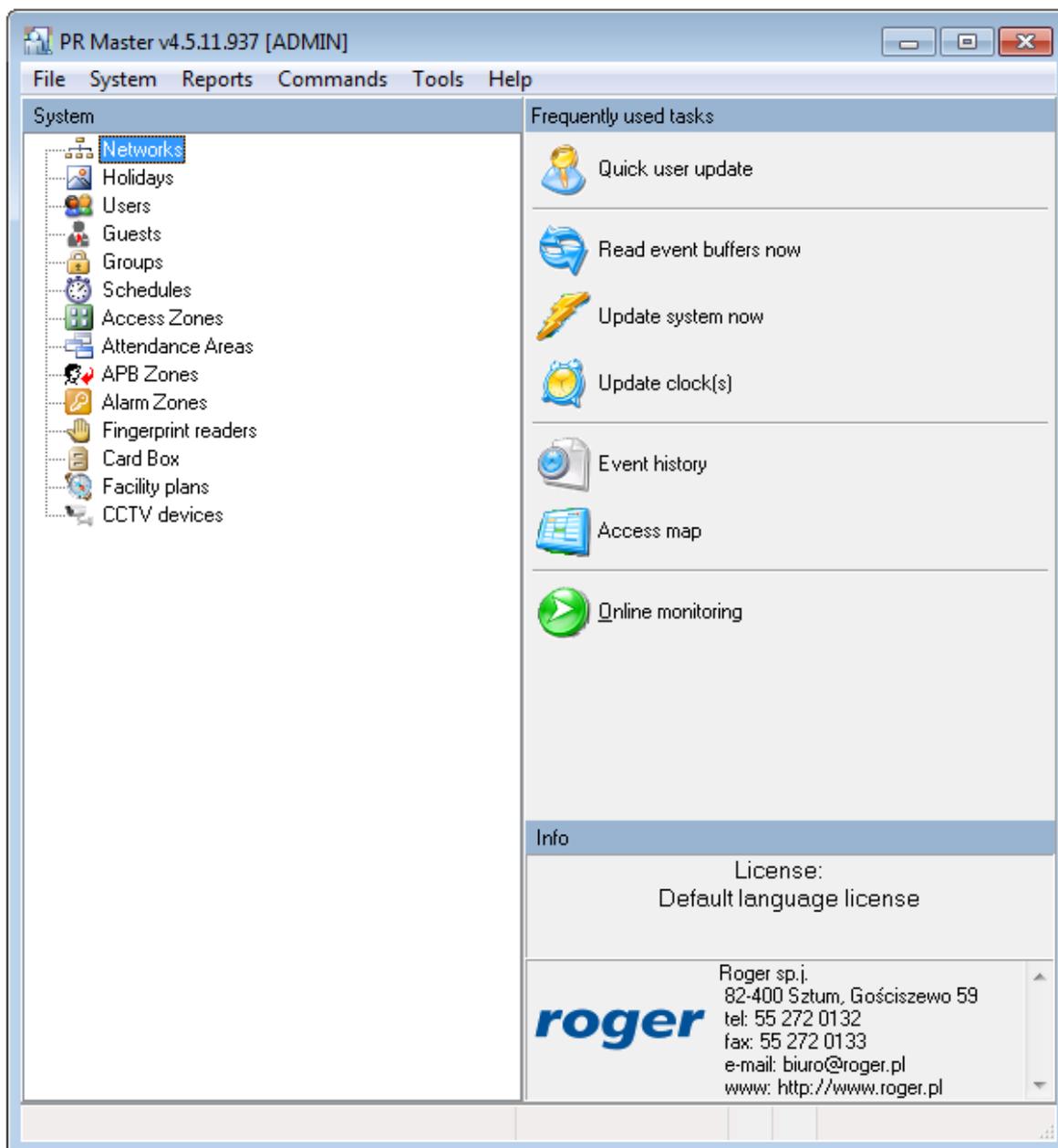


Figure 1.12. PR Master main window

In the top section of the window there is the program's main menu. On the left hand side there is a **System** navigation tree, and on the right hand side there is a list of frequently performed tasks. These are the three possibilities of getting access to the PR Master's functionality. They have the same effect, but only the menu gives access to the complete set of commands.

To prepare program for work you should perform the following steps:

1. Create an empty database. In order to do this, you need to use the **File/New system ...** command (see [section 3.1.1](#)).

2. In the **System** navigation tree click on the **Networks** icon or select the **Networks** command from the **System** menu (see [section 3.2.8](#)).
3. Add a new network (see [section 3.2.8.1](#)). Remember to give to the network a descriptive name. If you do not do this, the PR Master will assign to the networks default names: **Network A**, **Network B**, and so on.
4. Add controllers to the network (see [section 3.2.8.4](#)). Again, you should remember to give descriptive names to the controllers. The names should be properly chosen in order to allow their easy identification later on. If you want to assign a name to the controller, select the controller, click on the **Properties** button and enter a descriptive name in the **Controller name** field. Additionally if you want to assign names to controller's readers, in the same window select **Terminal ID0** and/or **Terminal ID1** tab and enter a descriptive name in the **Name** field.
5. Repeat steps 1–4 for the remaining networks in the Access Control System.
6. When all the networks (subsystems) are configured, you can define access zones. The installer should do this in cooperation with the end user (owner). A detailed description on how access zones should be defined can be found in [section 3.2.7](#).
7. After defining access zones, define time schedules for use in the system. You can find more information on this subject in [section 3.2.6](#). Once you define time schedules, define holidays in the current year. Information on how to define holidays can be found in [section 3.2.2](#).
8. Now you can define user groups. Read [section 3.2.5](#). Read carefully about how in the RACS 4 the groups are related to access rights. Define access rights for all the groups in specific access zones. In order to do this, assign time schedules to the zones. Time schedules describe time intervals when a group has rights in particular zone.
9. Now you can proceed to entering users data. Before you start doing this, you can create a proximity card set, you will assign the card to the users from. You can find more information on how to create such a cards container in [section 3.2.13](#). You can read about user management in [section 3.2.3](#).
10. Upload configuration settings to all the controllers in the system. In order to do this, use the **Update system now** command. You will find it on the frequently used tasks list on the right hand side of the program's main window. More information on the command for configuring the whole system can be found in [section 3.4.4](#).

At this moment, after uploading configuration settings to all the controllers, the system is initially prepared for work. Of course the system lacks an advanced configuration (e.g. attendance areas, alarm zones, APB zones), but these activities can be performed later and they require much less work. Because the main part of configuration work has been done, you should create a system backup now, so you could restore a basic configuration from backup copy in case of errors, system crash, and so on. You want to make sure, that the backup is stored on an external medium. Thanks to this it will be available also in case of disk failure. You can find more information on how to make backups in [section 3.5.12](#).

CHAPTER 2.

THE SYSTEM IN USE

So the RACS 4 has been commissioned to final user. In order to be able to use it properly, you should perform a few tasks. Firstly, they will ensure safe work of the system, and secondly they will allow to use PR Master software in full extent. All these tasks are described in this chapter.

2.1. INITIAL OPERATIONS

2.1.1. Defining password for the ADMIN user

Immediately after the system has been deployed, the password for the ADMIN user is empty. Because this user has unlimited rights in the PR Master, you should make sure that the ADMIN account is protected with password.

To define password for the ADMIN user:

1. Select **Tools/Program operators** command.
2. Select the ADMIN user.
3. Click on the **Set password** button. The **Change password** dialog box appears.
4. Because default password for the ADMIN user is empty, leave the **Old password** field empty.
5. In the **New password** text box enter a new password, which will be used from this moment on.
6. Confirm the new password by entering it again in the **Confirm password** text box.



For security purposes it is recommended to specify non typical password. It would be best if you could not find it in dictionaries. The best password should contain at least one digit and a symbol such as {, [,), {, [,). The password, once defined, should be remembered. It may also be written on a piece of paper, put into properly described envelope and stored in properly protected place (such as a safe).

Under no circumstances should anyone write passwords onto sticky notes and leave in the area around the computer (such as monitor).

2.1.2. Defining program operators

In a robust ACS, maintenance tasks can be divided between several operators. In particular, you could designate an operator responsible for adding users to the database and other operator responsible for doing backups. You can define individual accounts for such operators as to prevent accidental corruption of system's configuration by them. You can find more information on how to define operator accounts in [section 3.5.8](#).

2.1.3. Defining INSTALLER user

In case of PRxx1 series controllers the INSTALLER user has rights to enter the programming mode of controllers in order to program them manually with keypad commands but has no rights to

unlock the doors being controlled. This special user has no ID assigned. In order to do define the INSTALLER user in the PR Master, you should use the **System/Installer** command. You can find more information on this subject in [section 3.2.1](#). In RACS 4, Installer user is optional feature.

2.1.4. Planning of backup schedule

Access Control System is a dynamic object, where many events occur rapidly. Thus, you want to make sure, that the system's backups are made regularly. Thanks to backups you can restore all the events and the system's configuration in case of system failure. When the database is large, making full backup can take long time. Because of that, you can configure the backup schedule, so that the system automatically makes backup when it is less busy. You can find a detailed description on defining such a backup schedule in [section 3.5.12](#).



It is strongly recommended to perform regular backups of PR Master configuration as such configuration cannot be restored from RACS 4 devices.

2.1.5. Planning of system configuration update schedule

The RACS 4 consists of two parts: door controlling devices (controllers, network units and readers) and PR Master software for system management. Settings in both parts must comply to ensure proper operation, therefore all PR Master settings have to be send regularly to devices. Such synchronization of settings can be done manually or automatically. If the system is large, such update can take significantly long time. Therefore, you can configure the schedule, so that the system will automatically update when it is less occupied (e.g. at night). You can find a detailed description on defining of such schedule in [section 3.4.5](#).

2.1.6. Planning of reading event buffers schedule

In the RACS 4, events are recorded all the time, even if PR Master software is not started and regardless of PR Master mode of operation. If PR Master is off or is not in monitoring mode, events are recorded in controllers' buffers (PRxx2 series controllers) or CPR32-SE/CPR32-NET network unit if the system is equipped with them. Reading of event buffer is done on request and also whenever the application is switched into monitoring mode. In order to avoid significant discrepancies between database and event buffers of RACS 4 devices, you can configure schedule for periodic reading of event buffers. In order to do this, you need to use the **Commands/Read event buffers later**. This command is described in detail in [section 3.4.2](#).

2.2. ADVANCED MAINTENANCE OPERATIONS

The set of PR Master's advanced maintenance operation consists of the following activities:

- ◆ setting up the Anti-Passback function,
- ◆ defining attendance areas,
- ◆ defining alarm zones.
- ◆ defining facility plans.

These subjects will be described in the following sections.

2.2.1. Setting up the Anti-passback mechanism

Access Control System provides many options for controlling doors in facilities being controlled. It allows, among other things, to block the possibility to pass proximity cards (e.g. through a window) to unauthorized persons. The Anti-Passback function can be used exactly for this purpose. If you define it, a user will not be able to enter an APB zone, if he has not left it before.

You can find more information on defining APB zones, as well as on configuring it in the RACS 4 in [section 3.2.10](#).

2.2.2. Defining attendance areas

Attendance areas is one of the RACS 4's mechanisms which allow for controlling the location of user in the facility. An attendance area can be understood as a part of the area being controlled by the ACS which you can enter through a set of identification points (readers) and you can leave by another set of identification points (readers).

Attendance areas are defined in order to prepare attendance reports ([Reports/Attendance](#)), which further can be used for Time&Attendance. **Attendance report** shows time the user entered/left the area and total time he was present in the attendance area. You can also prepare report showing who entered to the particular area as first and who left it as last in defined time interval. You can find a detailed description on defining attendance areas in [section 3.2.9](#).

2.2.3. Defining alarm zones

Alarm zones enable to define a groups of controllers, which will be armed/disarmed concurrently. Such groups can be armed/disarmed manually or according to administrator defined schedule. It is also possible to define alarm zones hierarchy, so group of controllers could be armed/disarmed in compliance with the hierarchy levels (master-slave).

You can find more information on defining alarm zones in the PR Master in [section 3.2.11](#).

2.2.4. Defining facility plans

Facility plans is a tool designed for visual monitoring of access control system. By means of this functionality, the user can place icons of controllers on the interactive facility plan and then monitor and control them. Starting from version 4.3.3.522, PR Master allows to define up to 20 separate plans. After they are defined, they can be displayed in PR Master's monitoring mode.

You can find more information about defining and using facility plans in [section 3.2.14](#).

2.3. DAY TO DAY SYSTEM OPERATION

Roger Access Control System after its initial configuration, and after all the settings, permissions, zones and options have been set becomes ready to operate. There are much less operations in this state when compared to deployment phase, when many elements require configuration. Day to day operations in PR Master include:

- ◆ user management — defining new users, removing users, assignment to access groups,
- ◆ making system's backups,
- ◆ monitoring.

These activities will be described in the following sections.

2.3.1. User management

Users management is performed from users directory, which can be opened from the **System** navigation tree in the left part of the main PR Master's window or by using **Users** command from the **System** menu. You can also use **Quick user update** command from the **Tools** menu or from the **Frequently used tasks** list. The **Quick user update** command is also available in the monitoring mode (in the **Tools** menu).

All modifications of user settings in PR Master software have to be uploaded to controllers in order to be effective. The main difference between user dictionary invoked from the **System** menu, and **Quick user update** command lies in the information uploaded to controllers. In the first case all access control settings including user settings are uploaded to devices by administrator, while in the second only user settings are sent to controllers. Therefore the first method can be time-consuming, while the second enables quick management of user rights. Operations available in the users directory have been described in [section 3.2.3](#), and the **Quick user update** command is described in [section 3.5.2](#).

2.3.2. Making system backups

The PR Master database contains a lot of data. Possible loss of database and in consequence the whole configuration of the system from scratch can take a lot of time, especially when the ACS system is large. Thus, it is recommended to perform backups regularly.

PR Master is equipped with a mechanism that informs user that the changes have been made in the system. This is the floppy diskette icon shown on the status bar in the main PR Master's window (Figure 2.1). If such an icon appears, it is an indication, that the configuration has been changed and it is worth to make backup.

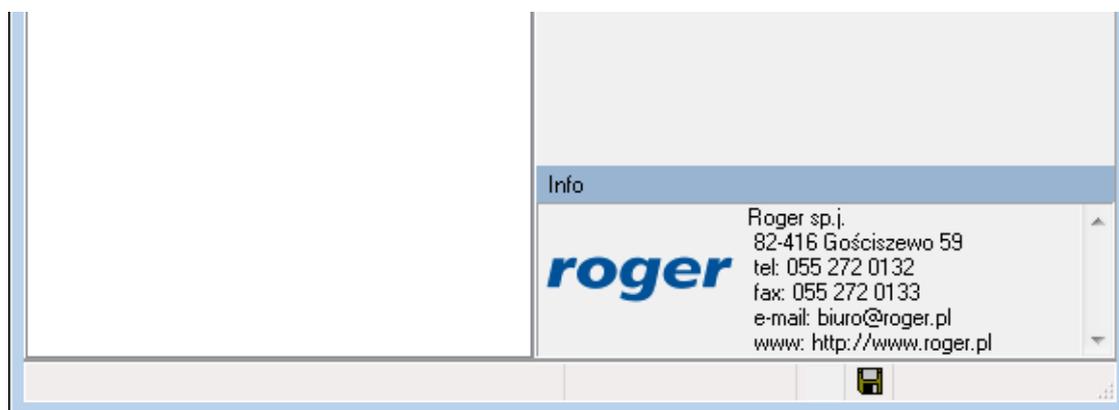


Figure 2.1. The floppy disk icon on the status bar informs about the need to make system backup

You can find a detailed description on defining backup schedule in [section 3.5.12](#).

2.3.3. System monitoring

The PR Master has two main modes of operation: configuration and monitoring. Configuration mode is used for modification and uploading settings to the system while monitoring mode enables online control of the system. The monitoring mode is used mainly on day to day basis, when the RACS 4 is stable and configured. In order to invoke monitoring mode, you can click on **Online monitoring** icon in the **Frequently used tasks** panel or select **Tools/Online monitoring** command from the **Tools** menu.

PR Master's online monitoring mode is described in detail in [Chapter 4](#).

CHAPTER 3. PR MASTER FUNCTIONALITY

3.1. FILE MENU

The **File** menu has been shown in Figure 3.1.

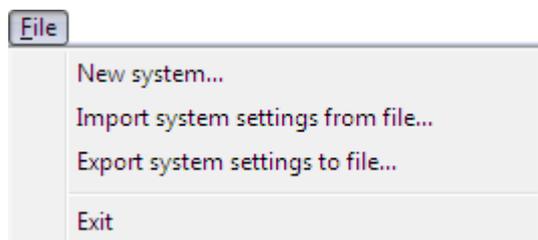


Figure 3.1. *File Menu*

3.1.1. New system... command

New system... command is used for clearing the database content in order to create a new, empty system. You should use it in order to configure a new system from scratch. If you select this command, the dialog box shown in Figure 3.2 appears.

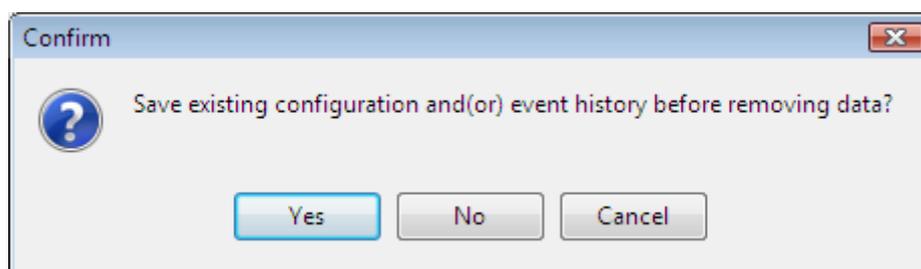


Figure 3.2. *You need to decide if you want to make backup of existing database*

If you answer **Yes** to this question, the other dialog box appears. There you can select file for the backup of the current database content (Figure 3.3). You can save a configuration and events in a compressed **Backup files (.zip)**, you can export database into **Data directory zip (*.ddz)**, you can save only settings in **Config files (*.xml)** or only events in **Events files (*.xml)**.

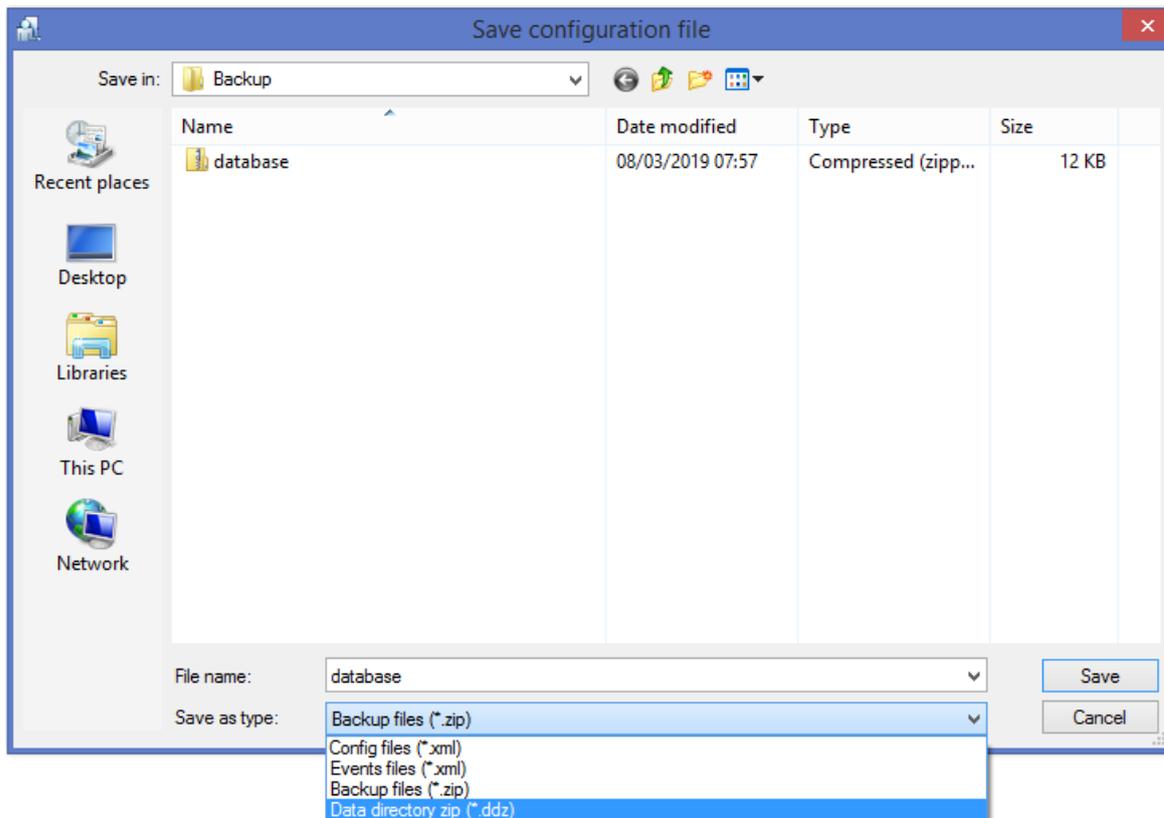


Figure 3.3. Selecting file where system settings will be saved



Using the **New system...** command without saving current settings will cause the data loss — all data about networks, controllers, schedules, users, events and all other information will be deleted. In order to protect your own work, it is recommended that you use this command with caution and make backups often.

After using the **New system...** command, the database is empty. You can notice that in the PR Master’s main window you will not find any settings.

3.1.2. Import system settings from file

The **Import system settings from file...** command allows to import previously saved configuration and/or events. After you select this command, the dialog box for selection of file is displayed (Figure 3.4).

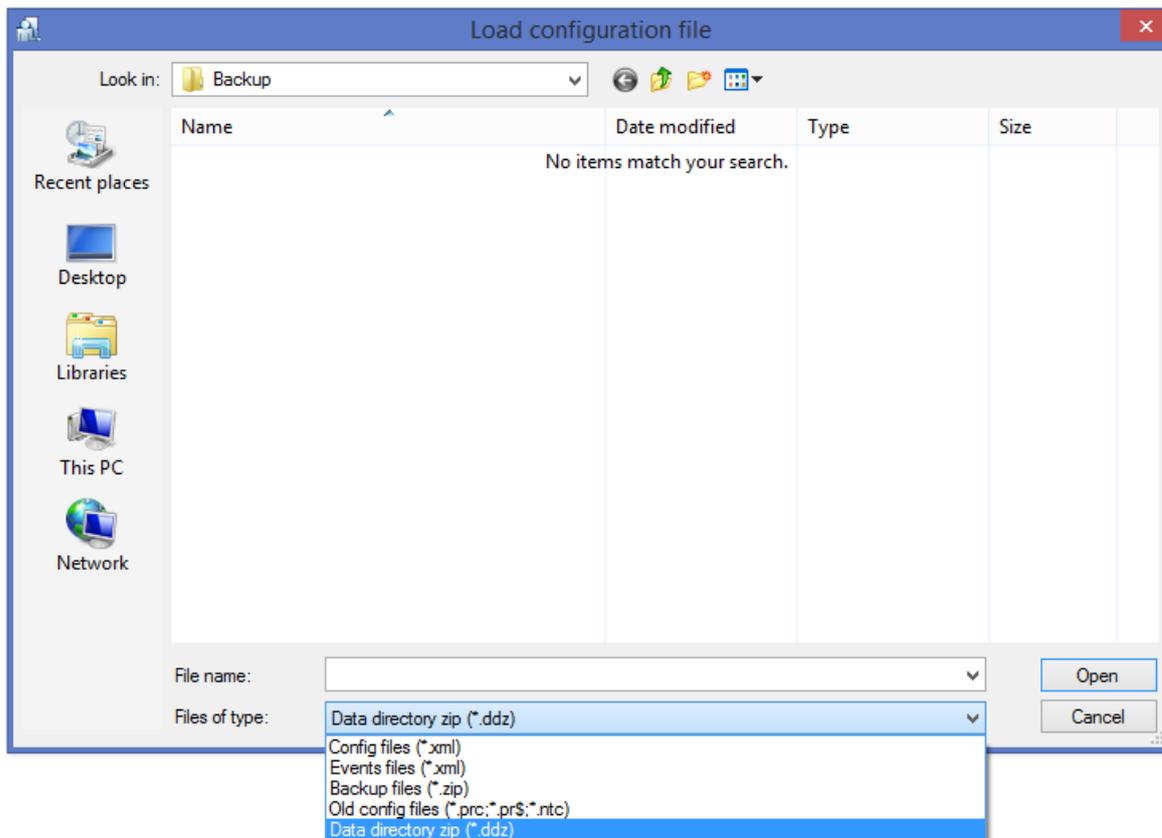


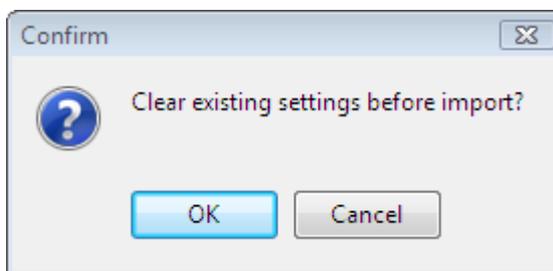
Figure 3.4. *Selecting file to import data from*

Following files can be selected for import:

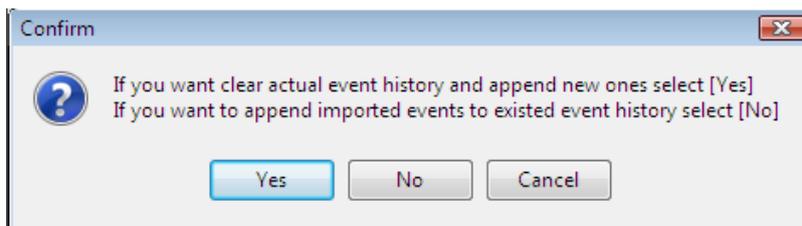
- ◆ configuration file **Config files (*.xml)**;
- ◆ events file **Events files (*.xml)**;
- ◆ configuration and events file **Backup files (*.zip)**;
- ◆ configuration file from previous versions **Old config files (*.prc; *.pr\$; *.rtc)**;
- ◆ database file **Data directory zip (*.ddz)**.

Depending on selected format, the system displays different question (Figure 3.5).

A — configuration files



B — events files



C — backup files or configuration files from previous versions

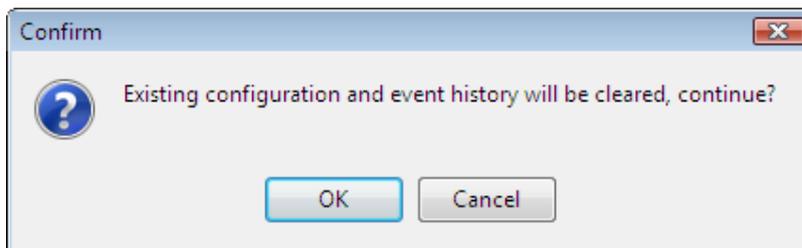


Figure 3.5. Questions on confirming an intent to import data

Depending on the option selected, the system will appropriately import information selected. When data is being imported, the progress bar shows percentage of task completion.



Importing data from external file causes a permanent change to the database content. Before you use this command it is recommended that you make a backup of the current database. Thanks to this you would be able to restore previous data in case of import failure.

3.1.3. Export system settings to file

The **Export system settings to file...** command allows to export current configuration, events or all the database content to external file. When you use this command, the dialog box for selecting a file for data export is displayed (Figure 3.6).

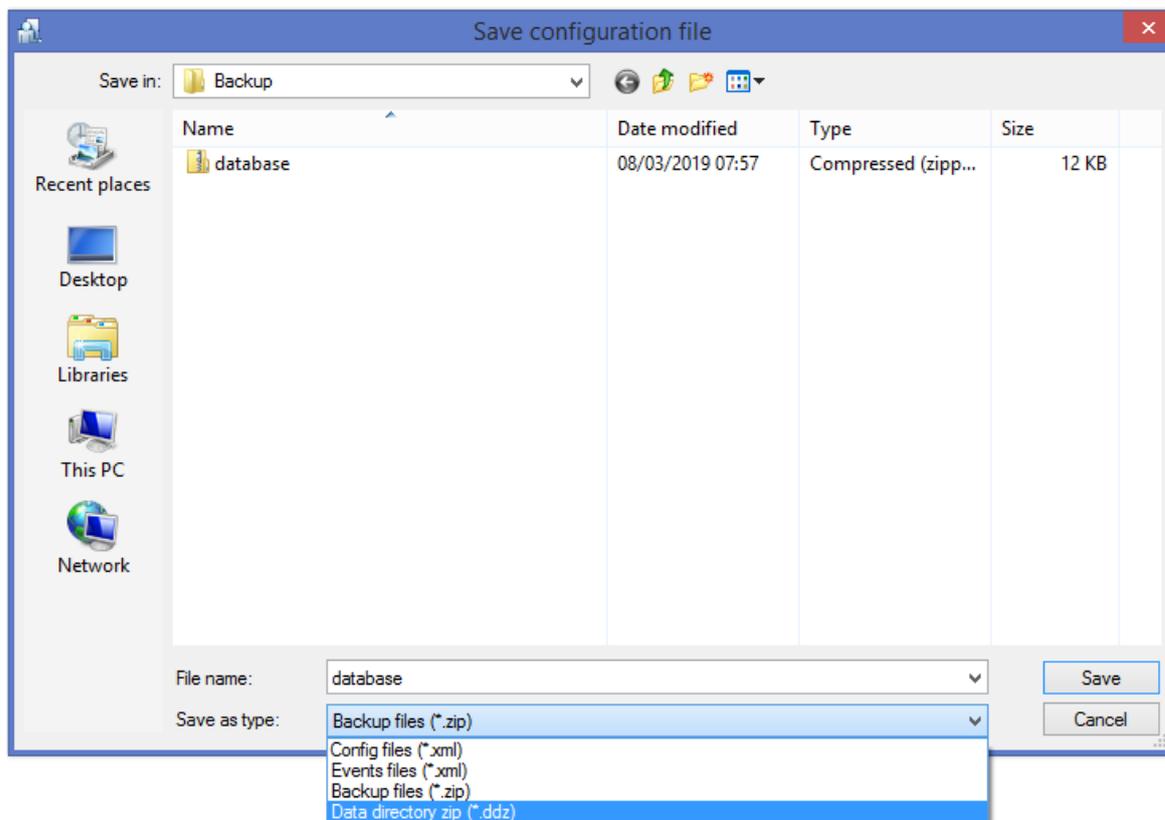


Figure 3.6. **Selecting file to export settings(data) to**

Following files can be selected for export:

- ◆ configuration file **Config files (*.xml)**;
- ◆ events file **Events files (*.xml)**;
- ◆ configuration and events file **Backup files (*.zip)**;
- ◆ database file **Data directory zip (*.ddz)**.

If you select backup file format, you can enter an optional password which is supposed to protect against access to the file by unauthorized persons (Figure 3.7).

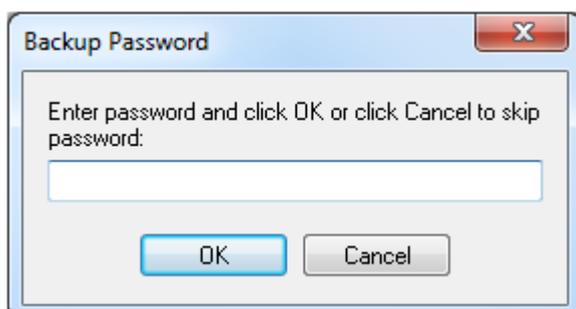


Figure 3.7. **Entering a password to protect the backup file**

3.1.4. Exit

The **Exit** menu will terminate a current program session. Before the system terminates it displays a confirmation question asking if you really want to close the program (Figure 3.8).

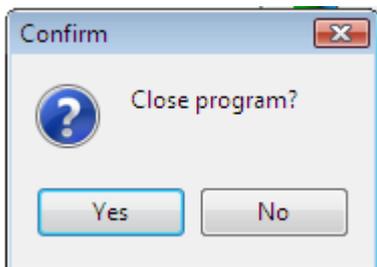


Figure 3.8. Confirmation of an intent to close the program

3.2. SYSTEM MENU

The **System** menu is shown in Figure 3.9.

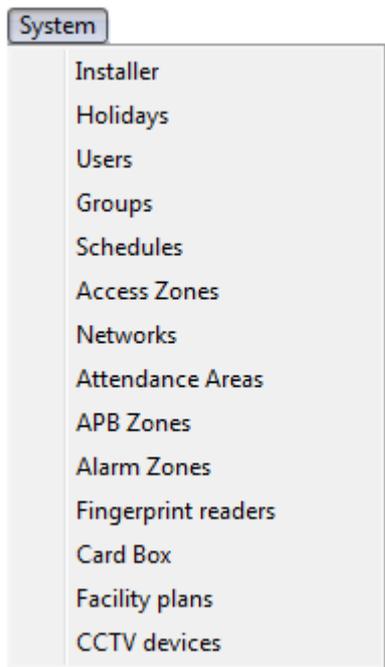


Figure 3.9. System menu

3.2.1. Installer



The **Installer** menu is usable only in regard of PRxx1 series controllers as these controllers can be programmed manually – see [Functional description of PRxx1 series controllers](#).

The **Installer** menu is used for defining the INSTALLER user in the system. Such user has rights to enter the INSTALLER programming mode of PRxx1 series controllers but has no rights to unlock the doors being controlled. This special user has no ID assigned.

If you select the **Installer** command, the **Installer** dialog box appears (Figure 3.10).

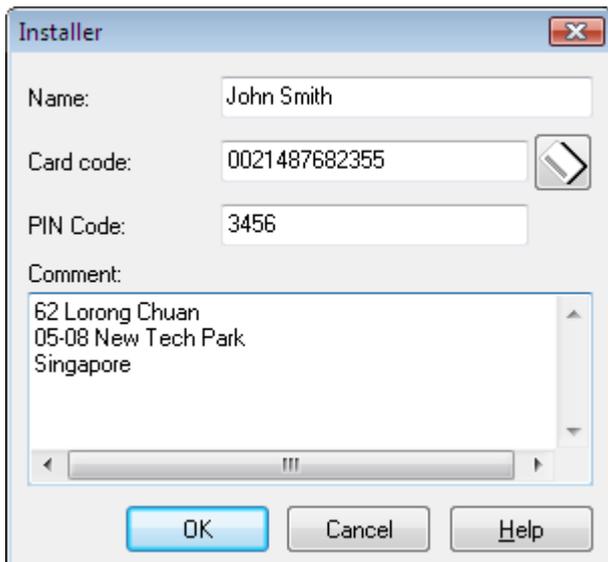


Figure 3.10. A dialog box for defining *INSTALLER* user

The  button next to the **Card code** field enables assignment of card to the *INSTALLER*. In the **Comment** field you can enter any information such as the *INSTALLER* user contact data.

3.2.2. Holidays

There are various types of schedules in the RACS system (general purpose, door mode, identification mode, and so on). They are defined for weekdays. You can find more information on schedules in [section 3.2.6](#). The **Holiday** command is used for defining holidays in current year.

In case of holidays it is possible to define special rules (schedule), that differs from applied weekly schedule. Up to 4 schedules can be used for holidays in particular year. When defining holiday user can define starting and ending date.

If you select the **Holiday** command the holiday directory displays — a dialog box similar to the one shown in Figure 3.11.

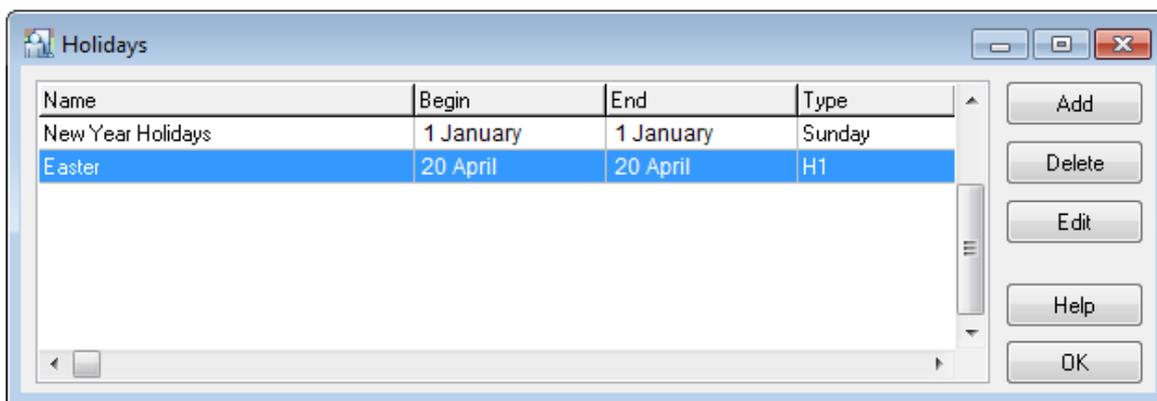


Figure 3.11. Holidays defined in the system

The **Add** button allows for defining a new holiday in the system (Figure 3.12).

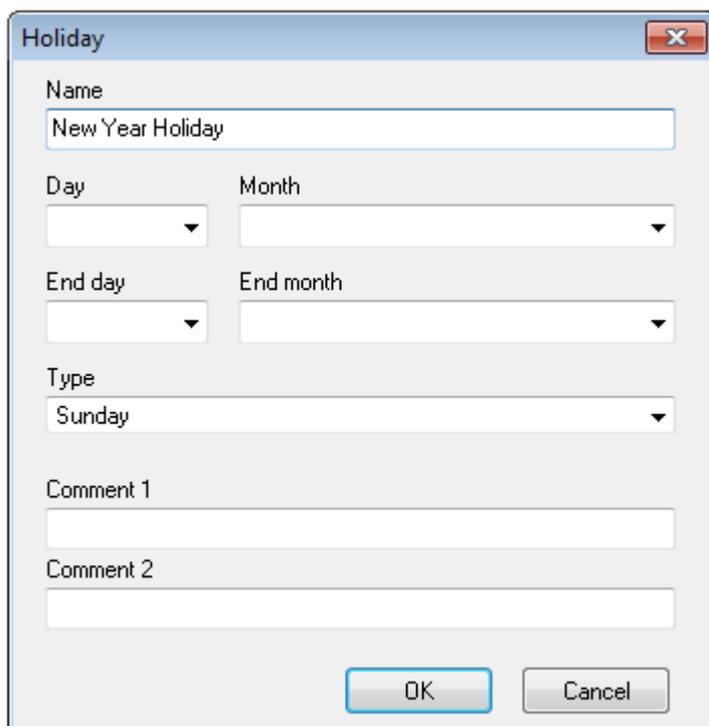


Figure 3.12. *Defining a new holiday*

The **Edit** button makes possible to modify settings for the holiday defined earlier, and the **Delete** button allows for erasing the holiday selected.

3.2.3. Users

There are 4 types of users in the RACS 4:

- ◆ **MASTER** — has right to open doors, arm/disarm controllers and to enter manual programming mode of controllers. It has ID=0.
- ◆ **SWITCHER Full**— has right to unlock doors, arm/disarm controllers. Users of such type can be assigned ID numbers in range of 01–49.
- ◆ **SWITCHER Limited** — has right to arm/disarm controllers. He does not have right to unlock doors. Users of such type can be assigned ID numbers in range of 50–99.
- ◆ **NORMAL** — user of this type can have right to unlock doors. They can be assigned ID numbers in range of 100 – 3999. NORMAL type users with ID above 1000 can additionally have a **Local SWITCHER** attribute, which gives them right to arm/disarm selected controller.

The **Users** command opens the system's user directory (Figure 3.13):

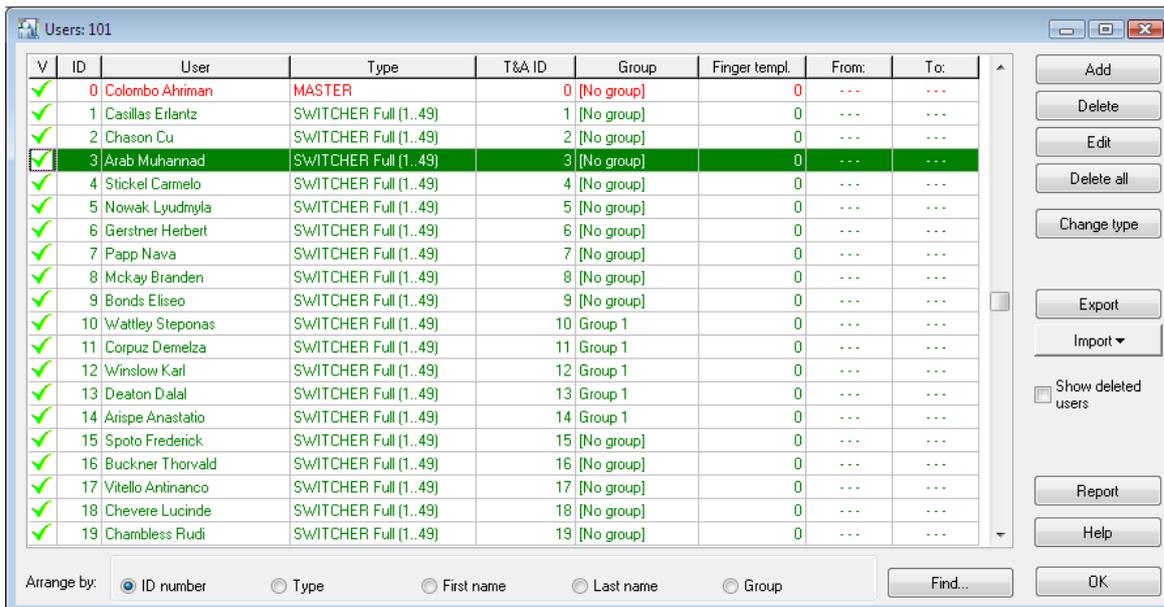


Figure 3.13. System user directory

Using this command you can add new users, delete them, modify their data, change their type as well as sort using various criteria. You can also display users previously deleted, export a list of users defined or import users from an external file. Additionally, from the **Users** window you can generate report containing list of users defined in the system. In the window's header, there is displayed string "Users" and current total number of users (in a case shown in the picture there are 101 users defined). The mark in the **V** column indicates, that a specific user is active. On the other hand, for the inactive users the mark is displayed.

Basic operations available from **Users** directory have been described in the following sections.

3.2.3.1. Adding new user

In order to add a new user to the system, you should click on the **Add** button. The **New user** dialog box displays (Figure 3.14). In this window you can select a specific user type (if you do this, the system will assign to the user a first free ID number from the type selected). You can also enter an ID. In order to do this you need to select a **Select ID** radio button. In such a case the system will specify user type based on entered ID.

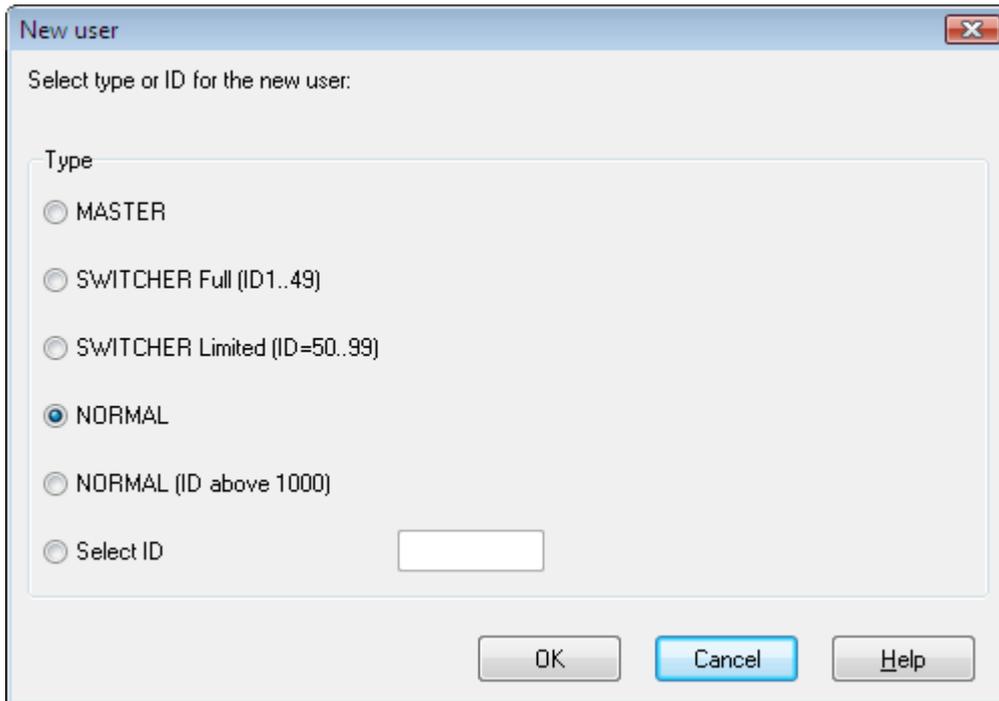


Figure 3.14. *Selecting user type*

If you click **OK** the **User properties** window appears (Figure 3.15).

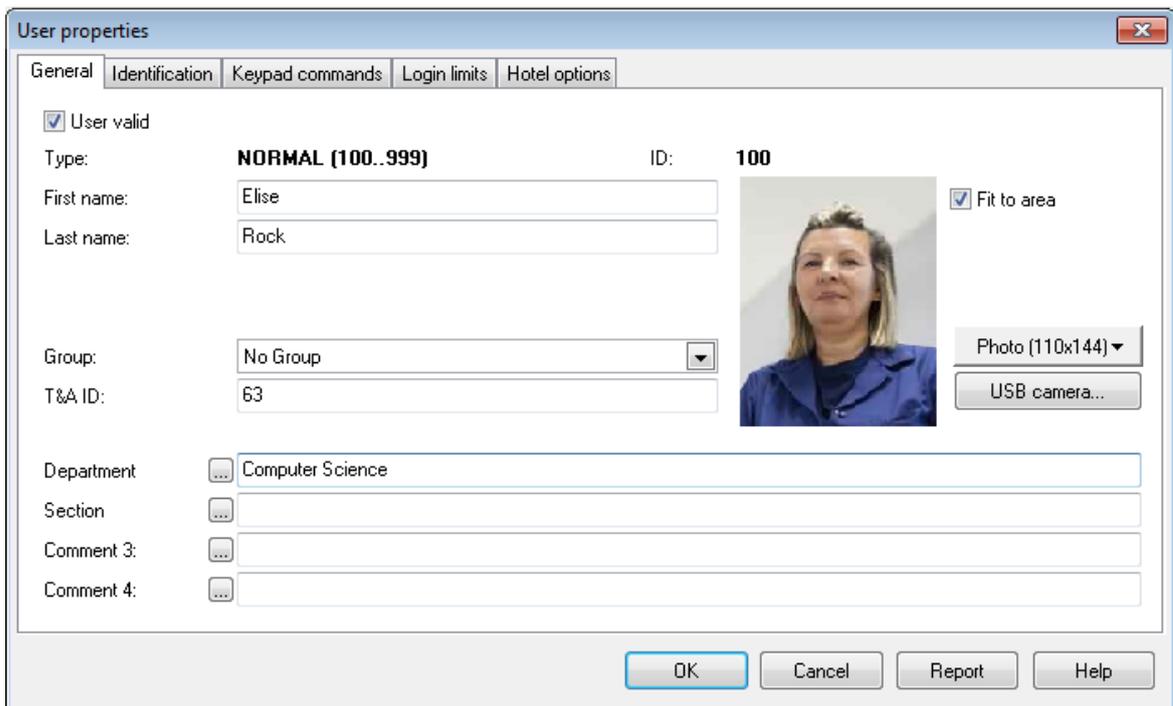


Figure 3.15. *User properties*

The **User properties** window is divided into 5 tabs:

General (Figure 3.15) — general user’s data including first and last name as well as access group, for which access rights are defined. At the bottom of the window, there are four comments fields.

They can be used for storing various information (e.g. Department and Section). In order to change a comment field name, you should click on the  button.

Identification (Figure 3.16) — user identification information — card number, PIN and fingerprint templates.

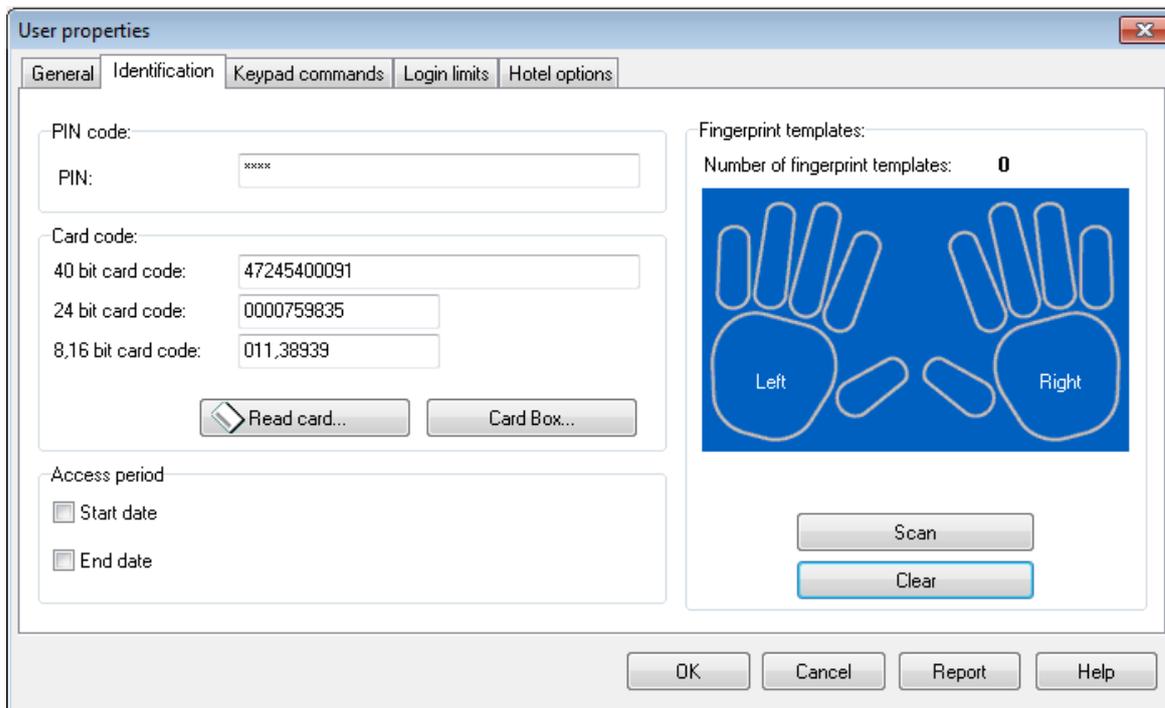


Figure 3.16. *User properties — Identification tab*

In this tab you enter basic data used for user identification. For reading cards you have two buttons at your disposal: **Read card...** and **Card box**. If you select the first one, the controller selection window displays where you can read a card. In some cases, especially when there is no reader in the vicinity of the operator’s console, this option is inconvenient. In such a case you can use the **Card box** command. This command give you access to the directory of cards which were read before. You can find instructions on how to create such a Card box in [section 3.2.13](#). In the **Access period** area you can enter start and end dates indicating a time interval when user identification data are valid. The **Fingerprint templates** area allows for managing fingerprints templates assigned to the particular user. They can be imported from the fingerprints reader by means of **Read from a reader** button (does not apply to RFT1000 reader) or scanned using a selected reader (the **Scan from reader...** button). The **Clear** button can be used for deleting fingerprint templates assigned to the user.

Keypad commands (Figure 3.17) — this is the tab, where you can assign to the user rights for entering keypad commands at particular controllers.

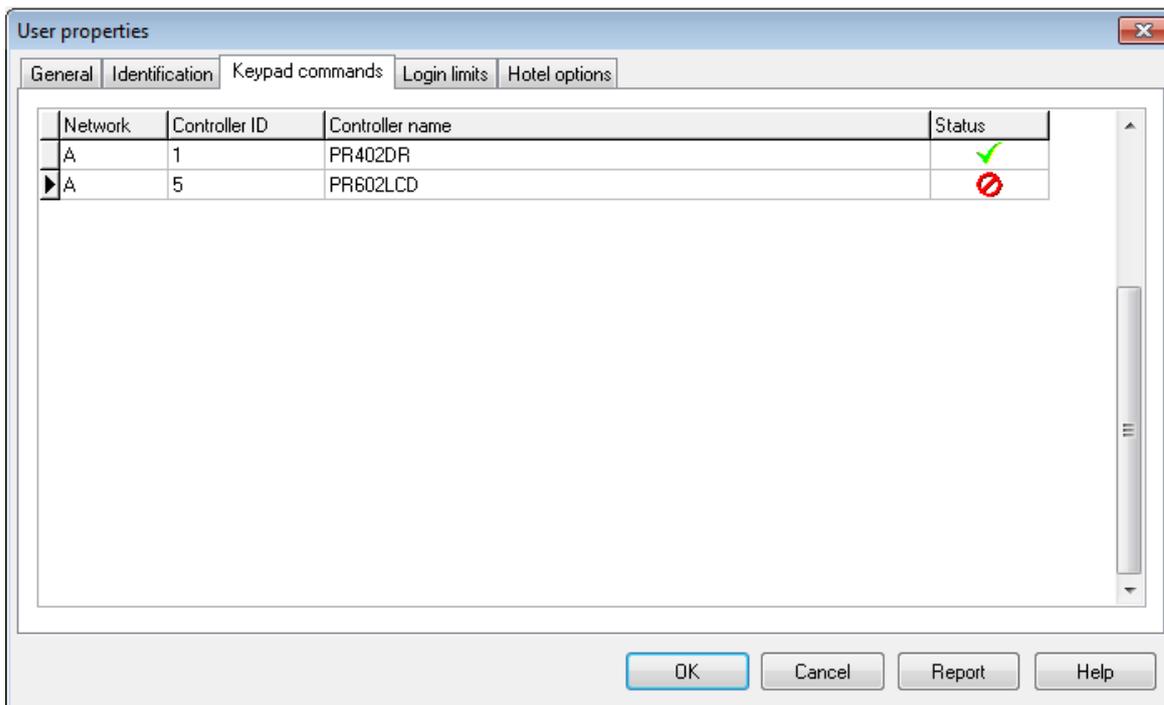


Figure 3.17. User properties — Keypad commands tab

Login limits (Figure 3.18) — this tab enables configuration of login limits for defined user. After you specify login limit, the controller will grant access to the user only specific number of times. Both manually and automatically renewed limits can be configured. More information is given in the document **Functional description of PRxx2 series controllers**. If login limits are modified then it is necessary to update new settings to controller(s).

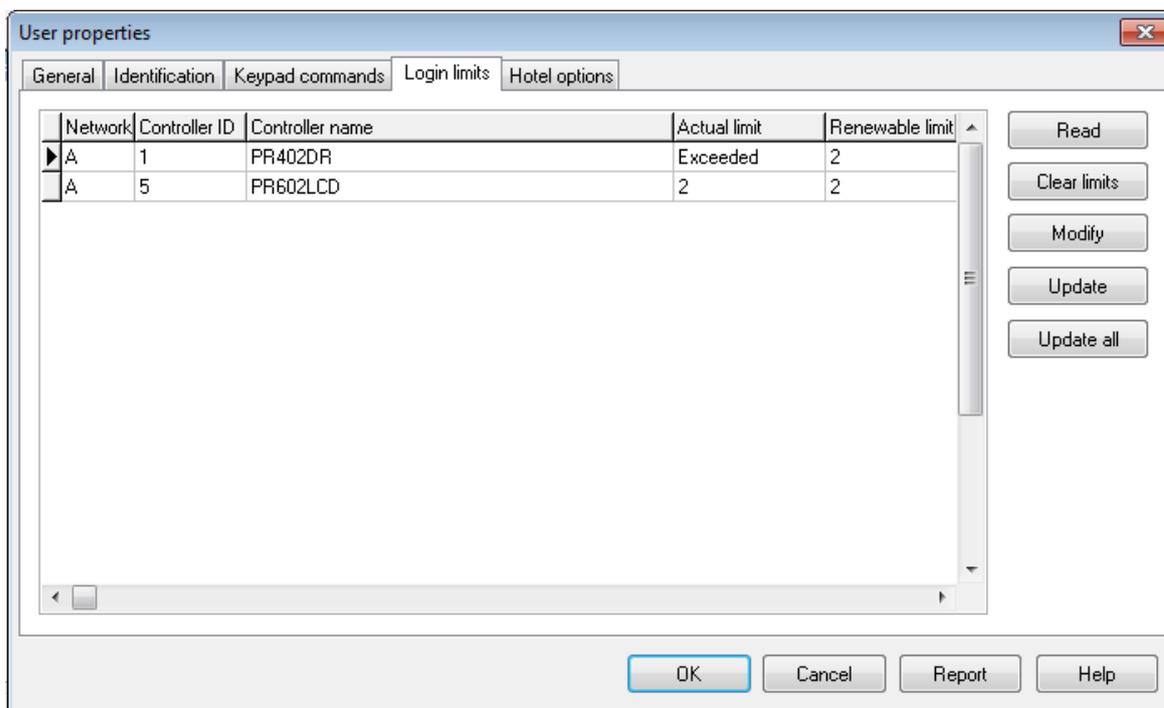


Figure 3.18. User properties — logon limits tab

Hotel options (Figure 3.19) — window which allows to specify that selected user is a hotel guest and to assign a guest number in selected hotel room.



Hotel room options are mainly dedicated to PR821-CH and PR621-CH controllers and also for standard PRxx1 series controller.

It is recommended to use **Guest** command to enrol guests in the system – see **section 3.2.4**

In order to define a „hotel room“ you need to invoke controller’s properties window, and select the **Hotel room** option.

In order the hotel options have effect, you need to send configuration to controller.

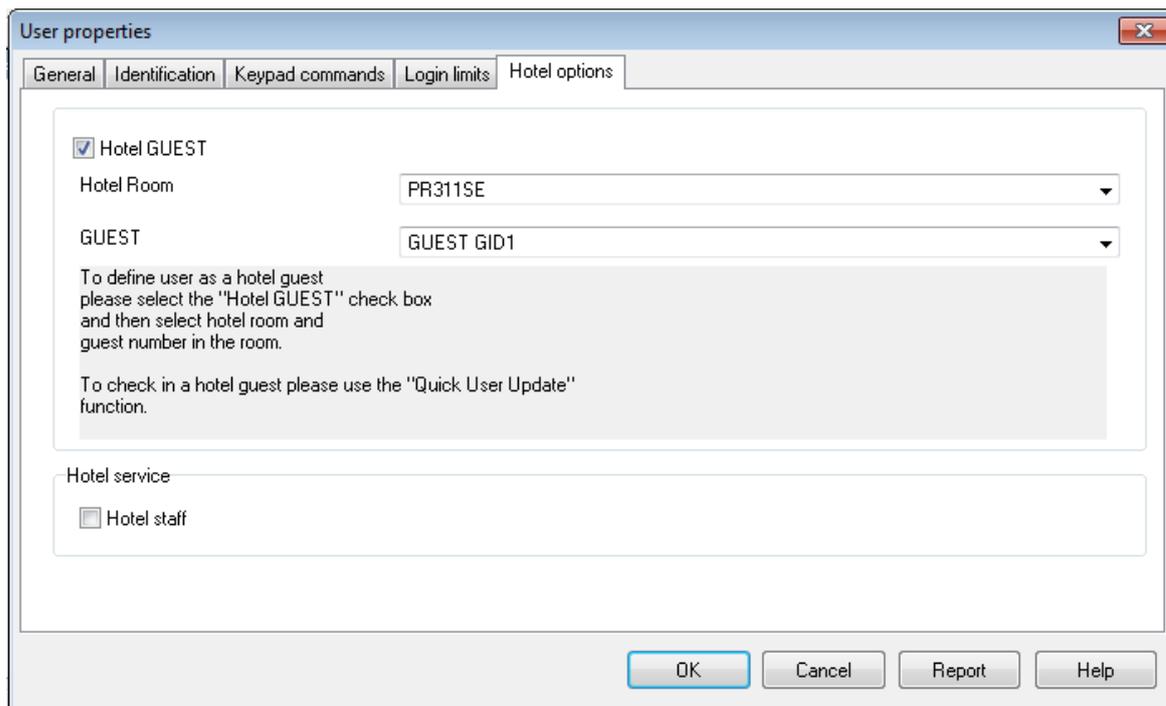


Figure 3.19. User’s properties — Hotel options tab

3.2.3.2. Deleting users

You can delete user by using **Delete** button from users directory. When you click the button, the dialog box appears for confirming your intent to delete the user (Figure 3.20).

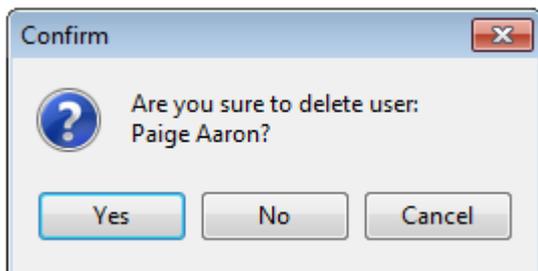


Figure 3.20 Confirming user deletion

If you click **Yes**, the user will be deleted. Before the user is deleted, the PR Master will ask you if the card assigned to the user being deleted should be returned to the Cardbox so that it could be assigned to the other user.

You also have a possibility to delete all the users defined in the system. If you want to perform such operation you should click on the **Delete All** button. Clicking on this button causes displaying dialog box with a question for confirmation your intent to delete all users (Figure 3.21).

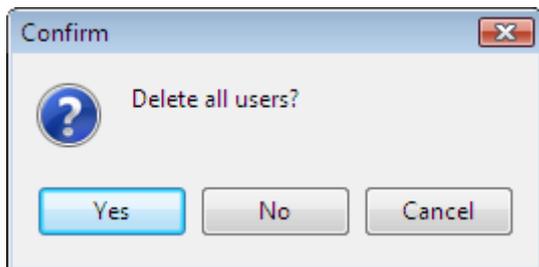


Figure 3.21 Confirming the intent to delete all users from the system



In order to protect yourself against the possibility to permanently delete all the users from PR Master's database, you should make sure, that the system's backups are made regularly. To protect users' data you can also export users list. It can be done using an **Export** button in the **Users** directory.

3.2.3.3. Finding users

The **Find** button in the **Users** directory lets you search for particular user data. This option is especially useful if there are many users defined in the system. Clicking on the button causes displaying a **Find user** window (Figure 3.22), where you can search for users by first or by last name. As you enter the last (first) name in the textbox, the system automatically sorts users using the field selected and finds the first record which applies to the searching criteria entered.



Figure 3.22. Searching for user data

3.2.3.4. User list export and import

For exporting and importing user list, the **Export** and **Import** buttons in the **Users** directory can be used respectively. After you select the **Export** command, the **Exporting users to a file** dialog box displays. You should select there a file to export data to. On the other hand, the **Import** button lets you import user data from the list which was exported before.

3.2.3.5. Generating user report

After entering all users data, you may want to generate a printed report. This is a good way to document information entered to the system. The **Report** button in the **Users** directory can be used exactly for this purpose. If you click on it, the **Users** report in the **Report** window appears (Figure 3.23).

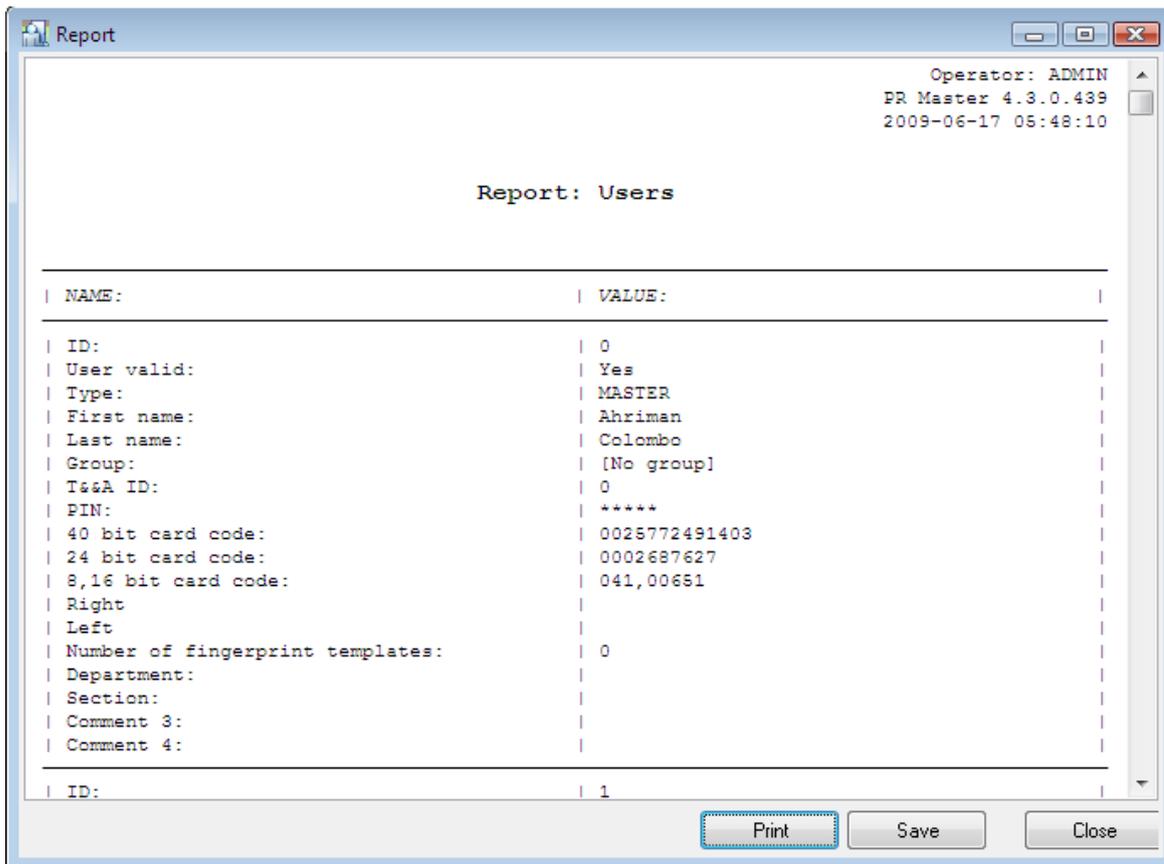


Figure 3.23 The “Users” report

From the **Report** window you can print the report on the printer selected (the **Print** button). The other option is to save the report to a file (the **Save** button).

3.2.3.6. Displaying and erasing previously deleted users

The **Show deleted users** checkbox allows for displaying users who were deleted from the system. If this checkbox is selected, then all the users (both existing and deleted) are displayed in the **Users** directory but deleted users are crossed out (Figure 3.24). Deleted users do not occupy available range of IDs and are still associated with events recorded in the past. Starting from PR Master 4.5.22 and according to GDPR it is possible to remove deleted user from the system with **Delete** button. Such removing erases the user completely from the system including the association with registered events.

In case of large number of deleted users it might be useful to erase them permanently from database to improve its efficient operation. When **Show deleted users** is selected then **Remove deleted** enables erasing of all deleted users.

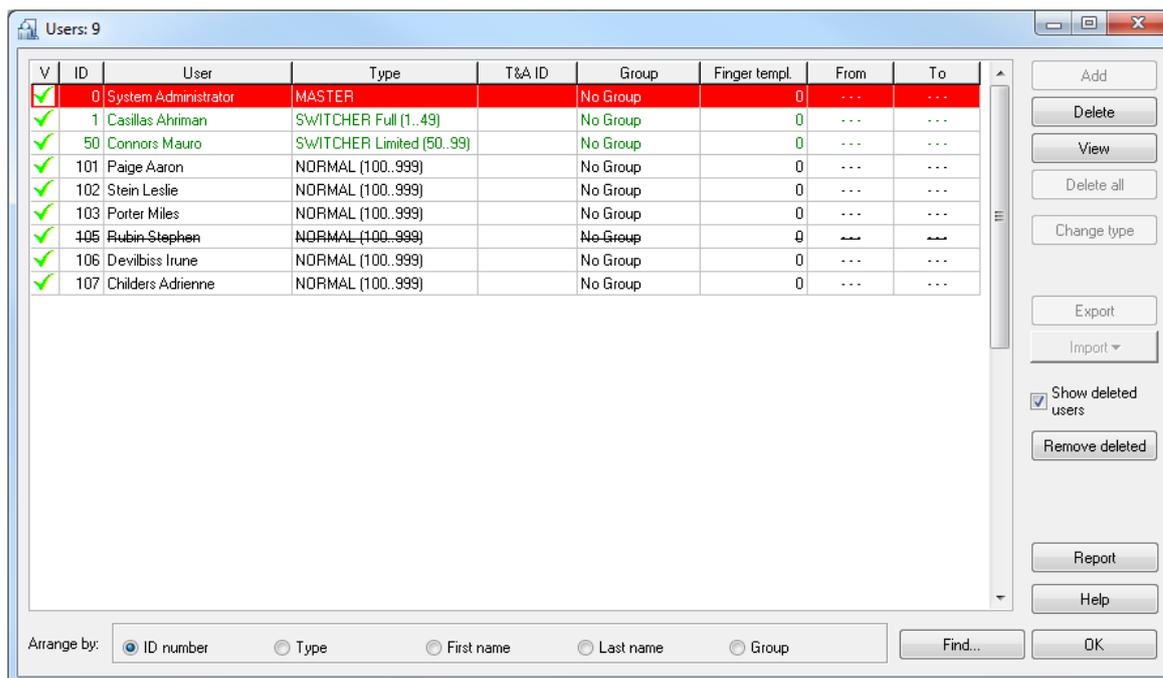


Figure 3.24. The users list together with deleted users data

3.2.4. Guests

The **Guests** command compared to **Users** command enables defining of special category of users (i.e. Guests) in RACS 4 system in simplified and quicker way because it does not require sending all settings to controllers. The command is dedicated to hotel systems based on PRxx1 series access controllers (particularly PR681-CH and PR621-CH controllers equipped with card holders) within RACS 4 system. In order to enable Guest adding it is necessary to activate the option **Hotel room** in controller properties in **General** tab. On the other hand if quick enrolment of any type users is required in the system with any Roger controllers then **Quick User Update** command (see [section 3.5.2](#)) can be used.

The **Guest** command opens the directory (Figure 3.25), which shows NORMAL type users with Guest attribute. In the window shown in the figure, Guests can be added, deleted and modified. It is also possible to sort Guests in regard of ID number, first name, last name, room name and group.

After selection of **Add** button Guest properties window is displayed and there is no need to select user type because NORMAL type is assigned by default. New window is developed on the basis of user properties window, therefore elements in **Guest properties** window basically are used in the same way as elements from **User properties** window (Figures 3.15 to 3.19). Following differences must be noted:

- ◆ it is necessary to use RUD-2 or RUD-3 reader when **Read Card...** button is used for reading Guest card number
- ◆ it is possible to specify default group in **Group** field (see [section 3.2.5.1](#))
- ◆ it is possible to specify default check-out time in **To** field (see [section 3.5.11.4](#))

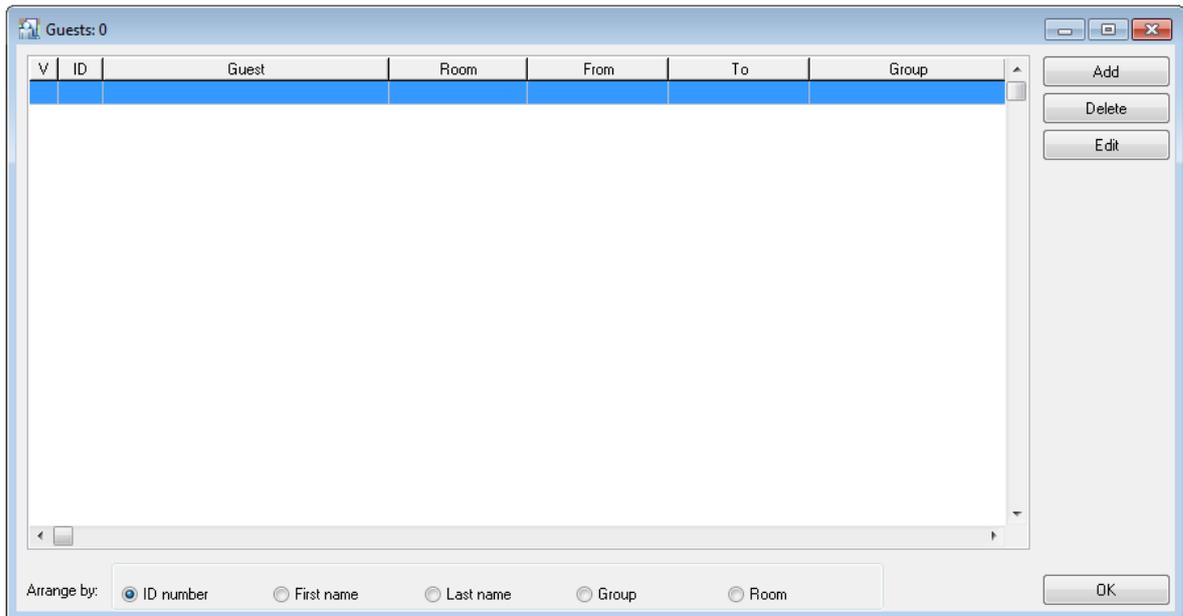


Figure 3.25. Directory for Guest type users

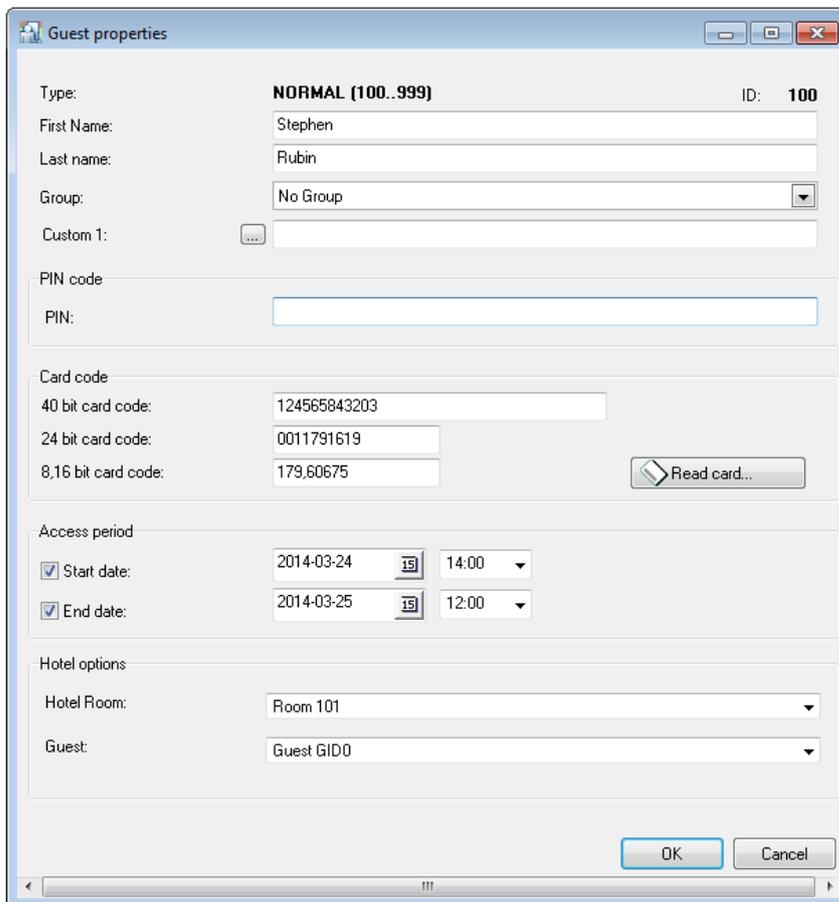


Figure 3.26. Guest properties

3.2.5. Groups

Users in the RACS 4 can be divided into 250 groups. Every user can be assigned to one of them. Users belonging to the same group have the same access rights for rooms and floors. Defining access rights in the RACS 4 requires defining when and where the users belonging to system's groups will be given access. For every group you can also define rights for 32 floors (0–31) in up to four elevators. The rights to the floors cannot be restricted by time schedules.

A newly registered user in the system can be assigned to two built-in groups i.e. so called **No Group** and then he has rights to enter all the rooms and floors without any time limitations or **No Access Group** and then he has no access rights. Administrator can define his own user groups and assign users respectively

Users assigned to the group **No group** have no access to rooms only when:

- ◆ the input line configured as **Locked door mode** is triggered
- ◆ the controller has the door mode **Door Locked**
- ◆ if the controller is in the Armed mode and at the same time the option **Access disabled when controller armed** is activated

If you use the last of mentioned conditions, then you can achieve such effect that users who were not assigned to any group (the **No group** setting) can be temporarily blocked as long as the controller is in the armed mode and are given access again when the controller is in disarmed mode).

The **Group** command opens the system's group directory (Figure 3.27):

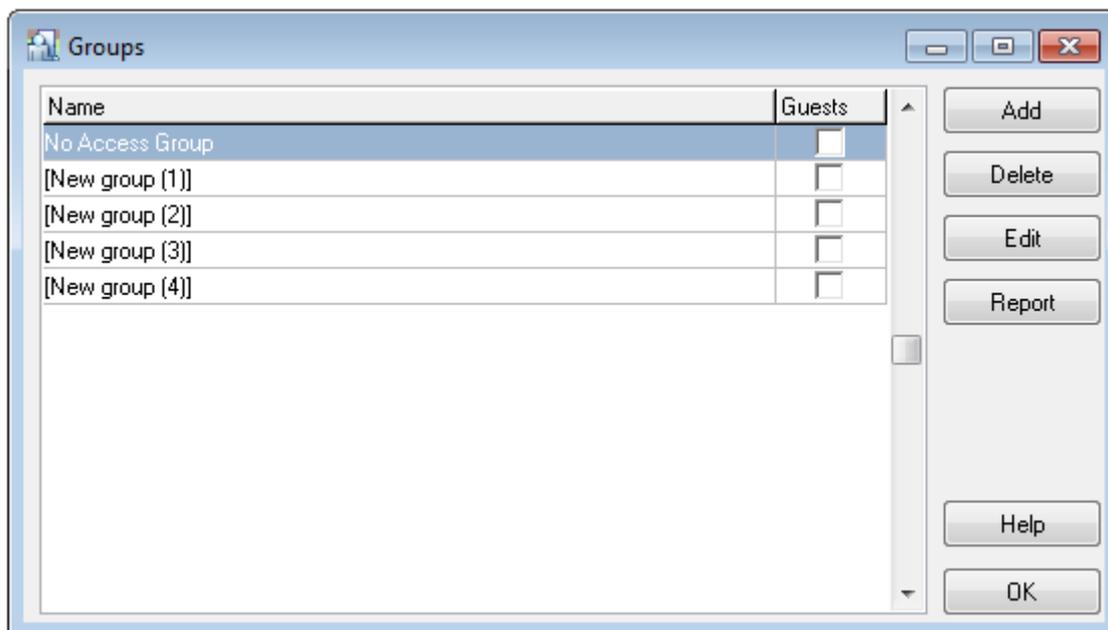


Figure 3.27. Group directory

Groups enable defining of access rights in the RACS 4. Terminals (readers) connected to controllers form so called access zones (see [section 3.2.7](#)). Users are assigned to groups, and groups have access rights to zones based on selected schedules (see [section 3.2.6](#)). Therefore you can specify, for instance, that user John Smith belonging to the group **Technicians** has access to the **Garage** zone from Monday to Friday from 7.30 AM to 3.30 PM.

In order to properly define a group, you should firstly define access zones and secondly define time schedules. Then you should define access rights for group members in the specific zones, according

to the time schedules assigned to them. On top of that you can also define group’s rights to specific floors (if the ACS is controlling access to floors). If you perform all the operations listed above, the only thing to do is to assign users to the defined group. Users belonging to the group have all the rights defined for this group.

3.2.5.1. Adding new group

In order to add a new group, you need to click on the **Add** button in the Group directory (Figure 3.27). The **Group properties** window appears (Figure 3.28). Using this window you can define the name for a group, enter descriptive comments and specify group’s access rights for access zones defined in the system. By default, new group has no access rights in the access zones defined in the system (for every access zone there is the **Never** schedule assigned). Optionally you can also select the checkbox **Default Guest group** in order to mark this group as default group when guest is added by means of **Guests** option (see [section 3.2.4](#)).

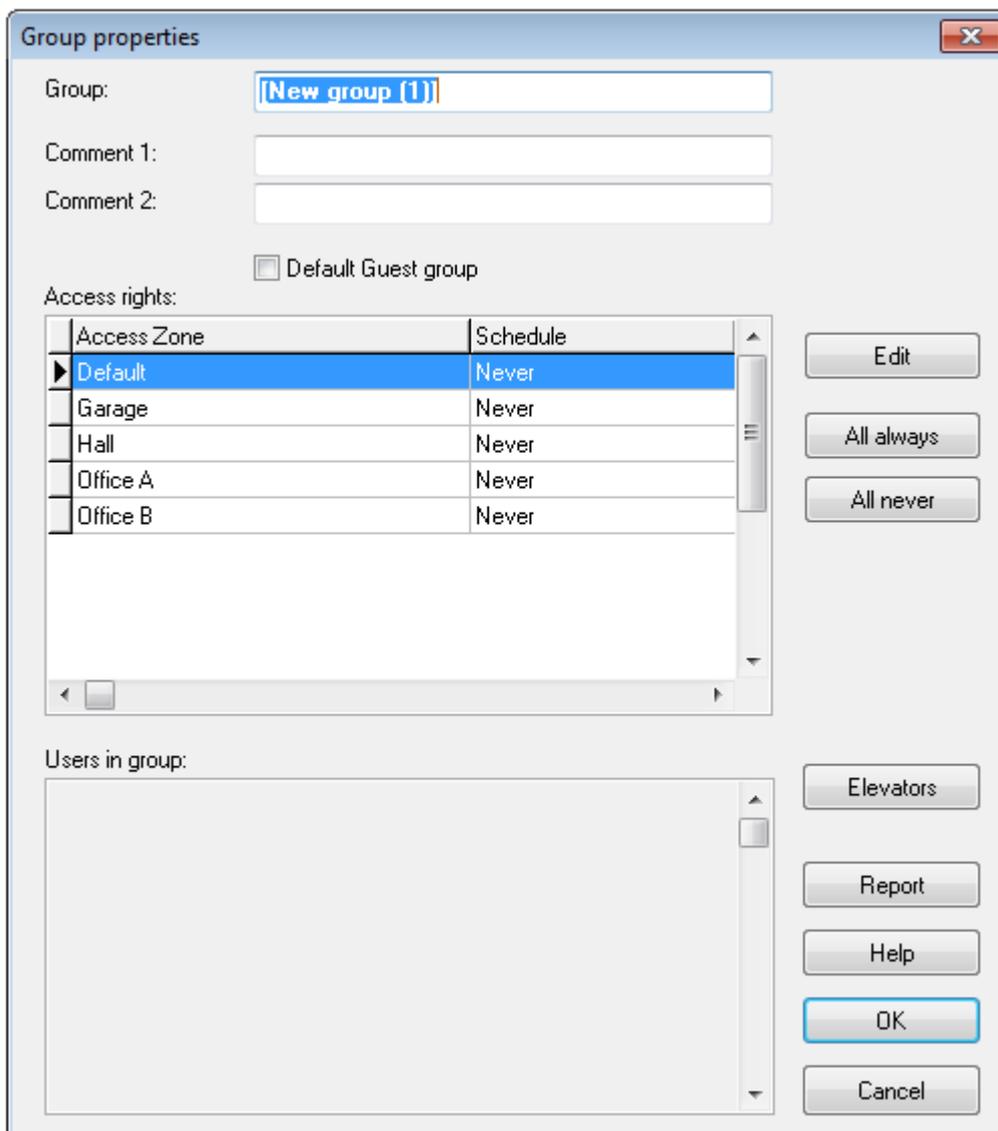


Figure 3.28. Group directory

In the **Group** field you should enter a group name. By default the system assigns the name **New group(#)**, where **#** is a consecutive group number. In fields **Comment 1** and **Comment 2** you can enter any group description.

In order to change a time schedule for all access zones from **Never** to **Always**, you should click on the **All Always** button. On the other hand, clicking on the **All Never** button, assigns **Never** schedule to all access zones. You can also assign other schedules for individual zones. The **Edit** button serves this purpose.

The **Elevators** button opens **Access to floors and elevators dialog box** (Figure 3.29).

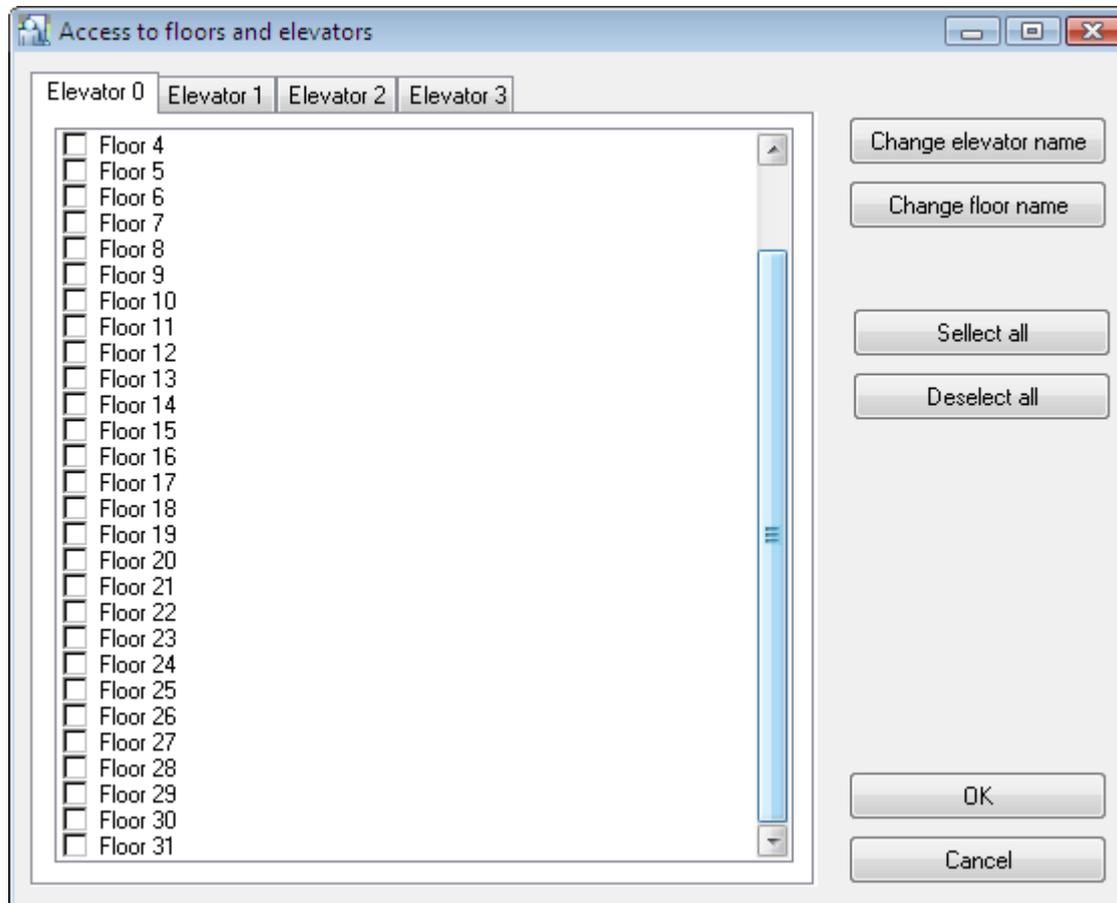


Figure 3.27. *Defining access to floors and elevators*

This dialog box is divided into four tabs with default names **Elevator 0**, **Elevator 1**, **Elevator 2**, **Elevator 3**. These names can be changed using the **Change elevator name** button. Particular floors are labeled with default names **Floor 0..Floor 31**. In order to change particular floor name you should select it and use the **Change floor name** button. In order to define specific group's access rights to the selected floor, you should check the checkbox bound to it. The **Select all** button selects all the floors, and the **Deselect all** unselects all the floors.

In order to use access control in elevators you need to use PRxx2 series controllers and XM-8 expanders. Moreover XM-8 expanders need to be activated in controller properties, in the tab **Options**.

After defining all the access rights for the group selected, you can generate report, where all the access rights for the group selected will be listed. In order to do this, you should click on the **Report** button in the **Group properties** dialog box. The **Report window** with the **Access rights** report displays (Figure 3.30).

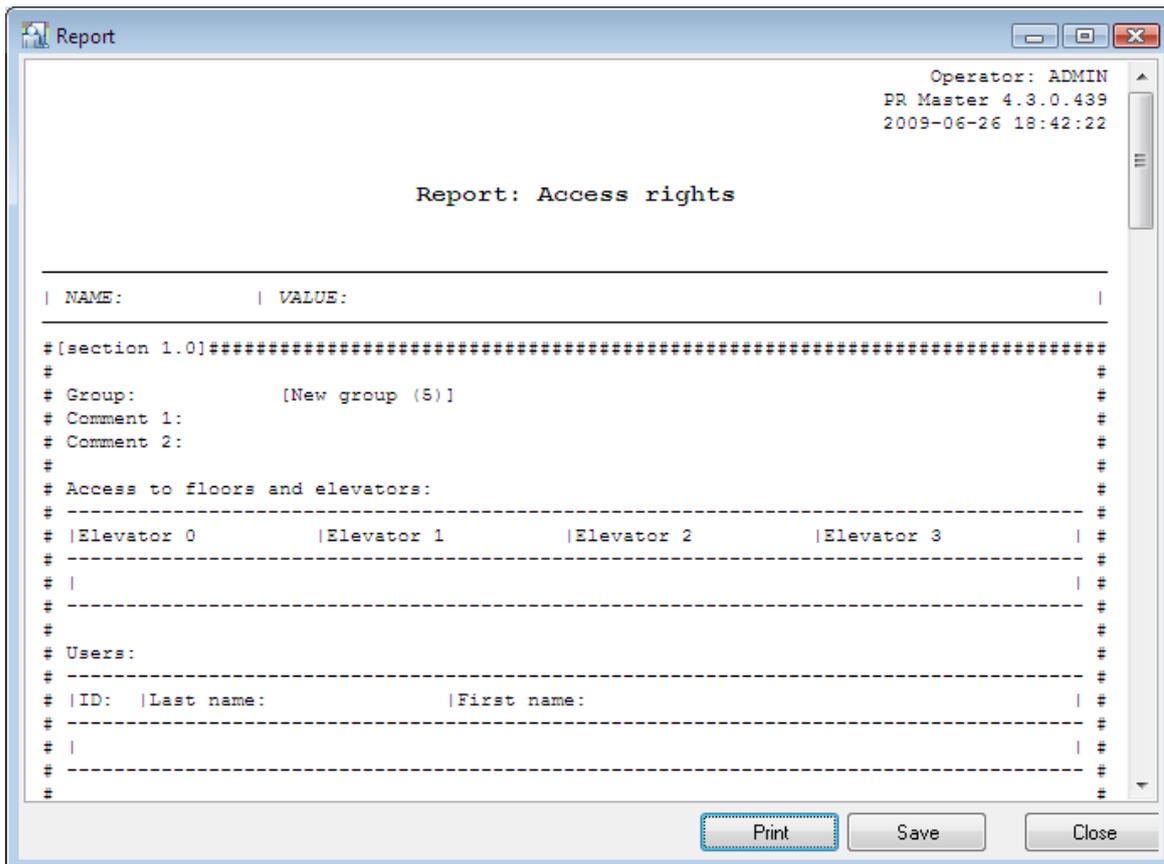


Figure 3.30. The Access rights report

3.2.5.2. Assigning users to groups

In order to assign an user to a group, you should make use of the users directory. After you select the **Users** command from the **System** menu (or when you click the **Users** icon in the **System** pane of the main program's window), you should select the user and then click on **Edit** button. In the **User properties** dialog box, in the **Group** list box on the **General** tab, you should select group, the selected user belongs to. After you make all the changes you should click **OK**.



The procedure described applies to the situation where a group has been defined after the users directory was created. However, more conveniently would be to create groups first, and assign them to users when users data is entered to database.

When users are assigned to groups, you can display list of users belonging to particular group. In order to do this, you can open a group directory and click on the **Edit** button. The **Group properties** window appears (Figure 3.31).

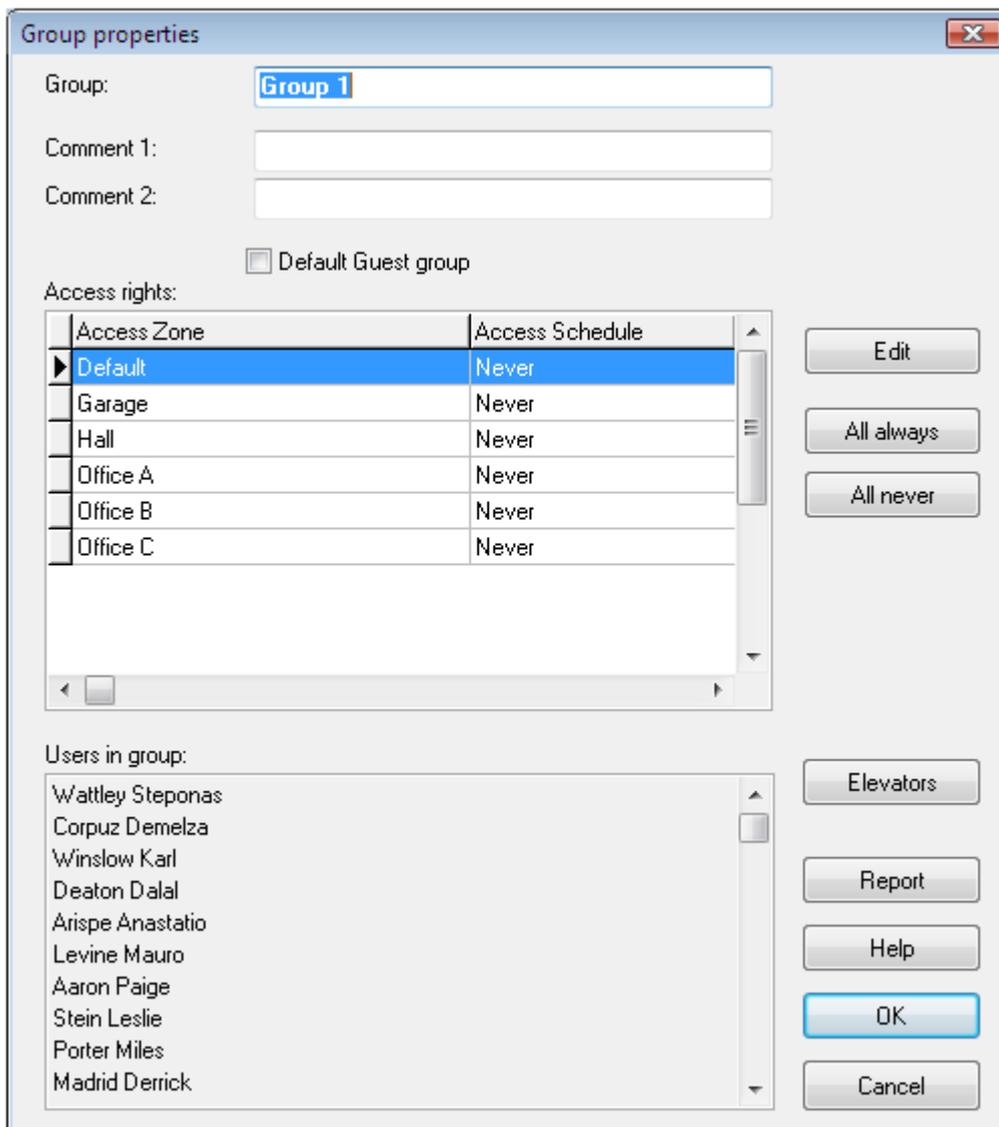


Figure 3.31. *Editing group's properties. In the Users in group area the list of users belonging to the group is displayed*

3.2.5.3. Deleting groups

In order to delete group, you should click on the **Delete** button in the **Groups** dialog box. Before the group is deleted, the **Confirm** dialog box appears. There you can confirm or cancel your intent to delete the group. After the group is deleted, users who belonged to it before, are assigned to the group **No group**.

3.2.5.4. Generating groups report

After you enter all data for all groups, you may want to generate a printed report. This is a good way to document information entered to the system. The **Report** button in the main window of the group directory can be utilized for this purpose. If you click on it, the **Group** report will appear in the **Report** window (Figure 3.32).

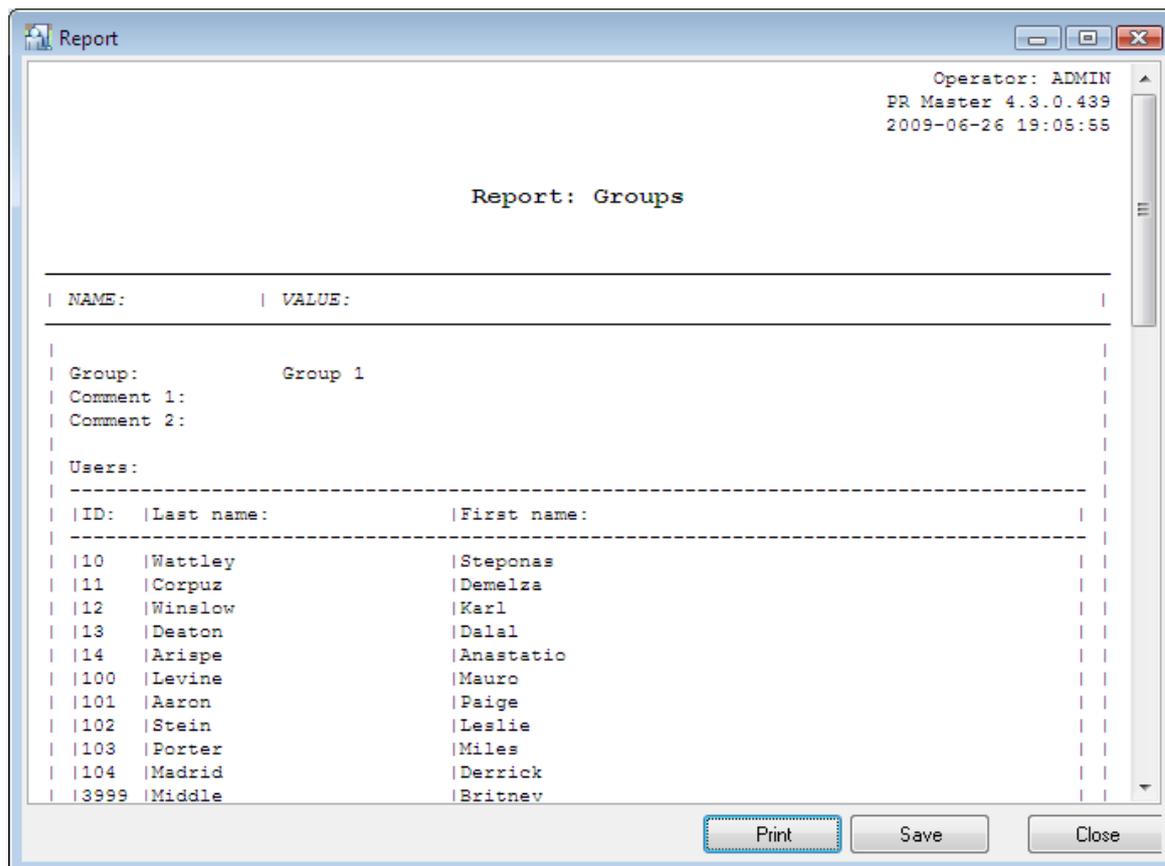


Figure 3.32. Groups report

3.2.6. Schedules

A schedule is a set of rules with From... - To... time intervals. Time intervals are defined for every weekday (from Monday to Sunday) and separately for holidays (H1, H2, H3 and H4). There are 5 schedules types in the RACS 4:

- ◆ general purpose,
- ◆ T&A mode,
- ◆ APB reset,
- ◆ door mode,
- ◆ identification mode.

For managing schedules in the RACS 4 the **Schedule** command is used. When you select this command, the dialog box shown in Figure 3.33 appears.

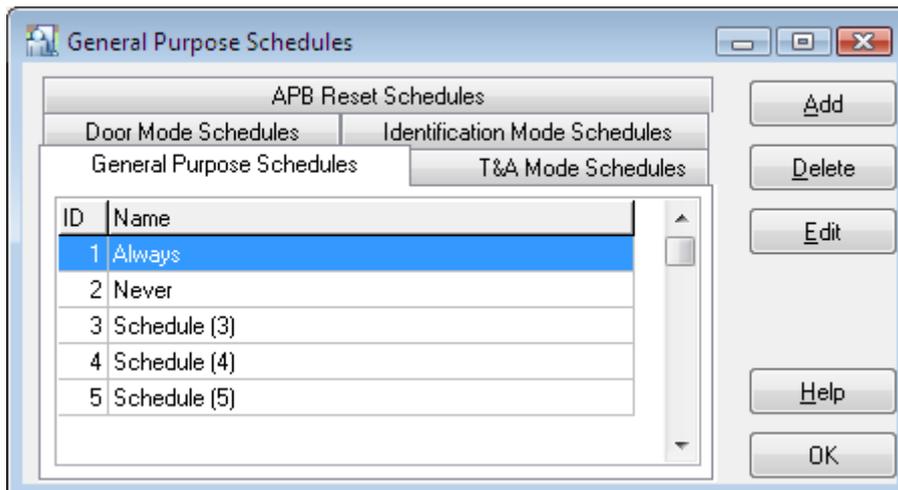


Figure 3.33. Schedule management

The window is divided into tabs with names of schedules types available in the RACS 4. You can add a new schedule (the **Add** button), remove a schedule (the **Delete** button) or modify its properties (the **Edit** button).

3.2.6.1. General purpose schedules

A general purpose schedule can be assigned to one or more control functions in the controller. For instance, the same schedule can be assigned for controlling access rights of access group, controlling an output line or for blocking an input line.

By default there are two general purpose schedules in the RACS 4: **Always** and **Never**. These schedules can neither be erased nor modified.

General purpose schedules are used for:

- ◆ access rights to zones — for example you can define an access right for the **Technicians** group to the **Garage** zone from Monday to Friday from 8.00 AM to 4.00 PM;
- ◆ two user mode — you can define time intervals when two user mode is effective — in this mode, two users with access rights need to identify in order to get access to room;
- ◆ Facility Code function – you can define time intervals when Facility Code functionality is effective;
- ◆ input lines activity;
- ◆ output lines activity;
- ◆ high security mode – you can define time intervals when two readers must be used by user with access rights in order to get access.

In order to add a new general purpose schedule, you should select the **General Purpose Schedules** tab in the schedules directory, and click on the **Add** button. The **Schedule** dialog box appears where you can define a new schedule (Figure 3.34).

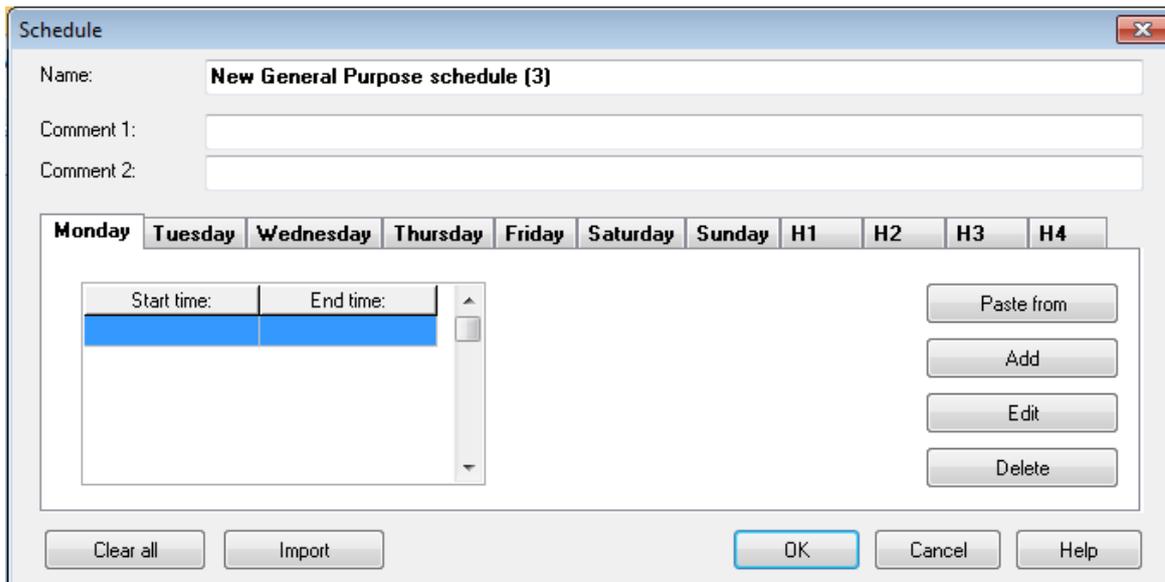


Figure 3.34. Defining a new general purpose schedule

In the **Name** field you can enter a schedule name. In fields **Comment 1** and **Comment 2** you can enter any descriptive comments. The **Add** button can be used for defining a new time interval. When you click the button, the dialog box **Time period** appears, where you enter start and end times. Time intervals should be defined for all the weekdays for which the schedules is to be applicable. In order to do this you should click on the specific weekday tab (**Monday..Sunday**) or the holiday (**H1..H4**) and enter a time period which should be applicable. You can also use the **Paste** button, which allows for copying time intervals from another weekday. The **Delete** button erases time interval selected. If you want to delete all the time intervals, you should use the **Clear all** button. The **Import** button lets you import schedule settings from another general purpose schedule. The schedule definition should be confirmed by clicking **OK** button.

3.2.6.2. T&A mode schedules

Time and attendance mode schedules (T&A) allow the controller to automatically switch between different T&A registration modes. T&A modes are used if PR Master software is used in connection with RCP Master software for T&A purpose.

T&A schedule controlling T&A registration describes time intervals (weekdays and times) when the particular T&A registration mode applies. Thanks to this, the identification point in the controller can be used for registering different entrance and exit types depending upon requirements.

The schedule controlling T&A registration mode is defined in a similar fashion to any other schedules. You only need to indicate the event type (entry, exit, on-duty exit, etc.) which should be logged when the schedule is applicable (Figure 3.35).

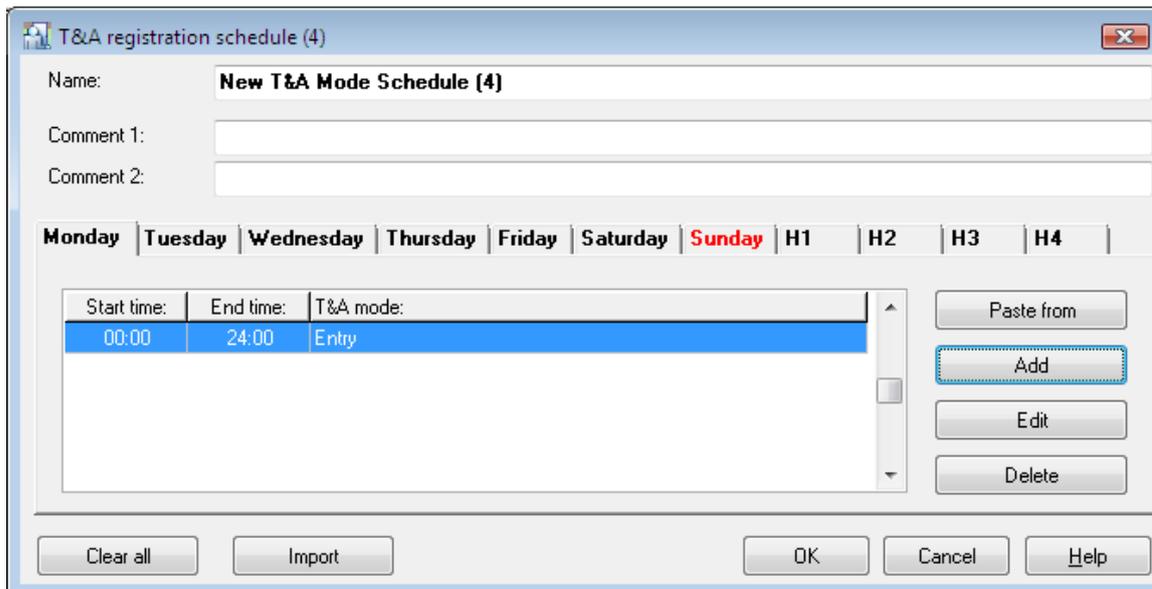


Figure 3.35. Defining a new T&A mode schedule

By default there is **Always in Default T&A Mode** schedule defined in the PR Master. This schedule can neither be erased nor modified.

3.2.6.3. APB reset schedules

The purpose of the Anti-Passback feature is to protect against the possibility to use proximity card of the user at entry to the zone if it had not been used at exit before. To put it differently, the user can not enter the APB zone if he had not left it before. The function is aimed to protect against the possibility that one user passes its card to another user to allow him to enter the zone. More information on APB is given in the document **Functional description of PRxx2 series controllers**.

APB Reset Schedules are used for resetting status of this function. Directly after the reset, every user registered on the controller has unspecified status in the APB registry (it can not be said if his last login was on entry or on exit). Because of that, every user can use his credentials both on entry and on exit. From the moment the status was reset, the controller begins to enforce a need to follow APB rules.

APB reset schedules are defined in similar fashion to general purpose schedules. Except for time interval you need to define specific time, when APB register is to be reset (Figure 3.36).

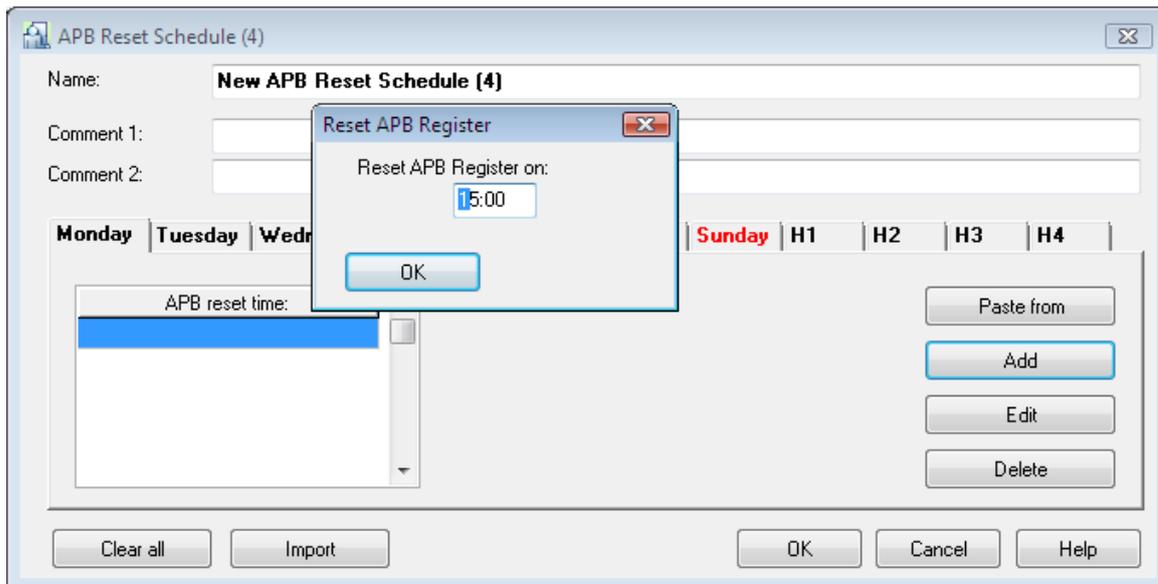


Figure 3.36. Defining a new APB reset schedule

By default there is one APB Reset schedule named **Never** defined in the PR Master. It means, that the APB function will never be reset. This schedule can neither be erased nor modified.

3.2.6.4. Door mode schedules

There are following special door modes in the RACS 4:

- ◆ **Cond. Unlocked** — door is locked until opened by the first authorized person.
- ◆ **Unlocked** — door is unlocked for all.
- ◆ **Locked** — door is locked for all.

Beyond the periods when special mode is in force, the door works in a Normal mode i.e. it is locked for all user without access rights.

The door mode schedule allows the controller to automatically switch between different door mode schedules. When defining this type of the schedule you need to specify time intervals and indicate door mode which should be applicable in the interval selected.

Adding a new schedule is done in the same manner as for general purpose schedule. The difference is that when you edit a time interval, you need to define a door mode (Figure 3.37).

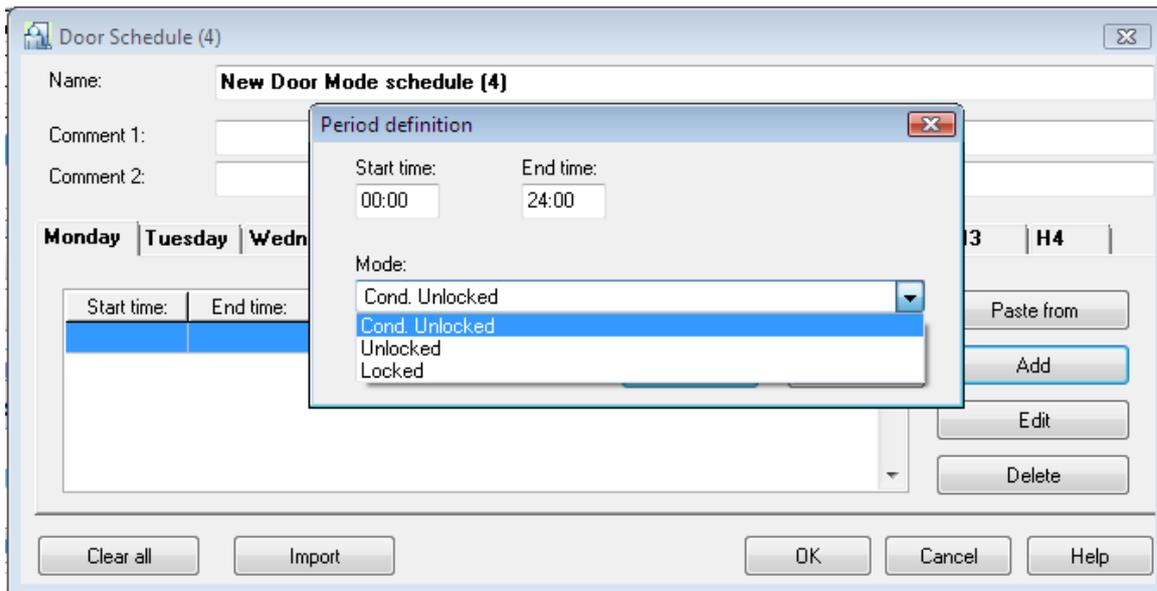


Figure 3.37. Defining a new door mode schedule

Default **Always in Normal Door Mode** schedule is defined and used in the PR Master unless administrator defined door mode schedule is selected and assigned. This default schedule can neither be erased nor modified.

3.2.6.5. Identification mode schedules

The following identification modes can be defined in the RACS 4:

- ◆ **Card or PIN** — user can use a card or a PIN code for authentication. He can use one or the other.
- ◆ **Card only** — users can use cards only for authentication.
- ◆ **PIN only** — users can use PINs only for authentication.
- ◆ **Card and PIN** — in order to successfully authenticate, user must use both his card and PIN.

The identification mode schedule allows the controller to automatically switch between different identification mode schedules. When defining this type of the schedule you need to specify time intervals and indicate identification mode which should be applicable in the interval selected.

Beyond the periods the identification mode specified is in force, the default identification mode selected in the controller’s properties is applicable.

Adding a new schedule is done in the same manner as for general purpose schedule. The difference is that when you edit a time interval, you need to specify the identification mode (Figure 3.38).

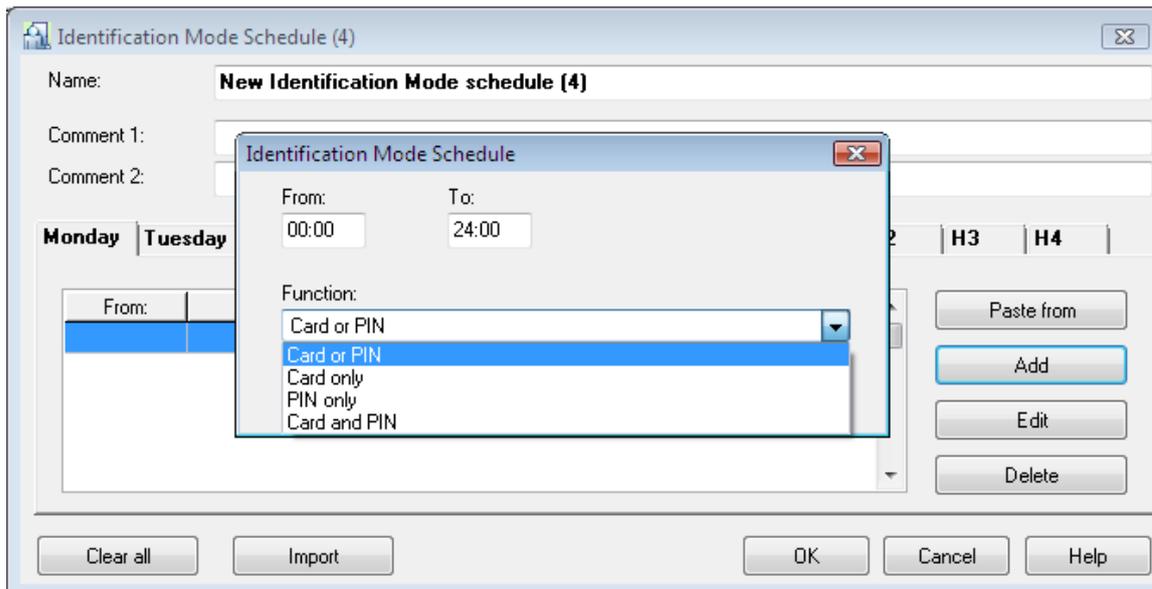


Figure 3.38. Defining a new identification mode schedule

By default there is **Always in Default Identification Mode** schedule defined in the PR Master. It means, that the controller always work in its default identification mode. This schedule can neither be erased nor modified.

3.2.7. Access zones

An **access zone** is a set of selected access points (terminals). The access zone can be a specific place e.g. Garage, Hall, Office. Defining access zones enables defining access rights not for individual door but for group of doors to particular area in the facility.

Every access point (reader) connected to controller, should be assigned to administrator defined access zone. After you add a new controller to the system, its terminals (readers) are assigned by default to **Default** zone.

Access point is a location in the facility controlled by the controller. Because the controller can control both entry and exit, every terminal can be assigned to a individual access zone.



The terminal belongs to the zone, to which it allows entry to (not exit from).



In the older types of controllers (PR201, PR301, PR311) both terminals had to be assigned to the same zone. In such types of controllers the access zone is assigned on the controller's level (i.e. both terminals belong to the same zone).

Selecting the **System/Access Zones** command causes displaying access zones directory (Figure 3.39).

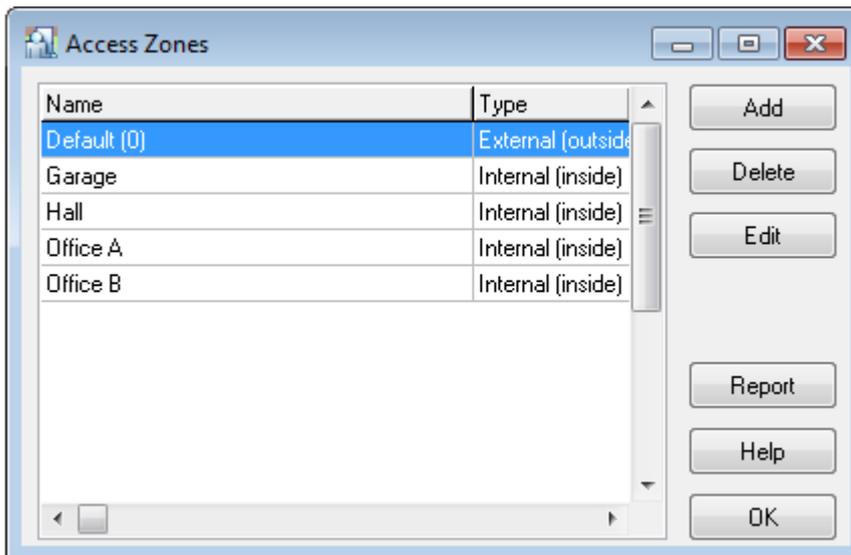


Figure 3.39. Access Zones directory

Using controls available in this window you can add a new access zone (the **Add** button), remove an access zone (the **Delete** button) modify access zone’s properties (the **Edit** button) as well as print the **Zones** report containing a list of access zones defined in the system.

3.2.7.1. Adding new access zone

In order to add a new access zone, you should click on the **Add** button. The **Access Zone properties** window appears (Figure 3.40). Using this window you can define the name for a zone, enter descriptive comments and indicate if the zone is **External** or **Internal**.

The **internal zone** is located inside the facility. An **external zone** (public zone) is everything located outside of the facility. According to this, you should assign to external zones all the terminals allowing exit from the facility being controlled (which is the same as entering the public zone). Usually there are several internal zones, and one external zone in the system. However you can imagine a complicated system, where several external zones can be differentiated.



Thanks to the terms of internal and external zones you can tell how many persons at any specific moment are inside the facility, and how many are outside. If you want to prepare such classification you can use the **Tools/Users Attendance within Access Zones** command.

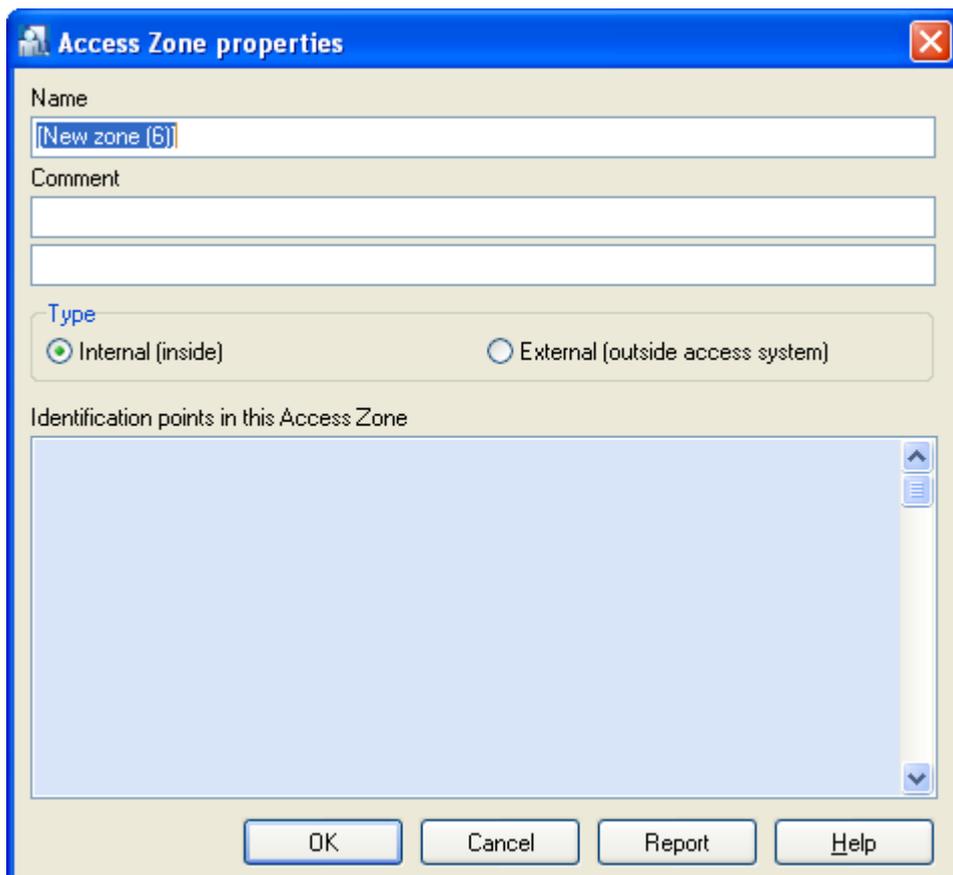


Figure 3.40. *Defining a new Access Zone*

In the **Name** field you should enter an access zone's name.

By default the system assigns the name **New zone(#)**, where **#** is a consecutive zone number. In fields **Comment 1** and **Comment 2** you can enter any zone description. Immediately after you define an access zone, the list of identification points belonging to it is empty. The zone is completely defined only after you assign readers (terminals) to it. It can be done from the controller's properties window.

3.2.7.2. Deleting access zone

In order to delete an access zone, you should click on the **Delete** button in the **Access Zones** dialog box. Before the zone is deleted, the **Confirm** dialog box appears, where you can confirm or cancel your intent to delete the zone. After the zone is deleted, identification points which belonged to it before are assigned to the **Default** zone.

3.2.7.3. Assigning identification points to zones

In order to assign an identification point to an access zone, you should open the controller's properties window. Depending on the controller type, you specify an access zone for the controller or for individual terminals (Figures 3.41 and 3.42). In general, in the older types of controllers (PR201, PR301, PR311) both terminals belong to the same access zone. In newer types of controllers, each terminal can be assigned to a separate access zone.

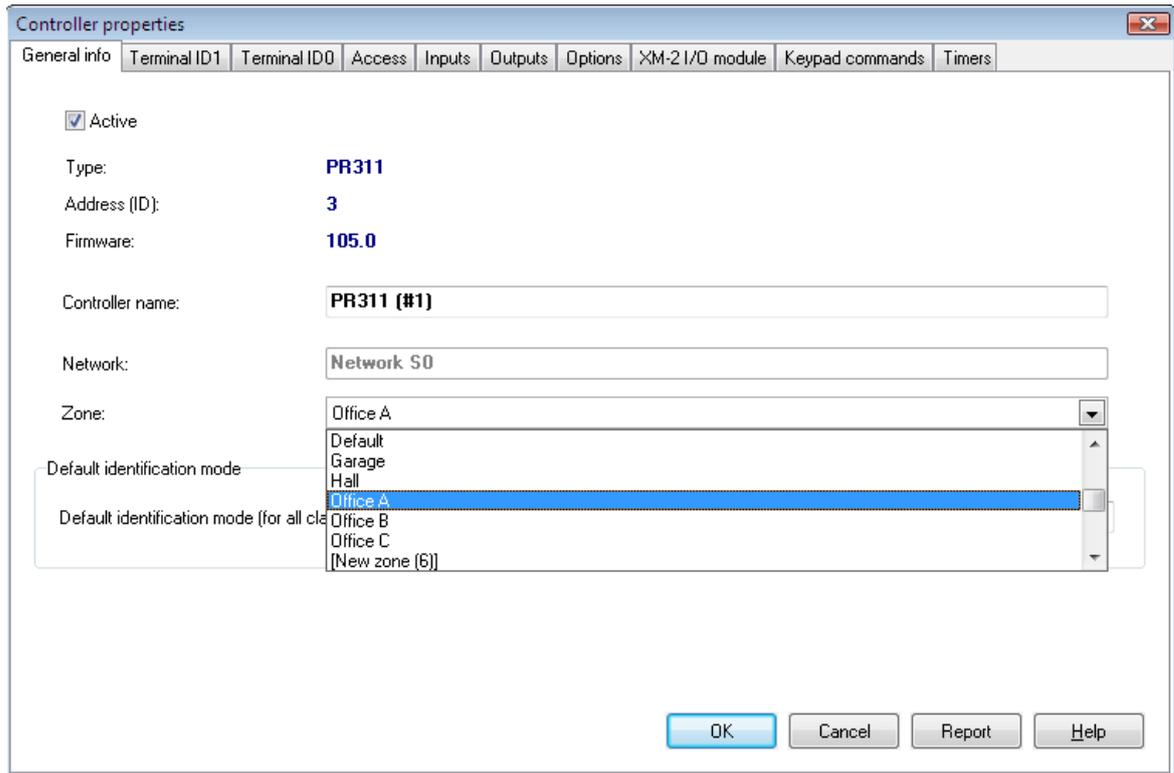


Figure 3.41. Assigning controller to the access zone — PR 311

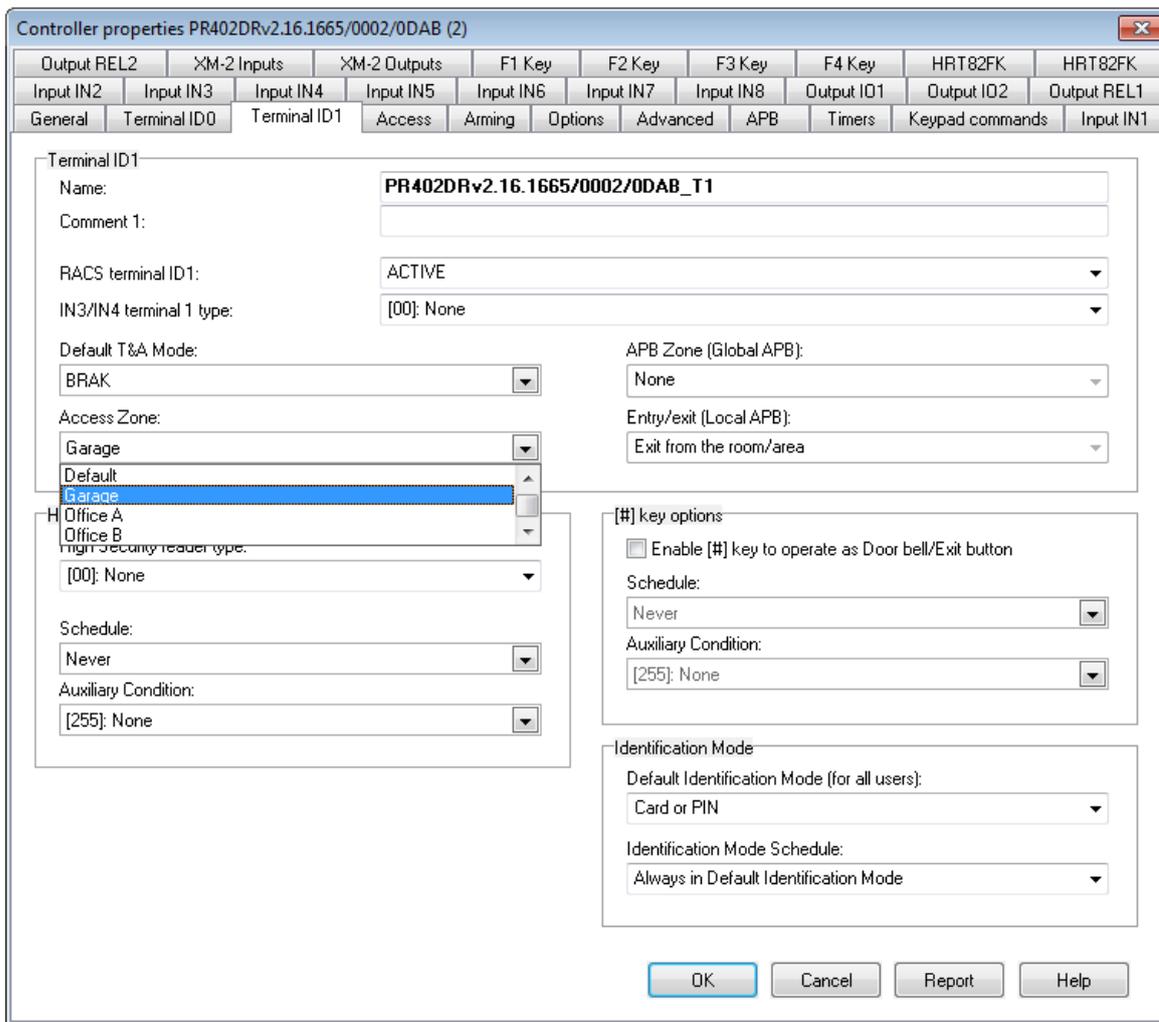


Figure 3.42. Assigning controller to the access zone — PR402DR

3.2.7.4. Generating zones report

After you enter all data for all the zones, you may want to generate a printed report. This is a good way to document information entered to the system. The **Report** button in the main window of the access zones' directory can be used exactly for this purpose. If you click on it, the **Zones** report will appear in the **Report** window (Figure 3.43).

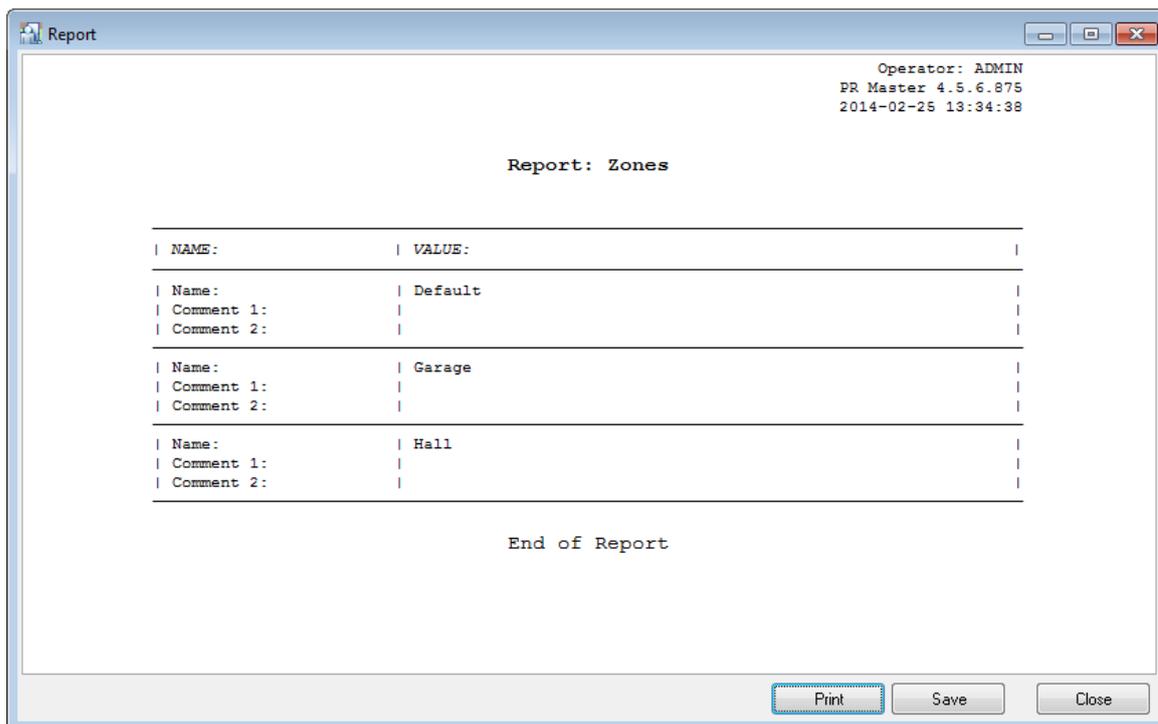


Figure 3.43. The Zones report

3.2.8. Networks

Roger Access Control System may consist of up to 250 networks (subsystems). Each network can contain up to 32 access controllers with terminals but the total number of controllers in the whole system should not exceed 1000 units.

Each network is connected to the managing computer by means of communication interface (e.g. UT-2USB, UT-4DR) or by means of CPR32-NET network controller, which has built-in communication interface.

Selecting the **System/Networks** command causes displaying window containing a list with networks installed in the RACS 4 (Figure 3.44).

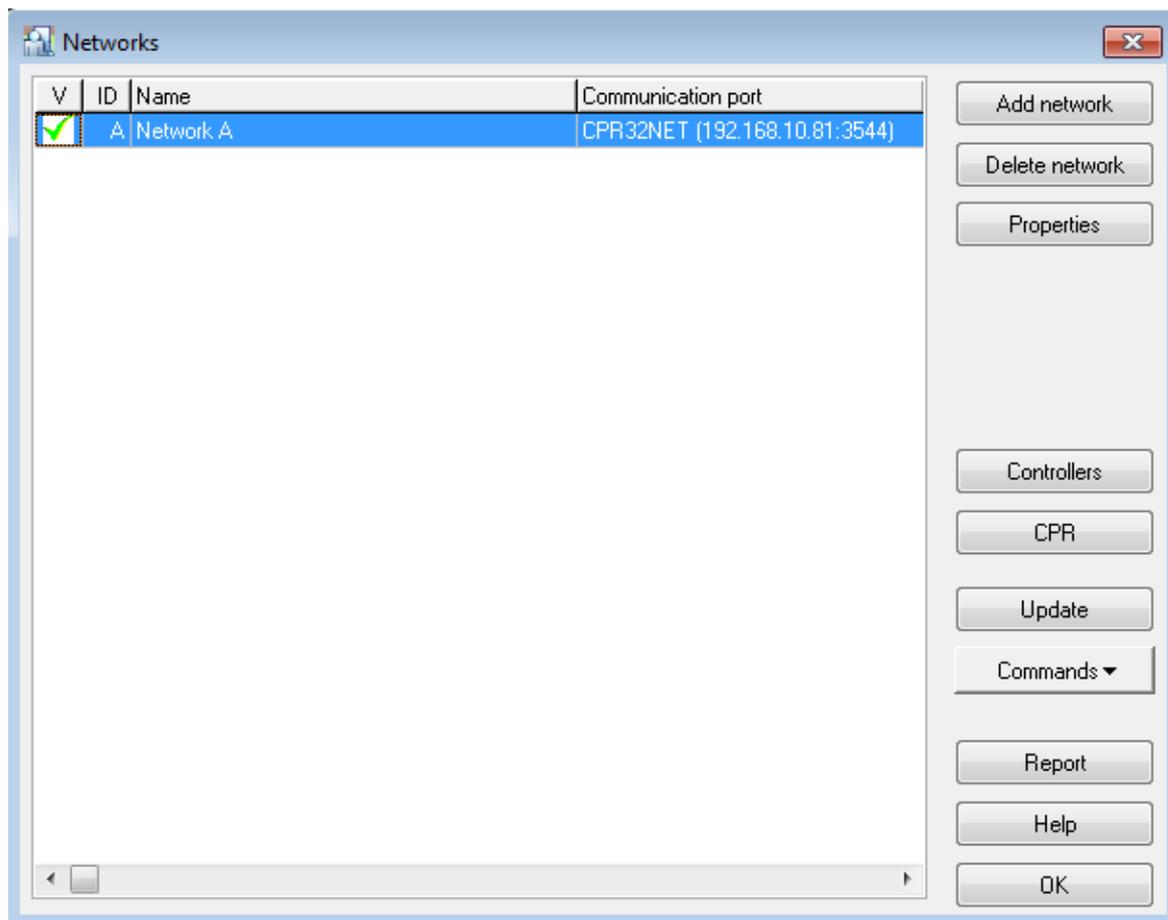


Figure 3.44. Network directory

From this window you can perform the following operations:

- ◆ adding a new network (the **Add network** button),
- ◆ removing a network (the **Delete network** button),
- ◆ updating network properties (the **Properties** button),
- ◆ managing a list of controllers belonging to the network (the **Controllers** button),
- ◆ displaying the CPR32-SE/CPR32-NET settings (the **CPR** button).
- ◆ updating configuration settings to all the controllers in the selected network (the **Update** button).
- ◆ executing commands for the network selected (the **Commands** button),
- ◆ generating **Networks** report (the **Report** button),

3.2.8.1. Adding new network

In order to add a new network to the system, you should click on the **Add network** button. The **Network properties** dialog box displays (Figure 3.45).

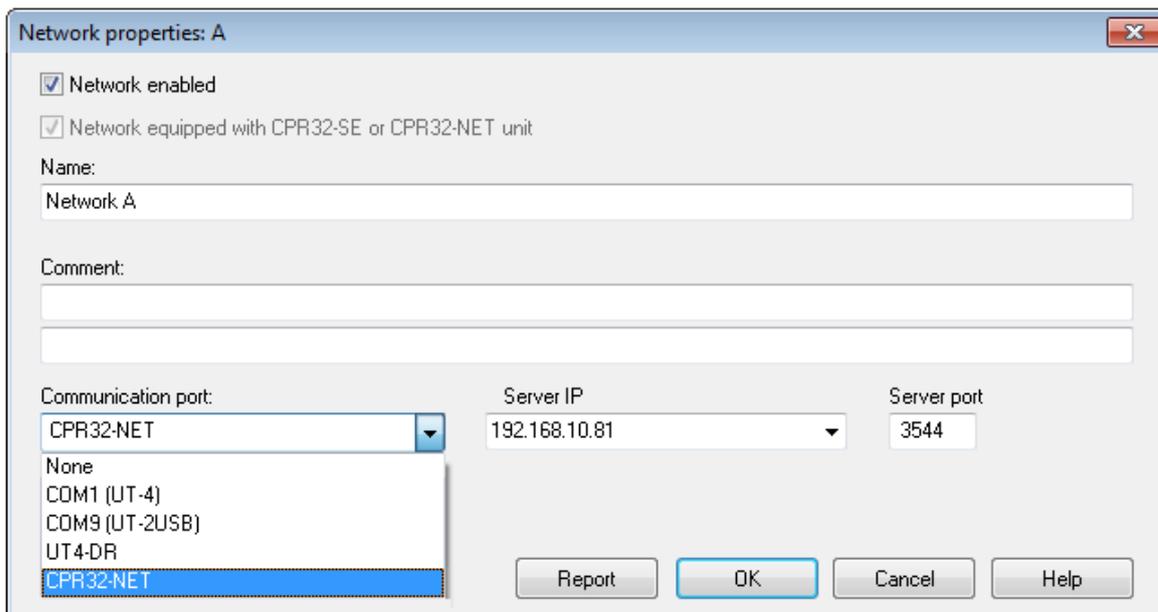


Figure 3.45. Adding New Network

For a system you have just defined, you should perform the following operations:

- ◆ indicate whether or not the network is enabled (the network can be disabled, for instance while it is being configured),
- ◆ select an option indicating whether or not the system is equipped with a CPR network controller,
- ◆ select a network name (optionally with comments),
- ◆ assign communication port,
- ◆ optionally select interface type.

You should pay special attention to the operations of assigning **Communication port**, indicating an interface type and selecting whether or not the network is equipped with a CPR network management unit. If you do this incorrectly, you will not be able to communicate with the network.



If the network is equipped with CPR32-SE network management unit, and the installer does not select an appropriate checkbox when defining the network, the PR Master will not be able to correctly communicate with controllers. Thus addresses conflicts may occur, for instance when detecting controllers.



If the CPR32-SE network management unit is connected while a new virtual serial port is being created (for instance for UT-4 or UT-2USB interfaces), Windows may improperly recognize a communication in the virtual port as a **Microsoft Ballpoint** device. Thus it will not be possible to assign a port to the network, because the PR Master will be unable to open a serial port. A solution in this case is to remove the **Microsoft BallPoint** device from Windows (**Control Panel/Device manager**) or disconnecting CPR32-SE while a virtual serial port is being installed.

Types of communication ports

Every network belonging to the Access Control System is connected to the managing computer through a separate, dedicated communication channel (it may be physical or virtual). For connecting network to computer, following communication interfaces can be used:

- ◆ UT-2 — is used for connecting a network through a physical serial port RS232,
- ◆ UT-2USB/RCI-2 — is used for connecting a network through a USB port,
- ◆ UT-4/UT-4DR — is used for connecting a network through an Ethernet network,

Furthermore, CPR32-NET network controller has built-in Ethernet-RS485 communication interface so the network equipped with CPR32-NET does not require any of mentioned above communication interface.

Communication ports setup

Upon installation of communication interface it is necessary to select it in **Communication port** field. In case of UT-2USB device hint for particular COM port is displayed – see Figure 3.45

UT-4DR and CPR32-NET require selection in **Communication port** field and then selection of IP address from the list or manual entering of IP address in **Server IP** field– see Figure 3.45.

The process is quite different in case of UT-4 interface, because it requires to explicitly install drivers and to assign a virtual COM port by means of **Digi Configurator** tool. When you use the utility, the virtual port assigned to the device will be available in the PR Master and it will be possible to connect subsystem through it.

3.2.8.2. Removing networks

In order to remove a network, you should use the **Delete network** button in the **Networks** window (Figure 3.46). If the network contain any controllers, then selecting this command will display a warning informing about a need to remove all the controllers for the particular network. It can be done by using the **Controllers** button. If the list of controllers is empty, the system will allow to remove a network. However, before it executes this command, it will display a dialog box with a question about confirmation of an intent to remove the network.

3.2.8.3. Updating network properties

The **Properties** button can be used for modification of some of the network properties. Clicking on this button causes displaying a **Network properties** dialog box — exactly the same as was displayed when the network was being added. From this window you can enable/disable CPR management unit, rename the network, as well as change an interface type and COM port. You can also display report describing particular network properties.

3.2.8.4. Managing controllers in network

The **Controllers** button in the **Networks** directory allows for managing particular network's controllers. If you click on it, the list of controllers in the network will show up (Figure 3.46).

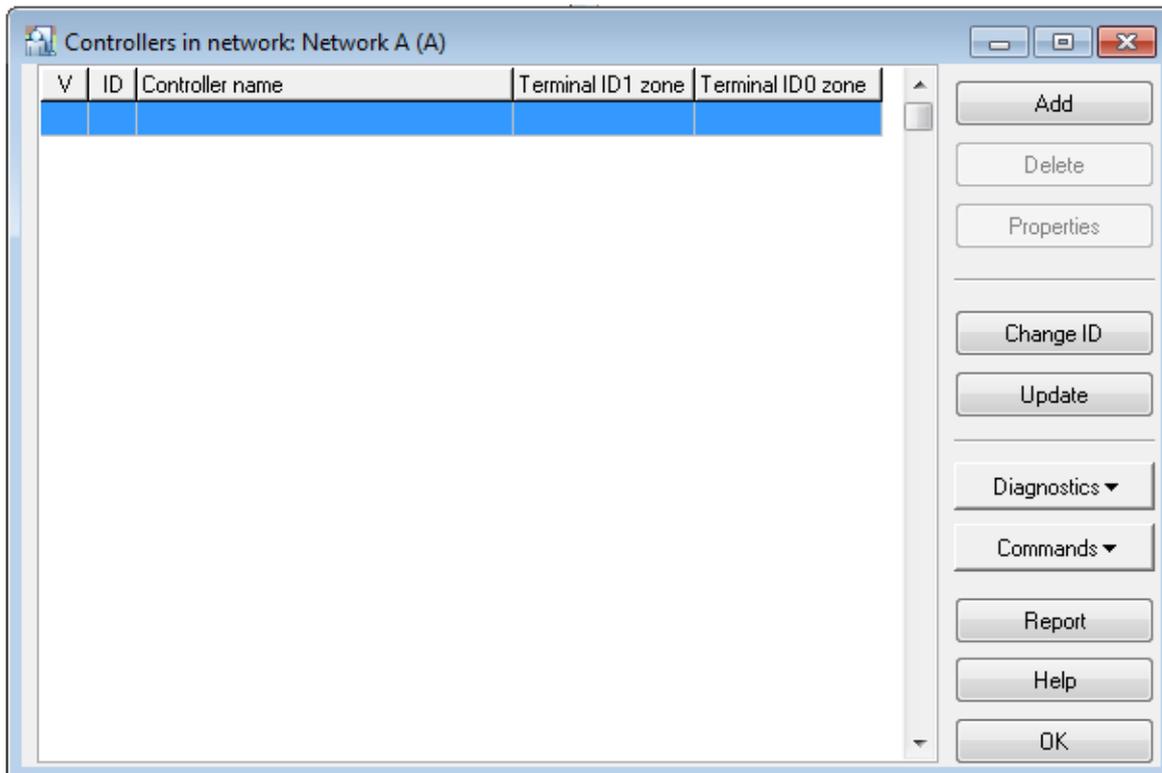


Figure 3.46. The list of controllers in the network — immediately after defining a new network is empty

From this window you can perform the following operations related to controllers of a particular network:

- ◆ add controllers,
- ◆ remove controllers,
- ◆ display and modify controllers’ properties,
- ◆ change ID addresses,
- ◆ upload configuration settings to the selected controller,
- ◆ perform diagnostic operations,
- ◆ send commands to the selected controller,
- ◆ generate report related to controllers in the network.

Adding controllers to the network

After defining a new network its controllers list is empty. In order to add a new controllers, you should click on the **Add** button. The system will start searching for controllers. While it is doing that, the PR Master shows a progress indicator showing ID addresses currently being searched (Figure 3.47).

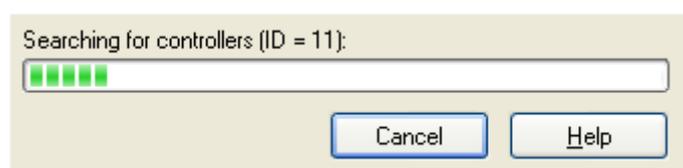


Figure 3.47. Searching for controllers in the network

The controllers found are immediately displayed in the network’s controllers directory. An installer can stop searching process at any time (e.g. if in his/her opinion all the controllers have been found) by clicking **Cancel** button. If the process of searching is not interrupted, the system will search addresses in the range from 00 to 100 and displays a message informing that controllers searching procedure has been completed.



If there are many errors during controller detection operation, it may be an indication that the network is equipped with CPR network management unit, and the installer did not select appropriate checkbox when defining the network. In such a case, you should go back to the Network properties window and select an appropriate option with CPR in the system.

Upon completion operation of adding controllers, the window with controllers can have a form as shown in Figure 3.48.

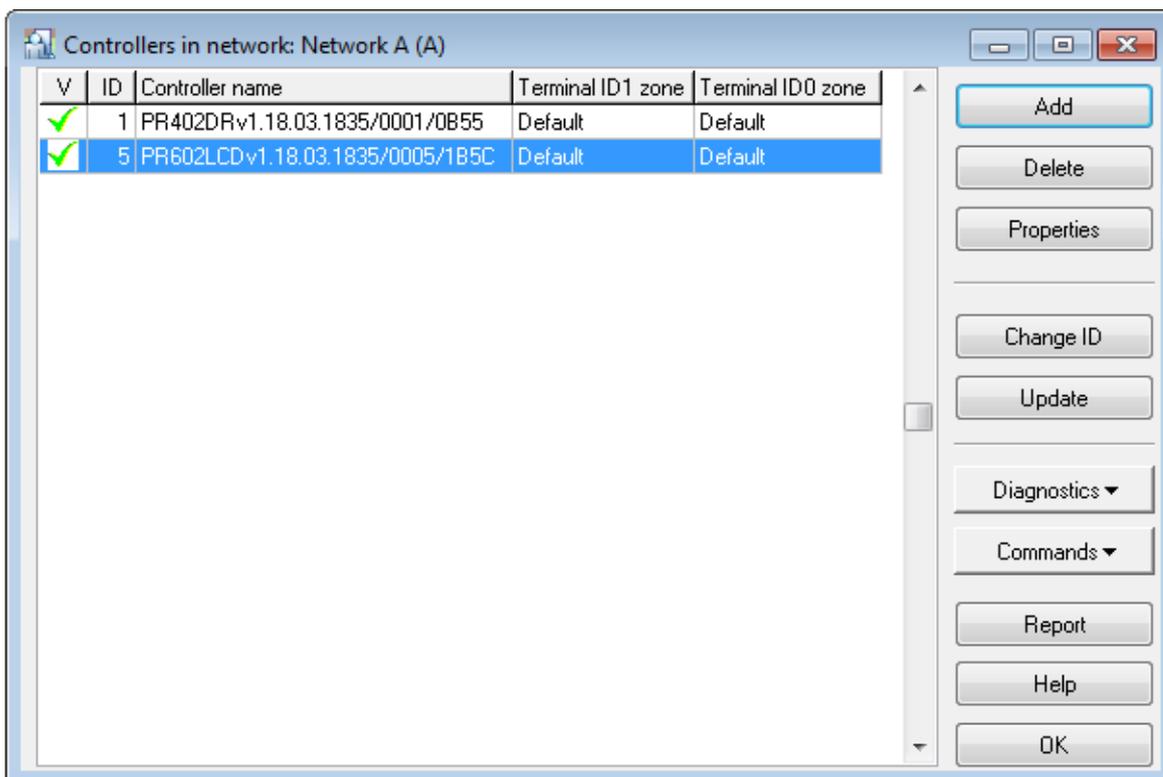


Figure 3.48. The controllers list upon completion the searching for controllers operation

Two additional buttons are now enabled: **Delete** and **Properties**. They allow for removing selected controller and changing its configuration respectively.

Deleting controllers from the network

In order to delete controller from the network you should click on the **Delete** button. As usual, before the controller is deleted, the system will display a confirmation question asking if you are sure to delete the controller. If you answer **Yes**, the controller will be deleted.



Deleting controller from the network is reasonable only on the condition that the controller has been physically disconnected from the access control system. If you delete controller which physically exists in the system, the PR Master program will stop to communicate with it. As a result, an old configuration (users permissions and so on) will remain unchanged in it. Thus, a delete operation should be done with special care. If you accidentally remove an existing controller, you should add it again (the **Add** button).

Browsing (modifying) controllers properties

Clicking on the **Properties** button displays a properties window for the controller selected. This is a mechanism which allows for defining the controller’s configuration. In order to perform the actual controller’s configuration, the configuration defined should be later sent to the controller. The controller properties window can have a different look depending on the controller’s type. An example of a **Properties** window for a PR402DR controller is shown in Figure 3.49.

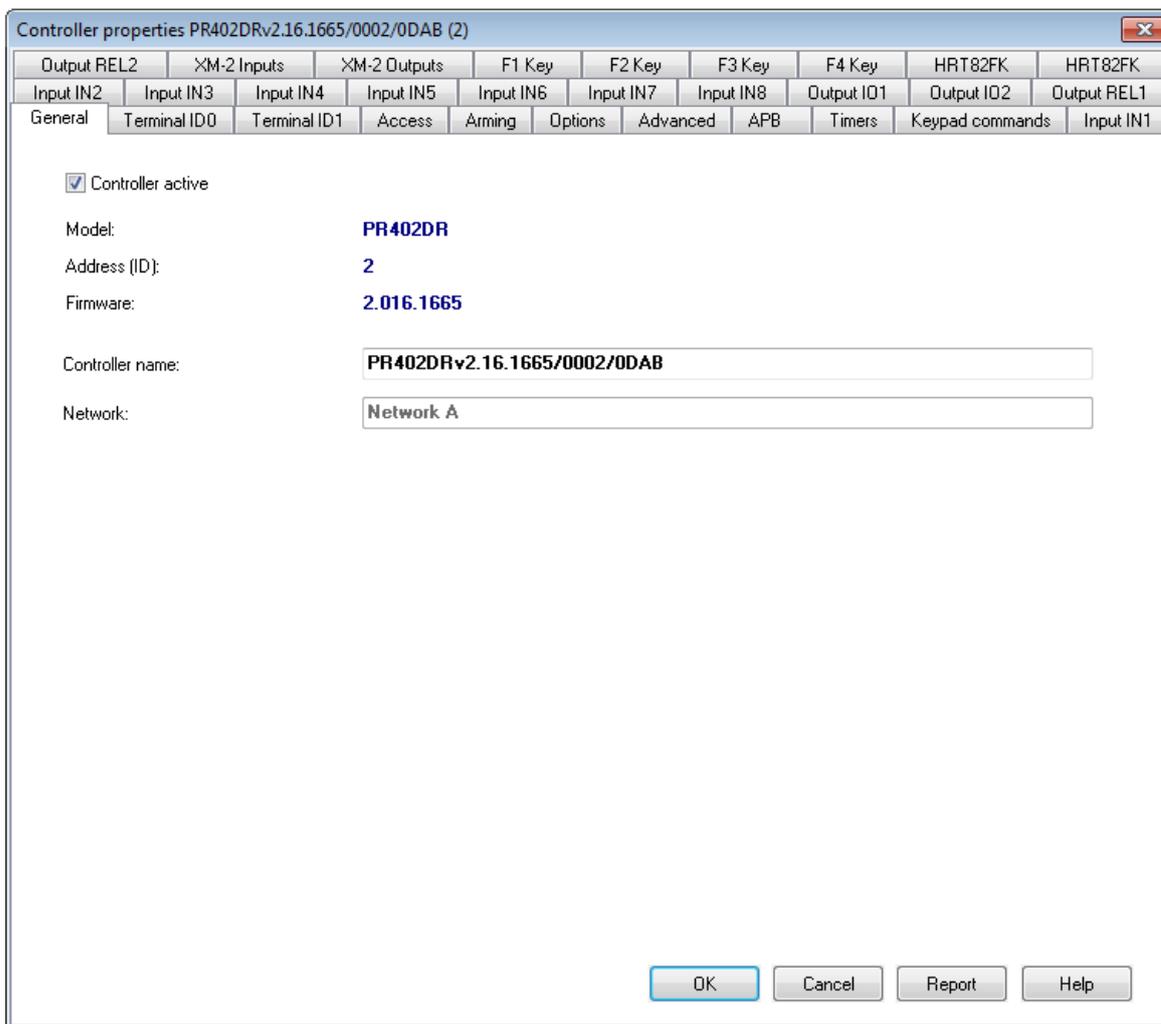


Figure 3.49. PR402DR controller properties

As you can notice in Figure 3.47, the window is divided into many tabs. Using them you can define controller’s configuration in detail. From this window, you can assign controller’s terminals to access zones, set up an identification mode and define behavior of function keys, among others.



A detailed description of all the settings for many different controller types is outside the scope for this manual. In most cases default settings will be sufficient to utilize controllers in physical installations. A detailed information about all the configuration options can be found in the manuals: [Functional description of PRxx2 series controllers](#) or [Functional description of PRxx1 series controllers](#).

Changing controller’s ID address

All the controllers manufactured by Roger have a factory default ID=00. To make communication via RS-485 bus possible, every device connected to it should have a different address (in the 00 – 99 range). Because of this, unique addresses should be assigned to specific controllers while installing the system. There are many methods for changing controller address and all of them are described in Installation Guides of particular controllers. One of possible methods consists in using PR Master software.

In order to change ID address for the selected controller, you should click on the **Change ID** button. The **Controller address** dialog box displays (Figure 3.50).

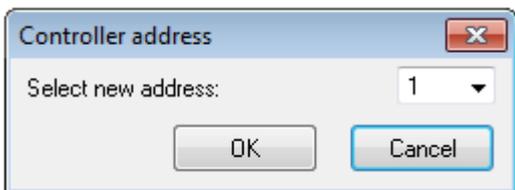


Figure 3.50. *Changing Controller’s ID Address*

If you enter a new address and confirm it by **OK** button, it will be automatically sent to the controller. The address updated will show up in the controllers list.

Sending configuration data to controller

After you make configuration changes in the controller’s properties window, you should send updated data to controllers. Only after changes are sent they start to have effect in the ACS. In order to send configuration, you should select a controller in the controllers list and click on the **Update** button. If at this time there are any events gathered in the controller, then before performing an update, the system will automatically download these events to database. After handling the events, the system displays a window with information about an update operation progress (Figure 3.51). When the transmission is completed, the system displays a window with information about transmission result (Figure 3.52).

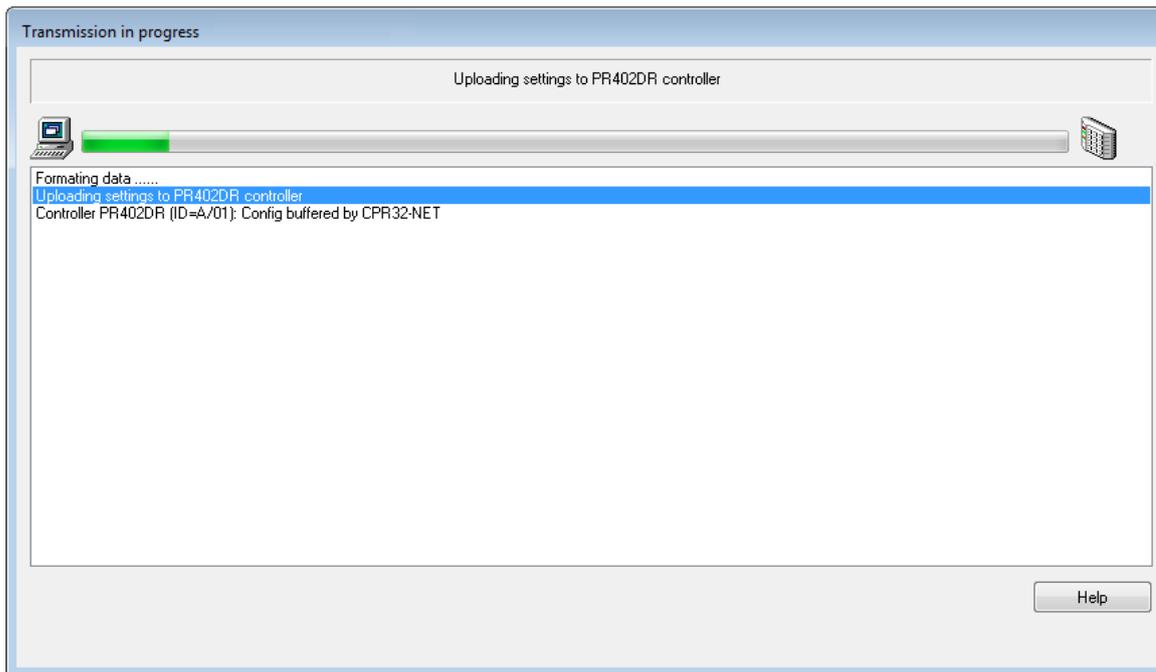


Figure 3.51. Sending configuration settings to selected controller

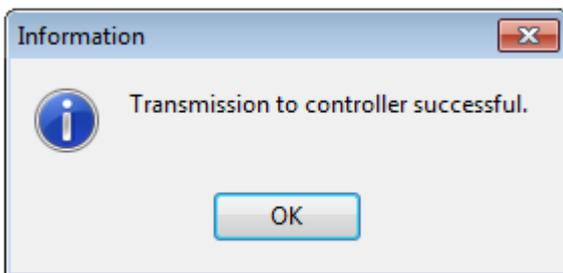


Figure 3.52. Successful configuration upload

Performing diagnostic operations

The **Diagnostics** button gives access to the diagnostic operations menu (Figure 3.53). From this window you can perform various operations aiming to verify system’s operation correctness. You can compare the settings in the controller with those in the PR Master, check if the program can communicate with the controller and CPR management unit, check communication between CPR network management unit and controllers, perform communication bus interference test, and make full or quick flash memory test.

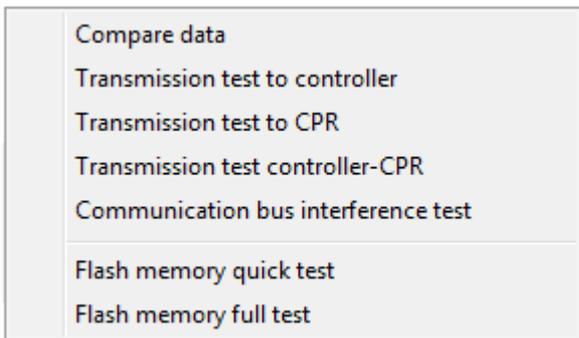


Figure 3.53. Diagnostic menu

Most of the communication tests available from this menu are performed at the communication protocol level. Because the RACS 4 is very resistant to interferences, the tests may give satisfactory results even if there are serious electrical interferences on the bus (Figure 3.54).

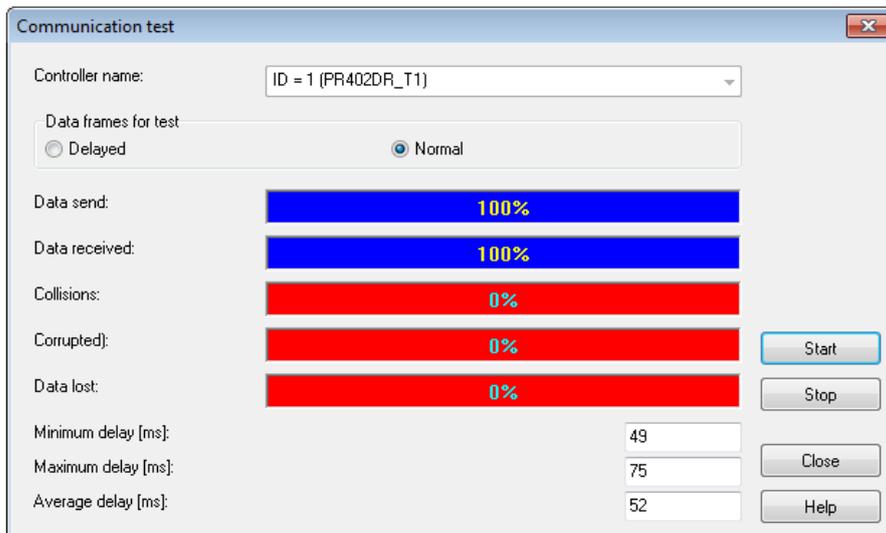


Figure 3.54. Communication test with the controller

A most accurate test allowing for detecting electrical problems on the bus is a **Communication bus interference test** (Figure 3.55). High numbers of state changes in the tests results is an evidence that there are interferences on the bus.

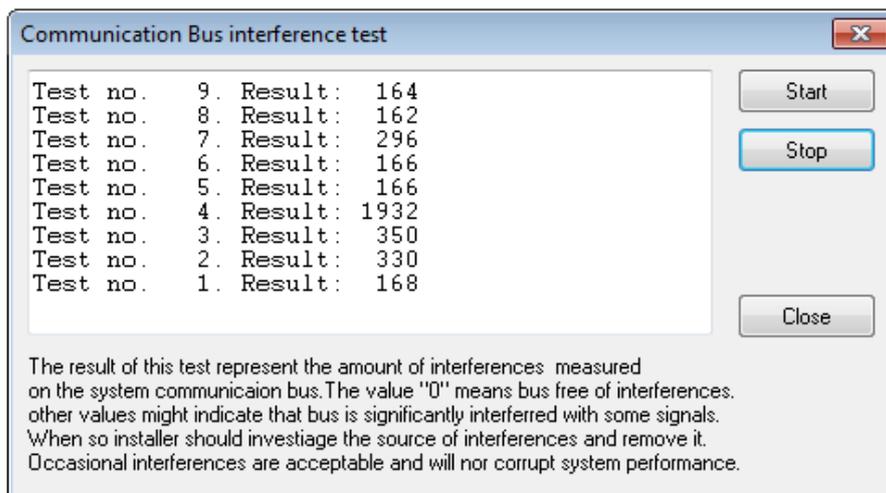


Figure 3.55. RS485 bus interference test — number of state changes more than zero indicates communication problems



Communication tests results with information of errors may be an evidence of communication problems but it can also mean that the system has been configured improperly. If, for instance, an installer does not indicate that the system is equipped with the CPR network management unit but actually it is equipped with it, then communication tests will show errors.

Sending commands to selected controller

The **Commands** button gives access to the command menu for the selected controller (Figure 3.56). The content of the **Command** menu may vary, depending on the controller type. The

Commands menu for the PR402DR controller is shown in Figure 3.56a, whereas in Figure 3.56b similar menu for the PR602LCD controller is presented.

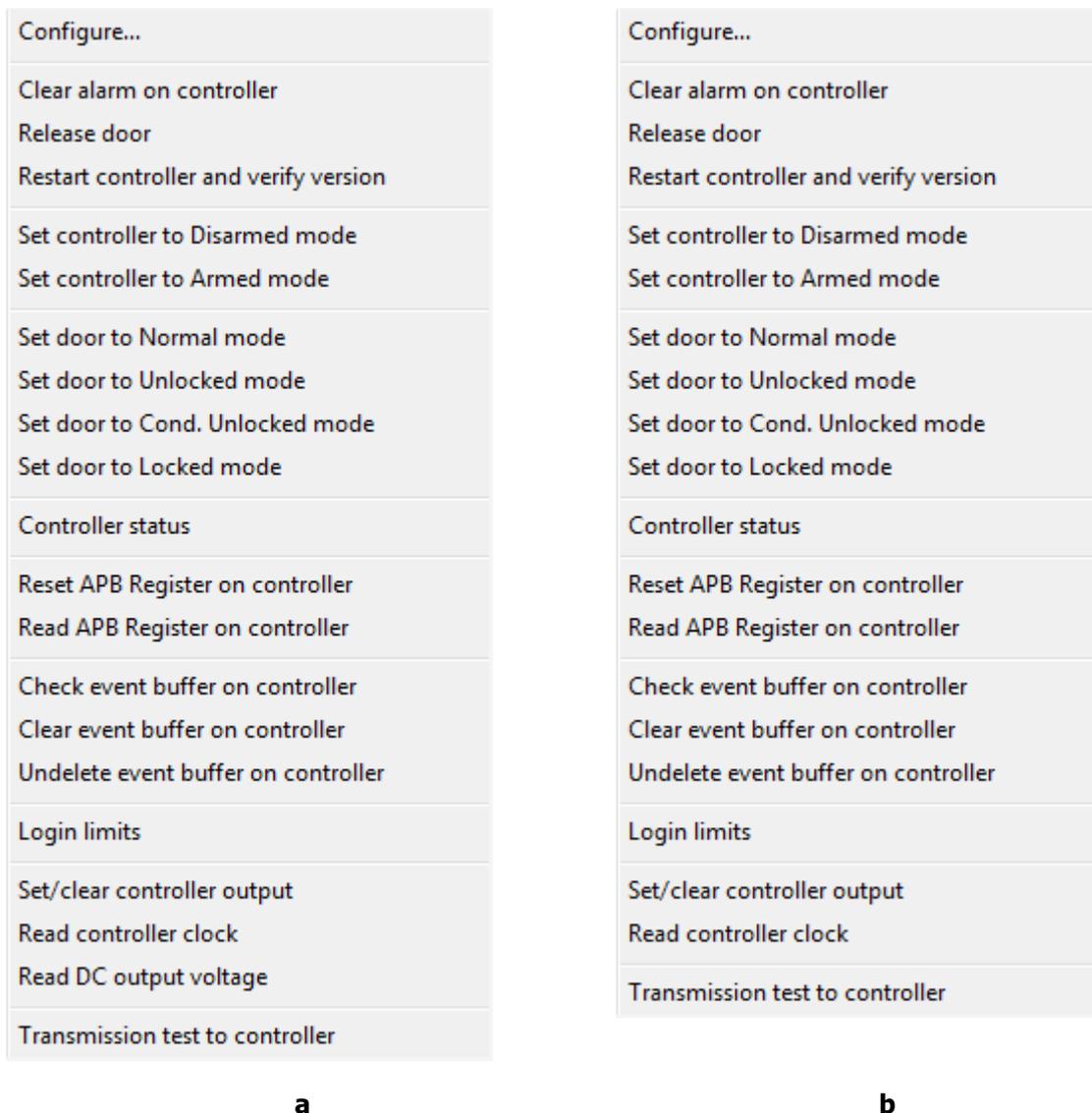


Figure 3.56. Commands menu (a) PR402DR controller; (b) PR602LCD controller

The **Commands** menu for the PR402DR controller contains an additional **Read DC output voltage** command , which is not available for the PR602LCD controller.



A detailed description of all the settings and taking into account all the controller types is outside the scope of this manual. Additional information about the commands can be found in following manuals: **Functional description of PRxx2 series controllers** and **Functional description of PRxx1 series controllers**.

Generating report of controllers in the network

After you enter all configuration data to the controller and test its operation, the printed report may be prepared. This is a good way to document controller’s configuration data. The **Report** button in the specific network’s controllers directory window can be used for this purpose. In order to

prepare the report, you should point the controller and click on the **Report** button. This will cause displaying the **Controllers** report in the **Report** window (Figure 3.57).

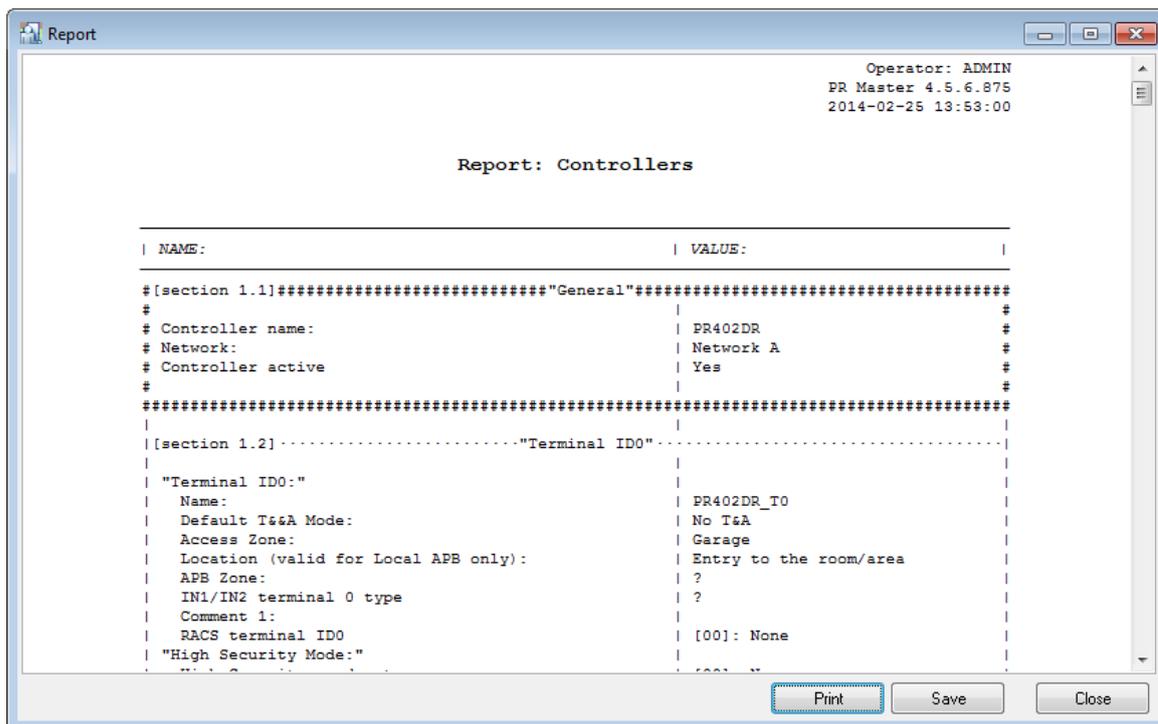


Figure 3.57. Controllers report

The **Controllers** report contain detailed information regarding configuration of the specific controller. Upon successful system configuration it is worth preparing a printed report for such a system. It may be helpful when troubleshooting problems at the later stage of system in production

3.2.8.5. Displaying CPR settings

CPR32-SE network controller is a device which is used in the RACS 4 as an external event buffer and it synchronizes time settings on controllers. The presence of CPR32-SE in RACS 4 system is optional and depends on functional requirements of the installation. In case of PRxx2 series controllers, CPR32-SE is used only for global functions (global APB and alarm zones), while in case of PRxx1 series controllers, it also offers event buffer and real time clock as PRxx1 controllers (in the opposite to PRxx2 controllers) are not equipped with them.

CPR32-NET unit ensures the same functionality as CPR32-SE unit and additionally it enables integration with intruder alarm panels of INTEGRA (SATEL) series and wireless door locks of APERIO (ASSA ABLOY) system, it performs the role of Ethernet-RS485 interface, enables operation with event buffer on external memory card (30 million events), enables synchronization with NTP server and encrypts communication by means of AES128 CBC standard.

For displaying CPR unit settings, the **CPR** button can be used. If the network is not equipped with the CPR then this button is disabled. Clicking on this button causes displaying a dialog box containing settings for CPR32 network management unit working in the network (Figure 3.58).

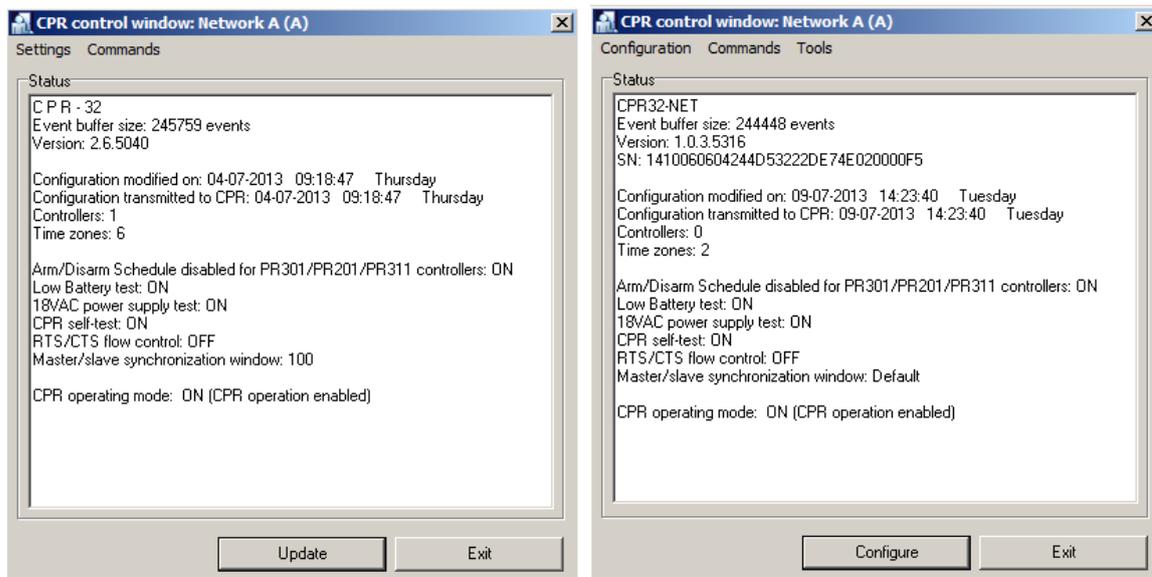


Figure 3.58. CPR32-SE and CPR32-NET network controller settings

CPR settings can be viewed in the window and new settings can be uploaded from PR Master by means of **Update/Configure** button.

3.2.8.6. Sending settings to controllers and CPR unit

The **Update** button in the network directory is used for sending settings to all controllers and CPR unit in the selected network. In case when the network contain many controllers, this operation can take a long time. Because of this it should be initiated as rarely as possible.

Operation of sending settings to controllers is initiated by clicking on the **Update** button. If at this moment there are any events collected in any controller or CPR, then they are downloaded to PR Master database. While downloading events, the system displays information window containing data on reading operation progress (Figure 3.59).

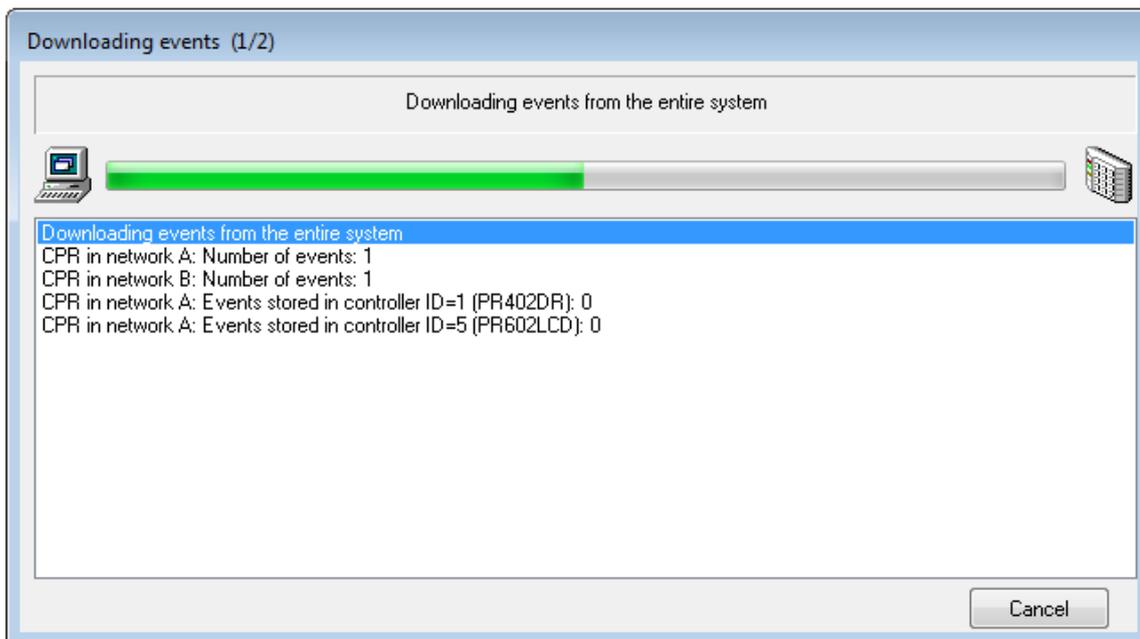


Figure 3.59. Reading events from the network before sending configuration

After displaying a message on completing reading events, the system proceeds to sending data to devices in the network (Figure 3.60).

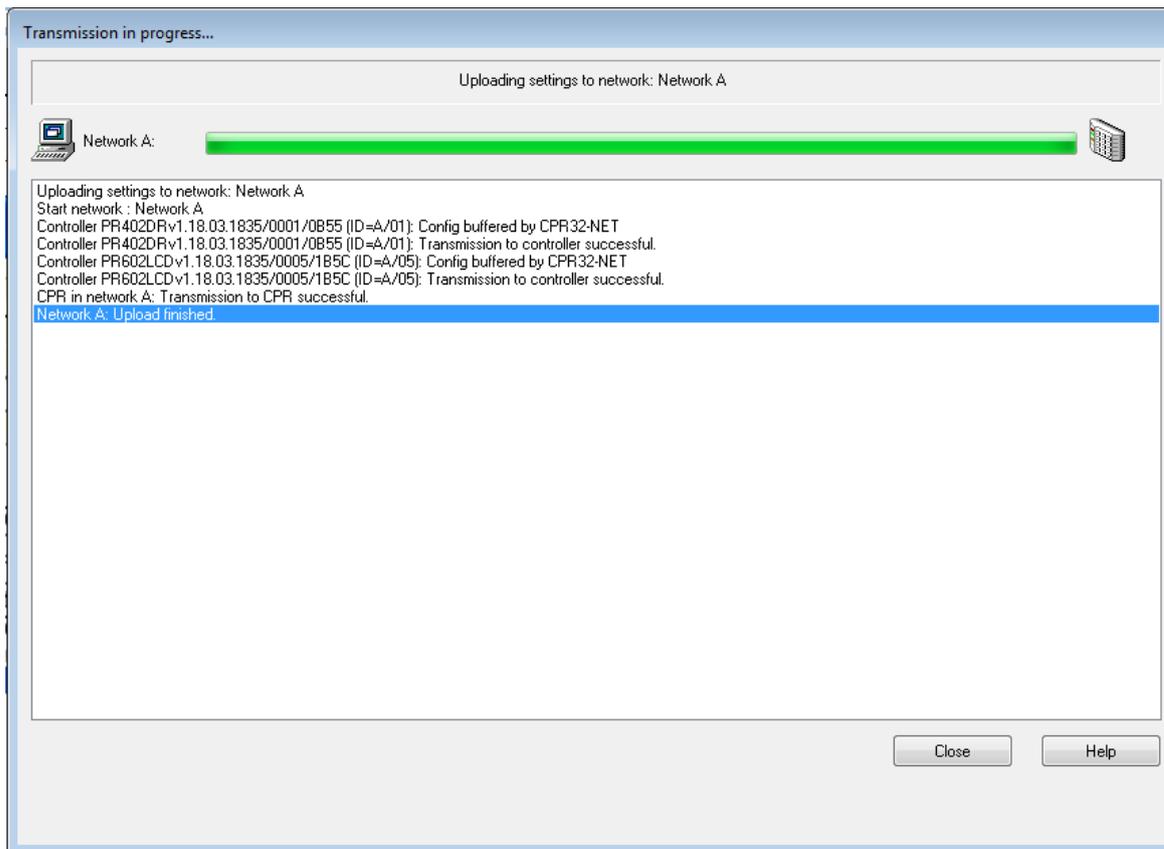


Figure 3.60. Sending Settings to the network — the operation progress window

3.2.8.7. Executing commands for the network

The **Commands** button in the **Networks** directory shows commands menu (Figure 3.61) which allows for executing commands for the network.



Figure 3.61. Commands menu in the network's directory

The menu allows for performing the following operations:

- ◆ **Clear alarms in network** — deleting all the alarms on all the controllers in the network. This option is useful when we do not want to wait 3 minutes before an alarm state disappears and we do want to perform this operation on all the controllers in the system simultaneously.
- ◆ **Set all controllers to Disarmed mode** — switches all the controllers in the network to disarmed mode.

- ◆ **Set all controllers to Armed mode** — switches all the controllers in the network to Armed mode.
- ◆ **Read Global APB Register** — this functionality reads a current global APB register in the network. This is a user list together with information in what APB zone they are currently logged on.
- ◆ **Clear Global APB Register** — this functionality resets the current global APB register in the network. Immediately after the reset, every user registered on the controller has unspecified status in the global APB registry (you cannot determine if the user logged recently on entry or on exit). From this moment on, the system starts to use APB rules.
- ◆ **Locate users within APB zones** — this function allows for answering the question on what is the APB zone, the selected user is currently logged in.
- ◆ **Assign user to APB zone** — this function can be used for manually assign selected user to the APB zone. When you select this command, the dialog box appears where you can choose an user and select APB zone for him. You can also reset APB status for the selected user by selecting the **APB status: unknown** menu item.

3.2.8.8. Generating Networks Report

The **Report** button in the **Networks** directory allows to generate summary report related to networks defined in the RACS 4. Sample report has been shown in Figure 3.62.

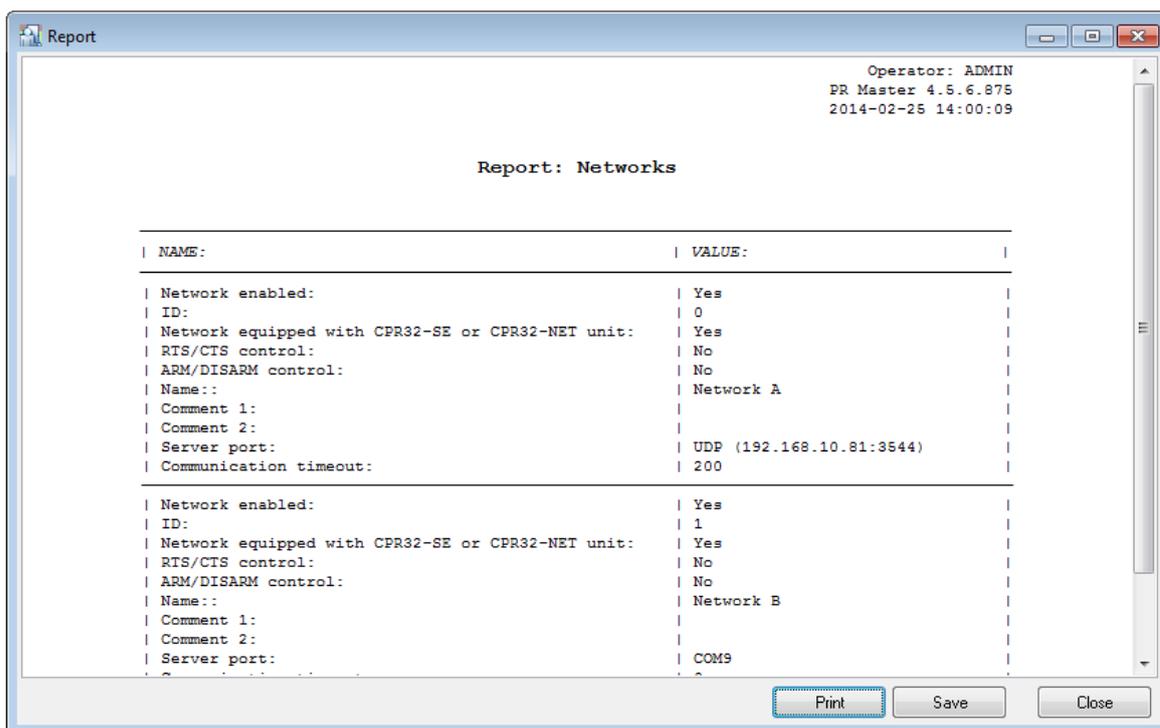


Figure 3.62. Networks report

3.2.9. Attendance areas

Attendance areas is one of the RACS 4’s mechanisms which allow for controlling location of the user in the facility. An attendance area can be understood as a part of the area being controlled by the ACS, you can enter through a set of identification points, and you can leave through other identification points.

Attendance areas are defined in order to prepare attendance reports (**Reports/Attendance**). Attendance report shows time the user entered/left the area and total time he was present in the attendance area.

Unlike time & attendance reports (T&A), attendance reports do not base on T&A modes, but only on defining which readers are responsible for entry and which are responsible for exit from the area. Based on attendance report you can calculate total attendance time for employees in a particular area (e.g. in the production hall).

If you select the **Attendance Areas** command, the **Attendance Areas** dialog box opens (Figure 3.63).

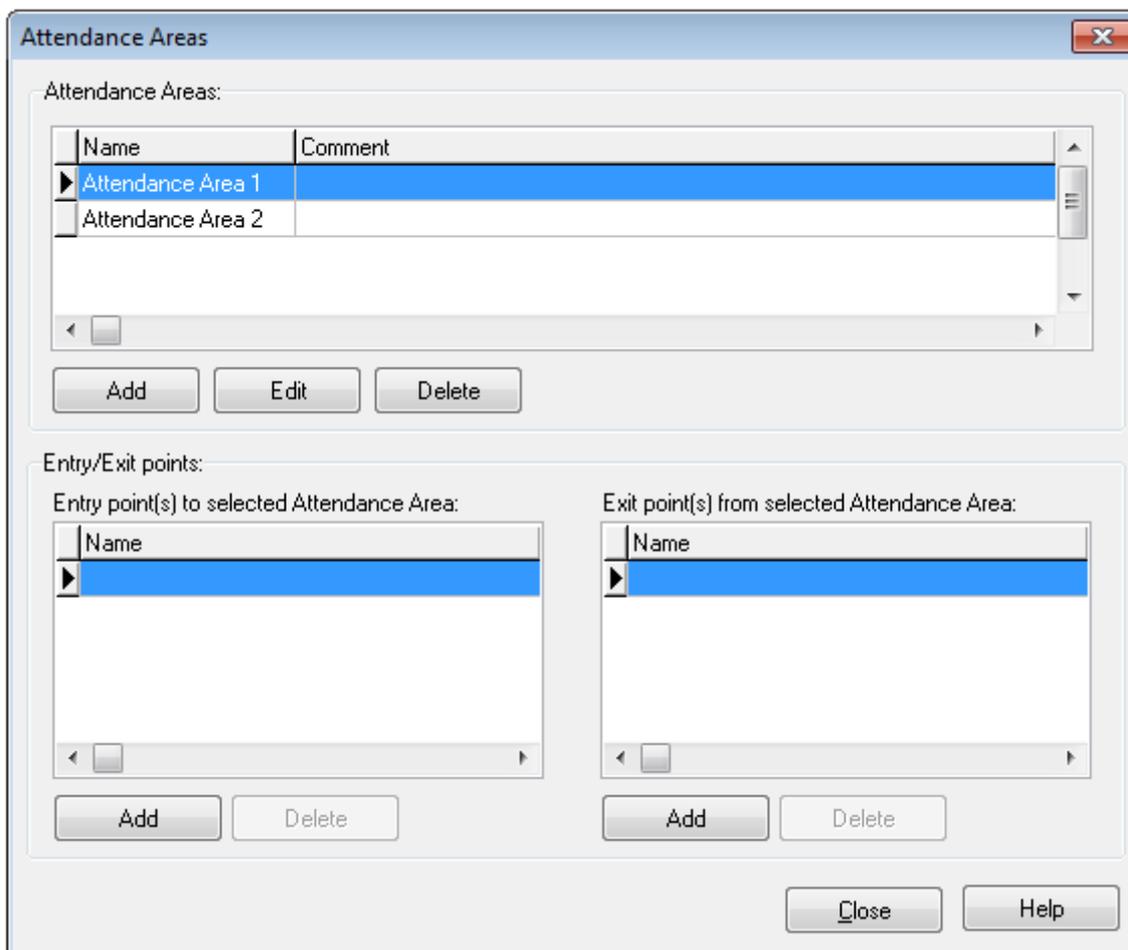


Figure 3.63. Attendance Areas directory

The window allows to perform the following operations:

- ◆ add a new attendance area,
- ◆ modify an existing attendance area,
- ◆ remove attendance area selected,
- ◆ add/delete entry points to the attendance area,
- ◆ add/delete exit points from the attendance area.

3.2.9.1. Adding a new attendance area

In order to add a new attendance area to the system, you should click on the **Add** button in the **Attendance Areas** group box — directly below the attendance areas list. The **Add new area**

dialog box displays (Figure 3.64). You should give a name to the attendance area, enter a descriptive comment and click **OK**.

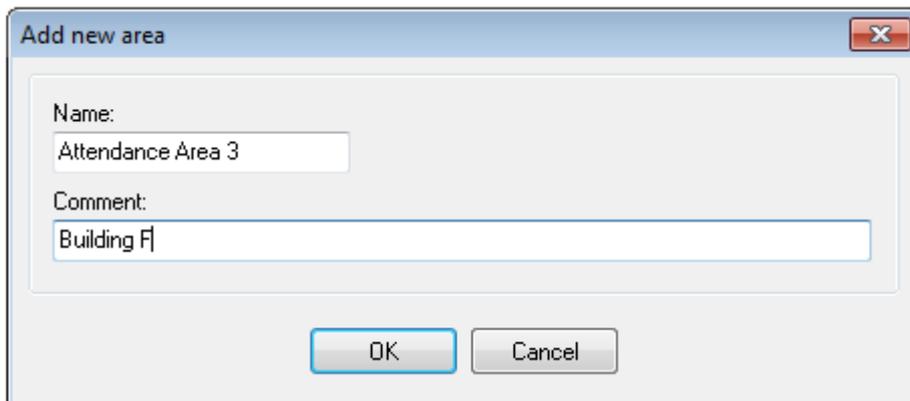


Figure 3.64. Adding a new attendance area

Adding/Deleting Entry and Exit Points To/From Attendance Area

Immediately after defining, the attendance area is empty — there are no defined entry points to the area nor exit points from the area. Only after identification points controlling entries and exits are defined, the attendance area makes proper sense (i.e. allows for controlling users attendance within it).

In order to add a new entry point to the attendance area, you should click on the **Add** button below the **Entry point(s) to selected Attendance Area** list. The **Add access point(s)** dialog box displays (Figure 3.65).



Figure 3.65. Adding entry points to attendance area

In the list there are all identifications point, which up to this point has not been assigned as entry points to the attendance area selected. T1 terminals of all the controllers in the system are

displayed in bold. Adding a new entry point to selected attendance area is as simple as selecting check box next to the identification point and clicking the **Add selected** button.

Exit points from the attendance area are added in the same manner. In this case, you should make use of the **Add** button present directly below the **Exit point(s) from selected Attendance Area**. A dialog box appears very similar to this, which has been shown in Figure 3.65. The difference is that the list does not contain identification points selected earlier as entry points to a particular area.

In order to delete an identification point to/from an attendance area, you should use the **Delete** button below the appropriate list. The program will delete selected identification point without displaying any additional warnings.

3.2.9.2. Modifying existing attendance area

In order to change name or comment related to attendance area defined earlier, you should select area the changes should be applied to, and then click on the **Edit** button in the **Attendance Areas** group box — directly below the attendance areas list. The **Edit area** dialog box displays (Figure 3.66). In this dialog box you can change a name or a descriptive comment related to the attendance area selected.

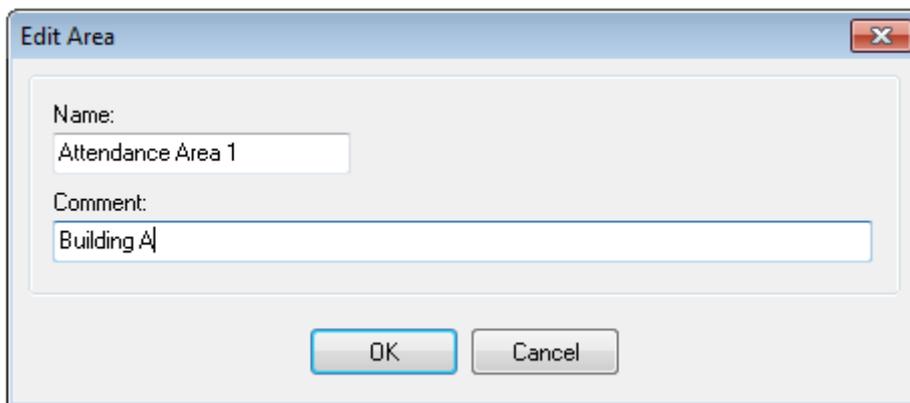


Figure 3.66. Modifying existing attendance area

3.2.9.3. Deleting Existing Attendance Area

In order to delete from the system the attendance area defined earlier, you should click on the **Delete** button in the **Attendance Areas** group box — directly below the attendance areas list. The system will delete the attendance area selected, together with identification points assigned to it.



You should be careful when using the **Delete** button, because the system does not display any warnings before the attendance area is deleted. Because of this you should remember about making backups regularly. They can protect the user against a need to enter all data from scratch

3.2.10. APB Zones

The purpose of the Anti-Passback feature is to protect against the possibility to use proximity card of the user at entry to the zone if it had not been used at exit before. To put it differently, the user can not enter the APB zone if he had not left it before. The function is aimed to protect against the possibility that one user passes its card to another user to allow him to enter the zone. More additional information on APB configuration is given in the document **Functional description of PRxx2 series controllers**.

Selecting the **System/APB Zones** command causes displaying APB zones directory (Figure 3.67).

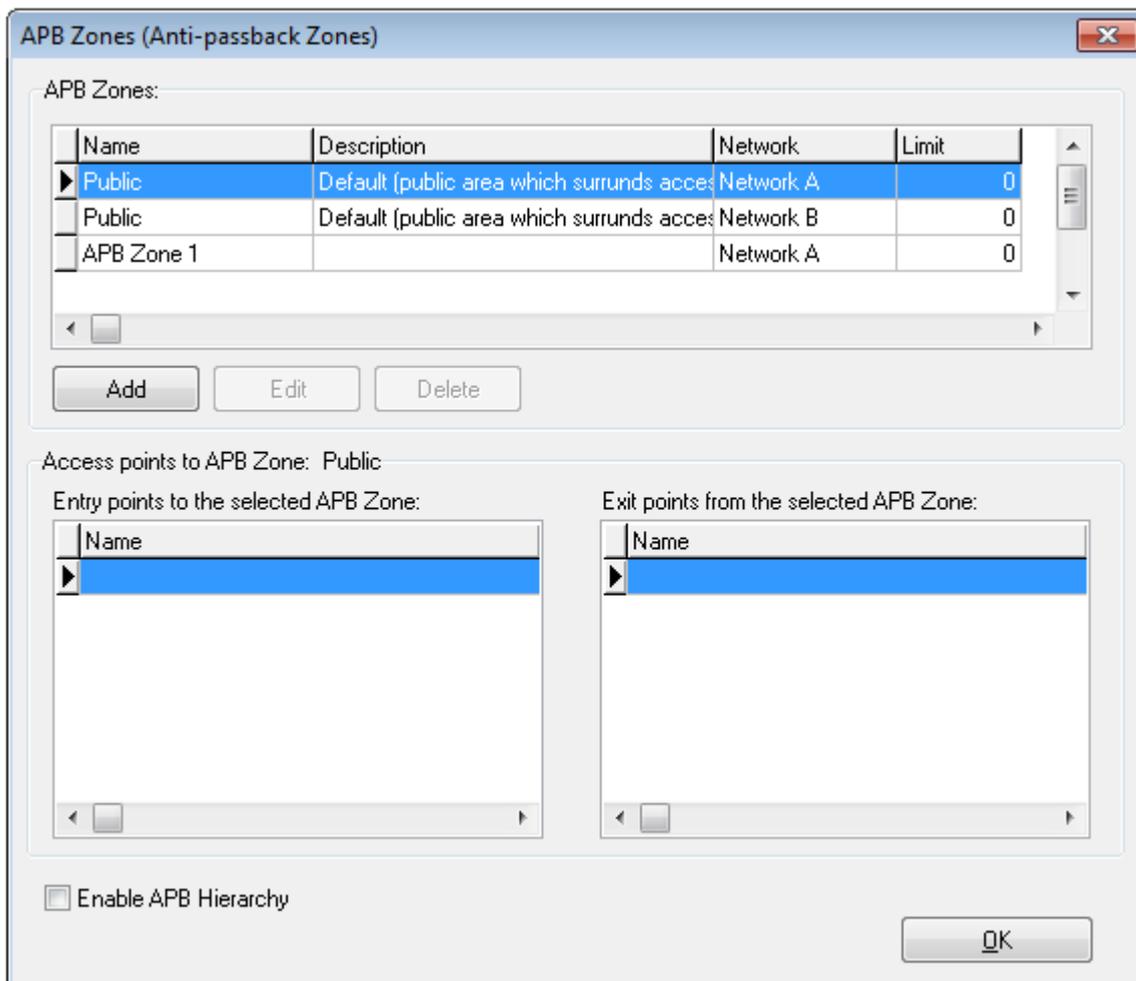


Figure 3.67. APB zones directory

Using controls available in this window you can add a new APB zone (the **Add** button), remove existing APB zone (the **Delete** button), modify APB zone’s properties (the **Edit** button).

3.2.10.1. Adding a new APB zone

In order to add a new APB zone, you should click on the **Add** button. The **Add new APB Zone** dialog box displays (Figure 3.68). Using this window you can define the name for the APB zone, enter descriptive comment and define limit for the number of persons present inside.

Figure 3.68. Adding a new APB zone

Immediately after you define an APB zone, the list of identification points belonging to it is empty. The APB zone is completely defined only after you assign readers (terminals) to it. It can be done from the controller's properties window level (see [section 3.2.10.3](#)).

3.2.10.2. Deleting APB Zone

In order to delete APB zone, you should click on the **Delete** button in the **APB Zones (Anti-passback Zones)** dialog box. After the zone is deleted, the system automatically cancels assignment of identification points which belonged to it before (the **None** setting).



You should be careful when using the **Delete** button, because the system does not display any warnings before the APB zone is deleted. You should absolutely remember to make system's backups. If you accidentally delete existing APB Zone, you can restore it from backup.

3.2.10.3. Assigning Identification Points to APB Zone

In order to assign an identification point to the APB zone, you should open the controller's properties window. First you should check the **Enable Anti-passback** option (the **Advanced** tab). Then you can select APB zone, to which the particular terminal belongs (it is being done in tabs for particular terminals). The APB zones settings are correct only on the condition that both controller's terminals are assigned to particular zones.

3.2.11. Alarm Zones

Alarm zones enable to define a groups of controllers, which will be armed/disarmed concurrently. Such groups can be armed/disarmed manually or according to administrator defined schedule. It is also possible to define alarm zones hierarchy, so group of controllers could be armed/disarmed in compliance with the hierarchy levels (master-slave). More additional information on Alarm Zones configuration is given in the document [Functional description of PRxx2 series controllers](#).

If a hierarchy between zones is defined, then the superior-subordinate relation can apply to them. The following arming/disarming rules applies in hierarchy:

- ◆ arming the parent zone causes arming all their child zones,
- ◆ disarming the parent zone has no influence on the arming state of child zones,

- ◆ arming the child zone does not cause arming the parent zone,
- ◆ disarming the child zone does not cause disarming the parent zone.

Selecting the **System/Alarm Zones** command, causes displaying directory of alarm zones defined in the system (Figure 3.69).

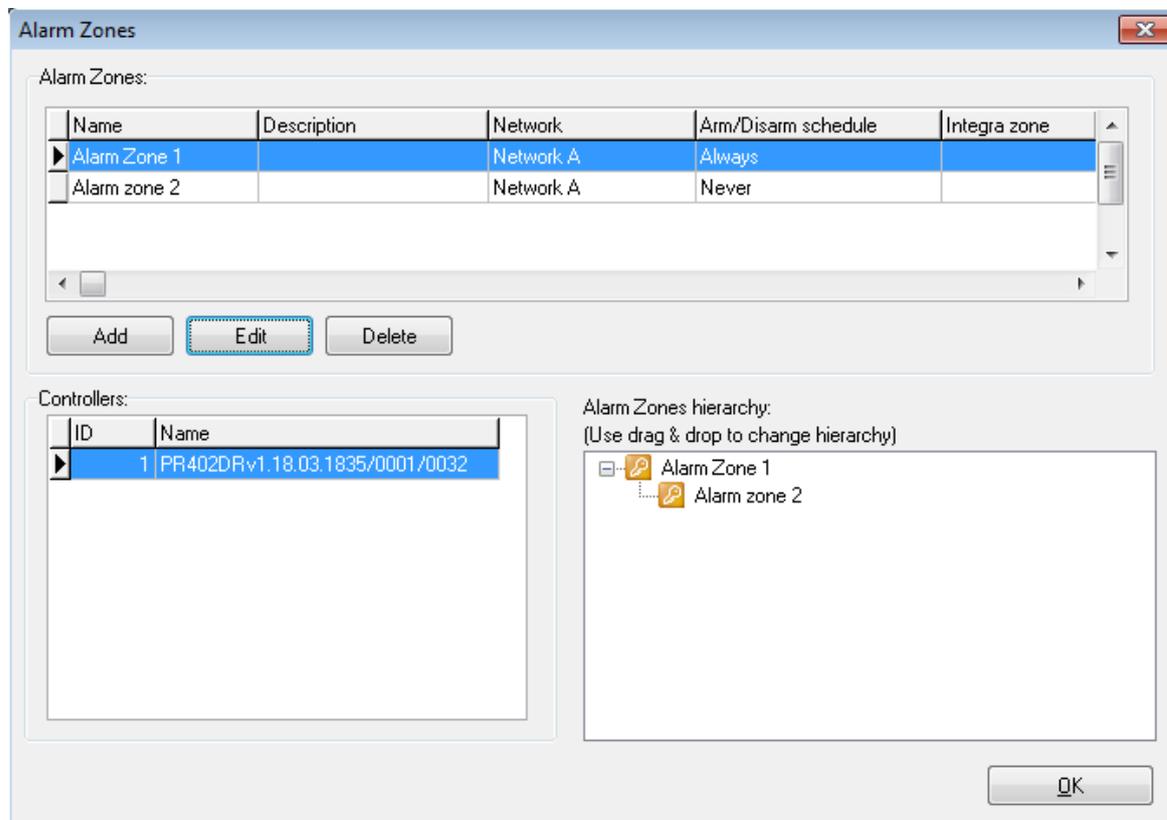


Figure 3.69. Alarm zones directory

Using controls available in this window you can add a new alarm zone (the **Add** button), remove existing alarm zone (the **Delete** button), modify alarm zone's properties (the **Edit** button) and modify alarm zones hierarchy.

3.2.11.1. Adding a new alarm zone

In order to add a new alarm zone, you should click the **Add** button. The **Add new Alarm Zone** dialog box displays (Figure 3.70). Using this window you can define the name for the alarm zone, enter descriptive comment and specify arming schedule for the controllers belonging to the zone. Additionally you can link alarm zone of RACS 4 system with alarm zone of INTEGRA (SATEL) intruder alarm system if such integration, which requires CPR32-NET unit is applied. More information on the integration is given in dedicated manual, which is available at www.roger.pl.

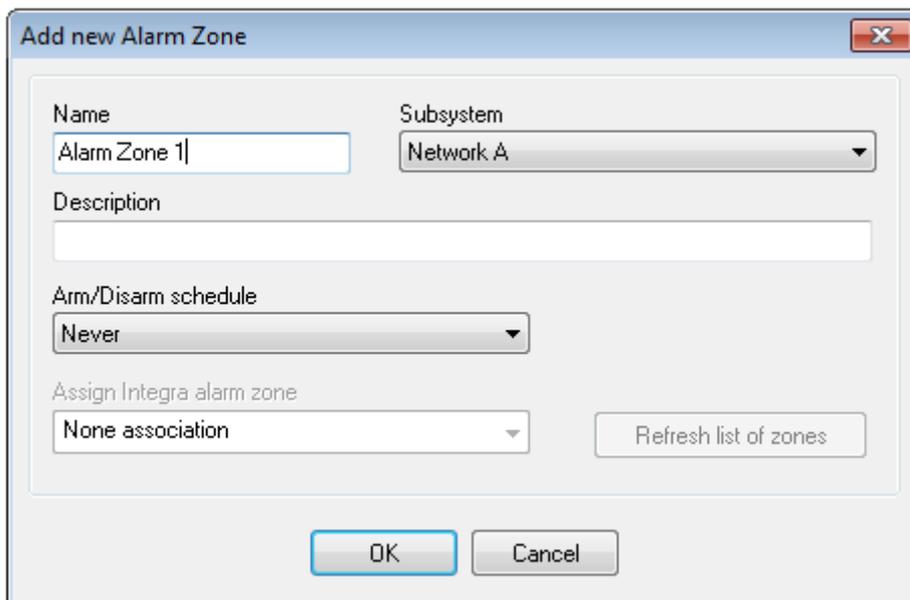


Figure 3.70. Adding a new alarm zone

Immediately after defining the alarm zone, the list of controllers belonging to it is empty. The Alarm zone is completely defined only after you assign controllers to it. It can be done from the controller’s properties window level (see [section 3.2.11.3](#)).

3.2.11.2. Deleting Alarm Zone

In order to delete alarm zone, you should click on the **Delete** button in the **Alarm Zones** dialog box. After the alarm zone is deleted, the system automatically cancels assignment of controllers which belonged to it before (the **None** setting).



You should be careful when using the **Delete** button, because the system does not display any warnings before the alarm zone is deleted. You should absolutely remember to make system’s backups regularly. If you accidentally delete an alarm zone, you will be able to restore it from backup.

3.2.11.3. Assigning Controllers to Alarm Zone

In order to assign a controller to alarm zone, you should open the controller’s properties window. In the **Arming** tab you should specify alarm zone, the particular controller belongs to (Figure 3.71).

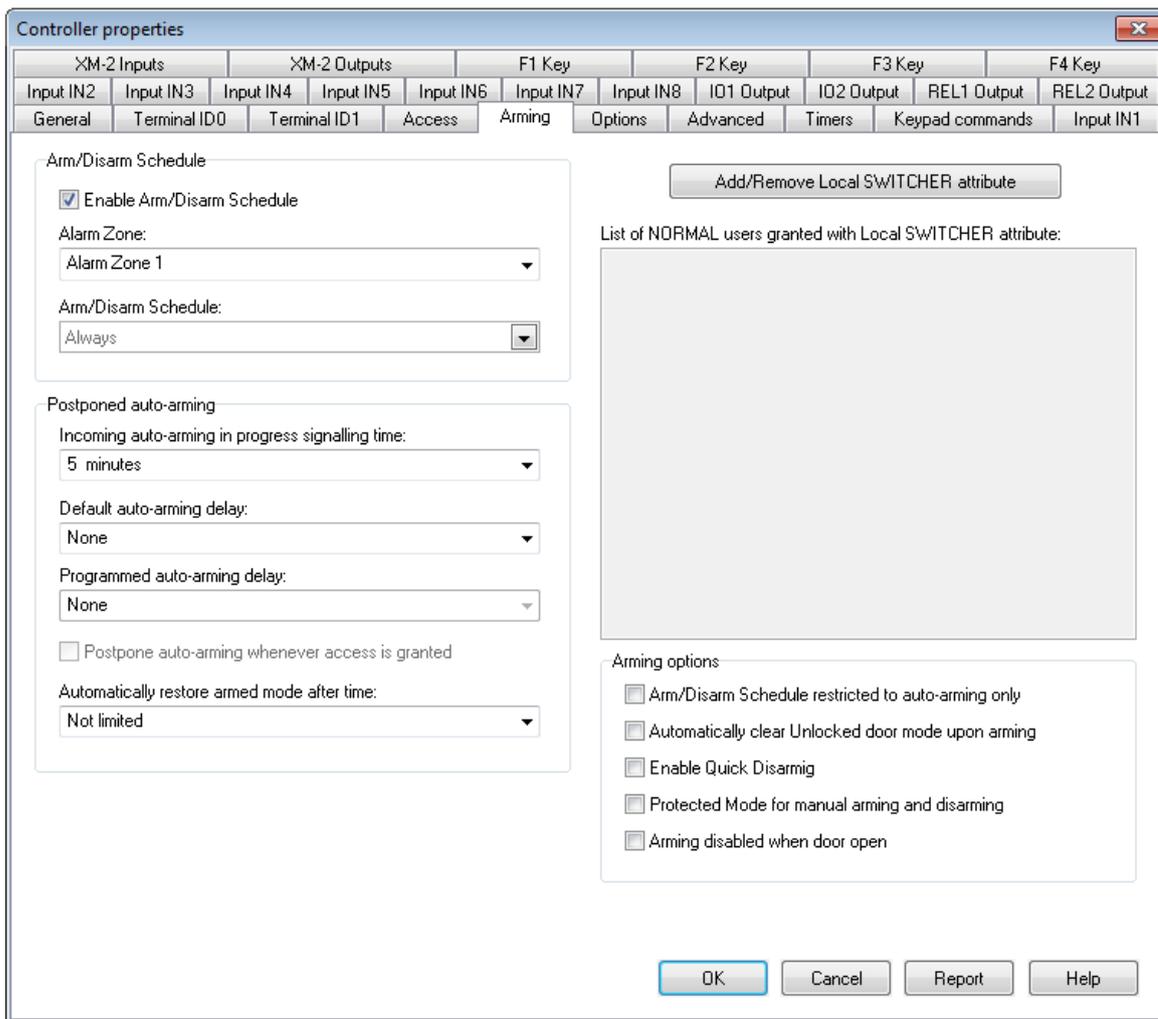


Figure 3.71. Assigning controller to alarm zone

After you confirm the changes, configuration should be sent to the controller. When you open alarm zone directory for the next time, selected controller will display on the controller list belonging to the zone.

3.2.12. Fingerprint readers

In the RACS 4 it is possible to use RFT1000 fingerprint readers and older, not offered for sale F7, F8, F10, F11 fingerprint readers (Fxx series cannot be mixed with RFT1000 in the same system). In case of RFT1000 readers it is recommended to connect them to controller by means of RACS CLK/DTA bus.

The **System/Fingerprint readers** menu command is used for managing readers installed in the system. Selecting this command will cause displaying fingerprint readers directory (Figure 3.72). Detailed description of RFT1000 installation and configuration in RACS 4 system is given in dedicated manual available at www.roger.pl.

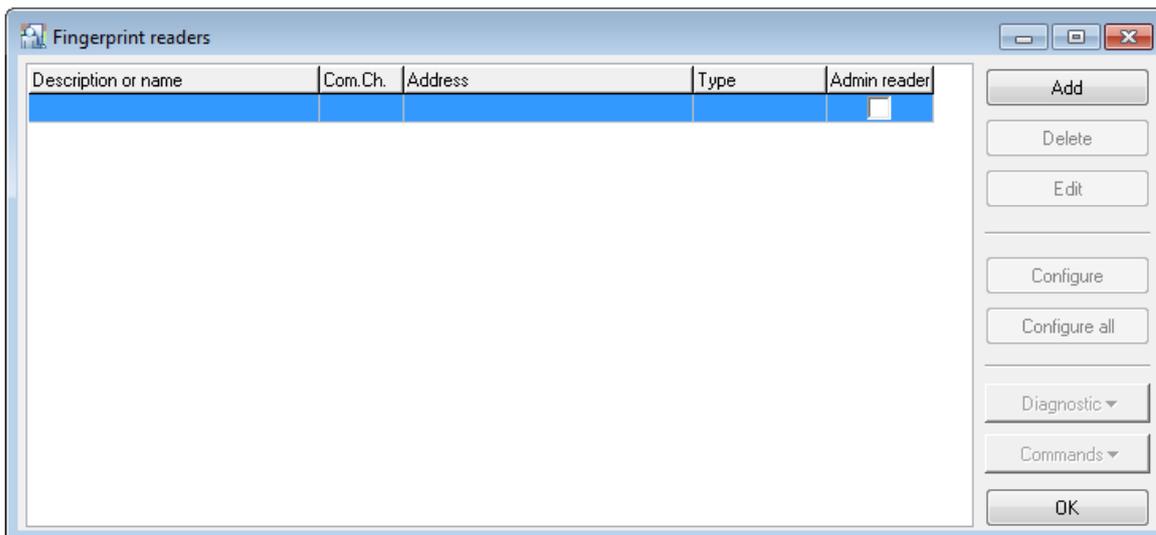


Figure 3.72. *Fingerprint readers directory*

From this window you can perform the following operations:

- ◆ add fingerprint readers,
- ◆ delete fingerprint readers,
- ◆ modify fingerprint readers' settings,
- ◆ configure selected fingerprint reader,
- ◆ configure all the fingerprint readers existing in the system,
- ◆ perform diagnostic operations,
- ◆ upload configuration settings to the selected reader.

3.2.12.1. Adding fingerprint readers

In order to add a new fingerprint reader, you should click on the **Add** button. The **Fingerprint reader configuration** dialog box displays (Figure 3.73).

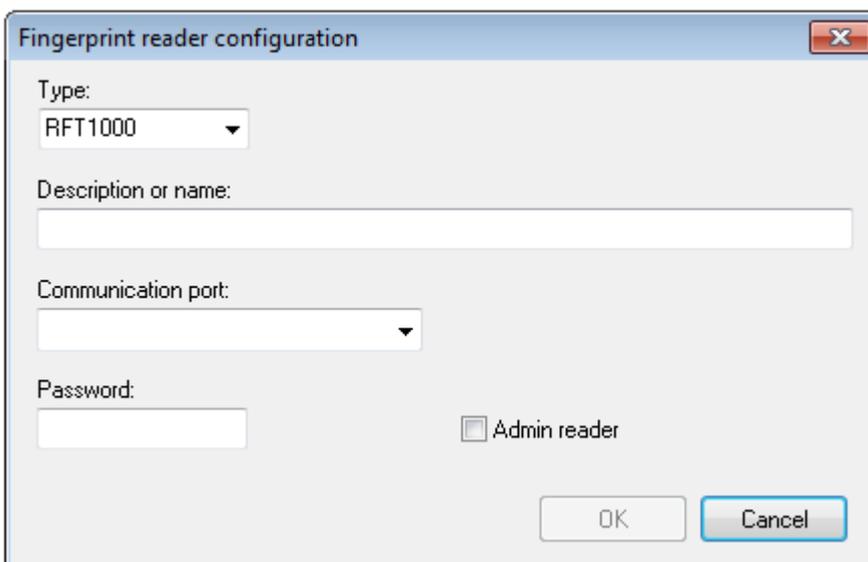


Figure 3.73. *Adding a new fingerprint reader*

In this dialog box you can select type of reader (**Type** field), enter reader's name (**Description or name** field), specify communication port for the reader (**Communication port** field) and optionally define communication password for the reader (**Password** field).

RFT1000 fingerprint readers can be connected to computer with PR Master software via Ethernet or RS-485. Both types of communication require further configuration i.e. respectively IP address and port or ID address (Figure 3.74).

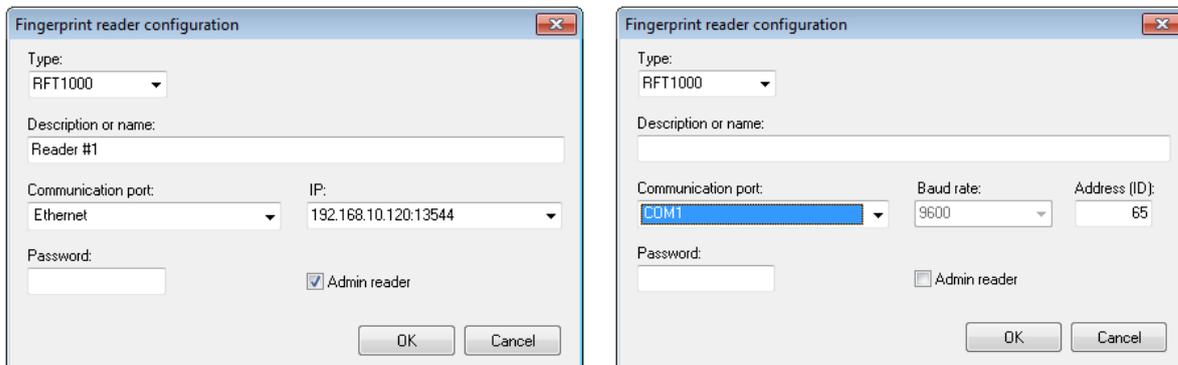


Figure 3.74. Adding a new fingerprint reader (Ethernet or RS485)

After adding a fingerprint reader to the system, it will show up in the list of fingerprint readers installed in the system (Figure 3.72). If the list of fingerprint readers is not empty, two additional buttons will be enabled: **Delete** and **Edit**. They allow for removing selected fingerprint reader from the system and changing its configuration respectively.

3.2.12.2. Removing fingerprint readers

In order to delete fingerprint reader from the system, you should click on the **Delete** button. Before the fingerprint reader is deleted, the system will display confirmation dialog box asking if you are sure to delete the reader. If you answer **Yes**, the fingerprint reader will be removed from the system.

3.2.12.3. Browsing (Modifying) Fingerprint Readers Settings

Clicking on the **Edit** button displays the **Fingerprint reader configuration** window with configuration data of the fingerprint reader selected. Using this window you can modify reader's name, change port and optionally enter new password (Figure 3.75).

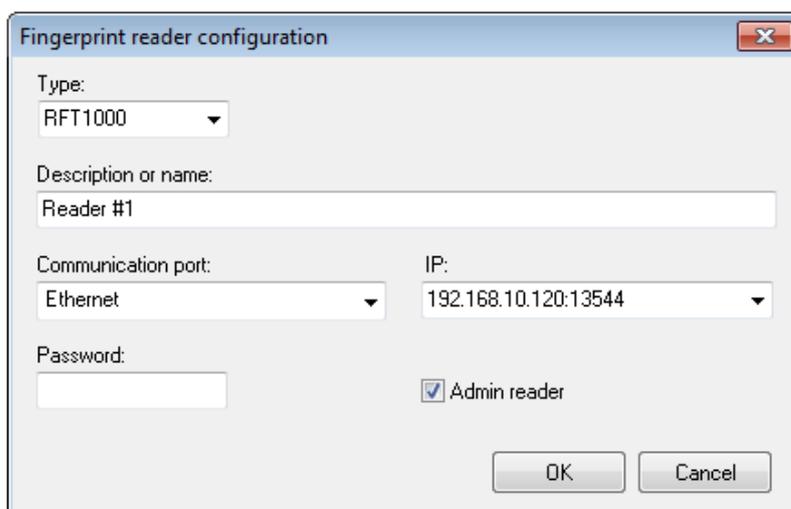


Figure 3.75. Modifying fingerprint readers' settings

3.2.12.4. Configuring fingerprint readers in the system

After you make configuration changes in the fingerprint reader’s settings window, you should send the changes to the reader. Only after the changes are sent they will have effect in the Access Control System. In order to send configuration, you should select a controller in the controllers list and click the **Update** button. The PR Master will communicate with fingerprint reader selected in the list and write changed settings into it. If this operation completes successfully, the system displays an appropriate message. A message will be displayed also in case when communication problems occur.

It is also possible to configure all the fingerprint readers installed in the system, In order to do this, you should click on the **Configure all** button. .

3.2.12.6. Performing diagnostic operations

The **Diagnostics** button gives access to the diagnostic operations menu (Figure 3.76). From this menu you can perform various actions in order to verify reader’s operation. You can read a reader’s firmware version, its MAC number, number of users and fingerprint templates in reader.

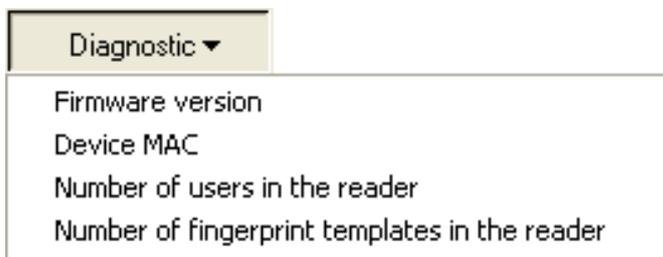


Figure 3.76. Diagnostic operations menu

3.2.12.7. Upload Configuration Settings to the Selected Reader

The **Commands** button gives access to the command menu for the selected fingerprint reader. Using these commands you can reset device or remove all the users stored inside. The **Commands** menu has been shown in Figure 3.77.



Figure 3.77. The Commands menu allows to send commands to the selected fingerprint reader

3.2.13. Card Box

The **Card Box** command opens proximity cards directory containing cards which have been registered in the system. This is a tool, which allows to manage cards in the RACS 4. Thanks to this tool, you can read a group of cards into the system, and then to assign them to users. This way, an operation of defining user does not require access to the reader.

If you select this command, the dialog box with card directory displays (Figure 3.78).

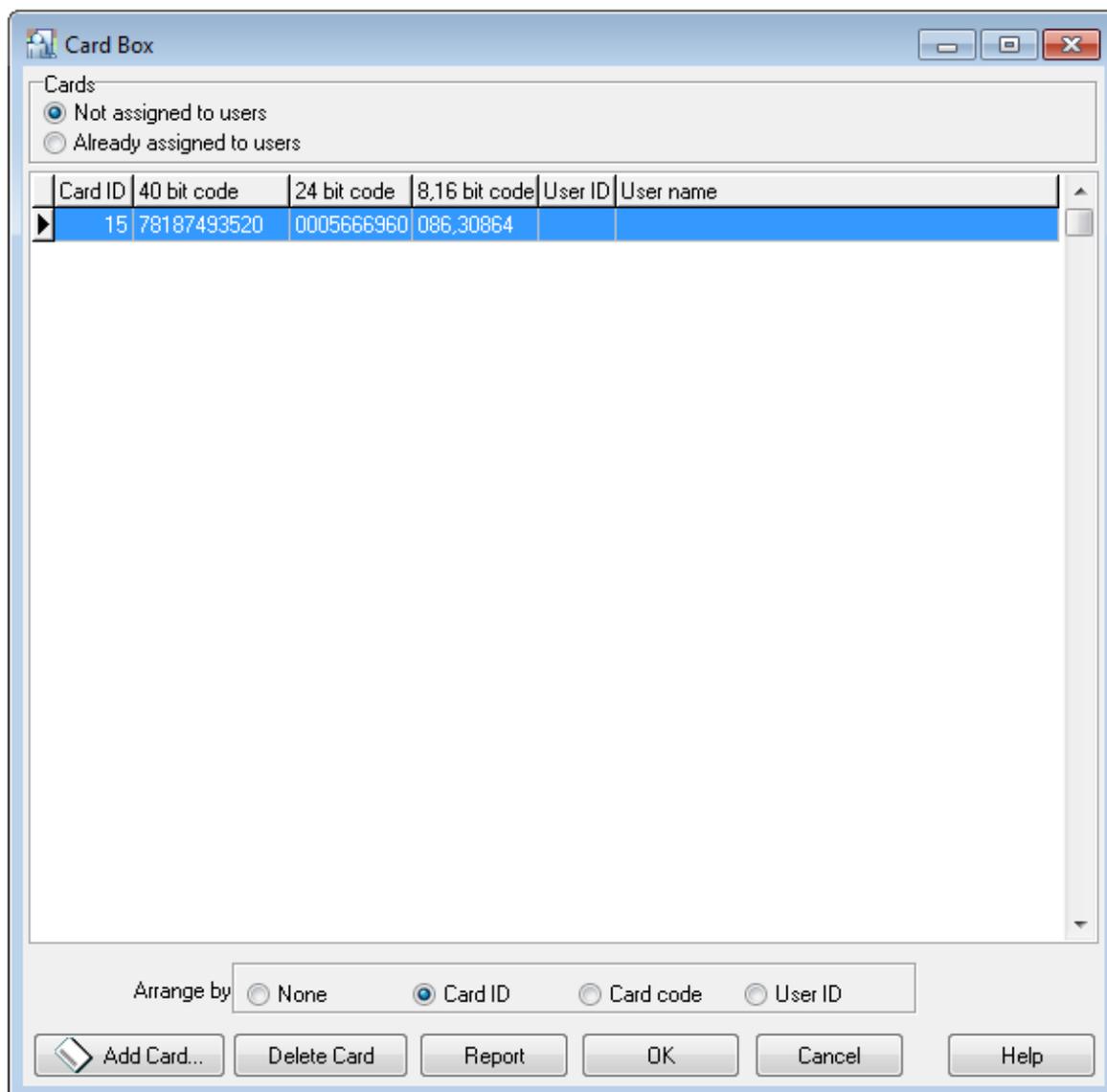


Figure 3.78. Directory of proximity cards registered in the RACS 4

From this window you can perform the following operations:

- ◆ display a list of unassigned cards existing in the system,
- ◆ show a list of cards which have been assigned to users,
- ◆ add a card to Card Box,
- ◆ sort a list according to the selected criteria,
- ◆ print report related to proximity cards registered in the system.

Showing a list of unassigned cards in the system

In order to show a list of cards which were not assigned to anybody in the system, you should click on the **Not assigned to users** radio button in the upper part of dialog box. The system will automatically show a list of cards which are present in container, but which were not assigned to any user.

Showing a list of cards registered in the system and assigned to users

In order to show a list of proximity cards which were assigned to users in the system, you should click on the **Already assigned to users** radio button in the upper part of the dialog box. System will automatically display a list of cards assigned to users (Figure 3.79).

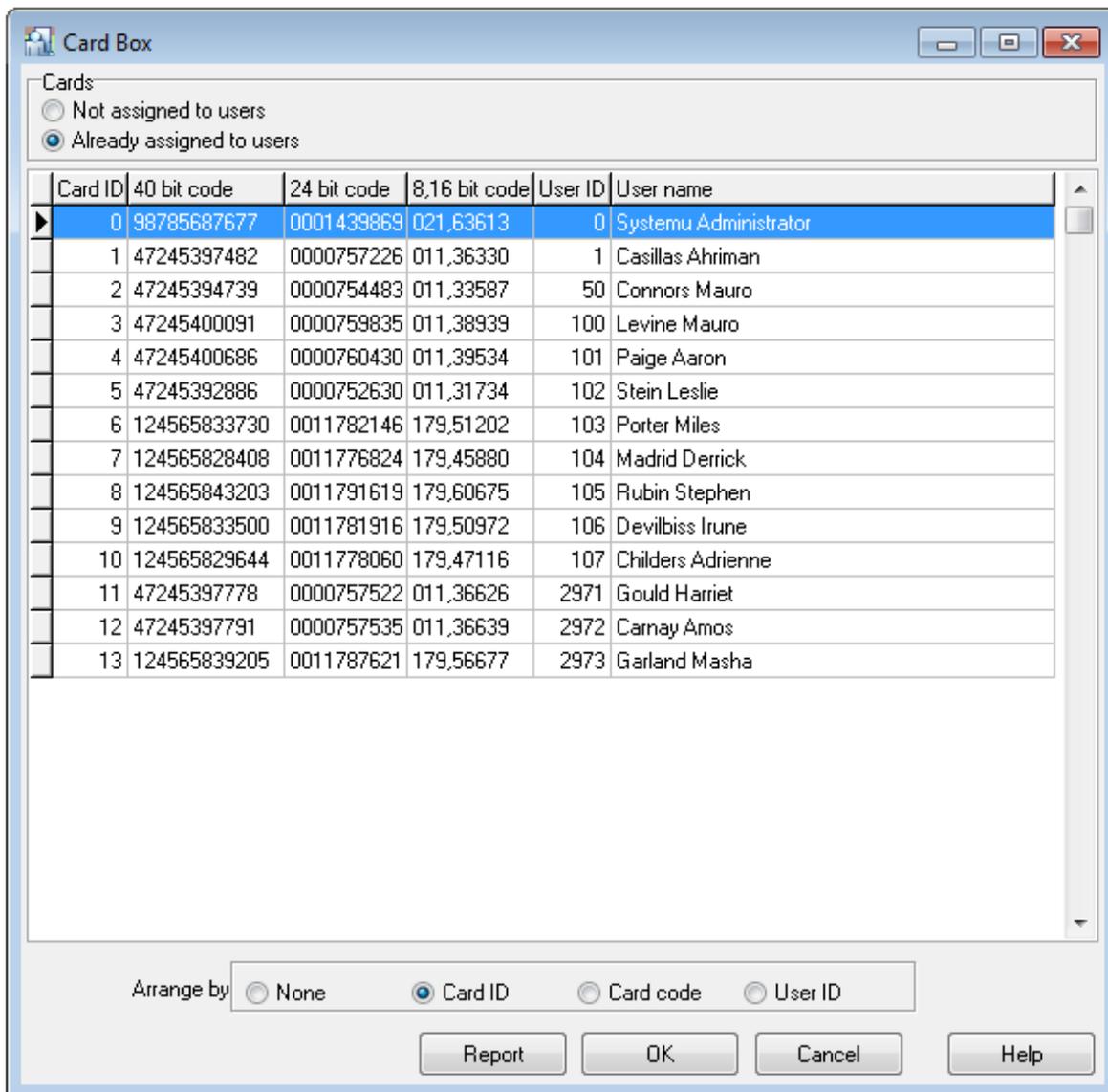


Figure 3.79. List of cards registered in the system which have been assigned to users

Adding card to Card Box

In order to add a new card to Card Box, first you should select the **Not assigned to users (free)** radio button. In reply, the program displays a list of cards which were registered in the system and not assigned to any user, and the **Add Card...** button appears on the bottom.

To initiate operation of adding a new card, you should click on the **Add Card...** button. In response the system displays the **Read card code** dialog box (Figure 3.80), where you can select reader used for reading a card.

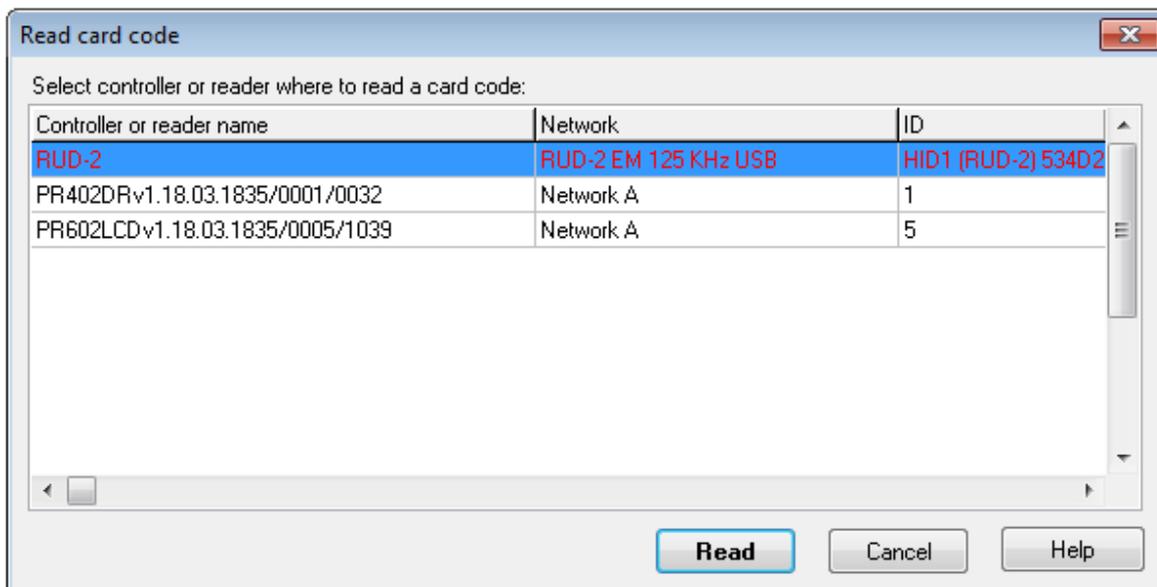


Figure 3.80. Reading card being added to Card Box

First, you should select a reader, which will be used for reading a card, and then click on the **Read** button. Then you should read a card using a reader selected. Reading operation may be repeated for additional cards. The system will automatically put them on the list. If card being read was previously registered in the system, the system displays the following warning (Figure 3.81):

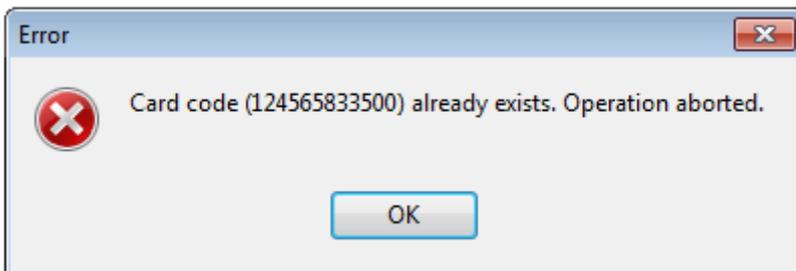


Figure 3.81. Message informing that the card was previously registered in the system

The reading cards operation can be interrupted by clicking on the **Cancel** button.

Deleting card from Card Box

In order to delete a card from the Card Box, you should click on the **Delete card** button. The system will display message box with request for confirmation an intent to remove a card. If you answer **Yes** to this question, the card will be deleted from the list of registered cards.



Only those cards which were not assigned to any users can be deleted from the Card Box. Thus, when the **Not assigned to users** radio button is selected, the **Delete Card** button is not available.

Sorting List According to Selected Criteria

List of cards in container can be sorted according to the following criteria:

- ◆ Card ID,
- ◆ Card Code,

- ◆ by user ID.

The sorting order can be selected using the **Arrange by** radio button. In order to sort cards according to the criteria, you should select a relevant radio button's.

Printing report related to proximity cards registered in the system

The PR Master allows to prepare printed report related to proximity cards registered in the system. This mechanism allows for creating both a list of cards which were not assigned to any users and these, which have already been assigned to users. In order to prepare such report, you should click on the **Report** button in the proximity cards directory window. Sample report for cards already assigned has been presented in Figure 3.82.

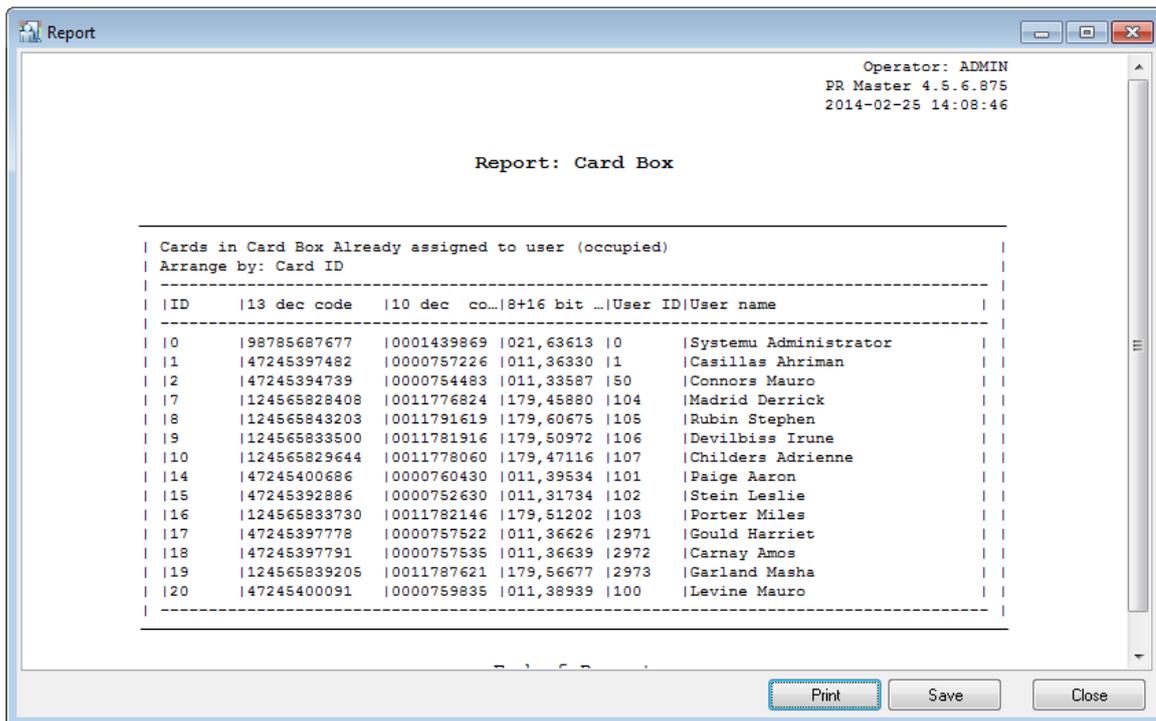


Figure 3.82. Report of proximity cards which were not assigned to system's users

3.2.14. Facility plans

The **Facility plans** command opens directory of facility plans in the RACS 4. The **Facility plan** is a graphic map (i.e construction design) on which selected controllers' icons are located. Facility plans after they are defined can be used in PR Master's monitoring mode using the **View/View Map** command (see **section 4.1.14**). You can define up to 20 individual facility plans in RACS 4.

Selecting the **Facility plan** command causes displaying window with facility plans directory (Figure 3.83).

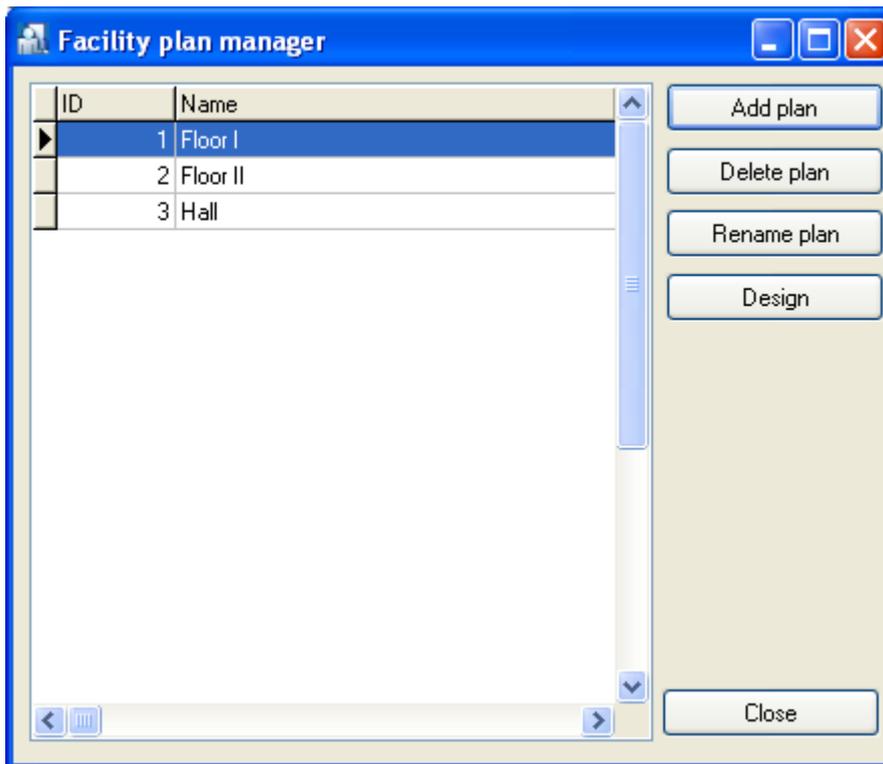


Figure 3.83. Facility plans directory

From this window you can perform the following operations:

- ◆ add a new facility plan — the **Add plan** button
- ◆ delete existing facility plan — the **Delete plan** button,
- ◆ rename existing plan — **Rename plan** button,
- ◆ design layout of controllers icons on the plan and specify graphic file with the background — **Design** button.

3.2.14.1. Adding new facility plan

In order to add a new facility plan, you should click on the **Add plan** button. The **Add facility plan** dialog box displays (Figure 3.84).

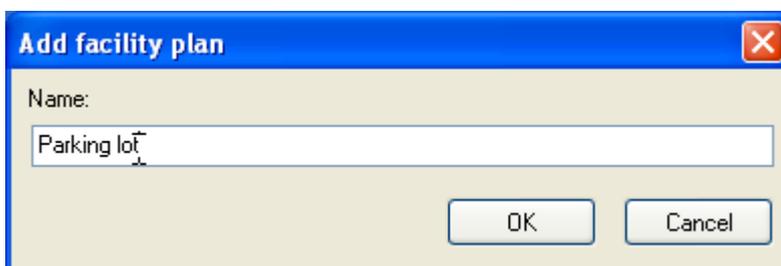


Figure 3.84. Adding new facility plan

In this window you should define a facility plan's name. The name you give here will be later used for identification. After entering the name in the **Name** field, you should click **OK**. The new plan will be added to the facility plans directory at the first free index (Figure 3.85).

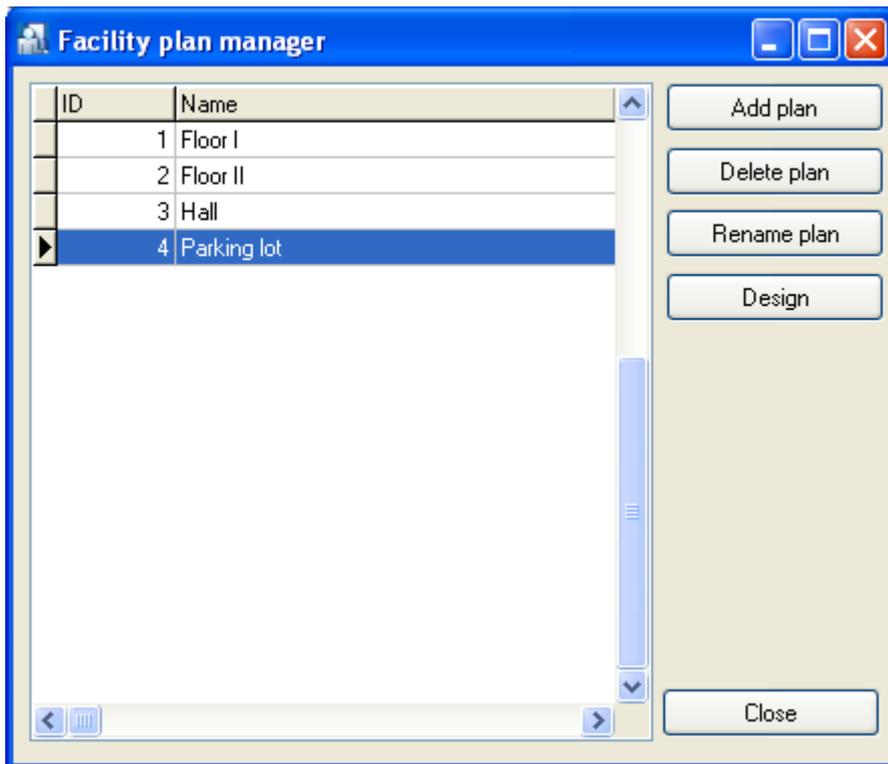


Figure 3.85. New plan — First floor — appeared as 4th in the list

3.2.14.2. Deleting facility plan

In order to delete facility plan you should click on the **Delete plan** button. The **Confirm** window asking for confirmation your intent to delete plan will appear. If you click **Yes**, the selected plan will be permanently deleted from database.



In order to protect yourself against the possibility to permanently delete facility plan from PR Master's database you should make sure, that the system's backups are made regularly. You can find more information on this subject in [section 2.3.2](#).

3.2.14.3. Renaming facility plan

If you want to rename facility plan, you should click on the **Rename plan** button. The **Rename facility plan** dialog box displays (Figure 3.86). You should enter a new facility plan's name in it and then click **OK**.

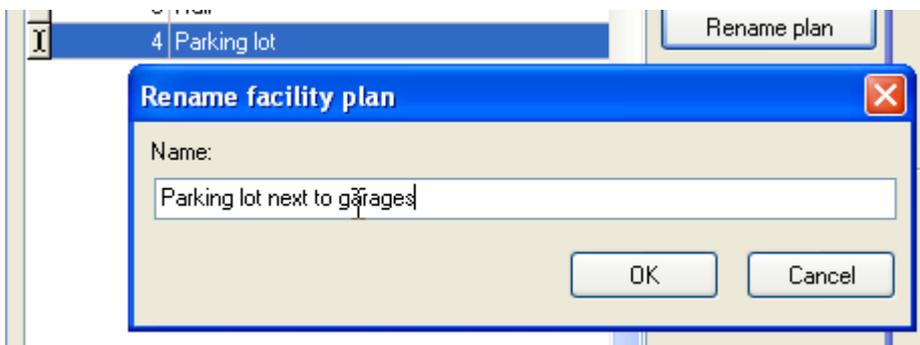


Figure 3.86. Renaming facility plan

3.2.14.4. Designing facility plan

In order to start designing facility plan, you should select it in the plans directory, and then click the **Design** button. The facility plan's designing window will appear. If this is a new plan, the window will be empty — similarly to the screen shown in Figure 3.87.

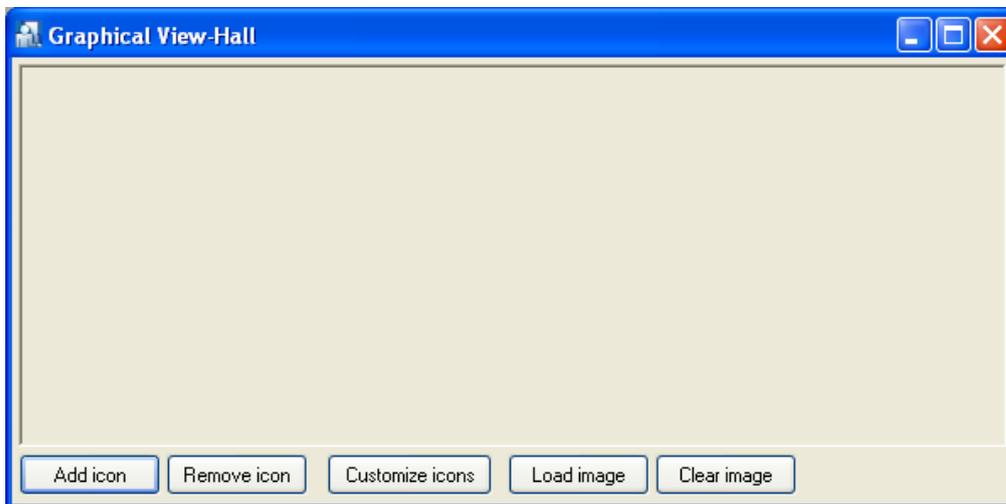


Figure 3.87. Designing facility plan — initial screen

You should start designing a facility plan by loading specific graphical sketch. It can be a constructional design of a floor or a map of a facility where access controllers were installed. In order to load a plan, you should click on the **Load image** button and select file containing graphical sketch(*jpg, *.bmp). Next you should manipulate with window size in order to adjust it to graphical sketch dimensions. After you perform these operations, the facility plan's designing window can look similar to the window shown in Figure 3.88.

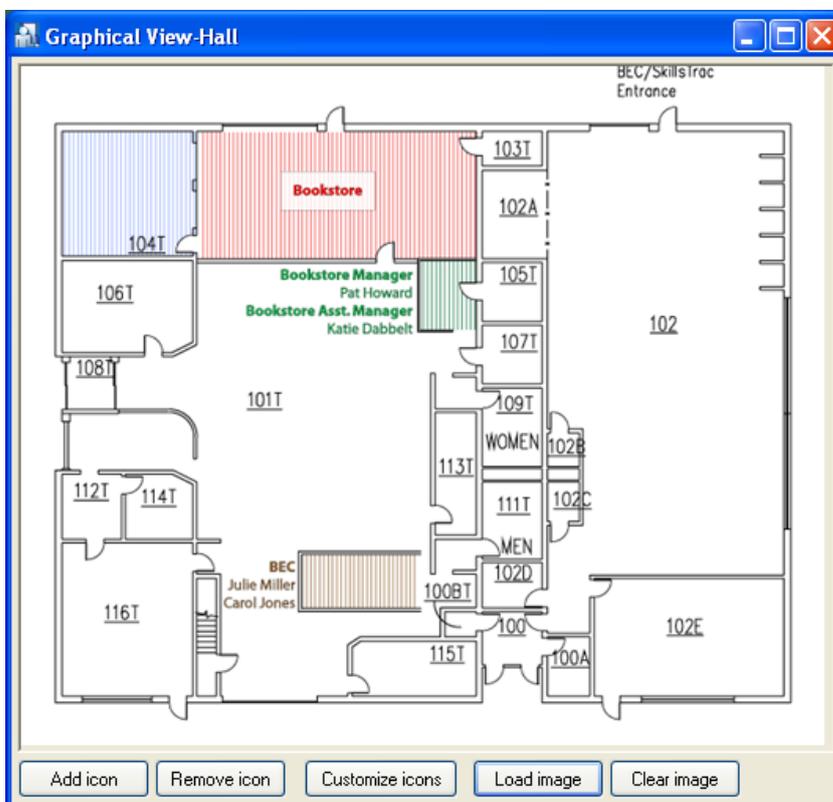


Figure 3.88. Designing facility plan — window after loading a graphical sketch

Now you need to add controllers icons to the plan. Clicking on the **Add icon** button causes displaying a list of available controllers (i.e. those which were not yet added to the plan).

On this list you need select controllers which should be added to the plan (by selecting checkboxes next to them), and then to click **Add selected** button. Immediately after adding icons to the plan, they shall appear on the left upper corner of the window. You should drag them to appropriate positions on the plan, so they could reflect actual location of controllers.

After you dispatch icons on the plan, the designing window can look similar to the window shown in Figure 3.89.

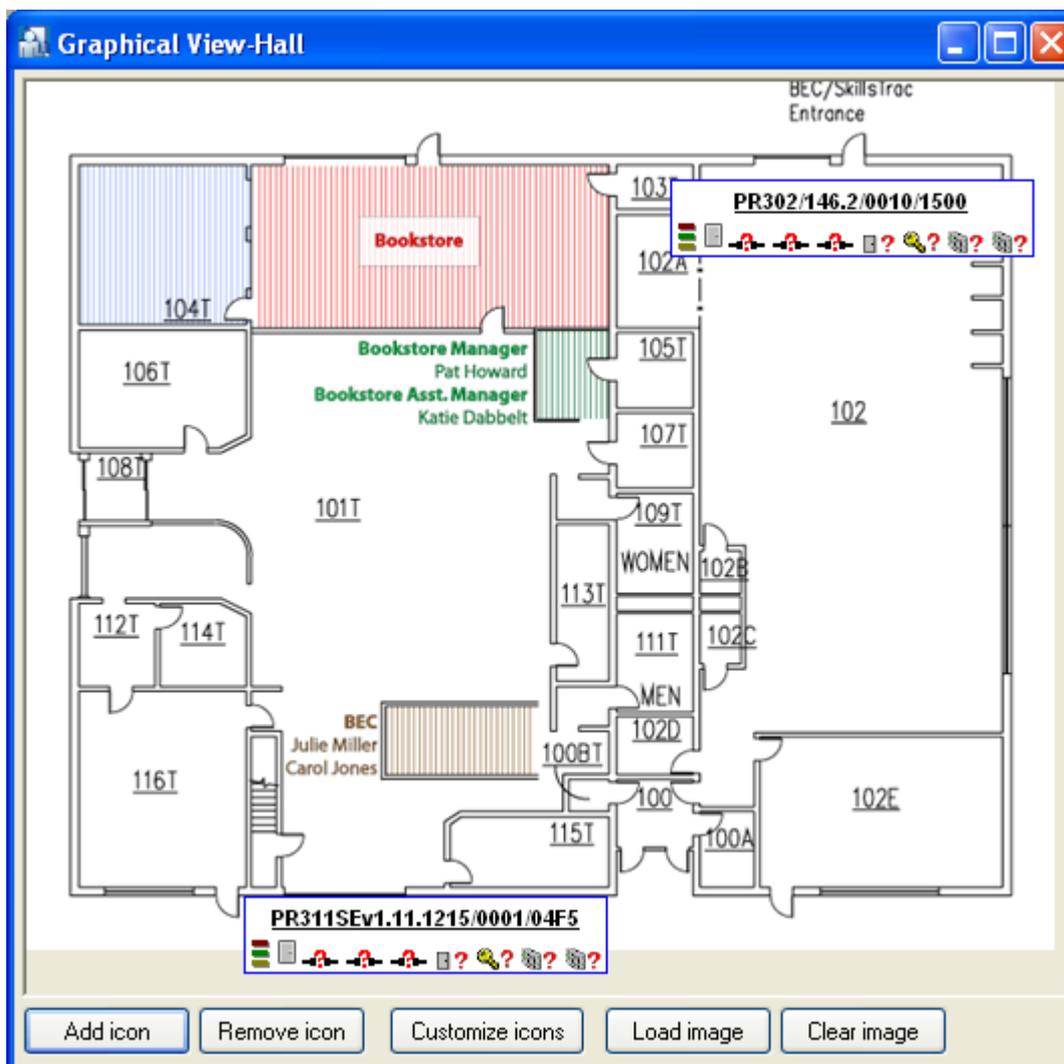


Figure 3.89. Designing facility plan — window after selecting, and dispatching controllers icons

At the end you should adjust a way icons are displayed. Depending on how the plan is detailed, you can customize the way icons are displayed on it.

Customizing icons

Icons can be edited in two ways:

- ◆ by right-clicking selected icon and invoking the **Customize this icon** (**Customize all icons**) command.

or

- ◆ by clicking on the **Customize icons** button.

After you select **Customize icons** command and choose controller to be modified, the **Icon Customization** dialog box displays (Figure 3.90).

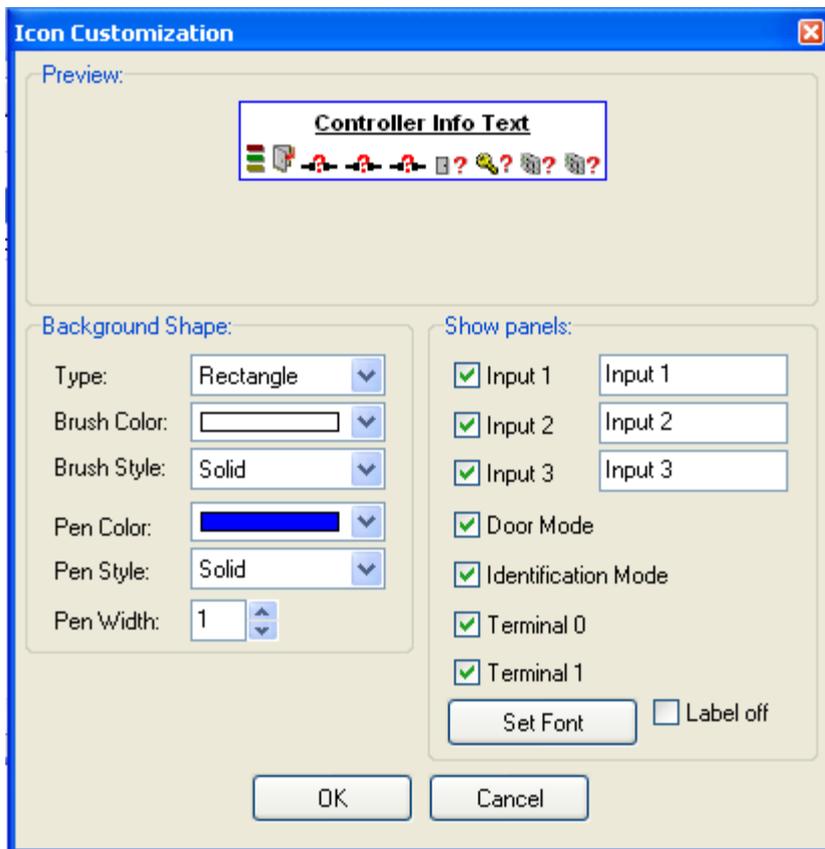


Figure 3.90. Customizing icons

Using this dialog box you can customize a way the icon is displayed on the map.

If you want the icon to represent only minimum information about the controller, you can clear checkboxes for particular details. You can even switch displaying label off (then you need to select **Label off** checkbox). The name of controller can be changed in its properties by clicking particular controller in the main window of PR Master software.

After you customize icons appearance, the plan can look similar to the window shown in Figure 3.91.

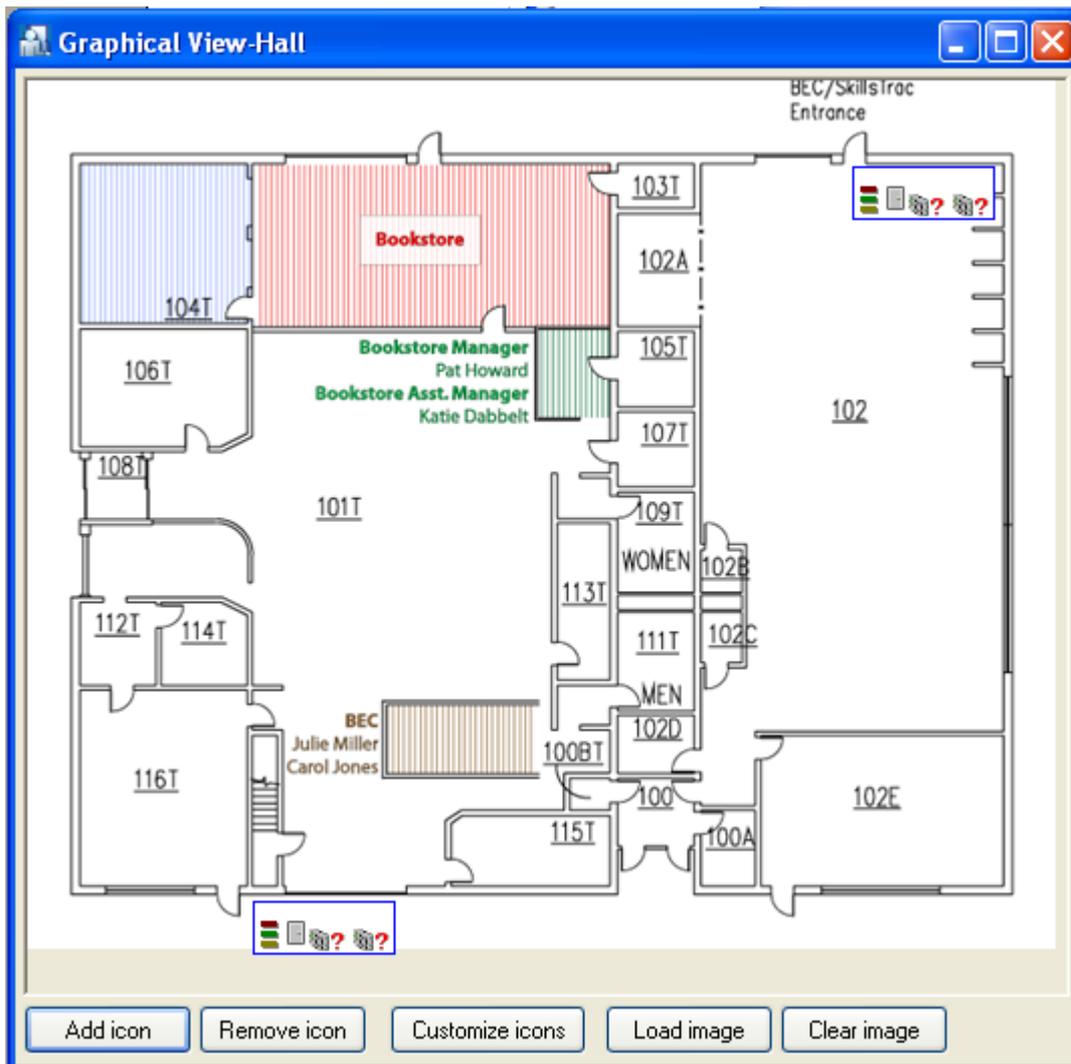


Figure 3.91. Designing facility plan — facility plan’s window in its final form

If you want to save designed plan, you should just close the designing window. You can now make use of the plan in PR Master monitoring mode (more information on using facility plan in monitoring mode is given in [section 4.1.14](#)).

3.2.15. CCTV devices

CCTV devices command is used in the integration of RACS 4 system with CCTV. The integration concerns first of all Dahua and HIK Vision DVR/NVR.

In general perspective, the integration consists in connection of events in access control system with video recorded by CCTV system. The integration was developed for operation in local area network (LAN) but practical tests proved that in many cases it can also be applied successfully in wide area network (WAN). The user can connect more than one DVR with RACS 4 system. As a result of integration following buttons were added in PR Master: **Play CCTV record** and **Real time monitoring** in Online monitoring mode (see [section 4.5](#)) and **Play CCTV record** in Event history (see [section 3.3.7.2](#)).

More information on the integration is given in dedicated manual, which is available at www.roger.pl.

Selection of **CCTV devices** command results in bringing the dialog box shown in fig. 3.92).

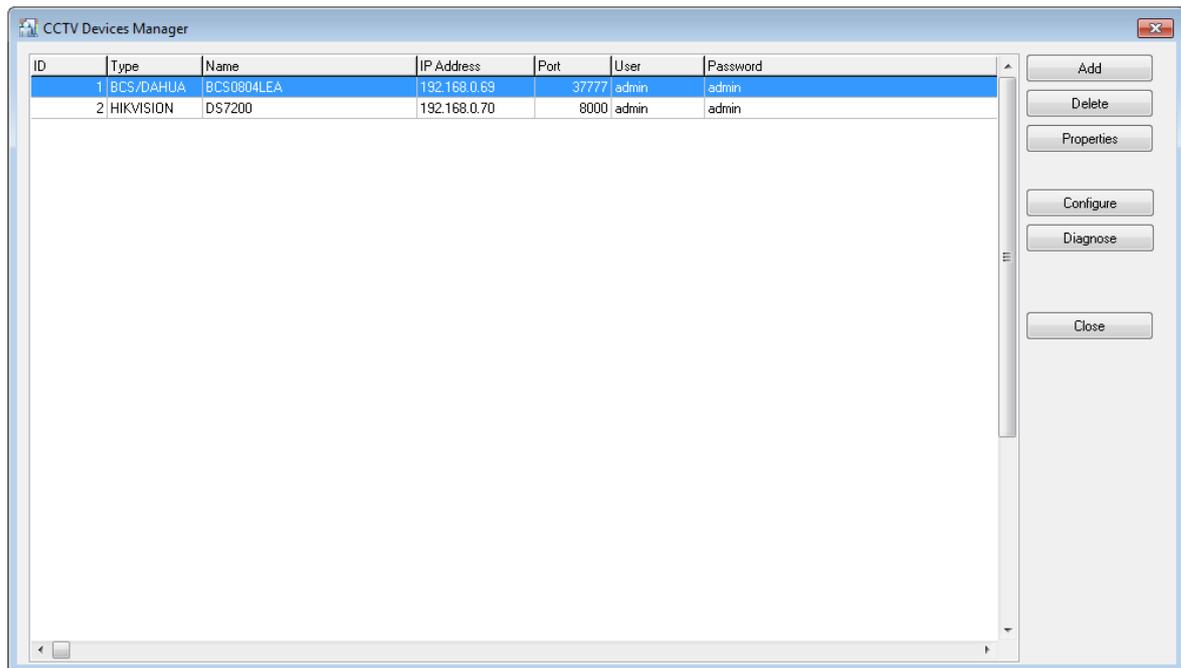


Figure 3.92. *CCTV Devices Manager*

Following buttons are available:

- ◆ **Add** – enables adding of DVR to the list of operating devices.
- ◆ **Delete** – enables deleting of DVR from the list of operating devices.
- ◆ **Properties** – enables modification of already added DVR.
- ◆ **Configuration** – enables configuration of selected DVR i.e. association of its channels (cameras) with readers and selected events.
- ◆ **Diagnose** – enables test of connection with selected DVR i.e. login test.

3.3. REPORTS MENU

The **Reports** menu is shown in Figure 3.93.



Figure 3.93. Reports menu

It contains commands for preparing printed reports related to information entered into the system. Most of commands in this menu causes displaying reports in **Report** window. There are two buttons available in this window. The **Print** button allows for printing report on the printer, and the **Save** button allows for saving report in **.rtf** or **.csv** documents.

3.3.1. Groups

The **Group** command causes displaying report containing information on groups defined in the system. The same report may be generated using **Report** button in the main window of the group directory. Selecting the **Report/Group** command causes displaying **Group** report in **Report** window (see [section 3.2.5.4](#)).

3.3.2. Users

The **Users** command causes displaying report containing information on users defined in the system. The same report may be generated using **Report** button in the main window of the users directory. Selecting the **Report/Users** command causes displaying **Users** report in **Report** window (see [section 3.2.3.5](#)).

3.3.3. Access zones

The **Zones** command causes displaying report containing information on access zones defined in the system. The same report may be generated using **Report** button in the main window of the access zones directory. Selecting the **Report/Zones** command causes displaying **Zones** report in **Report** window (see [section 3.2.7.4](#)).

3.3.4. Networks

The **Networks** command causes displaying report containing information on networks defined in the ACS. The same report may also be generated using **Report** button in the main window of the networks directory. Selecting the **Report/Networks** command causes displaying **Networks** report in **Report** window (see [section 3.2.8.8](#)).

3.3.5. Controllers

The **Controllers** command causes displaying report containing information on settings for all the controllers installed in the ACS. Similar report may also be generated using **Report** button in the controllers directory window of the selected network. The difference is that the report generated by the **Report/Controllers** command contains information on all the controllers installed in all the networks. Selecting the **Report/Controllers** command causes displaying **Controllers** report in **Report** window (see [section 3.2.8.4](#))

3.3.6. Access rights

Selecting the **Report/Access rights** command causes displaying **Access rights** report in **Report** window (Figure 3.94). This report contains summary list of all the users groups together with their access rights.

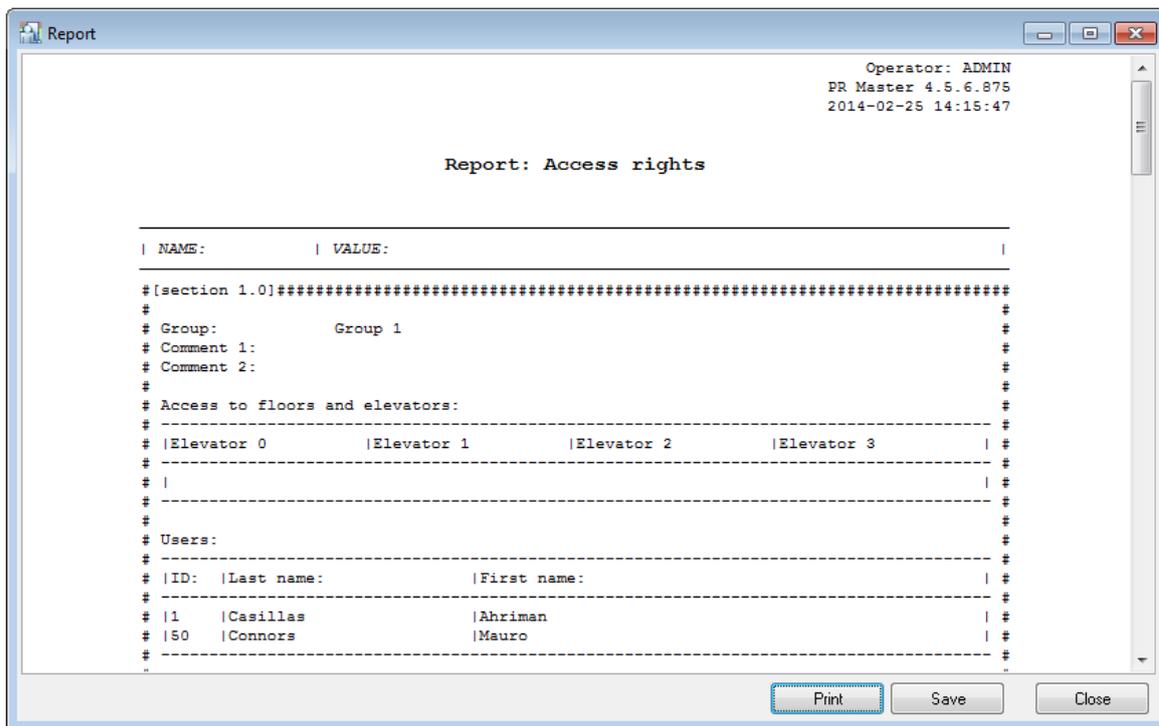


Figure 3.94. The Access rights report

3.3.7. Event history

The **Event history** command allows to prepare detailed events reports, T&A reports and special reports.

If you select this command then events are downloaded to PR Master’s database. In the next step **Event filter** dialog box is displayed (Figure 3.95).

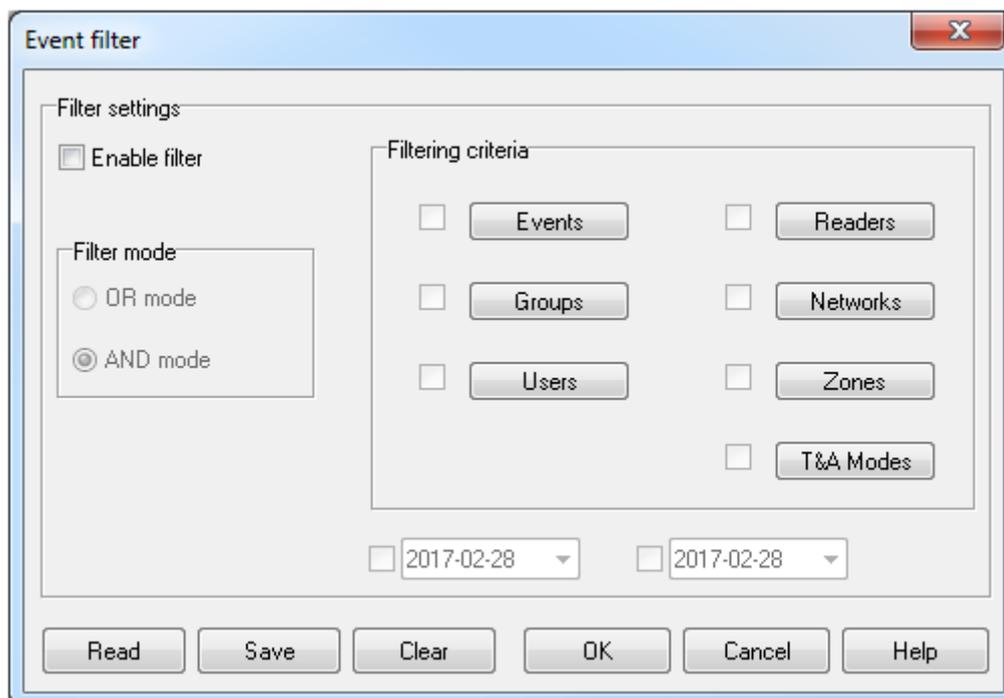


Figure 3.95. Filter settings for Event history

Using this dialog box you can define filter for events and then display for instance only **Access granted** events related to user Jan Kowalski. After the filter is defined, it can be saved to a file. Then you can quickly load from this file an appropriate set of rules.

Default maximal number of events processed and displayed in PR Master history equals to 300 000. It is possible to increase the number of processed events by starting PR Master software with /EVLIMIT=xxxxxx parameter where xxxxxx signifies the number of events. The maximal value of xxxxxx depends on PC computing power and based on practical tests it should not exceed 1 000 000 limit. The parameter does not increase the number of displayed events but allows to reach more events using adequate filters.

3.3.7.1. Defining filter

Before you are able to define a filter, you must select the **Enable filter** check box. It will activate controls for defining a filter. The filter is defined by selecting filter mode (**AND/OR**) and specifying filtering criteria. These criteria can be defined for seven parameters: event types, groups, users, readers, networks, zones and T&A modes. These parameters have corresponding buttons in the **Filtering criteria** area. In order to define criteria for the specific parameter, you should select checkbox next to the particular button. Then you should click on the button and define criteria.

Let us assume, that we want to include in event report only **Access granted** and **Access denied** events for users belonging to the **Group 2**. In order to define such a filter, we select a filter mode **AND** and checkboxes next to **Events** and **Groups** buttons. Then we click on the **Events** button. This will cause displaying **Events** dialog box (Figure 3.96).

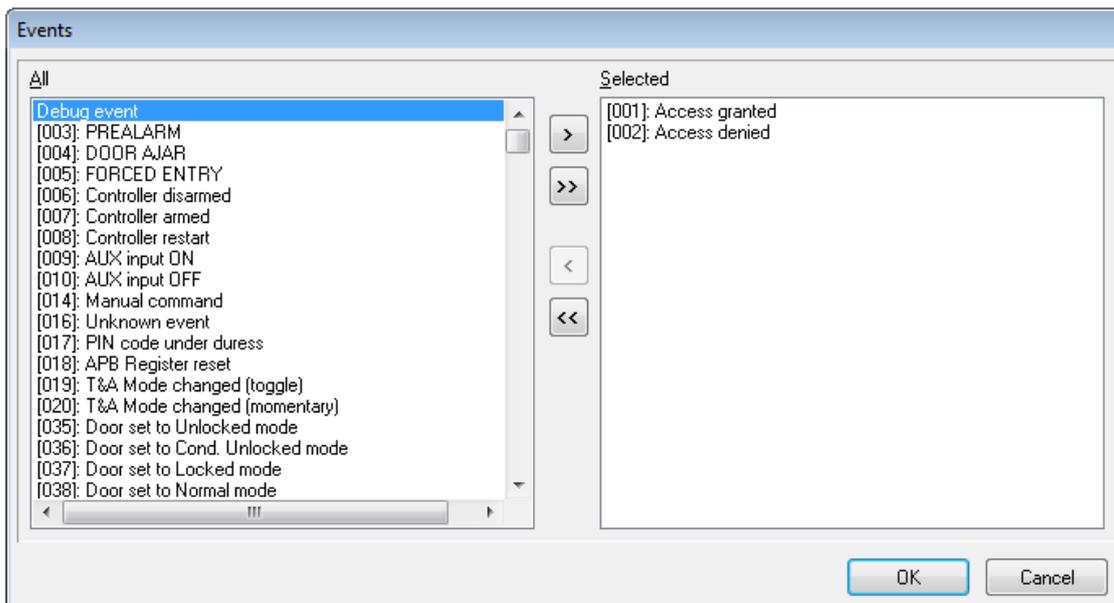


Figure 3.96. Defining filter criteria — event type

On the left side of the window there is list of events which have not been selected. Thus they will not show up in the report. If you double click an event on this list, it will be moved into the **Selected** list. You can also select a particular event and click on the > button. Clicking on the >> button will cause moving to the **Selected** list all the events from left side of the window. Selected events are deleted in a similar way. Double clicking an event on the list **Selected** will move it to the **All** list. You can also select a particular event and click on the < button. Clicking on the << button will cause moving to the **All** list, all the events currently present in the list on right side of the window.

Coming back to our example, in order to define a desired filter, you should double click entries corresponding to **Access granted** and **Access denied** events and click on the **OK** button. The event selection window closes, and we return back to the **Event filter** window. Now we click on the **Groups** button. This will cause displaying **Groups** dialog box (Figure 3.97).

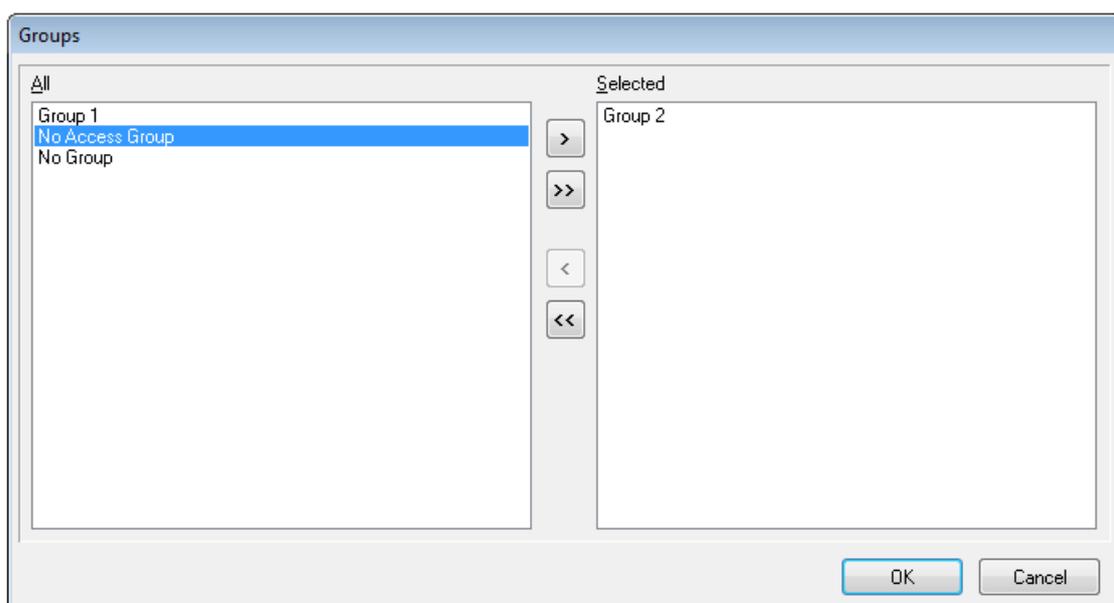


Figure 3.97. Defining event filter criteria — groups

We should select **Group 2** group and click **OK**.

You have successfully defined your first filter! In the event report there will be all the events of **Access granted** and **Access denied** type for **Group 2**. In a similar manner filter criteria for users, readers, networks, zones and T&A modes can be defined.

The filter defined in this way can be saved in a file. In order to do this, you should click on the **Save** button in the **Event filter** dialog box. Then, you should point a location, the file with filtering criteria should be saved (the file will have an **.rmf** extension) — Figure 3.98.

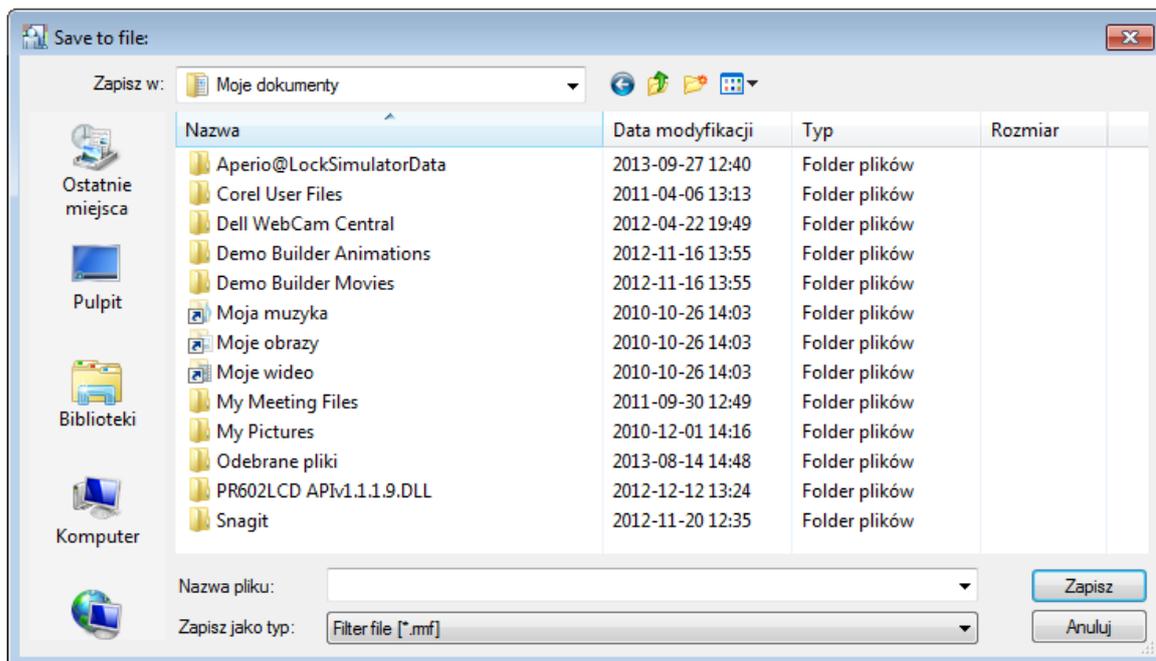


Figure 3.98. Saving filtering criteria to a file

The **Clear** button allows for clearing filter criteria defined so far. After clearing all the criteria defined earlier, you can start defining filter from scratch or read a filter defined earlier from a file. The second method is possible using the **Read** button. If you click on it, the **.rmf** file selection window appears. In order to load filter criteria defined earlier, you should select file containing the filter and click on the **Open** button.

Below the **Filtering criteria** area in the **Filter settings** dialog box, there are two date fields. The one shown on the left defines the start date, and the one of the right the end date. These dates specify time period for which an event report will be generated. With date fields are associated checkboxes (in similar fashion to the buttons in the **Filtering criteria** area). In order to define criteria for the start of period, you should select a checkbox next to the date field on the left, and then enter a date for beginning of period, for which the event report will be generated. Similarly, in order to define criteria for the end of period, you should select a checkbox next to the date field on the right, and then enter a date for the end of period, for which the event report will be generated.

3.3.7.2. Displaying event history

After you finish with defining filter, you should click **OK** in the **Event filter** dialog box. This will cause displaying **Event history** window (Figure 3.99).

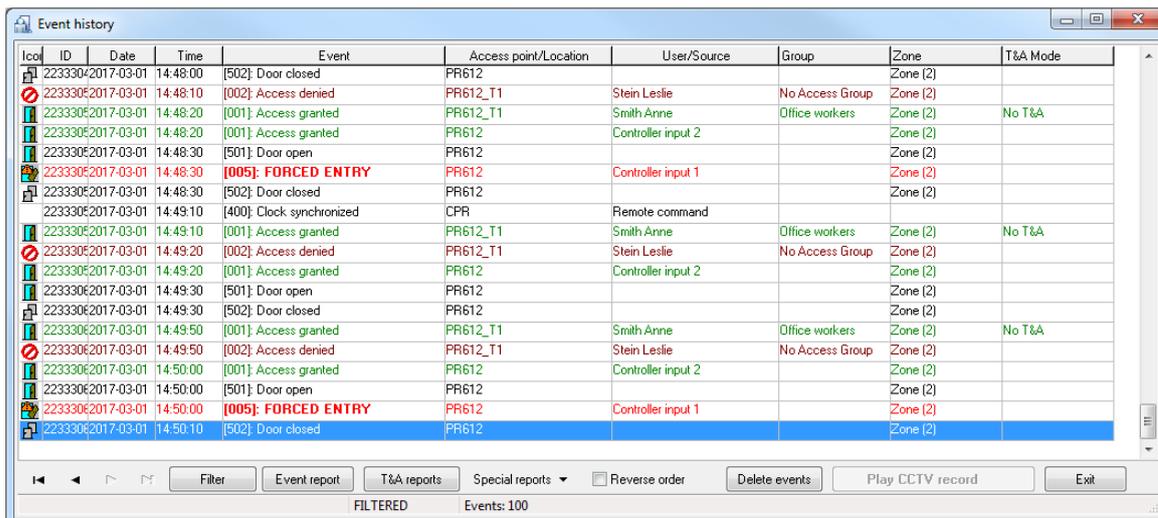


Figure 3.99. Event history

This window allows for browsing/modifying event list before events report is printed. From this level you can also print T&A report or special reports.

Buttons on the left side of the toolbar allow navigation through the events log. They are used for moving to the beginning of the event log, move by one event forward, move by one event backward, and move to the end of the event log respectively.

Clicking on the **Filter** button causes displaying the **Event filter** dialog box again. This way you can update filter defined earlier.

Printing event report

If you click on the **Event report** button, the **Event report format** dialog box will appear (Figure 3.100).

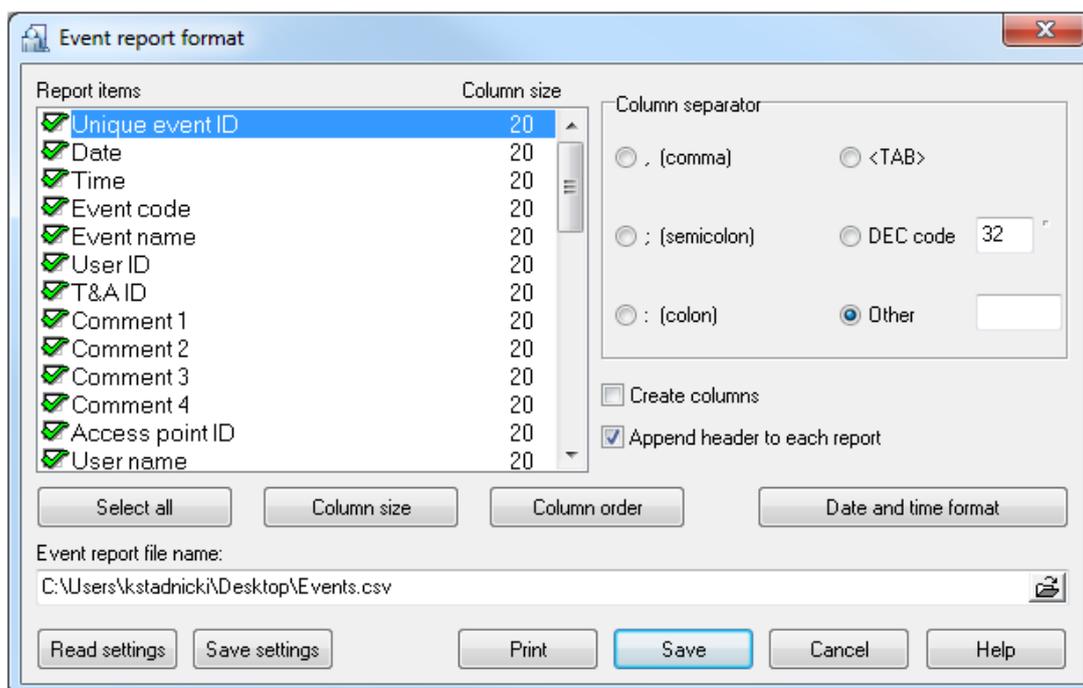


Figure 3.100. Event report settings

Using this dialog box you can configure in detail format of event history printout. You can select columns, which are to appear in the report, specify their width, change column order and set up date and time format.

Event report settings can also be written to a file (the **Save settings** button), and imported from it thereafter (the **Read settings** button).

When all the settings are set, you can click on the **Print** button. This will display report to be printed in the **Print event report** window (Figure 3.101).

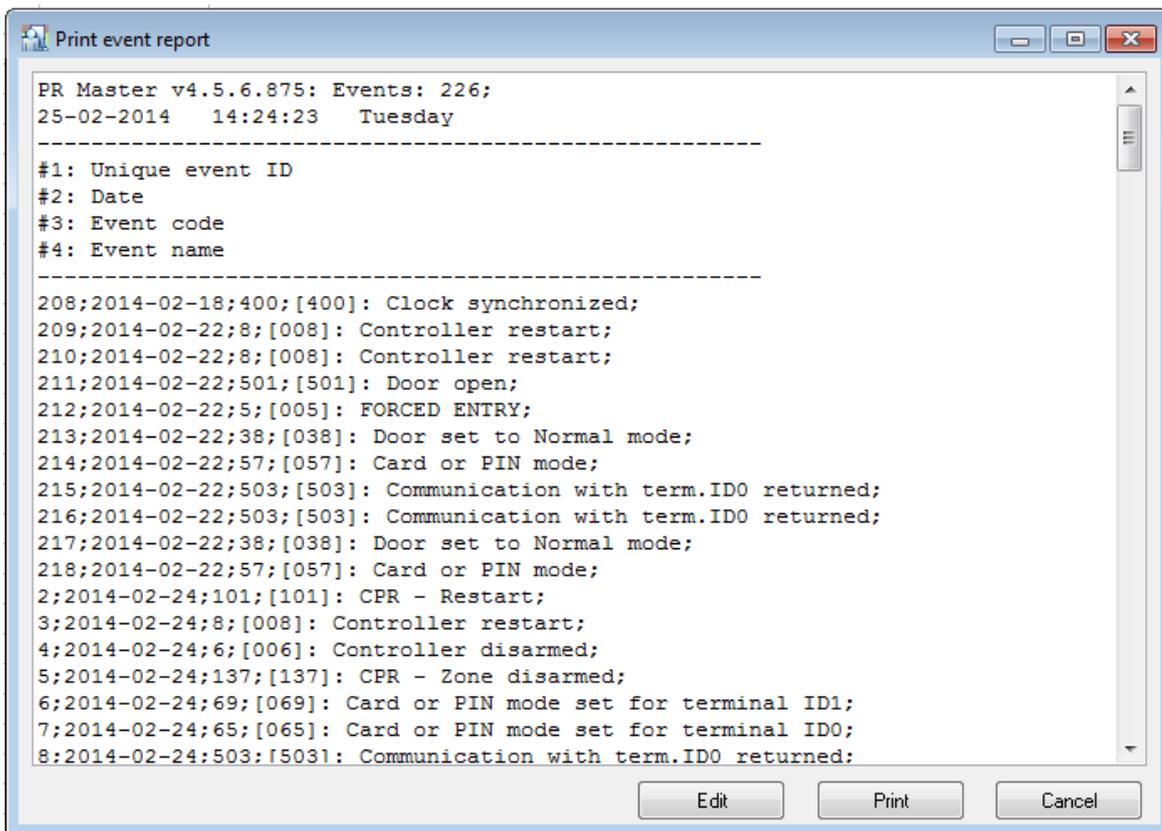
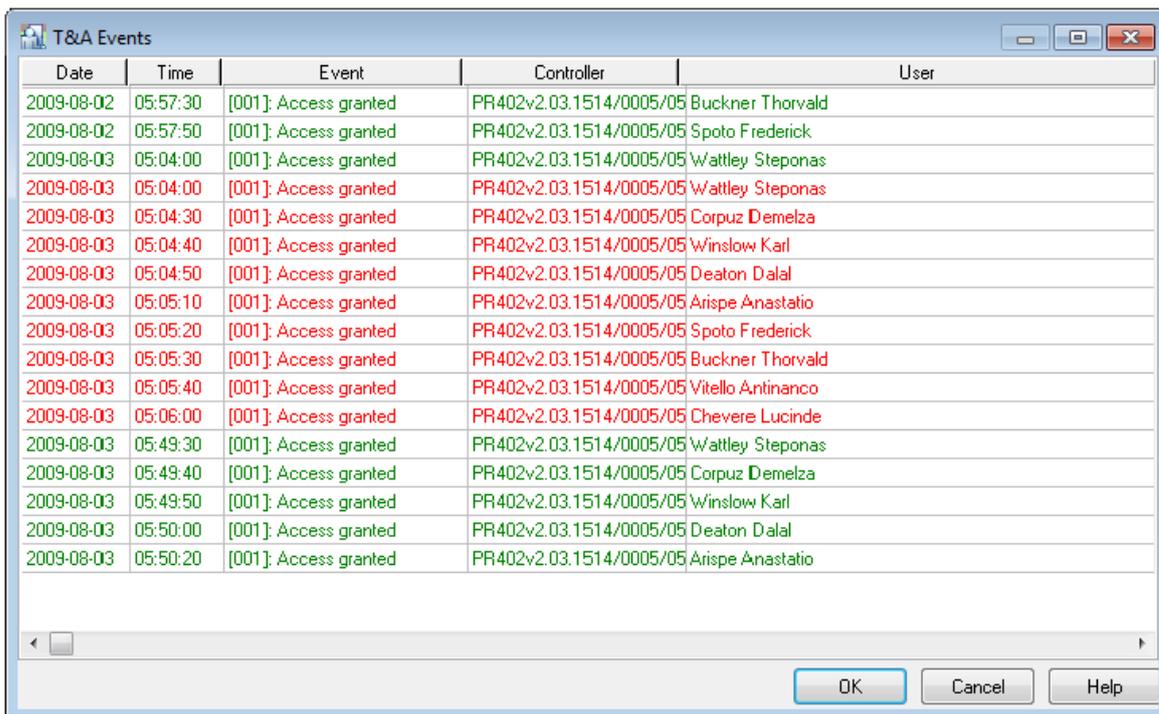


Figure 3.101. Printing Event History report

In order to actually start printing report on a printer, you should click on the **Print** button. Before this is done, you can select printer and configure its options using **Edit** button.

Generating T&A report

If you click on the **T&A reports** button, the **T&A Events** dialog box will appear (Figure 3.102).



Date	Time	Event	Controller	User
2009-08-02	05:57:30	[001]: Access granted	PR402v2.03.1514/0005/05	Buckner Thorvald
2009-08-02	05:57:50	[001]: Access granted	PR402v2.03.1514/0005/05	Spoto Frederick
2009-08-03	05:04:00	[001]: Access granted	PR402v2.03.1514/0005/05	Wattley Steponas
2009-08-03	05:04:00	[001]: Access granted	PR402v2.03.1514/0005/05	Wattley Steponas
2009-08-03	05:04:30	[001]: Access granted	PR402v2.03.1514/0005/05	Corpuz Demelza
2009-08-03	05:04:40	[001]: Access granted	PR402v2.03.1514/0005/05	Winslow Karl
2009-08-03	05:04:50	[001]: Access granted	PR402v2.03.1514/0005/05	Deaton Dalal
2009-08-03	05:05:10	[001]: Access granted	PR402v2.03.1514/0005/05	Arispe Anastatio
2009-08-03	05:05:20	[001]: Access granted	PR402v2.03.1514/0005/05	Spoto Frederick
2009-08-03	05:05:30	[001]: Access granted	PR402v2.03.1514/0005/05	Buckner Thorvald
2009-08-03	05:05:40	[001]: Access granted	PR402v2.03.1514/0005/05	Vitello Antinanco
2009-08-03	05:06:00	[001]: Access granted	PR402v2.03.1514/0005/05	Chevere Lucinde
2009-08-03	05:49:30	[001]: Access granted	PR402v2.03.1514/0005/05	Wattley Steponas
2009-08-03	05:49:40	[001]: Access granted	PR402v2.03.1514/0005/05	Corpuz Demelza
2009-08-03	05:49:50	[001]: Access granted	PR402v2.03.1514/0005/05	Winslow Karl
2009-08-03	05:50:00	[001]: Access granted	PR402v2.03.1514/0005/05	Deaton Dalal
2009-08-03	05:50:20	[001]: Access granted	PR402v2.03.1514/0005/05	Arispe Anastatio

Figure 3.102. Generating T&A report

Different events are marked with different colors depending on T&A mode. For example, all entries are marked in red, all exits — in green, and exits on duty are marked in blue.

Clicking on the **OK** button, allows writing T&A report in many different formats (Figure 3.103).

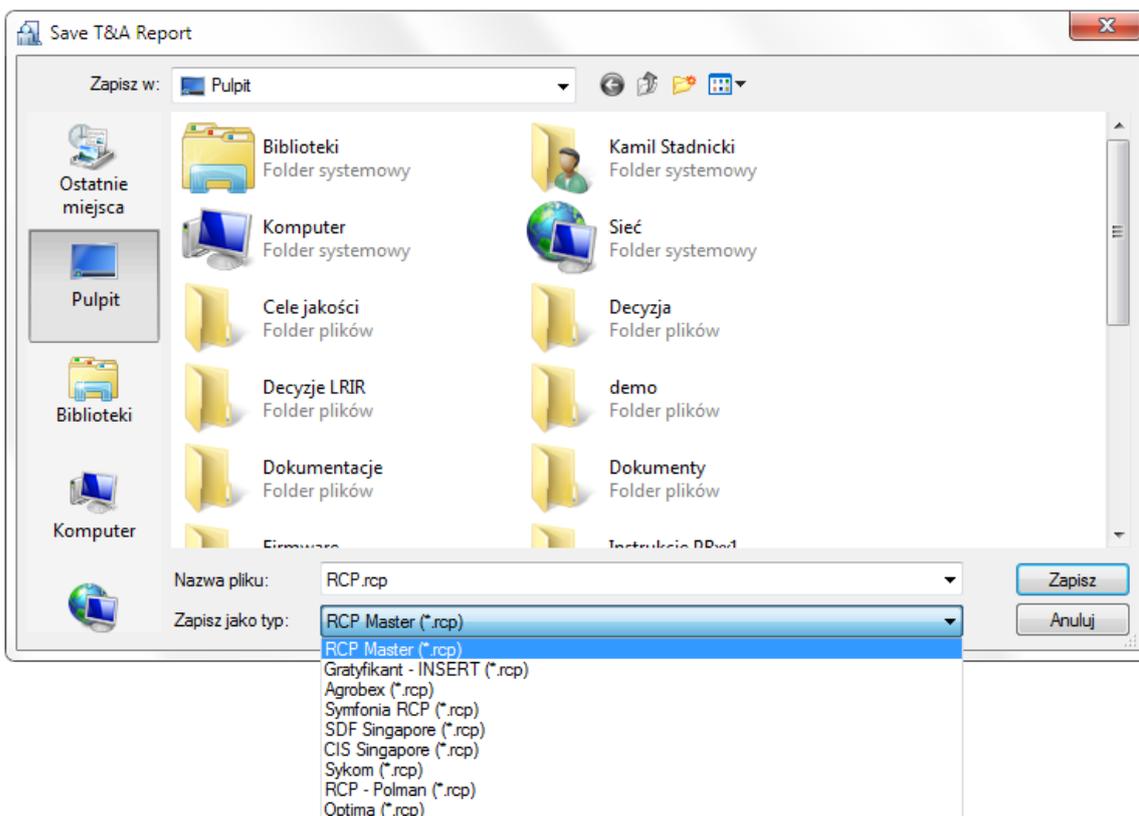


Figure 3.103. Saving T&A report in selected format

Thanks to the possibility for saving T&A report in other applications' format, the PR Master can exchange data with external T&A systems.

Special reports

The **Special Reports** menu has been created in order to define reports made on special users request. For instance the **Report 1** allows for displaying users who logged on the selected reader. Because special reports are very specific, and used for individual purposes, discussing them in detail is outside the scope of this document.

Reversing events order

By default, events in the **Event History** window are displayed from the oldest to the youngest. In order to reverse this order, you should select the **Reverse order** check box.

Deleting events from database

From the **Event History** window you can also delete old events from database. The **Delete events** button serves exactly this purpose. If you click on it, the **Delete events** dialog box displays (Figure 3.104).

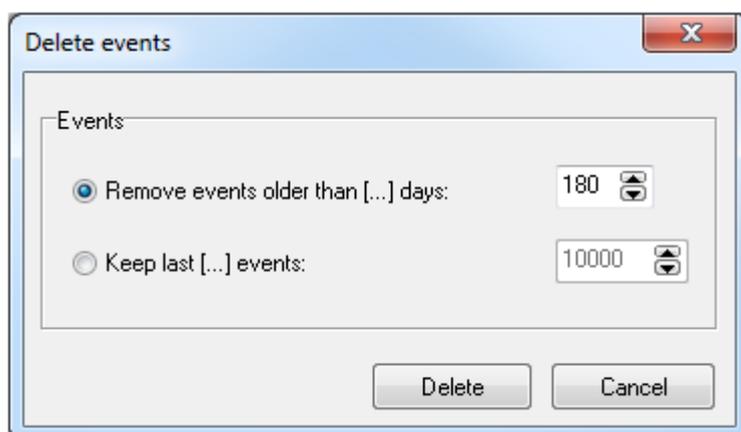


Figure 3.104. *Deleting events from database*

Using this dialog box you can delete from database events older than specific number of days (the **Remove events older than [...] days** option). You can also specify the number of events which should remain in the database after delete operation is completed (**Keep last [...] events** option).

After relevant options are selected, you should click on the **Delete** button, which will trigger actual operation of deleting events from database.

Closing event history

In order to close **Event history** window and move to the main PR Master's window, you should click on **Exit** button.

Play CCTV record

If the integration of RACS 4 with CCTV is configured in accordance with dedicated instruction, which is available at www.roger.pl, then it is possible to play video clips associated with selected events by means of **Play CCTV record** button. The button brings dialog box shown in fig. 3.105 and it is also available in Online monitoring mode (see [section 4.5.1](#)). In the dialog box, the operator can play video clip, adjust its time and obtain information on clip status. In case of GV600/4 video capture card, the operator can also save picture from video frame by right clicking the video clip and selecting adequate options.

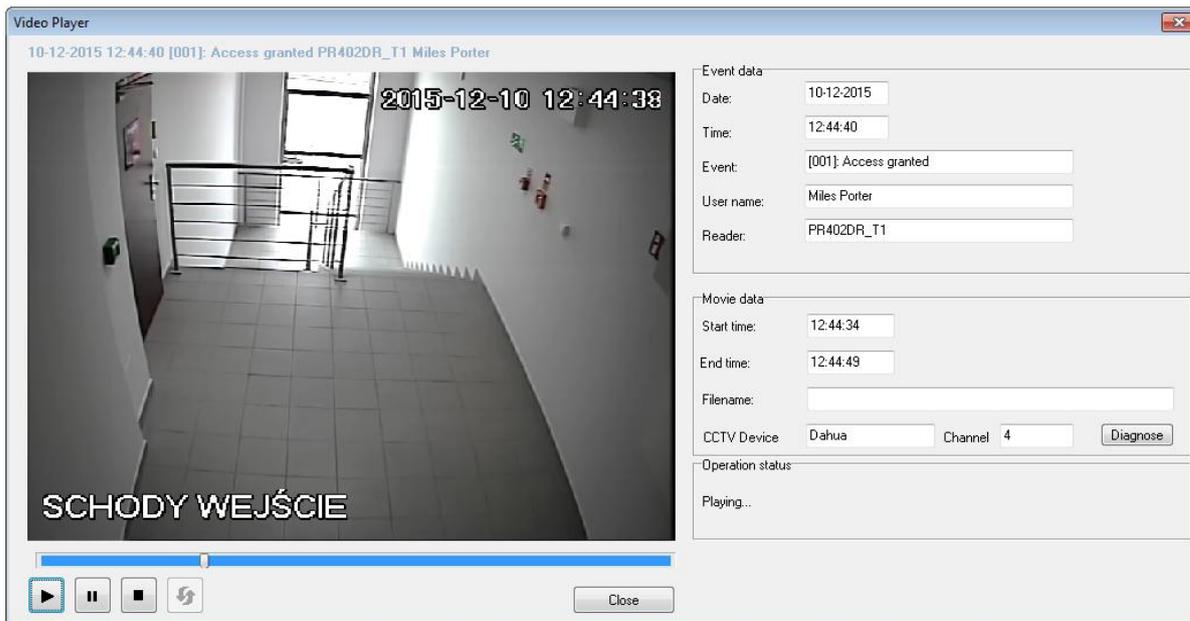


Figure 3.105. Video Player

3.3.8. Attendance

The **Attendance** command causes displaying report containing information on users' attendance in attendance areas defined. Using this command you can find out, for instance, how long persons from particular group were present in particular area. You can also prepare the First-In-Last-Out report showing who entered area as first and who left area as last in the date range selected. Prior to using Attendance Reports it is necessary to define Attendance Zones (see [section 3.2.9](#)). Selecting the **Report/Attendance** command causes displaying the **Users' attendance in defined Attendance Areas** dialog box opens (Figure 3.106).

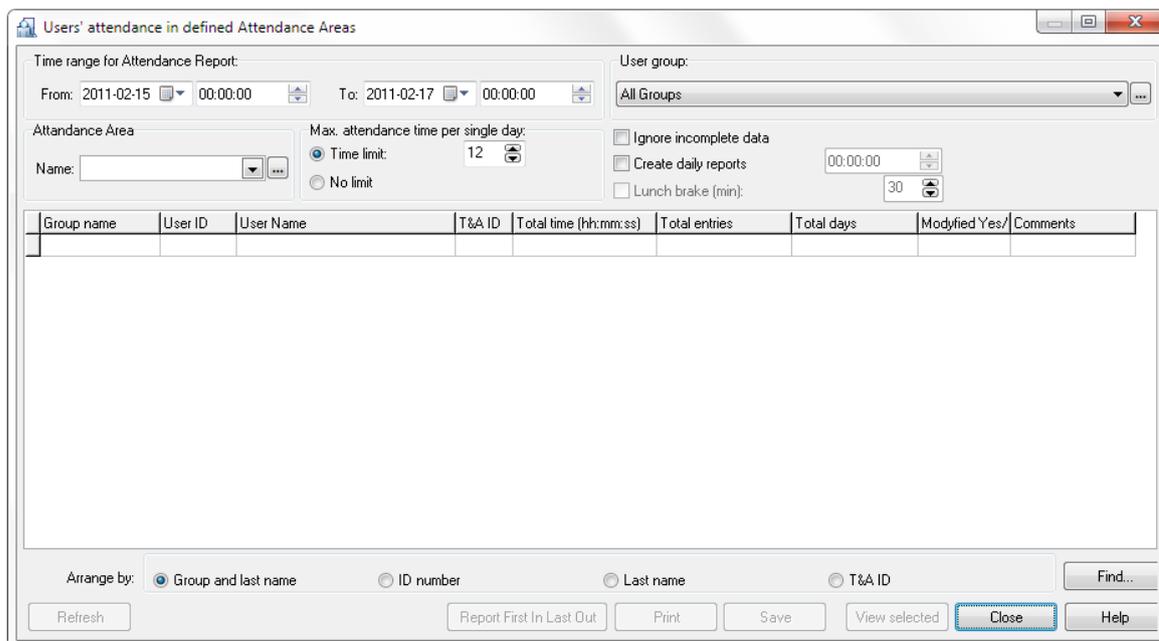


Figure 3.106. Generating report on attendance for previously defined Attendance Areas

The dialog box shown above allows the user to:

- ◆ determine report’s time range,
- ◆ specify users group, the report should apply to,
- ◆ specify an attendance area, the report should apply to,
- ◆ specify a maximum time within a day, a user is allowed to be present in the area,
- ◆ search for an employee by his name,
- ◆ sort records according to the defined criteria,
- ◆ save report to a file,
- ◆ print report to the printer.
- ◆ initiate generating the FILO report.

When you open the window, the attendance record list is empty. In order to generate the list, you should define report parameters: time frame, attendance area, maximum attendance time in the area, and optionally a group, the report should apply to. Then you should click on the **Refresh** button. This will cause displaying of attendance records in the window (Figure 3.107).



Internally, users in the Attendance Report are distinguished based on their IDs and not first and/or last names. Therefore instead of modifying or exchanging user IDs during reporting period it is recommended to do it at the end of period (e.g. at the end of month). Otherwise Attendance Report might become inconsistent.

Group name	User ID	User Name	T&A ID	Total time (hh:mm:ss)	Total entries	Total days	Modified Yes/	Comments
Workers	1	Casillas Ahirman		00:51:20	1	1		
Workers	107	Childers Adrienne		00:55:10	1	1		
Workers	106	Devilbiss Irune		00:55:30	1	1		
Workers	100	Levine Mauro		01:40:40	7	1		
Workers	104	Madrid Derrick		00:50:20	1	1		
Workers	101	Paige Aaron		00:29:50	1	1		
Workers	103	Porter Miles		01:39:50	1	1		
Workers	105	Rubin Stephen		00:47:40	1	1		
Workers	102	Stein Leslie		01:18:30	1	1		

Figure 3.107. User’s attendance in Attendance Area “Office” for users from “Workers” group

If you select the **Lunch break** checkbox after selecting **Create Daily Reports** checkbox and set the length of the break, the system will automatically adjust users’ attendance times (the lunch break time will be subtracted from total time).

Double clicking on any person in the list will cause displaying **Attendance report** dialog box (Figure 3.108).

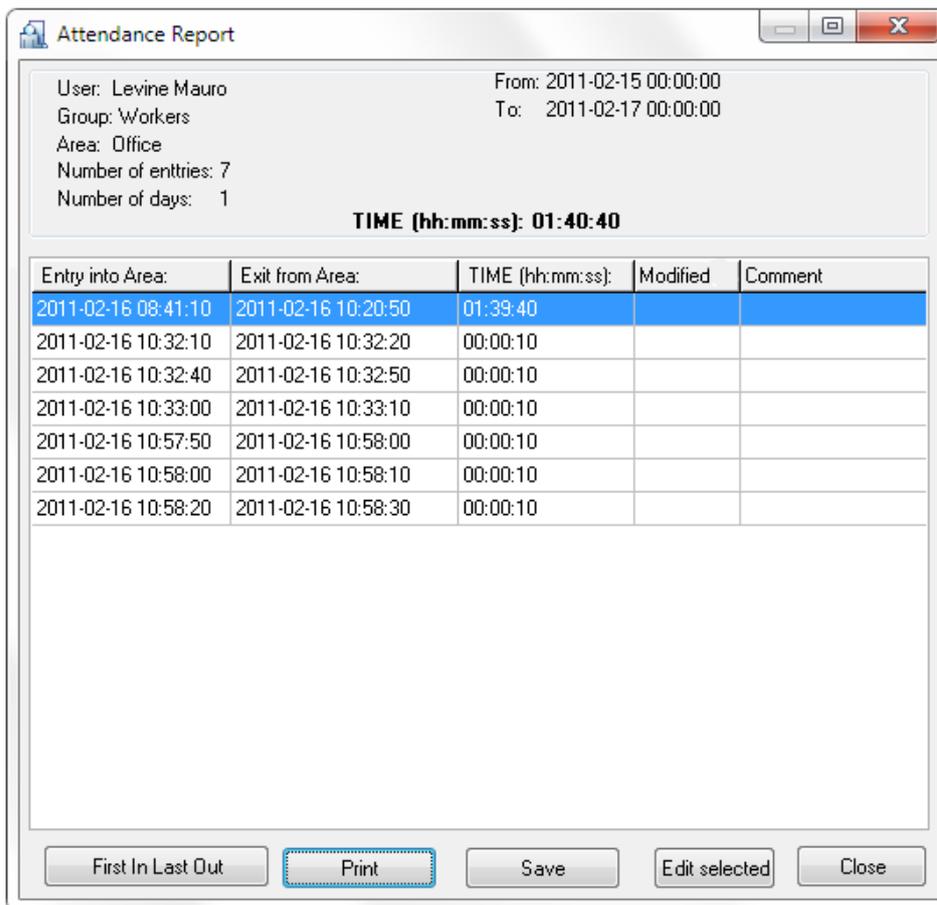


Figure 3.108. Attendance report for a selected user in the selected attendance area

In case there are wrong data in the event history related to the particular user, you can modify them. In order to do this, you should double click an item in the list. Then **Edit** dialog box shall display (Figure 3.109), where you can correct or modify time and add comments.

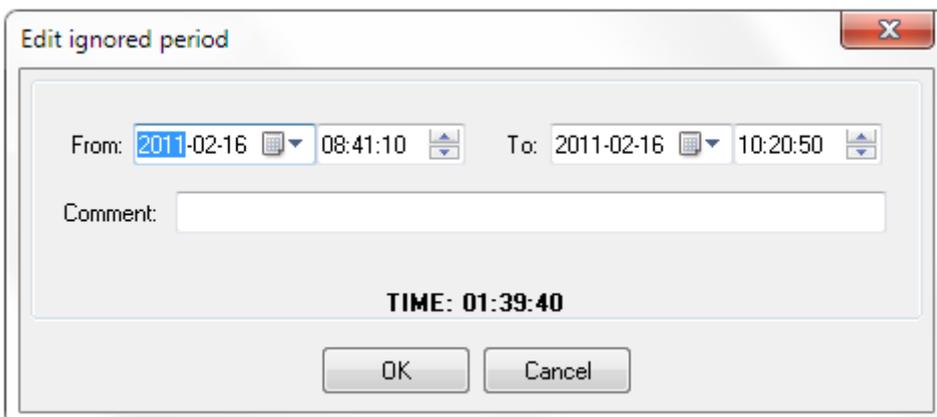


Figure 3.109. Correcting erratic entries in attendance report

If you modify an entry, and click on the **OK** button, a modified entry will be marked in the event list by the "V" mark.

In order to print events related to particular user, you should click on the **Print** button. The **Save** button allows to save report in **.rtf** or **.csv** formats.

If during the day user entered and left attendance area for several times, the program by default will show all the attendance periods and sum up the total time. However sometimes the more important information is first entry and last exit the user from the system. For this purpose you can use the **Report:First In Last Out** button visible in Figure 3.107. Clicking on it will cause displaying a summary with all the first entries and last exits in particular Attendance Area for selected time frame (Figure 3.110).

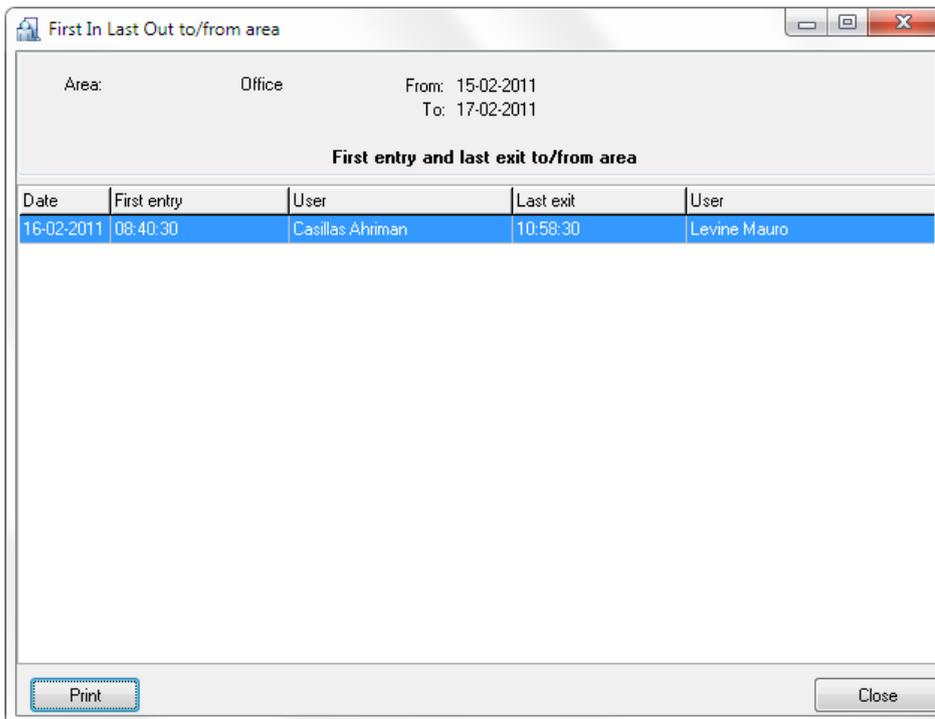


Figure 3.110. Report First In Last Out for selected Attendance Area in given time range

This report can be hard-copied on the printer or saved in **.rtf** or **.csv** formats.



Exactly the same report you can get when you select the **Create daily report** option before refreshing record list in attendance report window. However, for your convenience, the button **First In Last Out** has been added. This button generates summary of first entries and last exits independently on the fact if the user selected the **Create daily report** option or not.



There is a **Report: First In Last Out** button present in the main **Users' attendance in defined Attendance Areas** (Figure 3.107). This button generates report containing names of users who came as first to the Attendance Area and left it as last in the dates range selected. This report has been described more accurately in **section 3.3.8.1** below.

3.3.8.1. Report: First In Last Out

From time to time you need to know who entered particular area as first and who left it as last. It can be useful, for example, if you need to find out who opened a room at the beginning of the work, and who closed it when duty hours finished.

For this purpose you can use the **Report: First In Last Out** button located in the main **Users' attendance in defined Attendance Areas** (Figure 3.107). If you click on this button, the summary will be generated containing names of users who entered the area as first and who left the area as last in the dates range selected (Figure 3.111). This report can also be hard-copied on the printer or saved in **.rtf** or **.csv** formats.

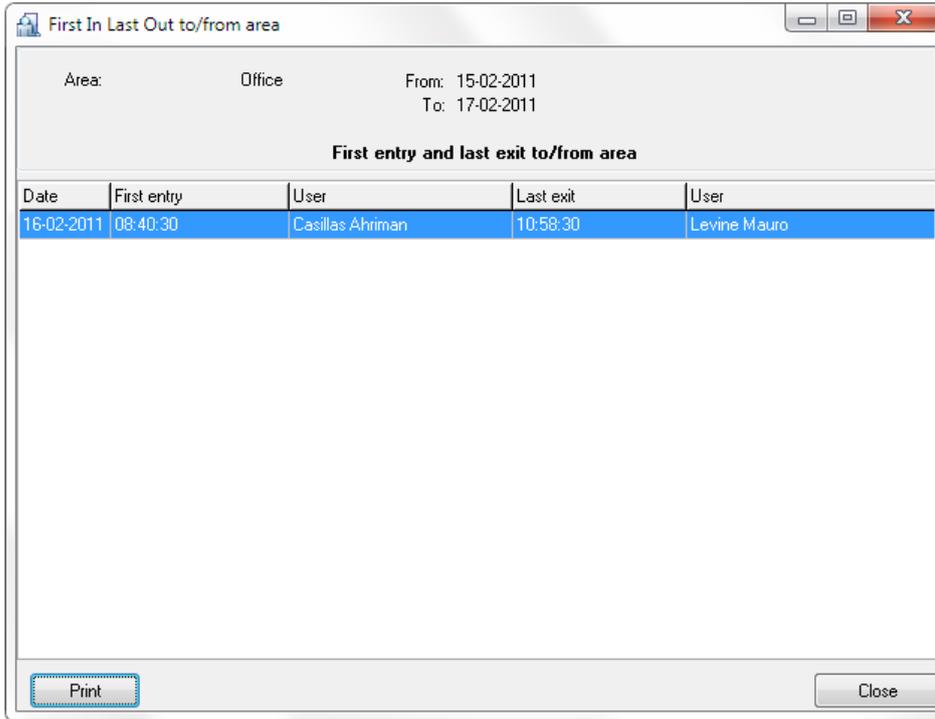


Figure 3.111. Report First In Last Out for selected time range

3.3.9. User modifications

The User modifications command enables to create report including operator modifications of user list in the system. The report registers such actions as user adding, deleting and modifying as well as user list importing and deleting.

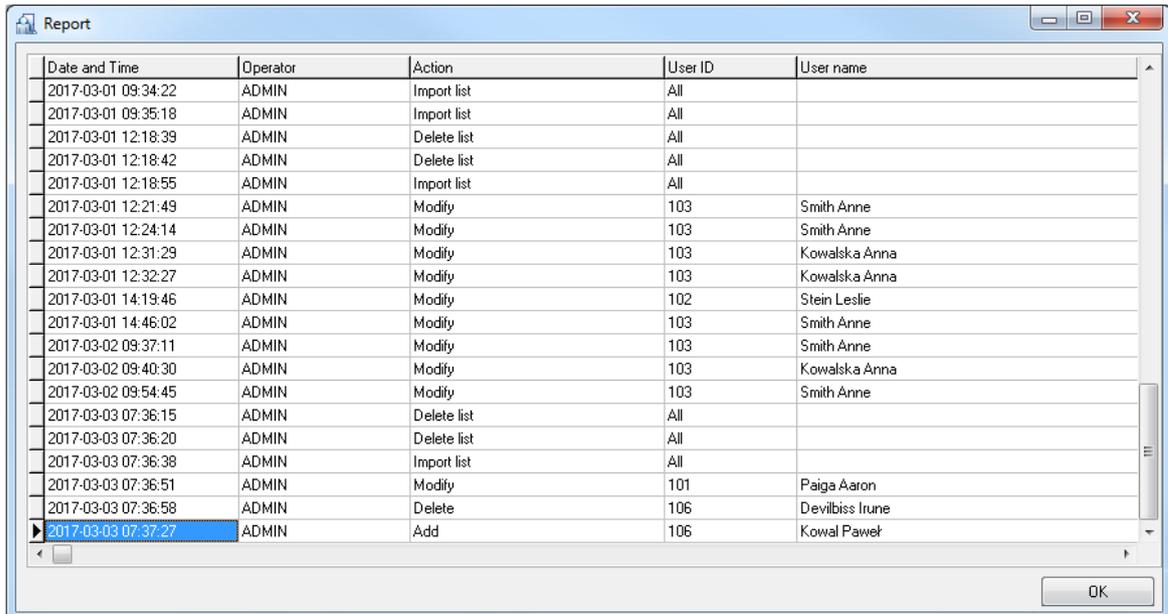


Figure 3.112. Example of 'User modifications' report

3.4. COMMANDS MENU

The **Commands** menu has been shown in Figure 3.112.

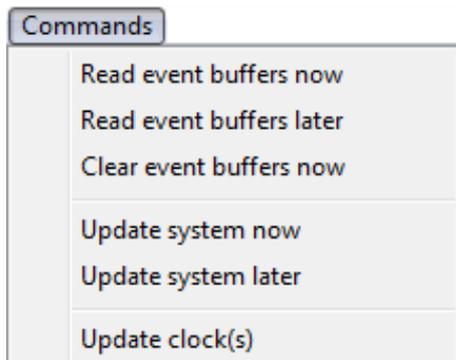


Figure 3.112. *Commands menu*

3.4.1. Read event buffers now

Events in the RACS 4 are recorded all the time — in PRxx2 series controllers or in CPR network management unit. When you select **Read event buffers now** command, then buffers' content will be moved to PR Master database. If the PR Master works in an online monitoring mode, events are written into database immediately after they happen. When you select the command, the system will ask if all events logged in the system should be read. If you answer **Yes**, the process of downloading events will be initiated (Figure 3.113).

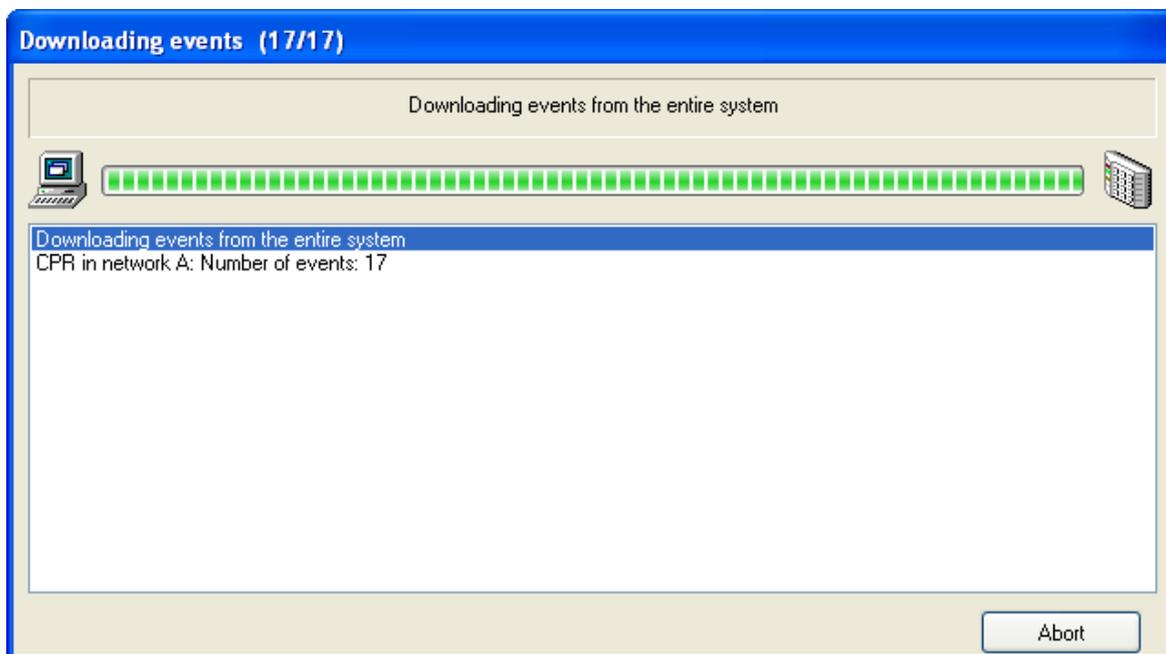


Figure 3.113. *Downloading events from the ACS to database*

If the process of downloading events is completed, the system displays a message with information of operation's success or failure.

3.4.2. Read event buffers later

In large Access Control System installation, the process of downloading events can be time-consuming. Therefore the operator can schedule this operation at particular time and selected days in a week. Such a schedule can be generated by the **Read events buffers later** command.

If you click on it, the **Read events buffer later** dialog box displays (Figure 3.114).



Figure 3.114. Scheduling automatic downloading events from the ACS

In the dialog box shown above you should specify time and select weekdays, when the system should automatically download events to database.

In order to enable this functionality, you should select the **Active** check box. Otherwise the schedule will not be executed.

3.4.3. Clear event buffers now

The **Clear event buffers now** command lets delete upon request some events present in devices' buffers in all the Access Control System's networks. If you select this command, the system first will ask you for confirmation. If you answer **Yes**, the content of all the event buffers will be deleted. Then the system displays a message informing you, that the operation was successful.

3.4.4. Update system now

The **Update system now** command is used for sending all the settings to all controllers and all CPR units in all the networks of the ACS. In case the ACS is large, this operation can take a long time. Because of this it should be initiated as rarely as possible i.e. after all the necessary changes are entered.

The system configuration operation is initiated by selecting the **Update system now** command. If there are any events collected at this time in the system's devices, the system will download them to database. Then it will display information window containing data on reading operation progress.

After the system displays message that all the events have been read, it goes into operation of configuring the entire system (Figure 3.115).

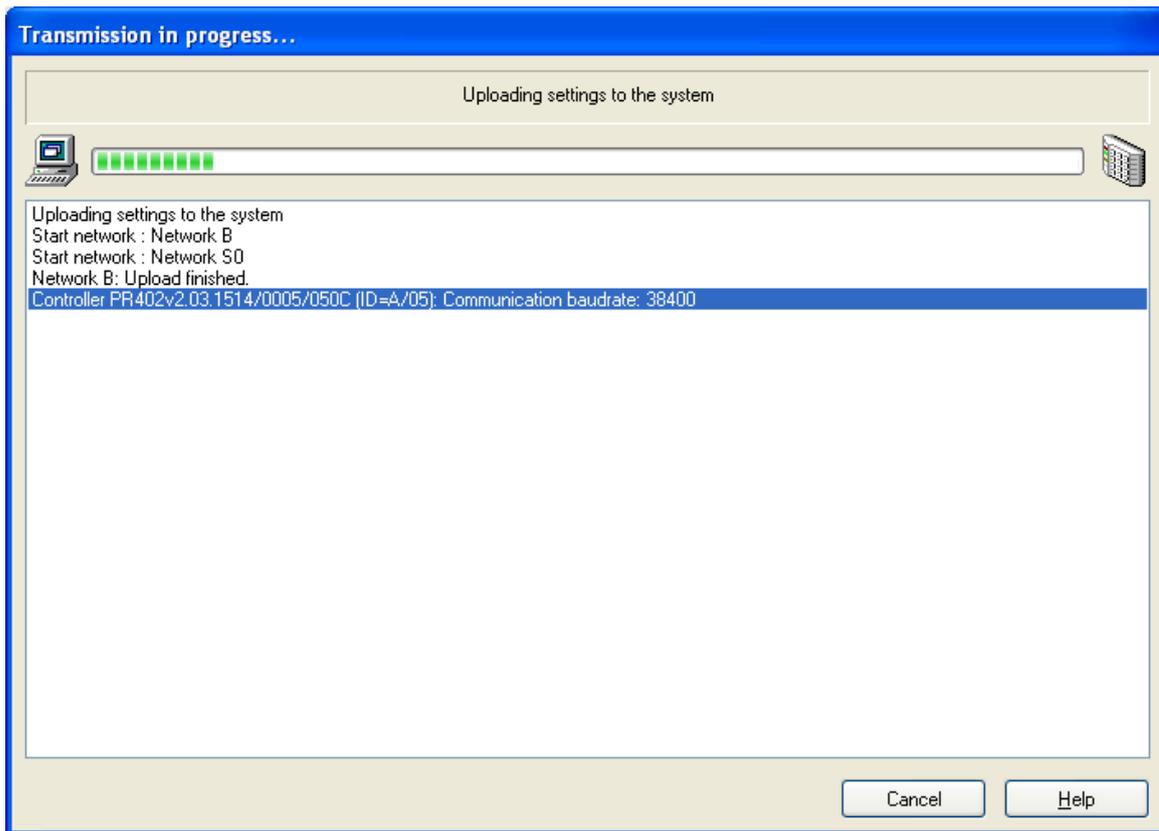


Figure 3.115. Configuring entire system — the operation progress window

3.4.5. Update system later

Because an operation of configuring the whole system can be time-consuming it is possible to schedule it for later. You can plan the update to be performed at particular times and selected days of week. The **Update system later** serves this purpose.

If you select this command, the **Update system settings later** dialog box displays (Figure 3.116).

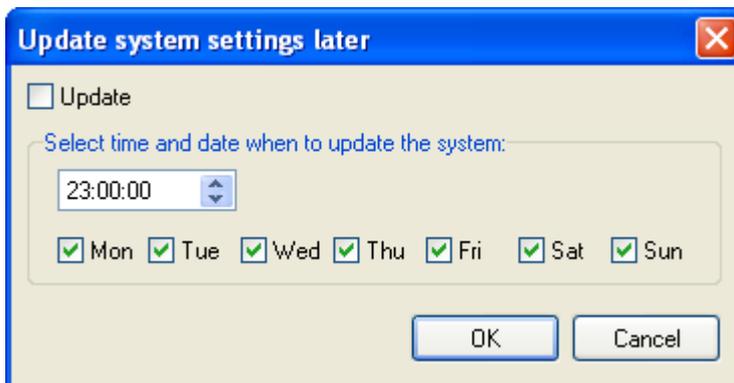


Figure 3.116. Scheduling automatic update for the entire system

In the dialog box shown above you should select weekdays, when an automatic system configuration should be performed and specify time for performing this operation.

In order to make this functionality active, you should select the **Update** check box. Otherwise the system updating schedule will not be executed.

3.4.6. Set system clocks

The **Update clock(s)** command allows for manual setting of clocks for all RACS 4 devices in accordance to system clock of the computer with PR Master software.

3.5. TOOLS MENU

The **Tools** menu is shown in Figure 3.117.

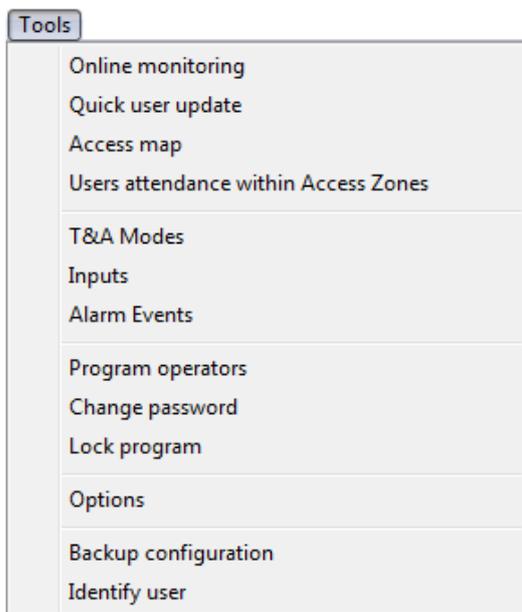


Figure 3.117. Tools Menu

3.5.1. Online monitoring

The **Online monitoring** command activates special mode of PR Master operation which enables online monitoring of events in the RACS 4. When PR Master operates in this mode, events are immediately appended to the system’s database and they are available for reporting. Every time you select the **Online monitoring** command, the PR Master reads events from all the buffers in the system. Then the system goes into an online monitoring mode (Figure 3.118).

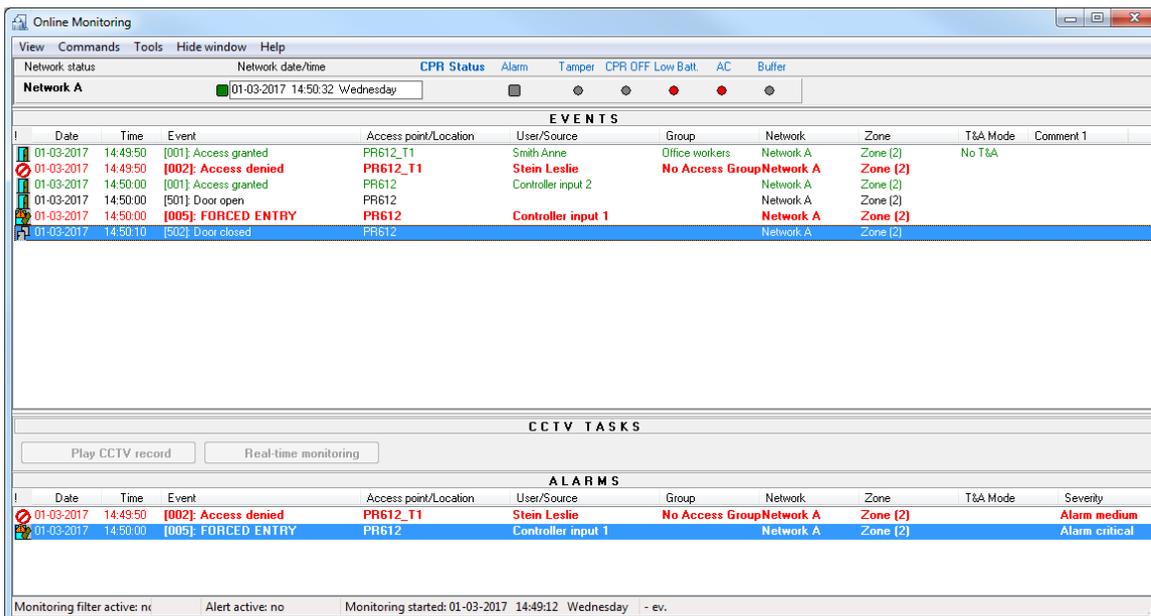


Figure 3.118. Online monitoring in PR Master

In this mode of operation, the PR Master uses other menu. It will be described in detail in **Chapter 4 - Online monitoring**.

3.5.2. Quick user update

Every change of user properties — i.e. change assignment to a group, replace of proximity card change the PIN code, requires sending data to controllers. In view of the fact, that the operation of sending the whole configuration to all the controllers in the system is time-consuming, and changes made in configuration are made much less often than user management tasks, you can use a **Quick user update** command. This operation allows for sending to controllers only these user settings, which have been modified.

Selecting this command causes displaying a simplified version of users directory (Figure 3.119).

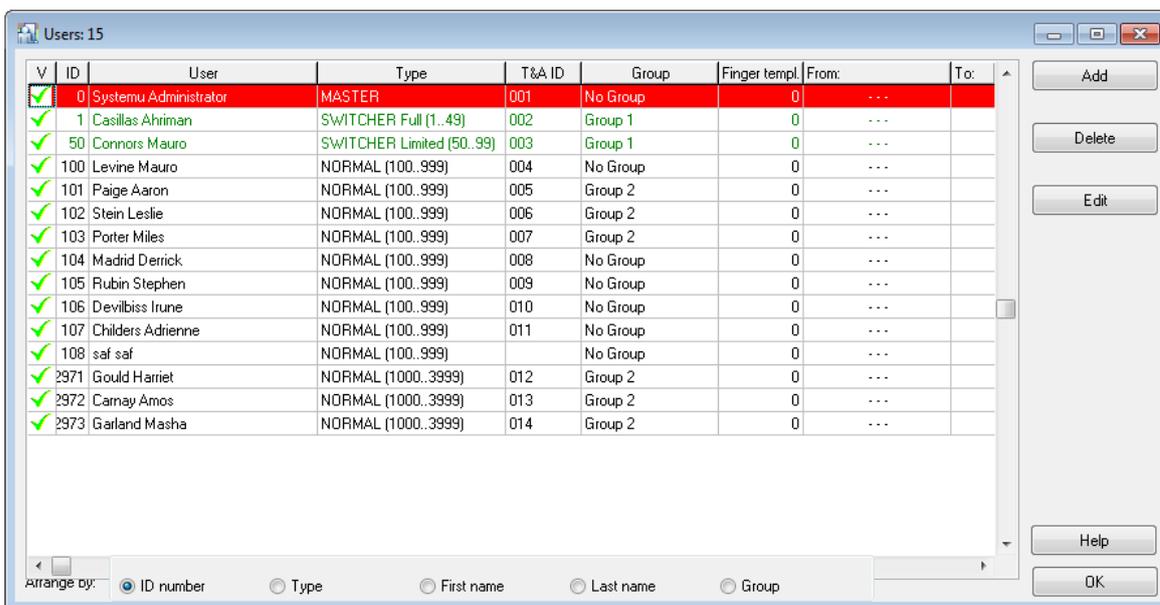


Figure 3.119. Quick user update

This window allows for adding, removing, and modifying users properties. If you add a new user or modify existing one and press OK button, then the PR Master software shall automatically upload new data to controllers (Figure 3.120).

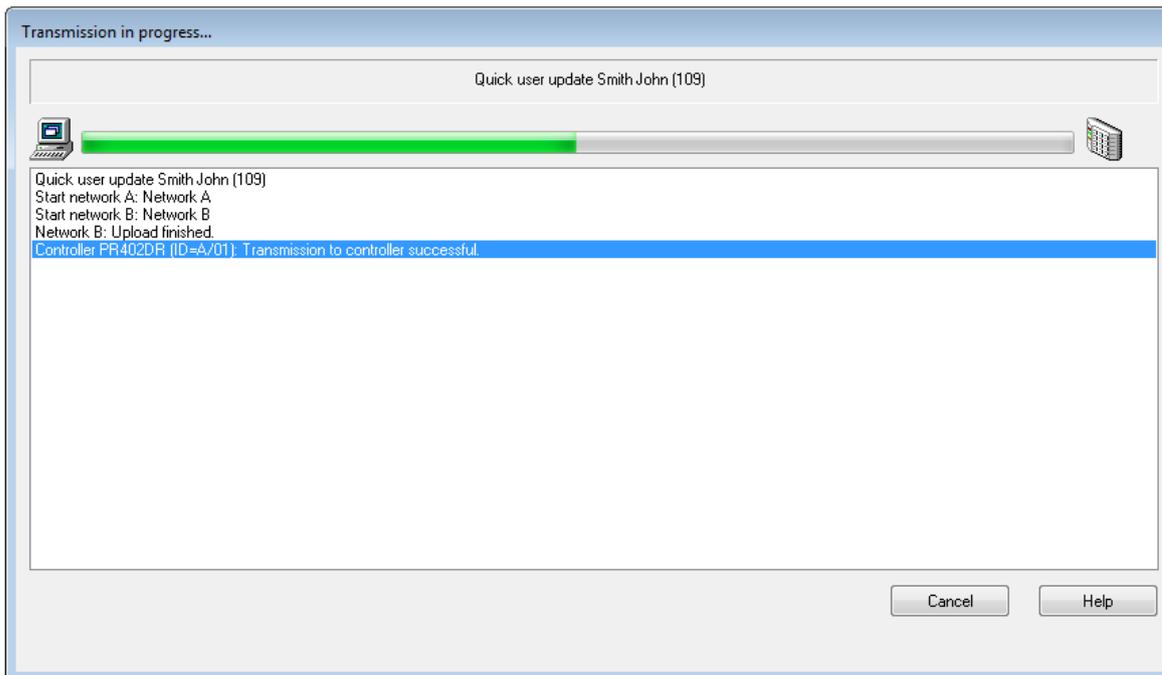


Figure 3.120. Online user update

Clearly this operation is performed much quicker than the update of entire system.

The quick user update operation applies to individual users. This means, that you cannot change settings for several users, and then upload them at once.

3.5.3. Access map

The **Access map** command displays a current access right state for the zones defined in the system. If you select this command, the system displays the **Access rights at: xx:xx** dialog box (Figure 3.121).

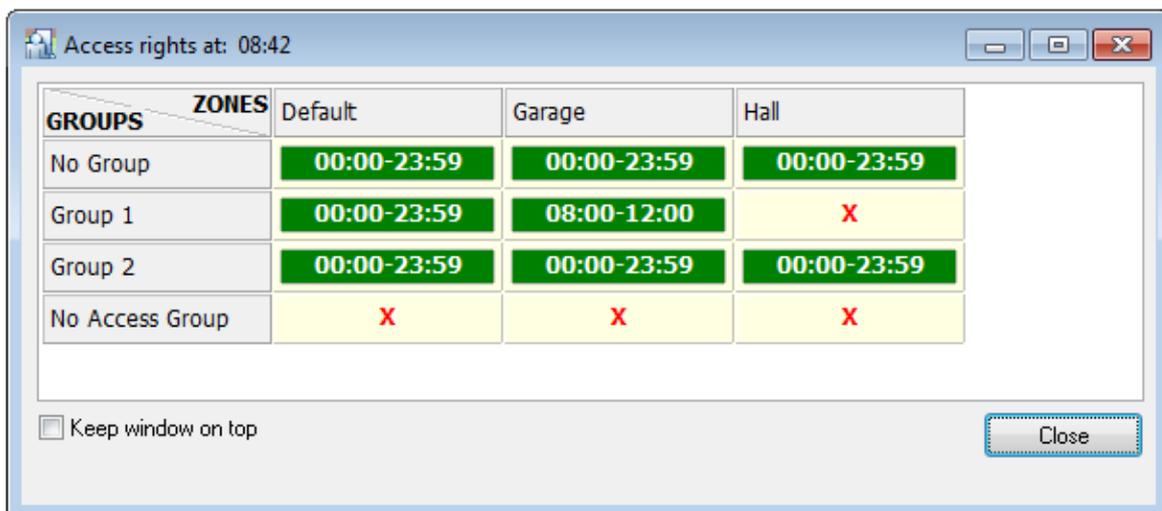


Figure 3.121. System's access rights map

If at given moment a particular group has access rights to a particular zone, then in the intersection of the group's row and the zone's column the time interval describing how long this right applies is

displayed. On the other hand, if the group does not have access right at this moment, the system displays red **x** mark.

3.5.4. Users' attendance in Access Zones

The **Users' attendance in Access Zones** displays a list of access zones together with a number of users logged in (Figure 3.122).

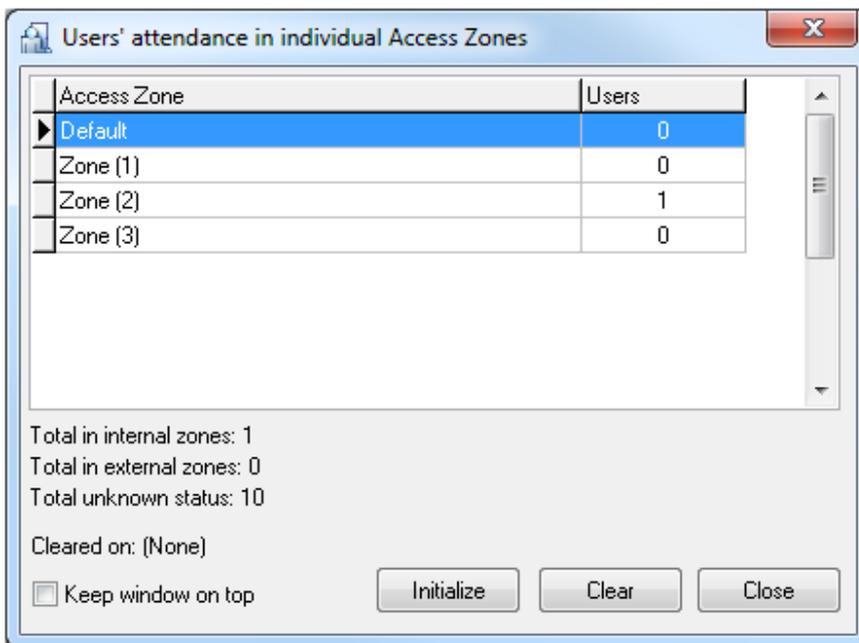


Figure 3.122. Number of users logged in access zones

The **Initialize** button causes initiating a table based on a current RACS 4 event history. The **Clear** button empties the table. From the moment, the table is emptied, the system starts counting number of users in particular access zones from scratch. But when you use the **Initialize** button again, the system removes an information about database is cleared.

3.5.5. T&A modes

The **T&A modes** command opens the T&A Modes directory (Figure 3.123).

Code	T&A Mode	LCD message	Parameter 1	Parameter 2
016	Exit	Exit	OUT	PRIV
017	On-duty exit (DDE)	On-duty exit	OUT	DUTY
018	Breakfast break	Breakfast	IN	PRIV
019	Lunch break	Lunch	IN	PRIV
020	Overtime 1	Overtime 1	IN	PRIV
021	Overtime 2	Overtime 2	IN	PRIV
022	Overtime 3	Overtime 3	IN	PRIV
023	Overtime 4	Overtime 4	IN	PRIV
024	Overtime 5	Overtime 5	IN	PRIV
025	Exit on request	Exit on request	IN	PRIV
026	On duty	On duty	IN	PRIV
032	No T&A	No T&A	BY	DUTY
033	Starting work at pos. 1	Position 1	IN	PRIV

Figure 3.123. T&A modes directory

Using this directory you can add custom T&A registration modes.

Adding a new T&A mode

In order to add a new T&A mode, you should click on the **Add** button. The **T&A mode** dialog box appears (Figure 3.124).

T&A Mode

Code: 001 LCD message: New T&A Mode

Name: New T&A Mode

Parameter 1 (Direction: entry, exit, internal or custom)

- Entrance
- Exit
- Internal door
- Custom

Mark: IN

Parameter 2 (private, on-duty or custom)

- Private
- On-duty
- Custom

Mark: PRIV

OK Cancel

Figure 3.124. Adding a new T&A mode

In this dialog box you should enter a mode’s code and its name. You can also add a LCD message for controllers equipped with LCD display. Then you should define two parameters which decide on how the T&A mode will be interpreted.

The **Parameter 1** describes if the particular T&A mode is entry, exit, internal door or custom type.

The **Parameter 2** describes if the particular T&A event is private, duty, or custom type.

After you define all the T&A mode properties, you should click **OK**. A new mode will appear in the T&A modes directory window (Figure 3.125).

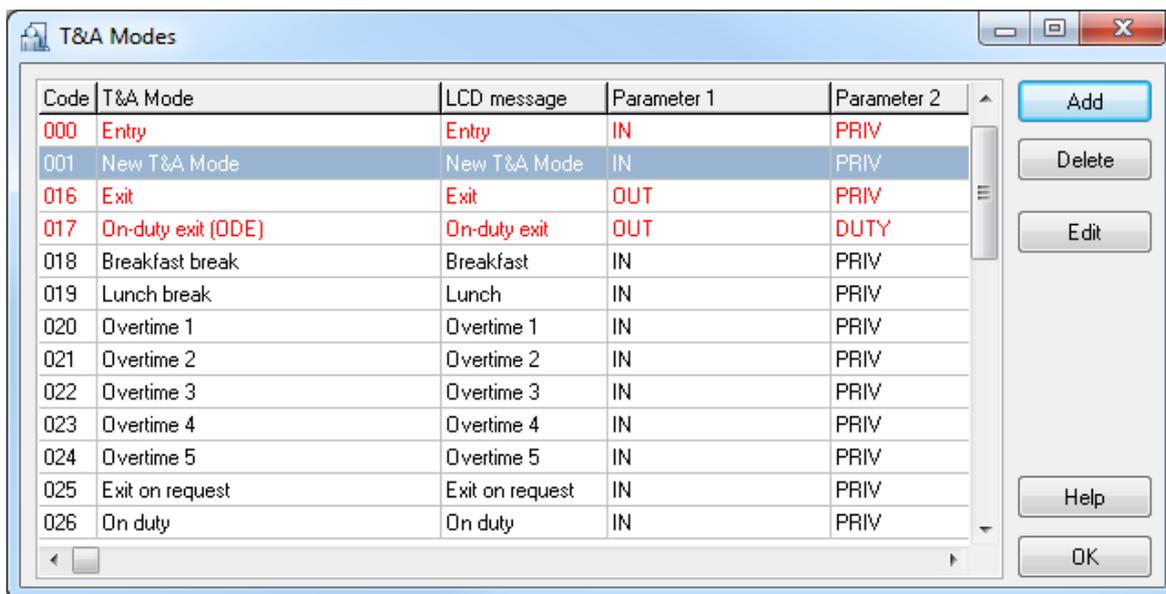


Figure 3.125. T&A mode with code 001 is added by operator

Deleting a T&A mode

Administrator defined modes can be deleted. The **Delete** button in the T&A modes directory window serves this purpose. If you click on it, the following warning will display (Figure 3.126).

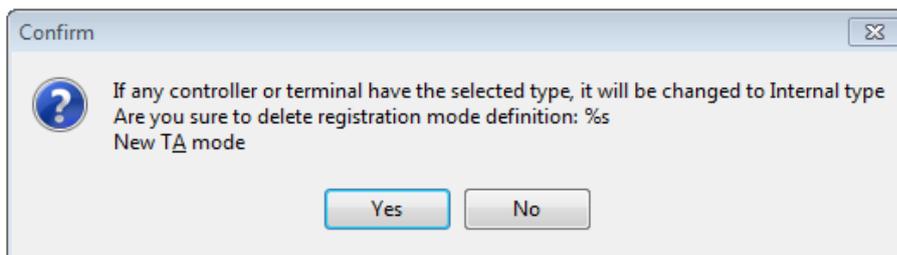


Figure 3.126. Deleting administrator defined T&A mode

If you answer “yes” to this question, the administrator defined T&A mode will be deleted from system. The terminals or controllers which previously registered this T&A mode, from this time on will register the **Internal passage** mode.

3.5.6. Inputs

The **Inputs** command opens a directory of input lines types available in RACS 4 (Figure 3.127).

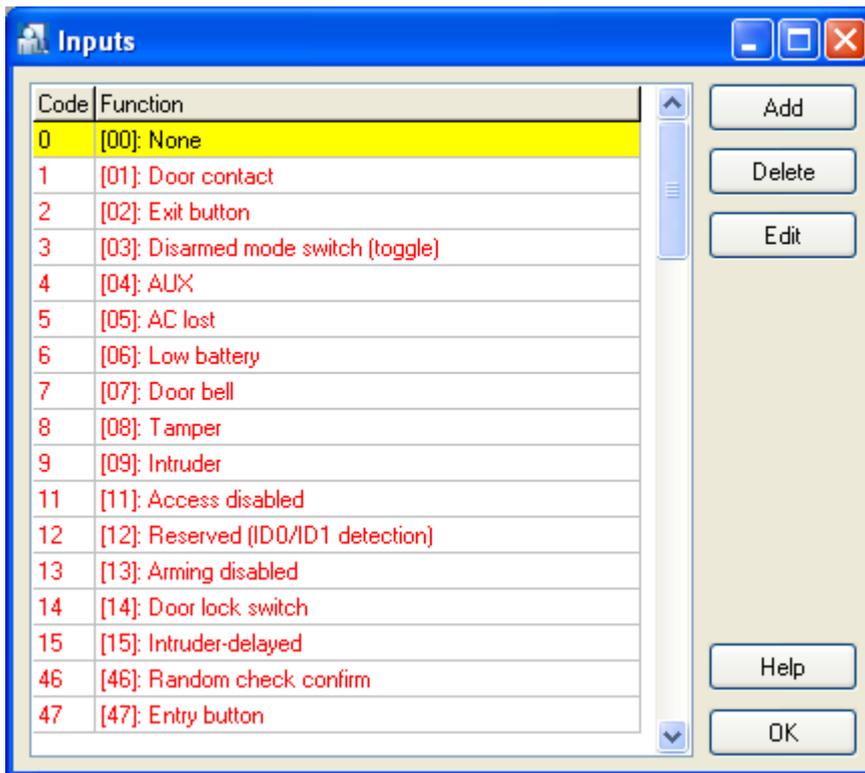


Figure 3.127. Input lines directory in the RACS 4

Using this directory, you can add custom input lines types. However you should note, that input lines types with codes from 00–100 range are predefined. They neither can be removed, nor modified. Administrator defined input lines types can be used when the controller should report status of other devices (e.g. gas detector).

Adding a new input line type

In order to add a new input line type, you should click on the **Add** button. The **Input types** dialog box displays (Figure 3.128).

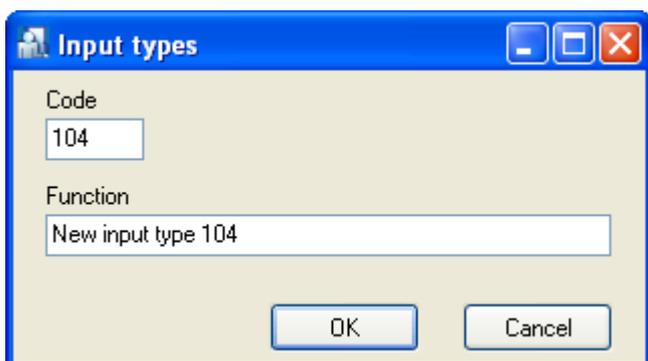


Figure 3.128. Adding a new input line type

In this dialog box you should enter input line type’s code and its name, and then confirm it with **OK** button. A new input line type will appear in the **Inputs** directory (Figure 3.129). You should note, that the administrator defined input line types display in black, whereas predefined modes display in red.

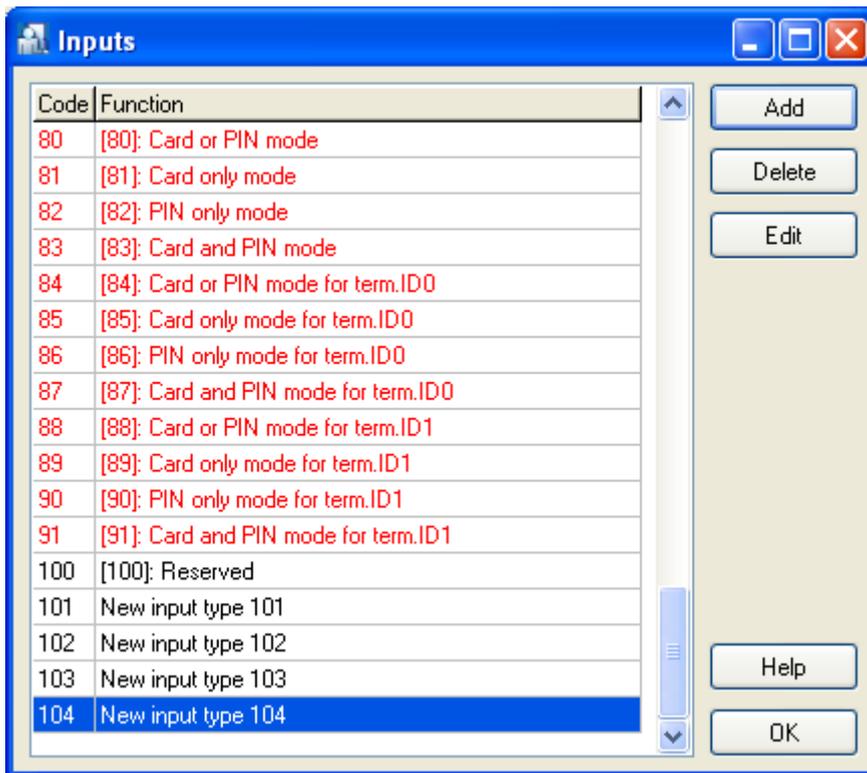


Figure 3.129. Input line type with code 101 has been added by user

Deleting Input Line Type

Administrator defined input line types can be deleted. You can use for this the **Delete** button in the controllers inputs' functions. If you click on it, the following warning will display (Figure 3.130).

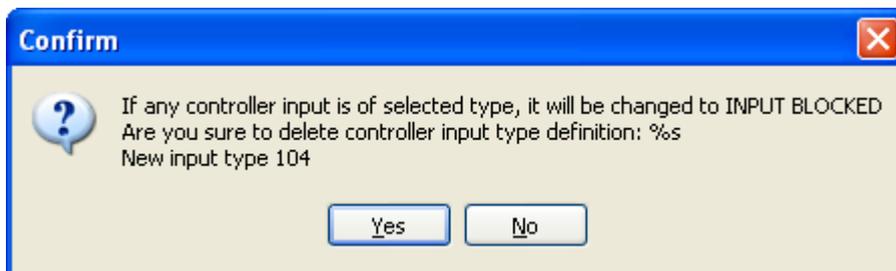


Figure 3.130. Deleting administrator-defined input line type

If you answer "yes" to this question, then the input line type will be deleted from system. Controller's inputs which were previously of this type, from this time will be changed to **INPUT BLOCKED** type.

3.5.7. Alarm Events

The **Alarm Events** command displays a list of events types registered in the RACS 4 (Figure 3.131).

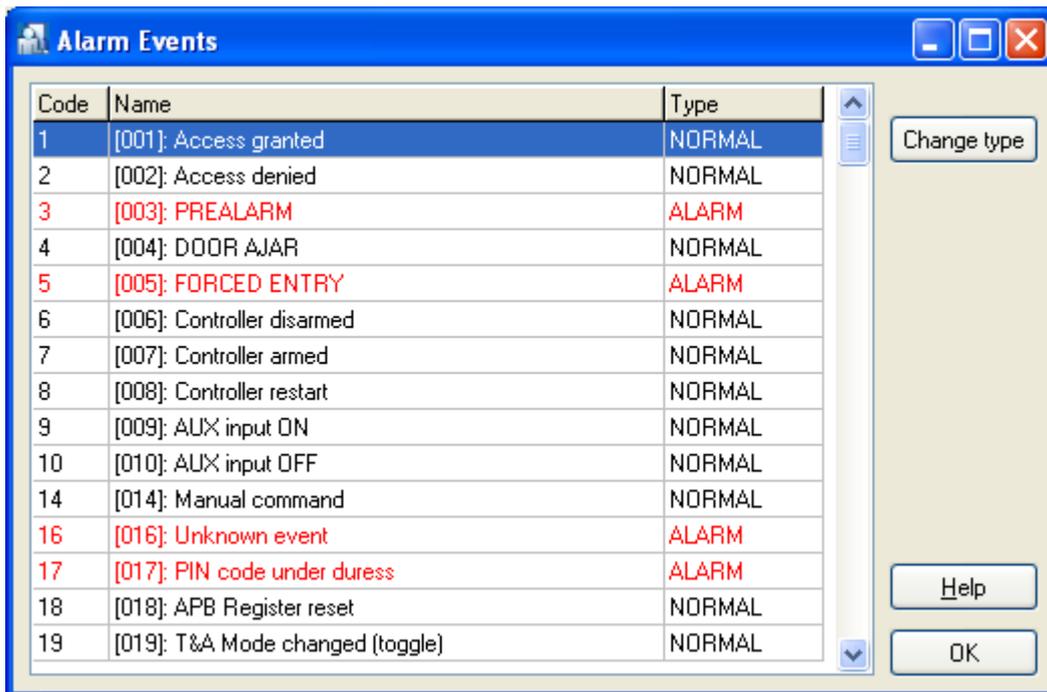


Figure 3.131. Alarm events types in the RACS 4

In this window there is a list of all the events being registered in the system. This tool allows to determine events which should be interpreted as alarm. In order to change an event type from normal to alarm, you should click on the **Change type** button.

When the system is operating in an online monitoring mode, the alarm event is additionally present in the **ALARMS** window. If such an event happens, the **Alarms** bar starts flashing in red.

3.5.8. Program operators

By default there is ADMIN user in the PR Master. He is allowed to run all the commands in the system. In large ACS systems, where many people are responsible for the maintenance of the software, using ADMIN account only may create a security risk. It may happen that one of users accidentally or intentionally modifies settings entered to the system by different person.

The **Operators** command lets create accounts of limited access rights to the selected set of program commands. Selecting this command causes displaying program’s operators directory (Figure 3.132).

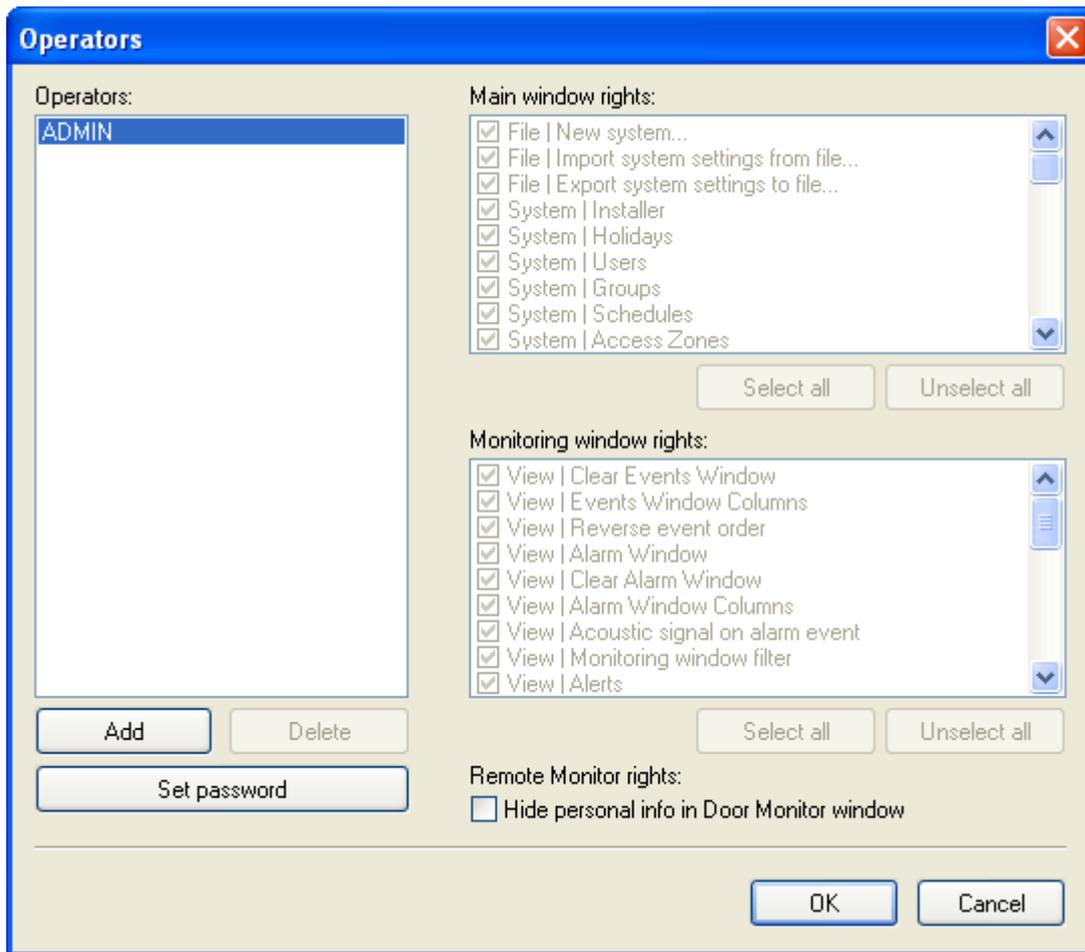


Figure 3.132. List of operators in the RACS 4

By default there is only one entry in this list — the ADMIN user. He has rights to run all the commands in the whole system, and nobody can revoke these rights.

In order to add a new operator to the system, you should click on the **Add** button. The system displays **New operator** dialog box, where you should enter login for the new operator and define password for him. After completing this operation new operator will appear on the list. At first he has no rights in the system — all the checkboxes in the **Main window rights**, **Monitoring window rights** and **Remote monitor rights** are unchecked. In order to grant right for the specific operator to the specific command, you should select checkbox next to the particular option. Let's assume that we want a new user to have rights only for adding new users. In this case, we should select **Tools | Quick user update** checkbox (Figure 3.133).

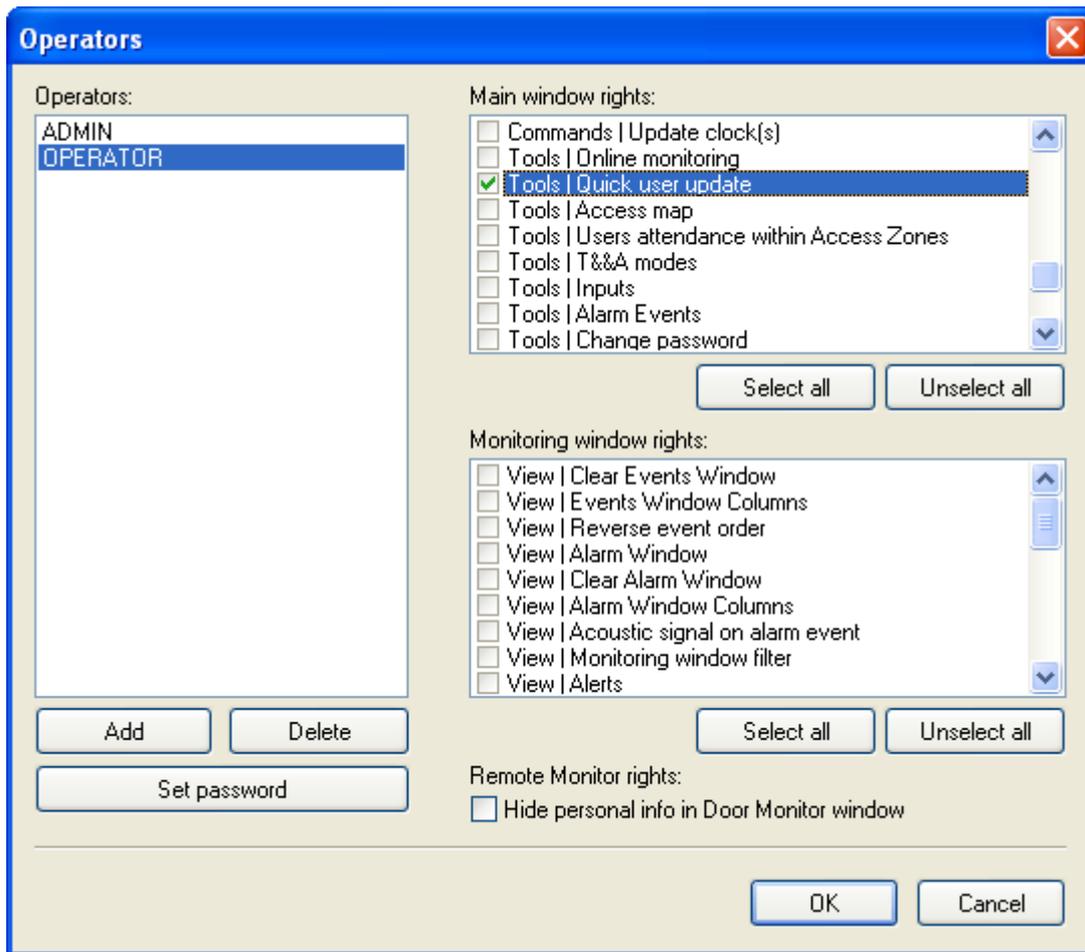


Figure 3.133. OPERATOR has rights to quick user update only

The **Select all** button present below particular option group cause selecting all the options in a group. Clicking on the **Unselect all** button cancels selection for all the options in the group.

The **Remove** button under operator list deletes system operator. Of course the user ADMIN cannot be deleted.

The **Set password** button allows for changing password for the selected operator (it is also possible for the ADMIN operator).

3.5.9. Change Password

The **Change password** command allows for changing password for the operator who is currently logged in. If you select this command, the **Change password** dialog box appears (Figure 3.134).

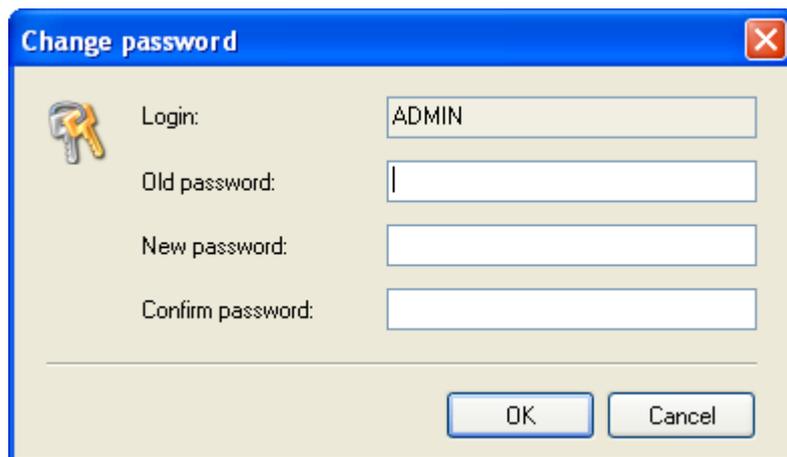


Figure 3.134. ADMIN password

In the **Old password** field you should enter a current account's password. In **New password** and **Confirm password** fields you should enter a new password, and then confirm them by the **OK** button.

3.5.10. Lock program

The **Lock program** command enables to lock temporary the access to PR Master software. It may be helpful when the operator must go away from the computer for some time. If you use this command, the program's window will be minimized. In order to unlock the program, you should enter a password for the user who is currently logged in.

3.5.11. Options

The **Options** command opens the program's options window. The window is divided into following tabs:

- ◆ Event reports
- ◆ T&A reports
- ◆ XML reports and email
- ◆ Misc. (1) and Misc. (2)
- ◆ Cards
- ◆ CPR32-NET
- ◆ Fingerprint readers
- ◆ AD integration

Options for each of these tabs are explained in following sections.

3.5.11.1. Event reports

The **Event reports** tab can be used for setting options for generating **PREvents.csv** file. It is shown in Figure 3.135.

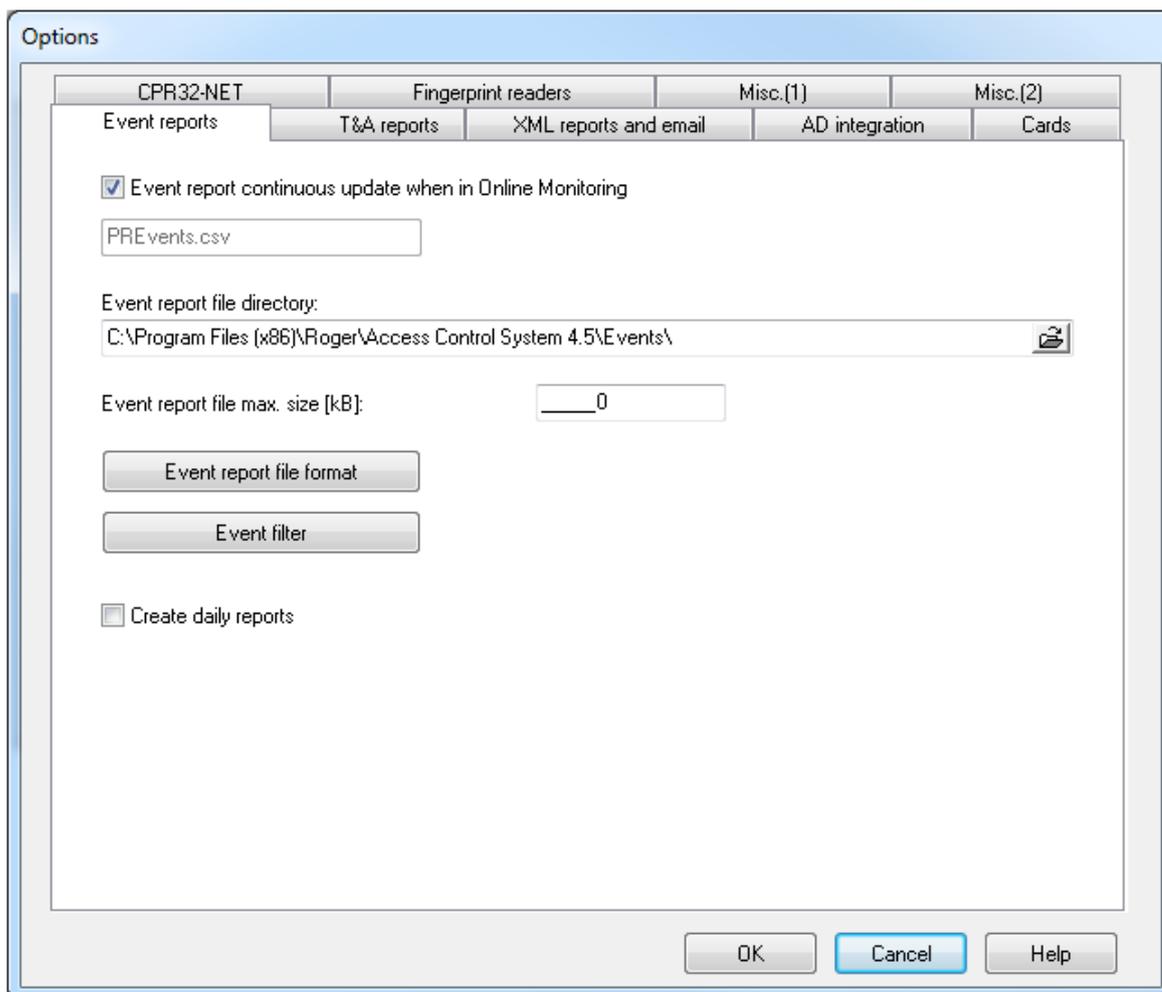


Figure 3.135. Options for generating Events report

All the controls within the tab are active only when the **Event report continuous update when in Online Monitoring** is selected.

The **Event report file directory** allows for specifying a directory, where **PREvents.csv** file will be stored. The **Event report file max. size [kB]** is used for determining a maximum size for the file containing report.

The **Event report file format** allows for defining report file content in details. If you click on it, the **Event report format** dialog box appears (Figure 3.136).

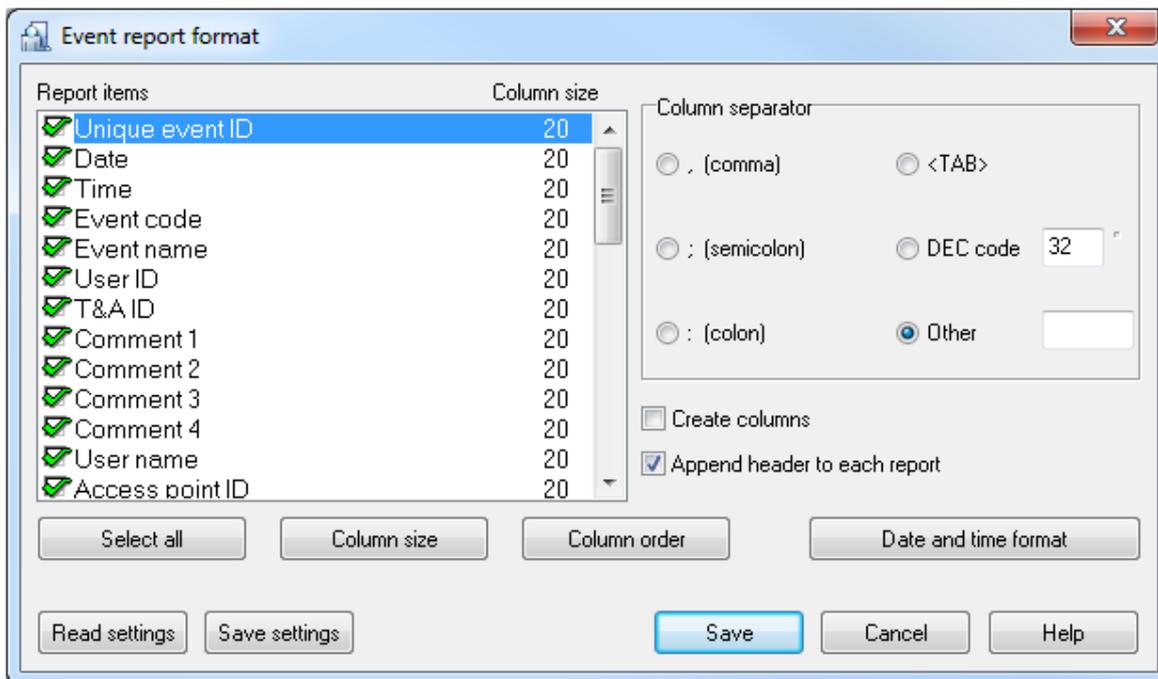


Figure 3.136. Defining format for the PREvents.csv file

Using this dialog box you can configure in detail the **PREvents.csv** file content. Operator can select columns to appear in the report, determine their size (width), change column order and specify date and time format.

PREvents.csv file format settings can be written to a file (the **Save settings** button), and imported from it later (the **Read settings** button).

Clicking on the **Event filter** button causes displaying the **Event filter** dialog box. It enables for example to save in **PREvents.csv** file only **Access denied** events for the selected user.



You can find more information on how filters can be defined in [section 3.3.7.1](#).

3.5.11.2. T&A reports

The **T&A Reports** tab can be used for setting options for generating **PREvents.rcp** file. It is shown in Figure 3.137.

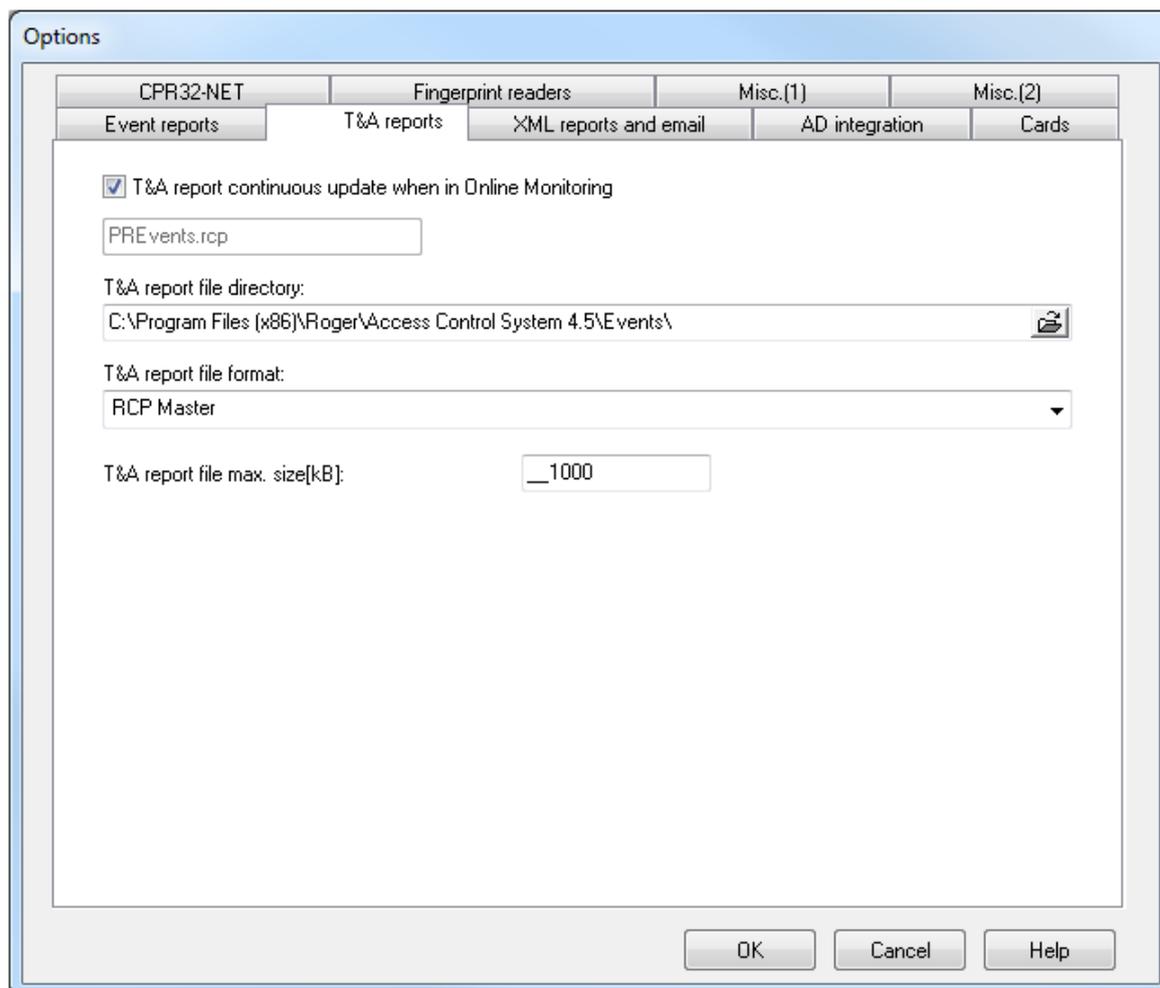


Figure 3.137. Options for generating T&A report

All the controls within the tab are active only when the **T&A report continuous update when in Online Monitoring** checkbox is checked.

The **T&A report file directory** allows to point the directory, where the **PREvents.rcp** file will be saved. The **T&A report file max. size [kB]** is used for determining a maximum size for the file containing report.

The **T&A report file format** field allows selecting one of available T&A report file formats. Following formats are available:

- ◆ RCP Master
- ◆ Gratyfikant ,
- ◆ Agrobex,
- ◆ Symfonia RCP,
- ◆ SDF Singapore,
- ◆ CIS (Singapore),
- ◆ Sykom
- ◆ RCP Access.
- ◆ Optima

3.5.11.3. XML reports and email

The **XML reports and email** tab is used for setting options for generating XML reports. Additionally it allows for setting up options for sending reports by e-mail. The tab is shown in Figure 3.138.

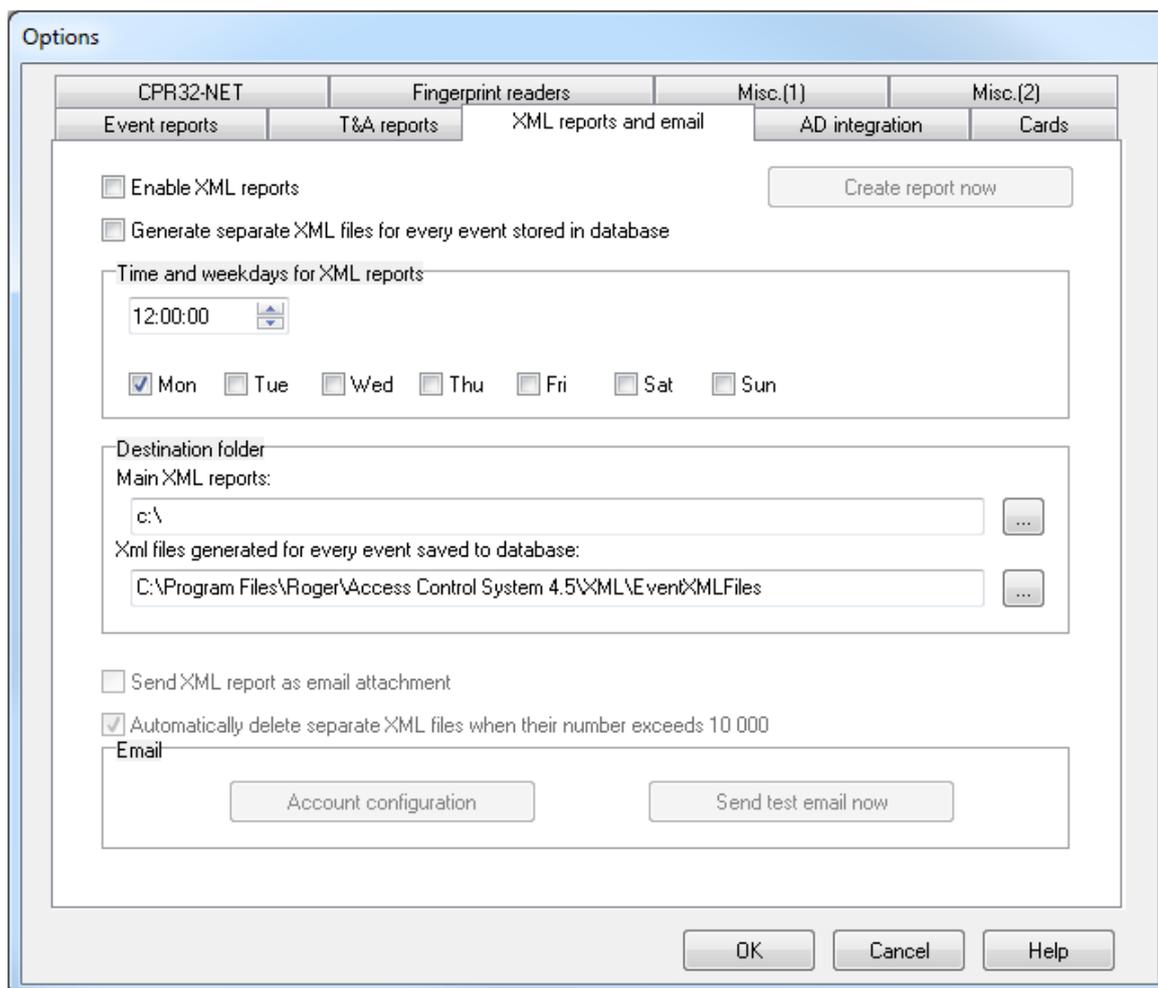


Figure 3.138. Options for generating T&A report

The options in **Time and weekdays for XML reports** and **Destination folder** areas are active only when the **Enable XML reports** checkbox is selected. But options in the **Email** area additionally require the checkbox **Send XML report as email attachment** to be selected.

In the **Time and weekdays for XML reports** area you should specify weekdays and times, when XML report should be generated. If you click on the **Create report now** button, the report will be created immediately. It will be saved in a directory specified in the **Destination folder** field in a file which name consists of the date and the time of generation.

If you select the **Send XML report as email attachment** checkbox, you can define an e-mail account where the e-mail report will be sent to. In order to do this, you should click on the **Account configuration** button. This will result in displaying **Mail configuration** dialog box (Figure 3.139).

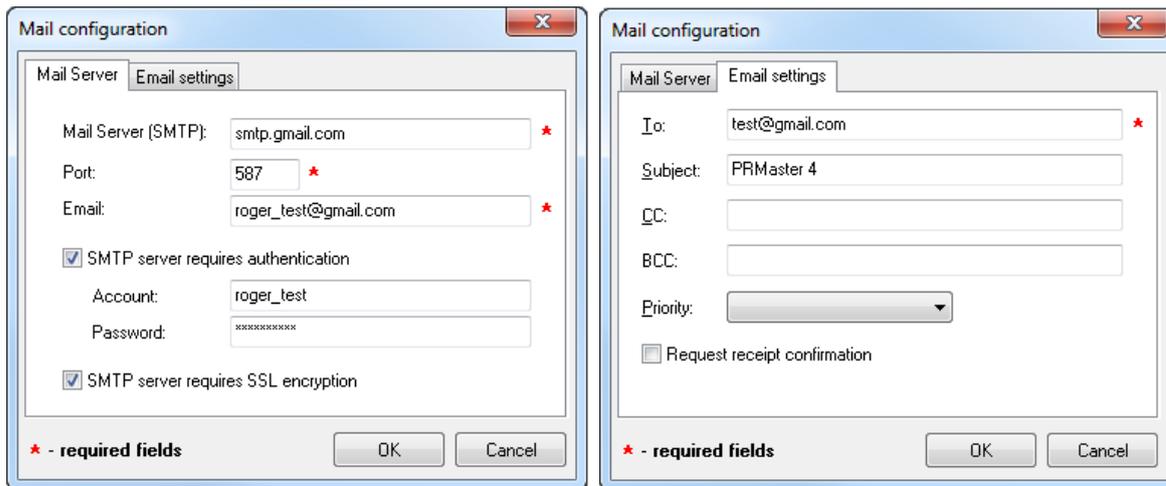


Figure 3.139. Mail account configuration for sending XML reports

The **Mail configuration** dialog box consists of two tabs: **Mail Server** and **Email settings**. An example on how these fields should be filled is shown in Figure 3.139. You should remember about entering a proper e-mail address, the report should be send to (the **To:** field in the **Email settings** tab) as well as about proper configuration of SMTP mail server options.

If the outgoing SMTP mail server requires authentication and SSL encryption, then you should select relevant options and enter both account and password of the email account used for email sending.

After you configure an e-mail account, you can make use of the **Send test email now** button. If all the settings are correct, the program will inform, that the e-mail has been sent properly (Figure 3.140).

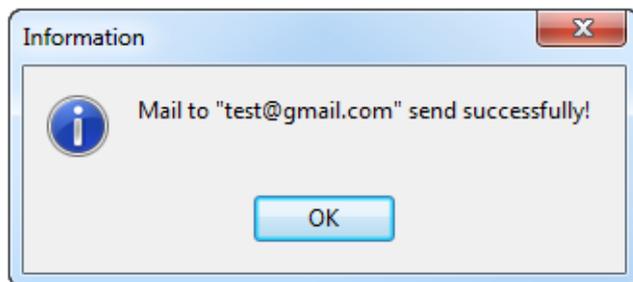


Figure 3.140. Mail configuration successfully completed

If you select **Generate separate XML files for every event stored to database**, then separate XML report will be generated in the subdirectory **EventXMLFiles** of the folder containing XML reports for every event saved to database. The files have names of the **ROGxxxxxxx.xml** format, where **xxxxxxx** indicates consecutive file's numbers. These files have the following content:

```
<ROG>
  <TIME>2010-07-01 08:42:40</TIME>
  <READER>1010</READER>
  <CARD>1E00EFD0B2</CARD>
  <ACCESS>N</ACCESS>
</ROG>
```

The fields have the following meaning:

- ◆ <TIME> — time when an event occurred,
- ◆ <READER> — reader’s id,
- ◆ <CARD> — card code or event code (in hex),
- ◆ <ACCESS> — this field can have values **T** or **N**. The **T** value means, that the controller has granted access, the **N** value means the opposite.

These XML files can be used for example for integration of RACS 4 system with other systems.

3.5.11.4. Misc

Two separate **Misc.(1)** and **Misc.(2)** tabs are available (Figure 3.141) and they include various options affecting system operation.

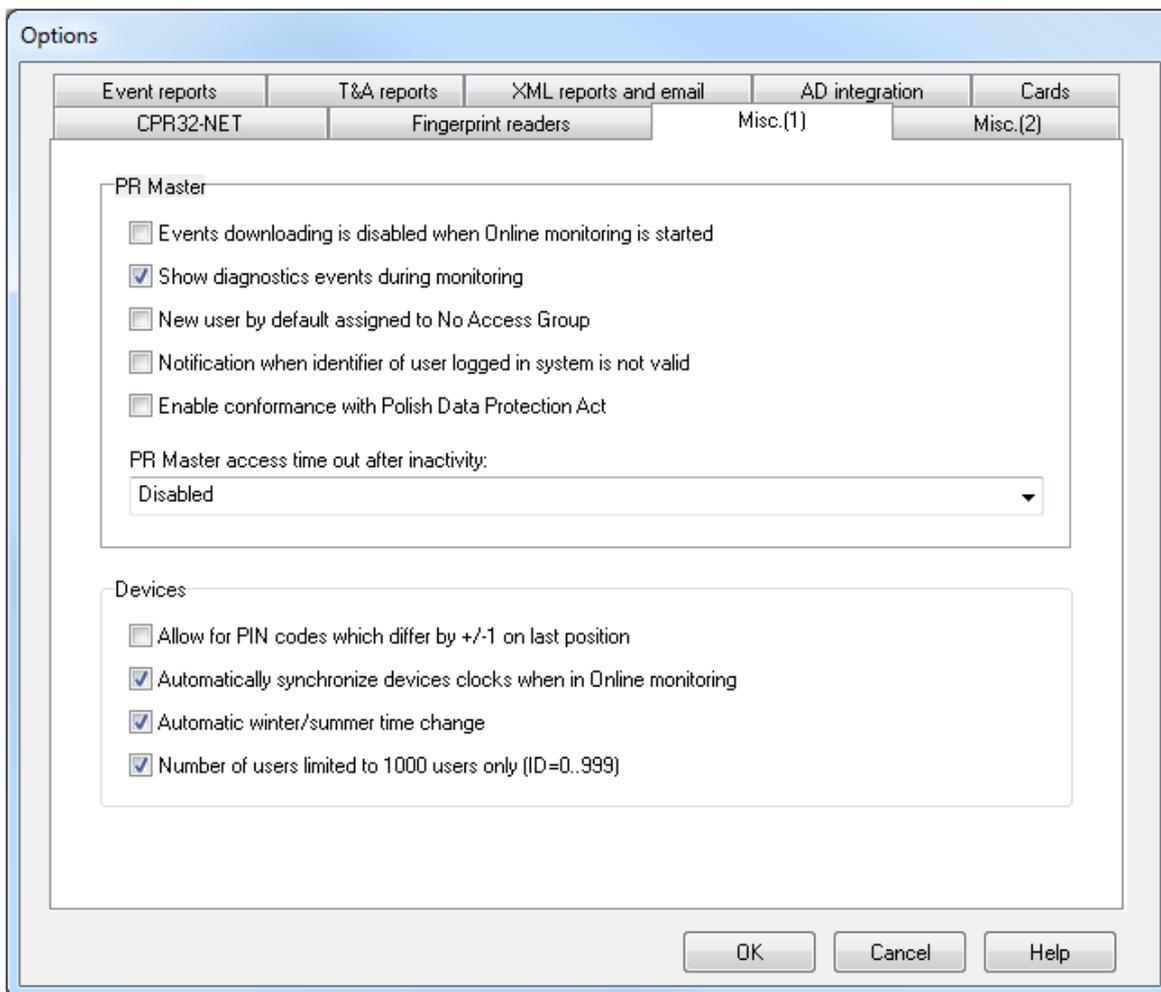


Figure 3.141a. Miscellaneous system options

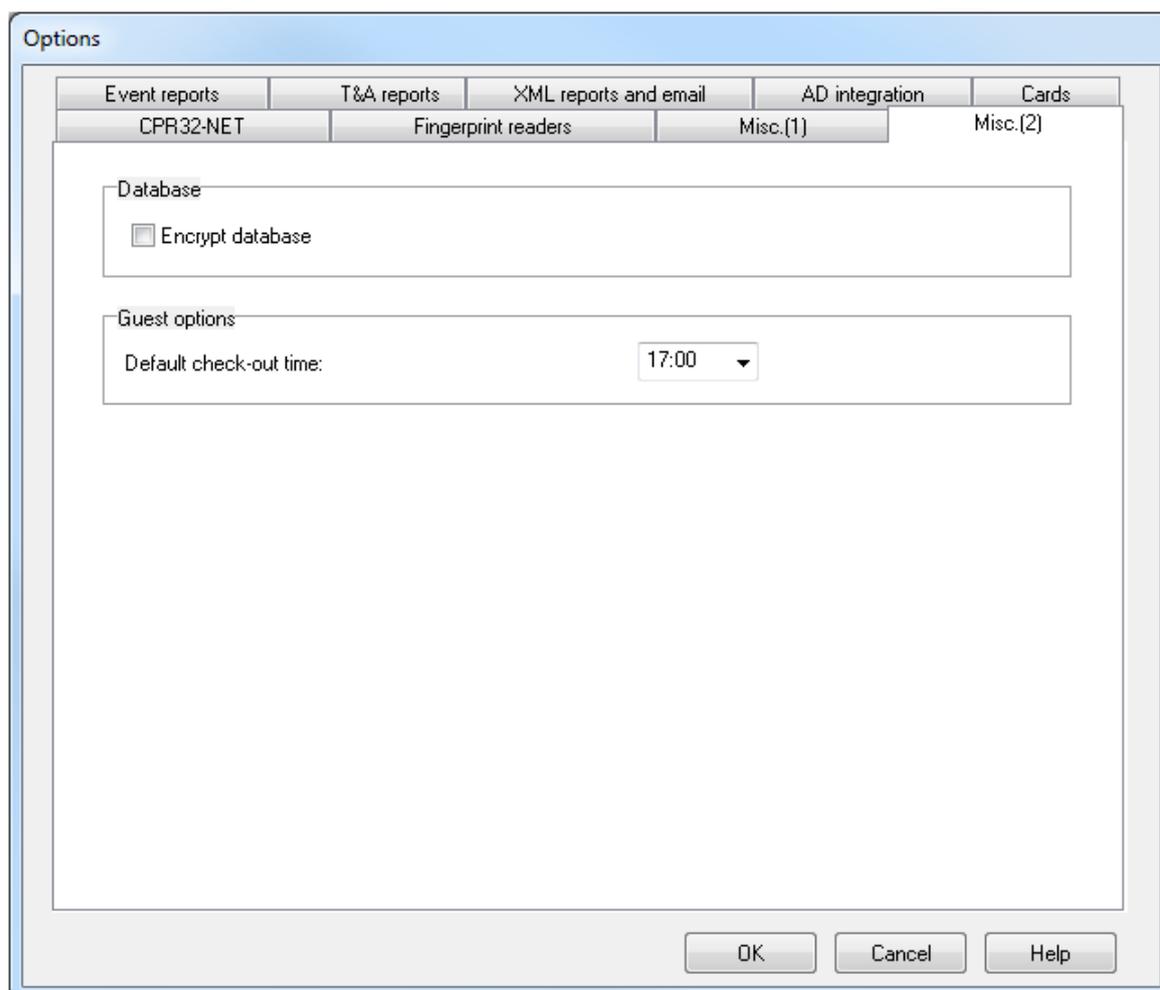


Figure 3.141b. *Miscellaneous system options*

In order to enable particular option, you should select checkbox next to the label containing its description or select from the list. Majority of options available in these tabs are self-explanatory.

When the **Events downloading is disabled when Online monitoring is started** checkbox is selected, then PR Master will not download events stored in devices when Online monitoring is started so the monitoring is started without delay. These events are not lost and still can be downloaded into database with **Read event buffers now** command – see [section 3.4.1](#) or any other method. If the option is not selected then when you enter Online monitoring, the PR Master will first read events from system buffers and write them to program's database.

The option **Notification when identifier of user logged in system is not valid** enables monitoring and detection of users with expired identifiers (cards, PINs, etc.). The access period for user identifier is defined within properties of such user in the tab **Identification**. In order to detect user with expired identifier it is necessary to start PR Master software in monitoring mode and such detection concerns users in internal Access Zones. Particular Access Zone can be defined as internal or external with the option **Access Zones** in the main window of PR Master software. When user with expired identifier is detected in monitoring mode then message window is displayed including basic information on such user. All users are verified automatically once per hour and it is possible to verify users on request selecting the tool **Users last login** and then the button **Verify expired** (see [section 4.1.10](#))

The option **Enable conformance with Polish Data Protection Act** is applicable for Polish market as it allows to satisfy requirements of:

- ◆ Act of Parliament from 29th August 1997 on personal protection data,
- ◆ Ordinance of Minister of Interior and Administration from 29th April 2004 on personal data processing documentation as well as technical and organizational conditions for IT devices and systems used in personal data processing.

When the option **Enable conformance with Polish Data Protection Act** is activated then it cannot be deactivated anymore for particular configuration (data base). When the option is checked then first and last names of users cannot be modified and new button is available in user properties – Figure 3.142.

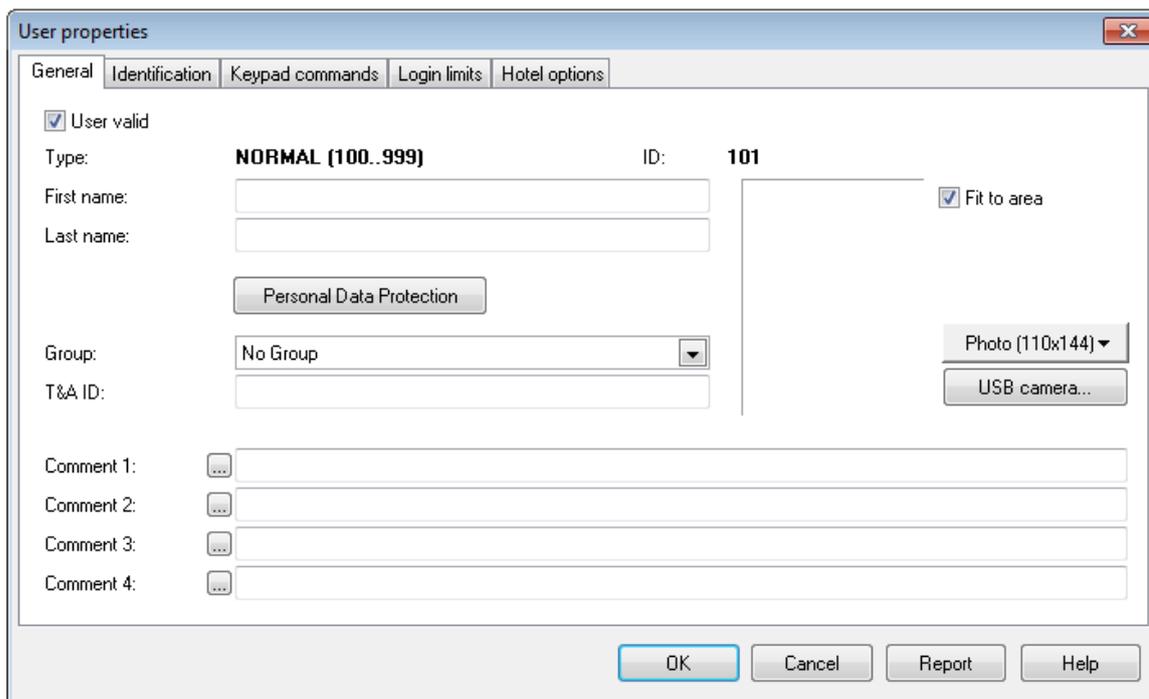


Figure 3.142. Personal Data Protection button

If the **Personal Data Protection** button is selected then window shown in Figure 3.143 is shown.

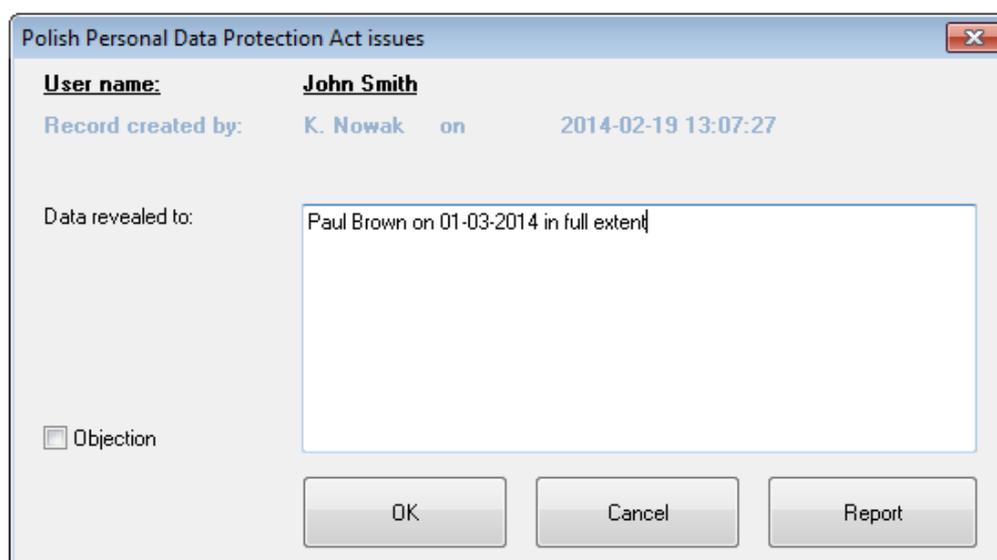


Figure 3.143. Personal Data Protection window

Name of the person who entered data as well as date when data was entered cannot be edited and they correspond to PR Master operator (see [section 3.5.8](#)). In the window a report can be generated by means of **Report** button and it can be further printed or saved to ***.rtf** or ***.csv** format.

The option **PR Master access time out after inactivity** enables to specify the time when PR Master becomes locked if the software is started but not used. In such situation when the time elapses, PR Master login window is displayed and in order to access the software it is necessary to enter valid password of current operator. Elapsing time is displayed in the bottom of PR Master main window.

The option **Allow for PIN codes which differ by +/-1 on last position** is related to DURESS signalling. If an user enters a PIN code which is increased or decreased by one on last position, the controller may read this as entering code under DURESS. Entering code under duress apart from normal controller reaction (opening the door, switching between ARMED/DISARMED mode) additionally triggers **FORCED ENTRY** event and it may cause signalling on controller's alarm output. For instance, if an user uses [6789][#] PIN code, then entering a code [6788][#] or [6780][#] will be interpreted by the controller as using the PIN code under duress. That is why, when this option is unchecked, the PR Master will not allow to define PIN codes differing by one on the last position. In case when using DURESS PIN codes in ACS is not necessary, you should select the **Allow for PIN codes which differ by +/-1 on last position** checkbox. After you select this option, the PR Master will allow for defining PIN codes in any form.

The option **Number of users limited to 1000 users only (ID=0..999)** is used when the number of users in the system is below 1000. When the checkbox is selected then the configuration upload to system devices is quicker.

The option **Default check-out time** enables setting default hour in the field **To** when Guest is added by means of the option **Guests** in the main window of PR Master (see [section 3.2.4](#)).

3.5.11.5. Cards

The **Cards** tab allows to select whether the card code of 40 bits length or 24 bits length should be used. This tab is presented in Figure 3.144.

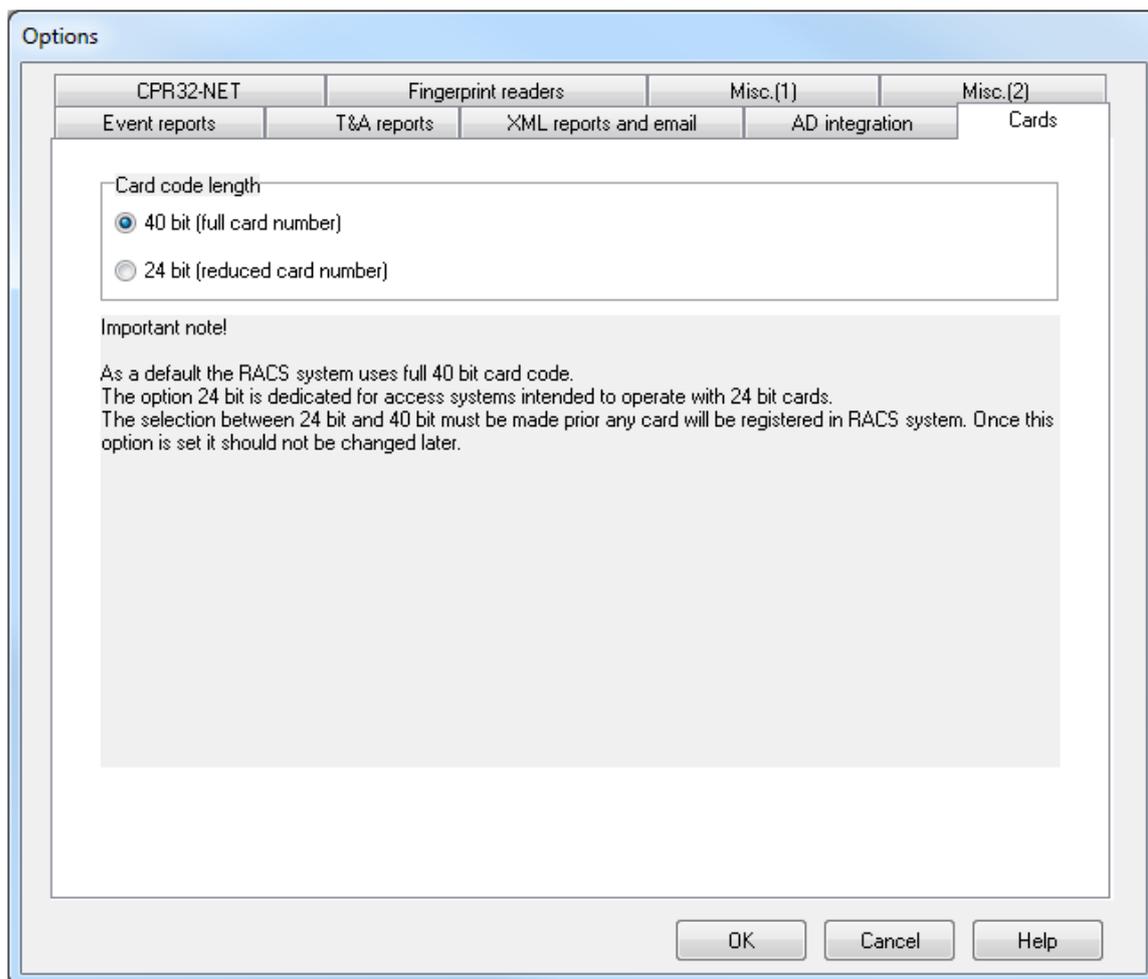


Figure 3.144. Card Code length options



You should remember that card code length options should be selected in the beginning of the database creation process. Before any card is registered. Changing option at a later stage may cause interferences in system's operation.

3.5.11.6. CPR32-NET

First of all, the **CPR32-NET** tab enables typing password for encrypted communication with CPR32-NET network controller. More information on encrypted communication with CPR32-NET is given in its manual which is available at www.roger.pl. This tab is presented in Figure 3.145.

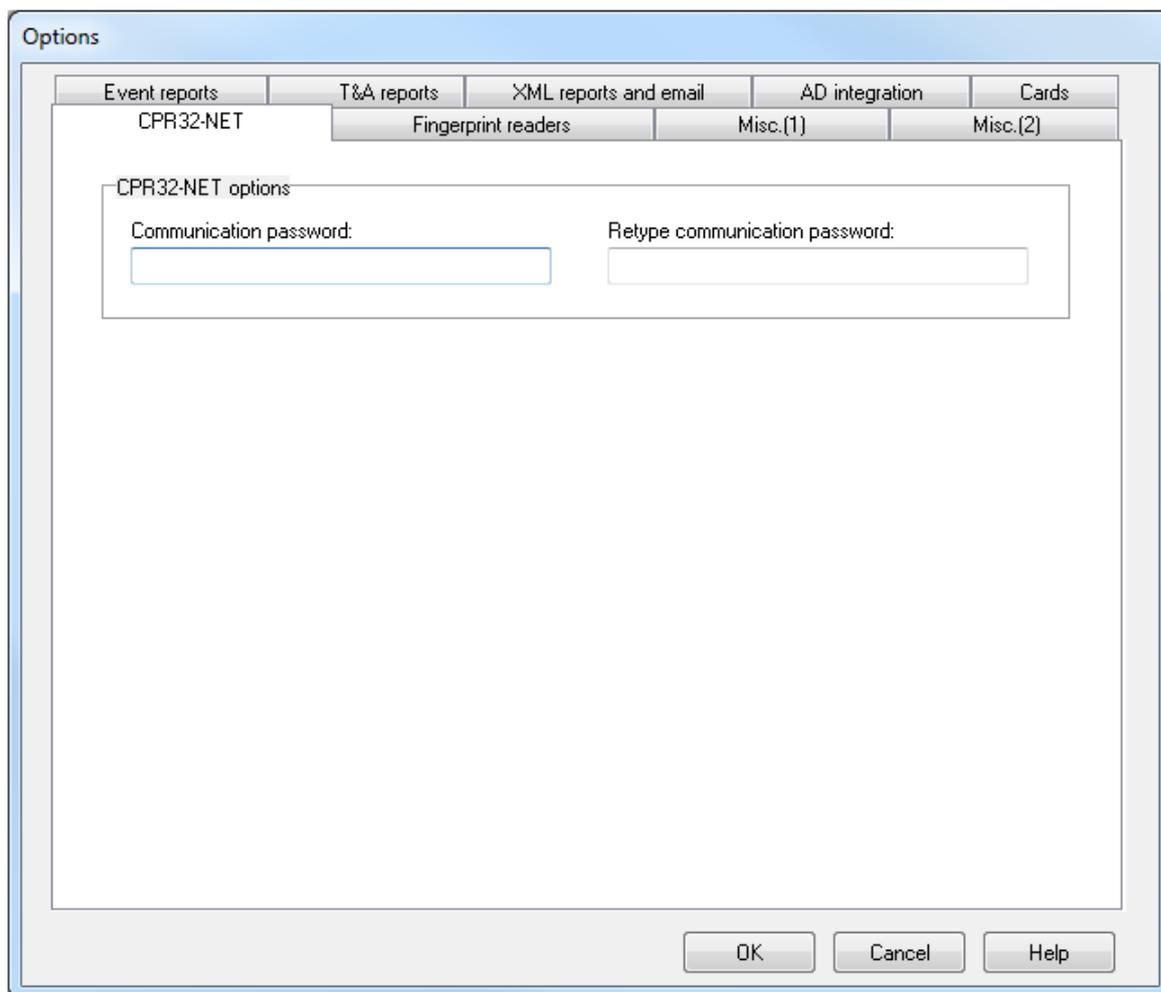


Figure 3.145. CPR32-NET options

3.5.11.7. Fingerprint readers

The **Fingerprint readers** tab enables selection of newer RFT1000 fingerprint reader or older, not offered for sale F7, F8, F9, F11 readers. Additionally in case of RFT1000 readers it is possible to select recognition mode. More information on RFT1000 reader is given in its manual, which is available at www.roger.pl. This tab is presented in Figure 3.146.

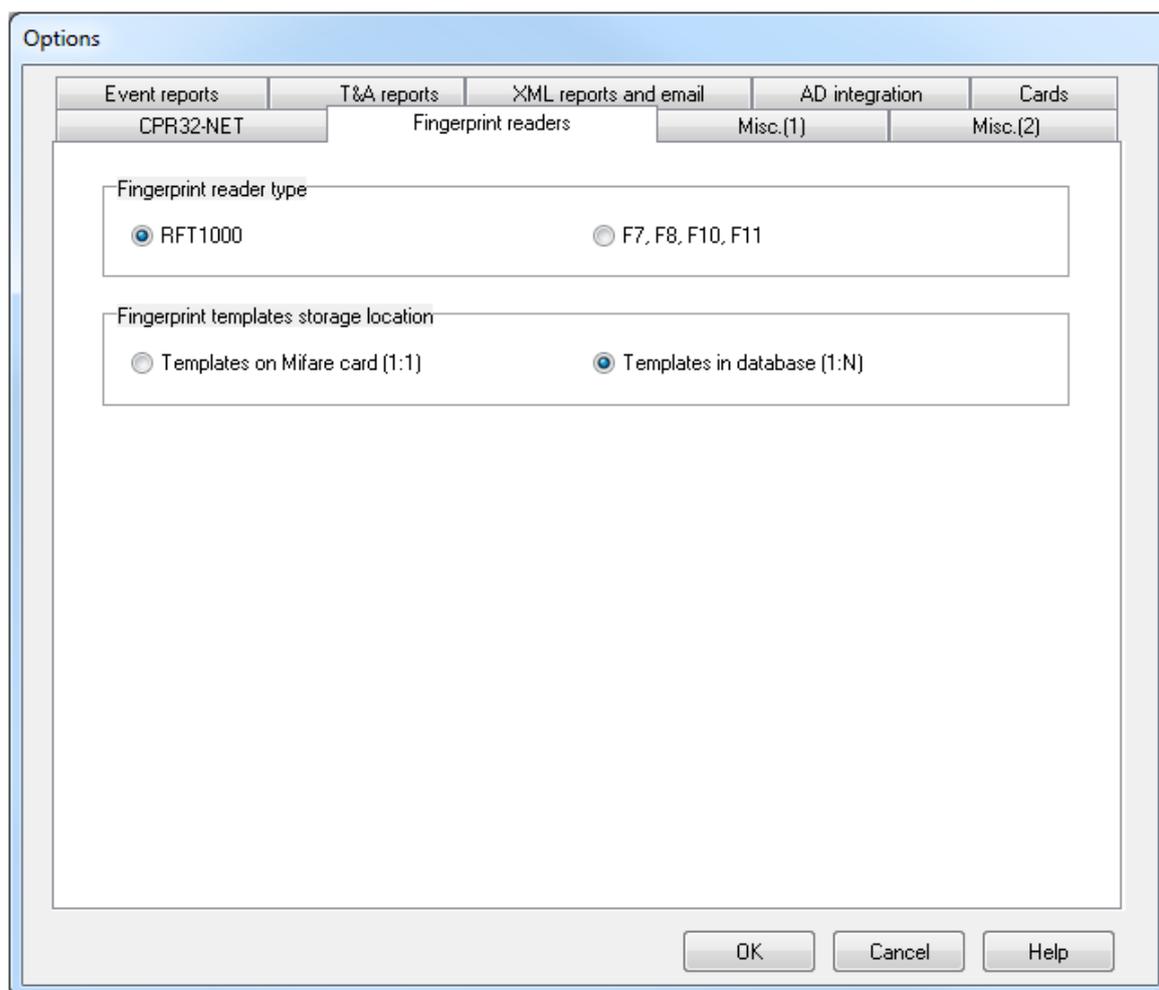


Figure 3.146. *Fingerprint readers options*

3.5.11.8. AD integration

The **AD integration** tab (Figure 3.147) concerns integration with Active Directory. The integration enables synchronization of Active Directory users with PR Master users but still it is necessary to assign access rights (Access Group) and upload new settings to controllers by means of PR Master software. When the integration is enabled then in the window opened by means of **Users** option in the main window of PR Master the option **Synchronize with Active Directory** is available (Figure 3.148). When selected, PR Master and AD users are synchronized in such way that new and modified users are imported from Active Directory while users not existing in Active Directory are removed from PR Master database. Additionally user deactivated in Active Directory are also deactivated in PR Master database. Users are compared based on their first names, last names and e-mail addresses. Therefore it is necessary to assign e-mail addresses to users within Active Directory. It is possible to synchronize all users from particular AD server or only selected users from AD server. In the first method it is necessary to specify AD server IP address while in the second method LDAP Queries are used. It is possible to enter multiple queries separated by semicolon [;]. Example of LDAP Query:

OU=SBSUsers,OU=Users,OU=MyBusiness,DC=ROGER,DC=local

where:

OU – Organizational Unit

DC – Domain Component

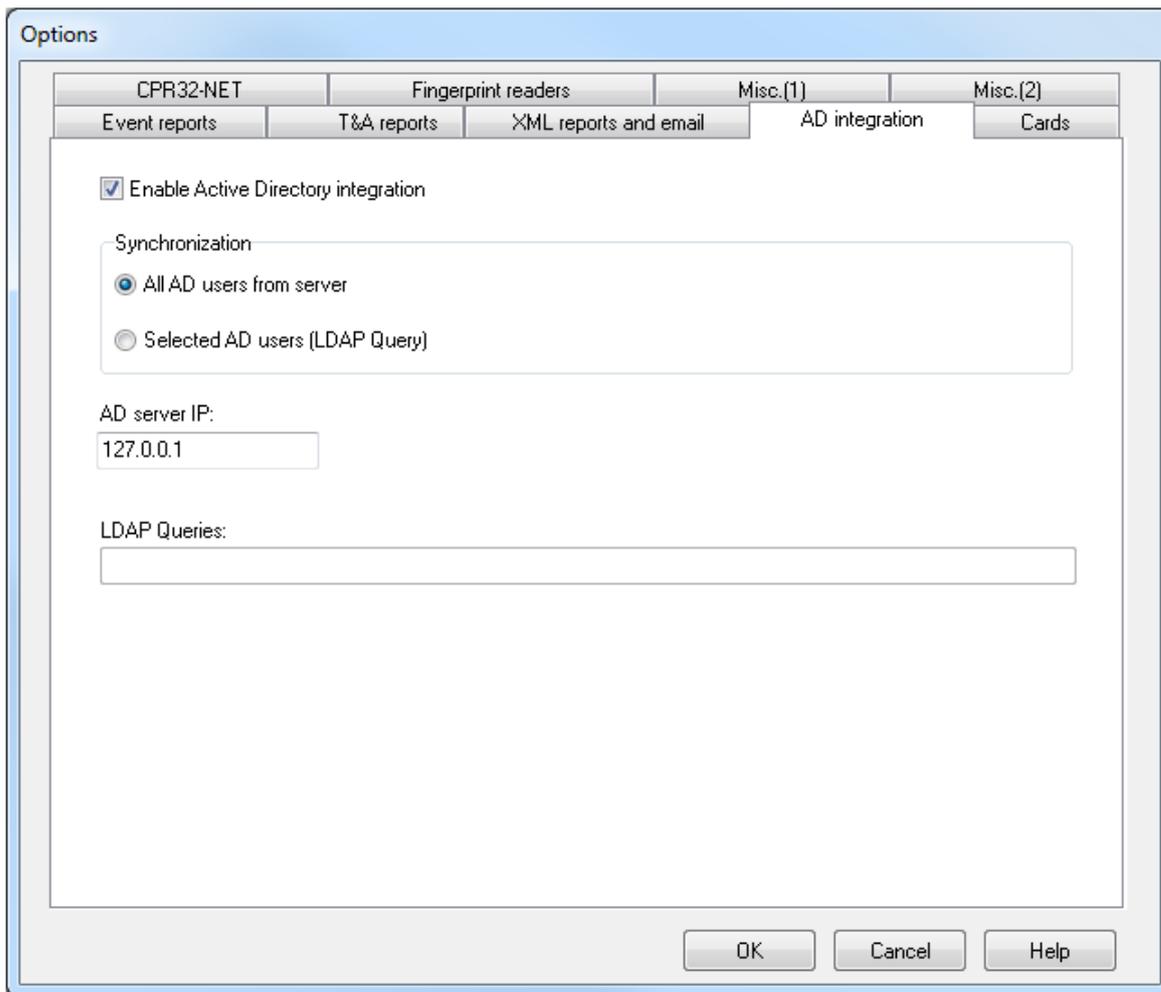


Figure 3.147. AD integration options

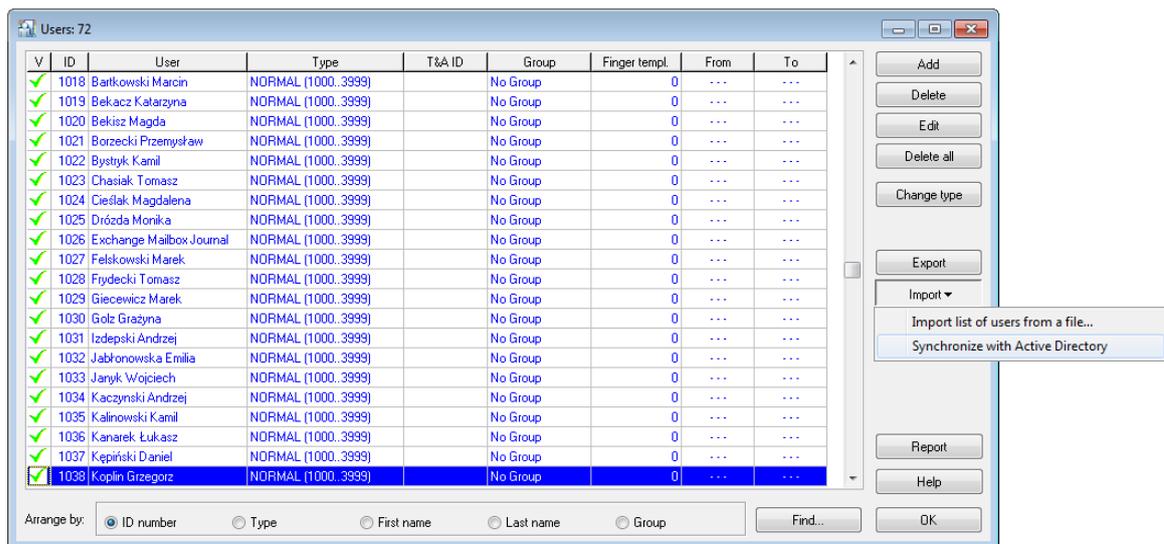


Figure 3.148. The option Synchronize with Active Directory

Users imported from Active Directory are displayed in blue so their access rights can be easily defined and new settings uploaded by means of Quick user update command as it is not necessary to upload the whole configuration to the system.



Users imported from Active Directory are assigned IDs over 1000. Therefore for the integration it is necessary to use PRxx2 series controllers which can maintain more than 1000 users.

Some users can be excluded from AD integration rules so they would not be removed from PR Master if they are not defined in Active Directory(e.g. cleaning personnel). In order to exclude particular user select the checkbox **Exclude from AD rules** (Figure 3.149) which is located in user properties in **General** tab. This checkbox is displayed only if AD integration is enabled.

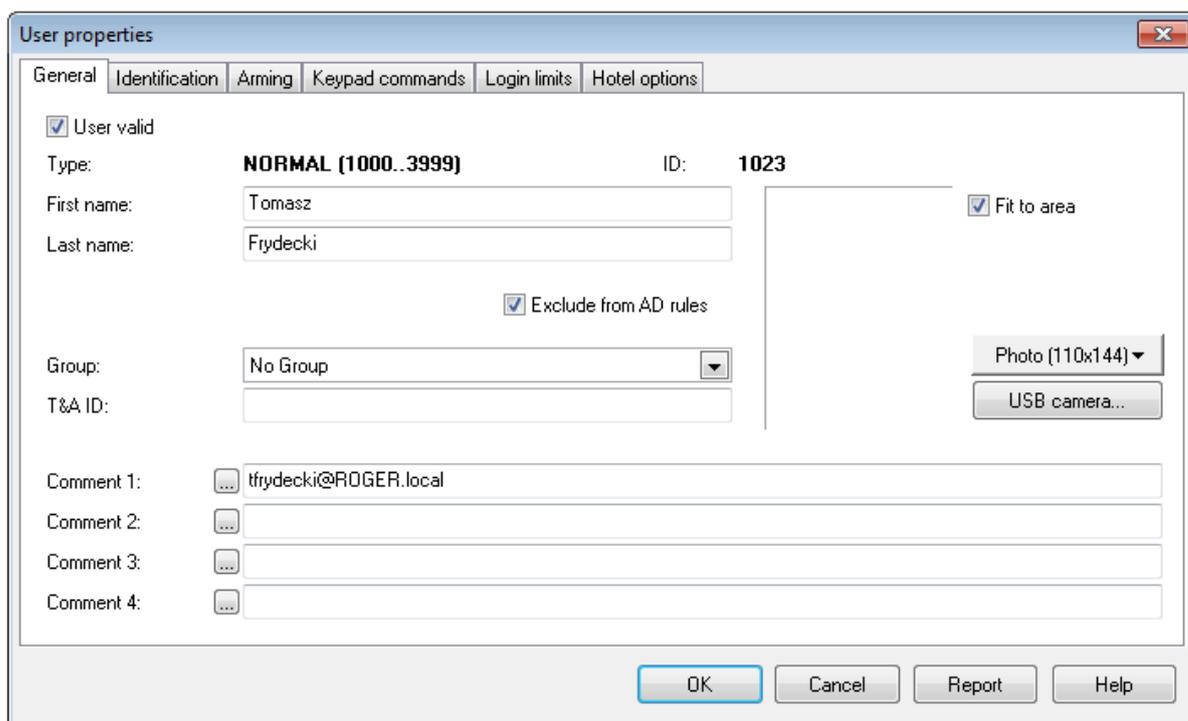


Figure 3.149. The option Exclude from AD rules

3.5.12. Backup configuration

Choosing the **Backup configuration** command results in displaying dialog box where backup mode and schedule can be defined (Figure 3.150). The majority of controls in this dialog box is active only after you select the **Enable auto backup** option. If this checkbox is not selected, then backups will not be created automatically. In such a case you can make backups manually. For this purpose you can click on the **Run backup now** button.

In the **Auto backup time and date** you should select weekdays and time, when backups are to be created. You should remember, that making full backup is time-consuming operation (especially when the database is large). Because of that, you should select the backup time in such way, as to avoid interfering with system operation as much as possible. The best if they were night hours, when there are relatively few events occurring in the system.

The **Delete backups older than selected number of days** allows to define storage period for backups. When the time elapses older backups are deleted from disk. This operation will be performed automatically, together with backup creation operation. Clicking on the **Remove now** button, causes removing old backups on request.

In the area **Backed up data in XML** there are two checkboxes i.e. **Configuration data** and **Event history**. Selecting particular checkbox will cause that data of specified type to be included in the backup. If you deselect both checkboxes no data will be stored.

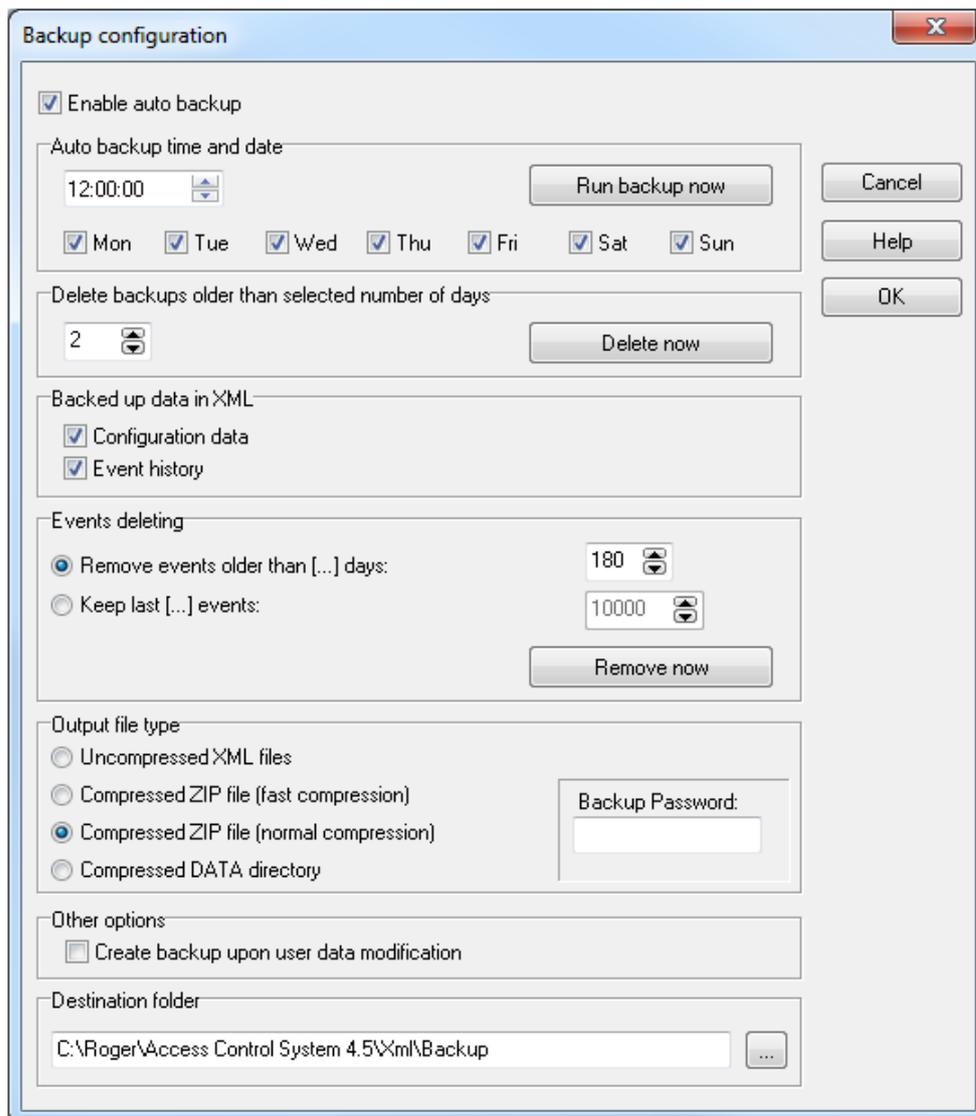


Figure 3.150. Backup options

The **Events deleting** let us define criteria for removing events from database. You can specify number of days which should elapse before events will be removed from database. You can also define an event history size as constant number of events which can be stored in database. If number of events exceeds this number, the oldest events will be deleted from database. Operation of deleting events is performed automatically, at the same time as the backup is created. Clicking on the **Remove now** button, causes removing events from database on request.

The **Output file type** allows for indicating format of a file, where a backup will be stored. You can select **Uncompressed XML**, XML formats with fast and normal ZIP compression or database backup in DDZ format. Optionally you can define password for ZIP and DDZ archives.

In the **Destination folder** area you should specify directory, where the backup is to be stored. Clicking on the  button enables selection of directory from the list.

3.5.13 Identify user

The **Identify user** command enables identification of proximity card, if it belongs to user defined in the system or it is unknown (Figure 3.151). When the window is opened then the first reader on the list is automatically selected and it is just enough to read particular card at this reader.

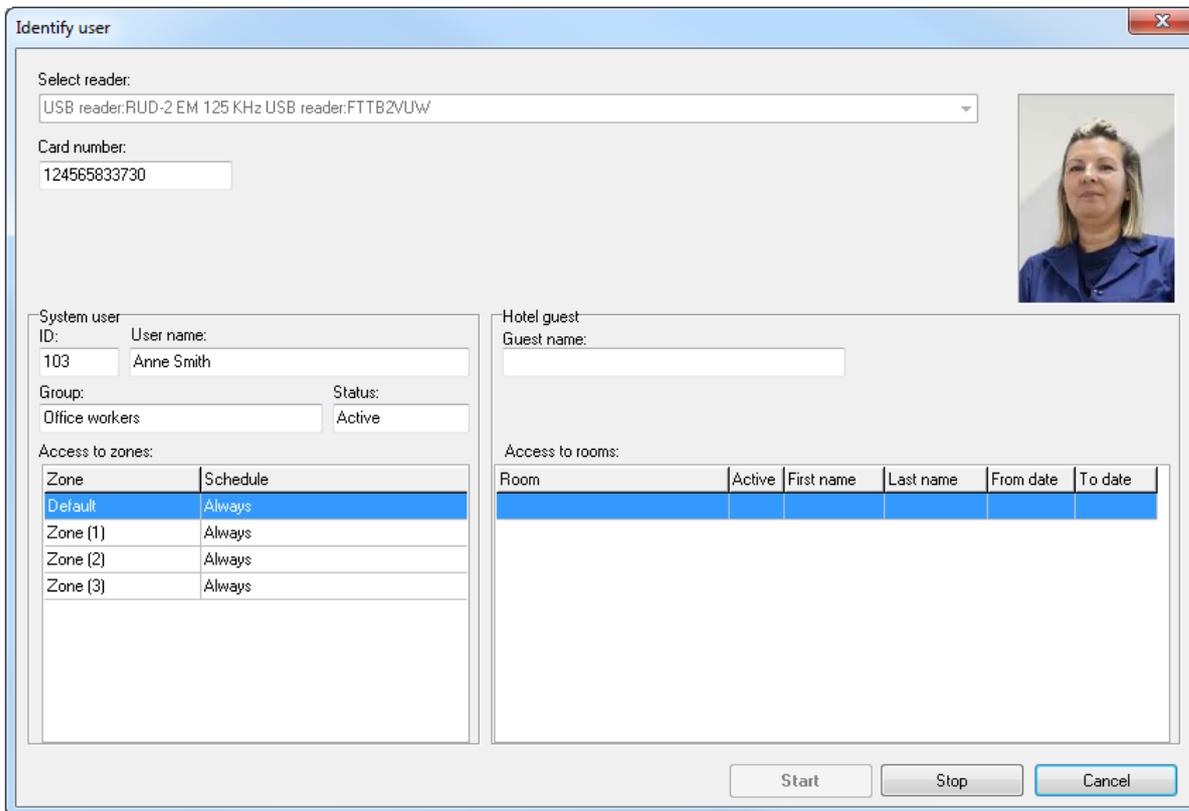


Figure 3.151. Identify user window

CHAPTER 4. ONLINE MONITORING

Online monitoring is a special mode of PR Master operation, in which events occurring in the RACS 4 are visualized in a real time and displayed in dedicated window. When PR Master operates in this mode, events occurring in the system are immediately appended to the system database and available for reporting. A monitoring mode can be turned on by selecting **Tools/Online monitoring** or clicking on the **Online monitoring** icon in the **Frequently used tasks** panel from the right side of the main program’s window. Program’s window in an online monitoring mode is shown in Figure 4.1.

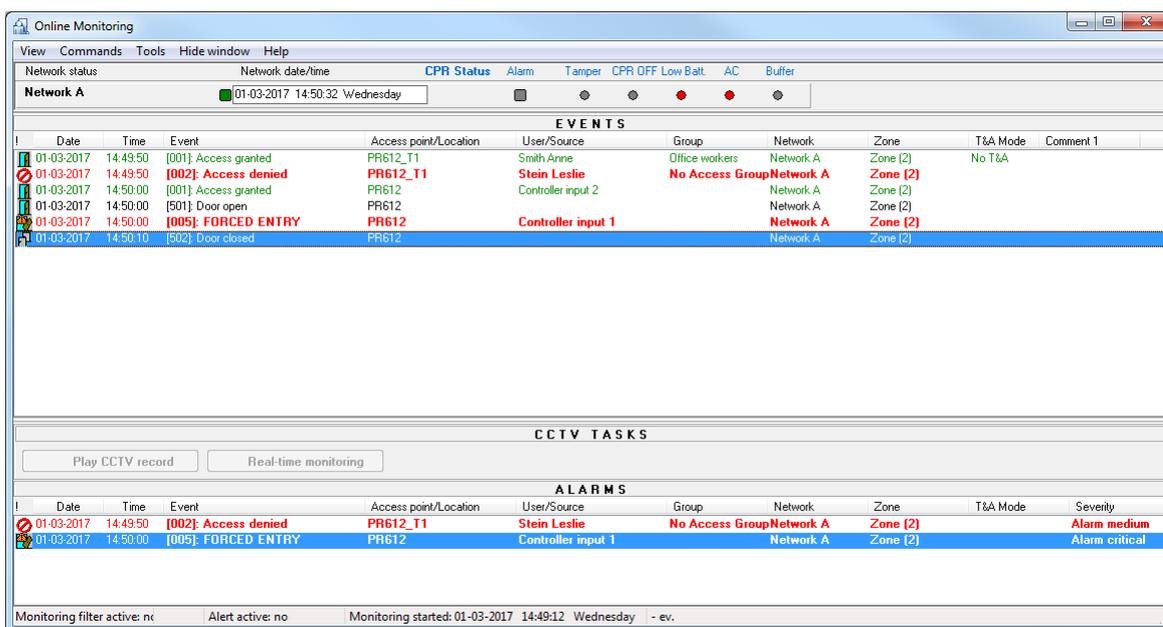


Figure 4.1. PR Master window in online monitoring mode

In this mode of operation the PR Master uses a separate menu and the PR Master’s main menu is not available. Below the menu bar there is a list of networks together with graphical feedback on alerts present in a particular network. Under the list of networks there is an **EVENTS** area, where events happening in the system are appended on an ongoing basis. Under the **EVENTS** area there is **CCTV TASKS** area when certain actions related to CCTV integration can be conducted. In the bottom there is **ALARMS** area, where messages about alarms activated in the system are displayed.

In the status bar you can find information regarding used filters, status for events signalling as well as date and time when monitoring began.

4.1. VIEW MENU

The **View** menu is shown in Figure 4.2.

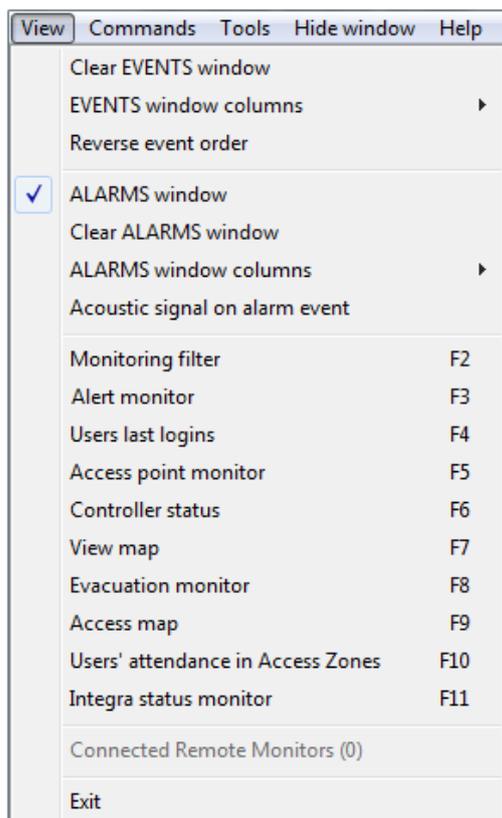


Figure 4.2. The PR Master's View menu in online monitoring mode

4.1.1. Clear EVENTS window

This command clears the **EVENTS** window and **ALARMS** window. However events are not actually deleted from database but only disappear from monitoring window. This function can be useful when we want to start observing events from particular moment and we do not want to be distracted by previous events.

4.1.2. EVENTS window columns

The **EVENTS window columns** command opens menu containing list of column to be selected (Figure 4.3). Selected columns are displayed in the **EVENTS** window.

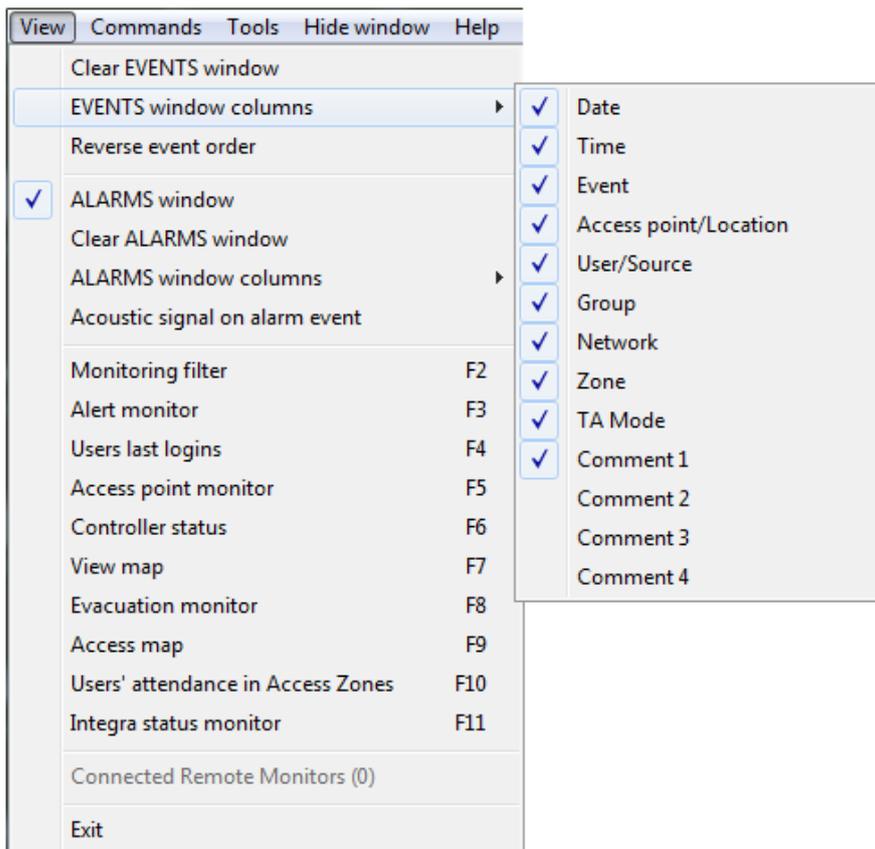


Figure 4.3. Selecting columns to be displayed in the EVENTS window

4.1.3. Reverse event order

By default, events in the **Online monitoring** window are displayed from the latest to the newest — i.e. at the top of the list the oldest events are displayed. If you select the **Reverse event order** option then at the top of the list the latest events are displayed.

4.1.4. ALARMS window

The **ALARMS window** is used for switching **ALARMS** window on/off. If it is selected, the **ALARMS** window is displayed.

4.1.5. Clear ALARMS window

This command clears the events displayed in the **ALARMS** window. However events are not actually deleted from database but only disappear from monitoring window. This function can be useful when we want to start observing alarms from particular moment and we do not want to be distracted by previous alarms.

4.1.6. ALARMS window columns

The **ALARMS window columns** command opens menu containing list of column to be selected (Figure 4.4). Selected columns are displayed in **ALARMS** window.

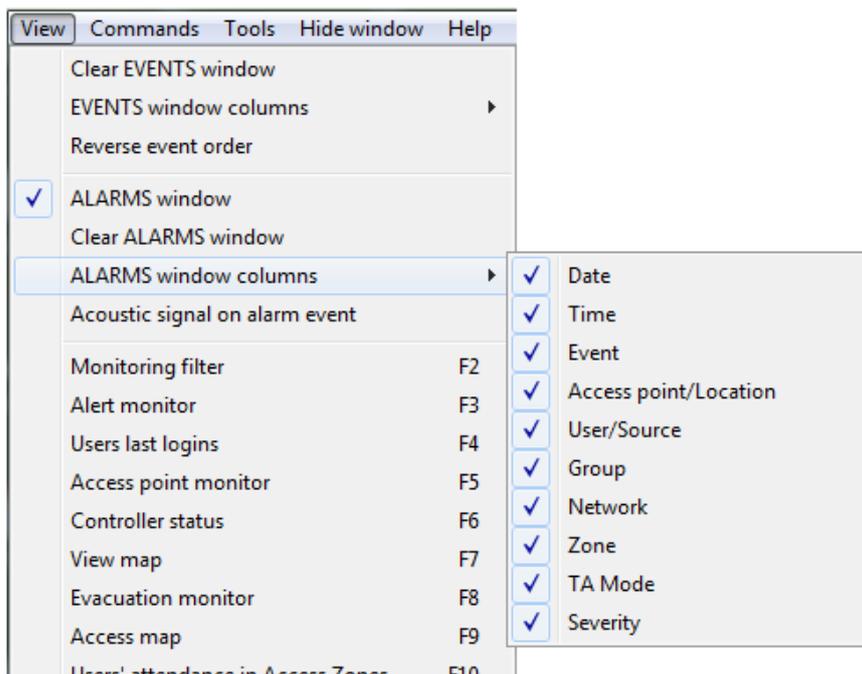


Figure 4.4. Selecting columns to be displayed in the ALARMS window

4.1.7. Acoustic signal on alarm event

When this option is selected then alarm events are additionally signalled acoustically by computer. When this option is not selected, then alarm events will be displayed in **EVENTS** and **ALARMS** windows without acoustic signal.

4.1.8. Monitoring filter

Selecting the **Monitoring filter** command causes displaying the **Monitoring filter** dialog box (Figure 4.5).

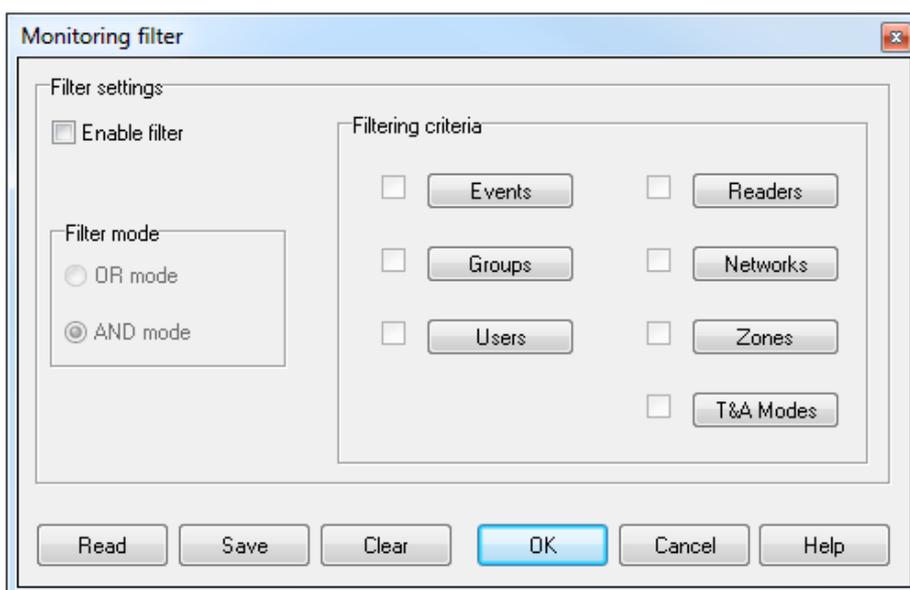


Figure 4.5. Defining filter in monitoring

This dialog box can be used in the same way as the dialog box for defining event filter (see [section 3.3.7](#)).



The filter concerns all the events registered from the moment, the monitoring online mode was turned on. This means that if the **Clear Events** window was used before defining filter, then in the list of events the events which were cleared before will also be included. Thus, the filtering command can be used for restoring the **Online monitoring** window content. To do that you need only to select the **Monitoring filter** command and click **OK** in the dialog box which will appear.

4.1.9. Alert monitor

The command can be used to define event filter for PR Master in monitoring mode to display alerts requiring operator confirmation. When the commands is selected then **Alert filter** dialog box is displayed (Figure 4.6a).

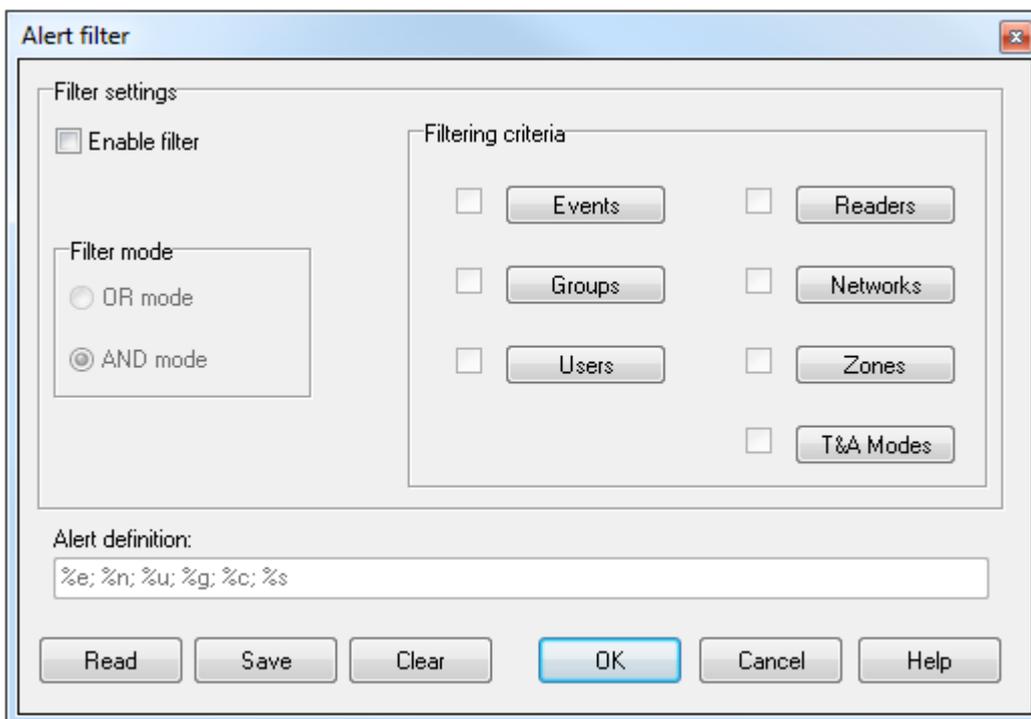


Figure 4.6a. Alert filter defining

This dialog box can be used in the same way as the dialog box for defining event filter (see [section 3.3.7](#)) but it includes additional **Alert definition** field. This field allows for defining additional message which is displayed when the alert occurs. Default definition format is %e; %u; %g; %c; %s where respective parameters correspond to event, user, group, controller/reader and network. Default definition can be restored with **Clear** button. Alternatively own text can be entered in **Alert definition** field and such text shall be displayed for all alerts.

When the event conforming with filtering criteria occurs in monitoring mode then **Alert list** dialog box is displayed. Any event can raise alert but it is more practical to associate alarm events with alerts. All alerts in **Alert list** are sorted by their severity (critical on the top). The severity of certain event type is defined in **Alarm Events** dialog box (see [section 3.5.6](#)). Alerts require confirmation by operator.

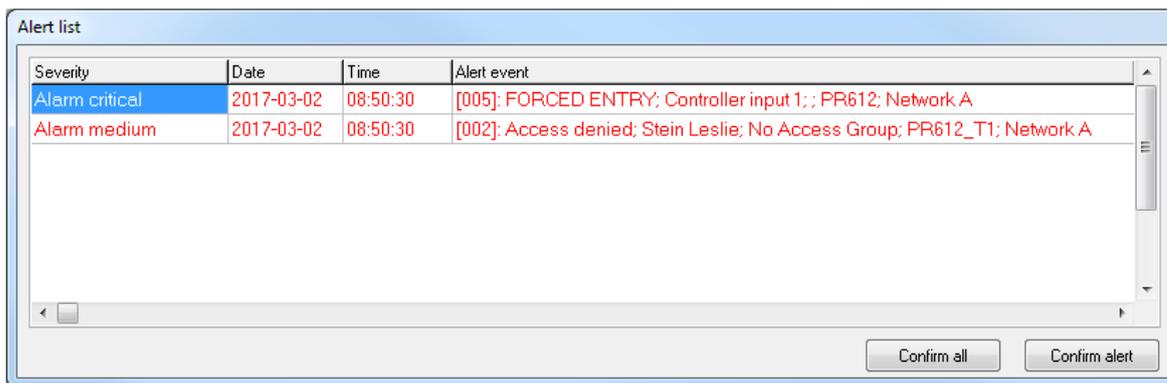


Figure 4.6b. Alert list example

4.1.10. Users last logins

The **Users last logins** command enables to determine the latest logins of all users i.e. location of users. If you select this command, the **Users last login** window is shown (Figure 4.7).

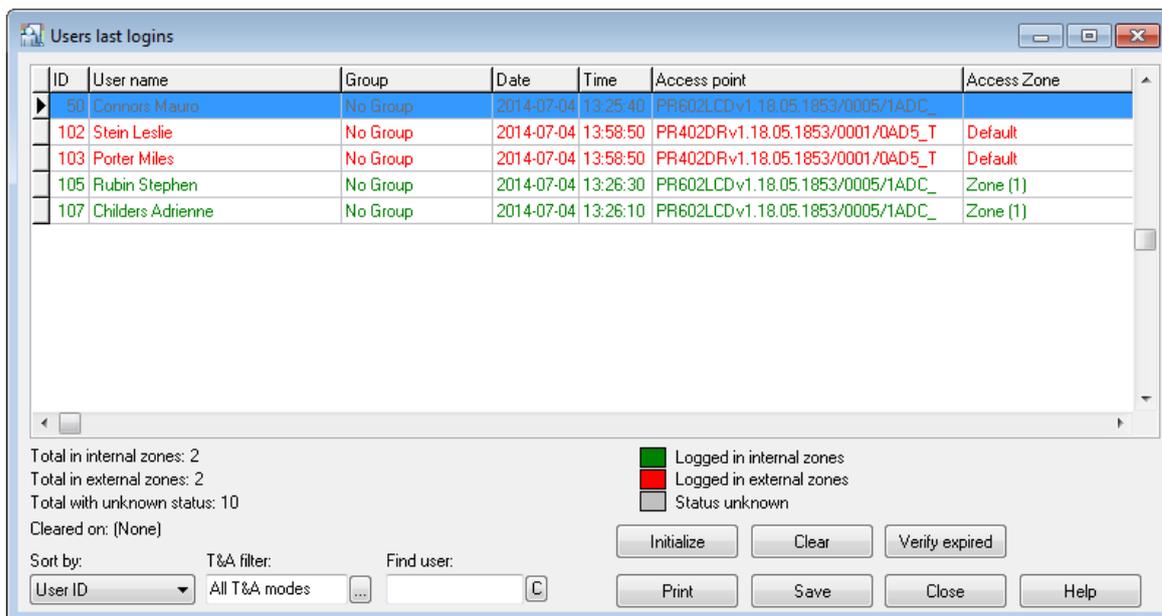


Figure 4.7. Places where users logged in recently

The window contains a list of users marked with different colours depending on their login status. Under the list there is a summary containing number of users with particular status and an explanation of colours meaning. External/internal types are defined during access zone configuration (see section 3.2.7). The **Sort by** listbox lets sort the list of users by their ID, name, group, date/time, reader and access zone. The **T&A filter** field allows to select only these controllers which registered indicated T&A mode. The **Find user** field allows to located user with particular last name on the list. System performs „active search” i.e as you enter successive letters, the system locates a user who satisfies criteria.

The **Initialize** button initializes a list of logins based on the current event history in the RACS 4. The **Clear** button clears the list of last logins and the button **Verify expired** is used for verification of users with expired identifiers (see 3.5.11.4)

The **Print** button lets you print the list of logins on the printer, and the **Save** button allows for saving it in **.rtf** or **.csv** file formats.

4.1.11. Evacuation Monitor

The **Evacuation monitor** command enables displaying of list with users, who require evacuation from the building/area with access control system. If you select this command, the **Evacuation monitor** window shall appear (Figure 4.8).

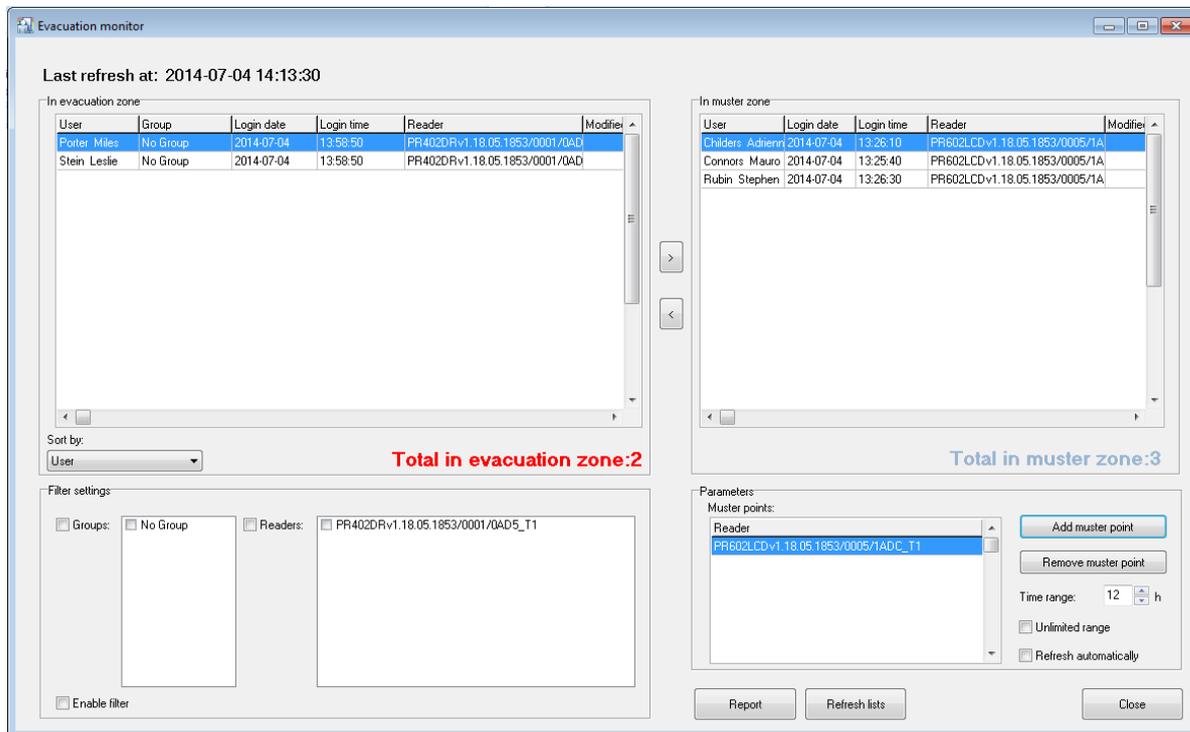


Figure 4.8. Evacuation monitor

The window contains two lists with users. The one on the left includes users, who did not reach muster point(-s) and require evacuation while the list on the right indicates users who reached muster point(-s). The muster point i.e. the reader in access control system can be selected in the area **Parameters** . In the same area the administrator can also set time range (12h by default) for all observations. The administrator can also manually move users between lists by means of < and > buttons. It might be required when particular user reaches muster point but without his proximity card. In the area **Filter settings**, it is possible to filter users in evacuation zone by User Group and reader of the latest identification. The report from Evacuation monitor can be generated and then printed and/or saved to **.rtf** or **.csv** format by means of the button **Report**. The configuration of Evacuation monitor is automatically saved by PR Master software. For example, if muster point is selected then it shall be saved and in case of the next starting of Evacuation monitor it shall be automatically loaded. Therefore the configuration of Evacuation monitor can be prepared in advance so in case of emergency the monitor is just started and no settings are required.

4.1.12. Access Point Monitor

The **Access Point Monitor** command lets you visualize information for particular reader/controller in real time. If you select this command, the **Access point monitor** dialog box displays (Figure 4.9).

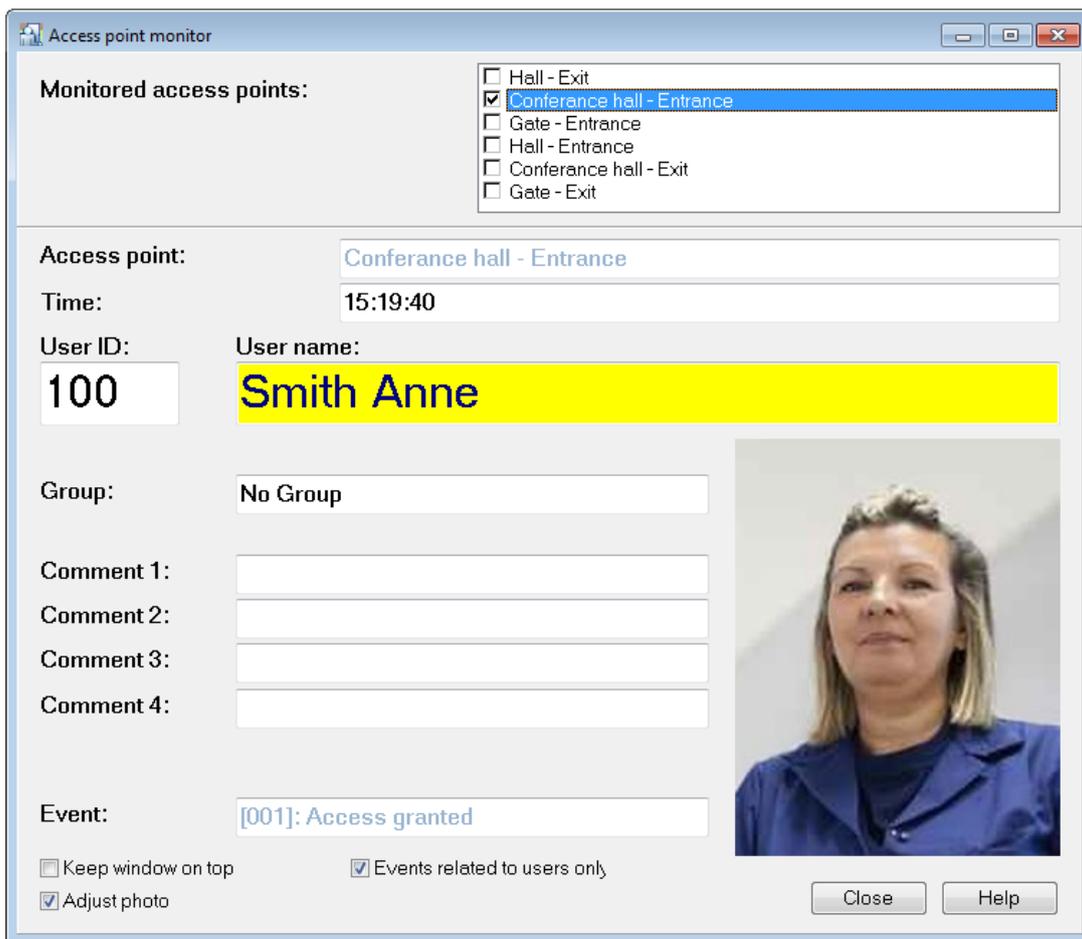


Figure 4.9. Access point monitor

In this window you should select identification points which are to be monitored. Events at particular door are displayed in the window. In this way you can verify, if particular card and/or PIN is used by the authorized person. This is especially useful in systems with many users.

If you select the **Events related to users only** option, then only events related to users such as access granted events are displayed in the window.

4.1.13. Controller status

The **Controller status** command displays a window containing information on controllers working in RACS 4 (Figure 4.10).

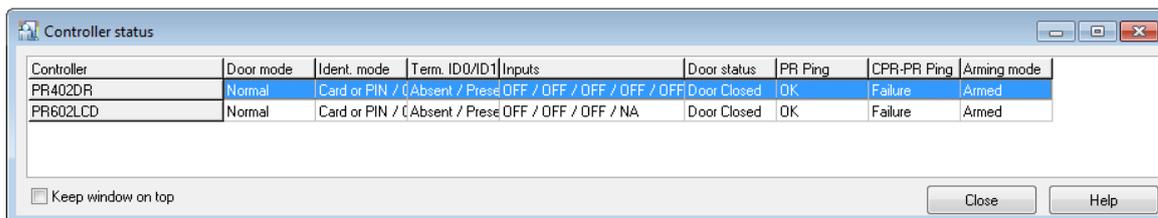


Figure 4.10. Controller status

From this window you can read such information as a door mode, ID0/ID1 terminals status, inputs status, door status, communication with the controller status and arming mode. Data in table is

refreshed every 5 seconds. The N/A symbol means that data is not available. Data can be sorted by double clicking in selected column.

4.1.14. View map

The **View map** command allows to visually monitor the system using facility plans defined earlier (see [section 3.2.14](#)). After you select this command, the **Facility plan manager** window displays (Figure 4.11) which lets user select facility plans to be displayed.

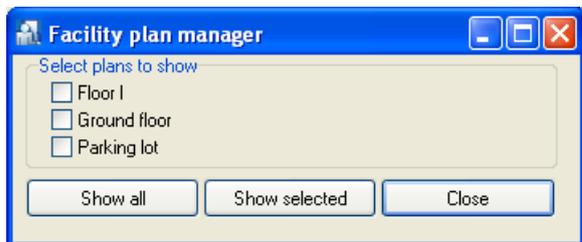


Figure 4.11. Facility plan manager — selecting plans for display

If you select checkboxes next to plans you want to display and then click **Show selected** button, the program will show facility plans defined earlier. Your monitoring screen can look as shown in Figure 4.12.

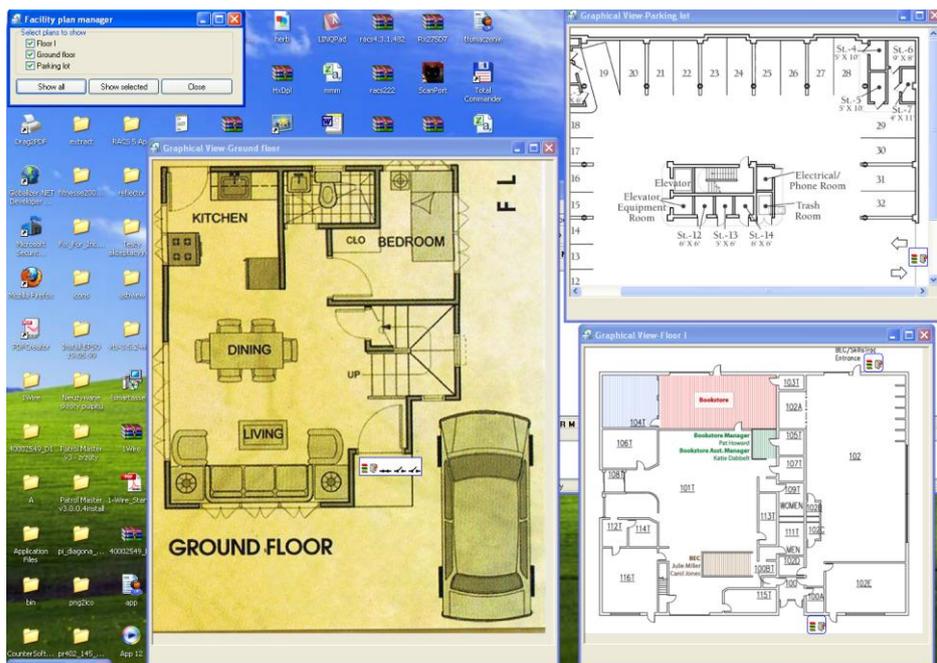


Figure 4.12. Visual mode of facility monitoring

In this mode you can track controller state in a real time as well as send commands to them. In order to get access to commands menu, you should right-click a controller's icon (Figure 4.13).

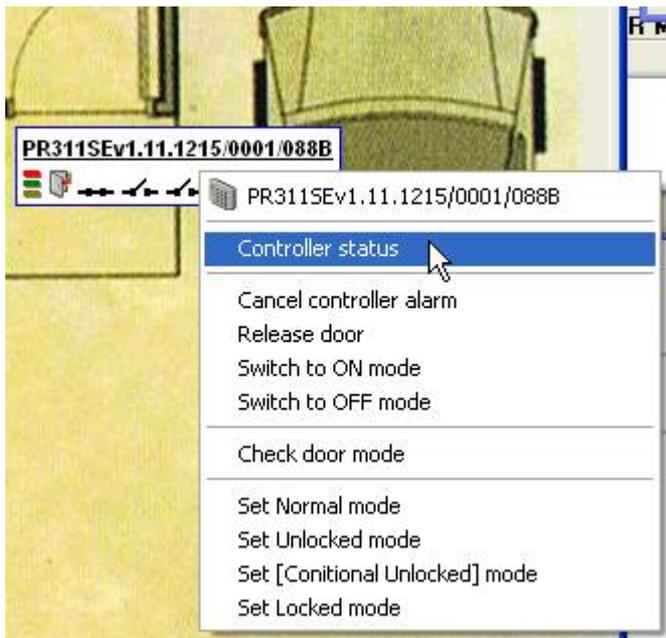


Figure 4.13. Controller's command menu

If you left-click particular controller icon, then full information about its state will be displayed. Thanks to this you can find out in detail what is going on with controller represented in the plan by means of minimized icon.

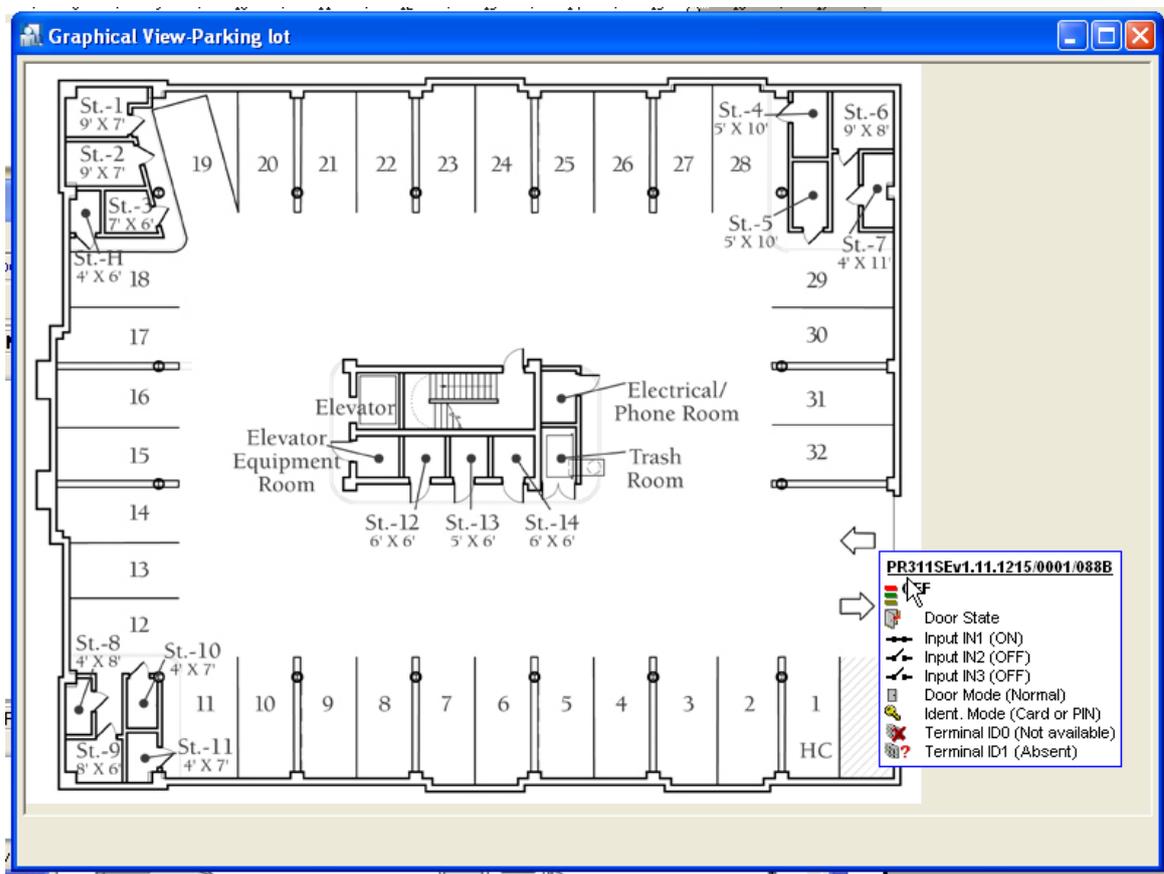


Figure 4.14. *After you click the controller icon, complete information on it will be displayed*

After you select facility plans to be displayed, you can close the **Facility plan manager window**. You can also freely move windows of specific plans, as well as close them. However you should note, that PR Master automatically remembers last location and layout of every plan. Thanks to this the plan will display at the same location, as it was when it was closed.

Closing the PR Master's monitoring window automatically closes all opened facility plans' windows.

4.1.15. Access map

This command is an equivalent to the **Tools/Access map** command which is described in **section 3.5.3**.

4.1.16. Users' attendance in Access Zones

The **Users' attendance in Access Zones** is an equivalent to the **Tools/Users attendance within Access zones** command which is described in **section 3.5.4**.

4.1.17. Integra status monitor

The command **Integra status monitor** is used when integration with INTEGRA (SATEL) intruder alarm panel is enabled. Such integration requires CPR32-NET network controller. More information is given in dedicated manual which is available at www.roger.pl.

4.1.18. Connected Remote Monitors

Remote Monitor program can be a client software to PR Master. It lets you remotely monitor the RACS 4. The **Connected Remote Monitors** command shows you how many Remote Monitor clients established connection with PR Master.

4.1.19. Exit

The **Exit** command closes PR Master's online monitoring mode. Before the system closes online monitoring mode, it displays a confirmation message asking if you really want to close this mode of program operation.

4.2. COMMANDS MENU

The **Commands** menu in PR Master online monitoring mode is shown in Figure 4.15.

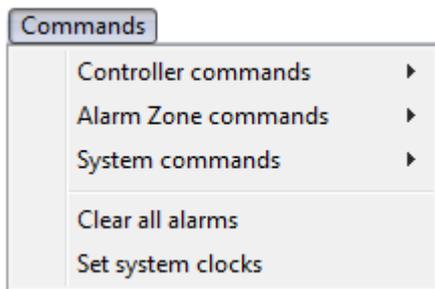


Figure 4.15. Commands menu

4.2.1. Controllers command submenu

The **Controller commands** submenu contains a list of commands which can be applied to selected controller. It is shown in Figure 4.16.

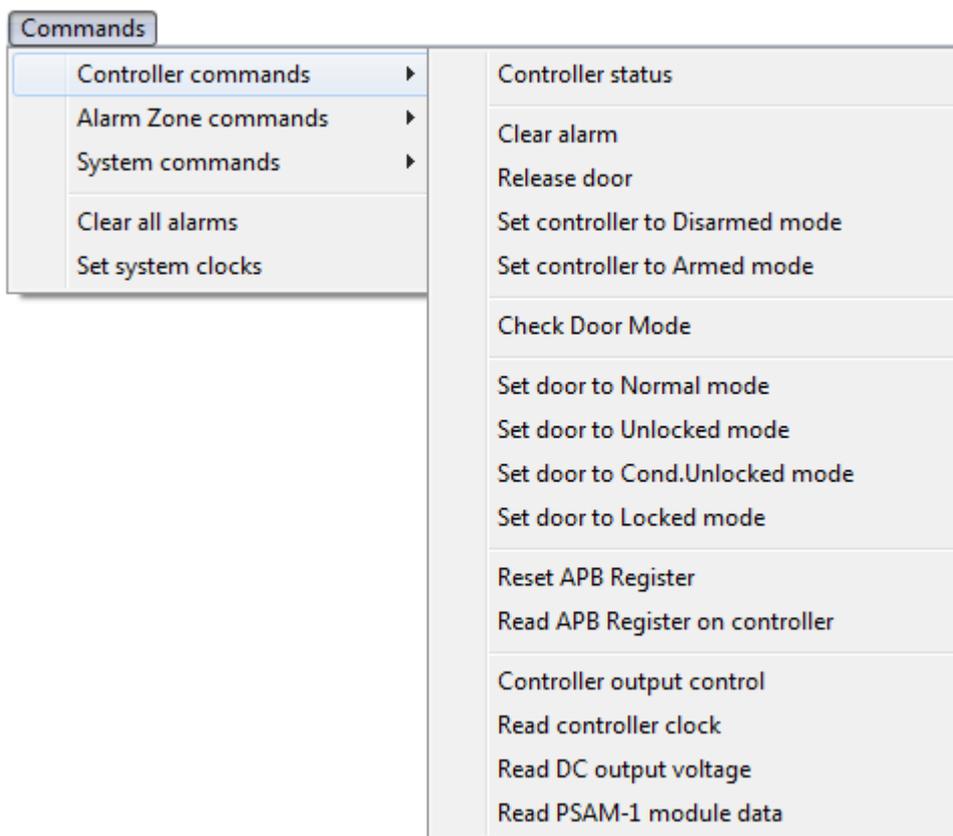


Figure 4.16. Controllers command submenu

Selection of any command from this submenu results in displaying controller selection window (Figure 4.17).

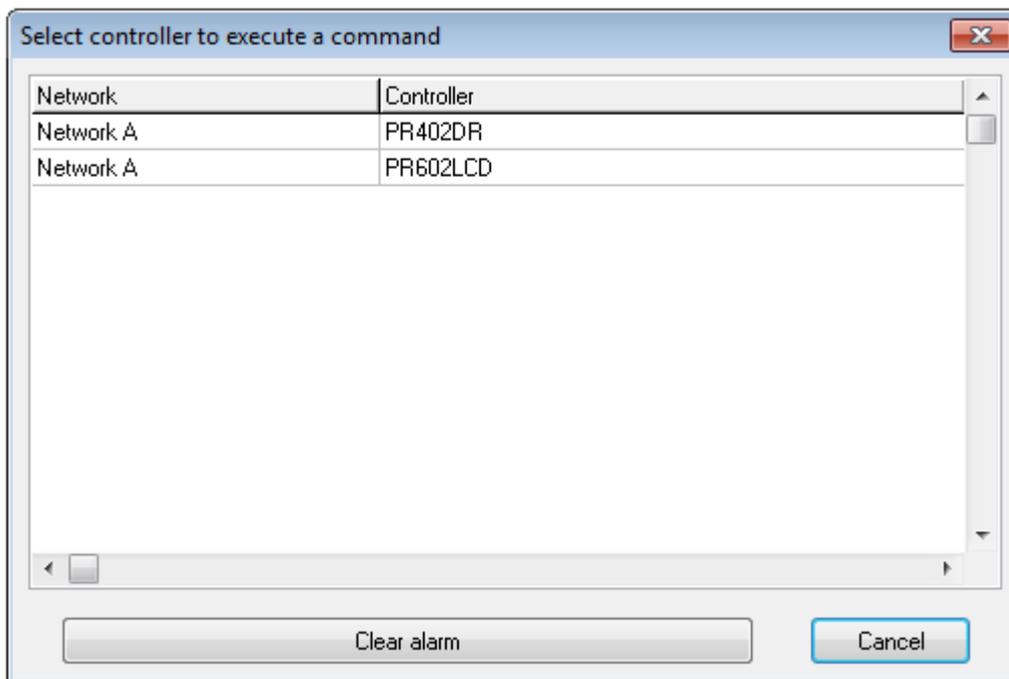


Figure 4.17. Controller selection window

You should select controller in the list, and then click the button with command’s name (in case of Figure 4.17 it is the **Clear alarm** command). If you do not select any controller the command will be executed for the first controller in the list.

4.2.2 Alarm Zone commands

The **Alarm Zone commands** submenu contains a list of commands which can be used for arming or disarming selected Alarm Zone. The submenu is shown in Figure 4.18.

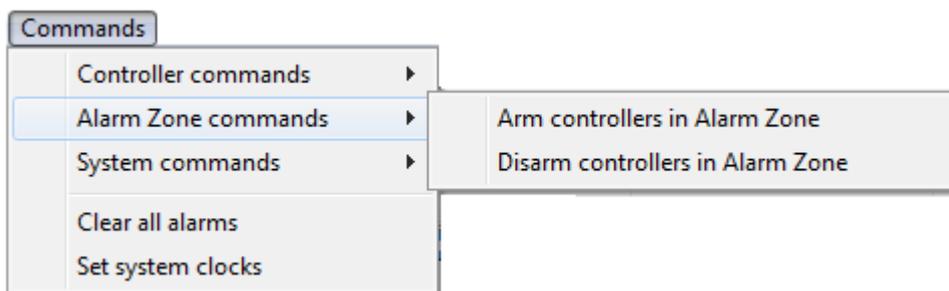


Figure 4.18. Alarm Zone commands submenu

Selection of any command from this submenu results in displaying Alarm Zone selection window (Figure 4.19).

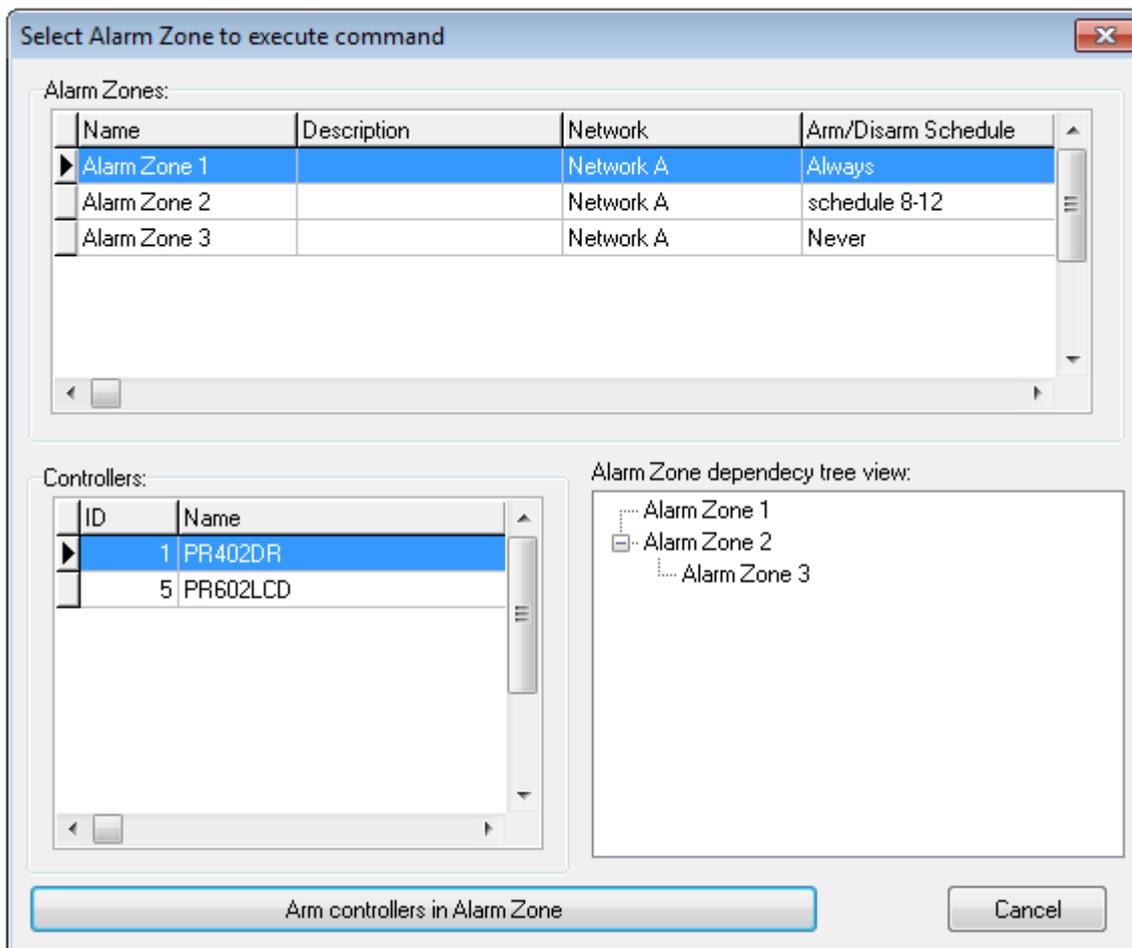


Figure 4.19. Alarm Zone selection window

4.2.3. System commands submenu

The **System commands** submenu contains a list of commands related to the whole system. The submenu is shown in Figure 4.20.

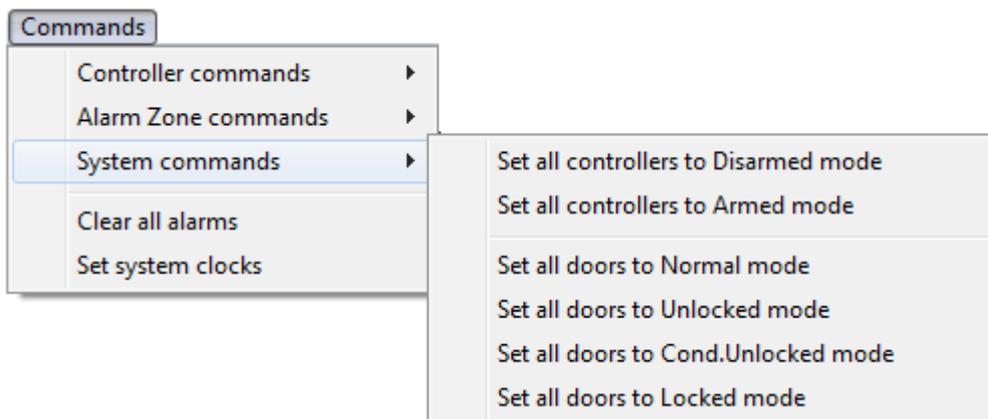


Figure 4.20. The System commands submenu

Command in this submenu concern all controllers in the system. After selection and execution of any command confirmation dialog box is displayed (Figure 4.21).

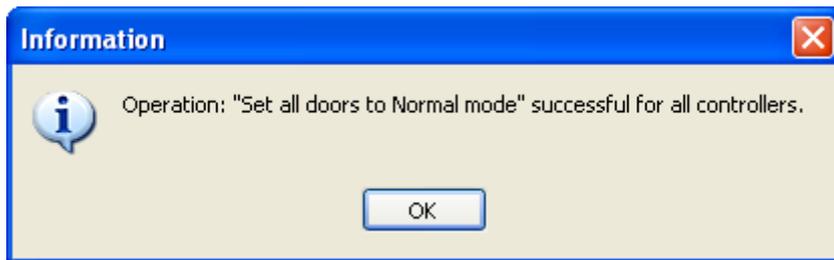


Figure 4.21. Confirmation on executing command on all the controllers in the system.

4.2.4. Clear all alarms

The **Clear all alarms** command cancels all alarms currently raised in the RACS 4. If there is no alarms at the moment, then executing the command will have no effect.

4.2.5. Set system clocks

The **Set system clocks** command allows for setting all RACS 4 devices' clocks in accordance to clock of computer with PR Master software. If you select this command, the system will display a message box with confirmation question (Figure 4.22).

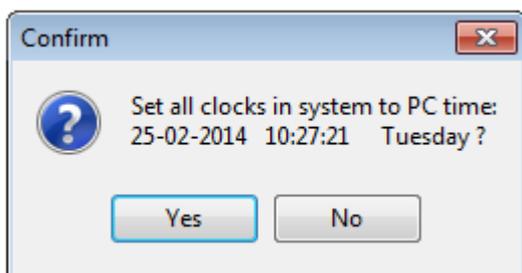


Figure 4.22. Setting clocks in the RACS 4

Answering **Yes** to the question displayed in this window will cause setting clocks of all the devices in the RACS 4 according to computer's system clock.

4.3. TOOLS MENU

The **Tools** menu in PR Master online monitoring mode is shown in Figure 4.23.

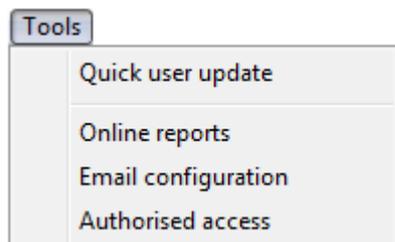


Figure 4.23. Tools Menu

4.3.1. Quick user update

This command is an equivalent to the **Tools/Quick user update** command which is described in [section 3.5.2](#).

4.3.2. Online reports

The **Online reports** command enables instant sending of all or selected events from the RACS 4 to specified devices, files or ports. If you select this command, the **Online reports setting** window is shown (Figure 4.24).

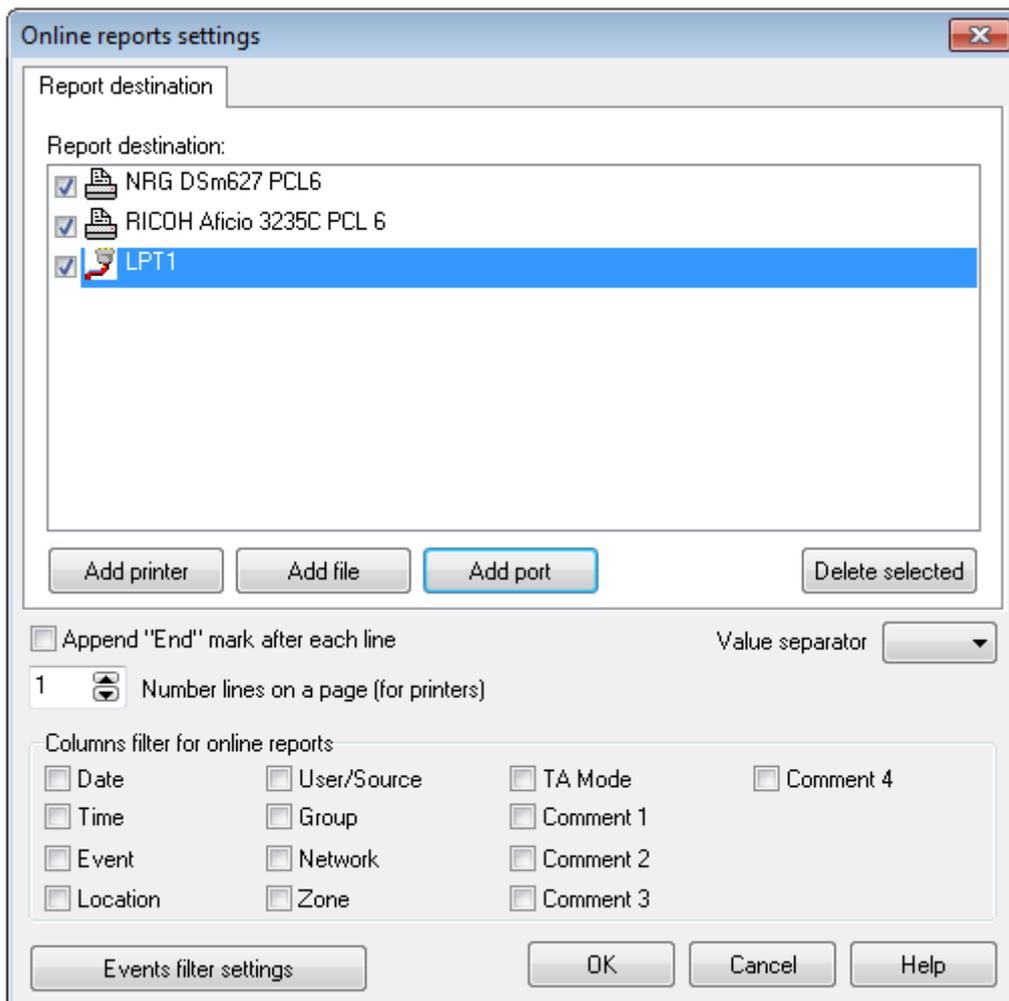


Figure 4.24. Online reports settings

The buttons **Add printer**, **Add file** and **Add port** in the **Report destination** area let you select printers, files and ports where the reports will be generated. The **Delete selected** button allows for deleting particular outputs from the list.

If you select the **Append "End" mark after each line** checkbox, then every event on the online report will be ended with a newline character. The **Number lines on a page (for printers)** lets you set number of rows on page in the hardcopy generated by the printer.

The **Value separator** list box allows to select special symbol which will be used to separate data. It can be comma, semicolon or special character (such as **CR** or **LF**).

Clicking on the **Events filter settings** button causes displaying the **Filter configuration** dialog box where you can define a filter for events being printed.



You can find more information on how filters can be defined in [section 3.3.7.1](#).

4.3.3. Email configuration

Selecting the **Email configuration** command causes displaying the **Email filter** dialog box (Figure 4.25).

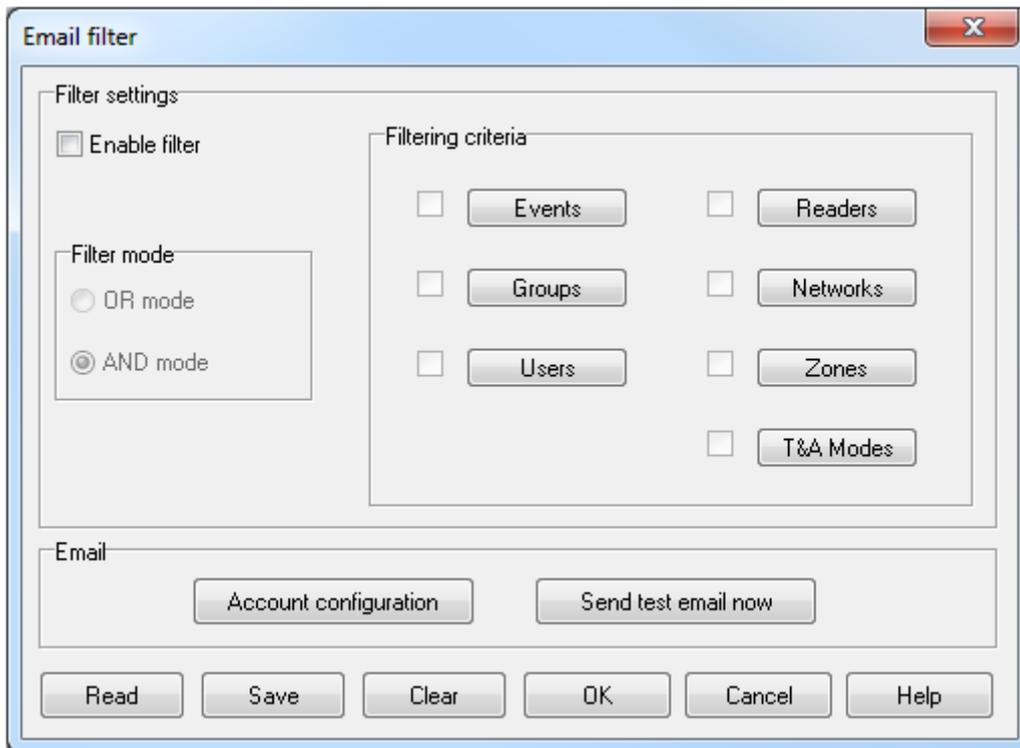


Figure 4.25. *Setting up event report sent by e-mail*

In this window you can specify events which will be sent by e-mail to selected address. In the **Filter settings** area you can select events, which will appear in the report. Before you send report, you should first define a filter (select **Enable filter** check box and define filter conditions in **Filtering criteria** box). You can find more information on how to define filter in **section 3.3.7.1**. More information on how to configure an e-mail account can be found in **section 3.5.11.3**.

4.3.4. Authorised access

The **Authorised access** command enables the operator of PR Master software to grant remotely access to user, who currently has no access rights at particular door. When the command is selected then **Authorised access** dialog box (Figure 4.26) is shown.

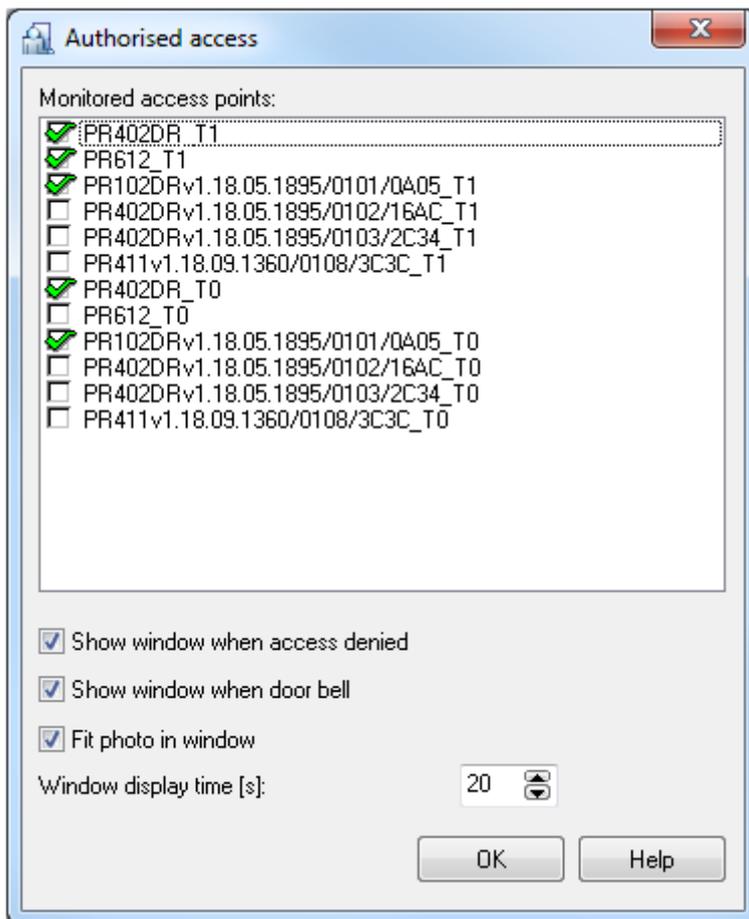


Figure 4.26. *Setting up an authorised access*

In the **Monitored access points** list you can select readers for authorized access. Checking the **Show window when access denied** checkbox will cause that the window **Authorised access** will show up in situation when the system would normally refuse the access. On the other hand, when you select the **Show window when door bell** checkbox, the window **Authorised access** will show up in response to an event of pressing the bell button connected to the controller. If you select the **Fit photo in window** check box, then the photo of user requesting authorised access will show up in the **Authorised access** window. The **Window display time** spin box defines time (in seconds) for which the **Authorised access** window shows up.

If the option **Authorised access** is configured then the system displays **Authorised access** dialog box (Figure 4.27) when the access is denied for the user.

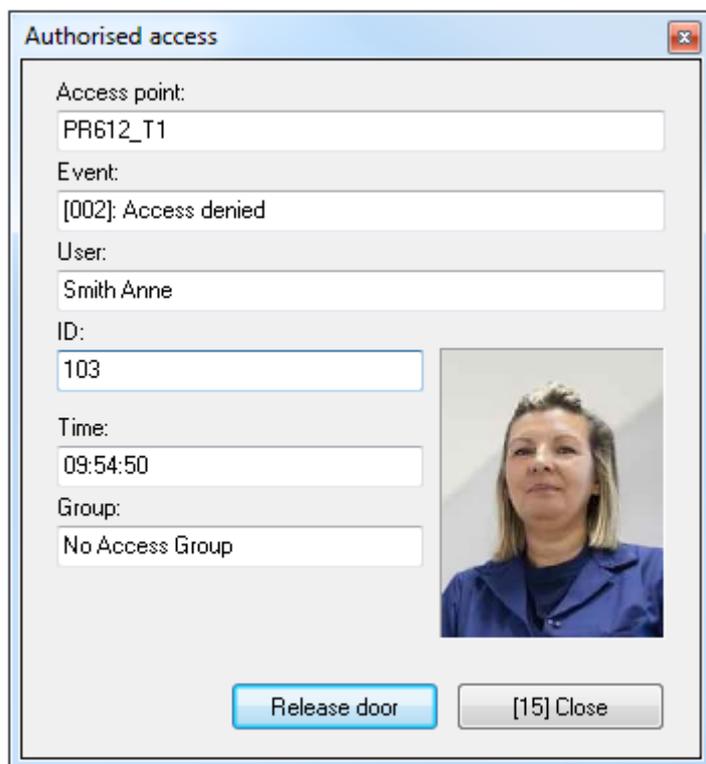


Figure 4.27. *Authorised access command*

In this window you can find information about the access point, the event as well as information on user requesting the access. In square brackets on the **Close** button the number of remaining seconds is displayed. When the time elapses the window is closed automatically. If during this time an operator clicks on the **Release door** button then the controller will open the door.

4.4. HIDE WINDOW

When selected, the **Hide window** command mode minimizes minimizing PR Master monitoring window. To reopen the window you should click on the PR Master icon on the Windows task bar and then enter the password of current operator.

4.5. PLAY CCTV RECORD AND REAL TIME MONITORING BUTTONS

4.5.1. Play CCTV record button

If the integration of RACS 4 with CCTV is configured in accordance with dedicated manual which is available at www.roger.pl, then it is possible to play video clips for selected events by means of **Play CCTV record** button. The button brings dialog box shown in Figure 3.105 and it is also available in Event history (see [section 3.3.7.2](#)). In the dialog box, the user can play video clip, adjust its time and obtain information on clip status. In case of GV600/4 video capture card, the user can also save picture from video frame by right clicking the video clip and selecting adequate options.

4.5.2. Real-time monitoring button

If the integration of RACS 4 with CCTV is configured in accordance with [section 3.2.14](#) then it is possible to watch real time video from cameras connected to DVR by means of **Real-time monitoring** button. The button brings dialog box shown in Figure 4.28.

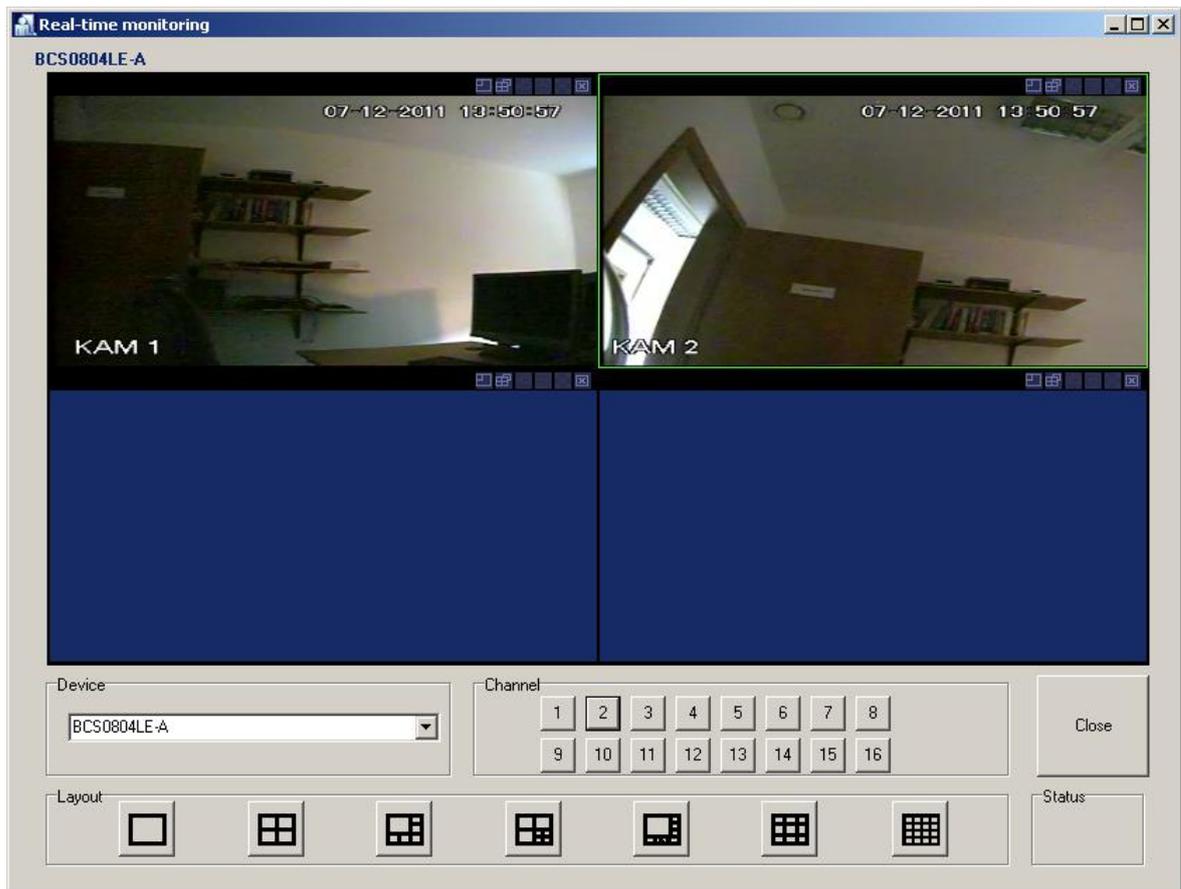


Figure 4.28. Real-time monitoring

CHAPTER 5.

REMOTE MONITOR SOFTWARE

Remote Monitor software after installation and then connection with PR Master software installed on different computer/server enables to control RACS 4 system in many ways. Therefore Remote Monitor offers the possibility to operate RACS 4 system from multiple workstations with some functional limitations. In order to establish and maintain communication between Remote Monitor and PR Master, the latter one must be started in online monitoring mode.

Remote Monitor installation file is located in PR Master software (by default **C:\Roger\Access Control System 4.5\RemoteMonitorInstall**). After selection of **setup 4.5.12.xxxx** file initial installation window is displayed (Figure 5.1). Further installation steps are similar to PR Master software (see **section 1.1**).



Starting from the version 4.5.20.xxxx, Remote Monitor software is no longer developed by Roger and is offered as is.

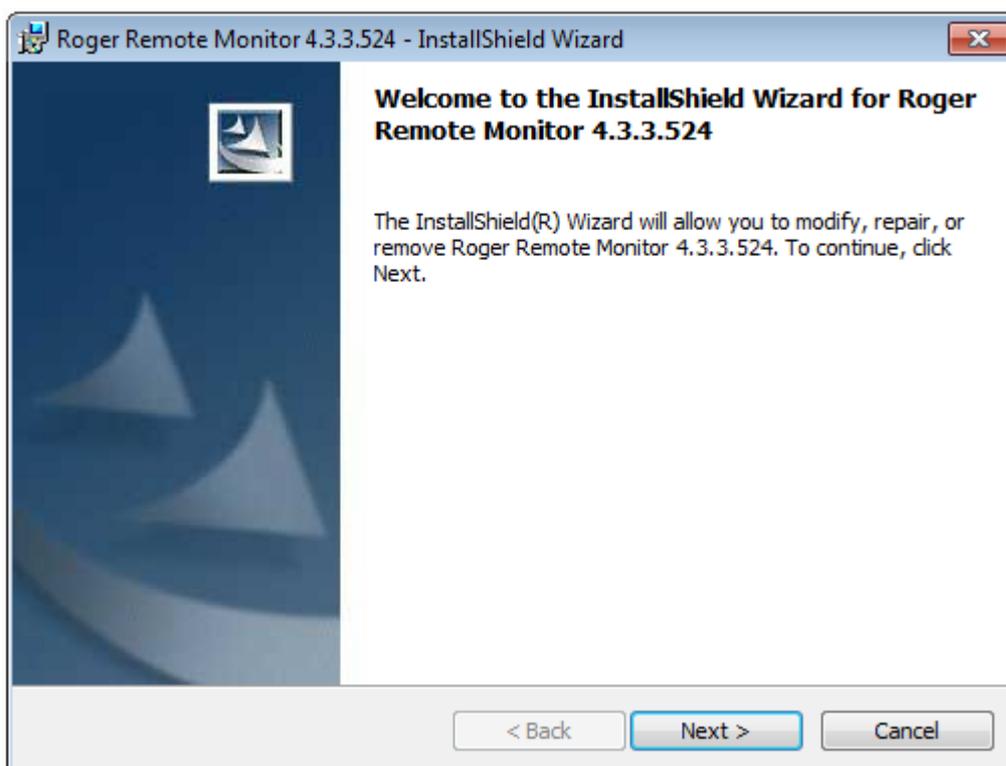


Figure 5.1. Installation screen

5.1. STARTING THE SOFTWARE

Prior to starting Remote Monitor software it is necessary to open config.ini file in PR Master folder (default path: **C:\Roger\Access Control System 4.5** and then to enter IP address of the computer with installed PR Master software. The example with 192.168.10.24 address is shown in figure 5.2.a.

When you start Remote Monitor for the first time after the installation, the language selector windows is displayed. Then it is necessary to connect with PR Master software (Figure 5.2b) selecting IP address of computer with PR Master from the list or entering IP address and port

manually. Default port for communication is 64181. Basically, Remote Monitor was designed for local area network (LAN) but it is possible to use it in wide area network (WAN).

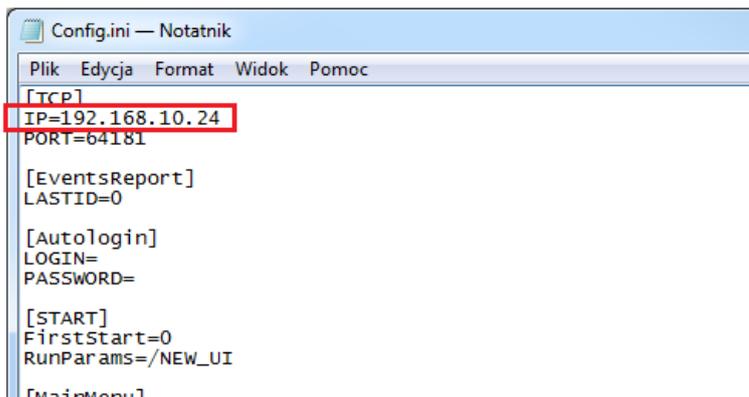


Figure 5.2a. Config.ini file of PR Master software

After establishing the connection, PR Master login window is displayed (Figure 5.2b). Enter PR Master operator’s login and password (see [section 3.5.8](#)). In case of default settings the login is ADMIN and there is no password. It is recommended to define passwords for PR Master operators.

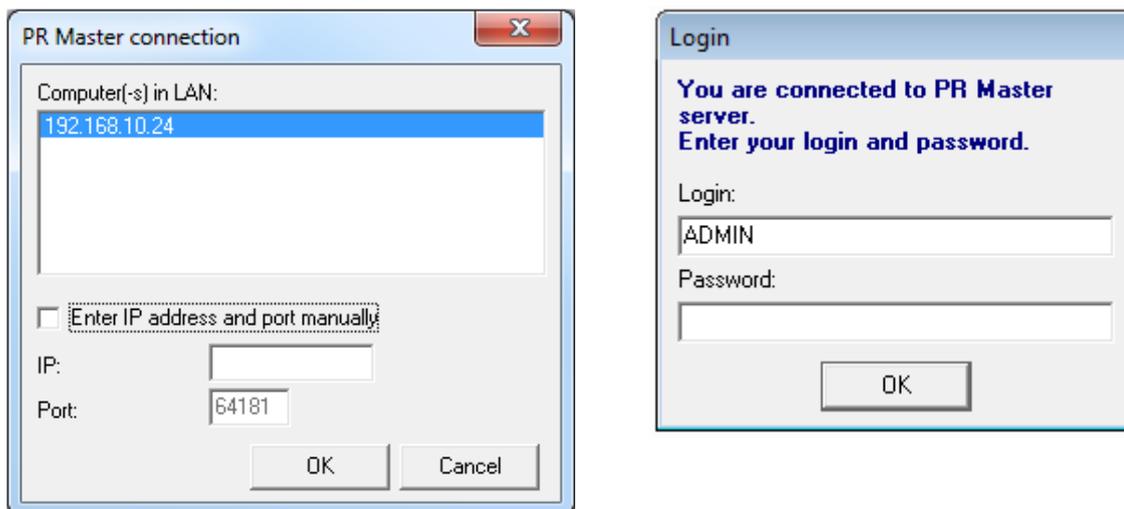


Figure 5.2b. Connection and login windows

After successful connection and login, the main Remote Monitor window is displayed (Figure 5.3) which is based on PR Master window in online monitoring mode (see [chapter 4](#)). It enables among others displaying current events from RACS 4 system.

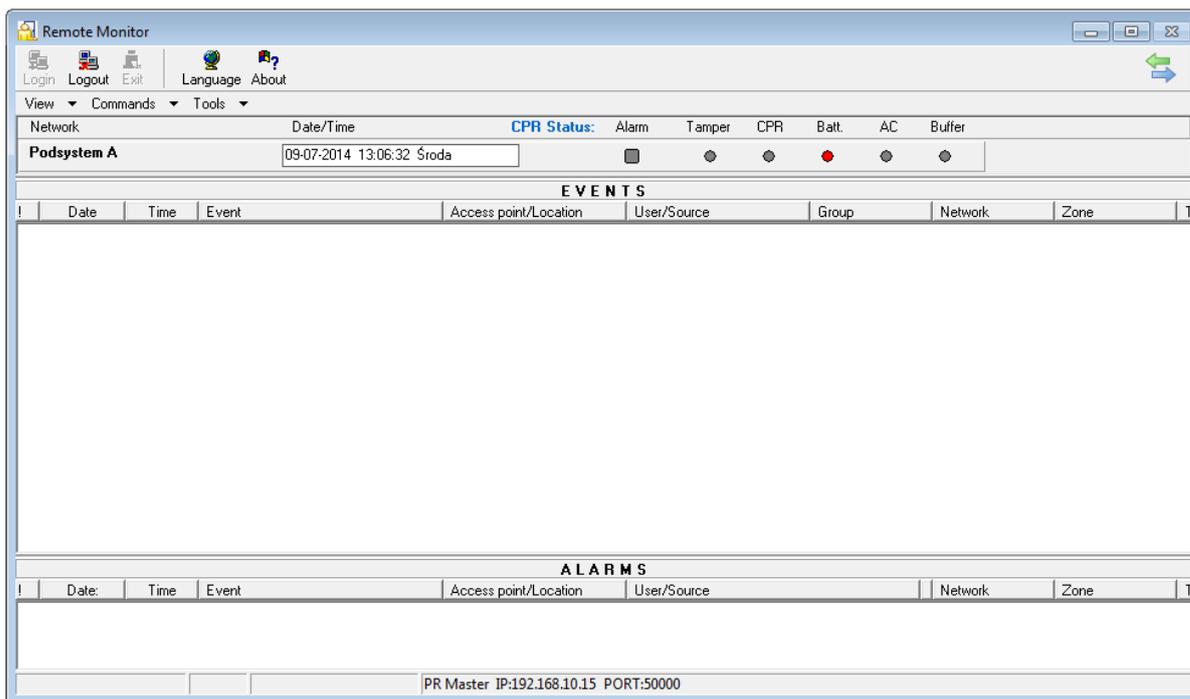


Figure 5.3. Remote Monitor main window

5.2. VIEW MENU

The **View** menu is shown in Figure 5.4.

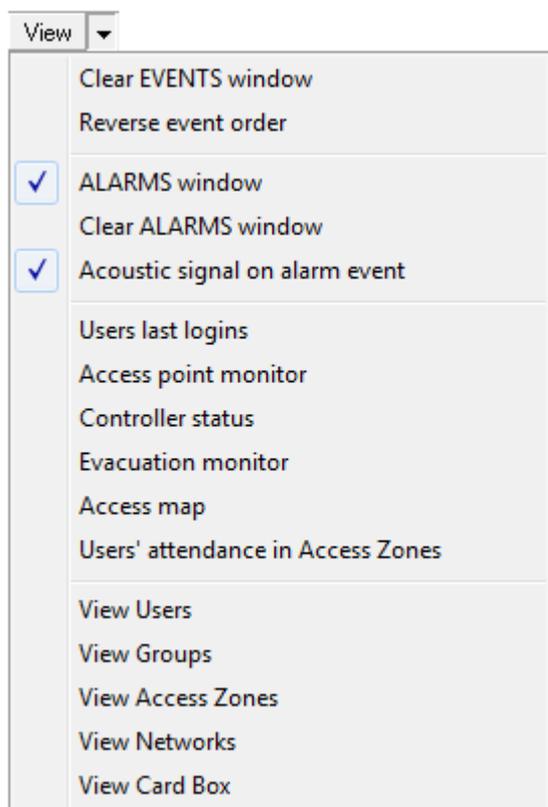


Figure 5.4. View menu in Remote Monitor

The **View** menu includes commands and tools which are also available in PR Master software in online monitoring mode. They are already explained in the present document (see [section 4.1](#)).

Additionally, using such commands as **View Users, View Groups, View Access Zones, View Networks and View Card Box** it is possible to read and view relevant data from PR Master.

5.3. COMMANDS MENU

The **Commands** menu is shown in Figure 5.5.

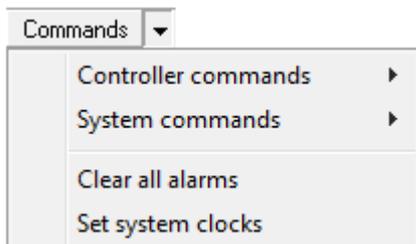


Figure 5.5. *Commands menu in Remote Monitor*

The **Commands** menu includes commands which are also available in PR Master software in online monitoring mode. They are already explained in the present document (see [section 4.2](#)).

5.4. TOOLS MENU

The **Tools** menu is shown in Figure 5.6.

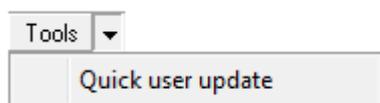


Figure 5.6. *Tools menu in Remote Monitor*

The **Tools** menu includes command for Quick user update in RACS 4. Users are added and edited in similar way as in PR Master software (see [section 3.2.3](#) and [section 3.5.2](#)). The window for quick user update in Remote Monitor software is shown in Figure 5.7. The software can operate only with RUD-2 and RUD-3 readers which can be connected to computer’s USB port. Card number can be enrolled when the reader is connected and the button **Read card** is selected. Alternatively cards can be also assigned using Card box.

User properties

User valid

Type: **NORMAL**

Fit to area

First Name:

Last Name:

Group:

T&A ID:

Card:

PIN:

Access period

Start date:

End date:

Custom 1:

Custom 2:

Custom 3:

Custom 4:

Photo (110x144)

Figure 5.7. Add user in Remote Monitor

Contact:
Roger sp. z o.o. sp.k.
82-400 Sztum
Gościszewo 59
Tel.: +48 55 272 0132
Fax: +48 55 272 0133
Tech. support: +48 55 267 0126
E-mail: support@roger.pl
Web: www.roger.pl