



# **PR MASTER USERS MANUAL**

Version 4.3

Rev. A

# CONTENT

Content .....	2
I. Introduction .....	4
Chapter 1. Preparing system to work.....	5
1.1. PR Master Installation .....	5
1.1.1. Roger ACS 4.3 Application Group Content.....	9
1.2. Running the Program for the first time .....	10
1.3. Quick Start .....	13
Chapter 2. The System in Production.....	15
2.1. Initial operations.....	15
2.1.1. Defining password for the ADMIN user .....	15
2.1.3. Defining the program operators .....	15
2.1.3. Defining INSTALLER user .....	16
2.1.4. Planning a backup schedule.....	16
2.1.5. Planning a system configuration update schedule .....	16
2.1.6. Planning a reading event buffers schedule.....	16
2.2. Advanced maintenance operations .....	17
2.2.1. Setting up the Anti-passback mechanism.....	17
2.2.2. Defining Attendance Areas .....	17
2.2.3. Defining Alarm Zones.....	17
2.2.4. Defining Facility plans .....	17
2.3. Day to day system operation .....	18
2.3.1. User management.....	18
2.3.2. Making System Backups .....	18
2.3.3. System monitoring .....	19
Chapter 3. PR Master functionality .....	20
3.1. File Menu.....	20
3.1.1. New system... Command.....	20
3.1.2. Import system settings from file .....	21
3.1.3. Export system settings to file .....	23
3.1.4. Exit.....	25
3.2. System menu.....	25
3.2.1. Installer.....	25
3.2.2. Holidays .....	26
3.2.3. Users .....	27
3.2.4. Groups .....	35
3.2.5. Schedules.....	41
3.2.6. Access Zones.....	47
3.2.7. Networks.....	52
3.2.8. Attendance Areas.....	68
3.2.9. APB Zones.....	71
3.2.10. Alarm Zones .....	73
3.2.11. Fingerprint Readers.....	76
3.2.12. Card Box .....	80
3.2.13. Facility plans.....	84
3.3. Reports menu .....	92
3.3.1. Groups .....	92
3.3.2. Users .....	92
3.3.3. Access Zones.....	92
3.3.4. Networks.....	92
3.3.5. Controllers.....	93
3.3.6. Access rights .....	93
3.3.7. Events history .....	93
3.3.8. Attendance .....	101
3.4. Commands menu .....	107

3.4.1. Read event buffers now .....	107
3.4.2. Read event buffers later .....	108
3.4.3. Clear event buffers now .....	108
3.4.4. Update system now .....	108
3.4.5. Update system later .....	109
3.4.6. Set system clocks.....	110
3.5. Tools Menu.....	111
3.5.1. Online monitoring .....	111
3.5.2. Quick user update.....	112
3.5.3. Access map .....	114
3.5.4. Users attendance within Access Zones .....	114
3.5.5. T&A modes.....	115
3.5.6. Inputs .....	117
3.5.7. Alarm Events .....	119
3.5.8. Program operators .....	120
3.5.9. Change Password .....	122
3.5.10. Lock program .....	123
3.5.11. Options .....	123
3.5.12. Backup configuration.....	130
Chapter 4. Online monitoring .....	133
4.1. View menu .....	133
4.1.1. Clear Events Window .....	134
4.1.2. Events Window Columns .....	134
4.1.3. Reverse event order .....	135
4.1.4. Alarm Window .....	135
4.1.5. Clear Alarm Window.....	135
4.1.6. Alarm Window Columns.....	135
4.1.7. Acoustic signal on alarm event.....	135
4.1.8. Monitoring window filter .....	135
4.1.9. Alerts .....	136
4.1.10. Users last logins.....	137
4.1.11. Access Point Monitor .....	138
4.1.12. Controller status.....	139
4.1.13. View map .....	140
4.1.14. Access map .....	142
4.1.15. Users' attendance in Access Zones .....	142
4.1.16. Connected Remote Monitors .....	142
4.1.17. Exit .....	143
4.2. Commands menu .....	144
4.2.1. Controllers command submenu .....	144
4.2.2. System submenu .....	145
4.2.3. Clear all alarms .....	146
4.2.4. Set system clocks.....	146
4.3. Tools Menu.....	146
4.3.1. Quick user update.....	146
4.3.2. Online reports.....	147
4.3.3. Email configuration .....	147
4.3.4. Authorised access .....	148
4.2. Hide window .....	150

# I. INTRODUCTION

PR Master 4.3 is the final version of RACS (**Roger Access Control System**) management software. RACS is an Access Control System based on CPR-32 network management units and PRxx controllers manufactured by Roger.

PR Master 4.3 is an application of Microsoft Windows 98, Windows NT, Windows 2000, Windows XP Windows Vista, and Windows 7 operating systems.

The program has two types of users:

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

This division is in keeping with Access Control Systems' 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 from then on is responsible for its day-to-day maintenance.

The PR Master 4.3 application should be installed by the installer — representative of the company deploying the ACS after physical installation of all the system components (controllers, network management units, 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 production. From then on, end users will utilize the application on day-to-day basis.

The purpose of this manual is to present all the functionalities of PR Master 4.3 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. Then the best to do is 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 update the PR Master from older into newer version. In such a case it is necessary to take all the steps needed for preserving data from previous version.

The Manual has been divided into 4 chapters.

In Chapter 1. "Preparing System to Work" an installation process and its initial set up have been described.

In Chapter 2 „Day to Day Maintenance“ a typical tasks performed on daily basis have been 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" a synthetic summary of all the program's menu and commands has been presented. The chapter describes all the menus, dialog boxes and alternative ways of invoking different functions.

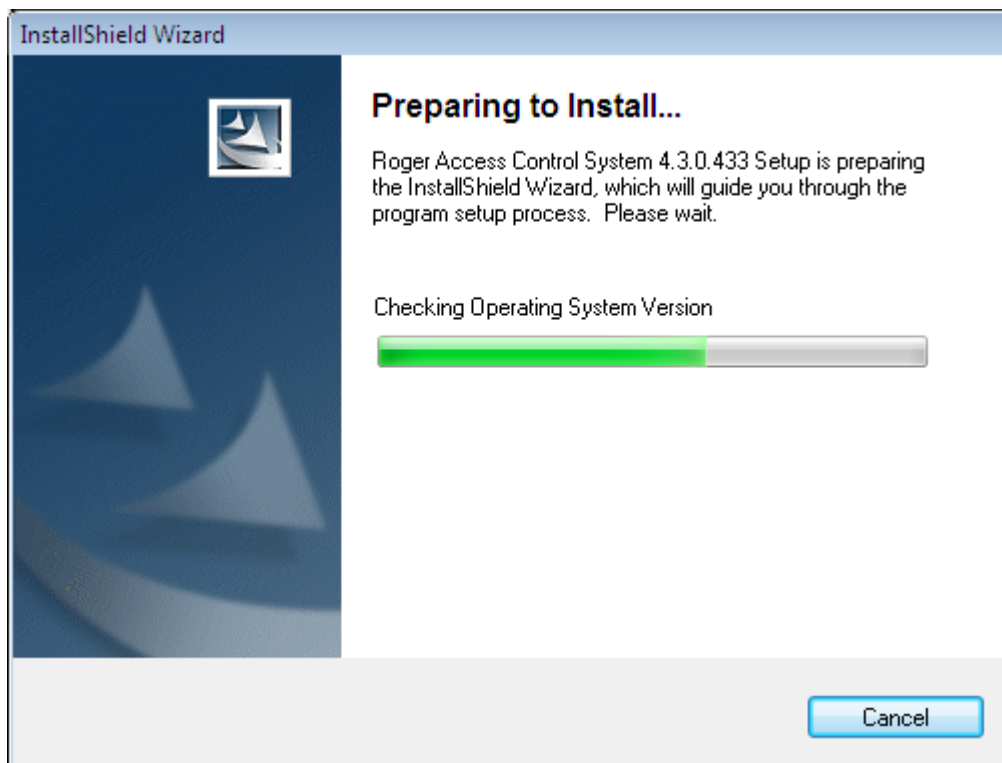
In Chapter 4 „Monitoring“, a monitoring mode of PR Master has been described.

# CHAPTER 1.

## PREPARING SYSTEM TO WORK

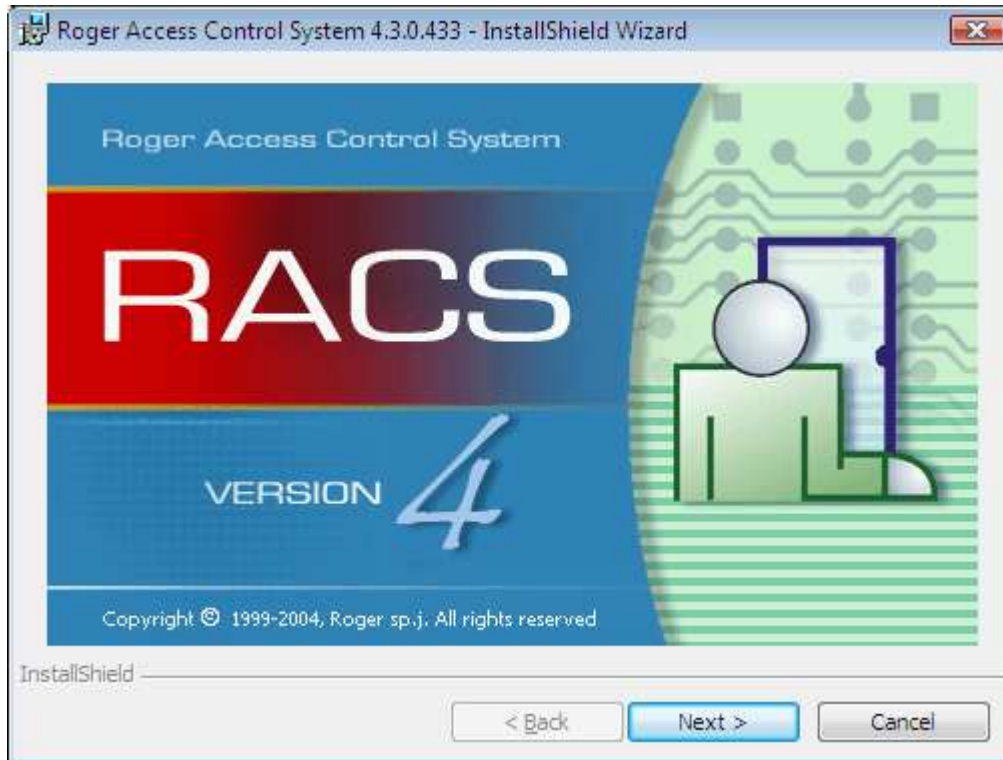
### 1.1. PR MASTER INSTALLATION

In order to set up the 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 **setup 4.3.x.xxx.exe**. After the file has been downloaded it should be executed, which results in displaying an initial installation screen (Figure 1.1).



**Figure 1.1.** *Preparing to install*

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

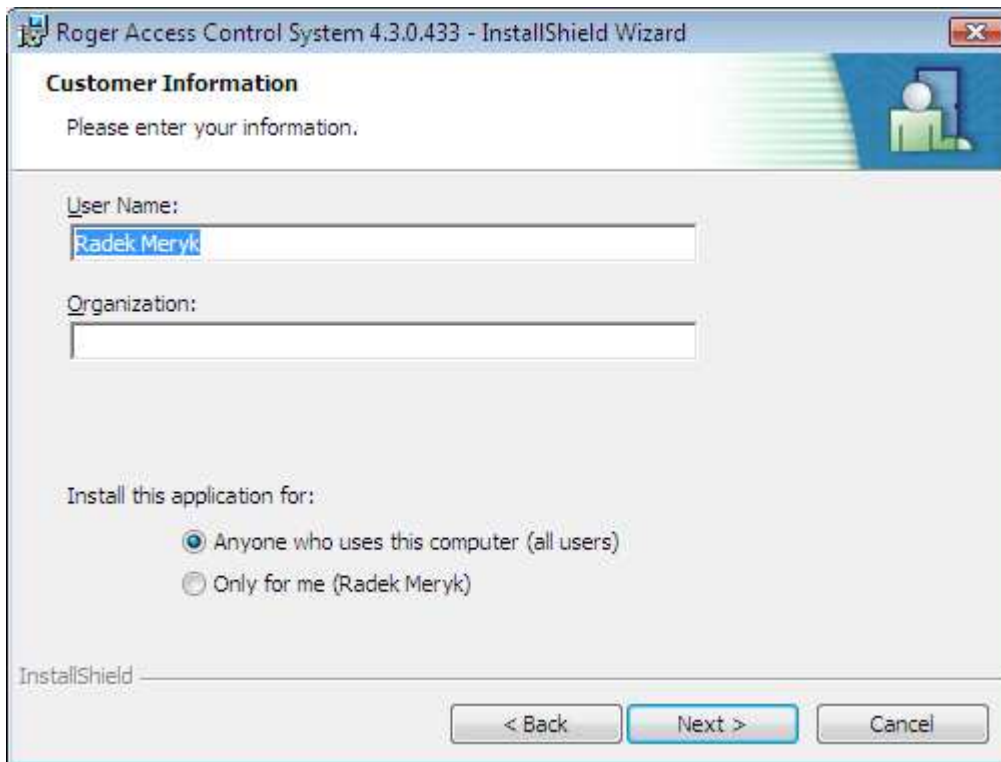


**Figure 1.2.** RACS installation wizard — step 1

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**.

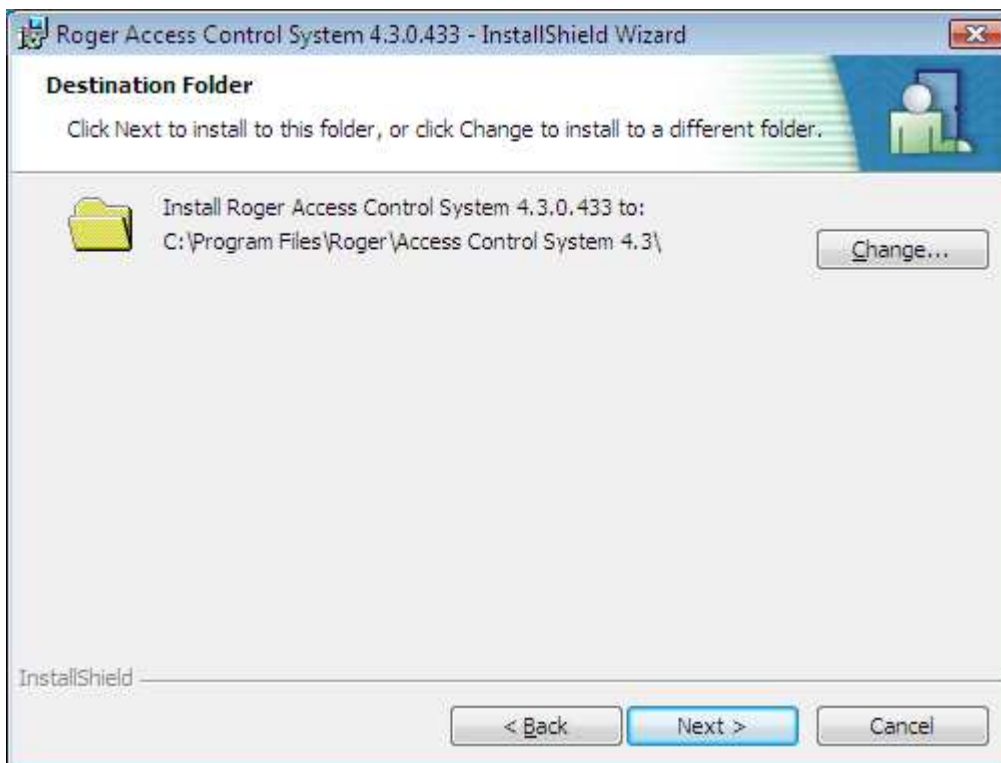
The next wizard's window is a screen containing license agreement. You should read it carefully, and place a check next to the **I accept the terms in the license agreement** option. If you don't select this option, the **Next** button will be disabled, and you will be unable to continue the installation. 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 there 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 the computer's users (**Anyone who uses this computer (all users)**).



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

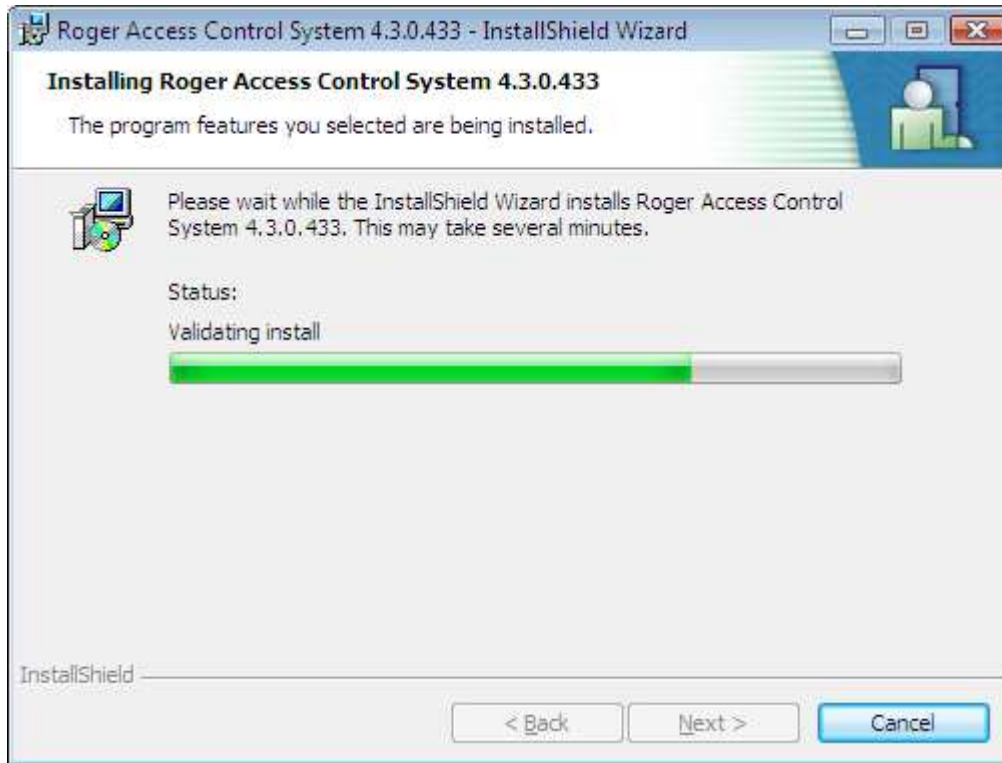
Upon entering this data, you should click **Next**. The destination folder selection window displays (Figure 1.4).



**Figure 1.4.** RACS installation wizard — destination folder selection

By default, the PR Master 4.3 application installs in the **C:\Program Files\Roger\Access Control System 4.3** 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 installation wizard — copying files and validating install

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



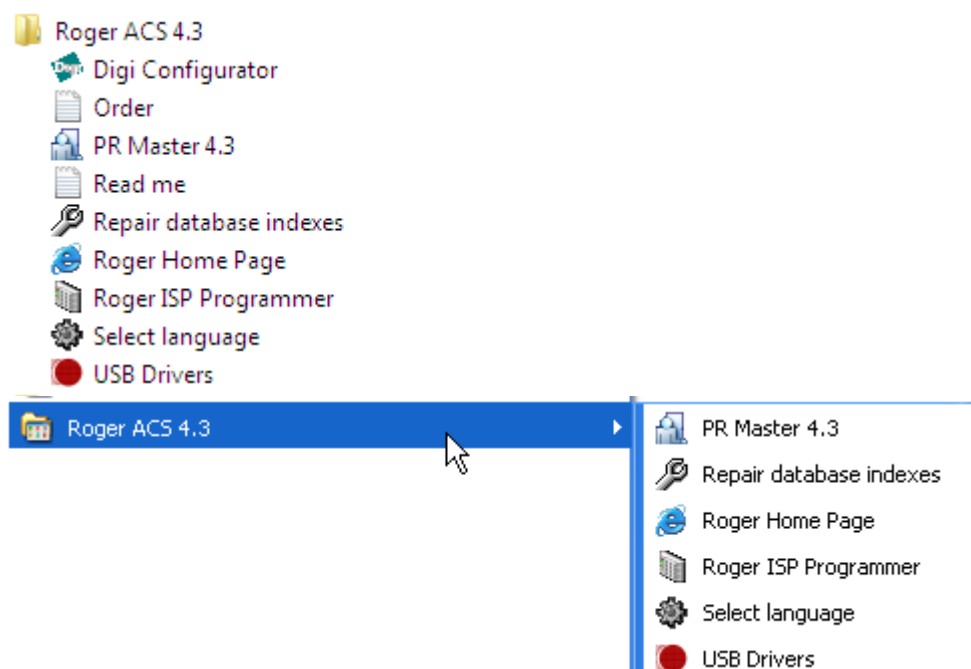


**Figure 1.6.** RACS installation wizard — the application has been successfully installed

If you click **Finish**, the system will display information that it is necessary to restart computer. Only after restart the installation will take effect. The installation is finished. Before you run the program for the first time, you should restart computer.

### 1.1.1. Roger ACS 4.3 Application Group Content

When you install the PR Master 4.3 application, the **Roger ACS 4.3** application group will be created. Its content has been shown in figure 1.7.



**Figure 1.7.** *The Roger ACS 4.3 Application Group Content*

The **Roger ACS 4.3** application group contains the following elements:

- ◆ **PR Master 4.3** — link to PR Master 4.3 application executable.
- ◆ **Repair database indexes** — a tool for repairing database's indexes.
- ◆ **Roger Home Page** — link to Roger website.
- ◆ **Roger ISP Programmer** — a tool for updating controllers firmware.
- ◆ **USB Drivers** — a tool for installing USB drivers.

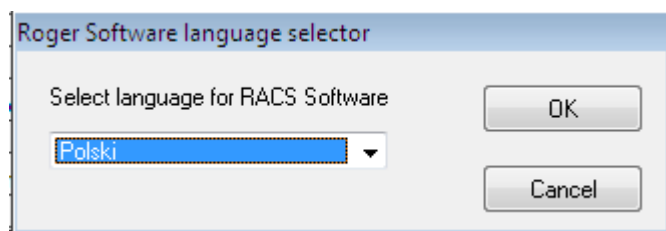


If the PR Master application was previously used in the computer where you install the system, then before running the setup program but after application uninstall, the best thing is to manually erase the folder where the application was installed. Most often the path to this folder is **C:\Program Files\Roger\Access Control System 4.3**.

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

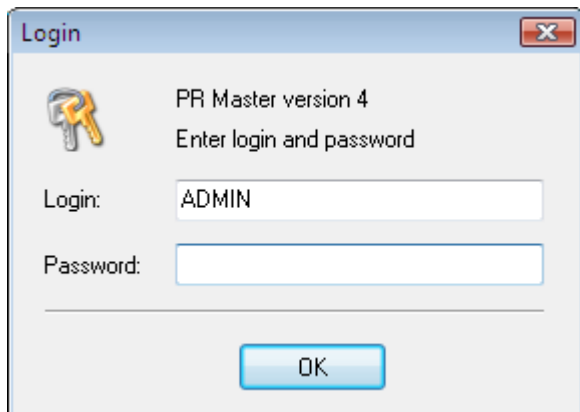
## 1.2. RUNNING THE PROGRAM FOR THE FIRST TIME

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



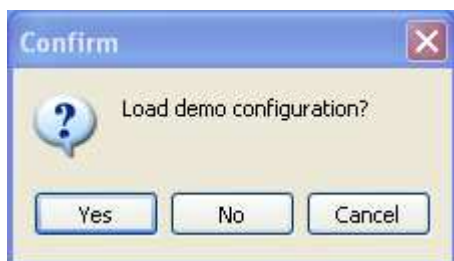
**Figure 1.8.** *Language selection for the PR Master 4.3*

In this dialog box you should select the user interface's 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, the language has been changed for. In this window you should click **OK** once again. Only then an initial PR Master logon screen appears (Figure 1.9).



**Figure 1.9.** PR Master 4.3 logon screen

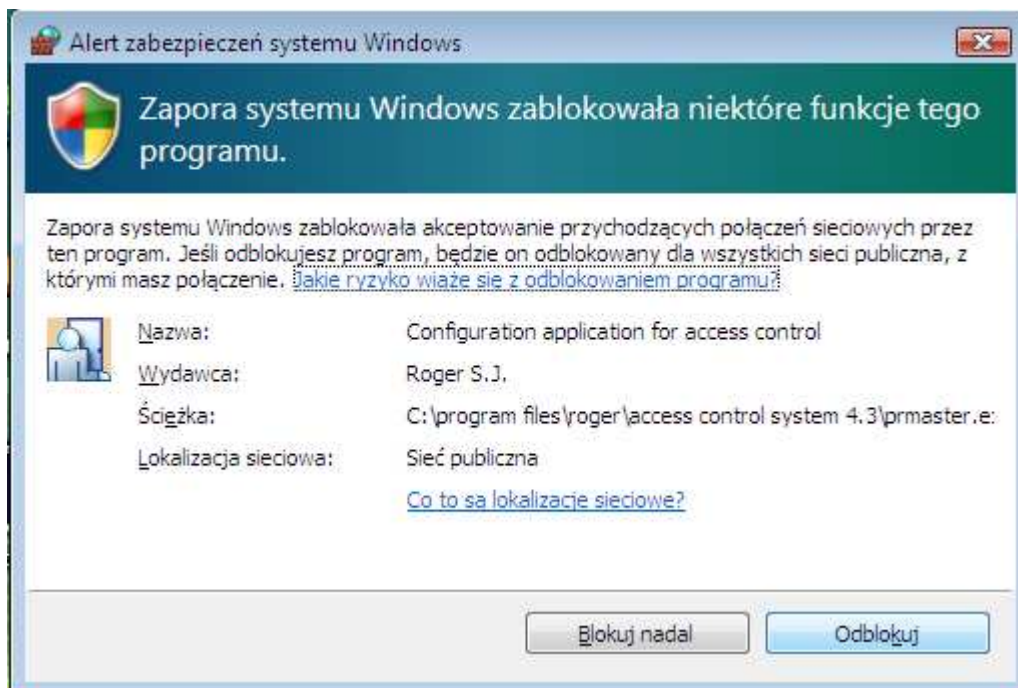
Default password for the ADMIN user is empty. So, you should click **OK**. The program will ask you if sample configuration should be loaded (Figure 1.10).



**Figure 1.10.** The program asks if the demo configuration should be loaded

If you want to familiarize with the program functionalities, you should click **Yes**. If you want to configure application for managing physically installed access control system, you should click **No**.

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.

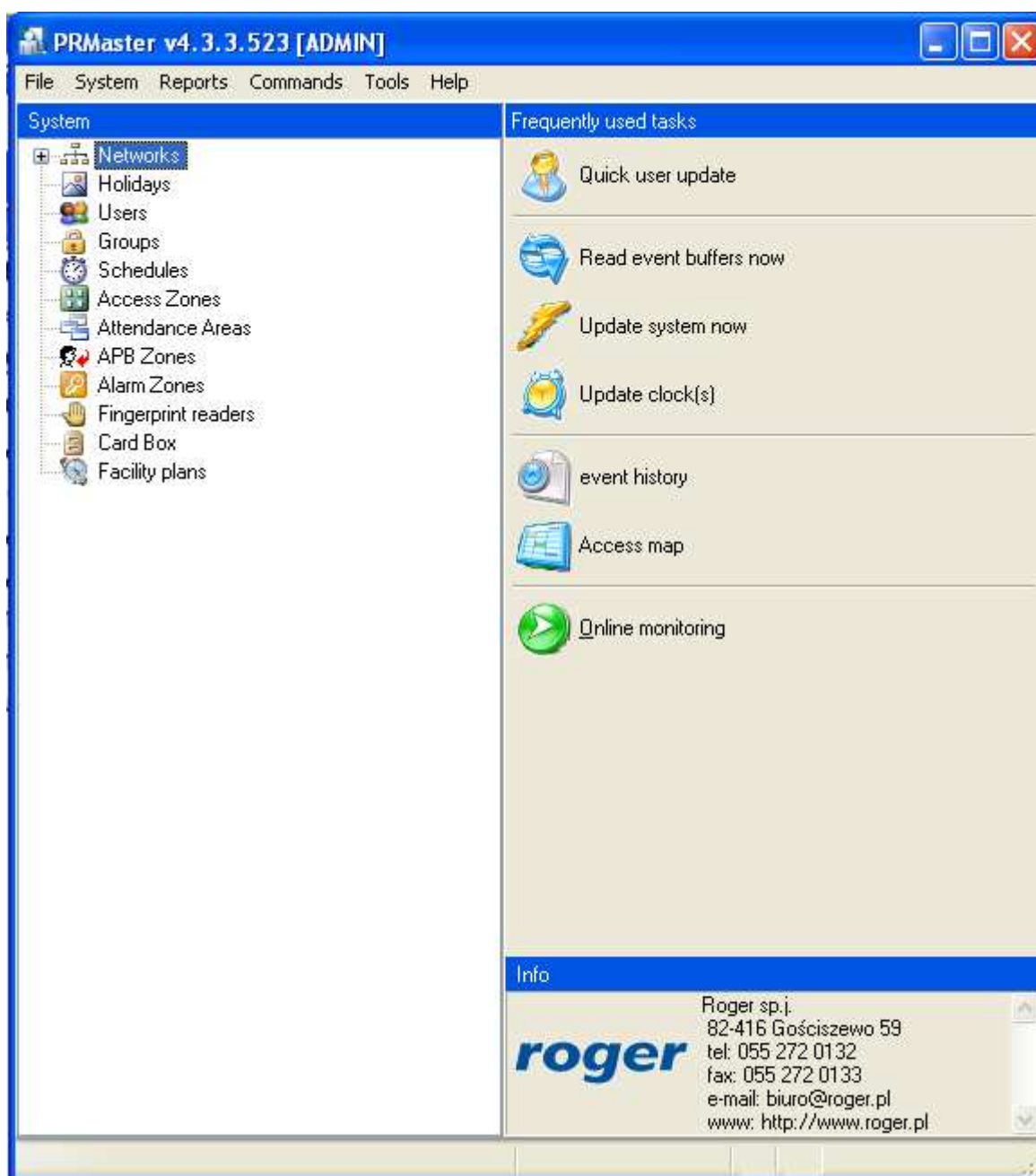


**Figure 1.11.** Windows firewall informs that network connections to the PR Master 4.3 application are blocked

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. QUICK START

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



**Figure 1.12.** PR Master 4.3 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 3.2.7](#)).
3. Add a new network (see [section 3.2.7.1](#)). 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 3.2.7.4](#)). 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.
5. Repeat steps 1–4 for the remaining networks in the Access Control System.
6. When all the networks have been configured, you can define access zones. The installer should do this in cooperation with the end user. A detailed description on how access zones should be defined can be found in [section 3.2.6](#).
7. After defining access zones, define time schedules for use in the system. You can find more information on this subject in [section 3.2.5](#). 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 3.2.4](#). Read carefully about how in the RACS 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, 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 [w punkcie 3.2.12](#). You can read about user management in [w punkcie 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 PRODUCTION

So the RACS has been put into production! In order to be able to use it properly, you should perform a few tasks. Firstly, they will assure a safe work for the system, and secondly they allow for using its possibilities to the maximum. All these tasks will be described in this chapter.

### 2.1. INITIAL OPERATIONS

After the system has been put into production, its administrator has to conduct several preparatory operations. They have been described in the following sections.

#### 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 was protected by safe 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 desirable that the password be difficult to guess. 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).

#### 2.1.3. Defining program operators

In a robust ACS, maintenance tasks can be divided between several persons. In particular, you can designate a person responsible for adding users to the database and the other person responsible for doing backups. In order that those persons have no full rights in the ACS so that they'll be unable to damage system's configuration, you can define separate accounts for them. You can find more information on how to define limited accounts in [section 3.5.8](#).

### 2.1.3. Defining INSTALLER user

In PR301 and PR201 controllers the INSTALLER user has rights to enter the programming mode of controllers 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 utilize the [System/Installer](#) command. You can find more information on this subject in [section 3.2.1](#).

### 2.1.4. Planning a 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 quite often. 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](#).

### 2.1.5. Planning a system configuration update schedule

The RACS consists of two parts: the one controlling passages (controllers, network units and connections) and the other responsible for system management (the PR Master software). They are components which have to have settings in compliance with one another. Only then they can cooperate smoothly. Because on one hand technical devices can be subject to crashes, disturbances or third parties interferences, and on the other hand, the settings can be modified in the program, you should make sure that from time to time, the system was synchronized automatically. Such synchronization relies on sending to the system all the settings entered in the PR Master. When the system is large, updating configuration data can take long time. Because of that, you can configure the schedule, so that the system will automatically do this when the system is less busy. You can find a detailed description on defining such a schedule in [section 3.4.5](#).

### 2.1.6. Planning a reading event buffers schedule

In the RACS, events are collected all the time, no matter whether the PR Master application is running or not and no matter of the mode it is working in. If the PR Master does not run in a monitoring mode, events are gathered in controllers' buffers, and if the system is equipped with a CPR-32 network unit, also in CPR-32's buffer. Reading event buffers is done on request and whenever the application is switched into monitoring mode. In order to prevent serious discrepancies between database content and events registered in the ACS, you can configure schedule for reading event buffers periodically. In order to do this, you need to use the [Commands/Read event buffers later](#). This command has been 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 passages 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 in [section 3.2.9](#).

### 2.2.2. Defining Attendance Areas

**Attendance areas** is one of the RACS'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 to through a set of identification points, and you can leave by a separate set of 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. 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 3.2.8](#).

### 2.2.3. Defining Alarm Zones

**Alarm zones** make possible to designate a group of controllers, which will be armed/disarmed according to the schedule selected. It is also possible to define an alarm zones hierarchy. Thanks to this the controllers will be armed/disarmed in compliance with the hierarchy levels (parent-child).

You can find more information on defining alarm zones in the PR Master in [section 3.2.10](#).

### 2.2.4. Defining Facility plans

**Facility plans** is a tool designed for visually monitoring the object being controlled. Using this functionality, the user can place icons on the object's plan and then to watch them in graphic mode. 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 3.2.13](#).

## 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, is becoming a stable system, where only some kind of activities are being performed. There is much less operation in this state when compared to deployment phase, when so many elements require configuration. Day to day operations in PR Master include:

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

These activities will be described in the following sections.

### 2.3.1. User management

Users management is performed from the users directory. It 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 utilize the **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).

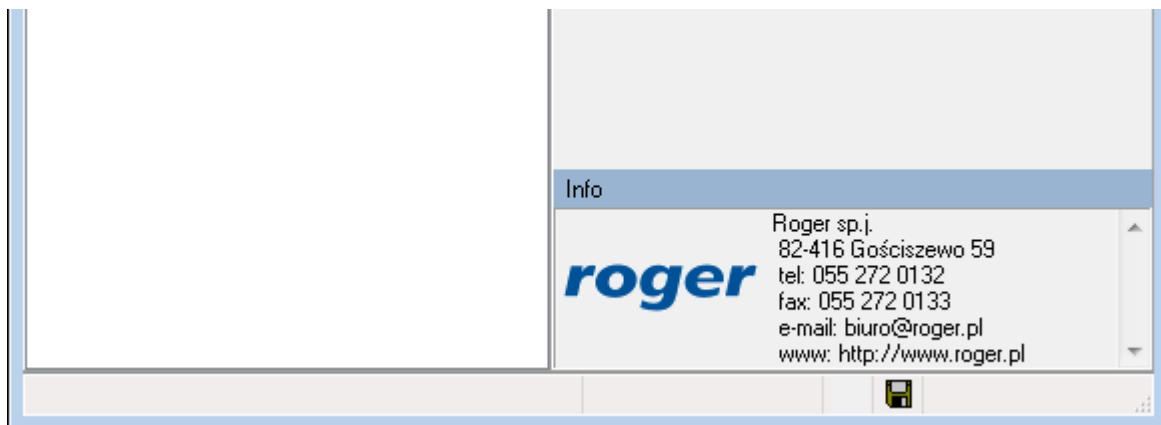
The main difference between using user dictionary invoked from the **System** menu, and **Quick user update** command lies in the way information is sent to controllers. Every change of user properties — i.e. change in assignment to groups, replace of proximity card, change the PIN code, requires sending 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, which allows for sending to controllers the modified user properties only.

Operations available in the users directory have been described in [section 3.2.3](#), and the **Quick user update** command has been described in [section 4.3.1](#).

### 2.3.2. Making System Backups

The PR Master 4.3 database contains a lot of data. Possible loss of it and configuring the system from scratch, especially when the ACS system is large, can take lots of time. Thus, you want to make sure, that the system's backups are made often.

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 you would want to make a fresh system's backup.



**Figure 2.1.** The floppy diskette 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

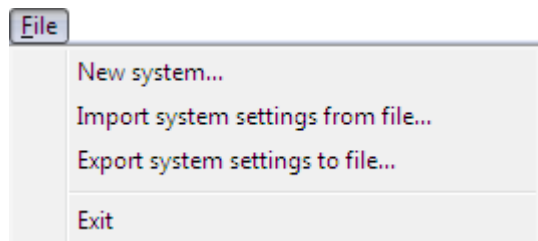
The PR Master has two main modes of operation: configuring and monitoring mode. Configuring mode, as you may guess, is designed to different configuration activities. The monitoring mode, on the other hand, allows for observation on what is going on the system. The monitoring mode is used mainly on day to day basis, when the RACS is stable and configured. In order to invoke monitoring mode, you can click on **Online monitoring** icon in the **Frequently used tasks** pane or to select **Tools/Online monitoring** command from the **Tools** menu.

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

## CHAPTER 3. PR MASTER FUNCTIONALITY

### 3.1. FILE MENU

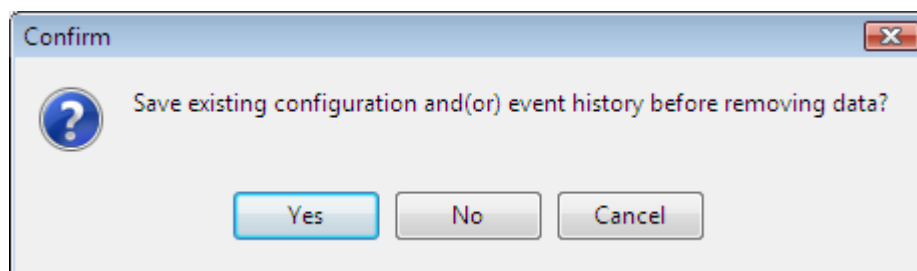
The **File** menu has been shown in Figure 3.1.



**Figure 3.1.** *File Menu*

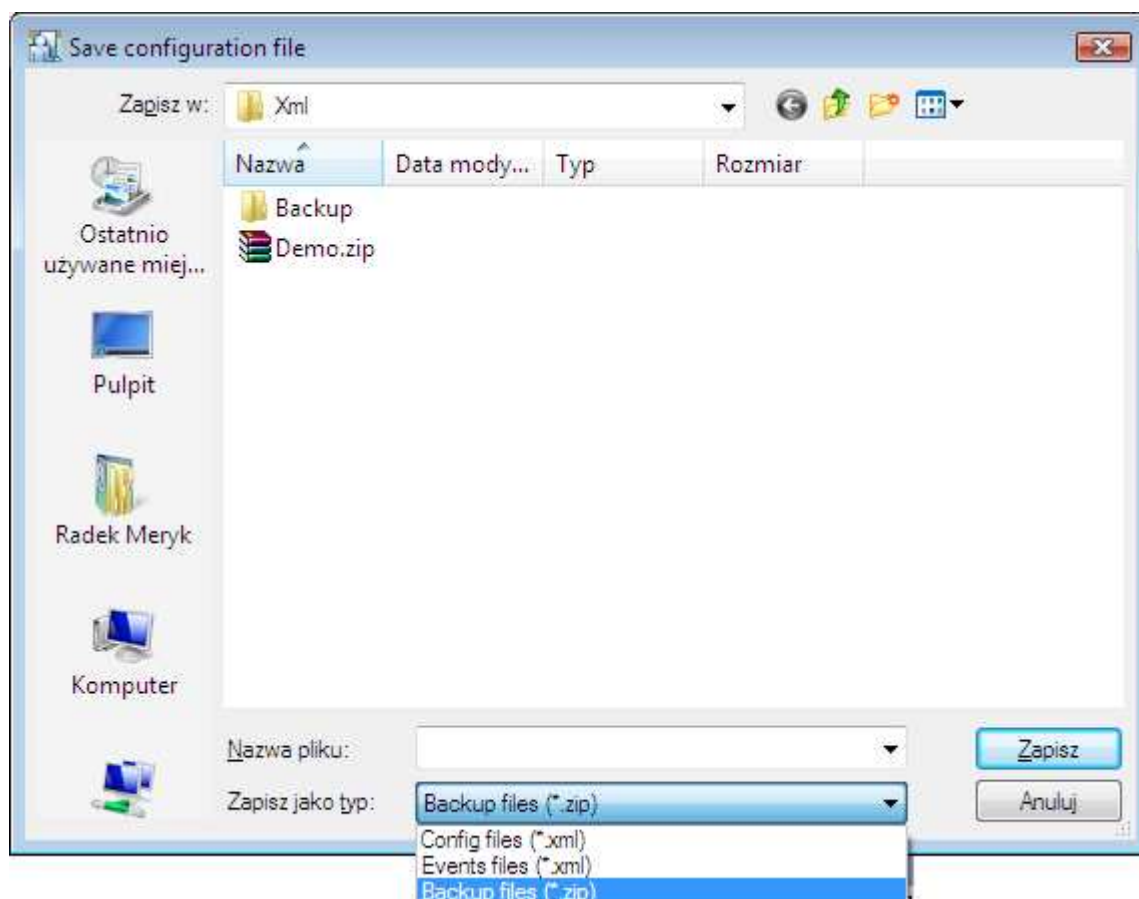
#### 3.1.1. New system... Command

**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 the backup of the current database content should be saved to (Figure 3.3). As you can see, you can save a backup file in a compressed format (**.zip**), but you can also select writing the settings only (**Config files (\*.xml)**) or writing settings together with events (**Events files (\*.xml)**).



**Figure 3.3.** Selecting file where system settings will be saved

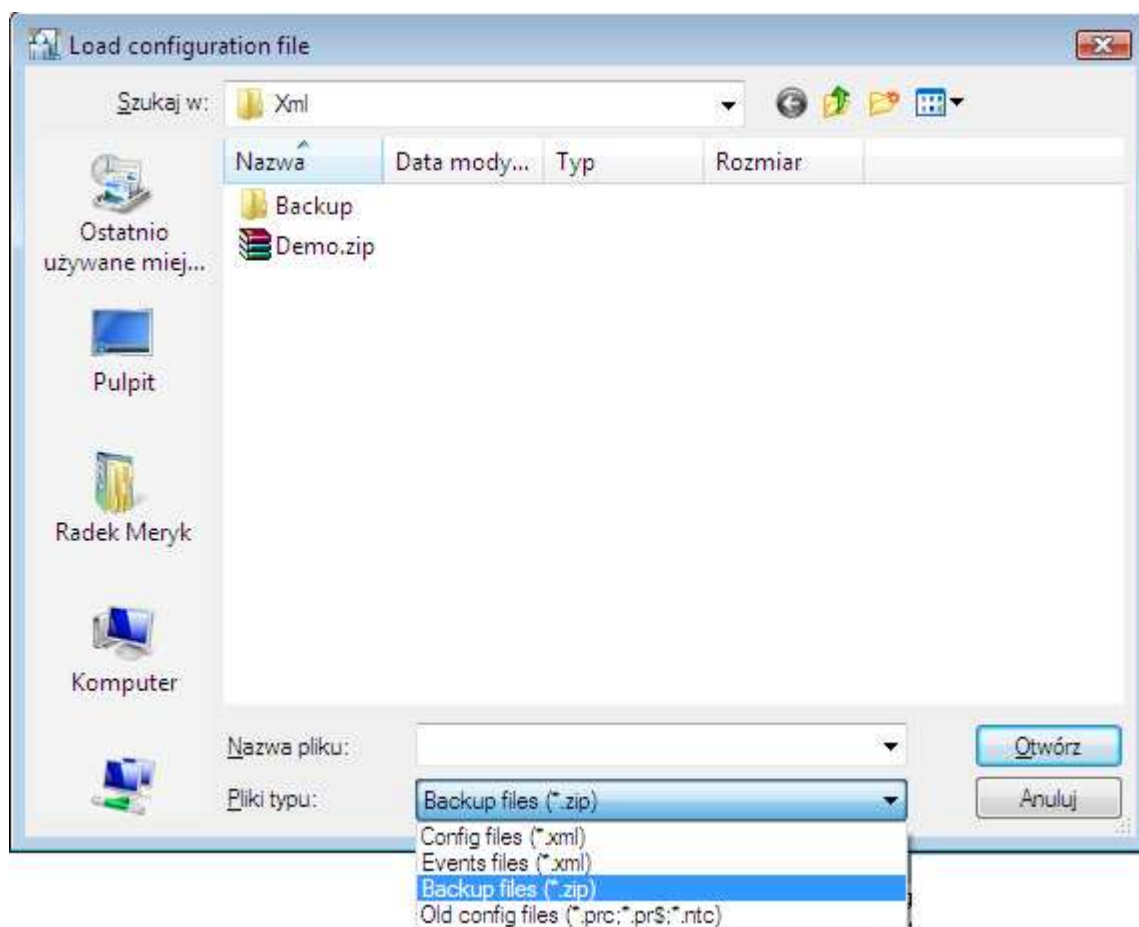


Using the **New system...** command without saving current settings will cause the data loss — all data about networks, controllers, schedules, users, events and all other information will be lost. In order to protect your own work, it is recommended that you use this command with caution and you make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

After completing the **New system...** command, the database is empty. You can observe that in the PR Master's main window — you will not find there any data which were there before.

### 3.1.2. Import system settings from file

The **Import system settings from file...** command allows for importing configuration (events) saved earlier or for restoring data from backup. After you select this command, the dialog box for selecting a file to import from will display (Figure 3.4).



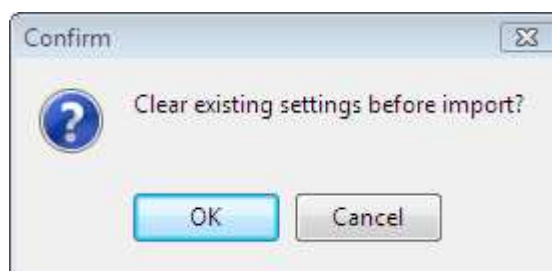
**Figure 3.4.** Selecting file to import data from

For files containing data to be imported, you can select the following file formats:

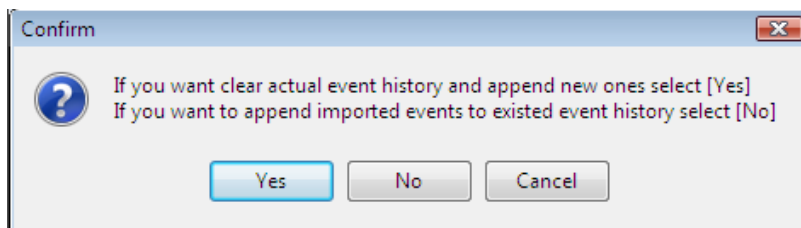
- ◆ configuration files (**Config files (\*.xml)**);
- ◆ events files (**Config files (\*.xml)**);
- ◆ backup files (**Backup files (\*.zip)**);
- ◆ configuration files from previous versions (**Old config files (\*.prc; \*.pr\$; \*.rtc)**).

Depending on the format chosen, the system asks different question regarding confirmation of all activities related to the import (Figure 3.5).

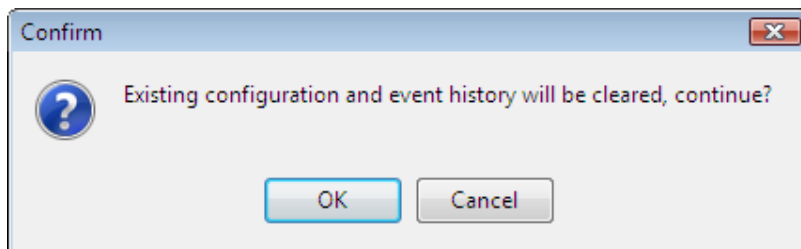
A — configuration files



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 for exporting current configuration, events or all the database content to external file. After you select this command, the dialog box for selecting a file to export data to will display (Figure 3.6).

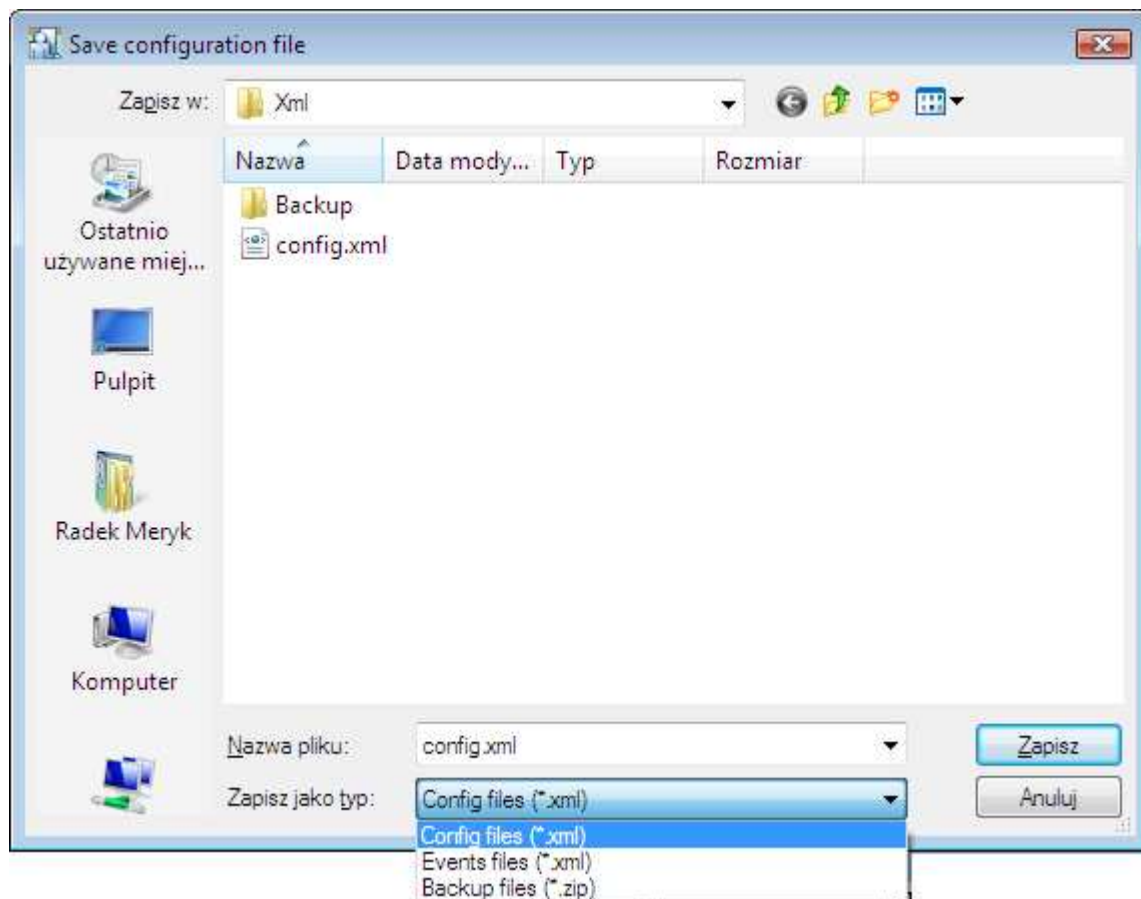


Figure 3.6. **Selecting file to export settings(data) to**

For selecting formats of export file you have the following options:

- ◆ configuration files (**Config files (\*.xml)**);
- ◆ events files (**Config files (\*.xml)**);
- ◆ backup files (**Backup files (\*.zip)**);

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).

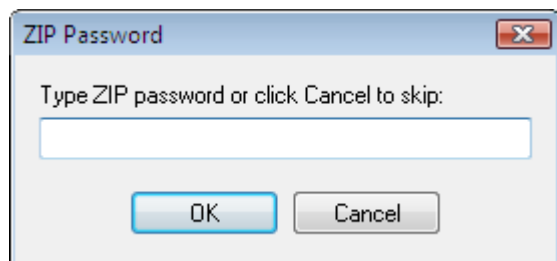


Figure 3.7. **Entering a password for protecting compressed zip file containing database backup**



### 3.1.4. Exit

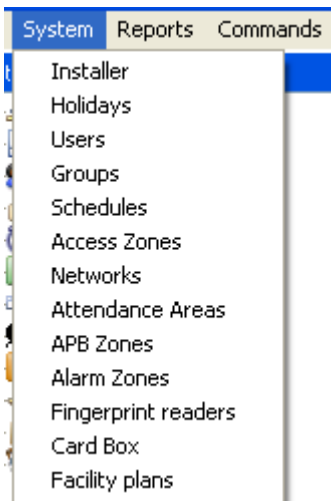
The **Exit** menu will terminate a current program session. Before the system terminates it displays a confirmation question asking if you really want to close the program (Figure 3.8).



**Figure 3.8.** Confirmation of an intent to close the program

## 3.2. SYSTEM MENU

The **System** menu has been shown in Figure 3.9.



**Figure 3.9.** System menu

### 3.2.1. Installer



The **Installer** menu has effect only for PR301 and PR201 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 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).

The dialog box 'Installer' has the following fields and content:

- Name: John Smith
- Card code: 0021487682355
- PIN Code: 3456
- Comment: 62 Lorong Chuan, 05-08 New Tech Park, Singapore

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

The  button next to the **Card code** field makes possible to assign a card to the *INSTALLER* user. You can do this using a transponder selected. In the **Comment** field you can enter any information such as the *INSTALLER* user contact data.

### 3.2.2. Holidays

There are many time schedules used in the system (general purpose, door mode, identification mode, and so on). They are assigned to specific weekdays. You can find more information on schedules in [section 3.2.5. Schedules](#). The **Holiday** command is used for defining holidays of the current year.

During holidays you can define different settings as those which would be inferred from the weekday the specific holiday falls on. Except for the possibility to assign a typical settings for a weekday, user has four special schedules at his disposal.

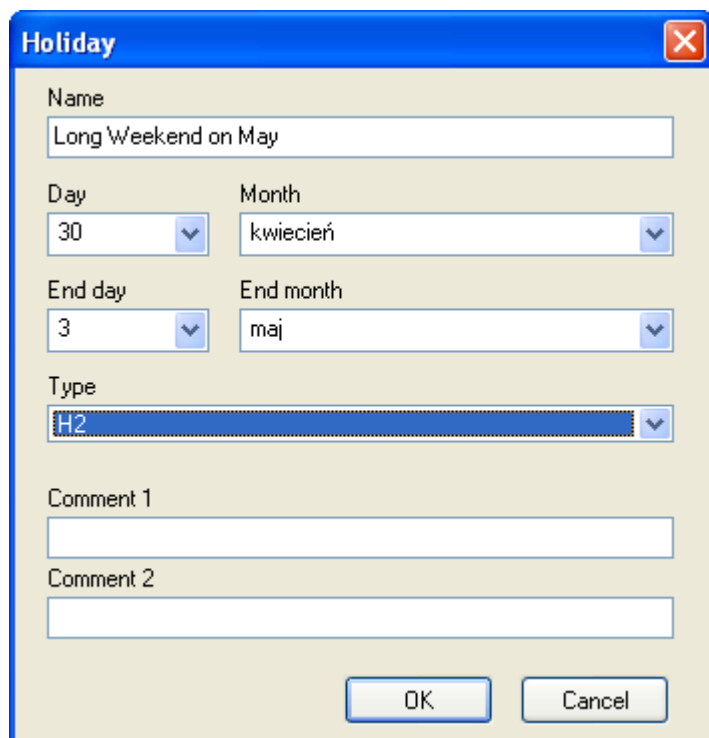
When defining holiday user can define time range when the particular holiday continues. It means that defining a separate time schedule for a long weekend requires indicating only its beginning and end.

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

Name	Begin	End	Type
Nowy Rok	1 styczeń	1 styczeń	Sunday
Easter 2010	3 kwiecień	5 kwiecień	Sunday
Long weekend on May	1 maj	3 maj	H1

**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*

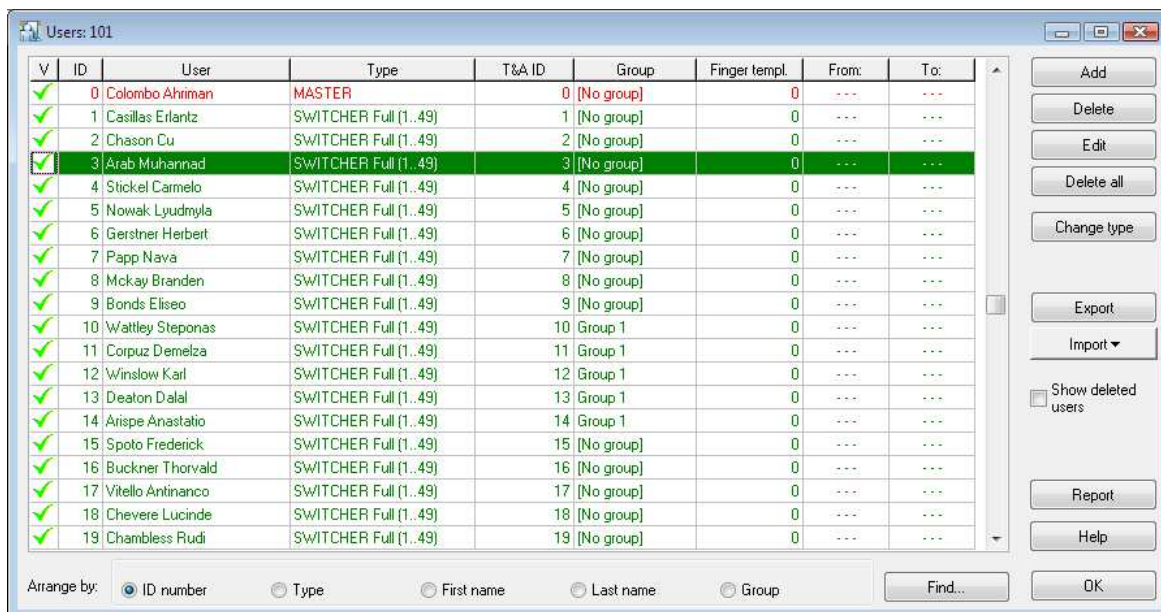
The **Edit** button makes possible to modify settings for the holiday defined earlier, and the **Delete** button allows for erasing the holiday selected.

### 3.2.3. Users

There are 4 types of users in the RACS:

- ◆ **MASTER** — has rights to open doors, arm/disarm controllers and to enter manual programming mode of controllers. It has an Id of 0.
- ◆ **SWITCHER Full**— has rights to unlock doors, arm/disarm controllers. Users of such type can be assigned Id numbers from 01–49 range.
- ◆ **SWITCHER Limited** — has rights to arm/disarm controllers. He does not have rights to unlock doors. Users of such type can be assigned Id numbers from 50–999 range.
- ◆ **NORMAL** — user of this type have rights to unlock doors only. They have identification numbers assigned from the range 100 – 3999. Users of **NORMAL** type having ID above 1000 can additionally have a **Local SWITCHER** attribute, which give them rights to arm/disarm the controller for which this attribute has been given.

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



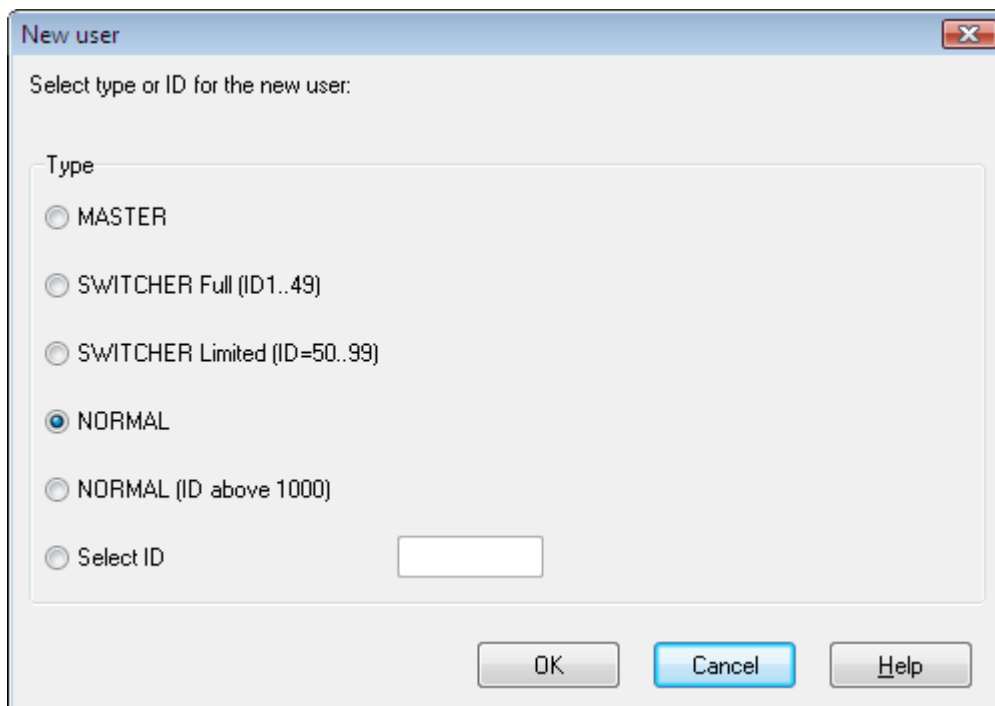
**Figure 3.13.** System user directory

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 windows' title, after the "Users" word there is a current users number (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 displays.

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

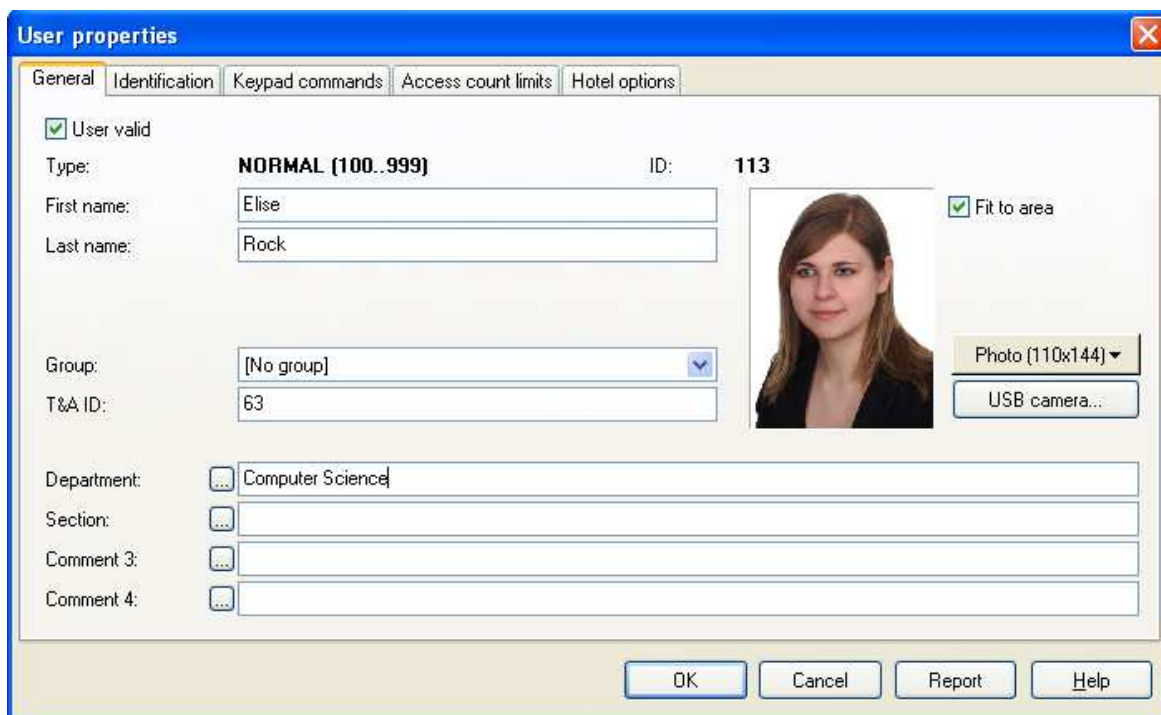
### 3.2.3.1. Adding New User

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 identification 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 infer a user type from the value of Id entered by the user.




**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. 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 — a card, a PIN and fingerprint templates if any.

**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 reader selection window displays where you would be able to read a card. In some circumstances, especially when there is no reader in the vicinity of the operator's console, this option is inconvenient. In such a case you can utilize 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 3.2.12. "**Card box**". 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 (the **Read from a reader** button) 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 commands on controllers selected.

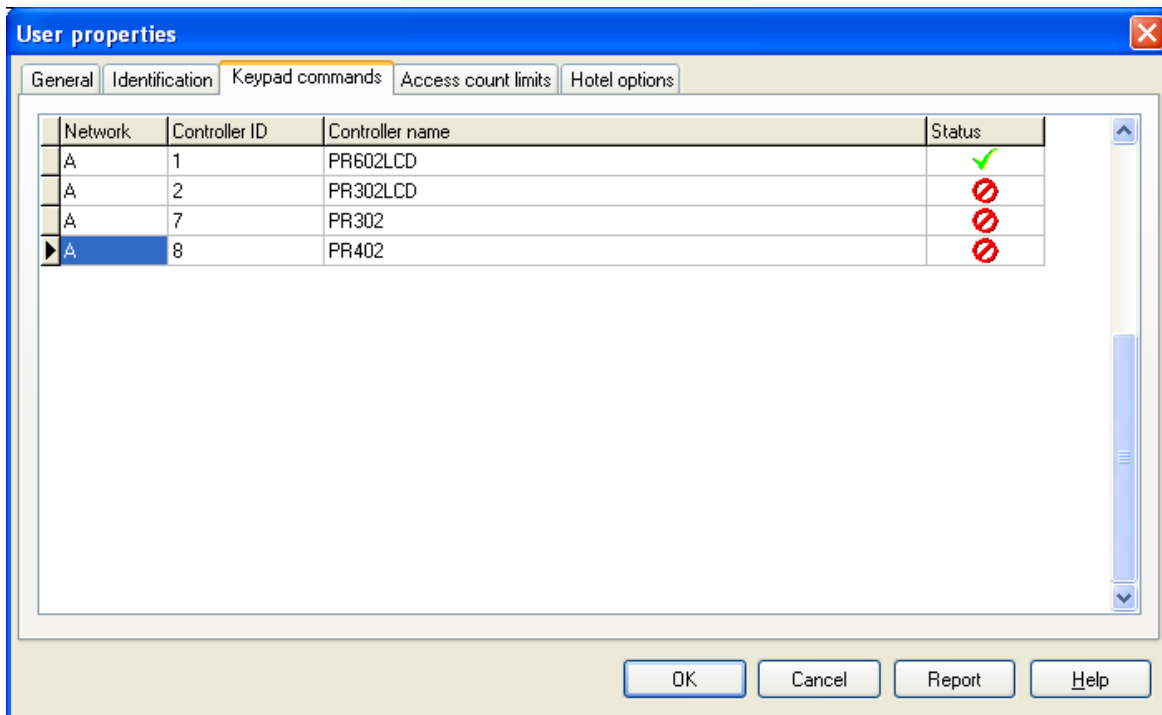


Figure 3.17. User properties — Keypad commands tab

**Access count limits** (Figure 3.18) — this is the tab allowing for reading login limits from controllers as well as for managing them in relation to the user selected. You can assign login limit on particular controllers for every user. After you enter the login limit, the controller will let the user log on only specific number of times. From this window you can modify login limit for the selected user. You also have option to erase the limit altogether. You should send data to controllers whenever you change the logon limit.

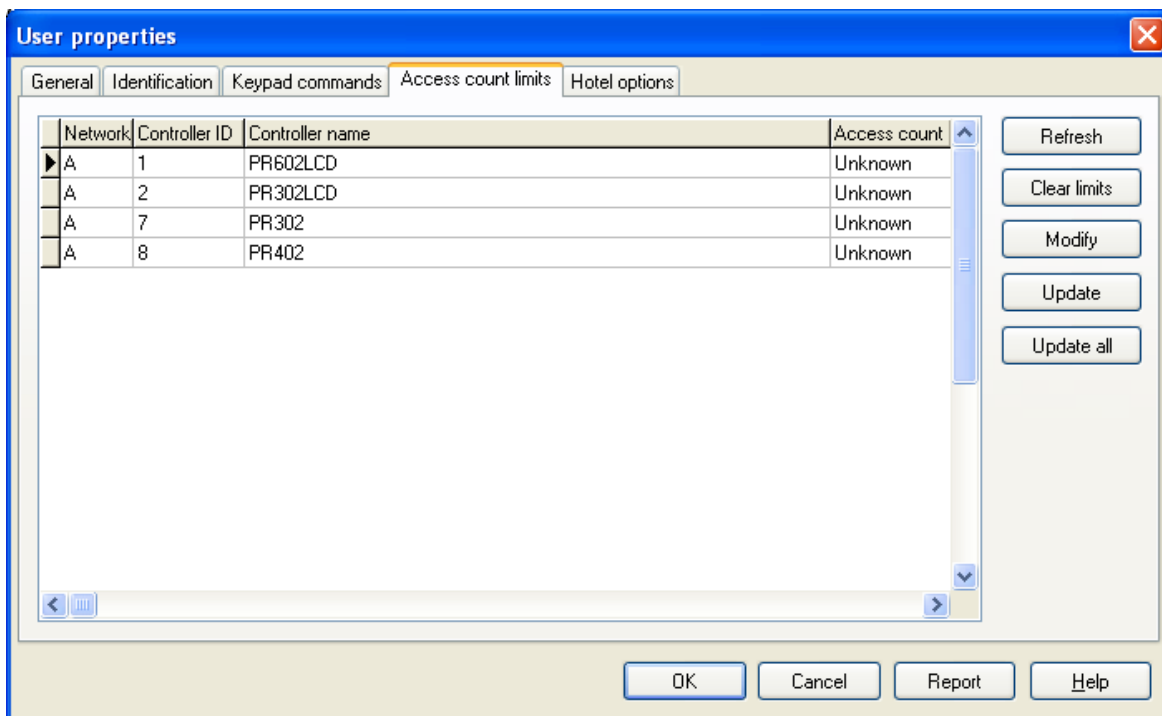


Figure 3.18. User properties — logon limits tab

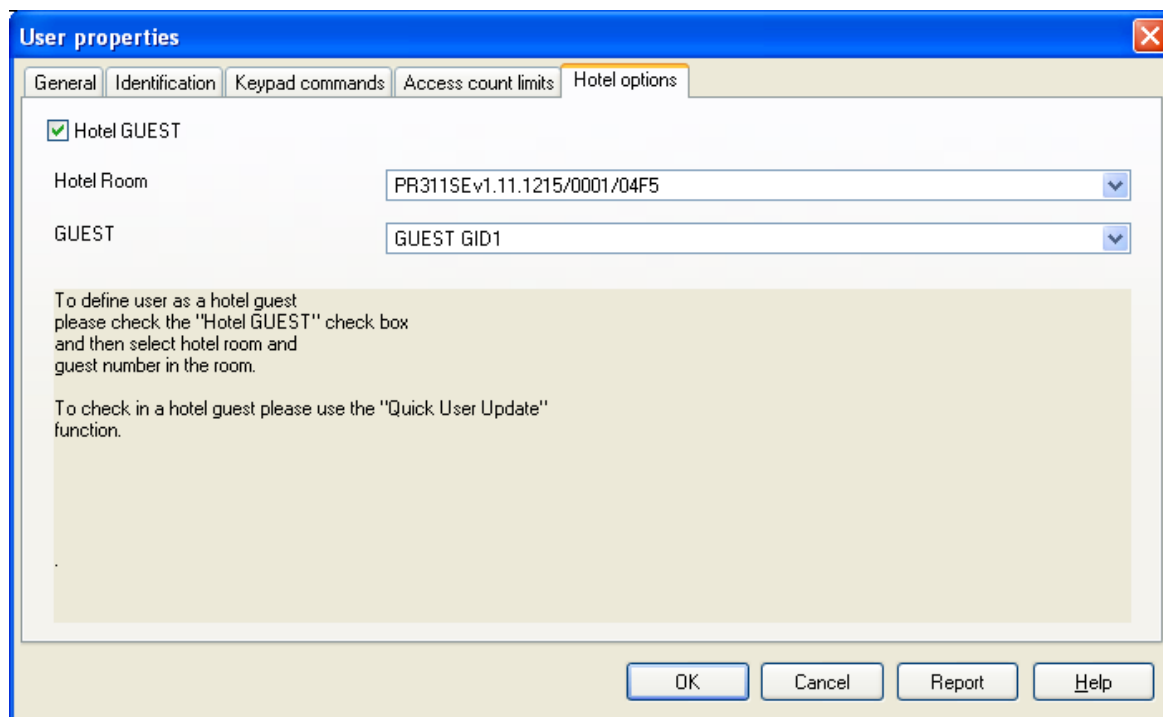
**Hotel options** (Figure 3.19) — window which allows to specify that selected user is a hotel guest and to assign a guest number in selected hotel room.



Hotel room options are available for PR311SE, PR311SE-BK, PR611, PR621, and PR411 controllers. You can find more info on this subject in the [PRxx1 Series Access Controllers. Functional Description and Programming Guide](#) which you can find on the Roger website.

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

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).

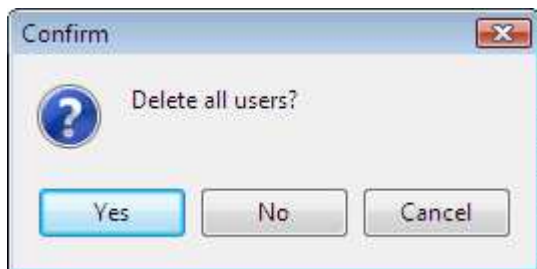


**Figure 3.20** Confirming user deletion

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.



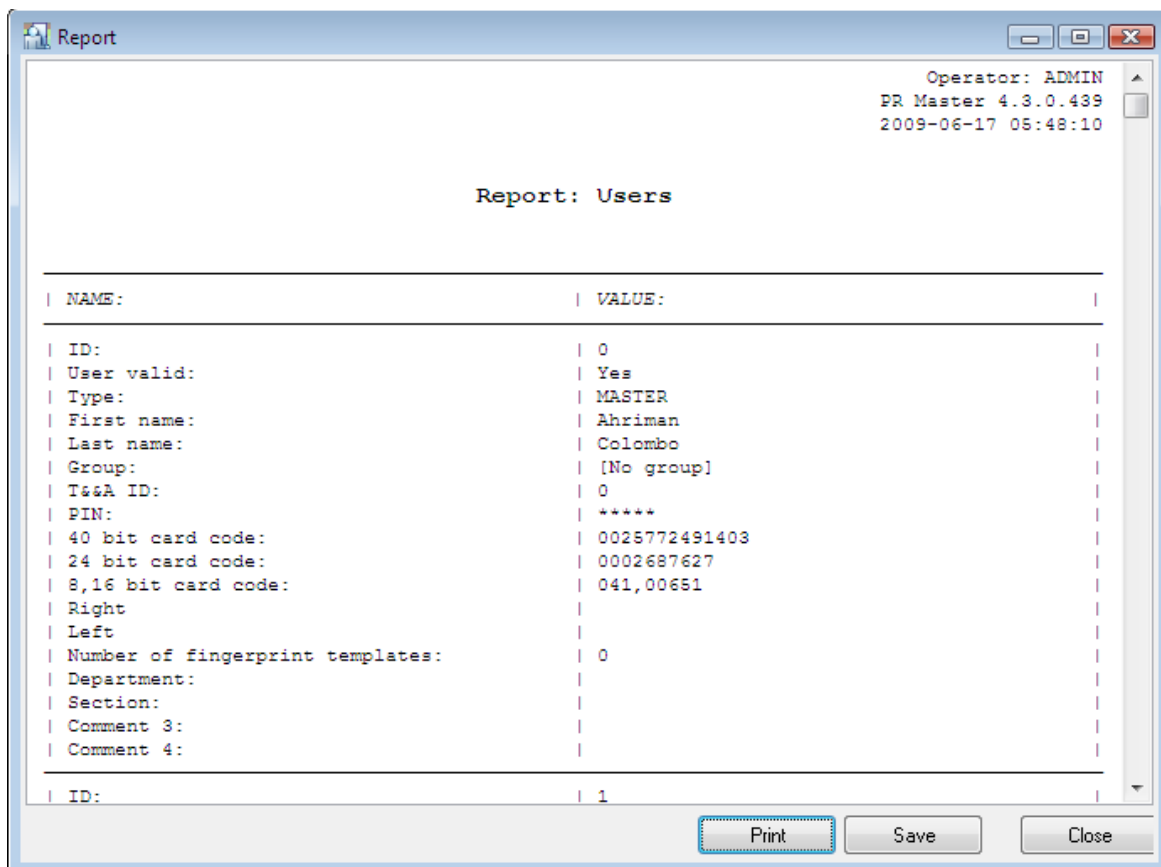
**Figure 3.21.** Searching for user data

### 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 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 displaying in the **Users** directory. Deleted users’ data displays as **strikeout** (Figure 3.24).

V	ID	User	Type	T&A ID	Group	Finger templ.	From:	To:
✓	25	Pollard Miles	SWITCHER Full (1..49)	25	[No group]	0	---	---
✓	26	Thompson May	SWITCHER Full (1..49)	26	[No group]	0	---	---
✓	27	Arent Allen	SWITCHER Full (1..49)	27	[No group]	0	---	---
✓	28	Cogdill Elhora	SWITCHER Full (1..49)	28	[No group]	0	---	---
✓	29	Seats Laurentia	SWITCHER Full (1..49)	29	[No group]	0	---	---
✓	30	Moseley Bertha	SWITCHER Full (1..49)	30	[No group]	0	---	---
✓	31	Henry Jack	SWITCHER Full (1..49)	31	[No group]	0	---	---
✓	32	Dawson-Lily	SWITCHER Full (1..49)	32	[No group]	0	---	---
✓	33	Yumo Alberto	SWITCHER Full (1..49)	33	[No group]	0	---	---
✓	34	Pratt Gonzalo	SWITCHER Full (1..49)	34	[No group]	0	---	---
✓	50	Connors Mauro	SWITCHER Limited (50..99)	35	[No group]	0	---	---
✓	51	Reed Sarah	SWITCHER Limited (50..99)	36	[No group]	0	---	---
✓	52	Bowles Lynette	SWITCHER Limited (50..99)	37	[No group]	0	---	---
✓	53	Conway Marie	SWITCHER Limited (50..99)	38	[No group]	0	---	---
✓	54	Vasquez Matthews	SWITCHER Limited (50..99)	39	[No group]	0	---	---
✓	55	Rasmussen Pearlle	SWITCHER Limited (50..99)	40	[No group]	0	---	---
✓	56	Bernard Rosella	SWITCHER Limited (50..99)	41	[No group]	0	---	---
✓	57	Kelly Jennifer	SWITCHER Limited (50..99)	42	[No group]	0	---	---
✓	58	Duffy Masha	SWITCHER Limited (50..99)	43	[No group]	0	---	---
✓	59	Kane Nina	SWITCHER Limited (50..99)	44	[No group]	0	---	---

Figure 3.24. The users list together with deleted users data

### 3.2.4. Groups

Users in the RACS 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 relies upon describing rules on when and where the users belonging to system's groups will be given access. For every group you can define rights for 32 floors (0–31) in up to four elevators. The rights to the floors can not be restricted by time schedules.

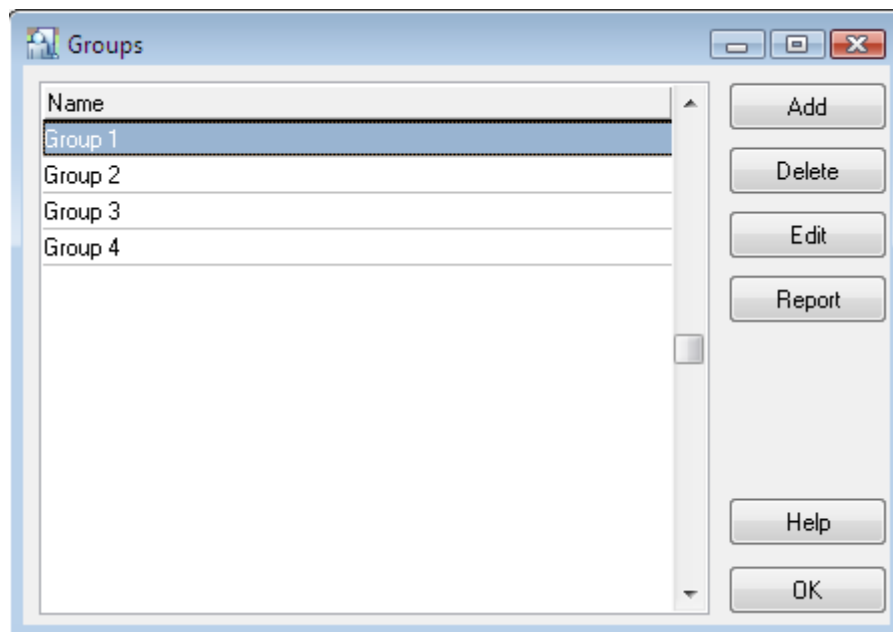
By default, a newly registered user in the system is not assigned to any access groups. The users who do not belong to any group (i.e. **No group**) have rights to enter all the rooms and floors without any time limitations. This is default settings for a newly registered user.

Users assigned to the group **No group** loses access for 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 OFF mode and at the same time the option **Access disabled when controller armed** is set.

If you use the last scheme, you can achieve an effect that users who were not assigned to any group (the **No group** setting) can be temporarily blocked (they are blocked if the controller is in the OFF state and are given access again when it switches back to the ON state).

The **Group** command opens the system's group directory (Figure 3.25):



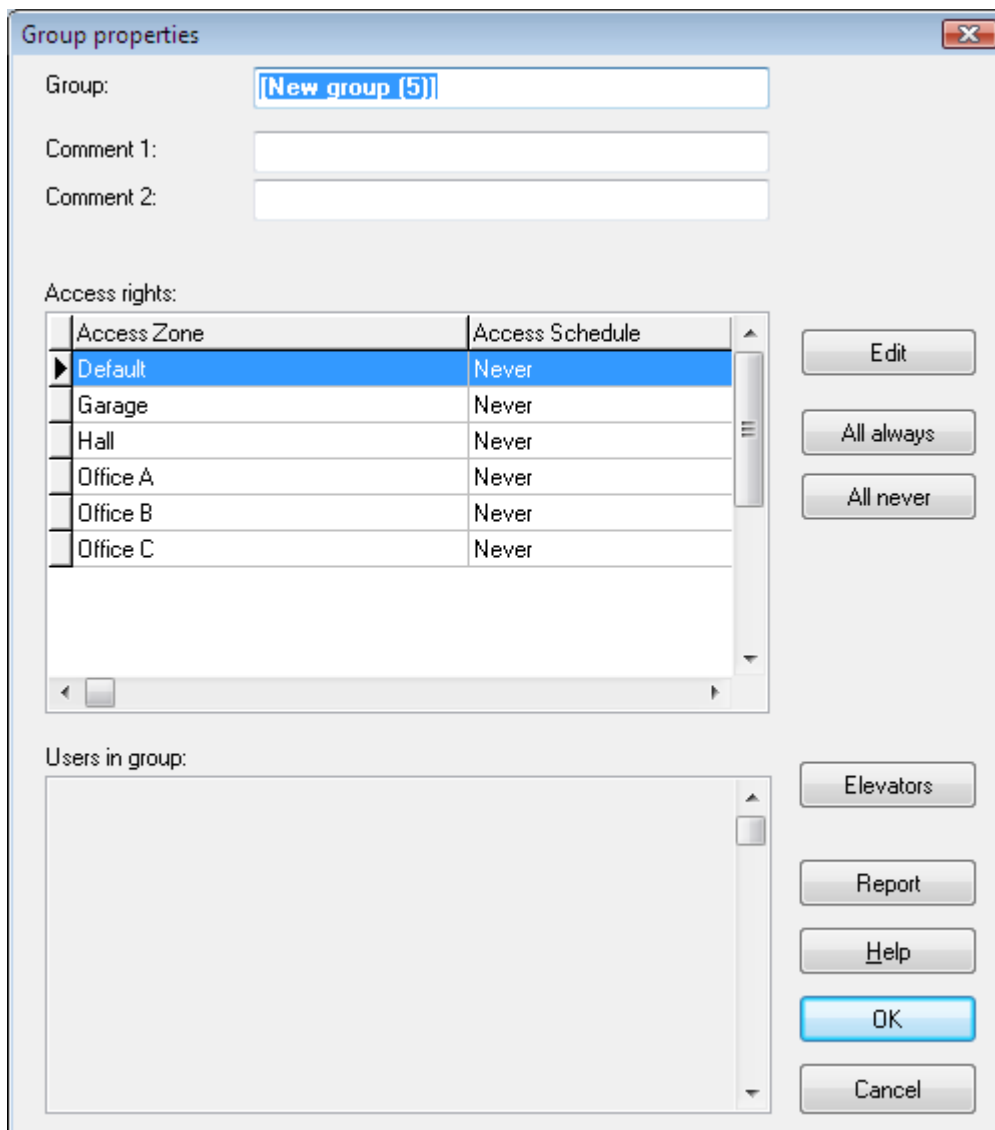
**Figure 3.25.** *Group directory*

The concept of groups is related to access rights in the RACS. From the hardware side, the terminals controlled by controllers make so called access zones (see [3.2.6. Access zones](#)). The users, on the other hand, belong to groups, and groups have access rights for specified zones. Additionally there are time schedule defined (see [3.2.5. Polecenie Harmonogramy](#)). Using them you can indicate, 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 need to 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.

### 3.2.4.1. Adding New Group

In order to add a new group, you need to click on the **Add** button in the Group directory (Figure 3.25). The **Group properties** window appears (Figure 3.26). Using this window you can define the name for a group, enter descriptive comments and describe groups' access rights for access zones defined in the system. By default, at the time of adding a group, it does not have any access rights in the access zones defined in the system (for every access zone there is the **Never** schedule assigned).

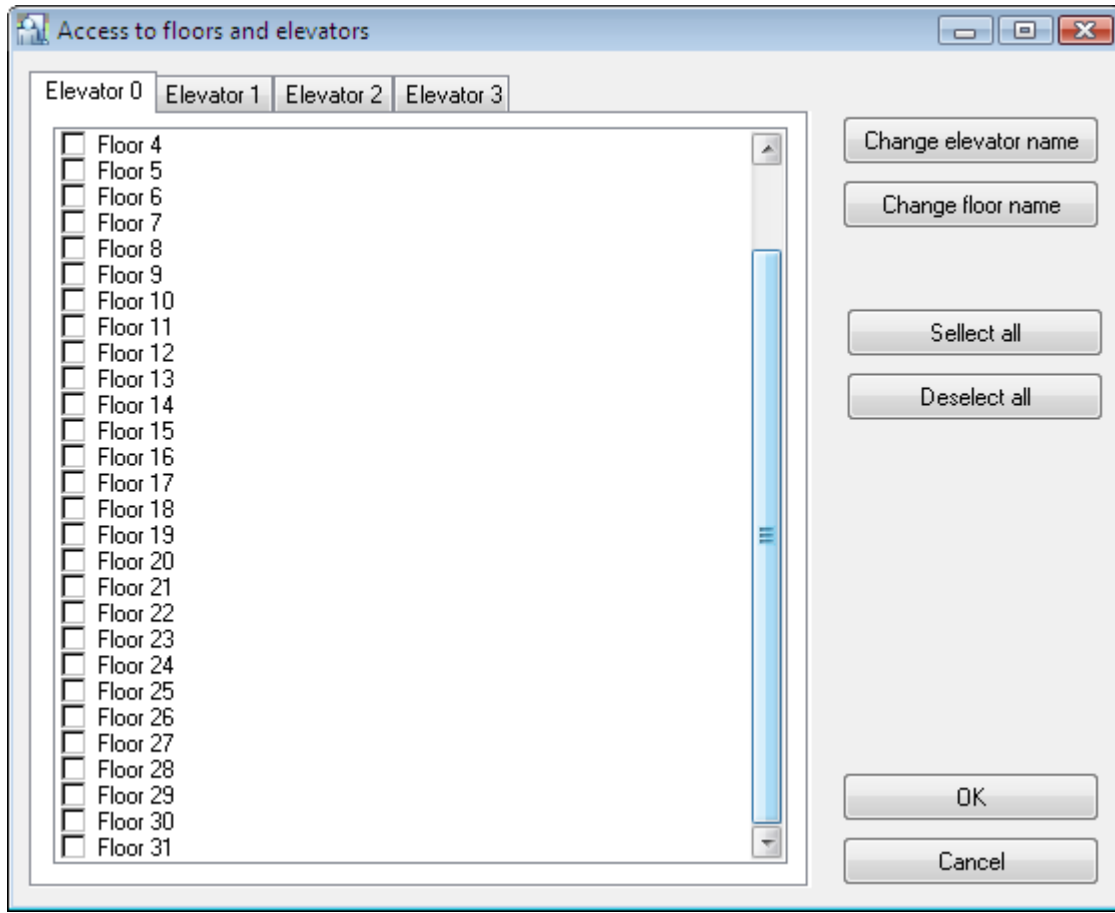


**Figure 3.26.** Group directory

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, sets an access schedule for all the zones to **Never** value. You can also assign separate schedules for individual zones. The **Edit** button serves this purpose.

The **Elevators** button opens **Access to floors and elevators dialog box** (Figure 3.27).



**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.

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 3.28).

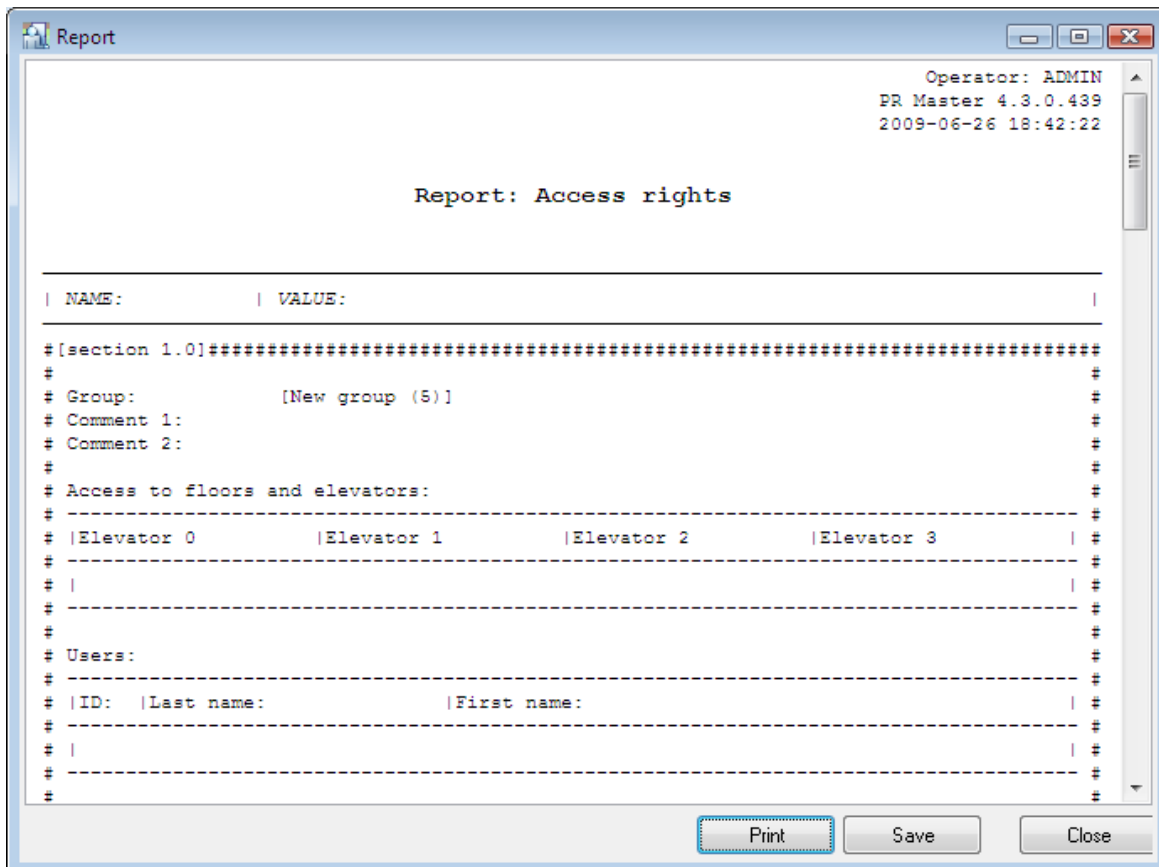


Figure 3.28. The Access rights report

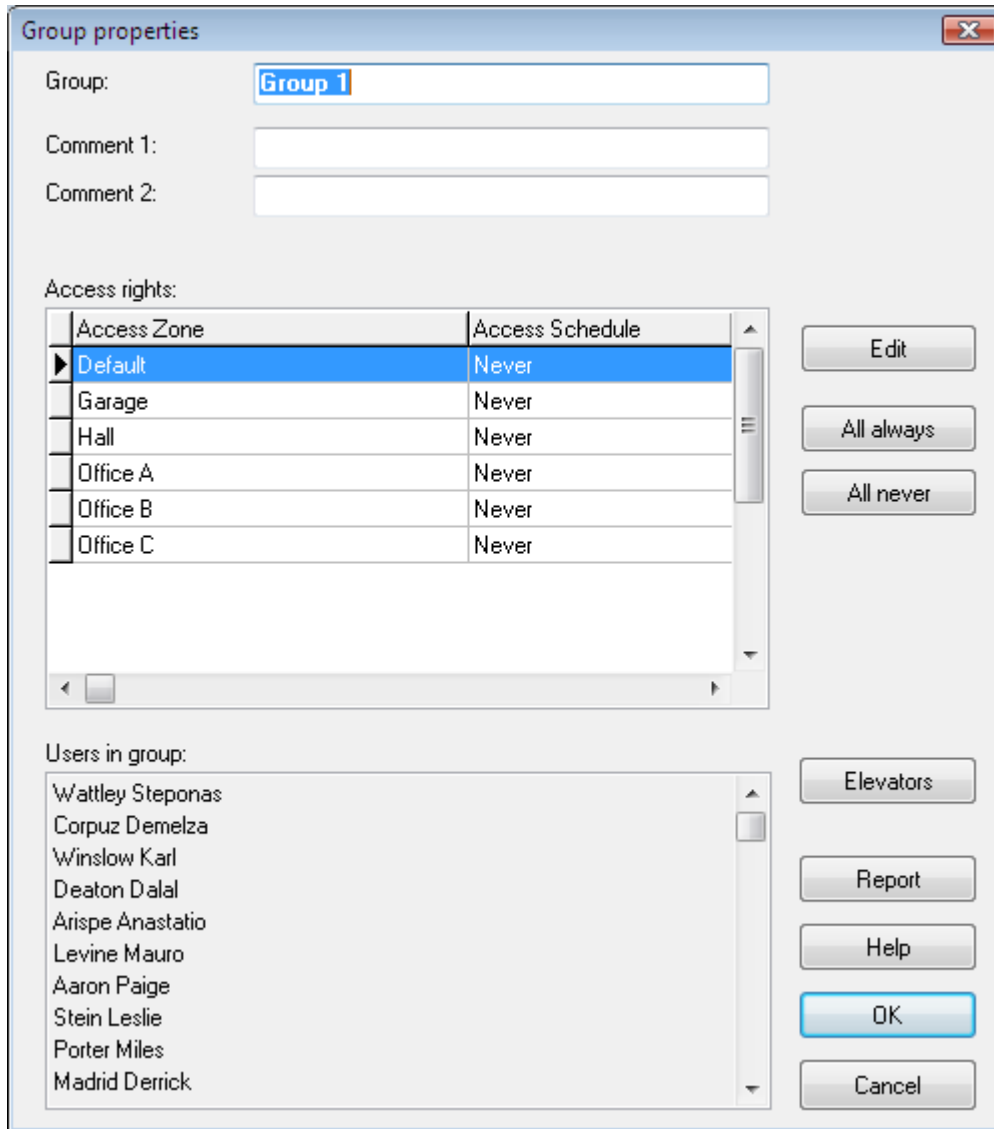
### 3.2.4.2. Assigning Users to Groups

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 3.29).



**Figure 3.29.** *Editing group's properties. In the Users in group area the list of users belonging to the group is displayed*

### 3.2.4.3. 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**.

### 3.2.4.4. 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 3.30).



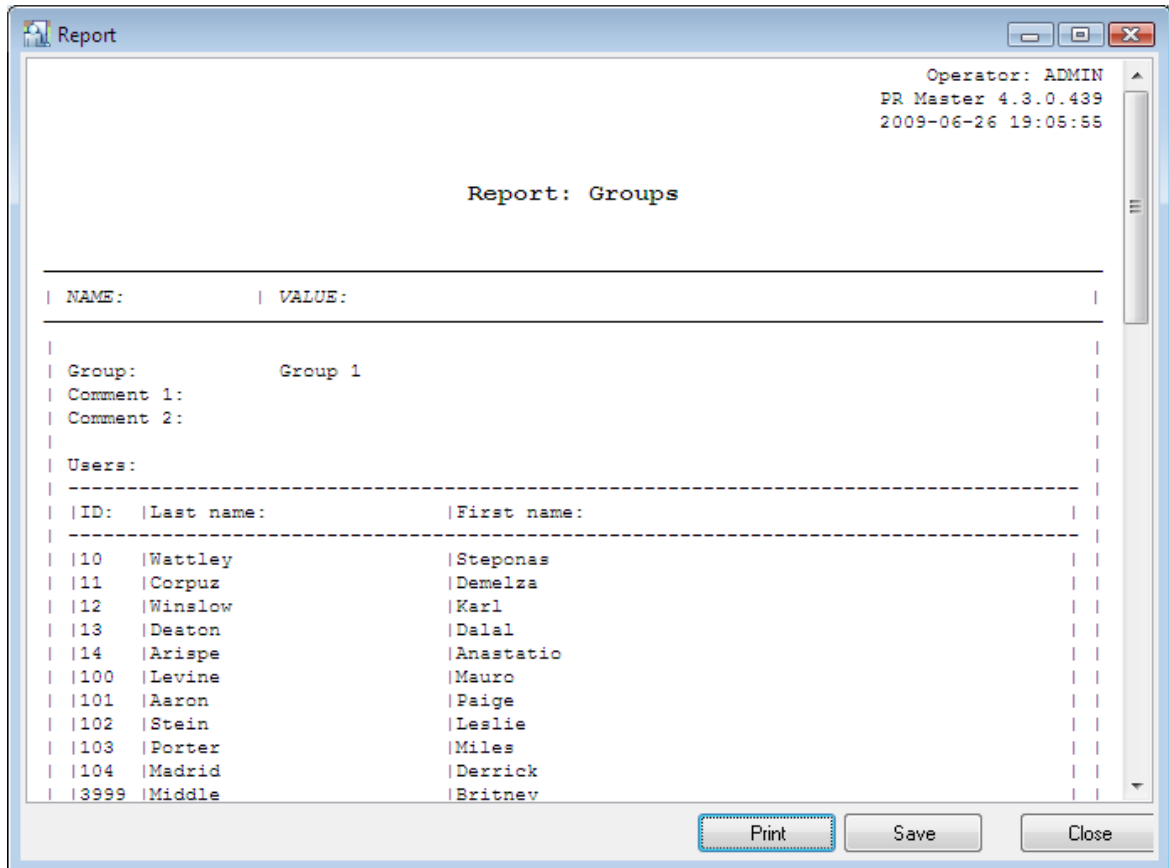


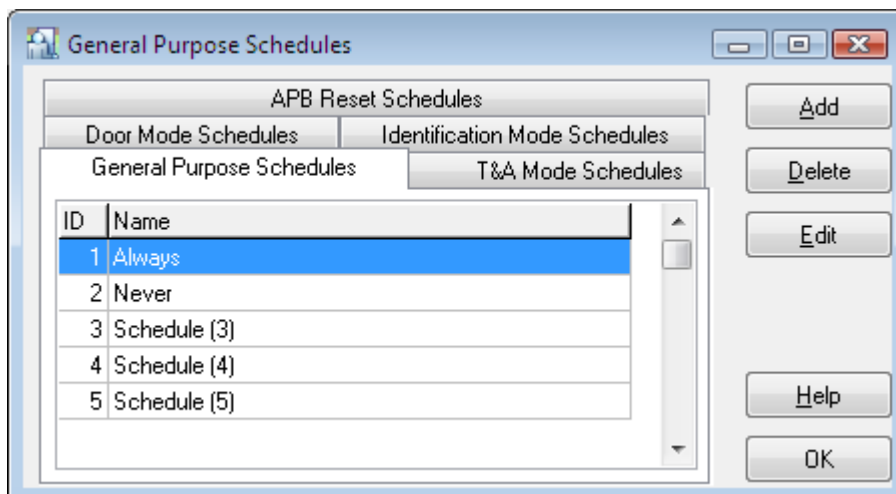
Figure 3.30. Groups report

### 3.2.5. Schedules

A schedule is a set of declarations of a From - To type 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:

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

For managing schedules in the RACS the **Schedule** command is used. When you select this command, the dialog box shown in Figure 3.31 appears.



**Figure 3.31.** Schedule management

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

### 3.2.5.1. General Purpose Schedules

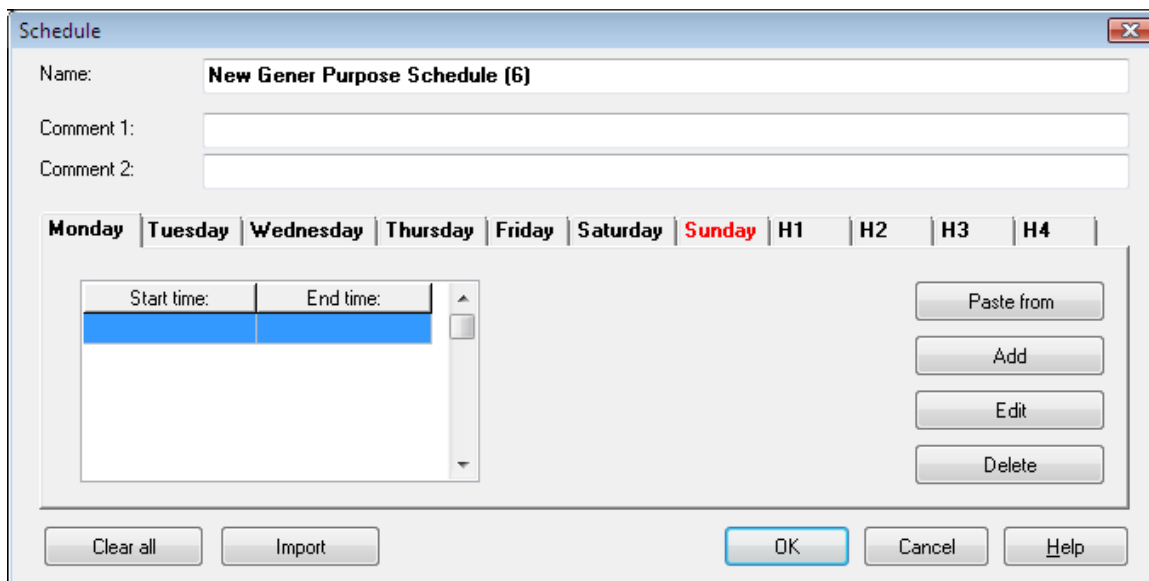
A general purpose schedule can be assigned to one or more control functions in the controller. For instance, the same schedule can be assigned for controlling an access, an output line or for blocking reading of an input line.

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

General purpose schedules are used for:

- ◆ defining 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;
- ◆ entering to zones in commission mode — you can define time intervals where it is possible to enter zones in commission mode — it requires presence of two persons and possibly some other condition;
- ◆ activity mode of the Facility Code function;
- ◆ input lines activities;
- ◆ output lines activities;
- ◆ high security mode (when entering to a zone requires an additional reader).

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 3.32).



**Figure 3.32.** *Defining a new general purpose schedule*

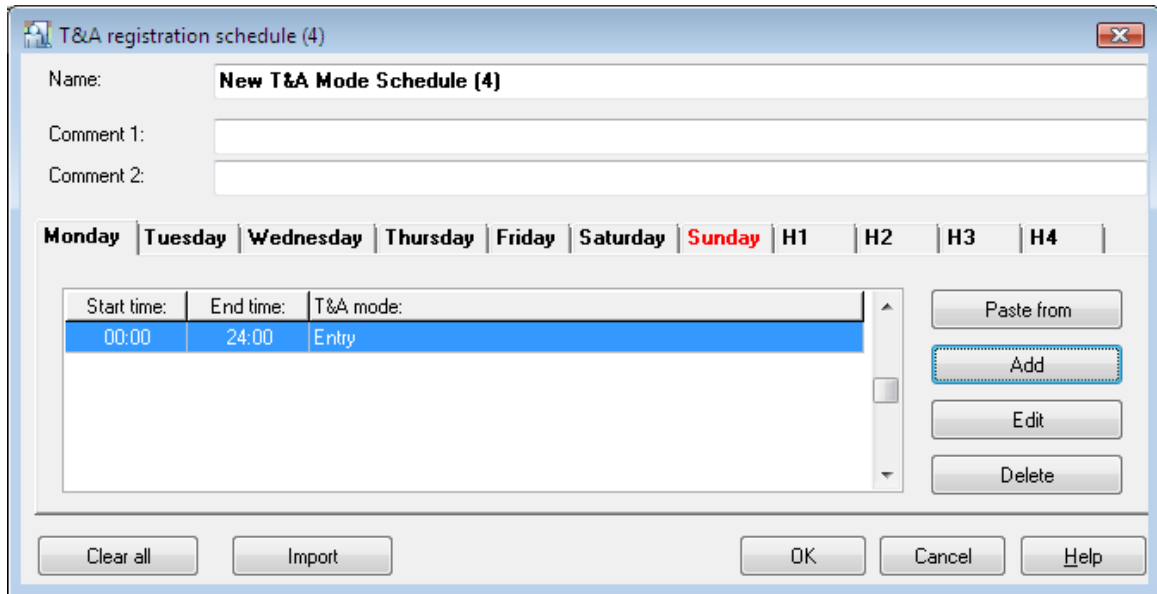
In the **Name** field you can enter a schedule name. In fields **Comment 1** and **Comment 2** you can enter any descriptive comments. The **Add** button can be used for defining a new time interval. When you click the button, the dialog box **Time period** appears, where you enter start and end times. 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.

### 3.2.5.2. 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 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 3.33).



**Figure 3.33.** 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.

### 3.2.5.3. APB Reset Schedules

The purpose of the Anti-Passback feature is to protect against the possibility to use an user credentials 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.

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 3.34).

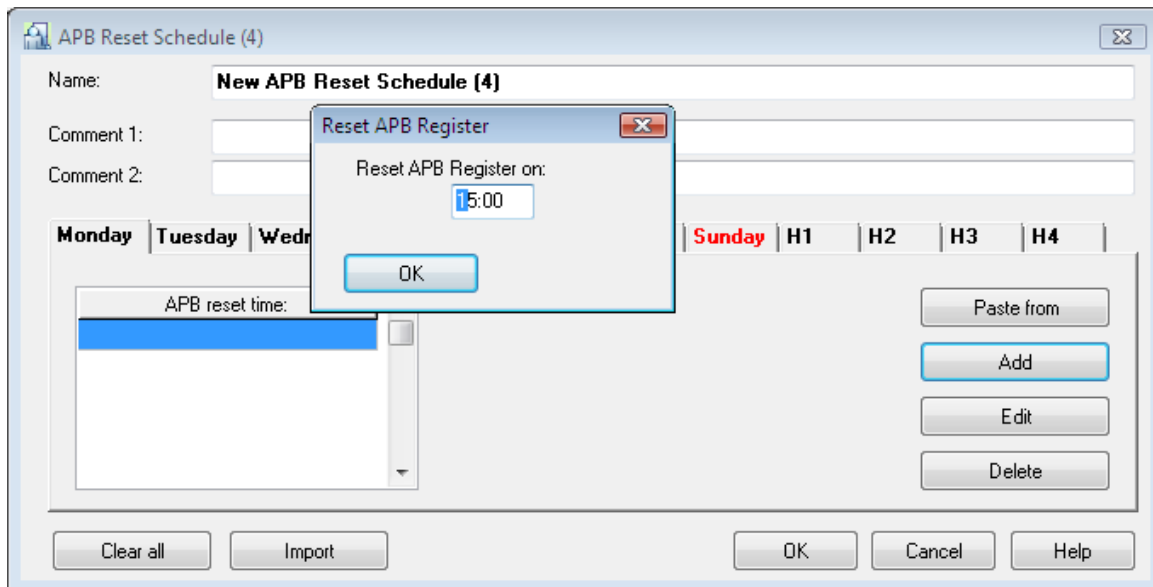


Figure 3.34. Defining a new APB reset schedule

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.

### 3.2.5.4. Door Mode Schedules

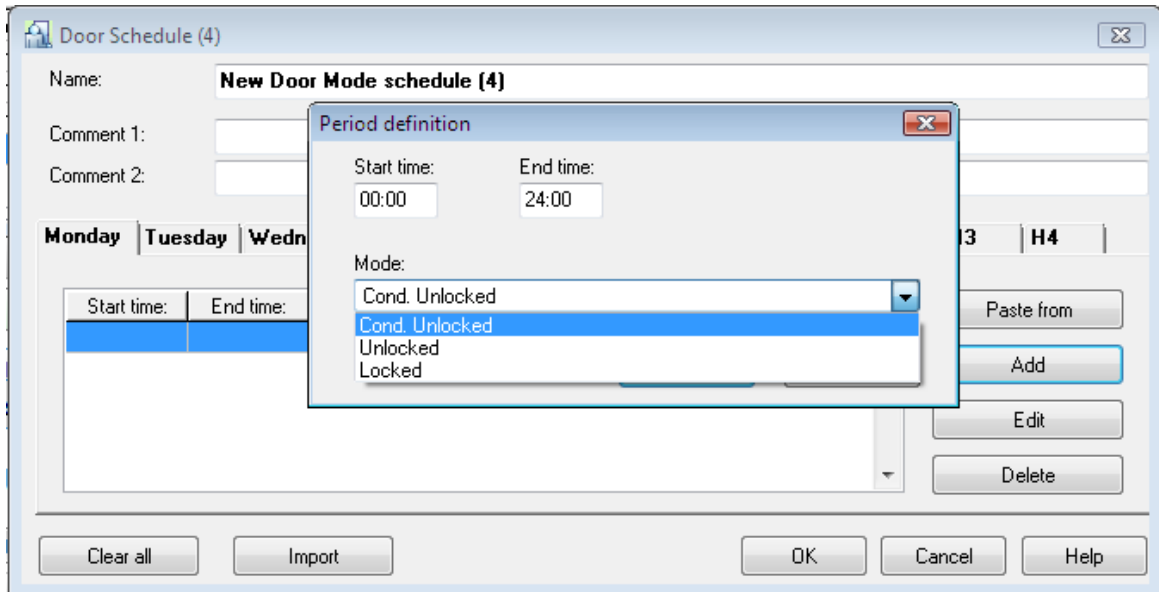
There are the following special door modes in the RACS:

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

Beyond the periods when special mode is in force, the door works in a standard mode — i.e. is locked and unlocks only when authorized user signs on.

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 3.35).



**Figure 3.35.** Defining a new door mode schedule

By default there is **Always in Normal Door Mode** schedule defined in the PR Master. It means, that a door always works in a standard way. This schedule can neither be erased nor modified.

### 3.2.5.5. Identification Mode Schedules

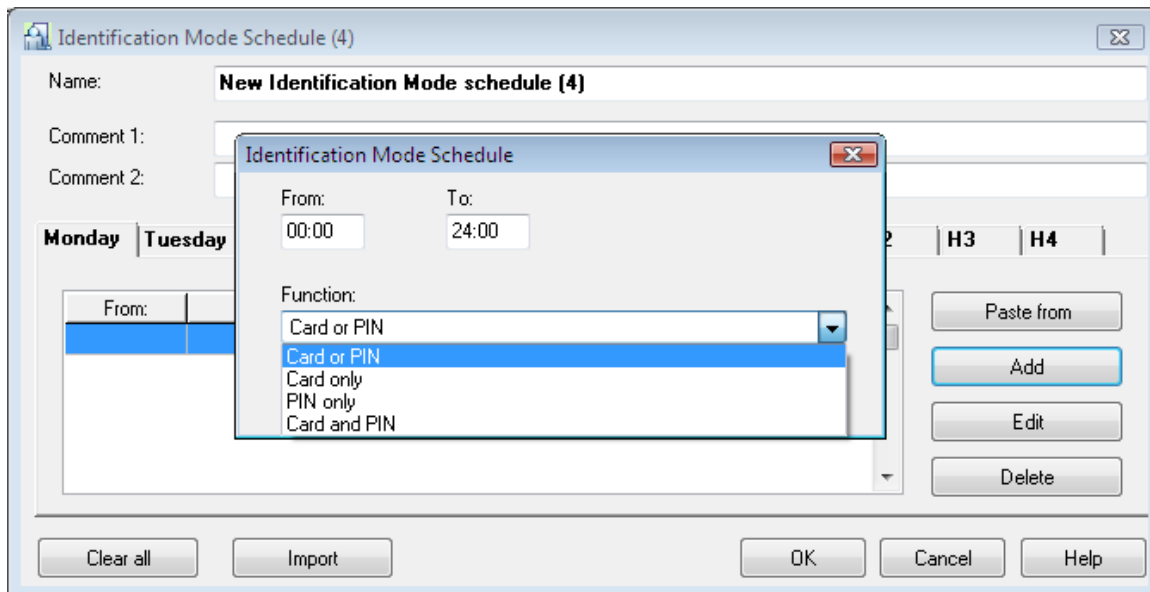
The following identification modes can be defined in the RACS:

- ◆ **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 3.36).



**Figure 3.36.** 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.

### 3.2.6. Access Zones

An **access zone** is a set of selected identification points (terminals), which in the RACS are treated as one entity. The access zone can be a specific place, e.g. a **Garage, Hall, Office**, and so forth. Defining access zones allows for defining access rights not for individual door but for devices group controlling access to the specific area in the facility.

Every controller, or to be specific every access point, should be assigned to the zone defined earlier. After you add a new controller to the system, it is the **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 of a newer type can be assigned to a separate zone.

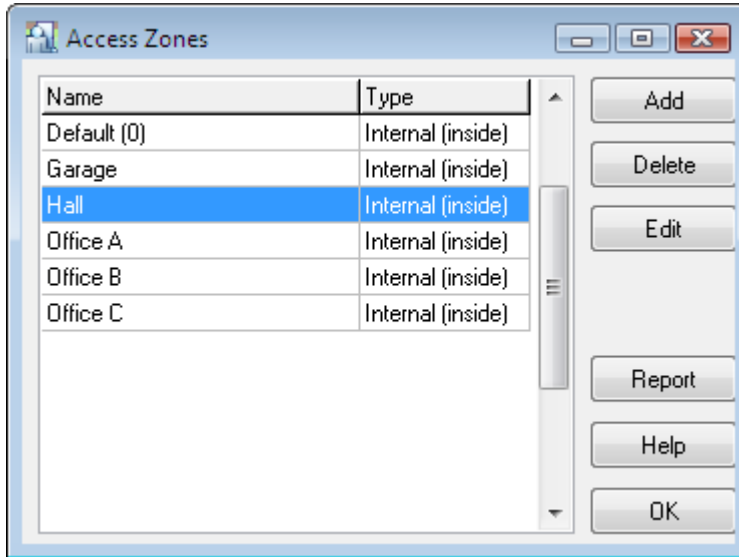


The terminal belongs to the zone, to which it allows entry to (not exit from).



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 3.37).



**Figure 3.37.** 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..

### 3.2.6.1. Adding New Access Zone

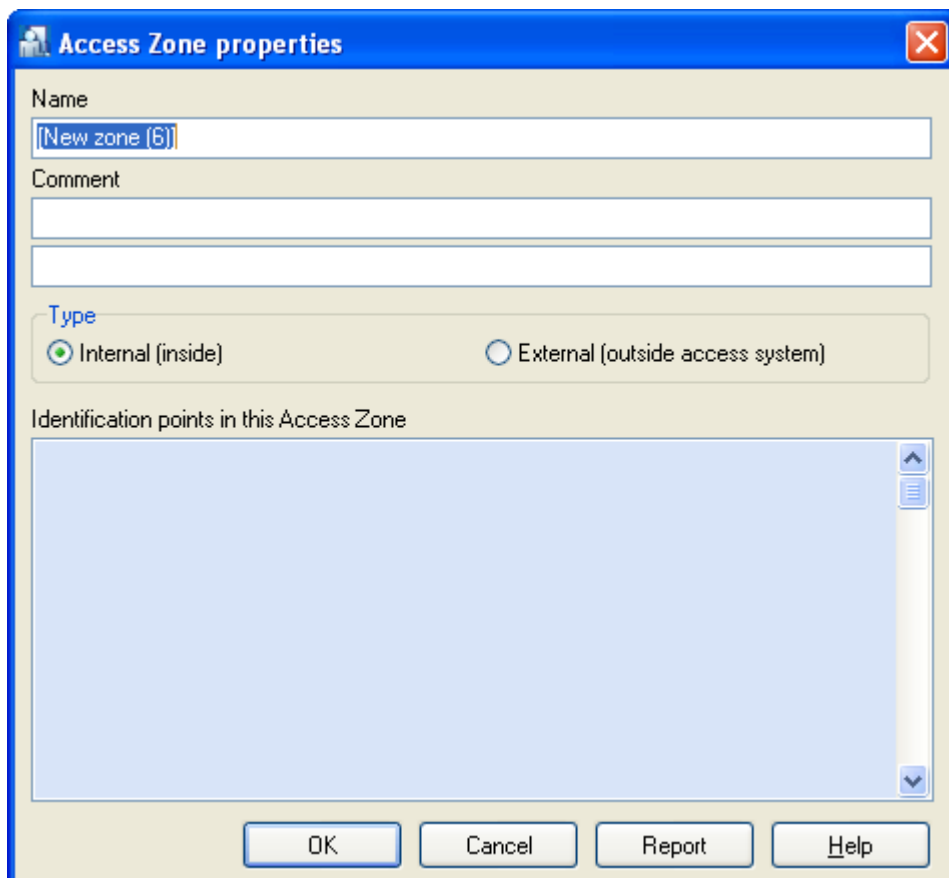
In order to add a new access zone, you should click on the **Add** button. The **Access Zone properties** window appears (Figure 3.38). Using this window you can define the name for a zone, enter descriptive comments and indicate if the zone is **External** or **Internal**.

The **internal zone** is located inside the facility. An **external zone** (public zone) can be thought of as 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 3.38.** *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.

### 3.2.6.2. 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.

### 3.2.6.3. 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 3.39 and 3.40). 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.

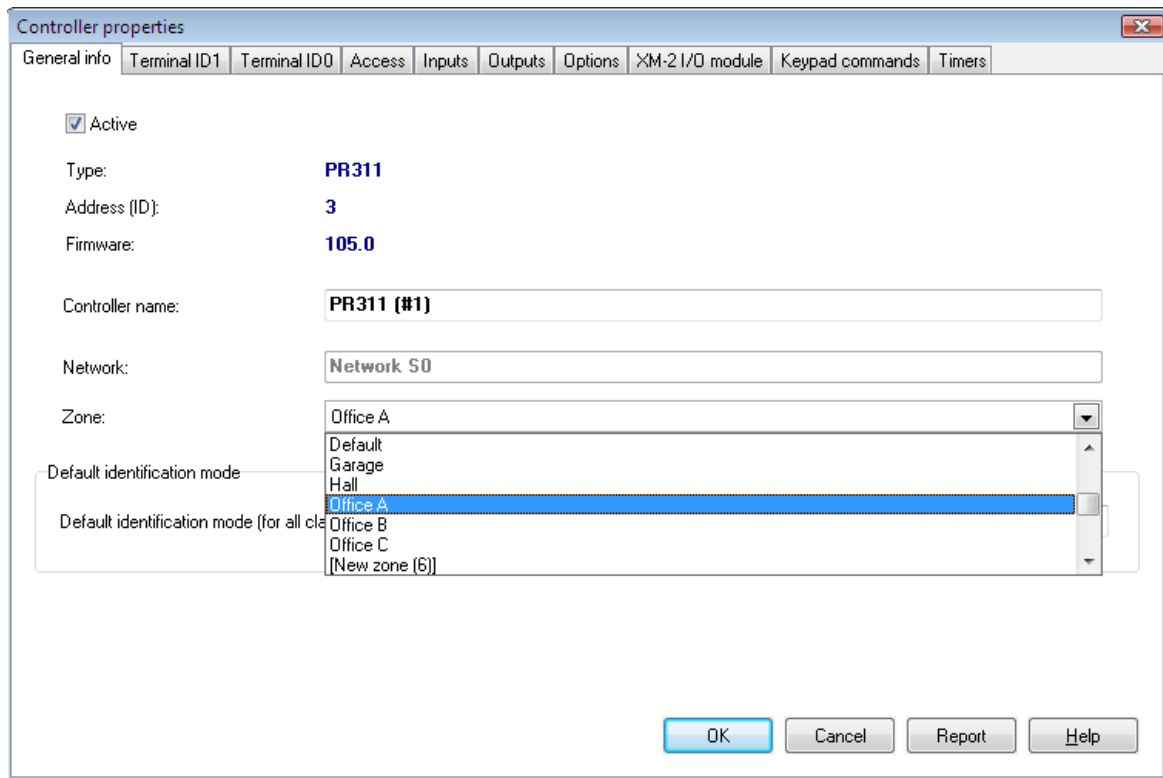


Figure 3.39. Assigning controller to the access zone — PR 311

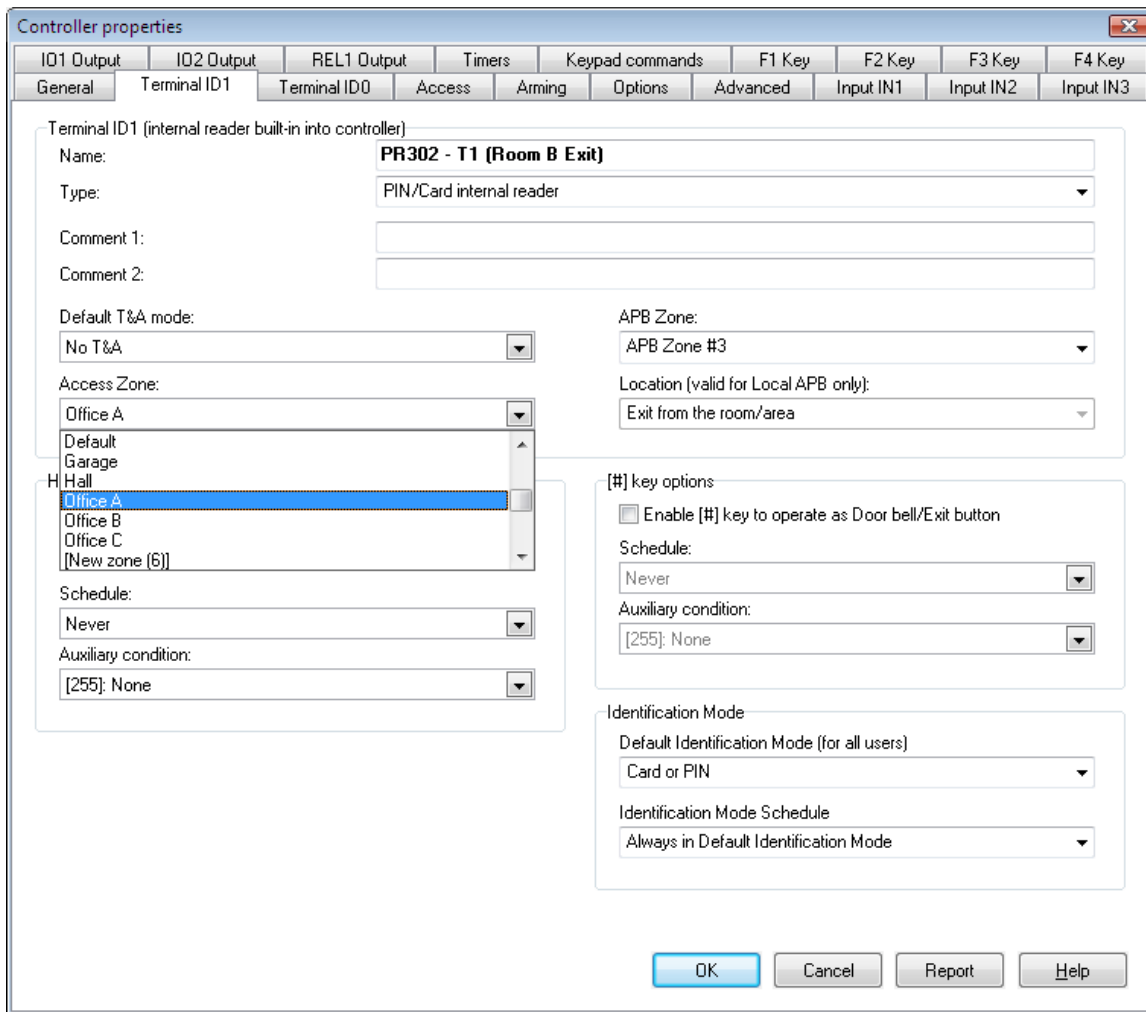
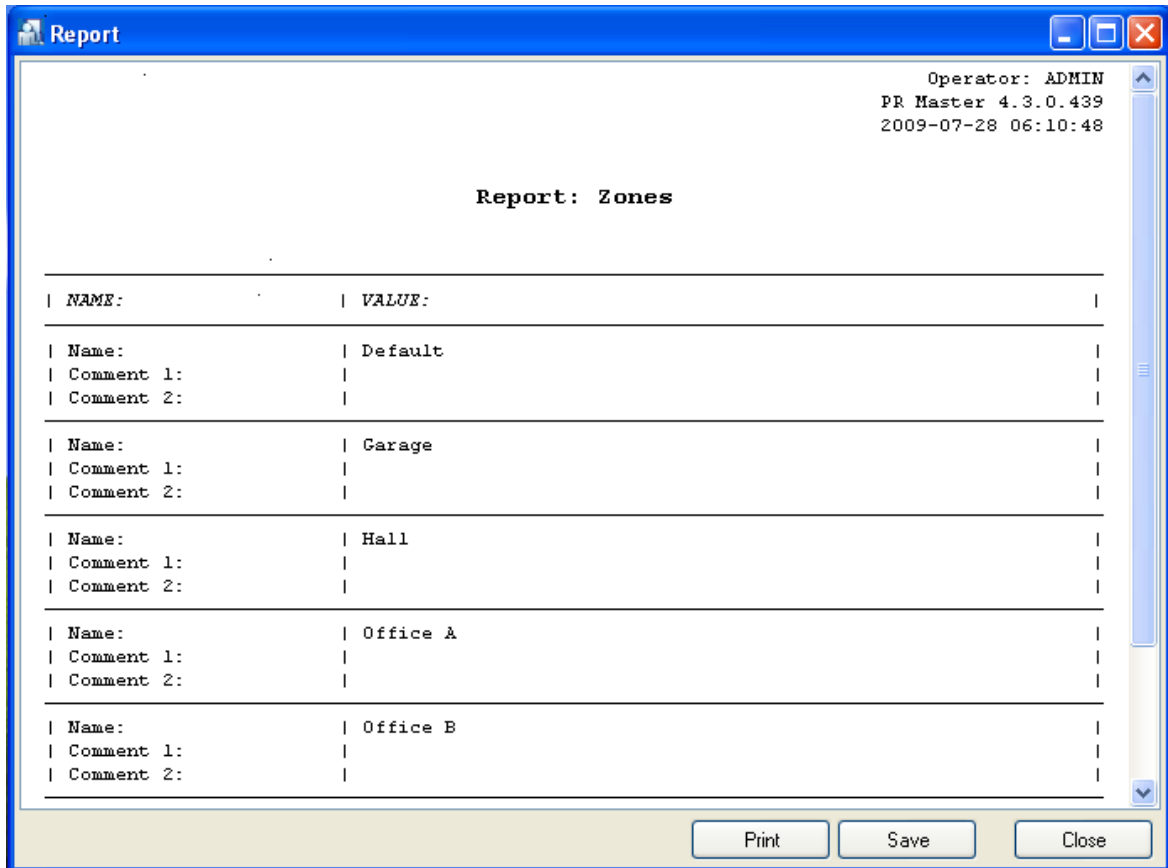


Figure 3.40. Assigning controller to the access zone — PR 302

### 3.2.6.4. 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 3.41).



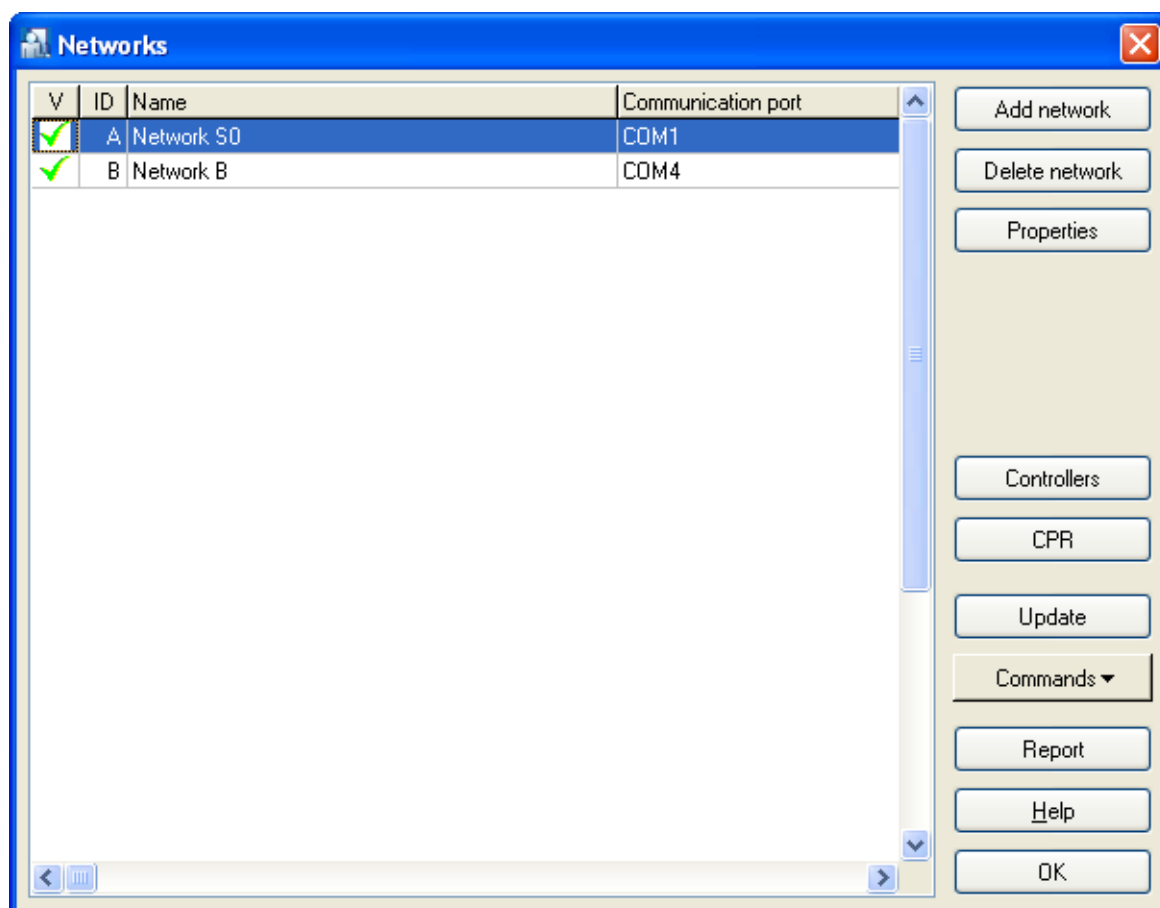
**Figure 3.41.** *The Zones report*

### 3.2.7. Networks

Roger Access Control System may consist of up to 100 networks. Each of it can contain up to 32 access controllers with terminals.

Each network is connected to the managing computer via serial port (physical or virtual) through specific communication interface (UT-2, UT-2USB or UT-4).

Selecting the **System/Networks** command causes displaying window containing a list with networks installed in the RACS (Figure 3.42).



**Figure 3.42.** Network directory

From this window you can perform the following operations:

- ◆ adding a new network (the **Add** 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 CPR-32 network management unit's 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),

### 3.2.7.1. 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 3.43).

**Figure 3.43.** 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 management unit,
- ◆ select a network name (optionally with comments),
- ◆ assign a COM port (physical or virtual),
- ◆ indicate interface type.

You should pay special attention to the operations of assigning a COM 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 CPR 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 devices. Thus addresses conflicts may occur, for instance when detecting controllers.



If the CPR network management unit is connected while a new virtual serial port is being created (for instance for UT-4 or UT-2USB interfaces), Windows will 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 CPR while a virtual serial port is being installed.

## Types of interfaces

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, special communication interfaces are being used:

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

Furthermore, because of many different communication conditions which may occur (in particular delays), in case of UT-4 interface you should indicate if it is used in LAN or WAN and what device version is being used.

## Virtual Serial Ports Setup

If the particular network is to be connected through a physical serial port, the only things to do is to connect the network to the computer through the physical port, set the communication port as the selected physical serial port (e.g. COM1) in the **Network properties** window and start to communicate. Because of a USB port features (its ability to hot-plug devices), the process of connection the network is similar also in case of an UT-2USB interface. Upon connecting the network through the USB, Windows will detect drivers and install appropriate software. 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.

In order to install the virtual serial port driver, you should utilize the **Digi Configurator** tool available in the Roger ACS program group (**Start/All programs/Roger ACS 4.3**). 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.

### 3.2.7.2. Removing Networks

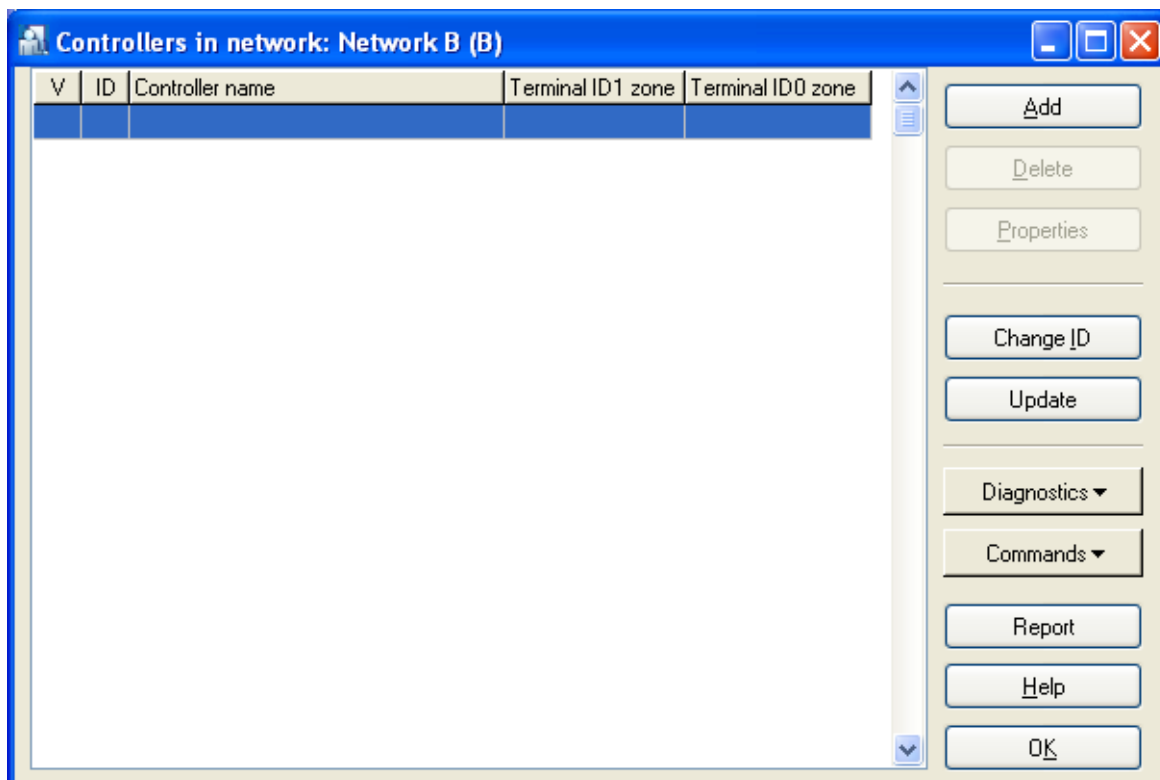
In order to remove a network, you should use the **Delete network** button in the **Networks** window (Figure 3.44). If the network contain any controllers, then selecting this command will display a warning informing about a need to remove all the controllers for the particular network. It can be done 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.

### 3.2.7.3. 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 (Figure 3.20). 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. You can also display report describing particular network properties.

### 3.2.7.4. 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 3.44).



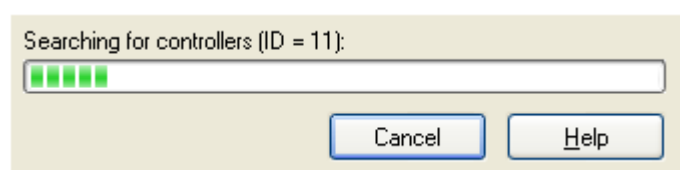
**Figure 3.44.** The list of controllers in the network — immediately after defining a new network it is empty

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 3.45).



**Figure 3.45.** Searching for controllers in the network

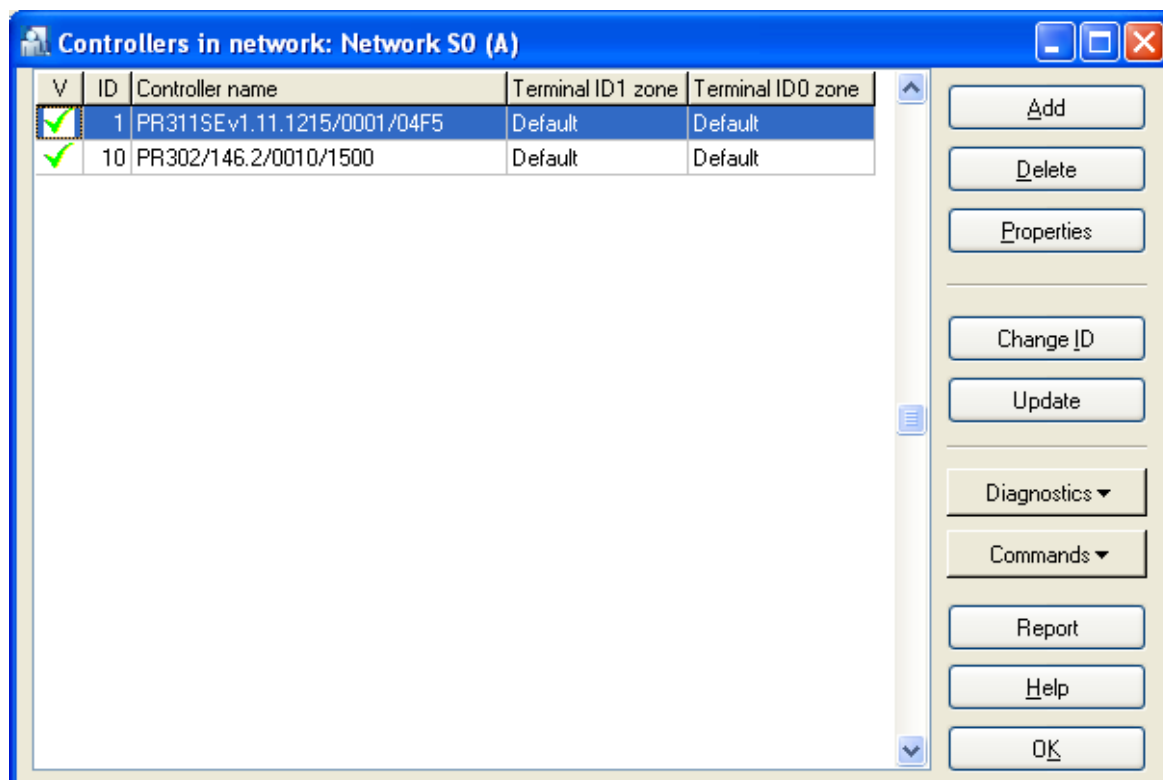


The controllers found are immediately displayed in the network's controllers directory. An installer can break the searching process at any time (e.g. if in his/her opinion all the controllers have been found) by clicking on the **Cancel** button. If the process of searching is not interrupted, the system will search addresses in the range from 00 to 1000 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 informing about the CPR in the system.

Upon completion operation of adding controllers, the window with controllers can have a form as shown in Figure 3.46.



**Figure 3.46.** The controllers list upon completion the searching for controllers operation

As you may notice, 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

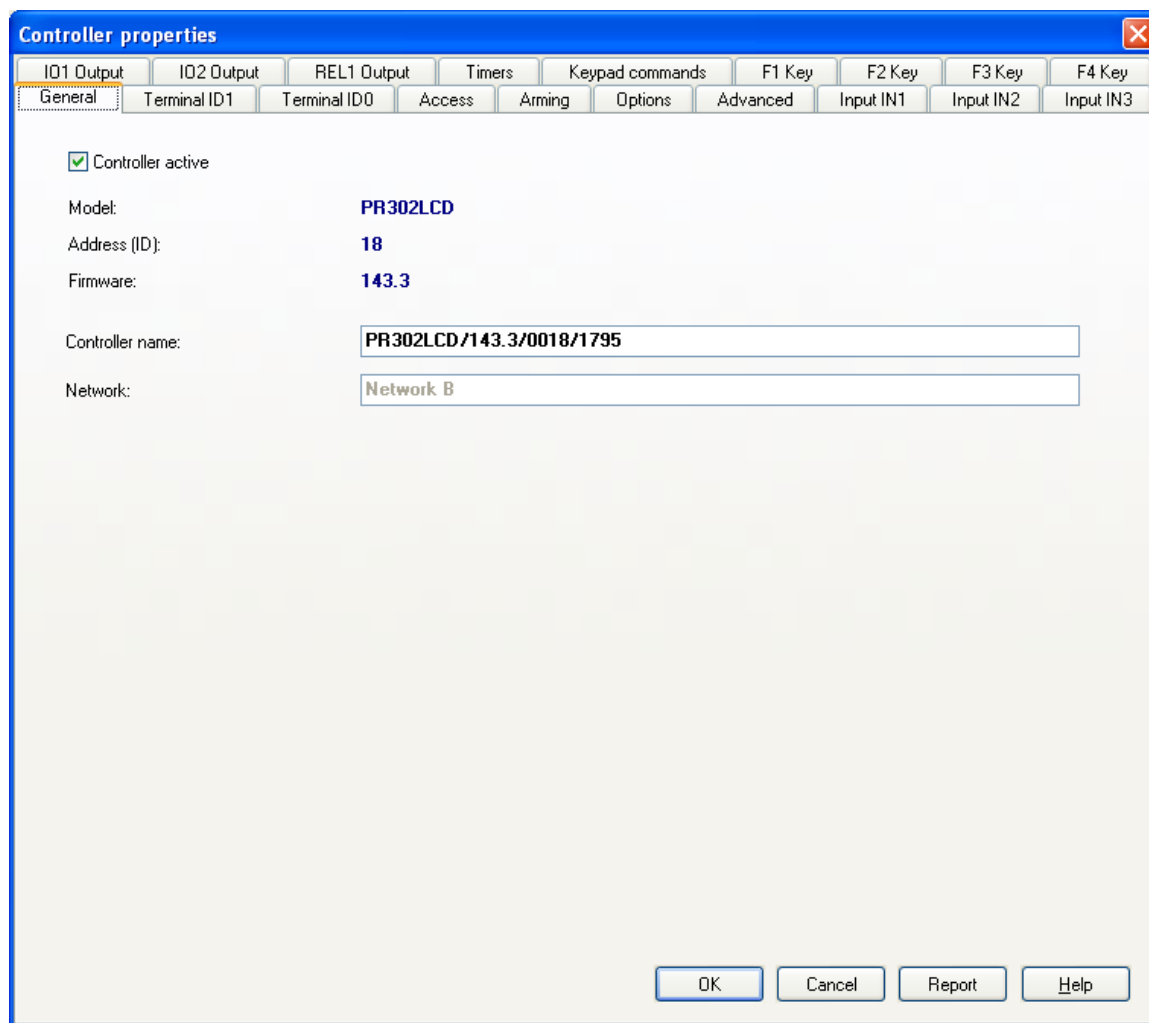
In order to delete controller from the network you should click on the **Delete** button. As usual, before the controller is deleted, the system will display a confirmation question asking if you are sure to delete the controller. If you answer **Yes**, the controller will be deleted.



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 PR302LCD controller has been shown in figure 3.47.



**Figure 3.47.** PR302 LCD controller properties

As you can notice in figure, 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.

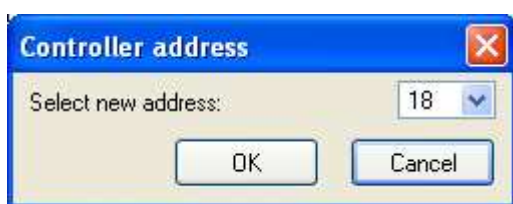


A detailed description of all the settings for many different controller types is outside the scope for this manual. In most cases default settings will be sufficient to utilize controllers in physical installations. A detailed information about all the configuration options can be found in the manual for the specific controller.

### Changing Controller's ID Address

All the controllers manufactured by Roger have a factory default ID=0. 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 ways for changing devices addresses available. One of possible options is to make use of PR Master 4.3 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 3.48).

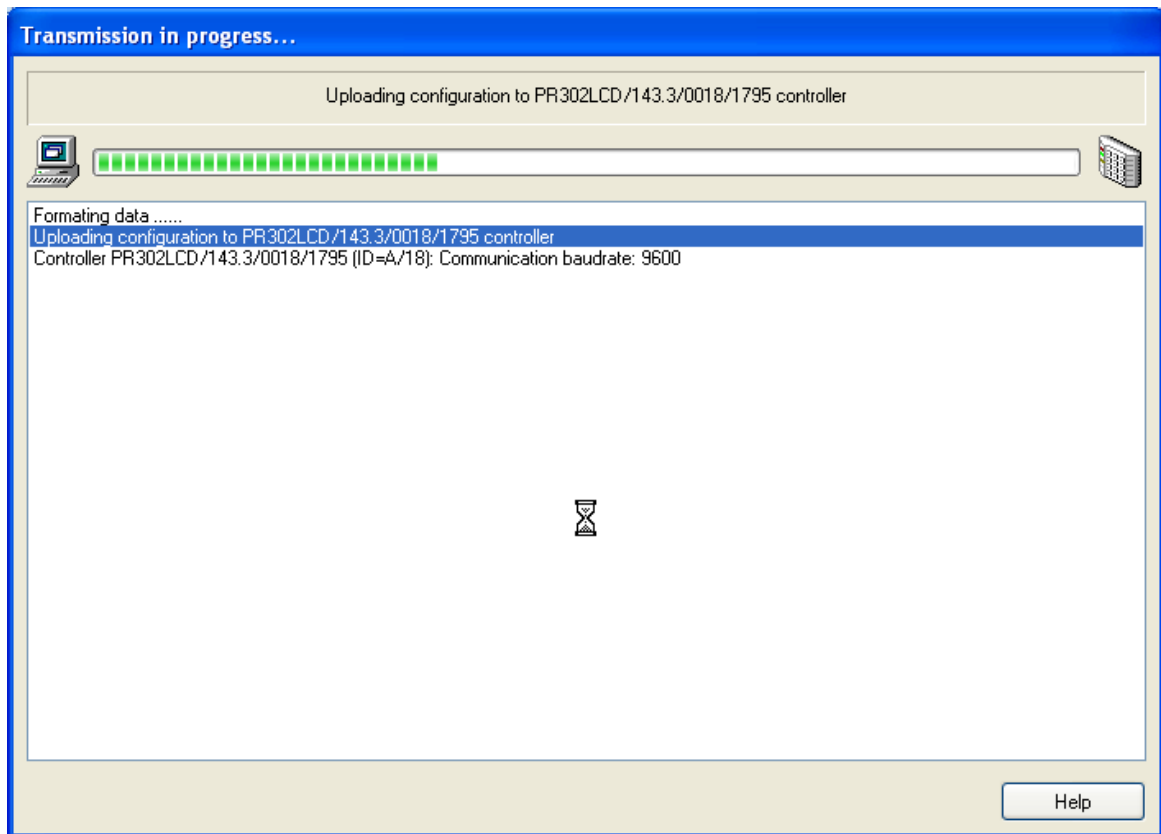


**Figure 3.48.** Changing Controller's ID Address

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 3.49). When the transmission is completed, the system displays a window with information about transmission result (Figure 3.50).



**Figure 3.49.** Sending configuration settings to the selected controller



**Figure 3.50.** Success! We have sent settings to controller

### Performing Diagnostic Operations

The **Diagnostics** button gives access to the diagnostic operations menu (Figure 3.51). 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-32 network management unit and controllers, perform communication bus interference test, and make full or quick flash memory test.

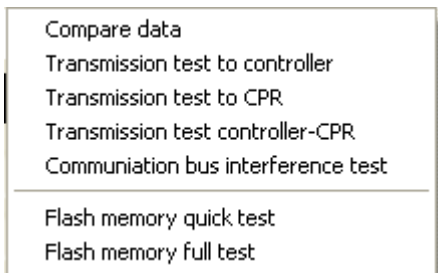


Figure 3.51. Diagnostic menu

Most of the communication tests available from this menu are performed at the communication protocol level. Because the RACS is very resistant to interferences, the tests may give satisfactory results even if there are serious electrical interferences on the bus (Figure 3.52).

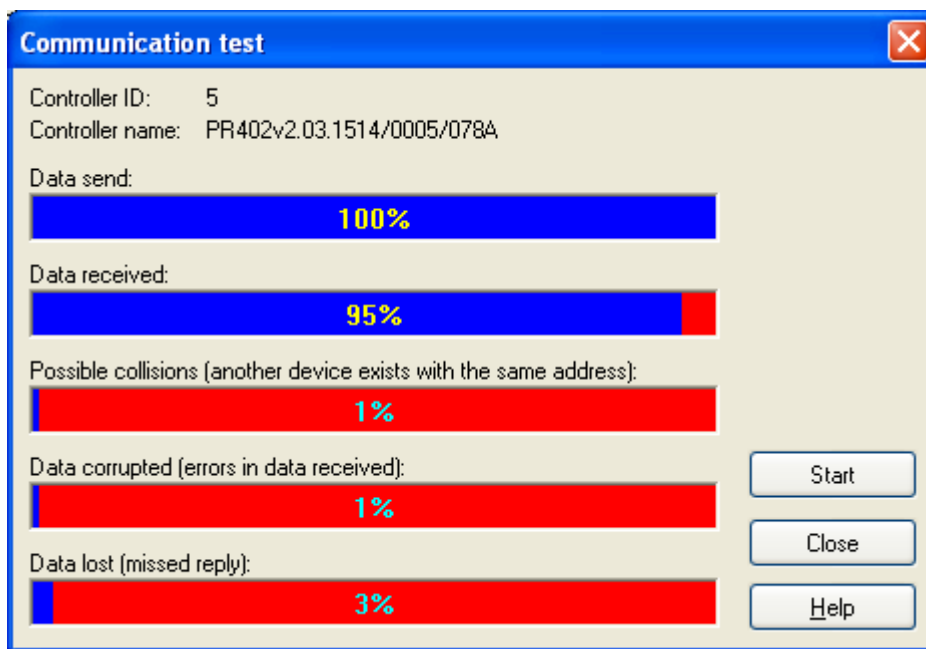
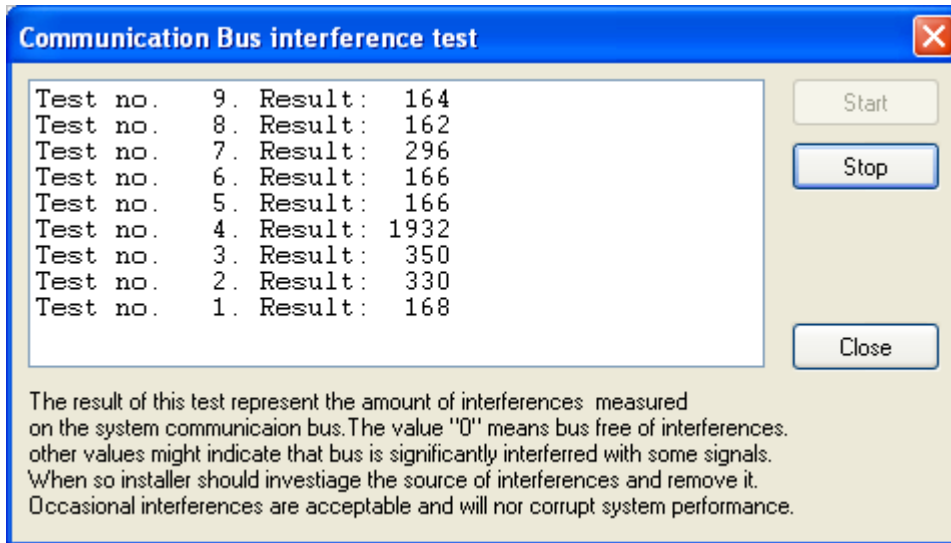


Figure 3.52. Communication test with the controller — despite of interferences, 95% of packets have been received

A most accurate test allowing for detecting electrical problems on the bus is a **Communication bus interference test** (Figure 3.53). High numbers of state changes in the tests results is an evidence that there are interferences on the bus.



An interference test for the RS485 bus is not available for all the controllers but only for the newest models updated to a newest firmware.



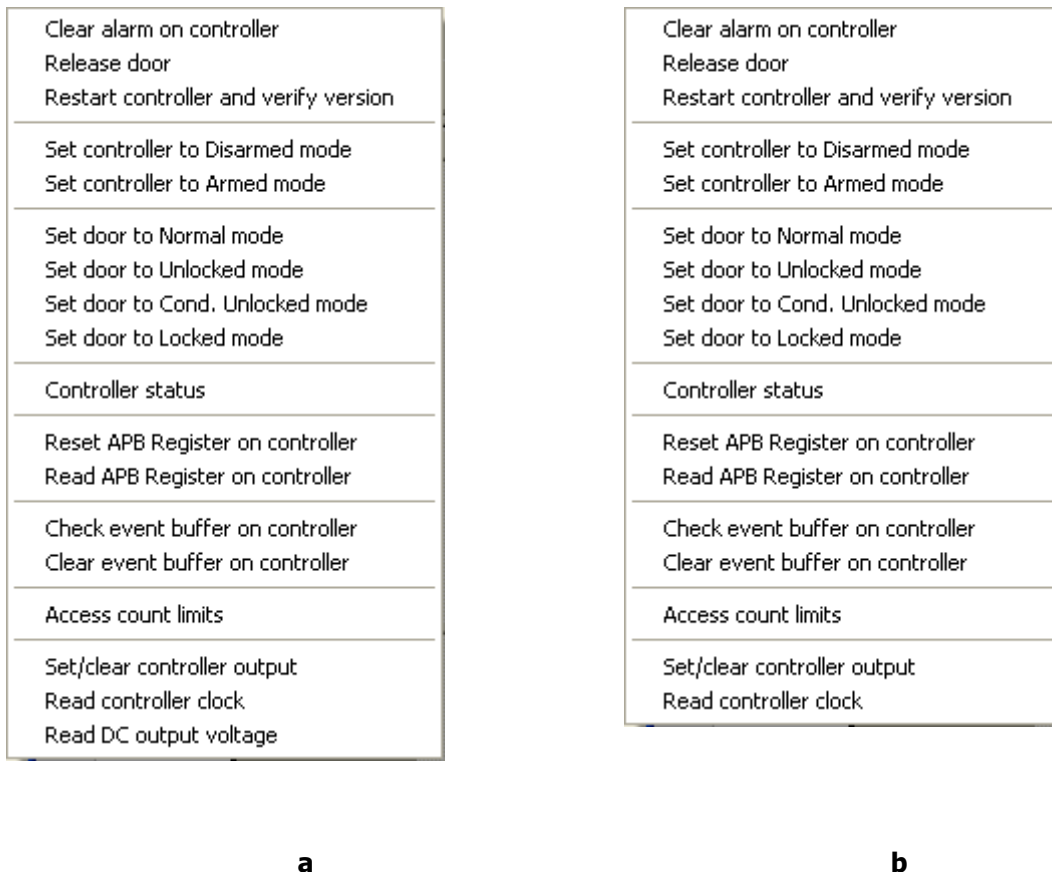
**Figure 3.53.** RS485 bus interference test — number of state changes more than zero indicates communication problems



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-32 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 3.46). The content of the **Command** menu may vary, depending on the controller type. The **Commands** menu for the PR 402 controller has been shown in figure 3.54a, whereas in figure 3.54b an analogous menu for the PR 302 LCD controller has been presented.



**Figure 3.54.** Commands menu (a) PR 402 controller; (b) PR 302 LCD controller

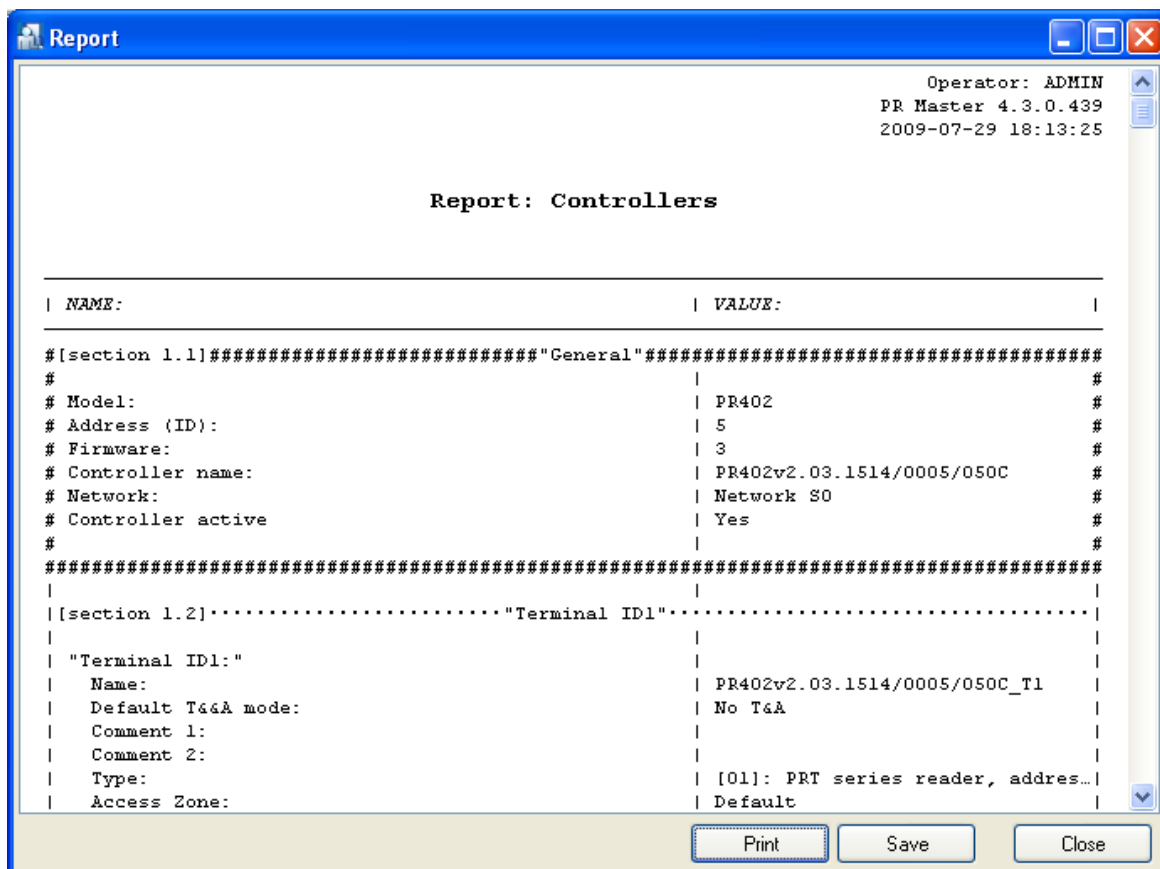
As you can see, the **Commands** menu for the PR 402 controller contains an additional **Read DC output voltage** command, which is not available for the PR 302 LCD controller.



A detailed description of all the settings and taking into account all the controller types is outside the scope of this manual. A detailed information about all the commands can be found in the manual for the specific controller.

### 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 3.55).



**Figure 3.55.** *Controllers report*

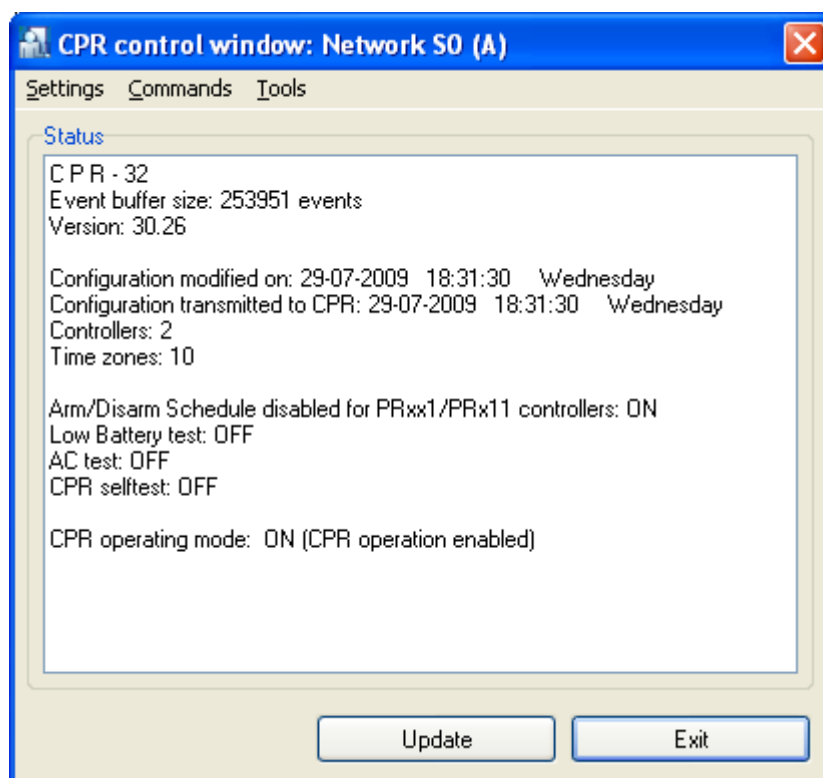
The **Controllers** report contain detailed information regarding configuration of the specific controller. Upon successful system configuration it is worth preparing a printed report for such a system. It may be helpful when troubleshooting problems at the later stage of system in production

### 3.2.7.5. Displaying CPR-32 Settings

CPR-32 network management unit is a device which is used in the RACS as an external event buffer. It synchronizes time settings on controllers and manages user rights on PRxx1 series controllers. Presence of CPR network management unit in the RACS is optional and results from functional requirements for the specific installation.

For displaying CPR-32 network management unit's settings, the **CPR** button can be used. If the network is not equipped with the CPR-32, this button is disabled. Clicking on this button causes displaying a dialog box containing settings for CPR-32 network management unit working in the network (Figure 3.56).





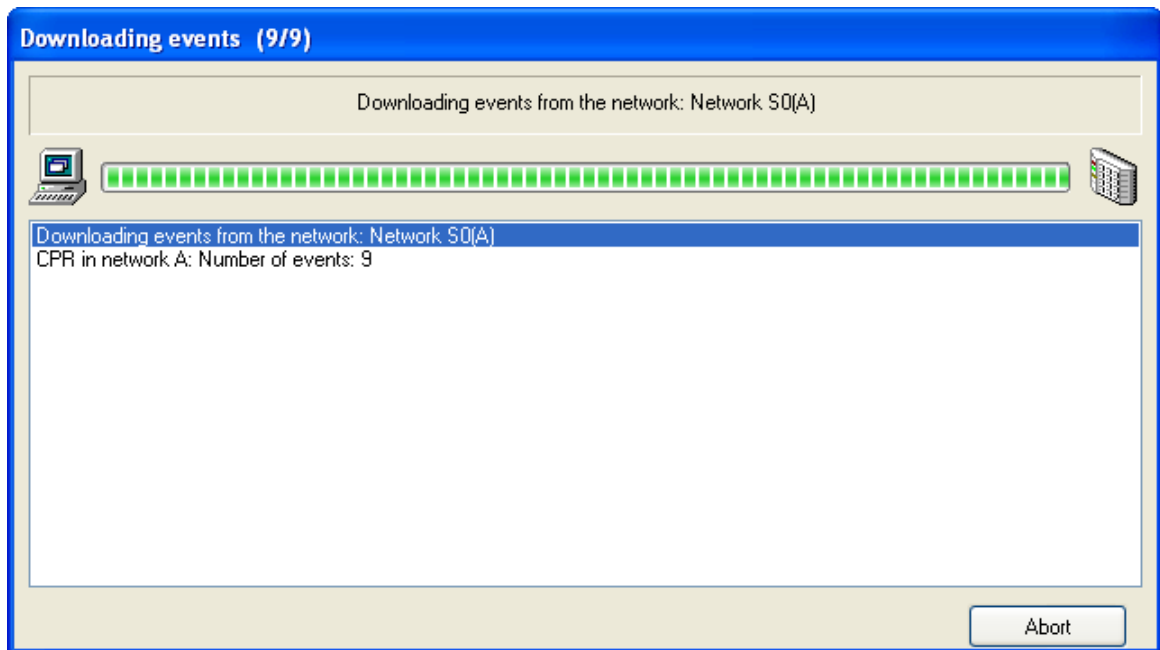
**Figure 3.56.** CPR-32 network management unit settings

An user can look at present settings and click **Exit** or he/(she) can select the **Update** button in order to send settings from the PR Master to the CPR-32 network management unit.

### 3.2.7.6. Sending Settings to Controllers and Network Unit

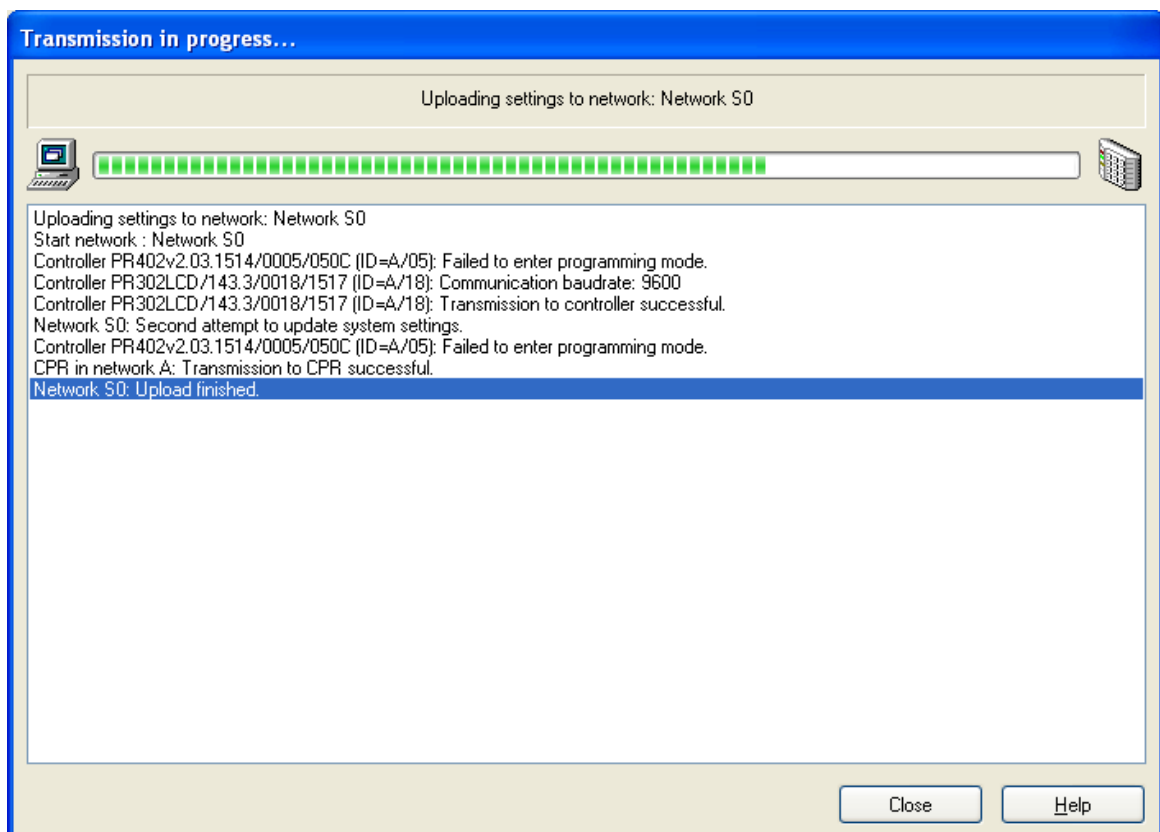
The **Update** button in the network directory is used for sending settings to all the controllers and CPR-32 unit in the selected network. In case when the network contain many controllers, this operation can take a long time. Because of this it should be initiated as rarely as possible.

Operation of sending settings to controllers is initiated by clicking on the **Update** button. If at this moment there are any events collected in the controller or the CPR, the system before performing an actual update will download them to database. While downloading events, the system displays information window containing data on reading operation progress (Figure 3.57).



**Figure 3.57.** Reading events from the network before sending settings to it

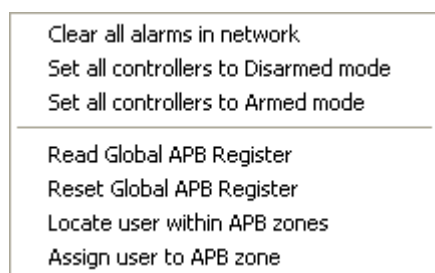
After displaying a message on completing reading events, the system proceeds to sending data to devices in the network (Figure 3.58).



**Figure 3.58.** Sending Settings to the network — the operation progress window

### 3.2.7.7. Executing Commands for the Network

The **Commands** button in the **Networks** directory shows commands menu (Figure 3.59) which allows for executing commands for the network.



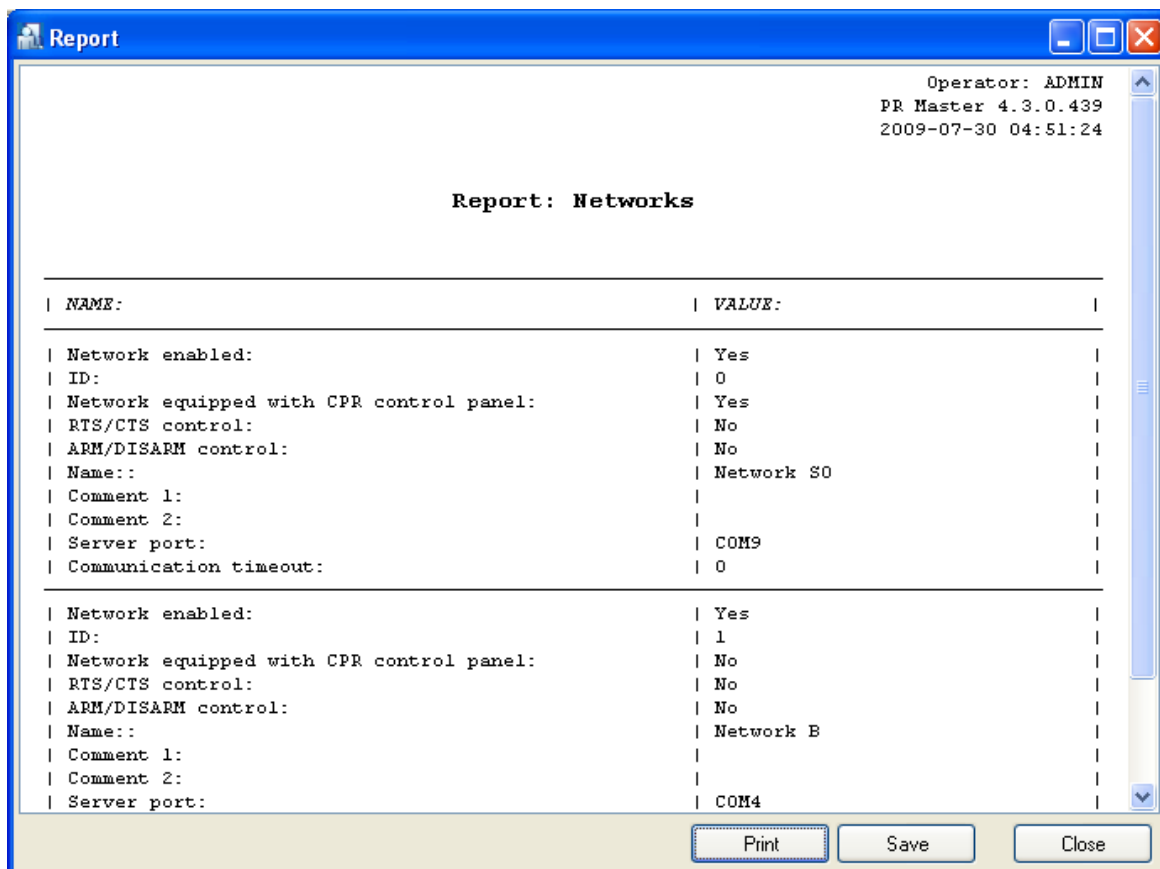
**Figure 3.59.** *Commands menu in the network's directory*

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 can not 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.

### 3.2.7.8. Generating Networks Report

The **Report** button in the **Networks** directory allows to generate summary report related to networks defined in the RACS. Sample report has been shown in Figure 3.60.



**Figure 3.60.** Networks report

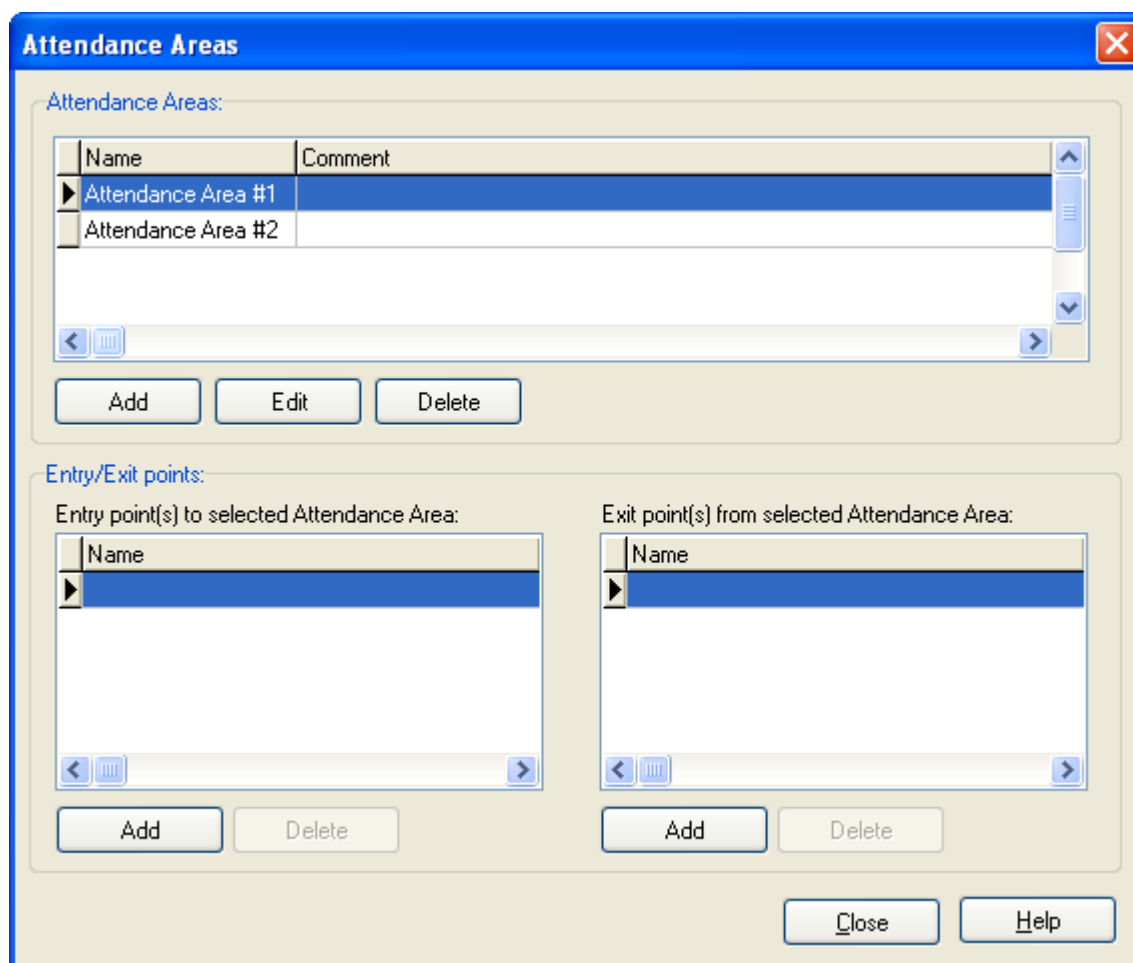
### 3.2.8. Attendance Areas

**Attendance areas** is one of the RACS'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 to through a set of identification points, and you can leave by a separate set of 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), system user's attendance reports do not base on T&A mode declarations, but only on defining, what reading device is responsible for entering to, and what for exiting from the area. Based on attendance report you can compute total time, employer was present in a particular area (e.g. in the production hall).

If you select the [Attendance Areas](#) command, the [Attendance Areas](#) dialog box opens (Figure 3.61).



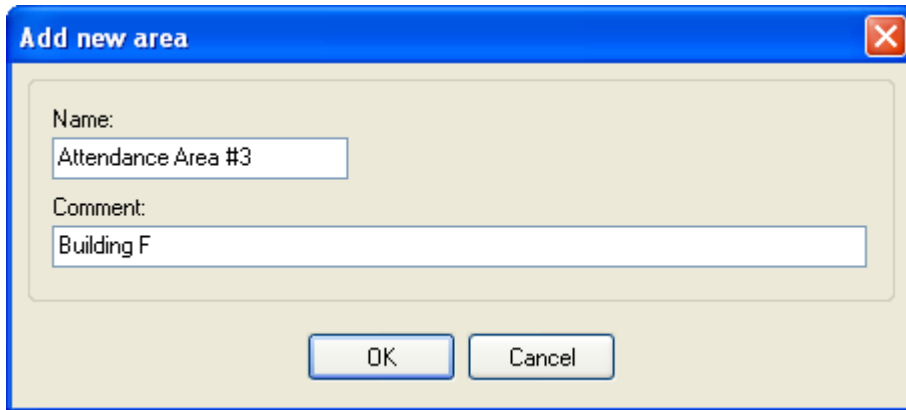
**Figure 3.61.** *Attendance Areas directory*

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.

### 3.2.8.1. 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 3.62). You should give a name to the attendance area, enter a descriptive comment and click **OK**.

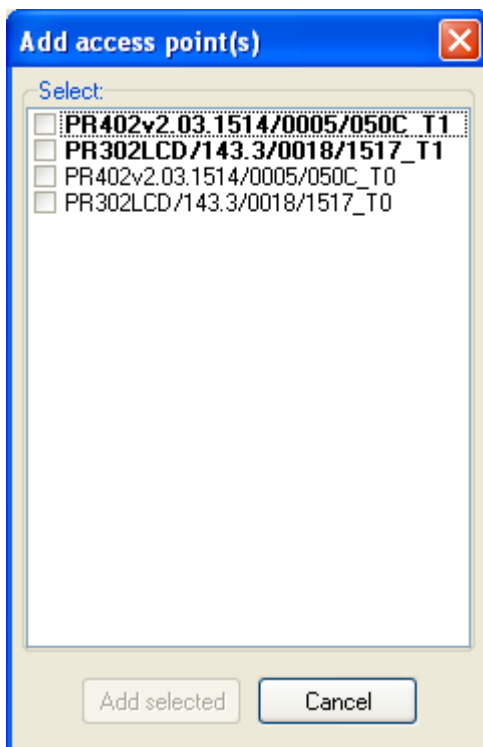


**Figure 3.62.** Adding a new attendance area

### 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 3.63).



**Figure 3.63.** Adding entry points to attendance area

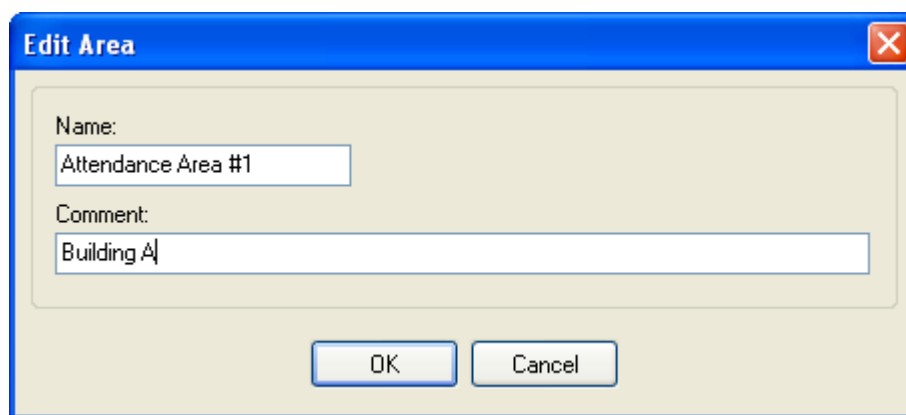
In the list there are all identifications point, which up to this point has not been assigned as entry points to the attendance area selected. T1 terminals of all the controllers in the system are displayed in bold. Adding a new entry point to selected attendance area is as simple as selecting check 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 3.63. 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.

### 3.2.8.2. 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 3.64). In this dialog box you can change a name or a descriptive comment related to the attendance area selected.



**Figure 3.64.** *Modifying existing attendance area*

### 3.2.8.3. 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

### 3.2.9. APB Zones

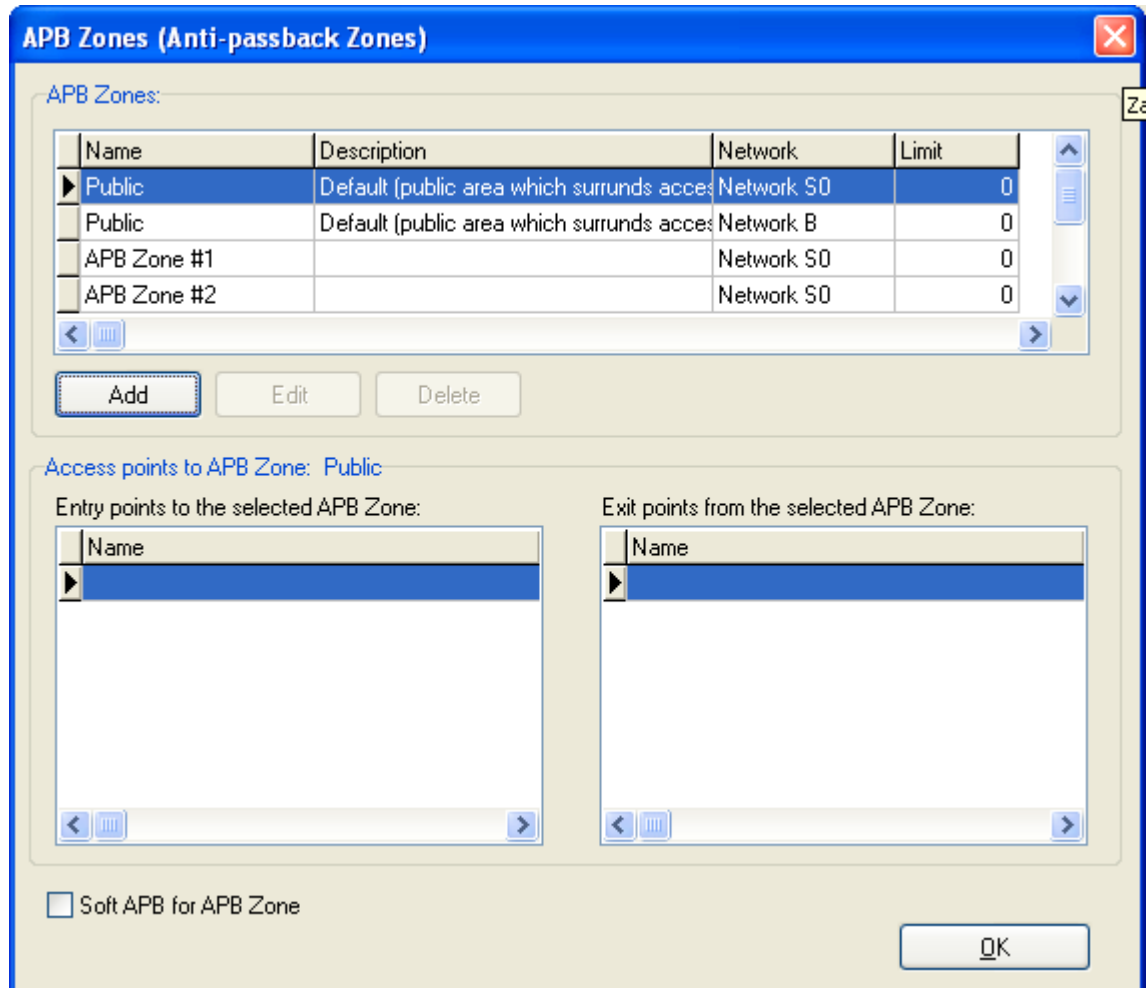
The purpose of the Anti-Passback feature is to protect against the possibility to use an user credentials at entry to the zone if it had not been used at exit before. To put it differently, the user can not enter the APB zone if he had not left it before. The function is aimed to protect against the possibility that one user passes its card to another user to allow him to enter the zone.

Defining the APB zone is as simple as assigning a set of identification points controlling entry to the zone selected, and a group of identification points controlling an exit from the zone. If an user enters the particular APB zone, he will not be able to enter the same zone again before he does not

leave it earlier. To be more exactly, if user does not make use of a card on exit from the zone, nobody else using the same card will be able to enter the zone.

Additionally, you can specify limit of persons who are present inside the APB zone. The system keeps track of the number of persons present in particular APB zones. If the number of persons present in the zone at any moment reaches the specified limit, then no new user will be able to enter the zone, before some group of persons do not leave it earlier.

Selecting the **System/APB Zones** command causes displaying APB zones directory (Figure 3.65).



**Figure 3.65.** 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).

### 3.2.9.1. 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 3.66). 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 3.66.** 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 3.2.9.3](#)).

### 3.2.9.2. 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.

### 3.2.9.3. 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.

### 3.2.10. Alarm Zones

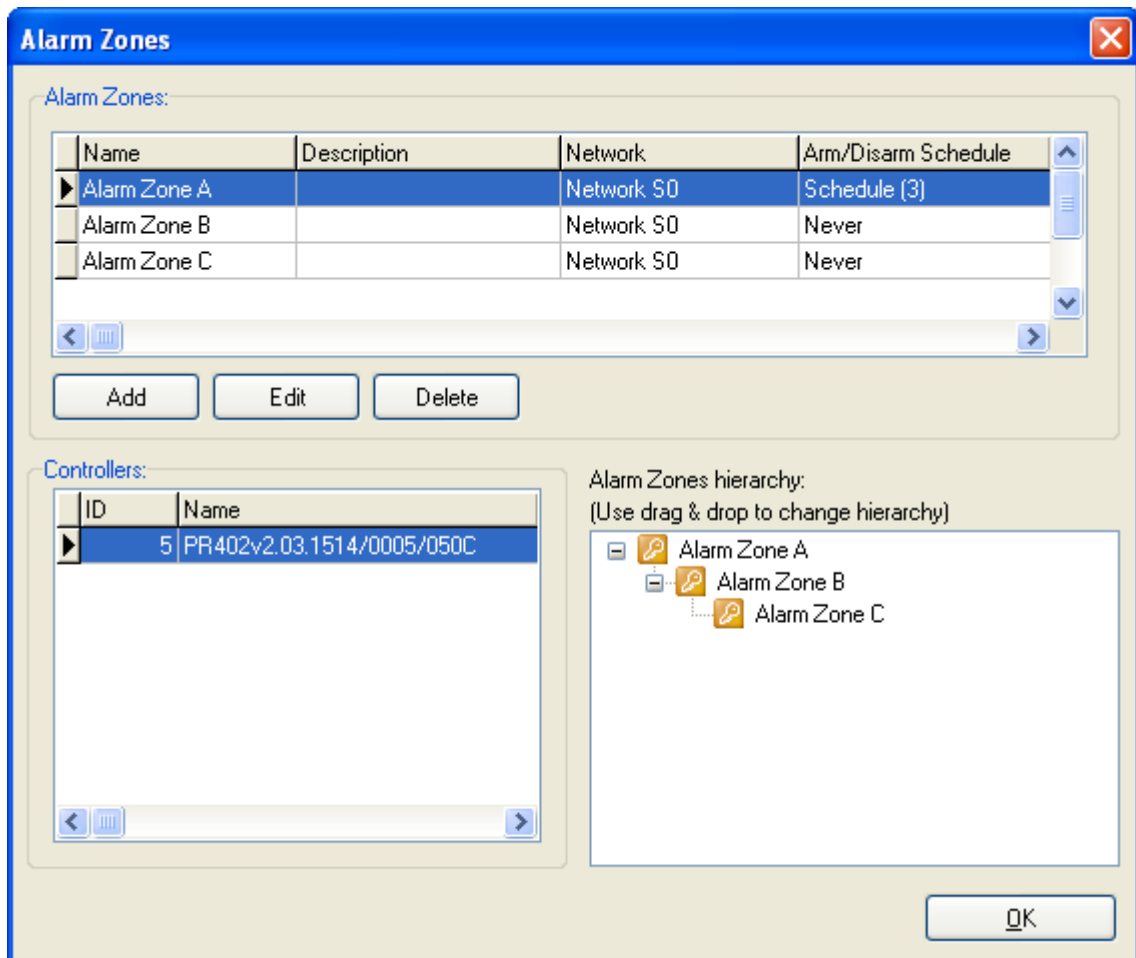
**Alarm zone** makes possible to designate a group of controllers, which will be armed/disarmed according to the defined schedule. It is also possible to define an alarm zones hierarchy. Thanks to this the controllers will be armed/disarmed in compliance with the hierarchy levels (parent-child).

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 3.67).

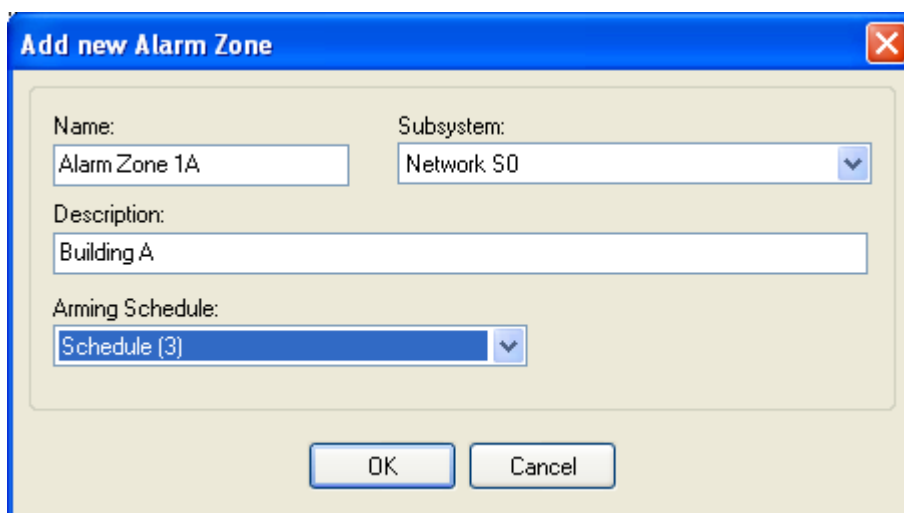


**Figure 3.67.** Alarm zones directory

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.

### 3.2.10.1. Adding a new alarm zone

In order to add a new alarm zone, you should click on the **Add** button. The **Add new Alarm Zone** dialog box displays (Figure 3.68). 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.



The screenshot shows a dialog box titled "Add new Alarm Zone". It has a blue title bar with a close button (X) in the top right corner. The dialog contains the following fields:

- Name:** A text box containing "Alarm Zone 1A".
- Subsystem:** A dropdown menu showing "Network S0".
- Description:** A text box containing "Building A".
- Arming Schedule:** A dropdown menu showing "Schedule (3)".

At the bottom of the dialog are two buttons: "OK" and "Cancel".

**Figure 3.68.** 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 3.2.10.3](#)).

### 3.2.10.2. Deleting Alarm Zone

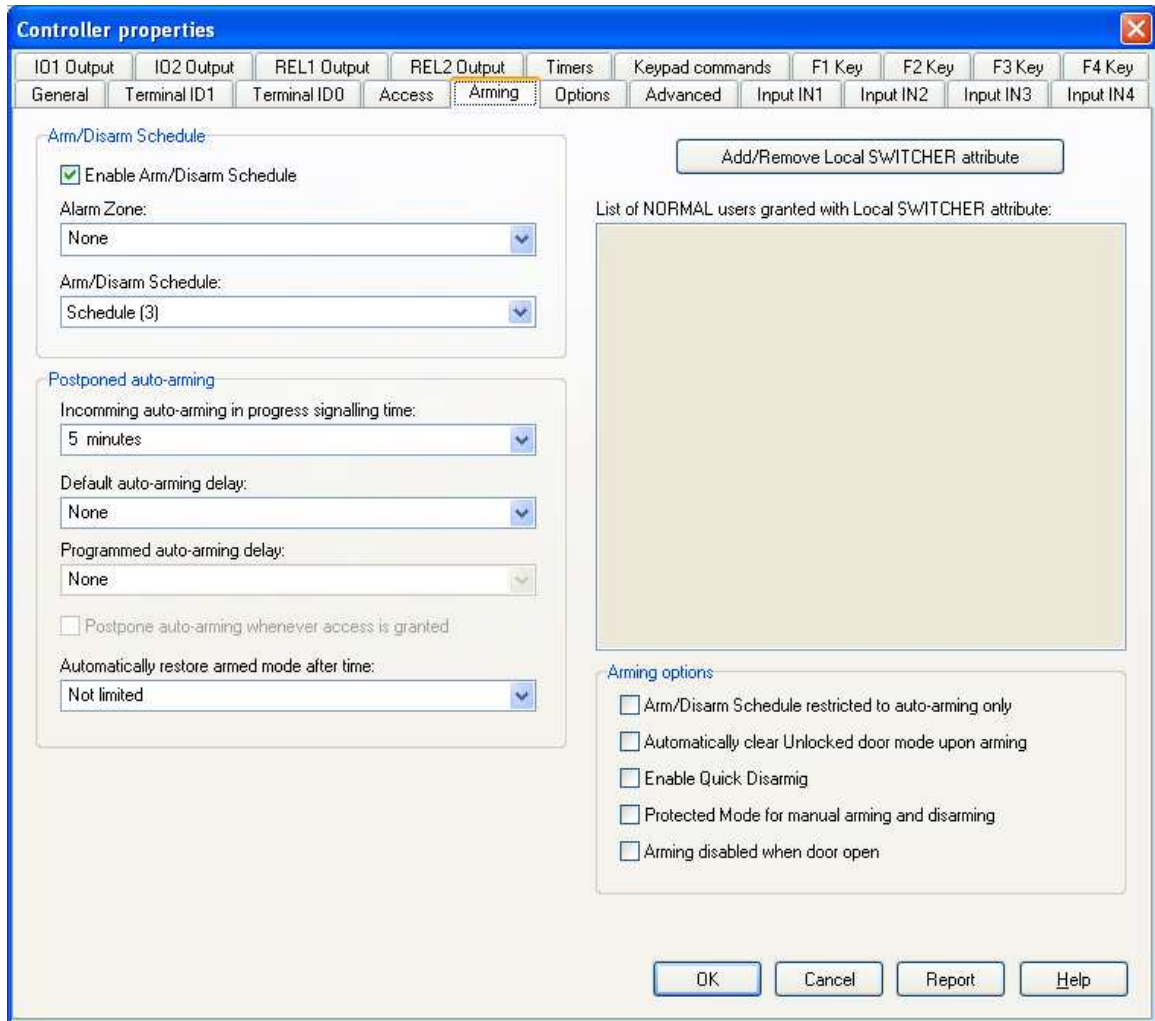
In order to delete alarm zone, you should click on the **Delete** button in the **Alarm Zones** dialog box. After the alarm zone is deleted, the system automatically cancels assignment of controllers which belonged to it before (the **None** setting).



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.

### 3.2.10.3. 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 3.69).



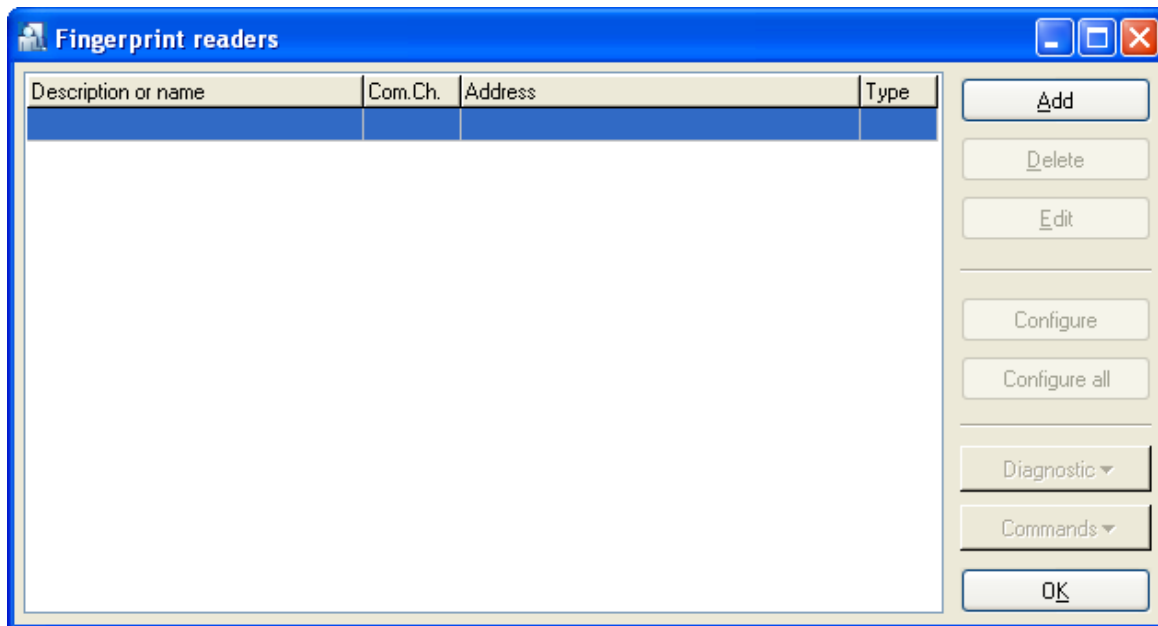
**Figure 3.69.** Assigning controller to alarm zone

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.

### 3.2.11. Fingerprint Readers

In the RACS it is also possible to use biometric readers F7, F8 and F10. Because these readers support Wiegand output format, they can be connected as slave device to PRxx2 series controllers.

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 3.70).



**Figure 3.70.** *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.

### 3.2.11.1. 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 3.71).

The dialog box titled "Fingerprint reader configuration" has a blue title bar with a close button. It contains the following fields:

- Description or name:** A text box containing "Fingerprint reader #1".
- Communication port:** A dropdown menu showing "COM3".
- Baud rate:** A dropdown menu showing "9600".
- Address (ID):** A text box containing "1".
- Password:** An empty text box.
- Type:** A dropdown menu showing "F10".

At the bottom right, there are "OK" and "Cancel" buttons.

**Figure 3.71.** Adding a new fingerprint reader connected through RS-485 serial bus

In this dialog box you should enter a fingerprint reader's name (the **Description or name** field), specify a serial port used for connecting the reader to the system (**Communication port** field), specify its ID address (**Address(ID)** field), optionally define a password giving an access to the reader (**Password** field) and select a reader type (**F7, F8 or F10** — **Type** field).

Fingerprint readers can be connected to RACS via RS-485 communication bus or via LAN. In the second case, you should select **TCP/IP** in the **Port** field. In such a case, the **Fingerprint reader configuration** dialog box will look a bit differently (Figure 3.72).

The dialog box titled "Fingerprint reader configuration" has a blue title bar with a close button. It contains the following fields:

- Description or name:** A text box containing "Fingerprint reader #1".
- Communication port:** A dropdown menu showing "TCP/IP".
- IP:** A text box containing "192.168. 1 . 10".
- Port:** A text box containing "4370".
- Password:** An empty text box.
- Type:** A dropdown menu showing "F10".

At the bottom right, there are "OK" and "Cancel" buttons.

**Figure 3.72.** Adding a new fingerprint reader connected through Ethernet LAN

In case the fingerprint reader is connected via Ethernet LAN, you should enter device's IP address and TCP port.

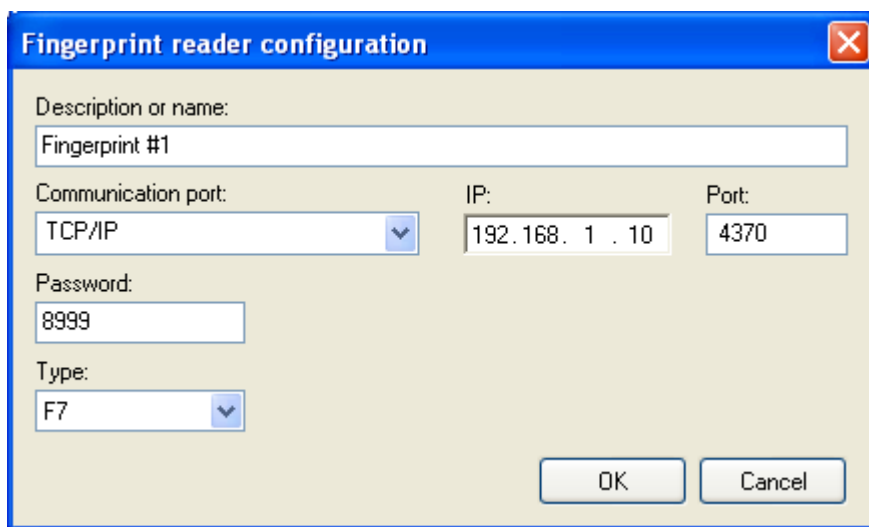
After adding a fingerprint reader to the system, it will show up in the list of fingerprint readers installed in the system (in the window shown in Figure 3.70). If the list of fingerprint readers is not empty, two additional buttons will be enabled: **Delete** and **Edit**. They allow for removing selected fingerprint reader from the system and changing its configuration respectively.

### 3.2.11.2. 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.

### 3.2.11.3. 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 used for connection or correct ID address and device type. Optionally you can also enter password (Figure 3.73).



**Figure 3.73.** *Modifying fingerprint readers' settings*

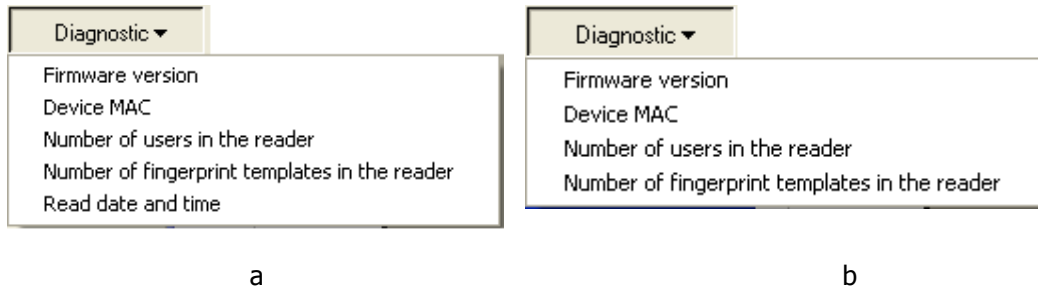
### 3.2.11.4. Configuring Selected Fingerprint Reader Or All the Fingerprint Readers in the System

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 on 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. .

### 3.2.11.6. Performing Diagnostic Operations

The **Diagnostics** button gives access to the diagnostic operations menu (Figure 3.74). From this menu you can perform various operations in order to verify system's operation correctness. You can read a reader's firmware version, its MAC number, number of users defined in a system, number of fingerprint patterns stored in the system. Furthermore you can read date and time from reader (the last option applies to the F7 reader type only). Diagnostic menu for F7 and F10 readers have been shown in Figures 3.74 a i b.



**Figure 3.74.** *Diagnostic operations menu — (a) F7 reader; (b) F10 reader*

### 3.2.11.7. 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 3.75.



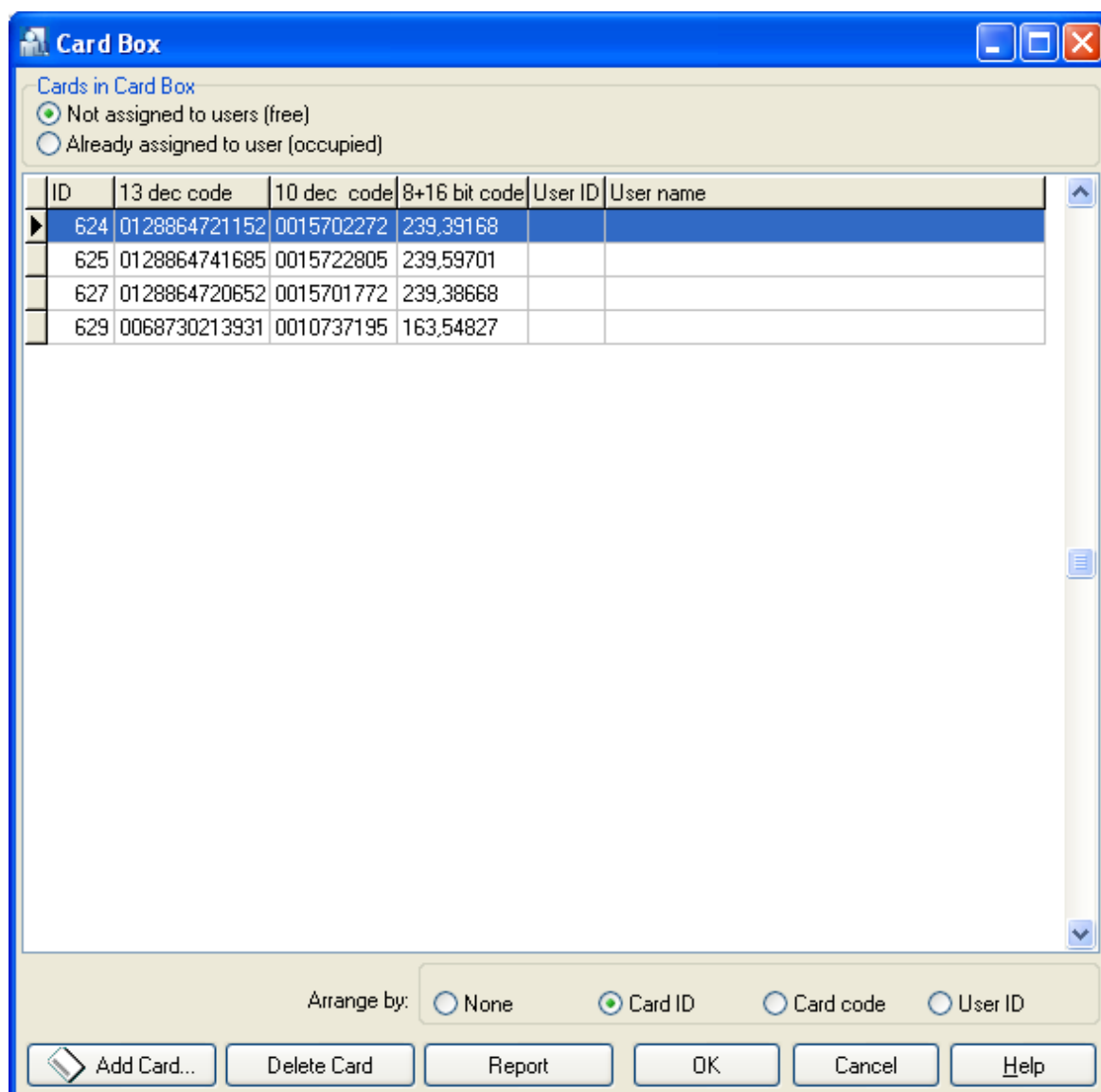
**Figure 3.75.** *The Commands menu allows to send commands to the selected fingerprint reader*

### 3.2.12. 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. 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 transponder in order to read card for him.

If you select this command, the dialog box with card directory displays (Figure 3.76).





**Figure 3.76.** Directory of proximity cards registered in the RACS

From this window you can perform the following operations:

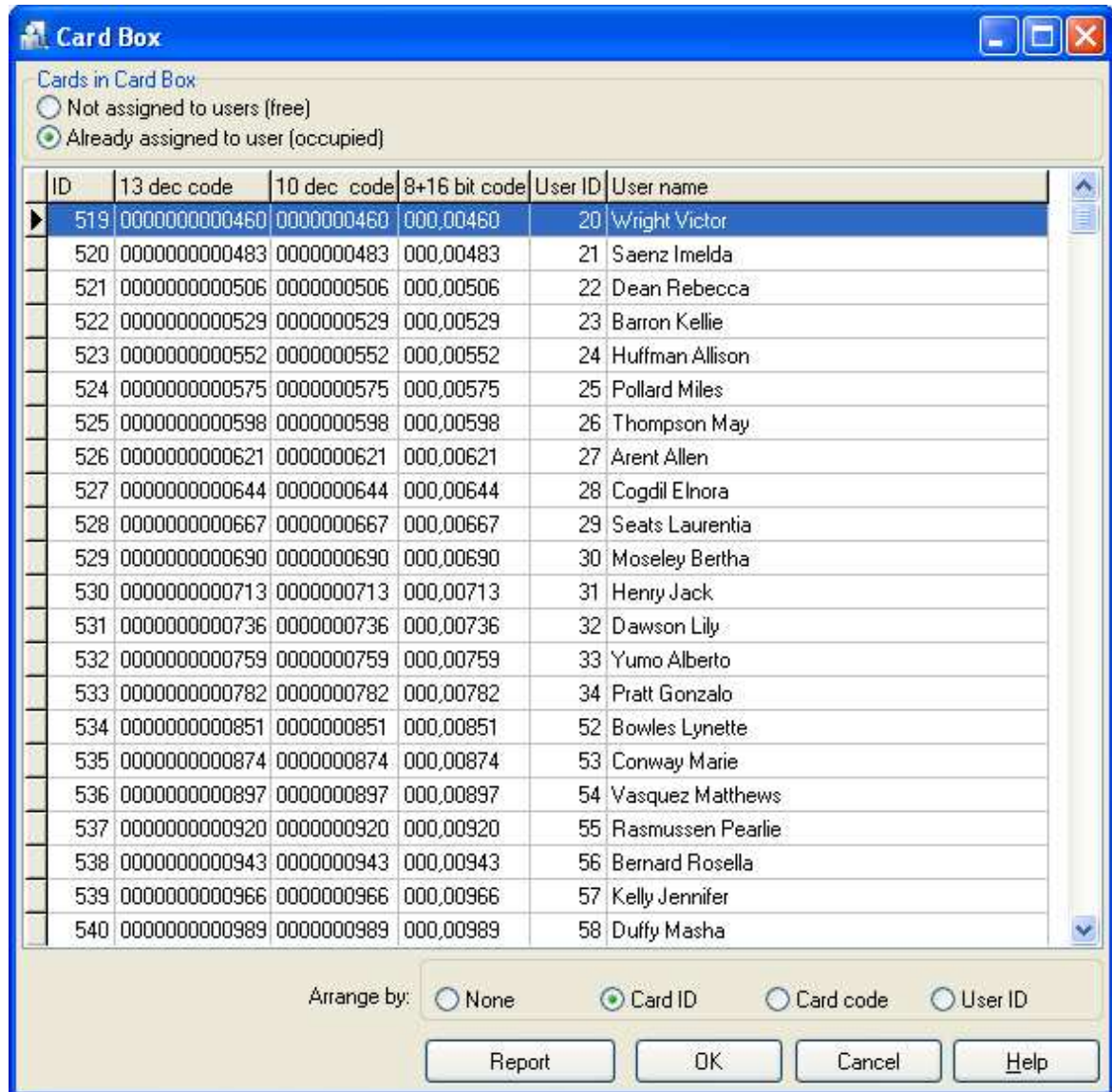
- ◆ display a list of unassigned cards existing in the system,
- ◆ show a list of cards which have been assigned to users,
- ◆ add a card to Card Box,
- ◆ sort a list according to the selected criteria,
- ◆ print report related to proximity cards registered in the system.

### 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(free)** 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 user(occupied)** radio button in the upper part of the dialog box. System will automatically display a list of cards assigned to users (Figure 3.77).

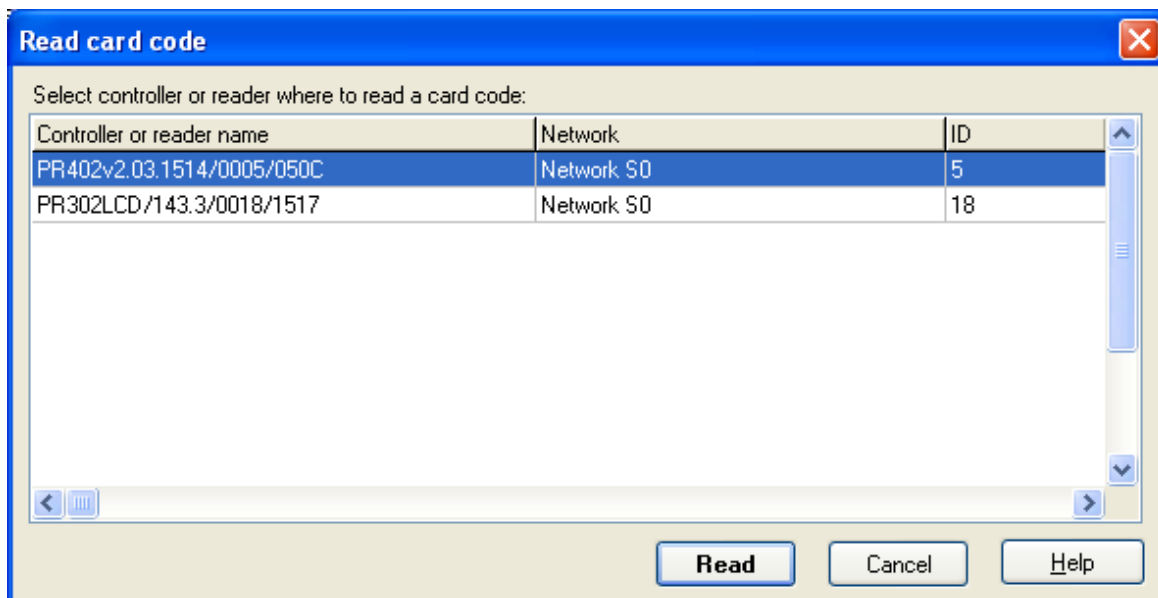


**Figure 3.77.** List of cards registered in the system which have been assigned to users

## Adding Card to Card Box

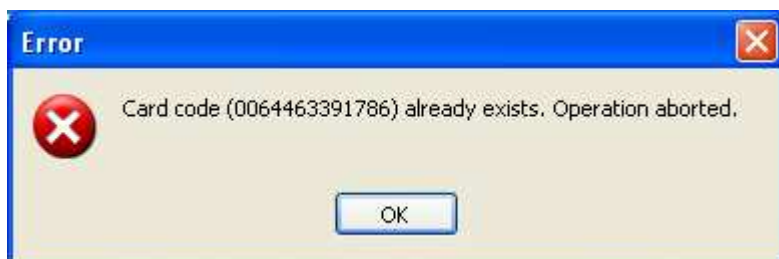
In order to add a new card to Card Box, first you should select the **Not assigned to users (free)** radio button. In reply, the program displays a list of cards which were registered in the system and not assigned to any user, and the **Add Card** button appears on the bottom.

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 3.78), where you can select reader used for reading a card.



**Figure 3.78.** 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 3.79):



**Figure 3.79.** 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 (free)** 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 adjusted using the **Arrange by** radio button. In order to sort cards according to the criteria selected, you should select a relevant radio button's value.

### 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 3.80.

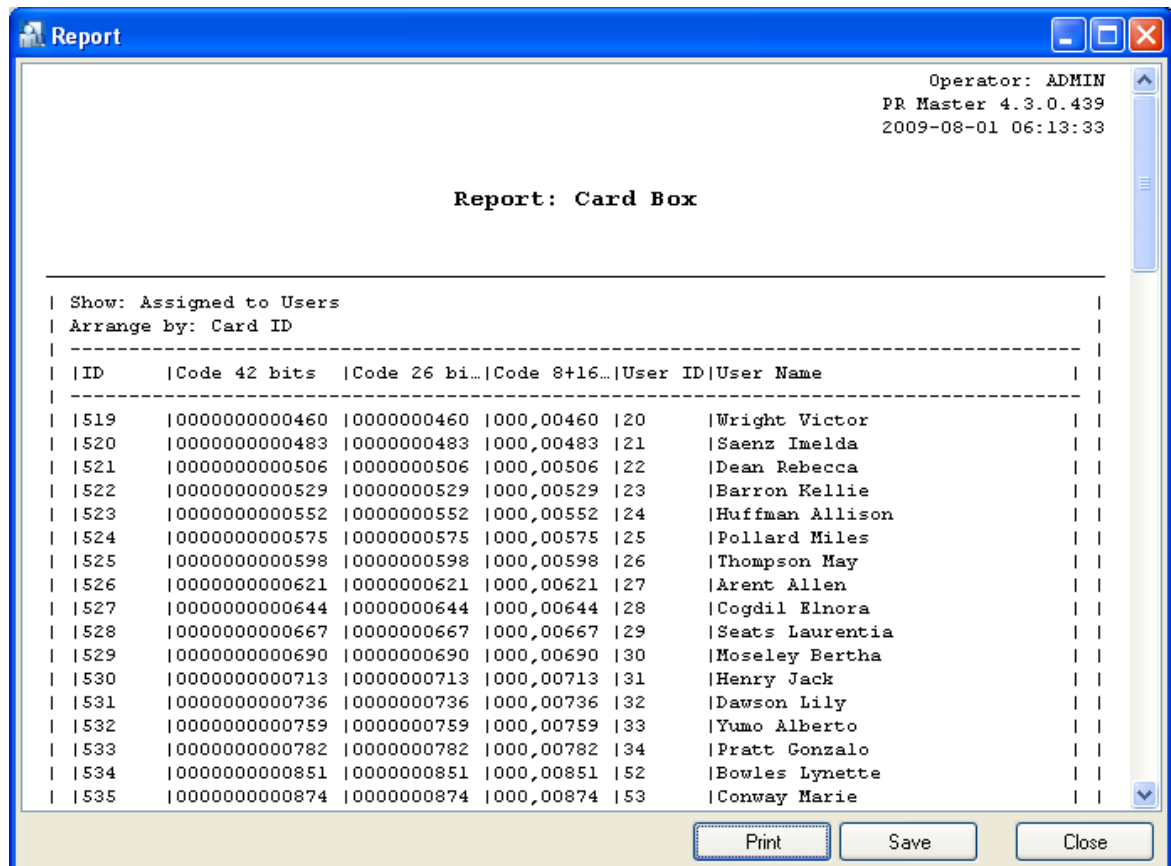
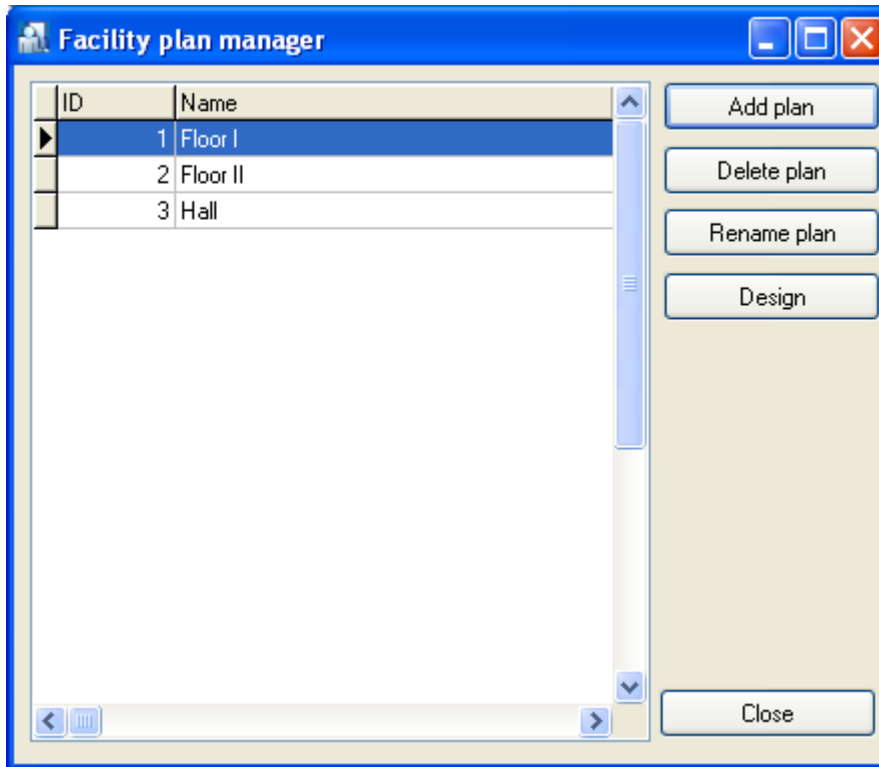


Figure 3.80. Report of proximity cards which were not assigned to system's users

### 3.2.13. Facility plans

The **Facility plans** command opens directory of facility plans defined in the RACS. The **Facility plan** is a graphic map (i.e construction design) on which selected controllers' icons were dislocated. Facility plans after they are defined can be utilized in PR Master's monitoring mode using the **View/View Map** command (see 4.1.13. View Map). You can define up to 20 separate facility plans in RACS.

Selecting the **Facility plan** command causes displaying window with facility plans directory (Figure 3.81).



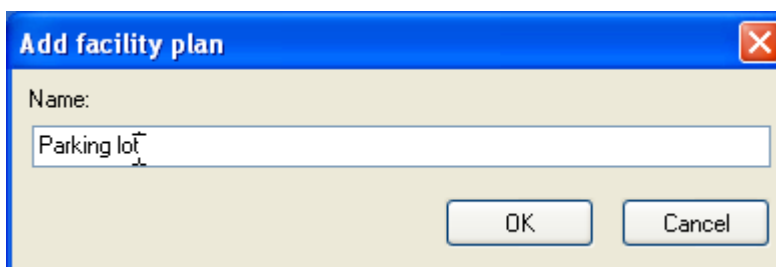
**Figure 3.81.** Facility plans directory

From this window you can perform the following operations:

- ◆ add a new facility plan — the **Add plan** button
- ◆ delete facility plan defined earlier — 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.

### 3.2.13.1. Adding new facility plan

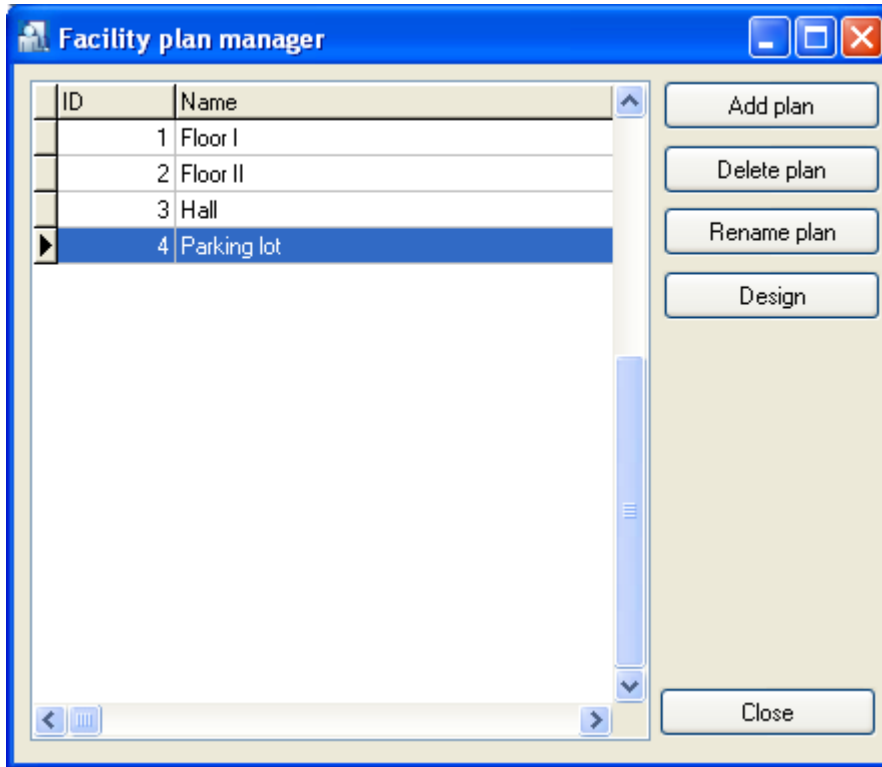
In order to add a new facility plan, you should click on the **Add plan** button. The **Add facility plan** dialog box displays (Figure 3.82).



**Figure 3.82.** 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. The name should uniquely indicate what plan we are thinking about. 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 3.83).



**Figure 3.83.** New plan — First floor — appeared as 4th in the list

### 3.2.13.2. Deleting facility plan

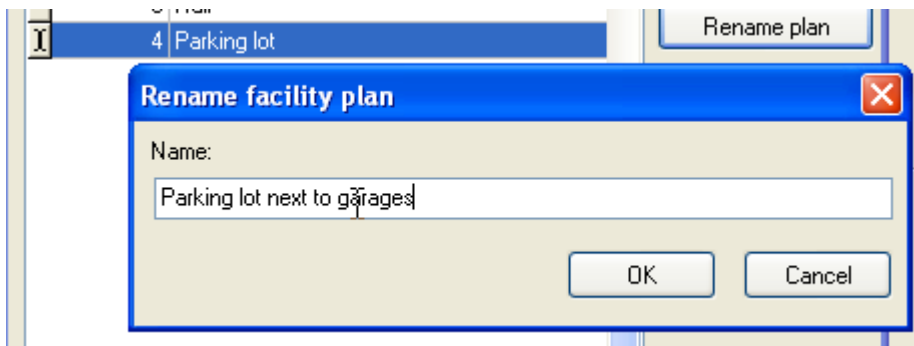
In order to delete facility plan you should click on the **Delete plan** button. The **Confirm** window asking for confirmation your intent to delete plan will appear. If you click **Yes**, the selected plan will be permanently deleted from database.



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](#).

### 3.2.13.3. Renaming facility plan

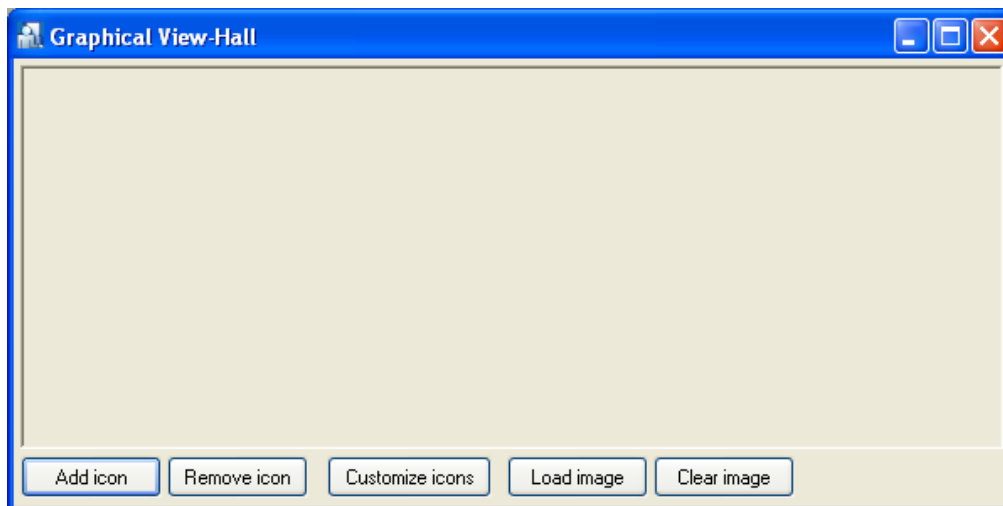
If you want to rename facility plan, you should click on the **Rename plan** button. The **Rename facility plan** dialog box displays (Figure 3.84). You should enter a new facility plan's name in it and then click **OK**.



**Figure 3.84.** Renaming facility plan

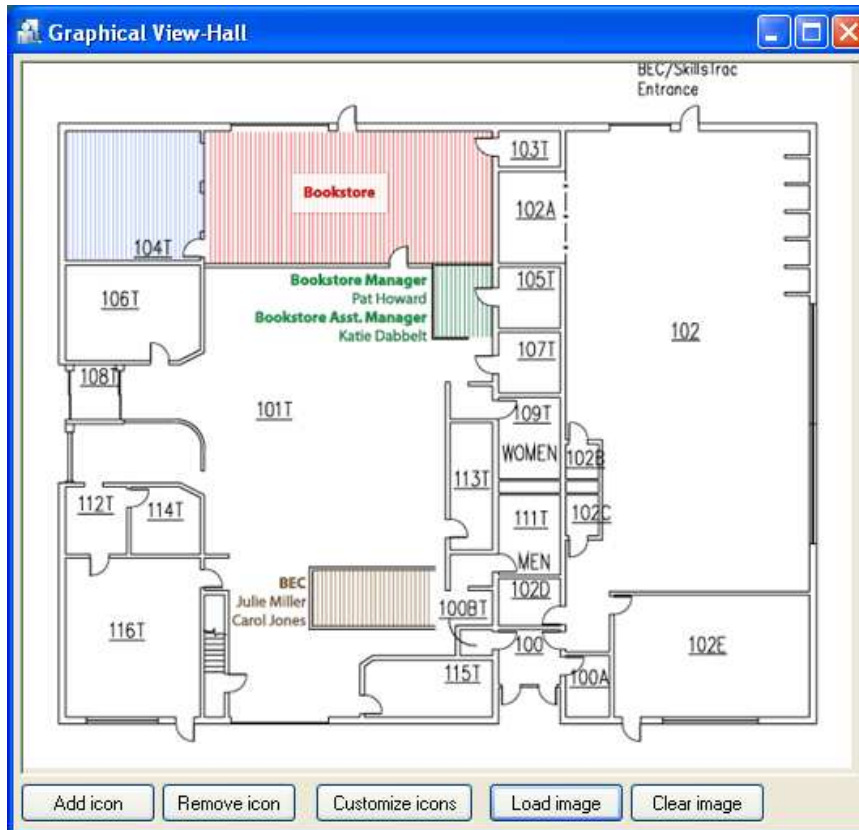
### 3.2.13.4. Designing facility plan

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 3.85.



**Figure 3.85.** *Designing facility plan — initial screen*

You should start designing a facility plan with 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. 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 3.86.



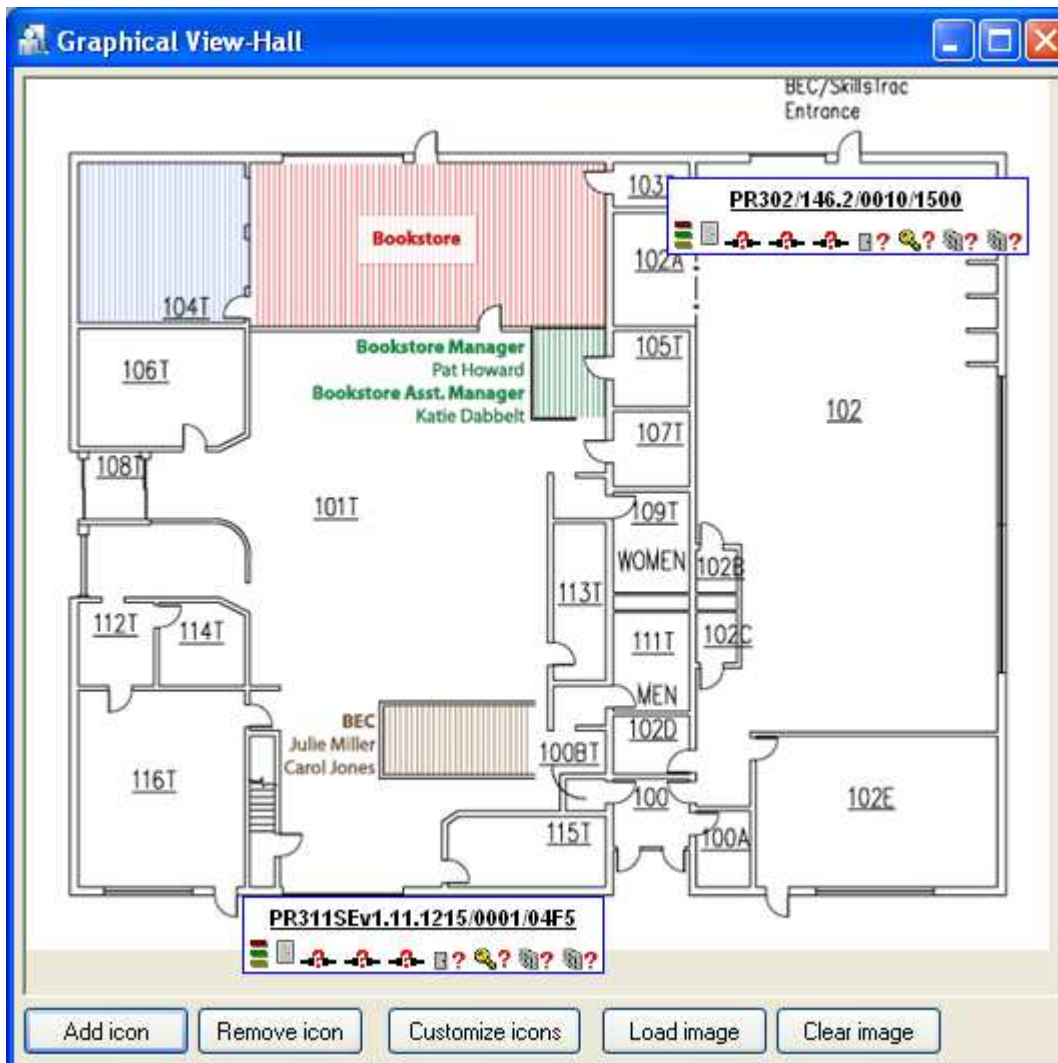
**Figure 3.86.** *Designing facility plan — window after loading a graphical sketch*

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 routinely display on the left upper corner of the window. You should drag them to appropriate positions on the plan, so that they reflect physical controllers locations.

After you dispatch icons on the plan, the designing window can look similar to the window shown in figure 3.87.





**Figure 3.87.** 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

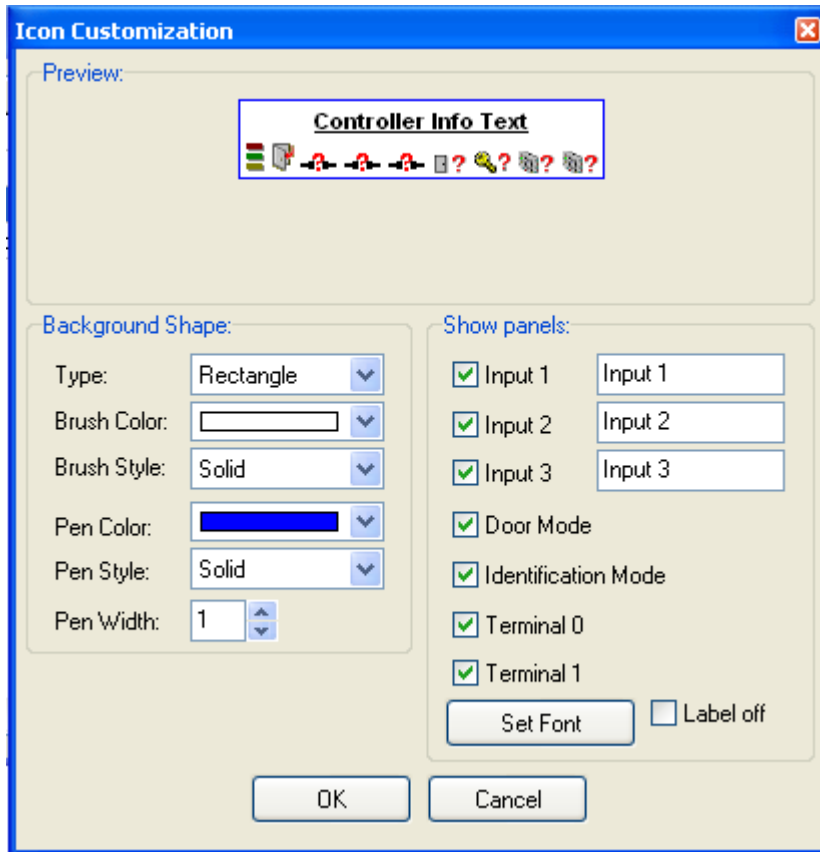
Icons can be edited in two ways:

- ◆ 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 3.88).

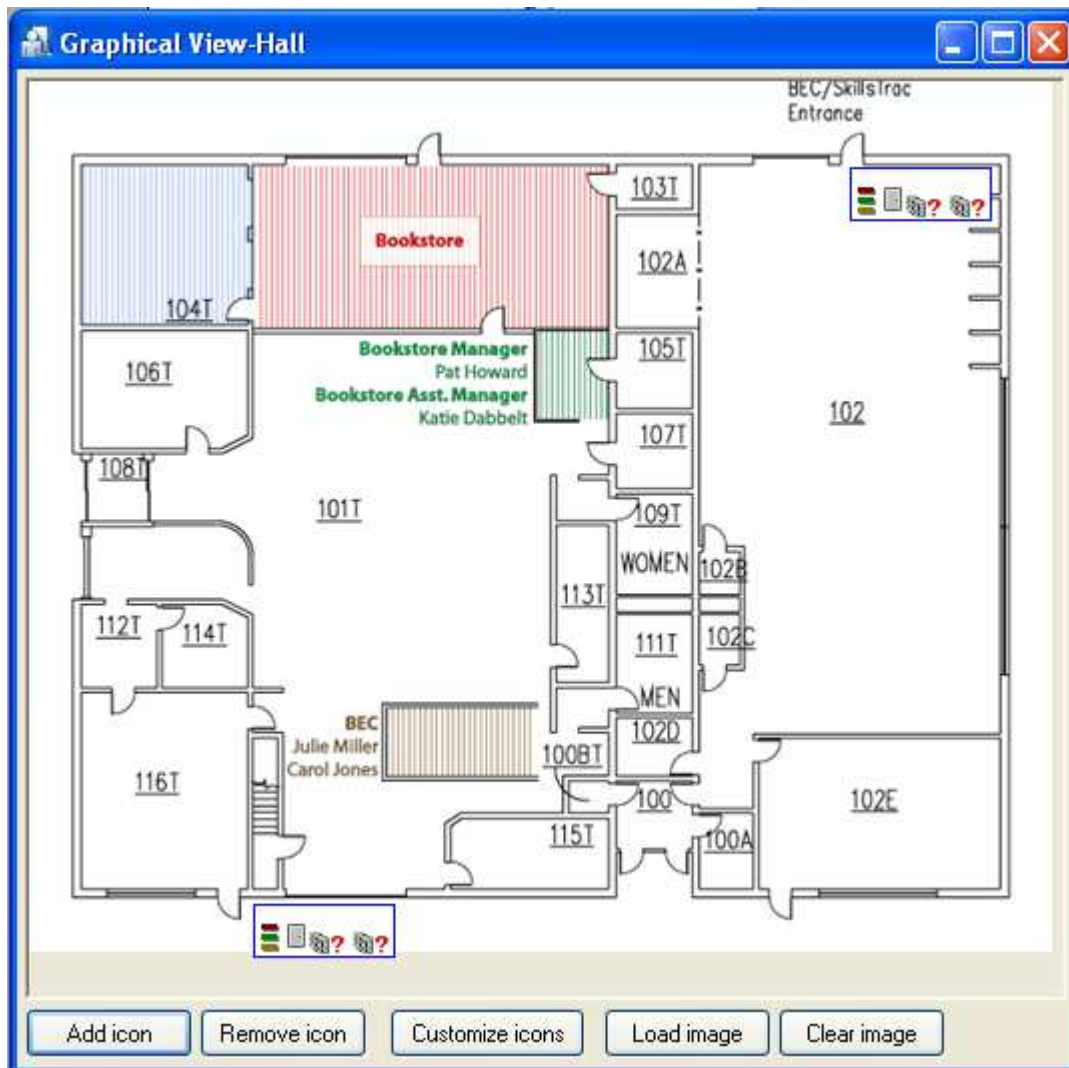


**Figure 3.88.** Customizing icons

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).

After you customize icons appearance, the plan can look similar to the window shown in Figure 3.89.



**Figure 3.89.** Designing facility plan — facility plan’s window in its final form

If you want to save the plan being designed, you should close the designing window. You can now make use of the plan defined in monitoring mode for watching system operation on maps (you can find more information on watching plans in monitoring mode in section [4.1.13. View Map](#)).

## 3.3. REPORTS MENU

The **Reports** menu has been shown in Figure 3.90.



**Figure 3.90.** *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 3.2.4.4](#)).

### 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 [3.2.3.5. Generating User Report](#)).

### 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 Figure 3.36 in [section 3.2.6.4](#)).

### 3.3.4. Networks

The **Networks** command causes displaying report containing information on networks defined in the ACS. The same report may 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 3.2.7.8](#)).

### 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 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 **Group** report in **Report** window (see **3.2.7.4. Managing Controllers In Network**

### 3.3.6. Access rights

Selecting the **Report/Access rights** command causes displaying **Access rights** report in **Report** window (Figure 3.91). This report contains summary list of all the users groups together with their access rights.

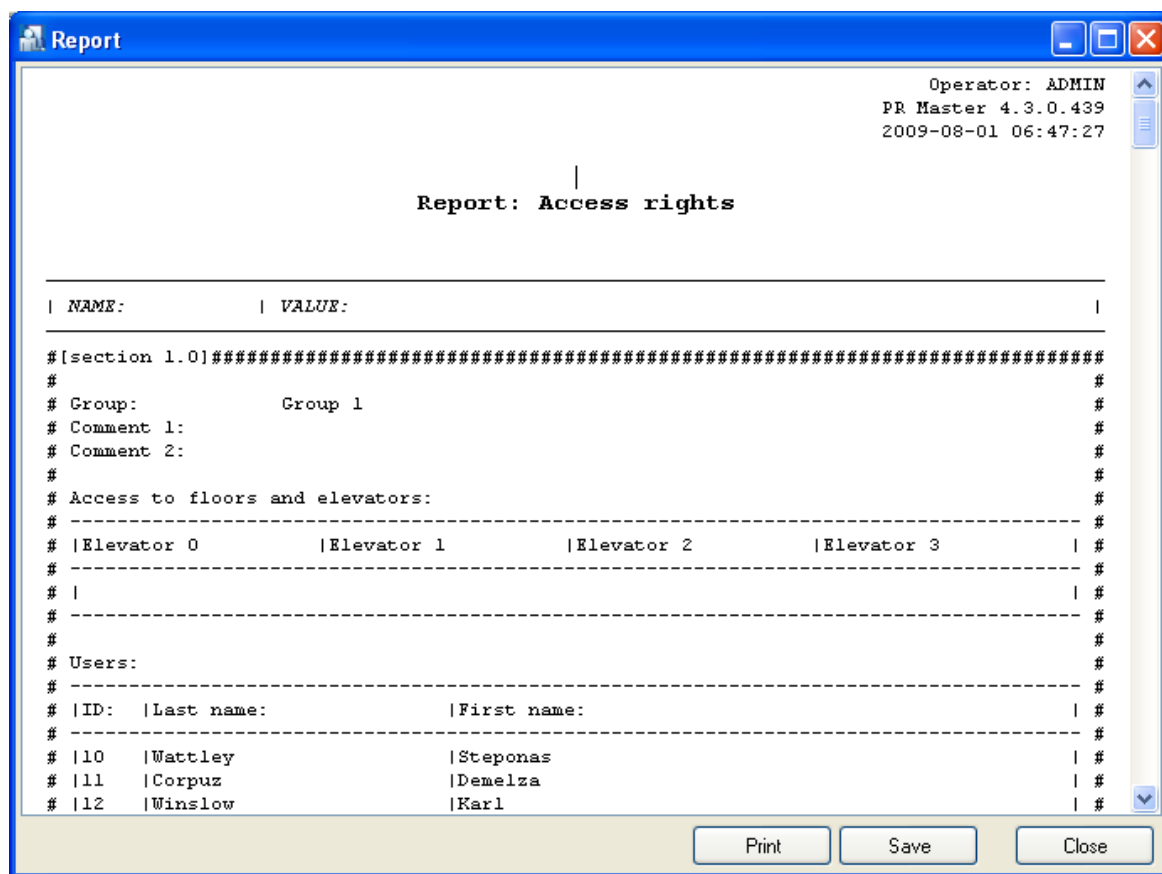
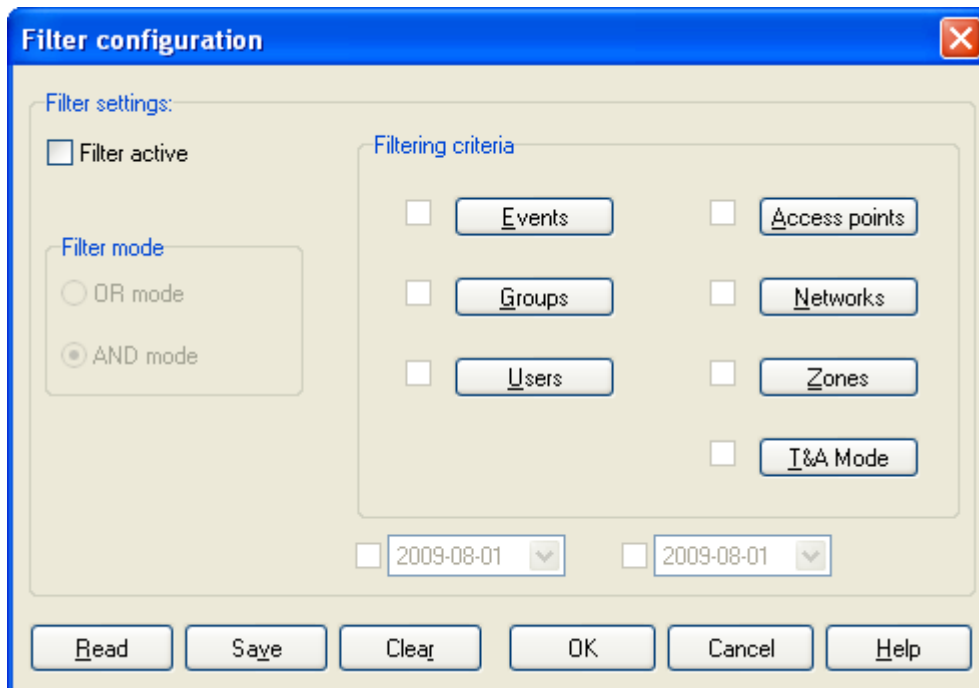


Figure 3.91. The Access rights report

### 3.3.7. Events history

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

If you select this command, system first downloads events to PR Master’s database. Then it displays the **Filter configuration** dialog box (Figure 3.92).



**Figure 3.92.** Filter settings for Events history report

Using this dialog box you should define any events filter. Thanks to this, you can 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.

### 3.3.7.1. Defining Filter

Before you are able to define a filter, you must select the **Filter active** check box. It will activate controls for defining a filter. The filter is defined by selecting filter mode (**And/Or**) and specifying criteria for event log's selected fields. 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 **Technicians** group. 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 3.93).

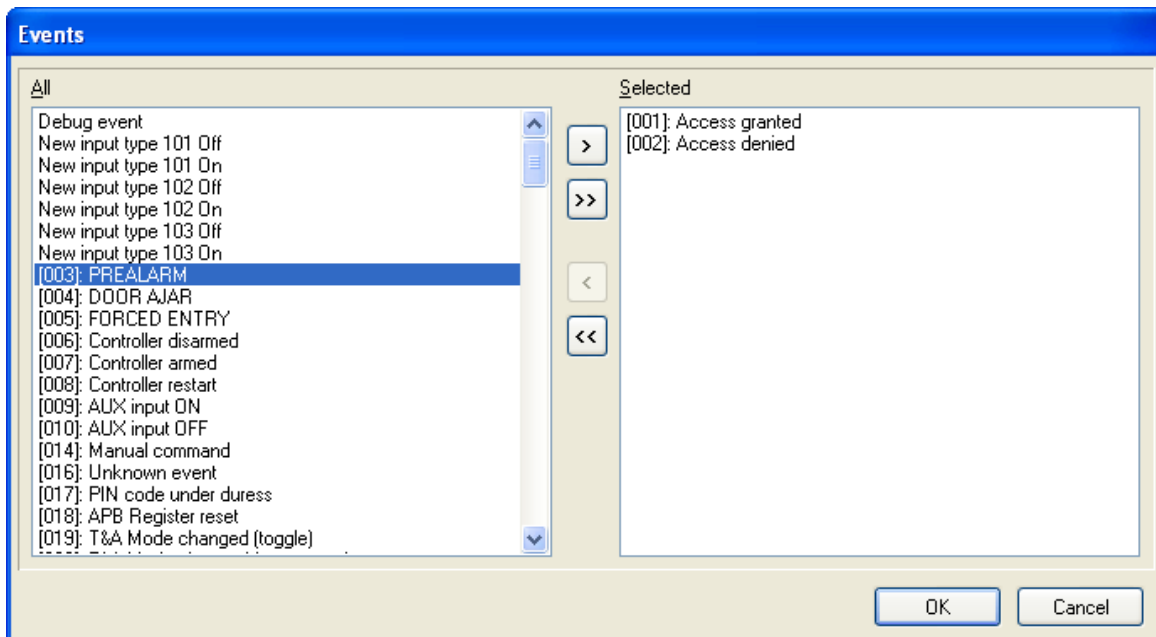
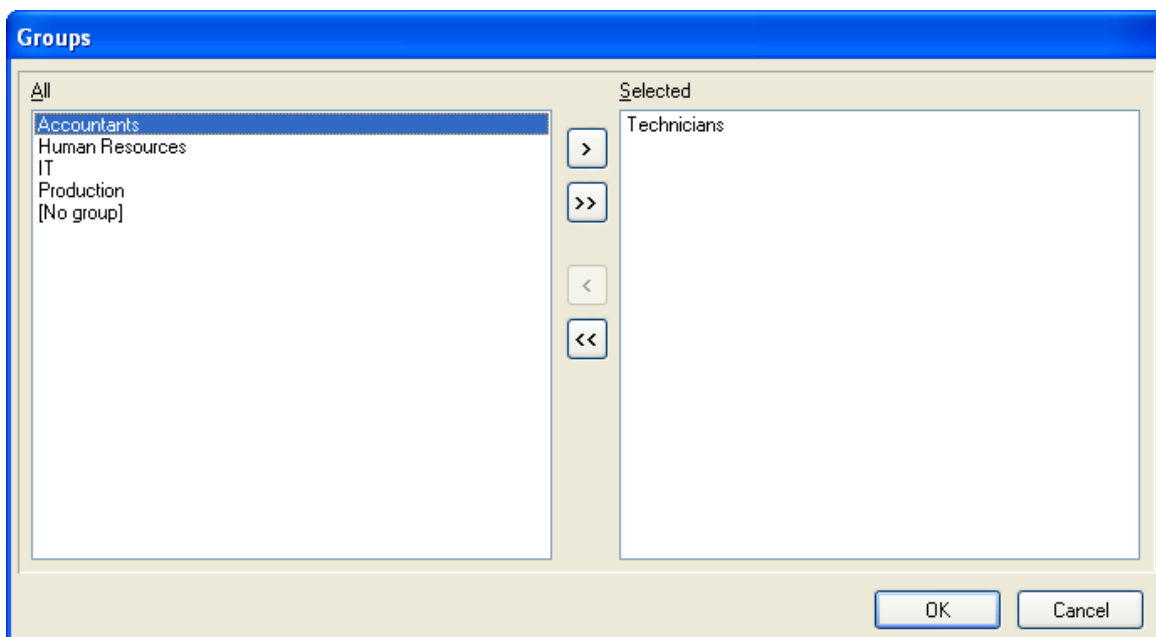


Figure 3.93. Defining filter criteria — event type

On the left hand 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, the event selected 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 hand side of the window. Selected events are deleted in a similar fashion. 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 hand 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 **Filter configuration** window. Now we click on the **Groups** button. This will cause displaying **Groups** dialog box (Figure 3.94).

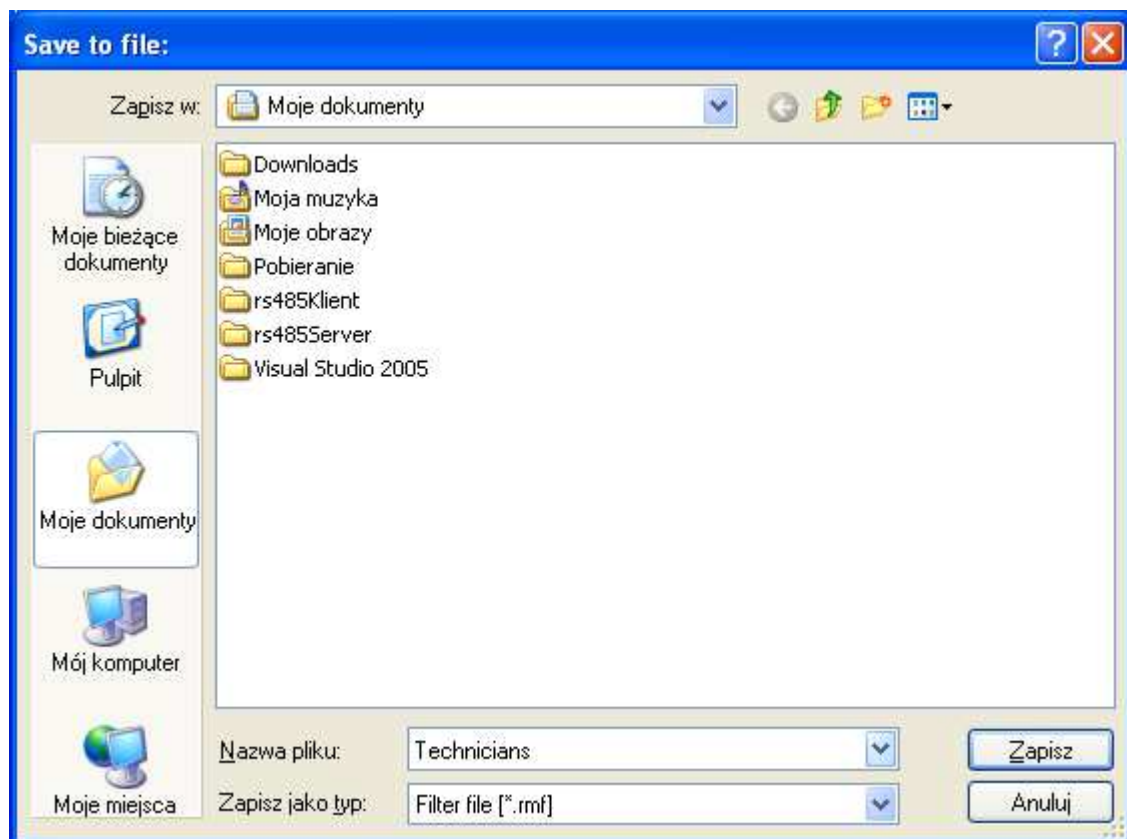


**Figure 3.94.** *Defining event filter criteria — groups*

We should select **Technicians** 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, from **Technicians** group. In a similar manner filter criteria for users, access points, 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 **Filter configuration** dialog box. Then, you should point a location, the file with filtering criteria should be saved (the file will have an **.rmf** extension) — Figure 3.95.



**Figure 3.95.** *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 configuration** 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 Log

After you finish with defining filter, you should click **OK** in the **Filter configuration** dialog box. This will cause displaying **Events history** window (Figure 3.96).

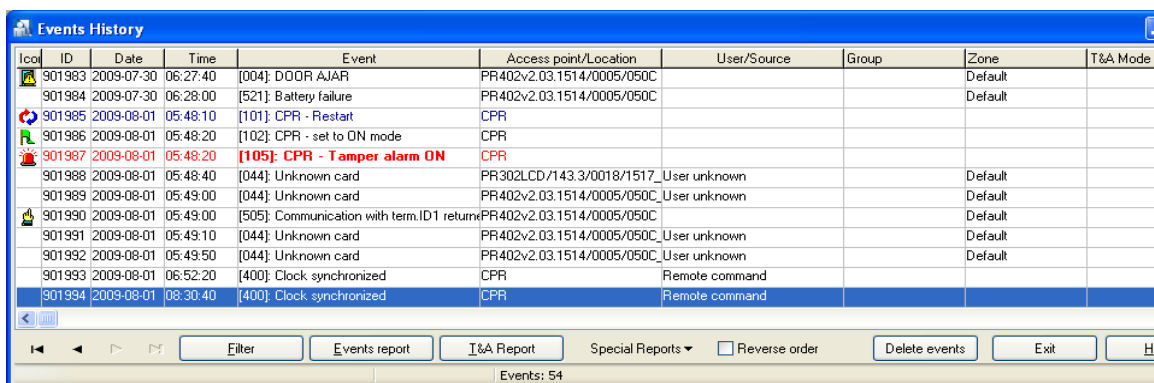


Figure 3.96. Events history

This window allows for browsing (make final changes) to the event list before events report is printed. From this level you can also print T&A report or special reports.

Buttons on the left hand side of the toolbar allow navigating 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 **Filter configuration** dialog box again. This way you can update filter defined earlier.

#### Printing Events History report

If you click on the **Events report** button, the **Event report format** dialog box will appear (Figure 3.97).

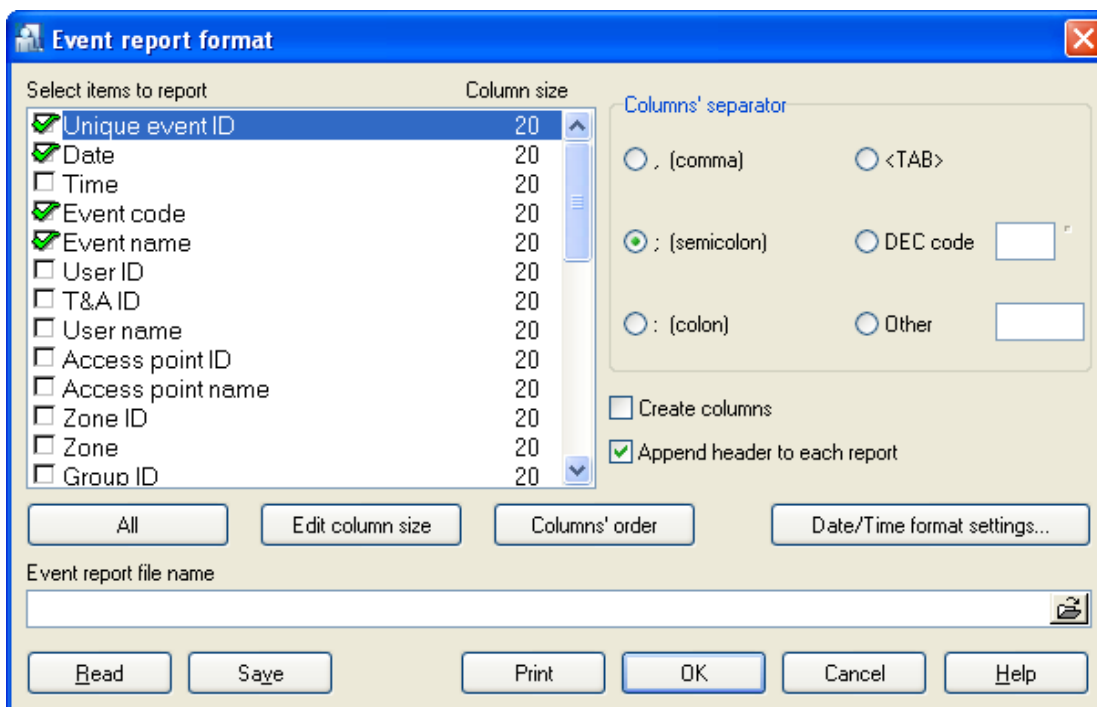
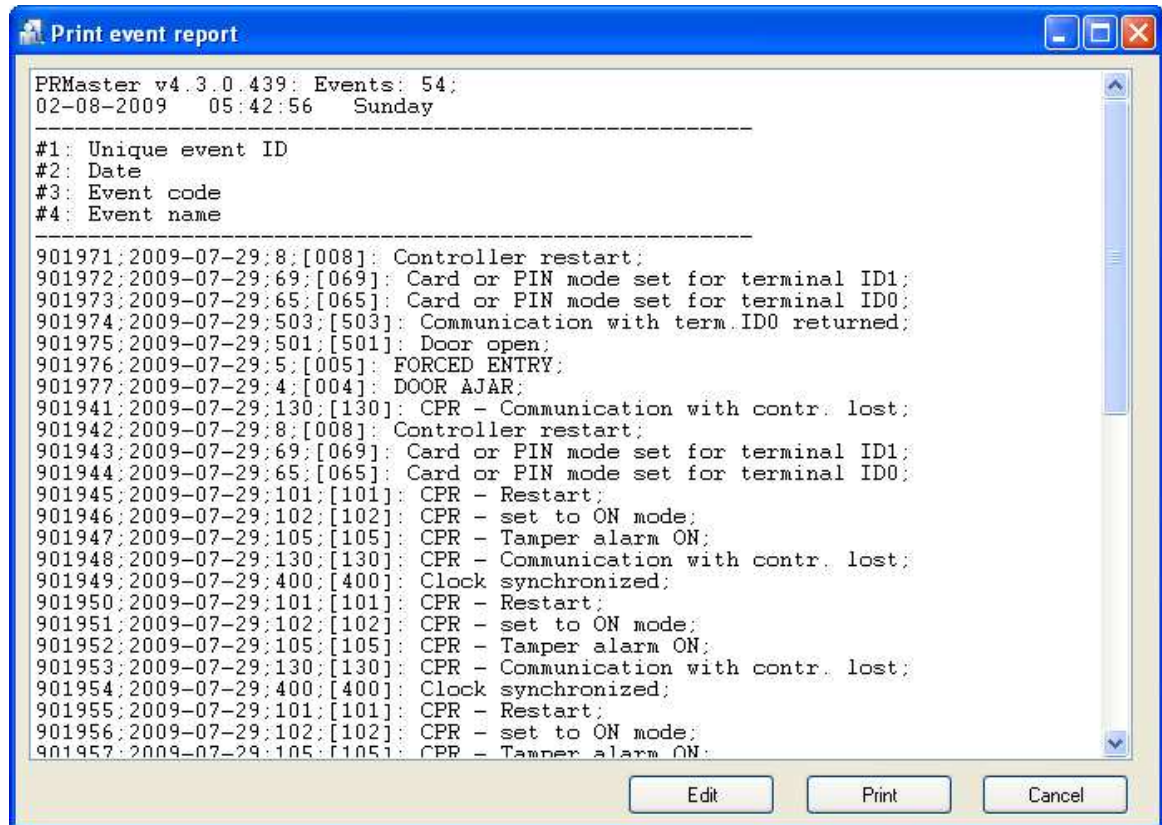


Figure 3.97. Events history settings

Using this dialog box you can configure in detail format of events 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.

Events report settings can also be written to a file (the **Save** button), and imported from it thereafter (the **Read** 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 3.98).



**Figure 3.98.** Printing Events 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

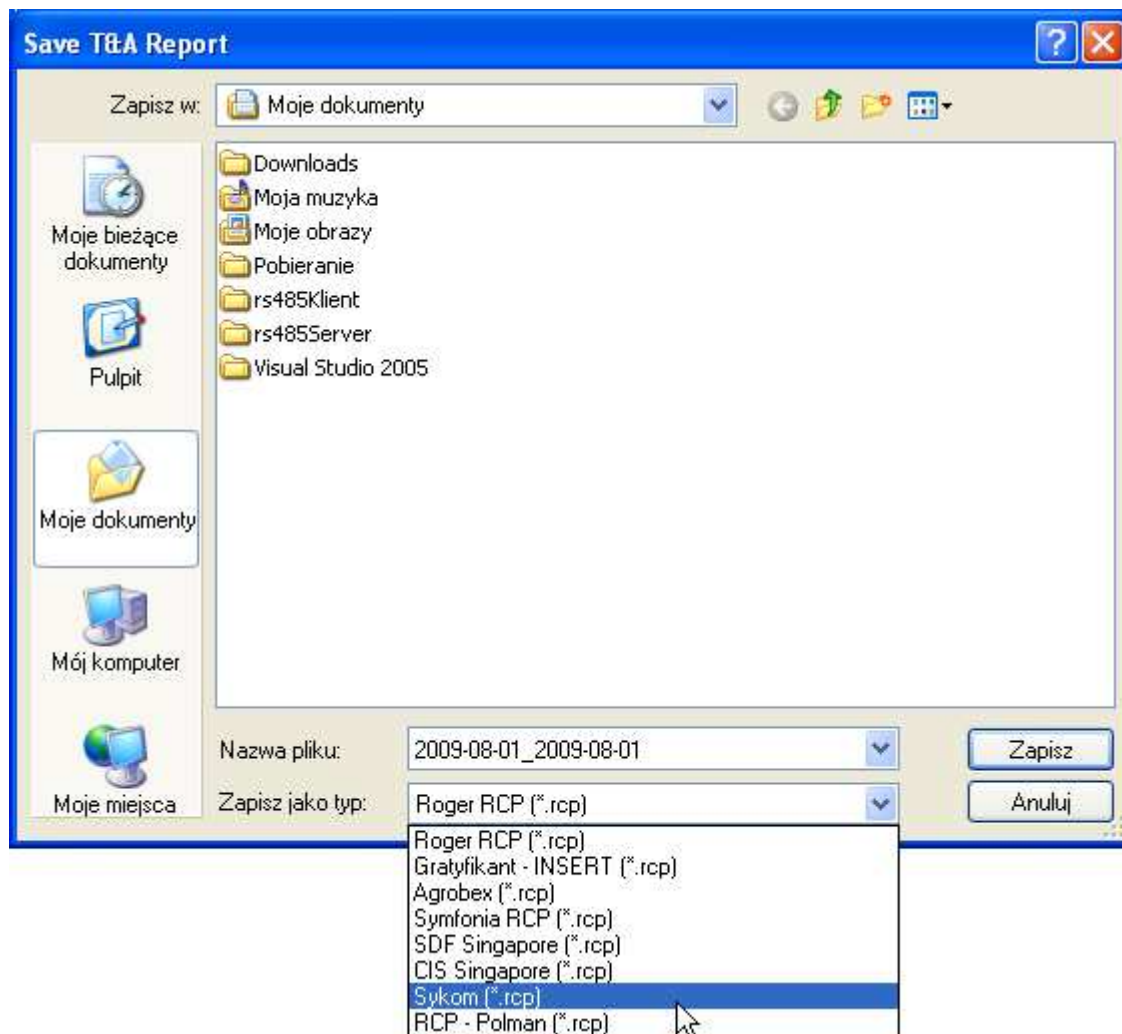
If you click on the **T&A Report** button, the **T&A Events** dialog box will appear (Figure 3.99).

Date	Time	Event	Controller	User
2009-08-02	05:57:19	[001]: Access granted	PR402v2.03.1514/0005/05	Chevère Lucinde
2009-08-02	05:57:20	[001]: Access granted	PR402v2.03.1514/0005/05	Vitello Antinanco
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 Anastasio
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	Chevère 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 Anastasio

**Figure 3.99.** *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 3.100).



**Figure 3.100.** 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

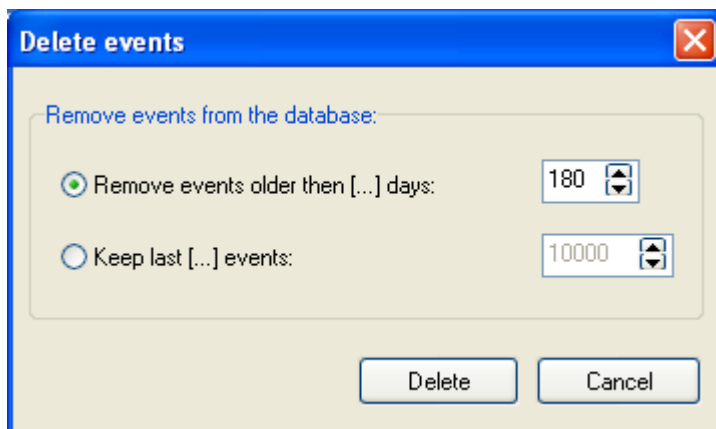
The **Special Reports** menu has been created in order to define reports made on special users request. For instance the **Report 1** allows for displaying users who logged on the selected reader. Because special reports are very specific, and used for individual purposes, discussing them in detail is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

### Reversing Events Order

By default, events in the **Events 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 **Events 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 3.101).



**Figure 3.101.** *Deleting events from database*

Using this dialog box you can delete from database events older than specific number of days (the **Older than following number of days** option). You can also specify the number of events which should remain in the database after delete operation is completed (the **Save only last following number of 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 Events History

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

## 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, for how long persons from particular group were present in the area defined. 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.

Selecting the **Report/Attendance** command causes displaying the **Users' attendance in defined Attendance Areas** dialog box opens (Figure 3.102).

**Figure 3.102.** *Generating report on attendance in attendance areas defined*

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 employer of a given name,
- ◆ sort records according to the defined criteria,
- ◆ save report to a file,
- ◆ print report to the printer.
- ◆ initiate generating the FILO report.

Immediately after 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 attendance records in the window (Figure 3.103).

Time range for Attendance Report:  
 From: 2009-08-28 00:00:00 To: 2010-07-29 15:19:49

User group: All Groups

Attendance Area: Name: Hala

Max. attendance time per single day:  
 Time limit: 12  
 No limit

Ignore incomplete data  
 Create daily reports: 00:00:00  
 Lunch brake (min): 30

Group name	User ID	User Name	T&A ID	Time (hh:mm:ss)	Modified Year
Administracja	114	Himes Horatia	64	00:04:30	
Administracja	117	Lee Gerardo	67	01:43:00	
Produkcja	101	Aaron Paige	51	25:06:40	
Produkcja	107	Childers Adrienne	57	46:24:40	
Produkcja	106	Devilbiss Irune	56	46:27:00	
Produkcja	109	Herman Poul	59	45:53:00	
Produkcja	108	Keller Esther	58	46:33:30	
Produkcja	100	Levine Mauro	50	46:05:10	
Produkcja	104	Madrid Derrick	54	Errors - incomplete data	
Produkcja	103	Porter Miles	53	46:20:20	
Produkcja	105	Rubin Stephen	55	46:27:10	
Produkcja	102	Stein Leslie	52	45:54:00	

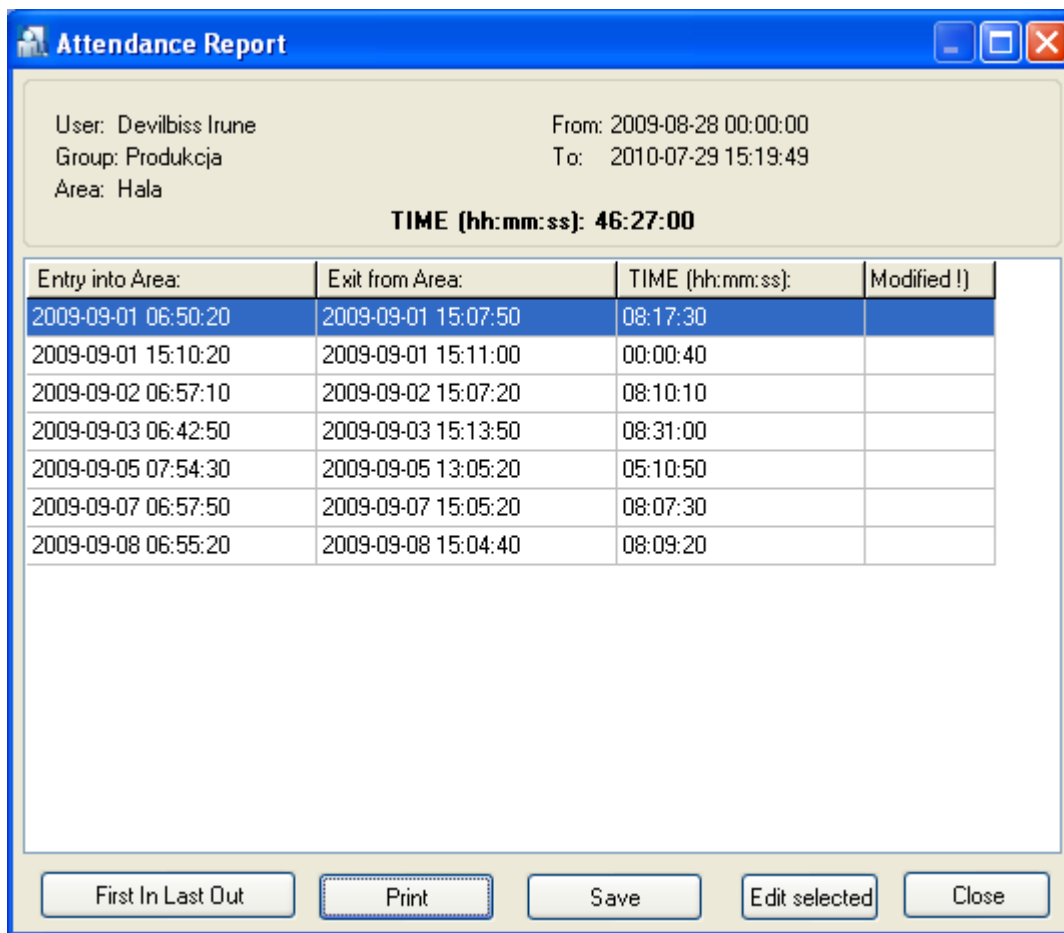
Arrange by:  Group and last name  ID number  Last name  T&A ID Find...

Refresh Report First In Last Out Print Save View selected Close Help

**Figure 3.103.** User's attendance in Attendance Area #1 for users from Manufacturing group

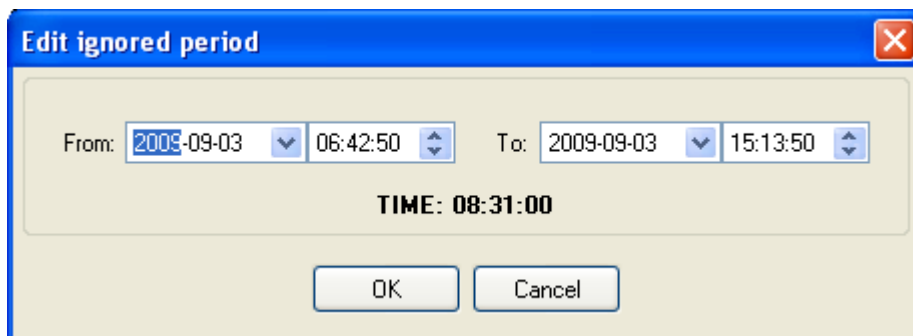
If you select the **Lunch break** checkbox and set the length of the break, the system will automatically adjust users' attendance times (the lunch break time will be subtracted).

Double clicking on any person in the list will cause displaying **Attendance report** dialog box (Figure 3,104).



**Figure 3.104.** Attendance report for a selected user in the selected attendance area

In case there are wrong data in the events history related to the particular user, you can modify them. In order to do this, you should double click an item in the list. In reply, the system displays **Edit** dialog box (Figure 3,105), where you can modify an entry logged in error.



**Figure 3.105.** Correcting erratic entries in attendance report

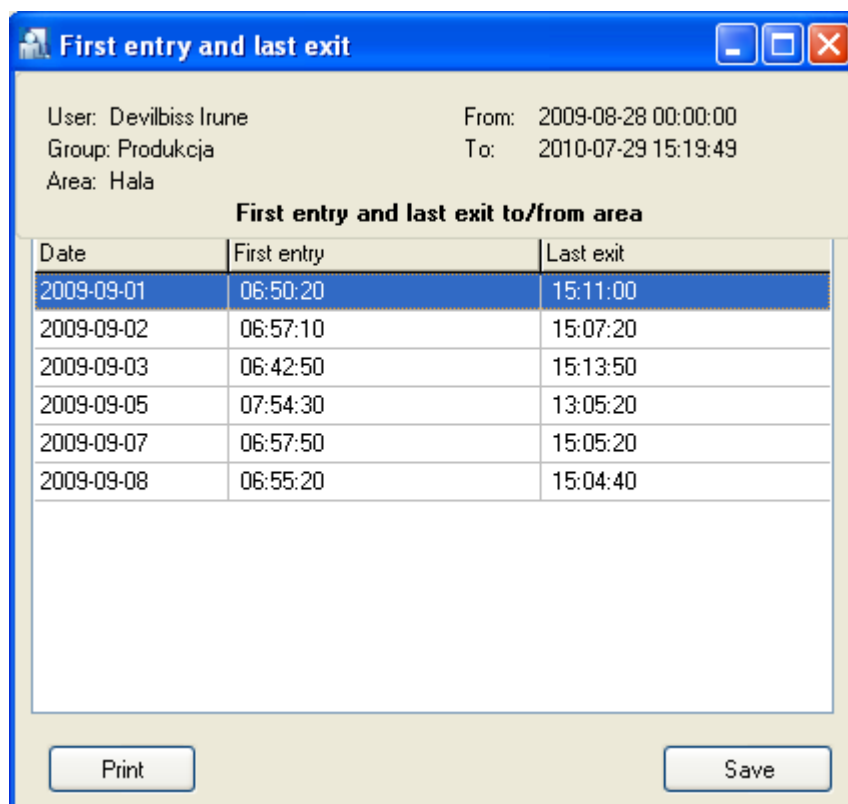
If you modify an entry, and click on the **OK** button, a modified entry will be marked in the event list by the "V" mark.

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 3.104. Clicking on it will cause displaying a summary with all the first entries and last exits of the selected user in chosen time frame (Figure 3.106).



Date	First entry	Last exit
2009-09-01	06:50:20	15:11:00
2009-09-02	06:57:10	15:07:20
2009-09-03	06:42:50	15:13:50
2009-09-05	07:54:30	13:05:20
2009-09-07	06:57:50	15:05:20
2009-09-08	06:55:20	15:04:40

**Figure 3.106.** Report First In Last Out for selected user in given date 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 3.103). 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 right below this frame.

### 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 3.103). 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.

Area: Hala From: 28-08-2009  
To: 29-07-2010

**First entry and last exit to/from area**

Date	First entry	User	Last exit	User
01-09-2009	06:49:40	Aaron Paige	15:11:20	Herman Poul
02-09-2009	06:56:20	Keller Esther	15:13:00	Keller Esther
03-09-2009	06:42:50	Devilbiss Irune	15:21:20	Keller Esther
05-09-2009	07:53:20	Himes Horatia	13:05:40	Herman Poul
07-09-2009	06:57:20	Stein Leslie	15:05:30	Herman Poul
08-09-2009	06:55:10	Madrid Derrick	15:04:50	Herman Poul

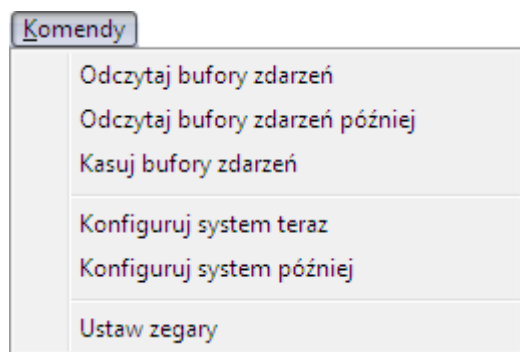
Print Close

**Figure 3.107.** Report *First In Last Out* for selected dates range

As usual, this report can be hard-copied on the printer or saved in **.rtf** or **.csv** formats.

## 3.4. COMMANDS MENU

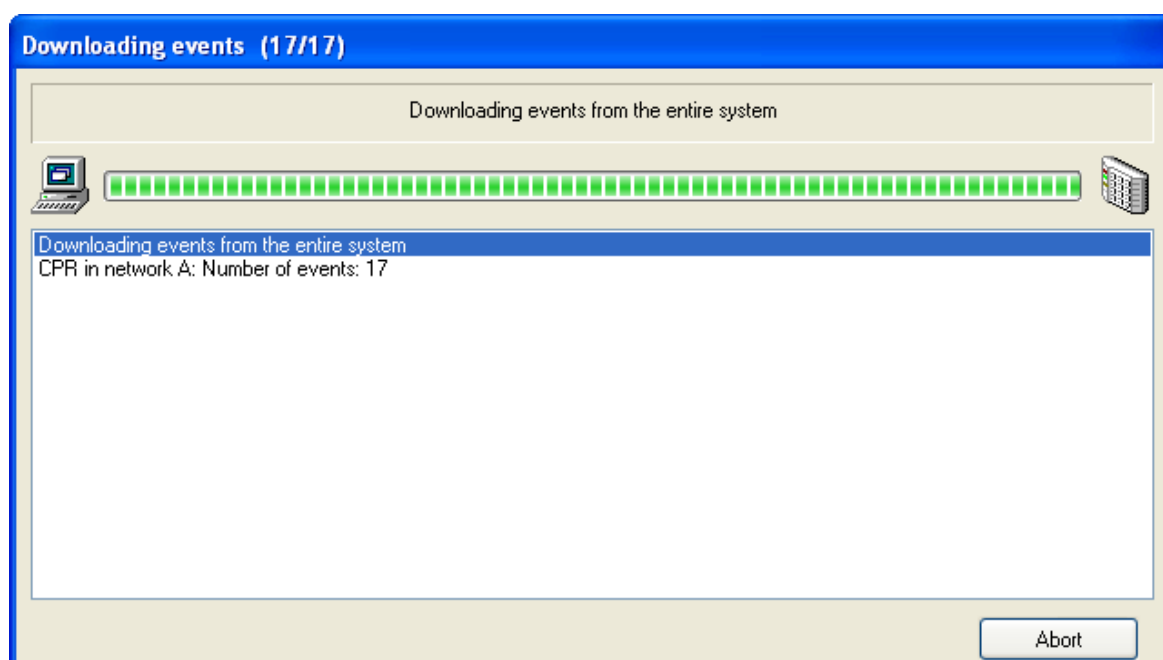
The **Commands** menu has been shown in Figure 3.108.



**Figure 3.108.** *Commands menu*

### 3.4.1. Read event buffers now

Events in the RACS are gathered all the time — on controllers and on 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 3.109).



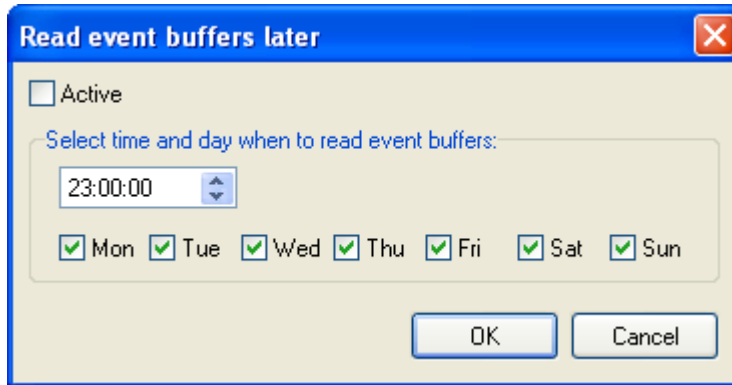
**Figure 3.109.** *Downloading events from the ACS to database*

If the process of downloading events is completed, the system displays a message with information of operation's success or failure. Then it will ask, if we want to set devices' clock according to the computer's system clock. If we confirm, the system will adjust devices' clock settings in the system.

### 3.4.2. Read event buffers later

In large Access Control System installation, the process of downloading events can be time-consuming. In order to avoid losing time for passive waiting, an 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 3.110).



**Figure 3.110.** 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 the controllers and all the CPR-32 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 — 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 3.111).

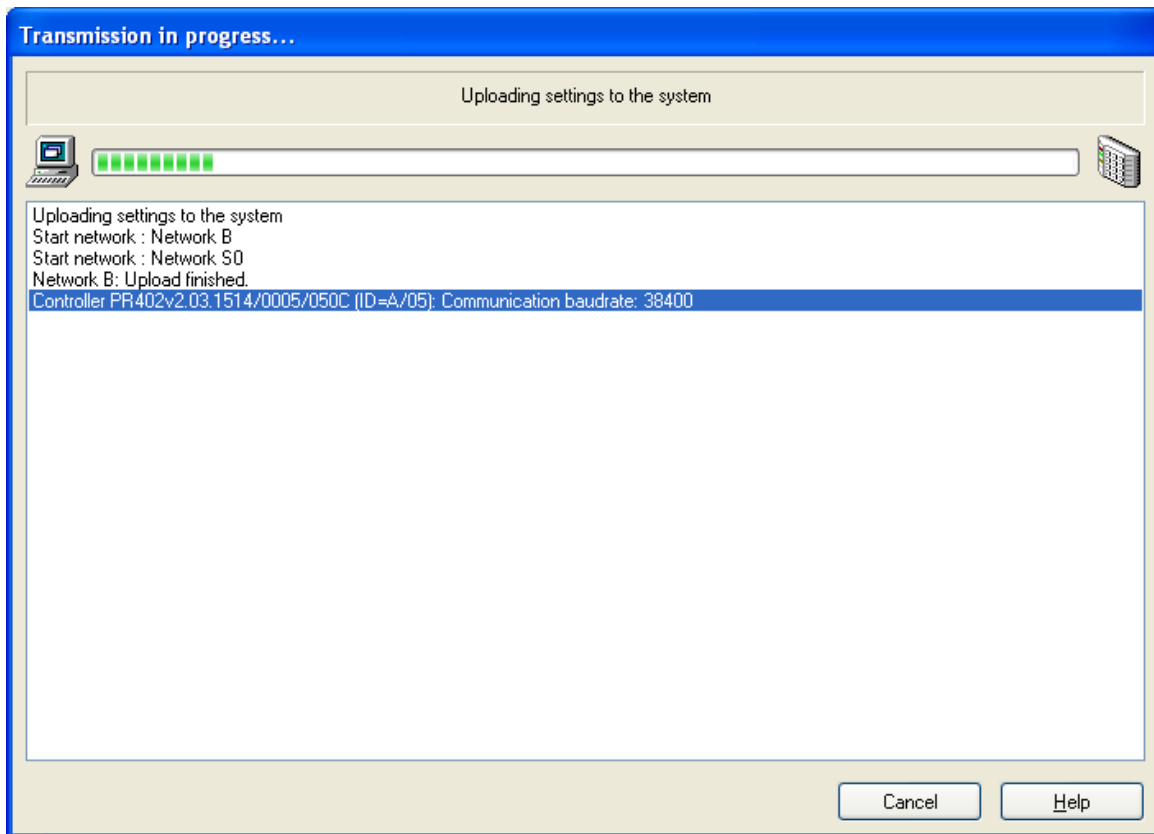


Figure 3.111. Configuring entire system — the operation progress window

### 3.4.5. Update system later

Because an operation of configuring the whole system is 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 3.112).

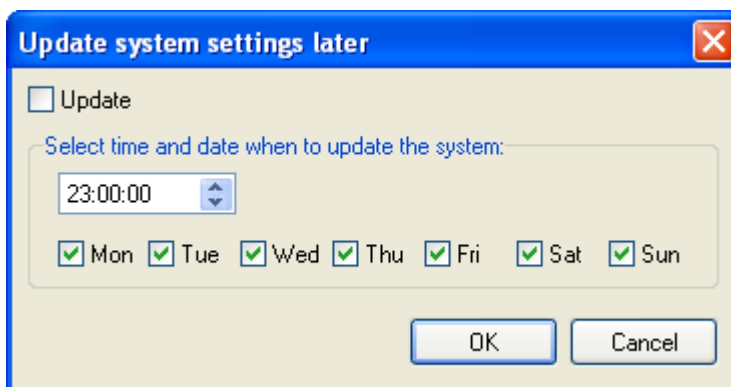


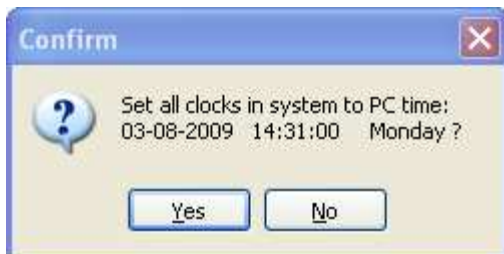
Figure 3.112. Scheduling automatic update for the entire system

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 setting RACS devices' clocks with accordance to system clock settings of the computer, the PR Master software is installed on. If you select this command, the confirmation dialog box displays (Figure 3.113).



**Figure 3.113.** *Confirming an intent to set clocks in RACS devices*

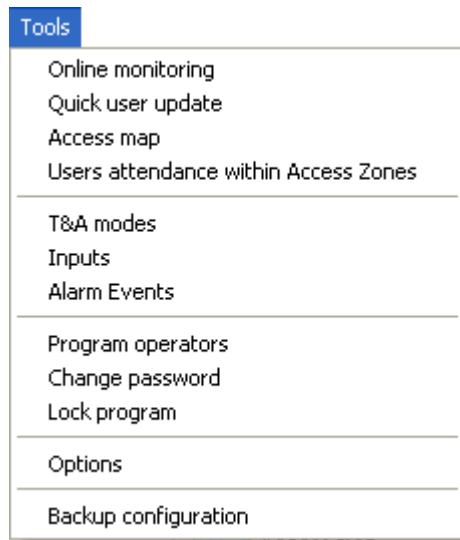
If this operation completes successfully, the system will display information message, that the command has been completed (Figure 3.114).



**Figure 3.114.** *Setting clocks operation has been successfully completed*

## 3.5. TOOLS MENU

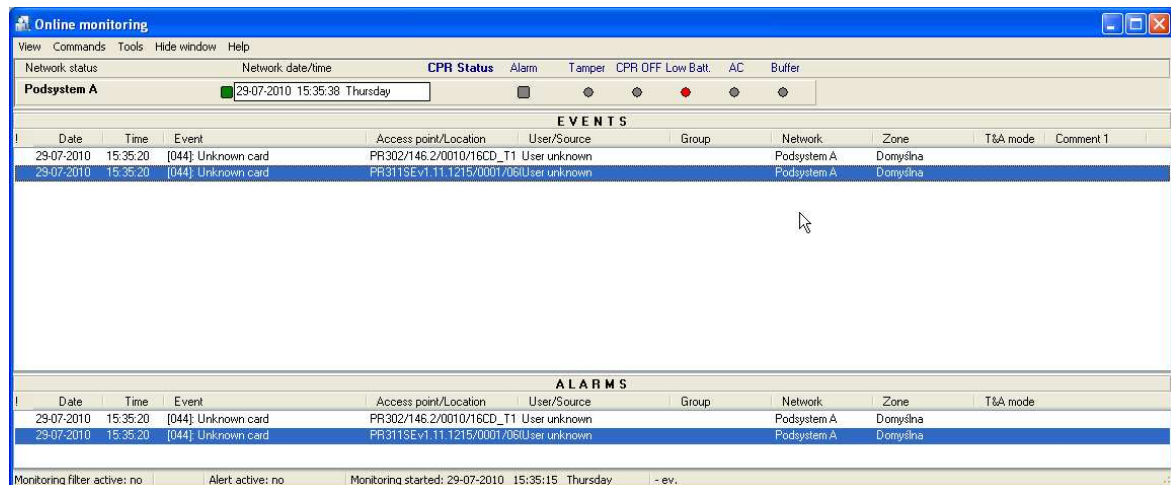
The **Tools** menu has been shown in Figure 3.115.



**Figure 3.115.** Tools Menu

### 3.5.1. Online monitoring

The **Online monitoring** command turns on a special mode of PR Master which allow watching in real time events happening in the RACS. When PR Master operates in this mode, events happening in the system are immediately appended to the system's database and 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 3.116).



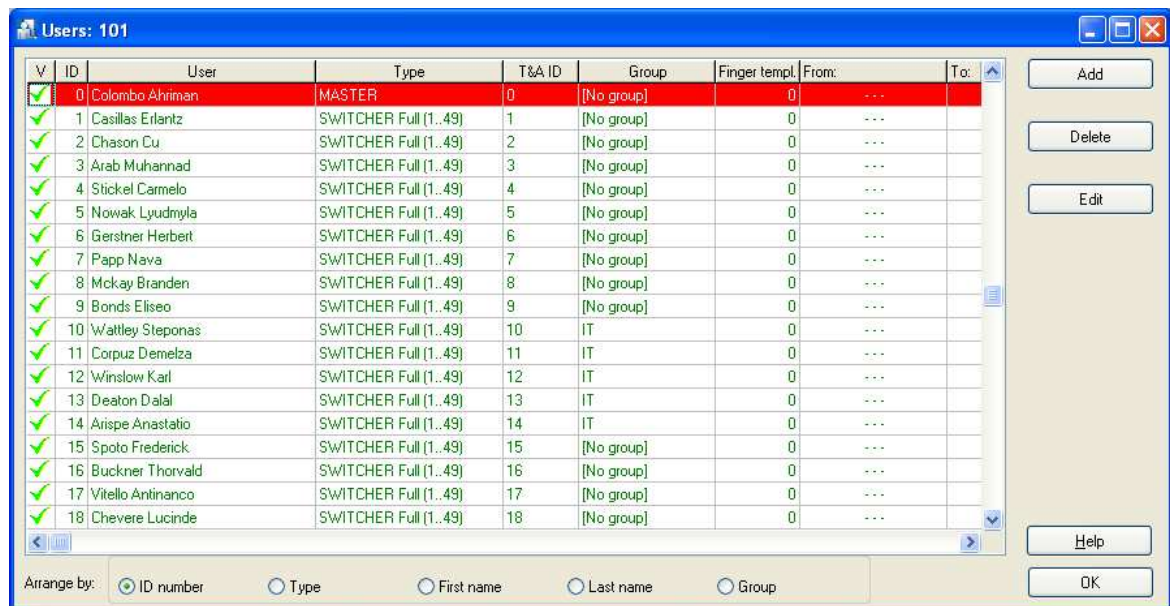
**Figure 3.116.** Online monitoring in PR Master

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

### 3.5.2. Quick user update

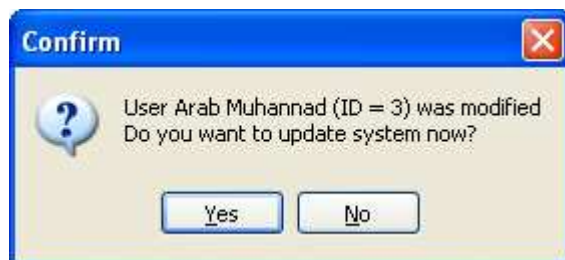
Every change of user properties — i.e. change assignment to a group, replace of proximity card change the PIN code, requires sending data to controllers. In view of the fact, that the operation of sending the whole configuration to all the controllers in the system is time-consuming, and changes made 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 3.117).



**Figure 3.117.** Quick user update

This window allows for adding, removing, and modifying users properties. If you add a new user to the system or update its properties, the system displays appropriate message (Figure 3.118).



**Figure 3.118.** Quick user update

If we answer **Yes** to this question, the system goes into the process of update properties only of this user, whose data have been changed (Figure 3.119).



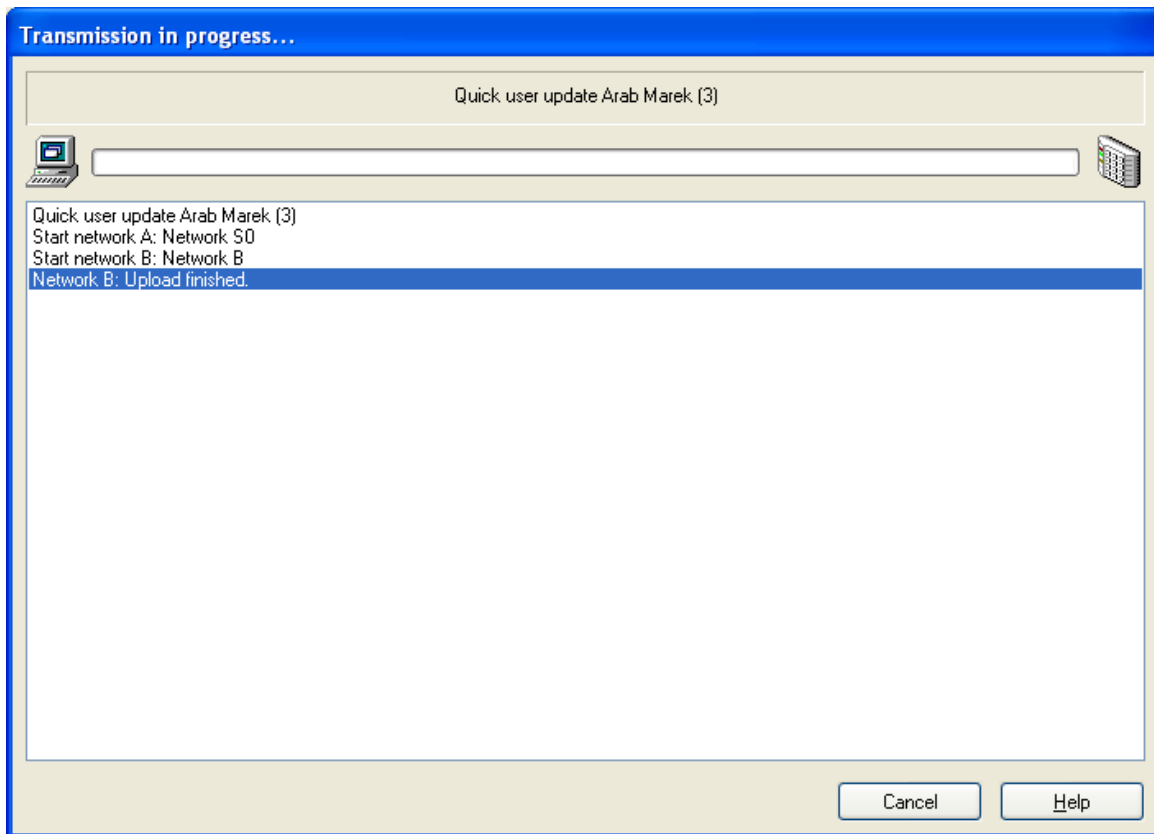


Figure 3.119. Online update of one user properties

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

The quick user update operation can be performed only one by one. This means, that you cannot change data for several users, and the send data for whole the group in bulk. The functionality will be available only on the condition, that after you change data of every user, they will be immediately sent to controllers. If you do not send data to controllers, then the **Quick user update** functionality will be blocked until you perform complete system configuration using **Update system now** command. If the **Quick user update** operation is blocked, and you attempt to use it, the system will display message similar to the one shown in figure 3.120.

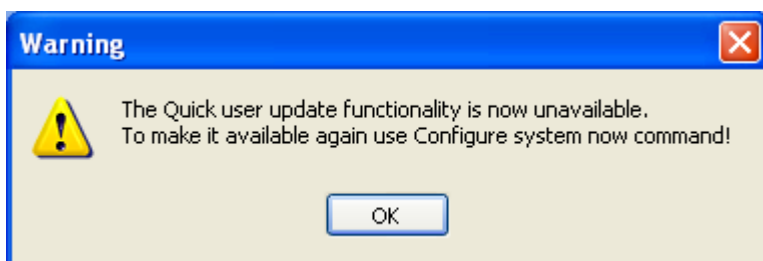


Figure 3.120. Message informing that the Quick User Update functionality was blocked

### 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).

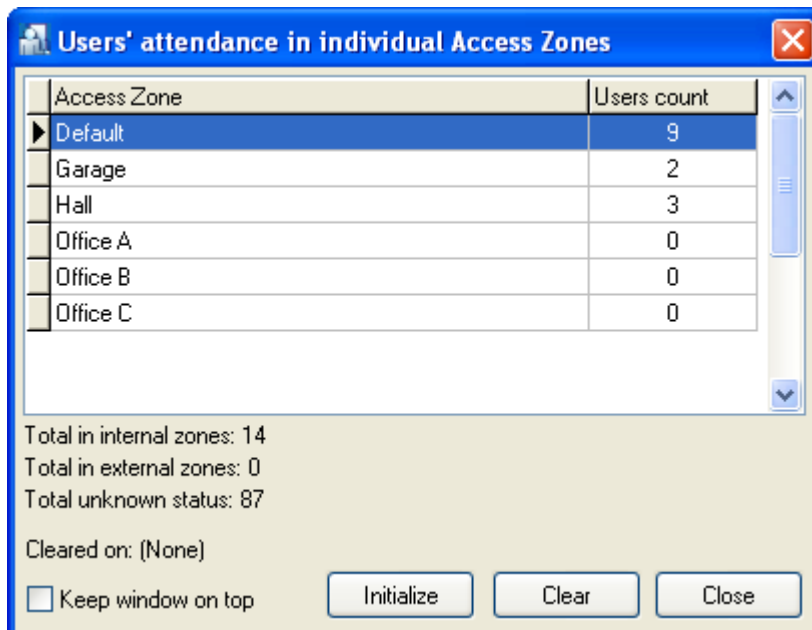


**Figure 3.121.** System's access rights map

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 in red an **x** mark.

### 3.5.4. Users attendance within Access Zones

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

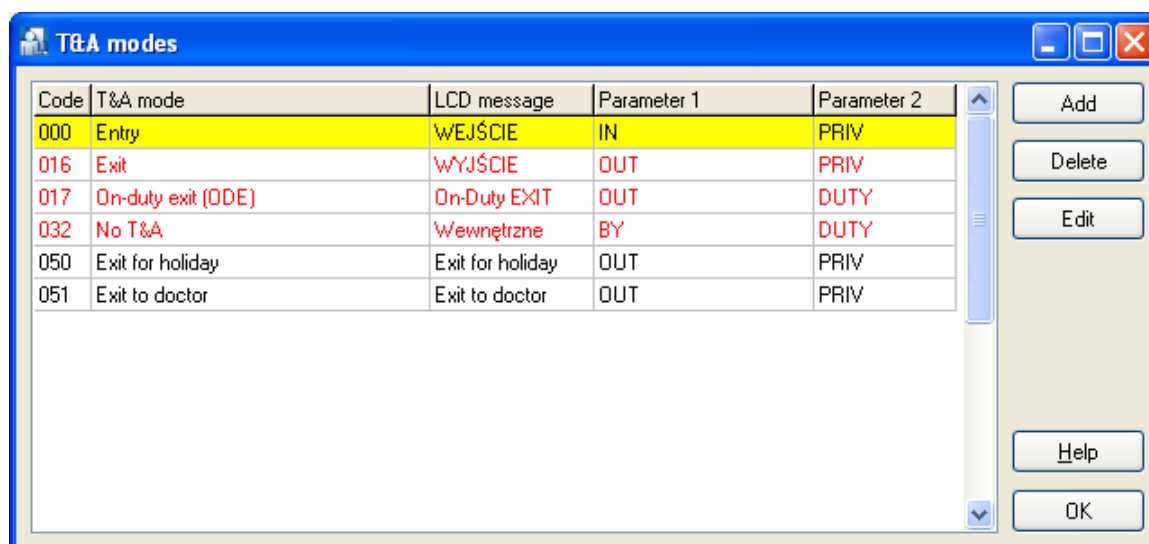


**Figure 3.122.** *Number of users logged in access zones*

The **Initialize** button causes initiating a table based on a current RACS 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 when a database was cleared.

### 3.5.5. T&A modes

The **T&A modes** command opens the RACS' T&A modes directory (Figure 3.123).



Code	T&A mode	LCD message	Parameter 1	Parameter 2
000	Entry	WEJŚCIE	IN	PRIV
016	Exit	WYJŚCIE	OUT	PRIV
017	On-duty exit (ODE)	On-Duty EXIT	OUT	DUTY
032	No T&A	Wewnętrzne	BY	DUTY
050	Exit for holiday	Exit for holiday	OUT	PRIV
051	Exit to doctor	Exit to doctor	OUT	PRIV

**Figure 3.123.** *T&A modes directory*

Using this directory, you can add custom T&A registration modes. However you should note, that T&A modes with codes from 00–49 range are predefined. They neither can be removed, nor modified.

#### 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).

The screenshot shows a dialog box titled "T&A mode" with a close button in the top right corner. The dialog is divided into several sections:

- Code:** A text box containing "052".
- LCD message:** A text box containing "New T&A mode".
- Name:** A text box containing "New T&A mode".
- Parameter 1 (Direction: entry, exit, internal or custom):** A group of radio buttons with "Entrance" selected. Below them is a "Mark" text box containing "IN".
- Parameter 2 (private, on-duty or custom):** A group of radio buttons with "Private" selected. Below them is a "Mark" text box containing "PRIV".
- Buttons:** "OK" and "Cancel" buttons are located at the bottom right of the dialog.

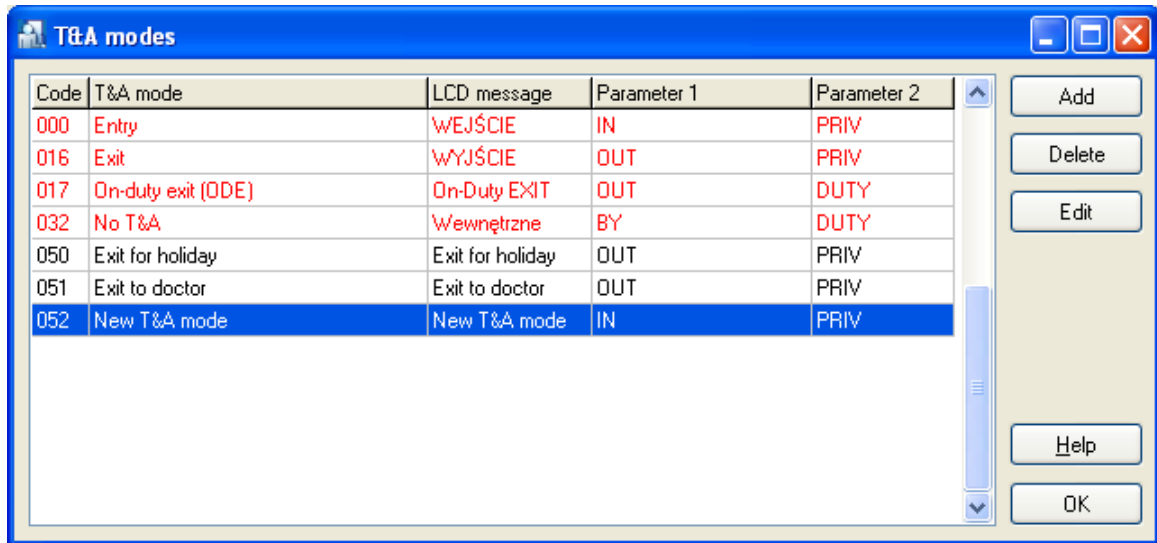
**Figure 3.124.** Adding a new T&A mode

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 an entry, exit, or internal door (so that it has no influence on T&A registration). You can also select a **Custom** radio box and define your own T&A registration mode.

The **Parameter 2** describes if the particular T&A event is of private, duty, or custom character (described by an individual mark).

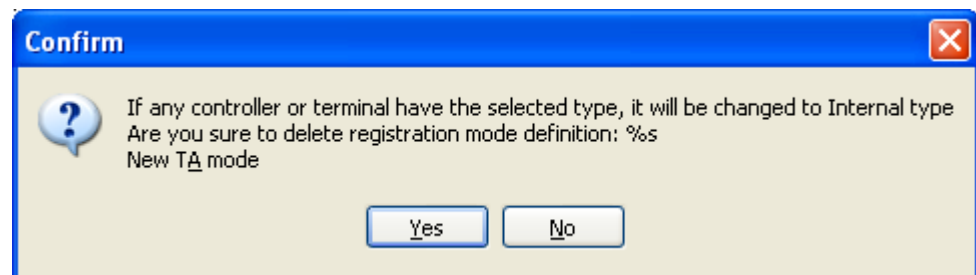
After you define all the T&A mode properties, you should click **OK**. A new mode will appear in the T&A modes directory window (Figure 3.125). You should note, that the user-defined T&A modes display in black, whereas predefined modes display in red.



**Figure 3.125.** T&A mode with codes 50-52 have been added by user

### Deleting a T&A mode

User-defined T&A 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).

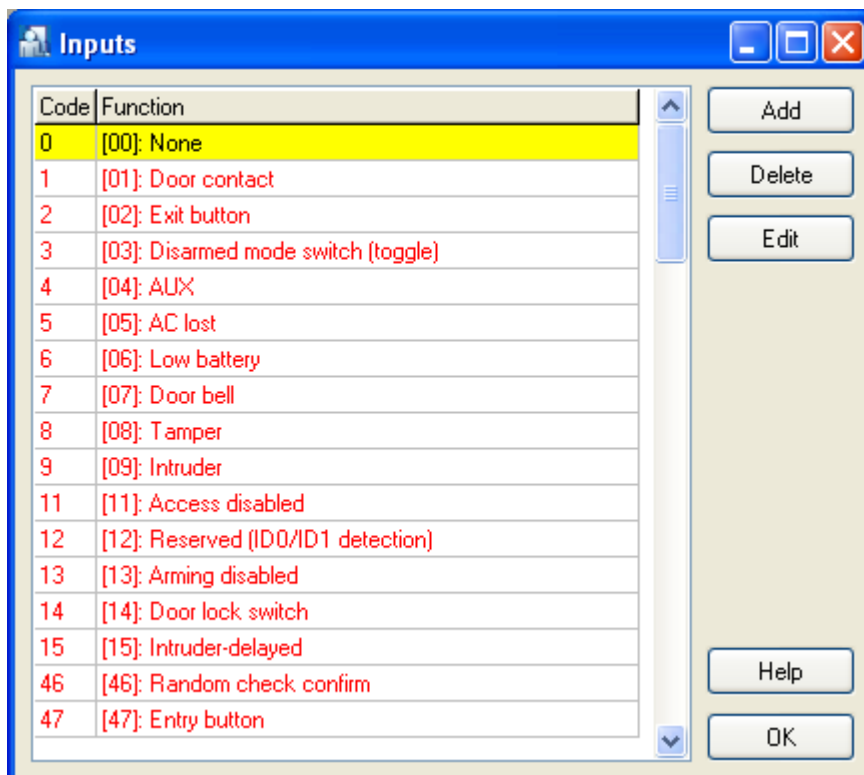


**Figure 3.126.** Deleting user-defined T&A mode

If you answer "yes" to this question, the user-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 (Figure 3.127).

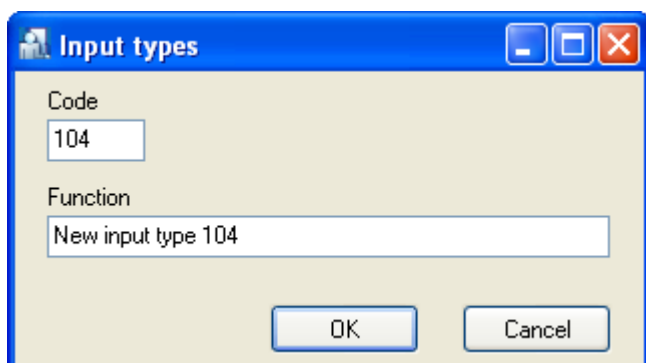


**Figure 3.126.** Input lines directory in the RACS

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. User-defined input lines types can be used when the controller should inform about other devices' status (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 user-defined input line types display in black, whereas predefined modes display in red.

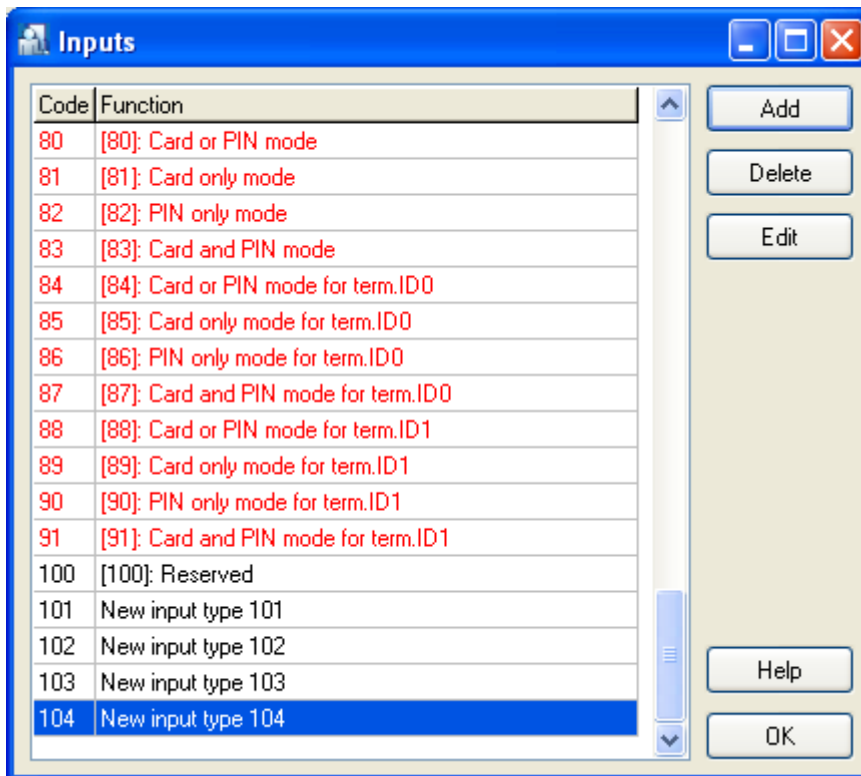


Figure 3.129. Input line type with code 101 has been added by user

### Deleting Input Line Type

User-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).

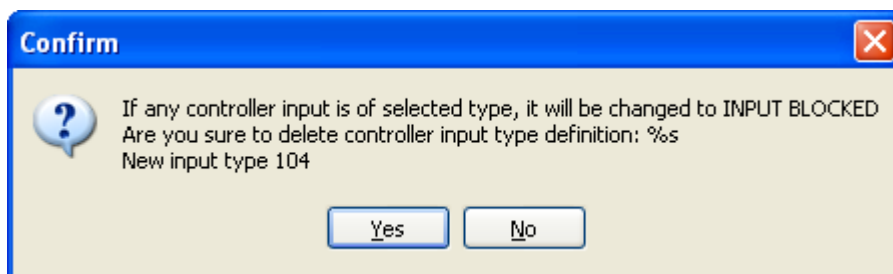
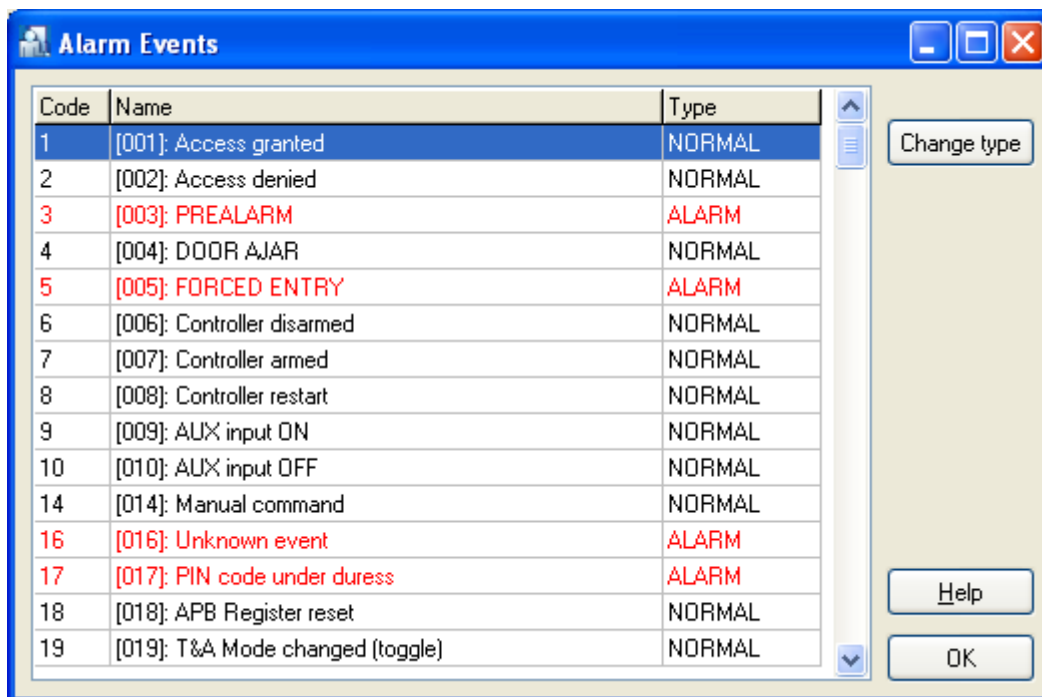


Figure 3.130. Deleting user-defined input-line type

If you answer "yes" to this question, the user-defined 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 (Figure 3.131).



**Figure 3.131.** Alarm events types in the RACS

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.

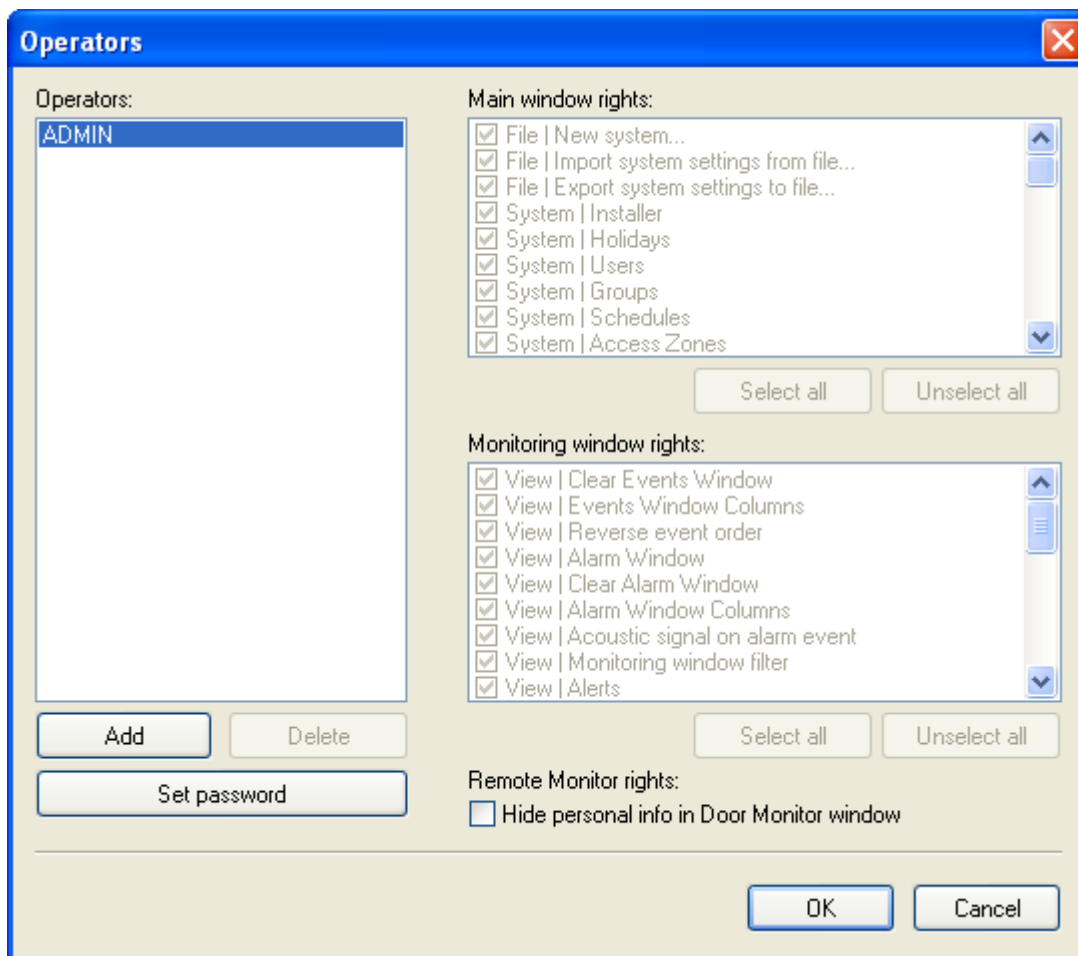
When the system is operating in an online monitoring mode, the alarm event is additionally present in the **ALARMS** window. If such an event happens, the **Alarms** bar starts flashing in red.

### 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).

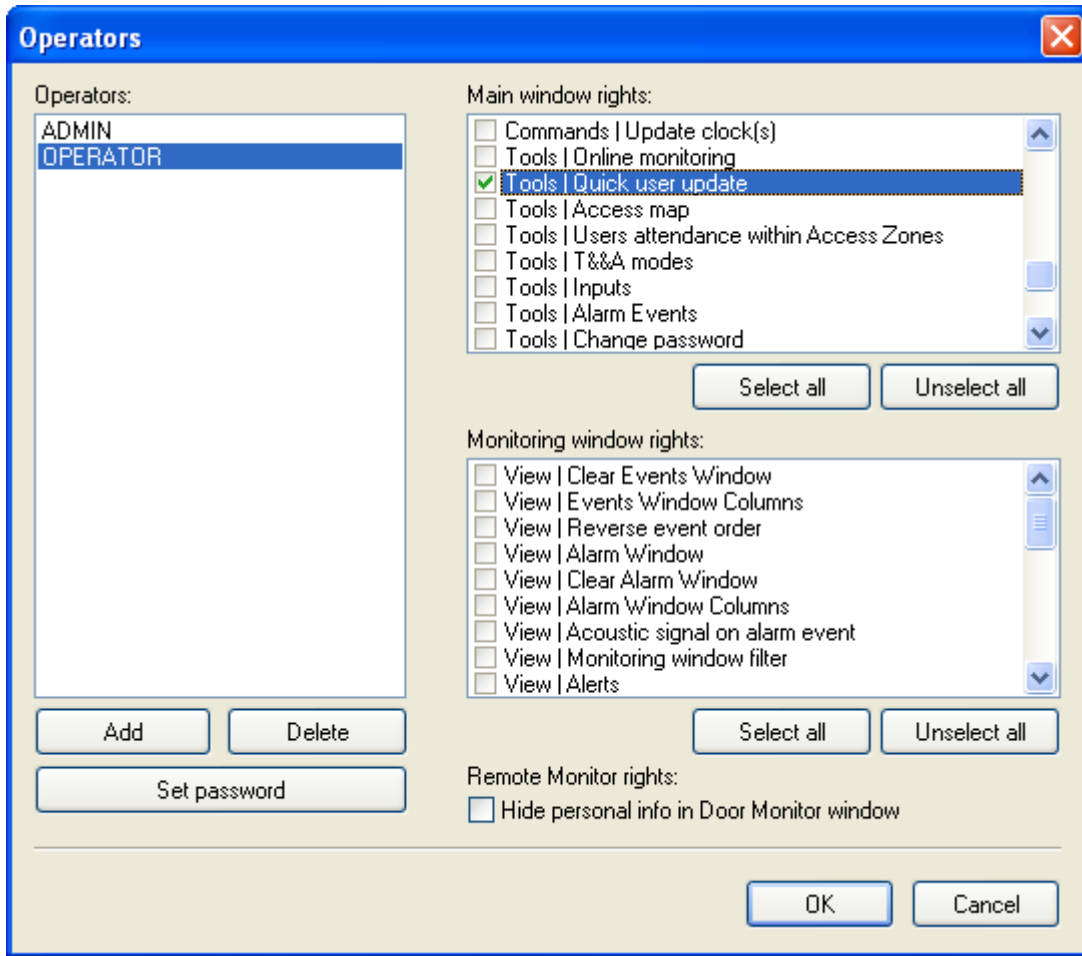




**Figure 3.132.** List of operators in the RACS

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.** User OPERATOR has rights to quick user update only

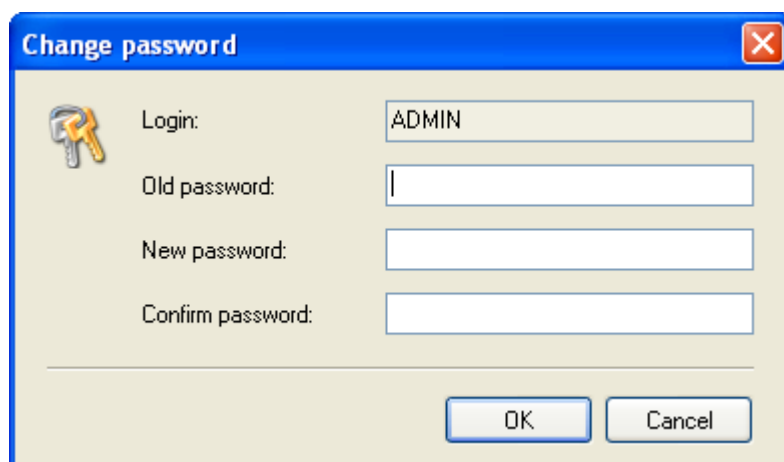
The **Select all** button present below particular option group cause selecting all the options in a group. Clicking on the **Unselect all** button cancels selection for all the options in the group.

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

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

### 3.5.9. Change Password

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



**Figure 3.134.** User OPERATOR has rights to quick user update only

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** button lets lock access to program's commands. It may be helpful when the operator is forced to go away from the keyboard 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

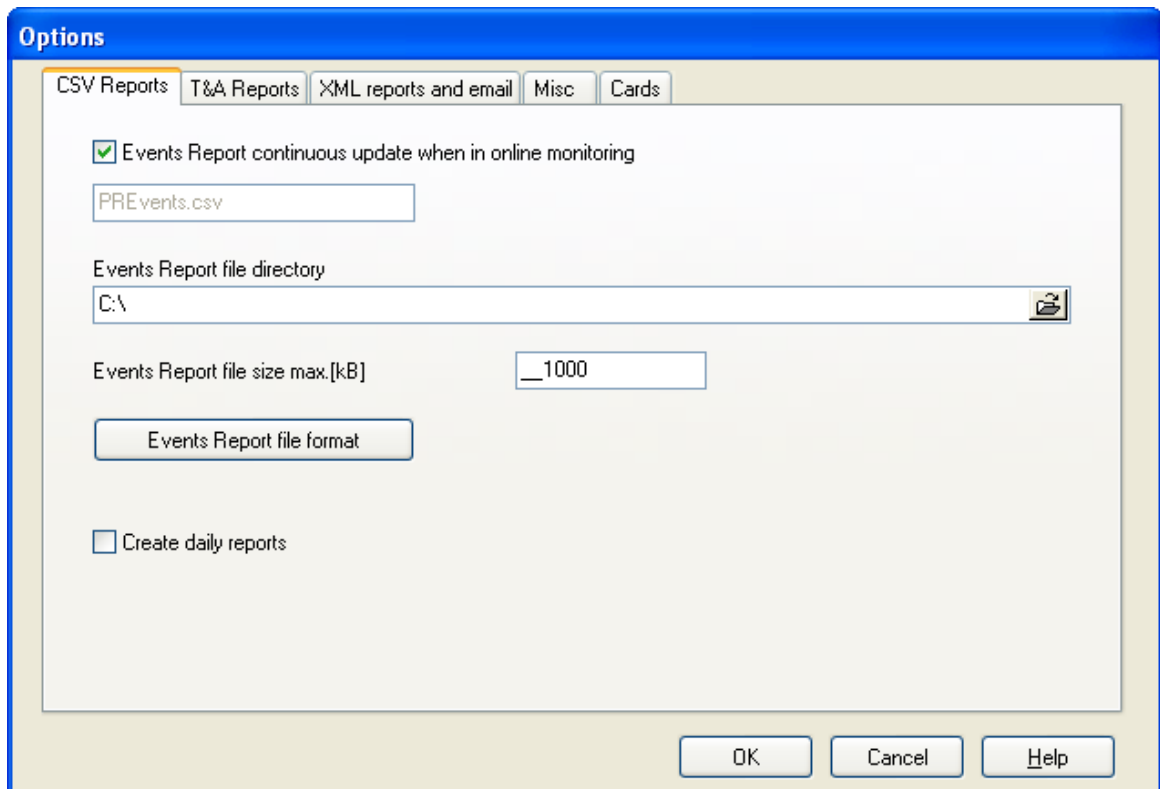
The **Options** command opens the program's options window. The window is divided into 5 tabs:

- ◆ CSV Reports
- ◆ T&A Reports
- ◆ XML reports and email
- ◆ Other
- ◆ Cards.

Options from each of these groups have been described in the following sections.

#### 3.5.11.1. CSV Reports

The **CSV Reports** tab can be used for setting options for generating **PREvents.csv** file. It has been shown in Figure 3.135.

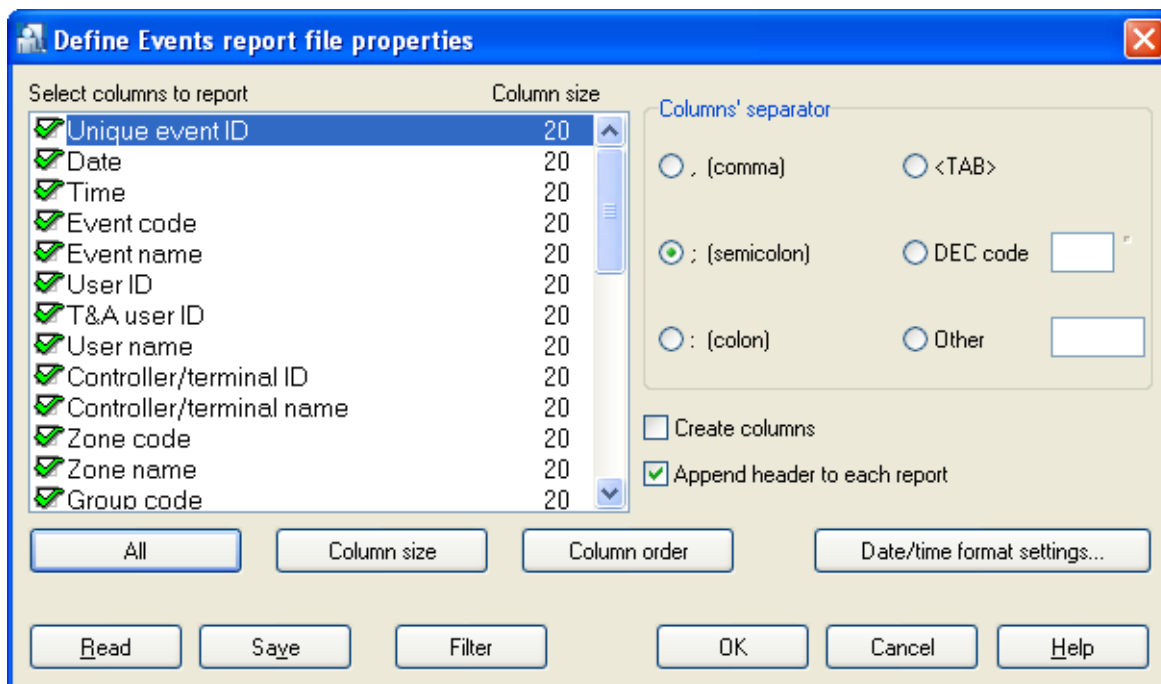


**Figure 3.135.** Options for generating CSV report

All the controls within the tab are active only when the **Events Report continuous update when in online monitoring**.

The **Events report file directory** allows for specifying a directory, where the **PREvents.csv** file will be stored. The **Events Report file size max.[kB]** is used for determining a maximum size for the file containing CSV report. By default, a maximum size for this file is 1000 kB.

The **Events Report file format** allows for defining in detail CSV report file content. If you click on it, the **Define Events report file properties** 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. User can select columns to appear in the report, determine their width, change column order and specify date and time format.

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

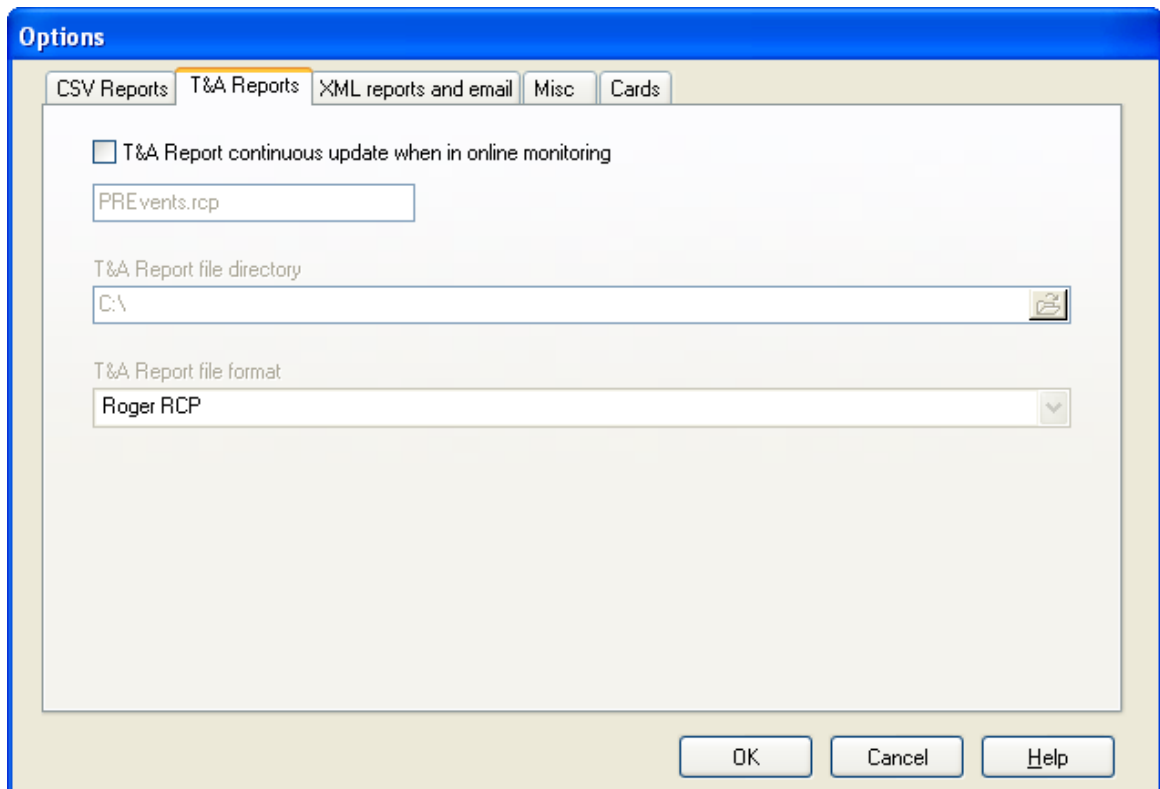
Clicking on the **Filter** button causes displaying the **Filter configuration** dialog box. Using it you can define any events filter. It is possible, for example, to save in **PREvents.csv** file only **Access denied** events for the selected user.



You can find more information on how filters can be defined in section 3.3.7.1. **Defining Filter**.

### 3.5.11.2. T&A Reports

The **T&A Reports** tab can be used for setting options for generating **PREvents.rcp** file. It has been 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 continuous update when in online monitoring** checkbox is checked.

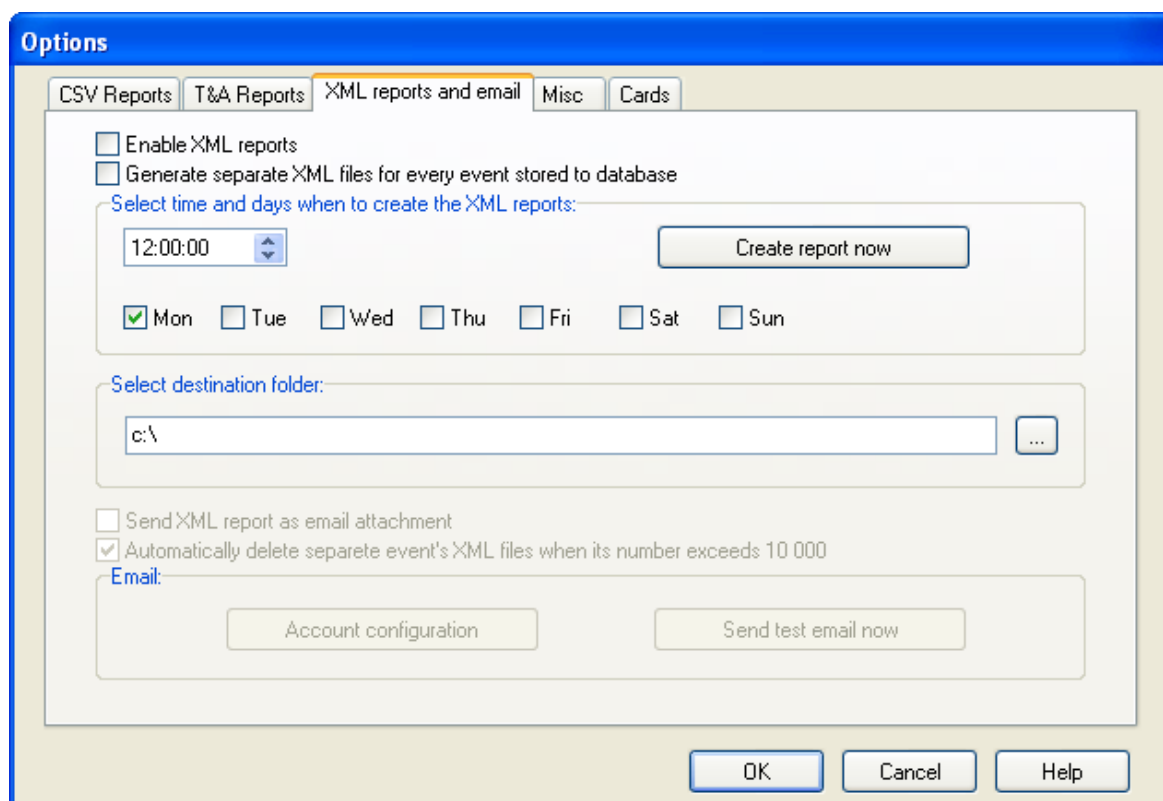
The **T&A Report file directory** allows to point the directory, where the **PREvents.rcp** file will be saved.

The **T&A Report file format** field allows selecting one of available T&A reports file formats. There are the following formats available:

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

### 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 has been shown in Figure 3.138.

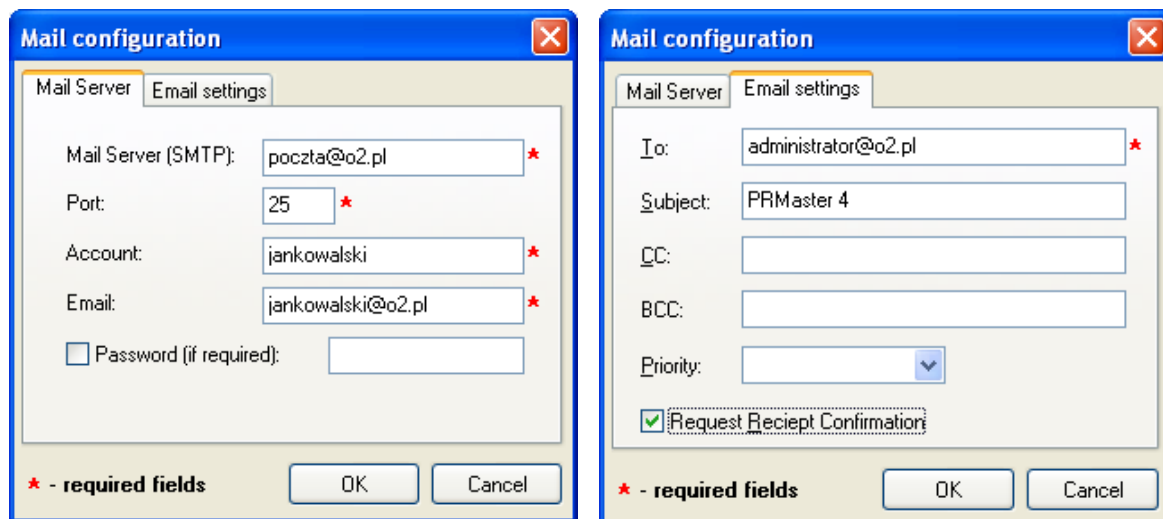


**Figure 3.138.** Options for generating T&A report

The controls in areas **Select time and days when to create the XML reports** and **Select destination folder** are active only when the **Enable XML reports** checkbox is selected. But the controls in the **Email** area are active only when the **Send XML report as email attachment** checkbox is selected.

In the **Select time and days when to create the 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 on the **Select 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, the e-mail report will be sent to. In order to do this, you should click on the **Account configuration** button. This will cause displaying **Mail configuration** dialog box (Figure 3.139).

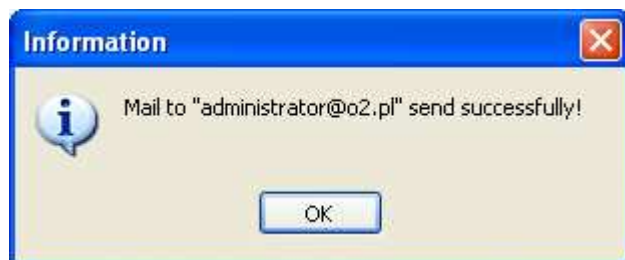


**Figure 3.139.** Mail account configuration for sending XML reports

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

If the outgoing mail server requires authentication, you should also check the **Password (if required)** check box, and to enter access password.

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 an 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,

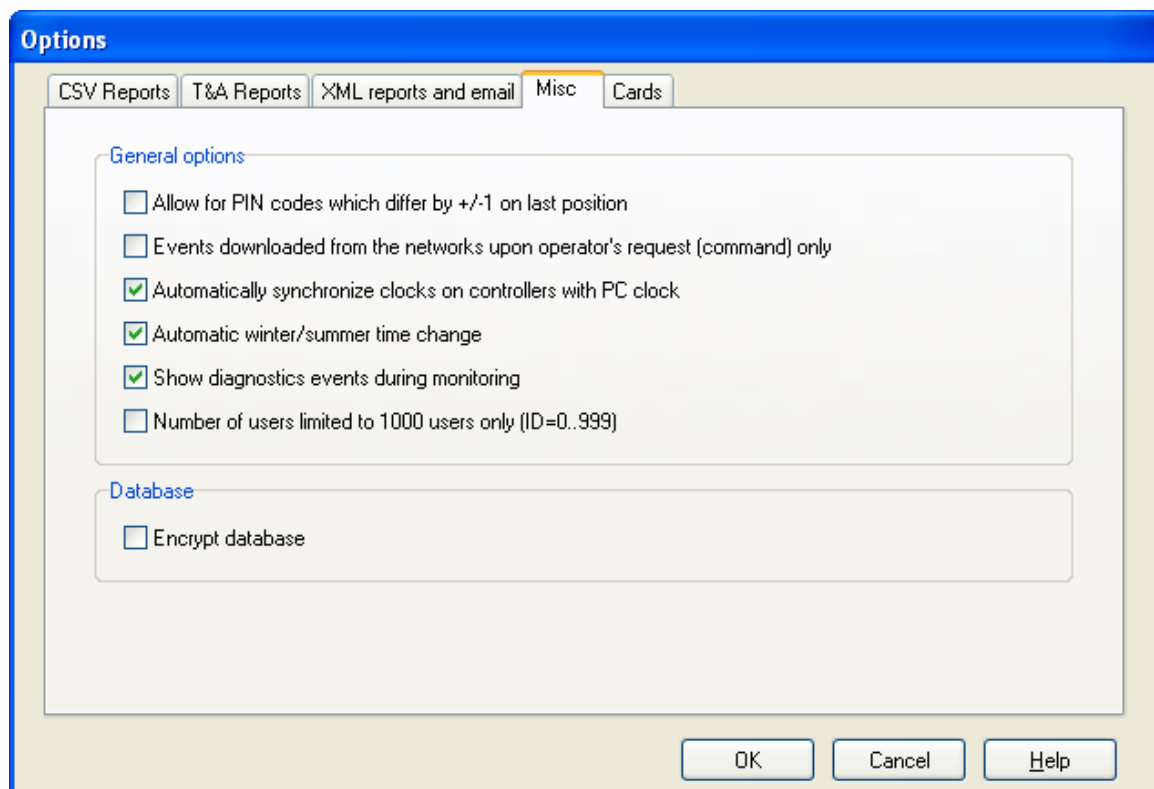


- ◆ <READER> — reader's id,
- ◆ <CARD> — card code or event code (in hex),
- ◆ <ACCESS> — this field can have values **T** or **N**. The **T** value means, that the controller has granted access, the **N** value means the opposite.

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

### 3.5.11.4. Other

The **Misc** tab (Figure 3.141) allows for configuration of various options having impact on how the system operates.



**Figure 3.141.** Miscellaneous system options

In order to enable particular option, you should select checkbox next to the label containing its description. Majority of options available in this tab are self-explanatory.

The first option in the list: **Allow for PIN codes which differ by +/-1 on last position** is worth special attention. It is related to DURESS signaling. 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) causes additionally that the event **FORCED ENTRY** is triggered and it may cause signaling on controller's alarm output.

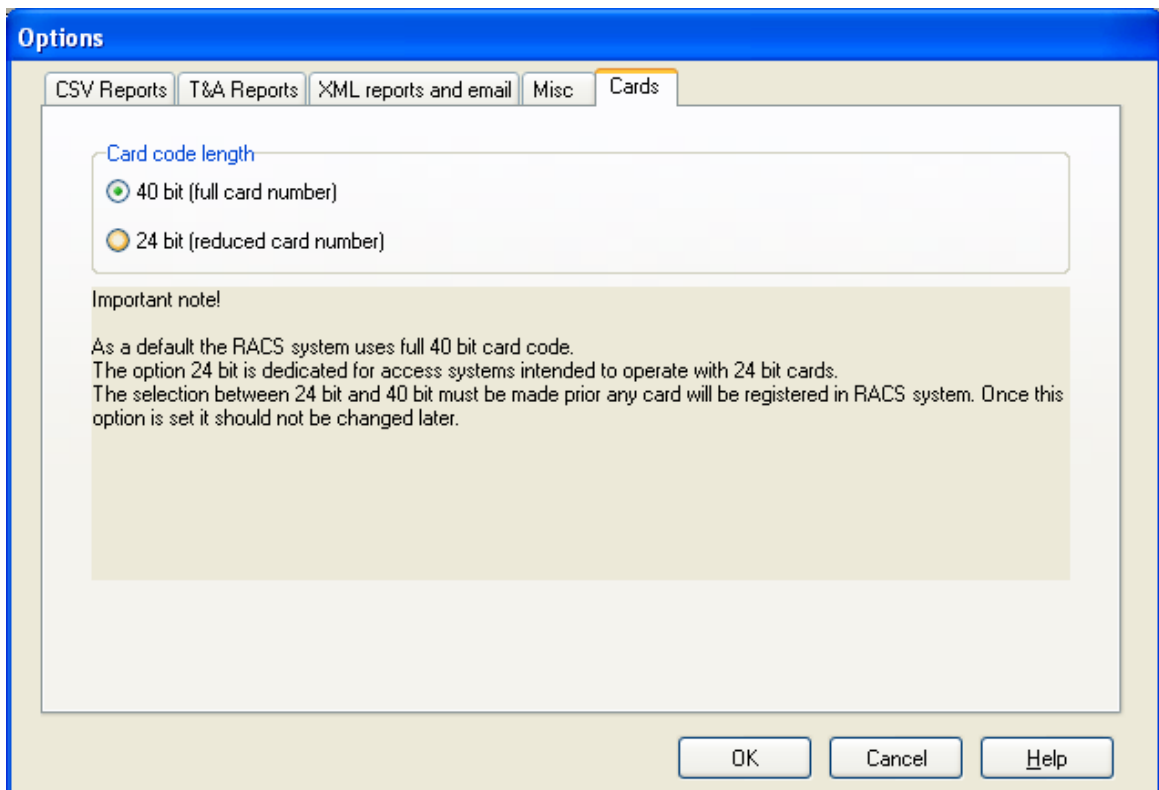
For instance, if an user uses [6789] PIN code, then entering a code [6788][#] or [6780][#] will be interpreted by the controller as using a PIN code under duress.

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 practical, 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 **Events downloaded from the networks upon operator's request (command) only** option also needs an explanation. By default, when you enter an online monitoring mode, the PR Master will read events from system buffers and write them to program's database. Because of this monitoring window directly after opening it is empty — do not contain any events. When the **Events downloaded from the networks upon operator's request (command) only** checkbox is checked, the system will read events from buffers only after online monitoring window is open. Thanks to this, events are displayed in the monitoring window and are appended to database immediately after they happen.

### 3.5.11.5. Cards

The **Cards** tab in the **Program options** window allows to select whether the card code of 40 bits length or 24 bits length should be used. This tab has been presented in Figure 3.142.



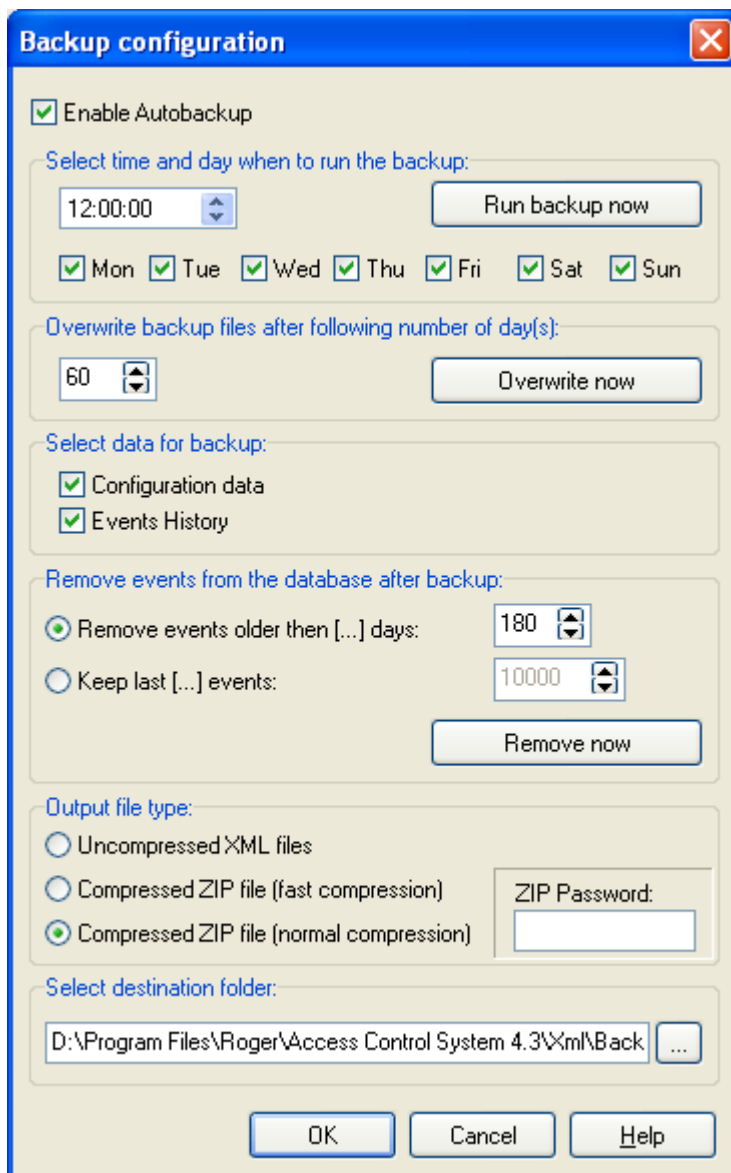
**Figure 3.142.** Card Code length options



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.

### 3.5.12. Backup configuration

Choosing the **Backup configuration** command causes displaying a dialog box allowing for defining a mode and a schedule for creating backups (Figure 3.143).



**Figure 3.143.** Options of creating system backups

The majority of controls in this dialog box is active only after you select the **Enable Autobackup** option. If this checkbox is not selected, then backups will not be created automatically. In such a case you can make backup manually. For this purpose you can click on the **Run backup now** button.


In the **Select time and day when to run the backup** you should select weekdays and times, 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, that will interfere with system operation as less as possible. The best if they were night hours, when there are relatively few events happening in the system.

The **Overwrite backup files after following number of day(s)** lets define storage period for backups. After it is expired, the backups will be 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 **Select data for backup** there are two checkboxes: **Configuration data** and **Event history**. Selecting particular checkbox will cause that data of specified type will be included in the backup. If you cancel selection these data will not be included.

The **Remove events from the database after backup** 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.

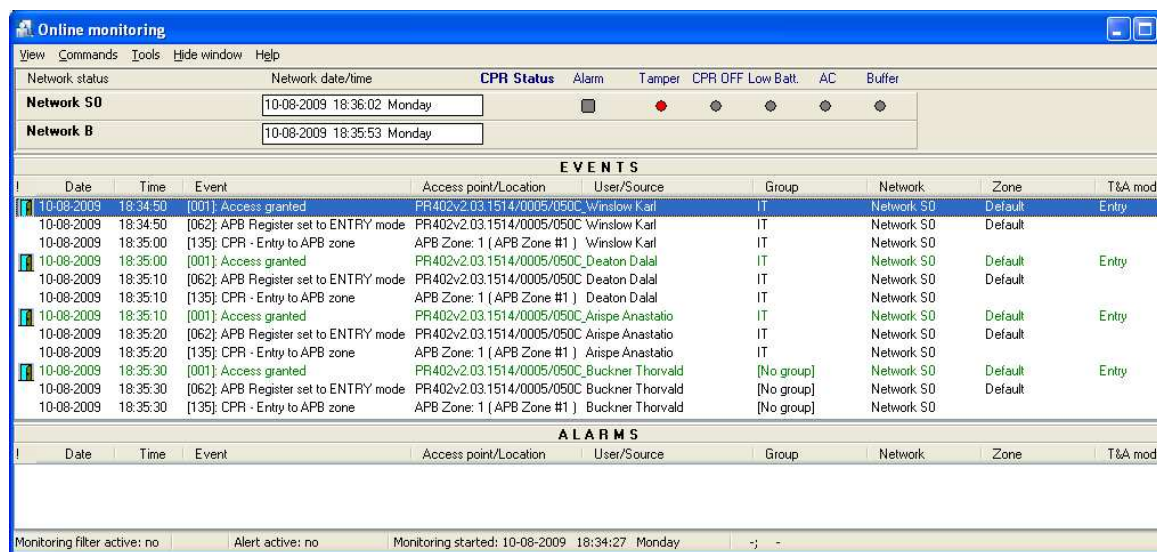
The **Output file type** allows for indicating format of a file, where a backup will be stored. You can select **Uncompressed XML** and XML formats with fast and normal ZIP compression. Optionally you can define password for the ZIP archive.

In the **Select destination folder** area you should specify directory, where the backup will be stored. Clicking on the  button allows for selecting directory from the list in a tree format.

# CHAPTER 4.

## ONLINE MONITORING

**Online monitoring** is a special mode of PR Master operation, in which events happening in the RACS are visualized in a real time and displayed in a specialized window. When PR Master operates in this mode, events happening 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** pane from the left hand side of the main program’s window. Program’s window in an online monitoring mode has been shown in Figure 4.1.



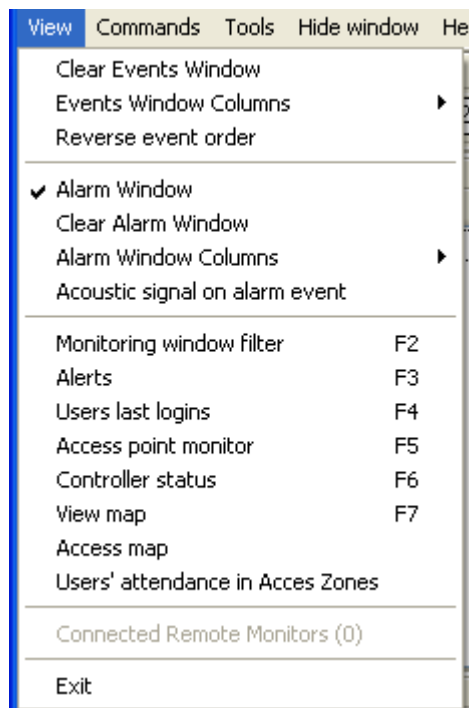
**Figure 4.1.** PR Master window in online monitoring mode

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 **ALARMS** area, where messages about alarms happening 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 has been shown in Figure 4.2.



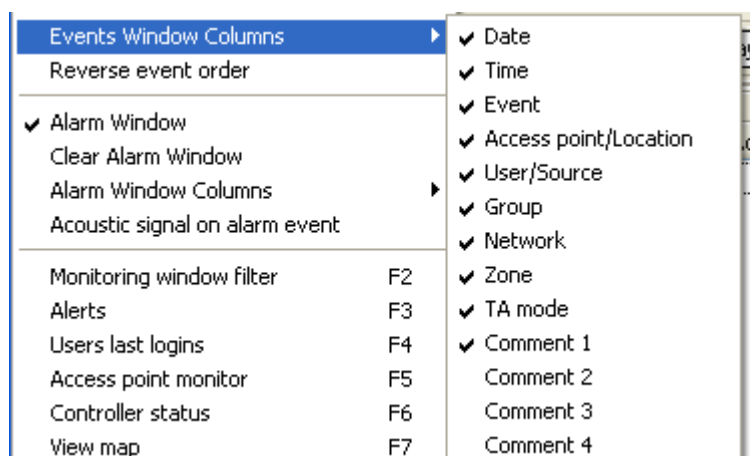
**Figure 4.2.** The PR Master's View menu in online monitoring mode

#### 4.1.1. Clear Events Window

This command clears the events window together with events displayed in **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 too many events happening in the monitoring window.

#### 4.1.2. Events Window Columns

The **Events Window Commands** command opens menu containing list of column to be selected (Figure 4.3). Selecting particular column will cause that this column will display 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 oldest to the youngest — i.e. at the beginning of the list the events which happened most recently are displayed. If you select the **Reverse event order** option, then at the top of the list events happened most recently will be displayed.

### 4.1.4. Alarm Window

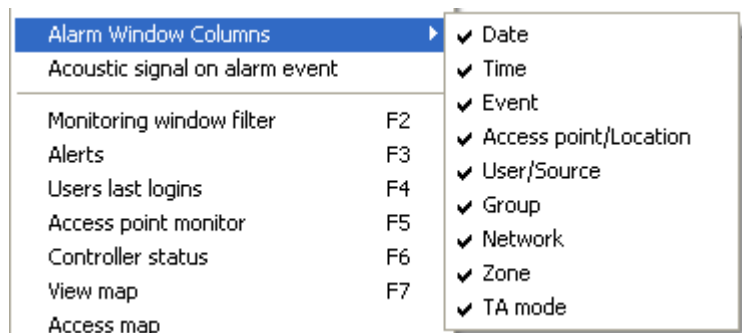
The **Alarm Window** option lets you switch on or off the **ALARMS** window. If it is selected, the ALARMS window is displayed.

### 4.1.5. Clear Alarm 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 alarms which happened earlier.

### 4.1.6. Alarm Window Columns

The **Alarm Window Columns** command opens menu containing list of column to be selected (Figure 4.4). Selecting particular column will cause that this column will be displayed in the **ALARMS** window.



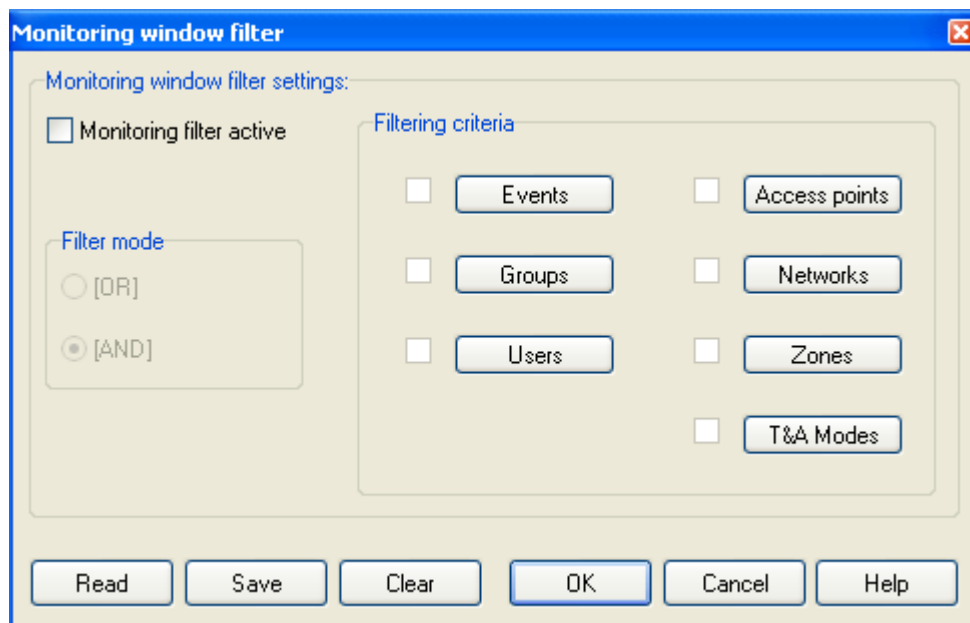
**Figure 4.4.** Selecting columns to be displayed in the ALARMS window

### 4.1.7. Acoustic signal on alarm event

Selecting this option causes that alarm events will be additionally signaled acoustically. When this option is disabled, an alarm event will display in windows **EVENTS** and **ALARMS** but without acoustic signal.

### 4.1.8. Monitoring window filter

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



**Figure 4.5.** Defining filter in Online monitoring window

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



The filter defined is related to 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 window filter** command and click **OK** in the dialog box which will appear.

#### 4.1.9. Alerts

Using this option allows for defining filter for the events which are to be signaled acoustically. If you select this command, the **Alert definitions** dialog box displays (Figure 4.6).



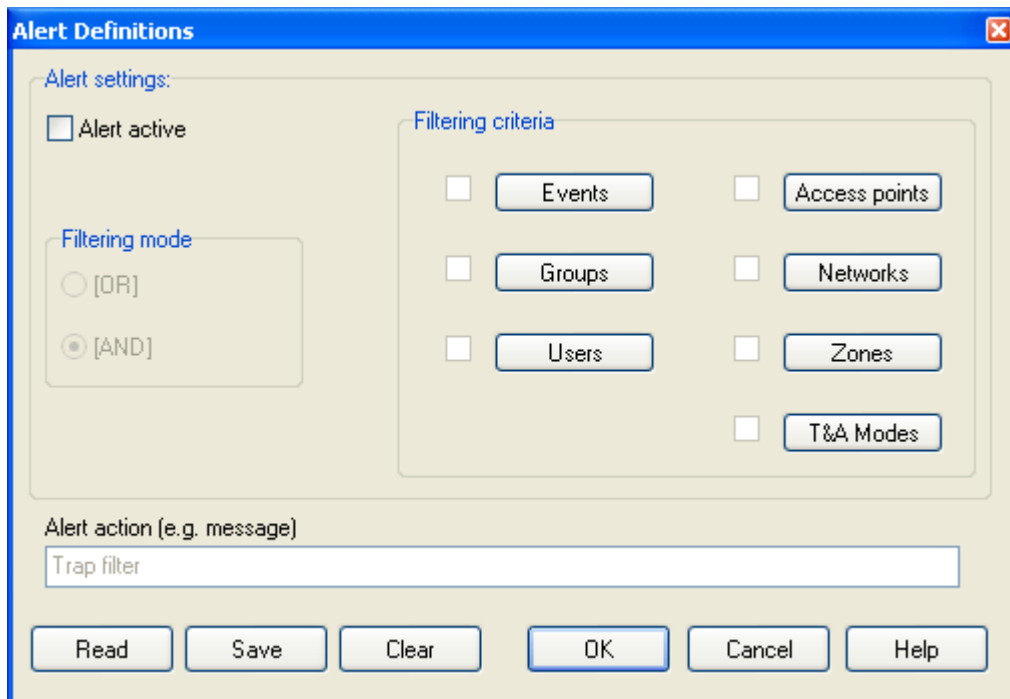


Figure 4.6. Defining filter for the events which are to be signaled acoustically

This dialog box can be used in the same way as the dialog box for defining events report filter (see section 3.3.7). This window differs from the one described in section 3.3.7 by one additional field: **Alert action (e.g. message)**. This field allows for defining an additional message which should be displayed when an alarm happens.

### 4.1.10. Users last logins

The **Users last logins** command lets locate a place (a reader) where particular user logged in for the last time. If you select this command, the **Users last login** window appears (Figure 4.7).

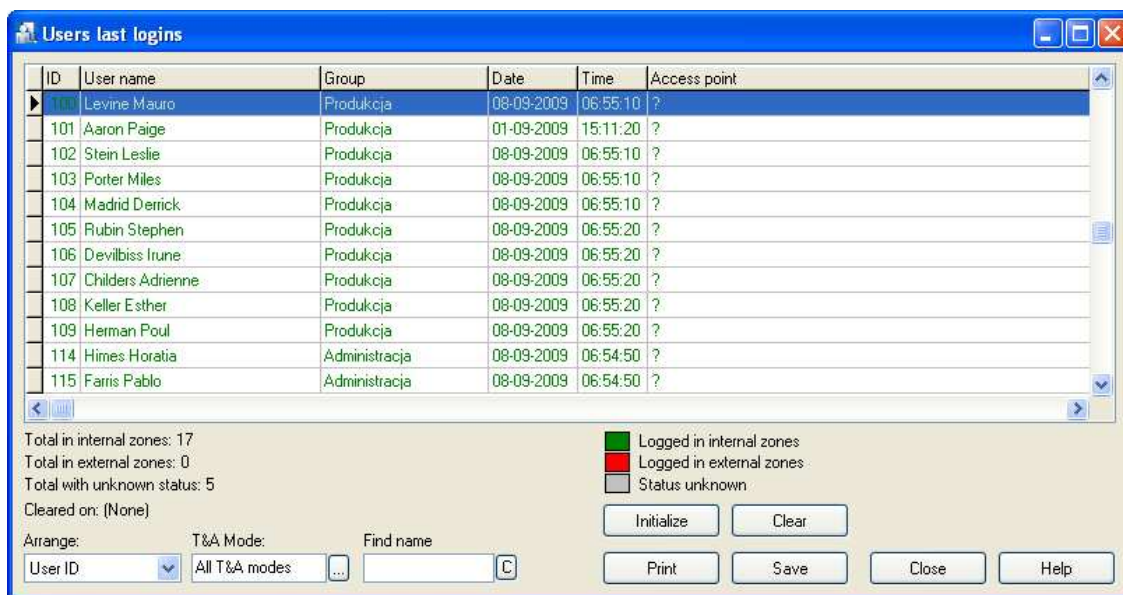


Figure 4.7. Places where users logged in recently

The window contains a list of users marked with different colors depending on their login status. Under the list there is a summary containing number of users with particular status and an explanation of colors meaning. The **Arrange** listbox lets sort the list of users by their ID, name, group, date/time or the reader. The **T&A Mode** field allows to select only these controllers which register the selected T&A mode. The **Find name** field allows locating in the list the user with given name. System performs „active search“ i.e as you enter successive letters, the system locates a user who satisfies a criteria defined.

The **Initialize** button initializes a list of logins based on the current event history in the RACS. The **Clear** button clears the list of last logins.

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. Access Point Monitor

The **Access Point Monitor** command lets you visualize information about user using its ID on selected passages. If you select this command, the **Access point monitor** dialog box displays (Figure 4.8).



**Figure 4.8.** Access point monitor

In this window you should select identification points which are to be monitored. In case the users logs in on one of the selected points, the program will display information regarding the event accompanied with user's data (among others his or her photo). In this way you can verify, if particular ID is used by the proper person. This is especially important in systems having many users.

If you select the **Events related to users only** option, then only these events which require using ID will be monitored in the window.

#### 4.1.12. Controller status

The **Controller status** command displays a window containing information on controllers working in RACS (Figure 4.9).

Controller	Door mode	Identification n	Terminals ID0	Inputs	Door status	PR Ping	CPR-PR Ping	Arming mode
PR311SEv1.11.1215/0001/088	Normal	Card or PIN / (Absent	ON / OFF / OFF / NA	Door open	OK	OK	Armed	
PR302/146.2/0010/1898	Normal	Card or PIN / (Present	ON / OFF / OFF / NA	Door open	OK	OK	Armed	

Figure 4.9. 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.,

### 4.1.13. View map

The **View map** command allows to visually monitor the system using facility plans defined earlier (see section 3.2.13. Facility plans). After you select this command, the **Facility plan manager** window displays (Figure 4.10) which lets user select facility plans to be displayed.

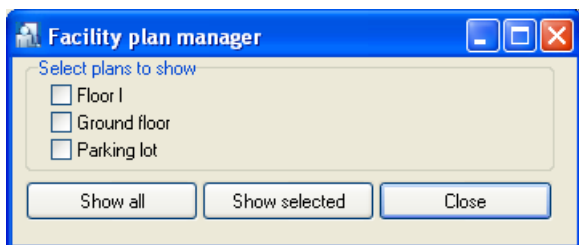


Figure 4.10. Facility plan manager — selecting plans for display

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 4.11.

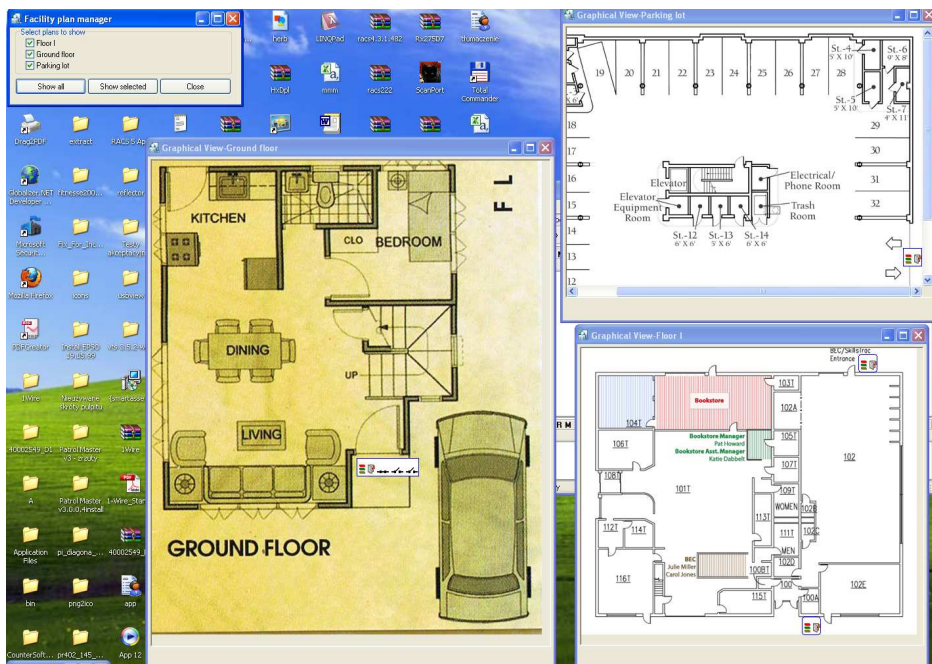
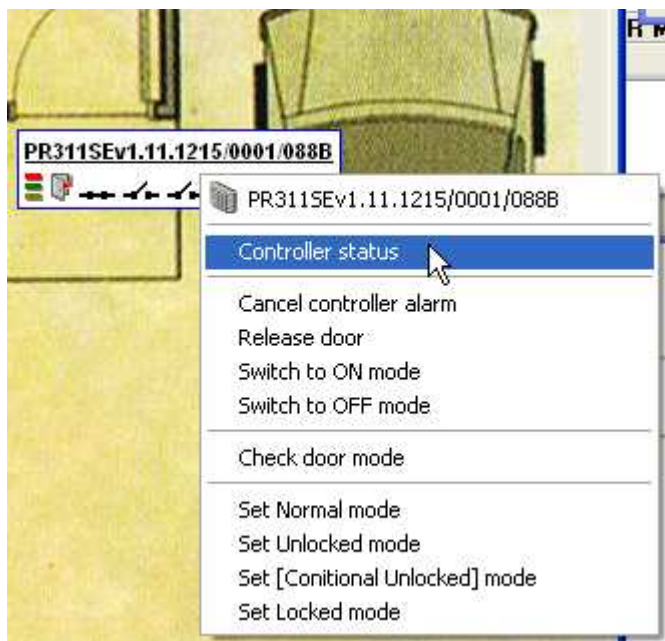


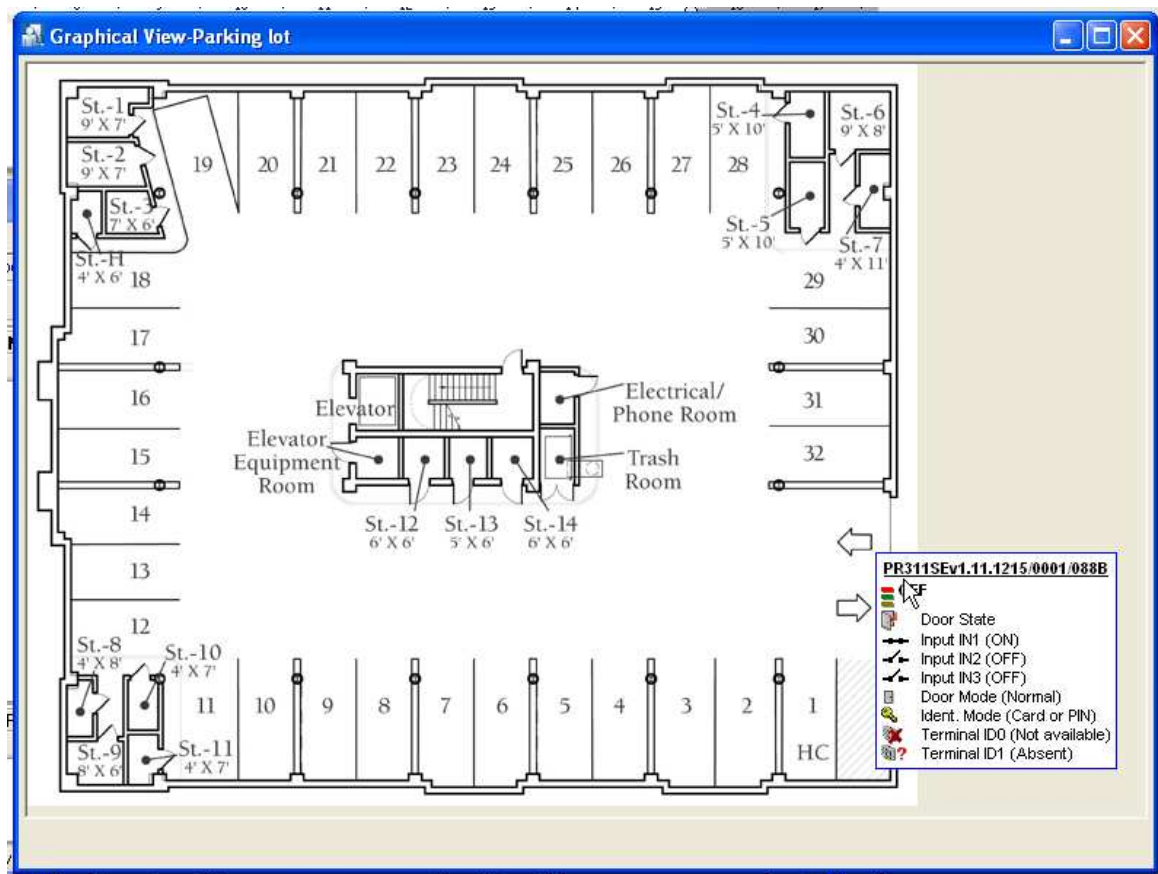
Figure 4.11. Visual mode of facility monitoring

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 4.12).



**Figure 4.12.** *Controller's command menu*

If you 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 a minimum icon.



**Figure 4.13.** 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.

#### 4.1.14. Access map

This command is an equivalent for the **Tools/Access map** command available outside the monitoring mode. It has been described in **section 3.5.3**.

#### 4.1.15. Users' attendance in Access Zones

The **Users' attendance in Access Zones** is an equivalent for the **Tools/Users attendance within Access zones** available outside the monitoring mode. It has been described in **3.5.4. Users attendance within Access Zones**.

#### 4.1.16. Connected Remote Monitors

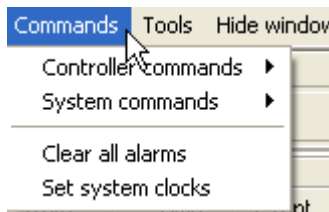
Remote Monitor program can be a client to PR Master software. It lets you remotely monitor the RACS. The **Connected Remote Monitors** command shows you how many Remote Monitor clients which established connection with PR Master are running.

### 4.1.17. Exit

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

## 4.2. COMMANDS MENU

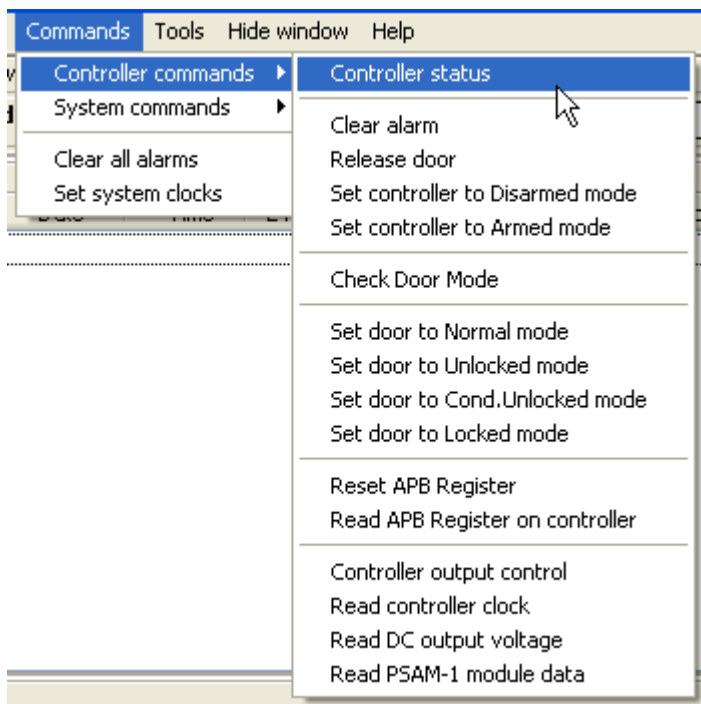
The **Commands** menu of an online monitoring mode has been shown in Figure 4.14.



**Figure 4.14.** *Commands menu*

### 4.2.1. Controllers command submenu

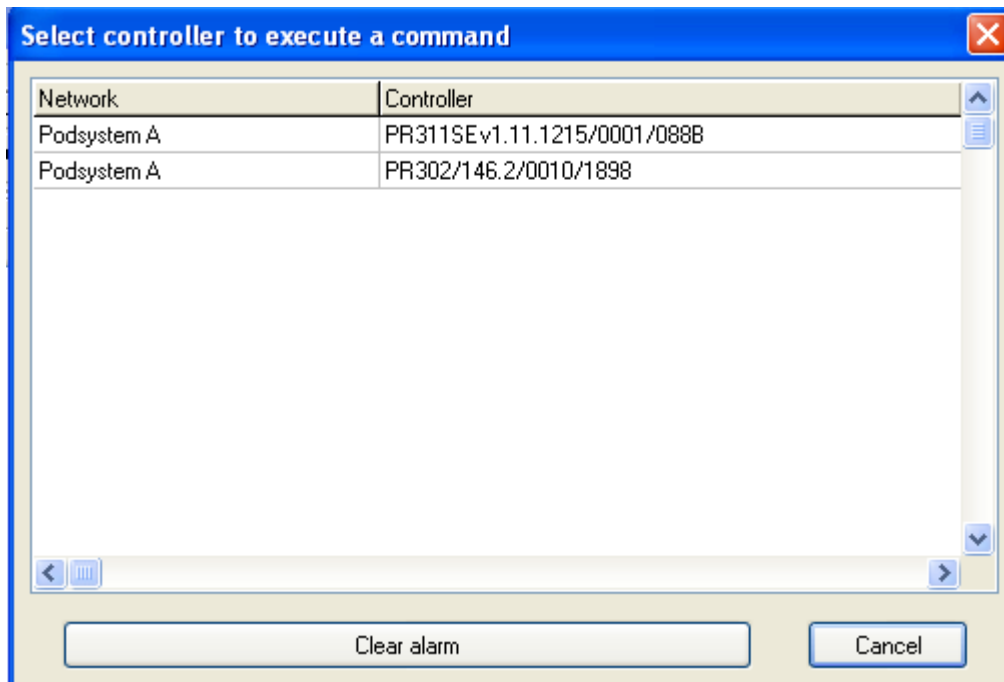
The **Controller commands** submenu contains a list of commands which can be run against selected controller. It has been shown in Figure 4.15.



**Figure 4.15.** *Controllers command submenu*

Selecting any command from this submenu causes displaying controller selection window (Figure 4.16).



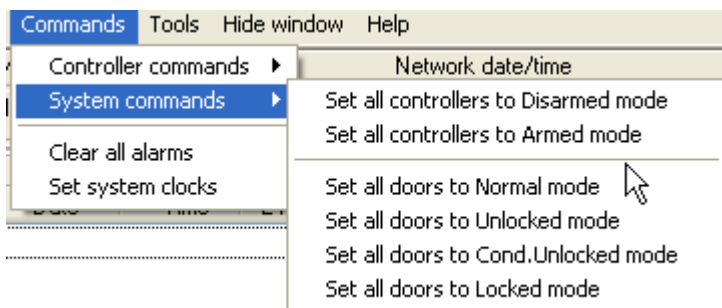


**Figure 4.16.** Controller selection window displayed before executing chosen command

You should select controller in the list, and then click the button with command’s name (in case shown in Figure 4.16 it is the **Clear alarm** command). In case when you do not select any controller the command will be executed against first controller in the list.

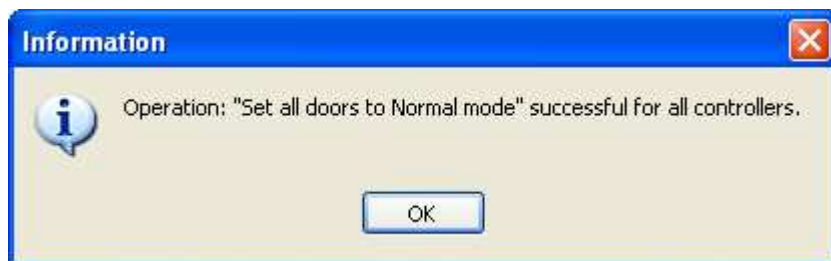
### 4.2.2. System submenu

The **System** submenu contains a list of commands related to the whole system. It has been shown in Figure 4.17.



**Figure 4.17.** The System commands submenu

Selecting any command from this submenu causes executing the command for all the controllers in the whole system. After an operation is performed, the program displays confirmation that it has been executed (Figure 4.18).



**Figure 4.18.** Confirmation on executing command on all the controllers in the system.

### 4.2.3. Clear all alarms

The **Clear all alarms** command causes cancellation of all the alarm currently existing in the RACS. If there is no alarms at the moment, then executing the command will have no effect.

### 4.2.4. Set system clocks

The **Set system clocks** command allows for setting all RACS devices' clocks with accordance to system clock settings of the computer the PR Master software is installed on. If you select this command, the system will display a message box with question for confirmation (Figure 4.19).

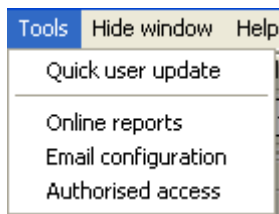


**Figure 4.19.** Setting clocks in the RACS

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

## 4.3. TOOLS MENU

The **Tools** menu of an online monitoring mode has been shown in Figure 4.20.



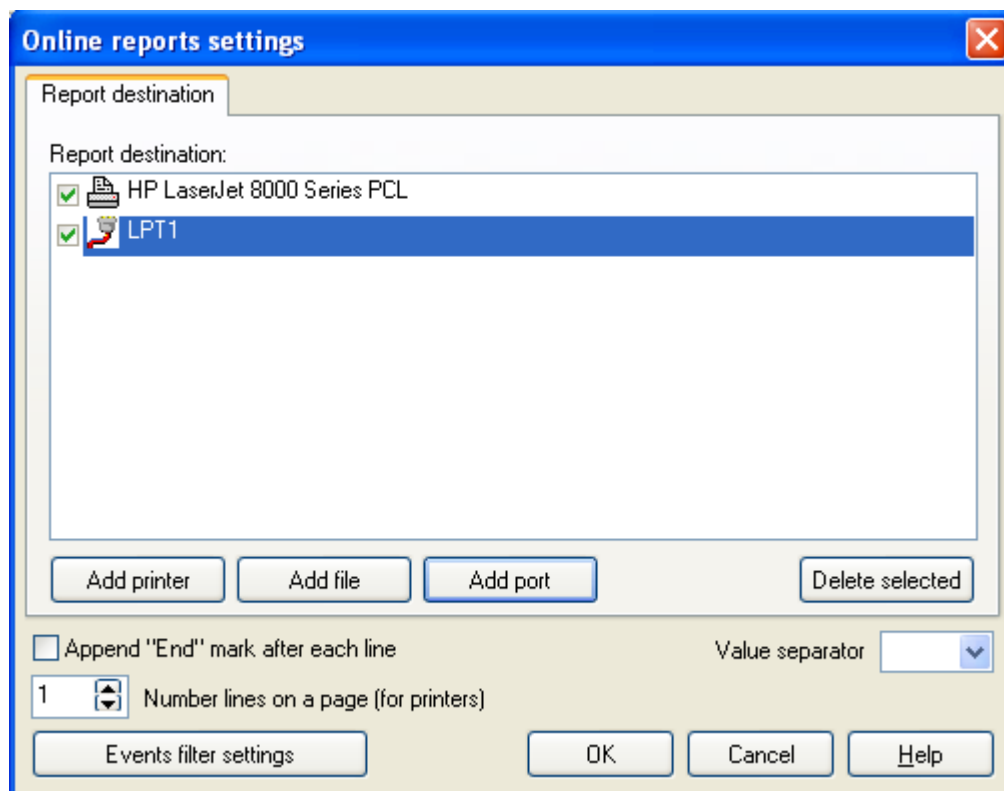
**Figure 4.20.** Tools Menu

### 4.3.1. Quick user update

This command is an equivalent for the **Tools/Quick user update** command available outside the monitoring mode. It has been described in **3.5.2. Quick user update**.

### 4.3.2. Online reports

The **Online reports** command lets you send on an ongoing basis all the events from the RACS to defined devices or files. If you select this command, the **Online reports setting** window appears (Figure 4.21).



**Figure 4.21.** *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** listbox allows to select special symbol which will be used to separate particular data. It can be comma, semicolon or special character (such as **CR** or **LF**).

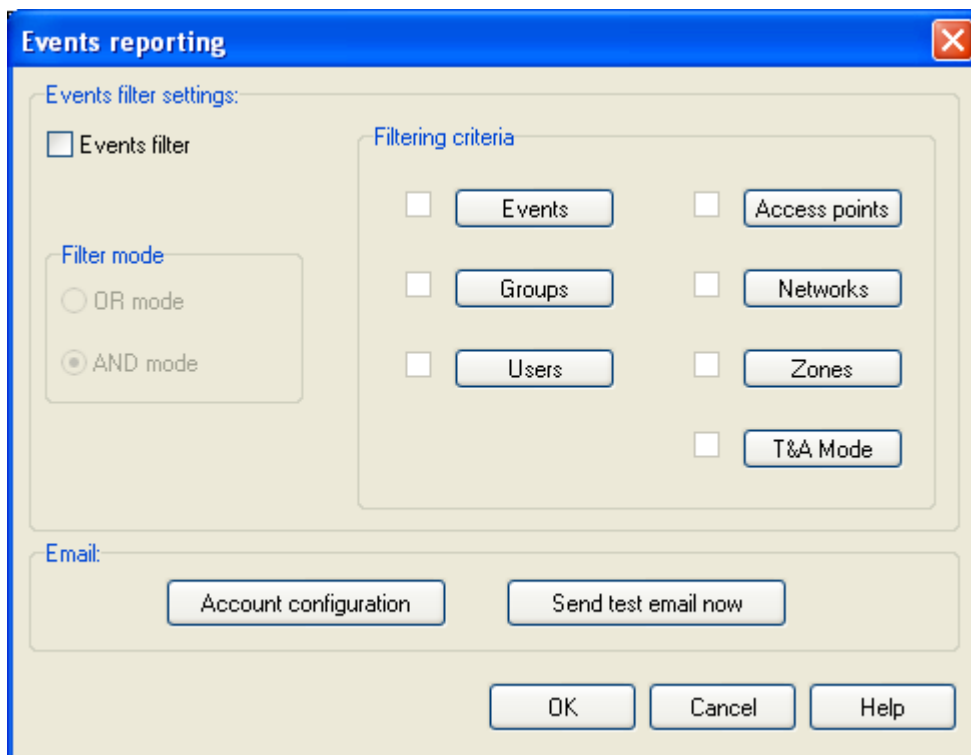
Clicking on the **Events filter settings** button causes displaying the **Filter configuration** dialog box where you can define a filter for events being printed.



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

### 4.3.3. Email configuration

Selecting the **Email configuration** command causes displaying the **Events reporting** dialog box (Figure 4.22).

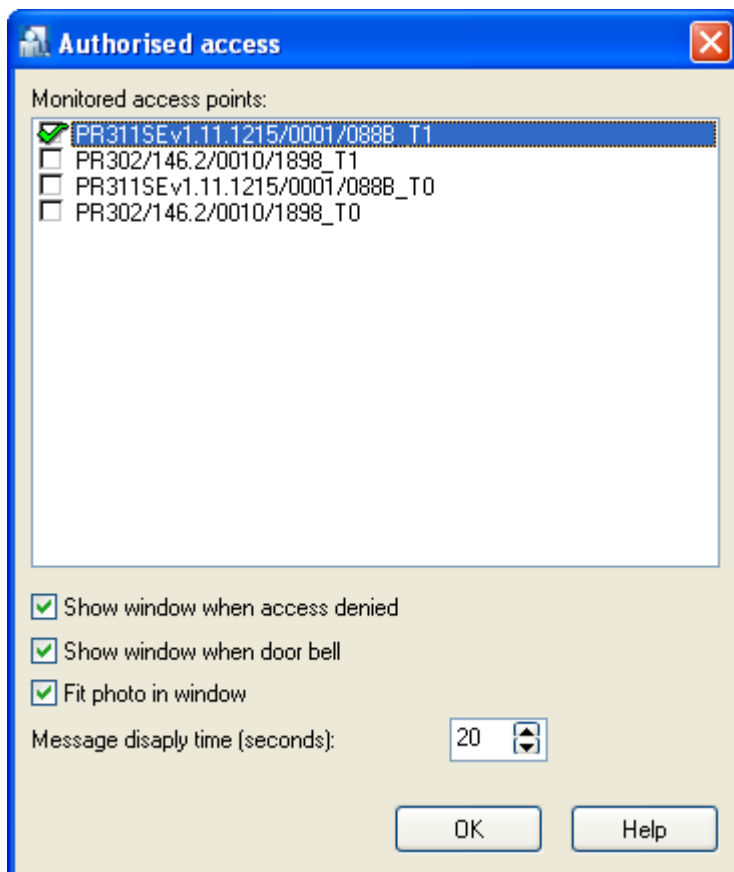


**Figure 4.22.** *Setting up events reports sent by e-mail*

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

#### 4.3.4. Authorised access

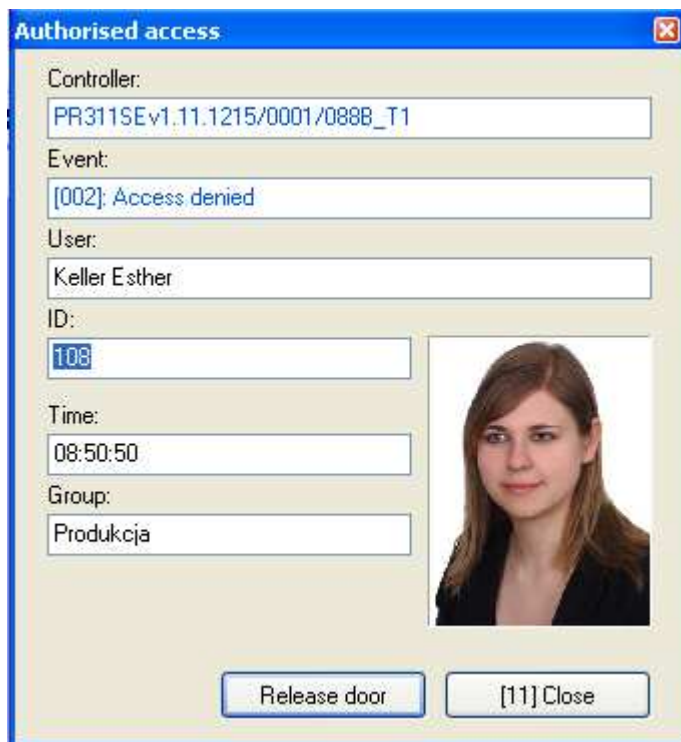
The **Authorised access** command allows for granting access to a person by the RACS operator in situation when the system would normally refuse to grant access. It may be useful for granting exceptional access to user trying to enter the facility beyond the period he has rights to enter or in reply to using bell. Executing this command will cause displaying **Authorised access** dialog box (Figure 4.23).



**Figure 4.23.** *Setting up an authorised access*

In the **Monitored access points** list you can select controllers, the access on request command should be applied to. 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 to grant 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. 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 **Message display time (seconds)** spin box defines time (in seconds) for which the **Authorised access** window shows up.

If the option **Authorised access** has been configured, then in case the system refuses access to the user, it displays at the same time the **Authorised access** dialog box (Figure 4.24).



**Figure 4.24.** *Authorised access command*

In this window you can find information about the controller, the event as well as information on user requesting an access. In square brackets on the **Close** button the number of seconds remaining until closing the window is displayed. If during this time an operator clicks on the **Release door** button, then the controller will grant to the user an access on request.

## 4.2. HIDE WINDOW

There is a **Hide window** command in the main menu of an online monitoring mode. Clicking on it causes minimizing the monitoring window. To reopen the window you should click on the PR Master icon on the Windows task bar.