



User Manual

preliminary document

© 2006 ... Roger Sp. J.

roger[®]

ROGER ACCESS CONTROL SYSTEM

Table of Contents

Part 1 Introduction to PR Master 4.2	1
Part 2 Glossary	2
Part 3 Using Help	3
Part 4 Installation, first start and registration	4
1 Autologin	6
2 Installation on MS Windows Server 2003	6
3 System requirements and installation tips	7
Part 5 System database of RACS	8
1 Local system database	9
2 Network system database	9
Part 6 Using program	12
1 Main window	12
2 Main menu	13
Edit	14
Installer	14
Arm/Disarm schedule.....	14
Holidays	16
Attendance.....	17
Card Box.....	19
F7 Fingerprint Readers.....	21
APB Zones	23
ARM Zones.....	24
Commands	26
Tools	26
Quick user update	26
T&A modes.....	27
Switching T&A Mode.....	28
Types of Inputs.....	29
Types of events.....	30
Program operators.....	31
Change password.....	32
Lock program.....	33
Options	33
Reports CSV.....	33
T&A Reports.....	34
XML reports and e-mail.....	35
Misc	37
Cards	38
Backup configuration.....	38
Part 7 Groups	39

1	Add access groups	40
2	Group properties	41
Part 8	Users	42
1	Add users	44
2	User Properties	45
3	Read card code	46
4	Delete users	46
Part 9	Time schedules.....	47
1	General purpose schedules	48
2	APB reset schedules	49
3	Door mode schedules	50
4	Identification Mode Schedule	51
5	T&A mode schedules	52
Part 10	Zones	53
1	Add access zone	54
Part 11	Networks.....	54
1	Network properties	56
UT-4 configuration	58	
Network properties.....	58	
DIGI configuration	59	
2	Configure CPR in network	68
3	Send network configuration	69
4	Update configuration of CPR	70
5	Controllers	70
Add controllers	71	
Controller properties	72	
General	72	
Terminal ID1, ID0.....	73	
Access	75	
Inputs IN1, IN2, IN3, IN4.....	76	
IO1, IO2 Output.....	79	
REL1, REL2 Output.....	80	
Options	81	
Advanced.....	84	
Timers	86	
[F1] - [F4] Key.....	86	
Keypad commands.....	87	
Send configuration settings to controller	89	
Diagnostics	90	
Commands to controller	92	
Microprocessor Firmware upgrade	93	
Part 12	Monitoring.....	96
1	View	96
Monitoring filter	97	
Events Alert	98	
User login table	99	

Access point monitor	100
Controller status	101
View map (Graphical View)	102
2 Commands	103
3 Tools	104
Operator rights	104
Online reports	105
Events mail configuration	106
Part 13 Events	108
1 Filter configuration	108
2 CSV Report	110
3 T&A report	111
4 Attendance in area report	114
5 Reports	115
Part 14 System with/without CPR.....	115

1 Introduction to PR Master 4.2



PR Master 4.2 is a software to supervise access control system based on control panels CPR-32 and PR controllers delivered by Roger Company.

The application is adapted to work in operating systems: Microsoft Windows 98, Windows NT, Windows 2000 and Windows XP.

- The software package can also function in Windows 95, however update of this system is necessary. Detailed description of update procedure is available on www.roger.pl site.
- The most stable work of RACS software can be achieved on Microsoft Windows XP and 2000 operation systems.

Main features of PR Master 4.2:

- operate with access control system database,
- configurable database backup files,
- configuration export/import to/from external XML file,
- automatic or interactive system events reading,
- events registry review and reports generation,
- events export to text files and payroll software,
- user time and attendance in defined system areas,
- interactive commands to controllers,
- real-time online events display,
- events monitoring on local and remote computers,
- event notifications to email accounts,
- online events reports to TXT files,
- operator selectable filtering of events,
- event notifications to email accounts,
- visualization of system work on graphic background (object map).

2 Glossary

Here are main concepts and definitions applied in following instruction. Many of the words or terms in this guide have more common definitions than used in industry. In this document, we've used them specifically in the context of access control system. For this reason, the following glossary of terms defines these terms as used in this guide.

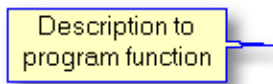
The most important concepts related to RACS:

- **RACS** - Roger Access Control System is a network access control system based on PRxx1, PRxx2 series controllers, PRT identification terminals (readers) and optional CPR control panel.
- **AC** - Access Control
- **T&A** - Time and Attendance
- **Control panel (CPR)** - element of RACS system, function as external events buffer, synchronize real time clocks of all controllers, manage access rights on controllers PRxx1 series. Control panel presence in RACS is optional and results from functional expectations.
- **Controller** - device which controls users movements within precincts of one passage (one-way or two-way). In case two-way passage, two access-points are required.
- **Terminal** - remote device (reader) which main purpose is to read identifier and send data to controller for further converting. Identifier can be e.g. proximity card, PIN code, fingerprint.
- **Proximity transponder** - electronic chip with unique code included, which reading is carried out with no-contact method. Transponders are offered as: ISO card, PVC card,
- **Access Point** - passage (entry/exit) where access is controlled by a controller.
- **User** - person registered in the access system database.
- **System operator** - person allowed to operate and supervise RACS system.
- **Events history** - pack of events registered during system work.
- **Events buffer** - battery sustained electronic memory where events are stored
- **Monitoring Mode** - working mode of PR Master, which consist in events visualization in a real mode. When PR Master remains in a Monitoring mode, occurred events are immediately appended to system database and are available to export and report generating.

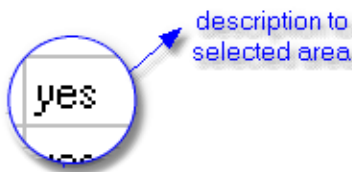
3 Using Help

To better understand this document and make using PR Master easier, we applied many types of callouts, notes and symbols. Every element of this help is used to different purposes.

Types of callouts used in Help:



Callout with yellow background and blue borders is applied to explain options, functions of the program windows and its contents



Blue text with shadow describes zoom or selected regions of windows

Area with blue outline is used to zoom or mark important part of windows



Describes interactive links



Under the light bulb symbol are hints, tips and warnings about operating program

See also:

[Link](#)

Here are additional links associated with topics. It appears inside the text too.

Text from paragraph

Blue text identifies a key words of the topic.

4 Installation, first start and registration

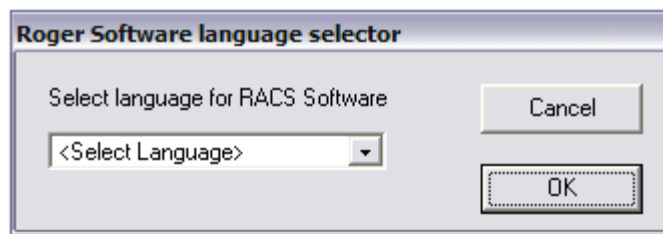
Software package is delivered on ROGER CD-ROM and available to download on www site www.roger.pl. To install RACS software from CD-ROM click on **start.exe**

PR Master package consist from programs:

- PR Master
- Language Selector
- Remote Monitor

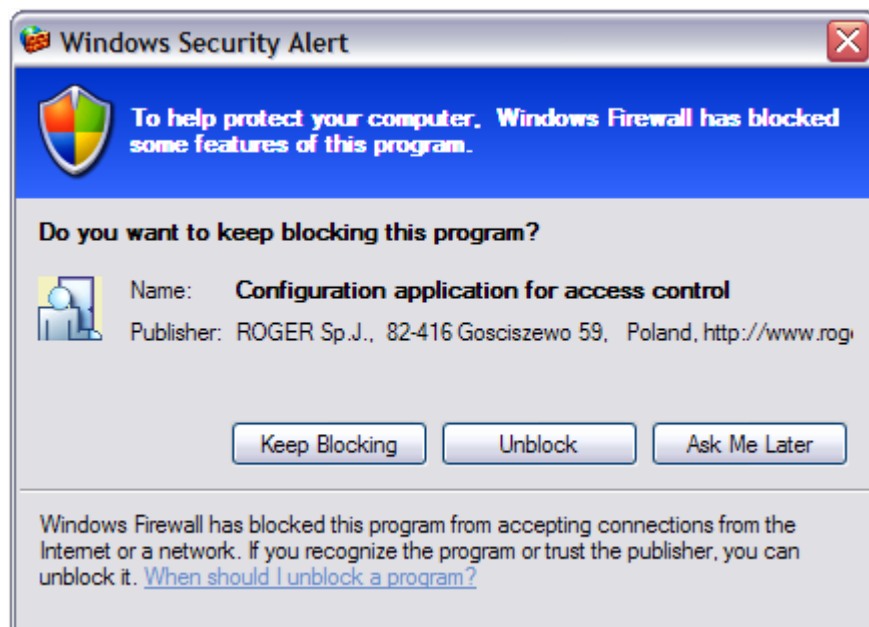
Program is installed in English language version. To [change language](#) you should:

- Choose from menu **Start -> Programs -> Roger ACS 4.2 -> Select language**.
- Select language from menu and click **OK**.



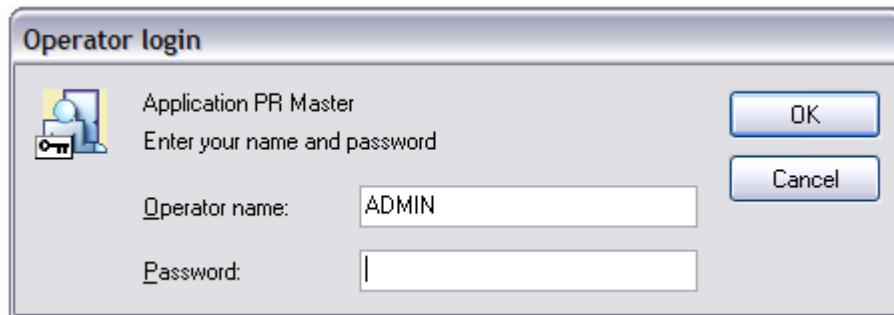
First start of PR Master

In case RACS package is installed on Windows XP with Service Pack 2 you should configure Windows Firewall properly. When you run PR Master for the first time following window will appear:

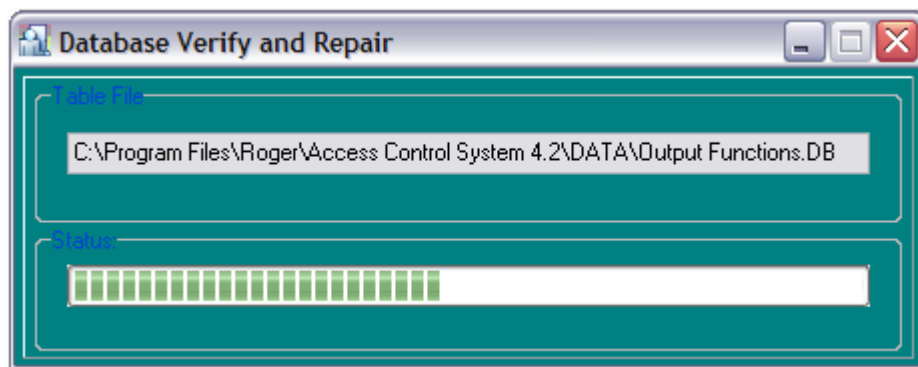


During the PR Master start, program trying to open ports to listen and communicate with Remote Monitor applications. If RACS will work with Remote Monitor you should click on **Unblock**, if not: click on **Keep Blocking**.

Operator Login



By default ADMIN operator without password is defined, click **OK** to log in.



Database Verify and Repair

Before every startup PR Master verify and repair database of RACS. Program automatically regenerate table file when detect error in database. It's available to repair database indexes from menu: **Start -> Programs -> Roger ACS 4.2 -> Repair database indexes**. Remember to close PR Master before you start Repair database procedure.

DEMO

When PR Master is started for the first time you have possibility to load DEMO configuration. It enables you to learn available features of the PR Master 4.2. In DEMO configuration you have one Network with many types of controllers and event register. Demo.zip file is located in main folder of the program, to open it click from main menu: **File -> Import**.

REGISTRATION

To [register program](#), copy licence file "PRlicence.ini" into directory ..\Program Files\Roger\Access Control System 4.2. Company Roger Sp. J. provides licence file after receive filled order form licence - file "**Order.txt**", which is in the main directory of the program and on site www.roger.pl



Note:

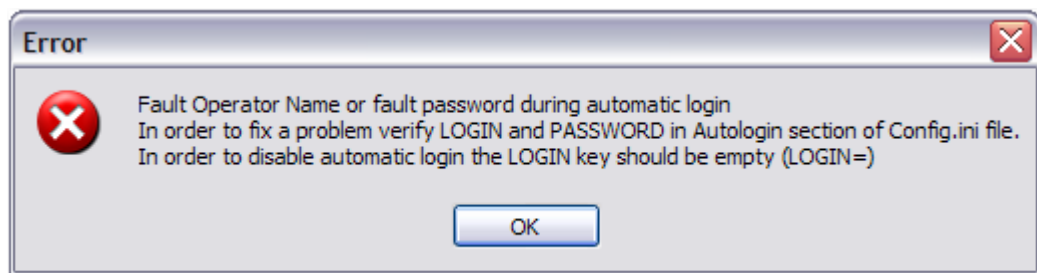
The software is fully functional even it is unregistered version, however program without licence file is restricted to eight controllers.

4.1 Autologin

Autologin function enables to log in to PR Master automatically. To utilize this feature you should make some changes in **Config.ini** file which is located in the main directory of the PR Master.

- open Config.ini file e.g. in Notepad
- find section:
[Autologin]
LOGIN=ADMIN
PASSWORD=
- enter your LOGIN and PASSWORD

During PR Master start, autologin section is verified. Next program trying to login with defined LOGIN and PASSWORD keys. If login procedure failed, the following communicate will appear:



You can return to default method of login procedure by remove of LOGIN and PASSWORD keys from Config.ini file.

Run MONITORING mode automatically

PR Master can be automatically started in Monitoring mode in case [Autologin] section is filled with LOGIN and PASSWORD. To enable this function follow these steps:

- create shortcut to PR Master application
- right-click on PR Master shortcut and select **Properties**
- click on **Shortcut** tab
- In **Target file** you should add after existing path: **[SPACE]: /AUTOLOGIN /MONITOR**
- click **Apply** and **OK**.

4.2 Installation on MS Windows Server 2003

When PR Master is installed on [MS Windows Server 2003](#) it's necessary to define PATH to RACS database.

To carry out this operation make the following steps:

- open **BDE Administrator** located in Control Panel
- click **Object** -> **New**,
- choose **STANDARD** in **Database Driver Name**,
- type name: **RACS_4_2_0** in case you have RACS4.2.X.X installed,
- enter **PATH** to RACS database (DATA catalog located in the main directory of the program)
- click on blue arrow from top panel to apply changes
- close BDE Administrator.

**Note:**

In special cases, modification of PATH is not possible. Access is blocked when RACS icon is highlighted on green. In this situation you should right-click on RACS icon and select **Close** from menu.

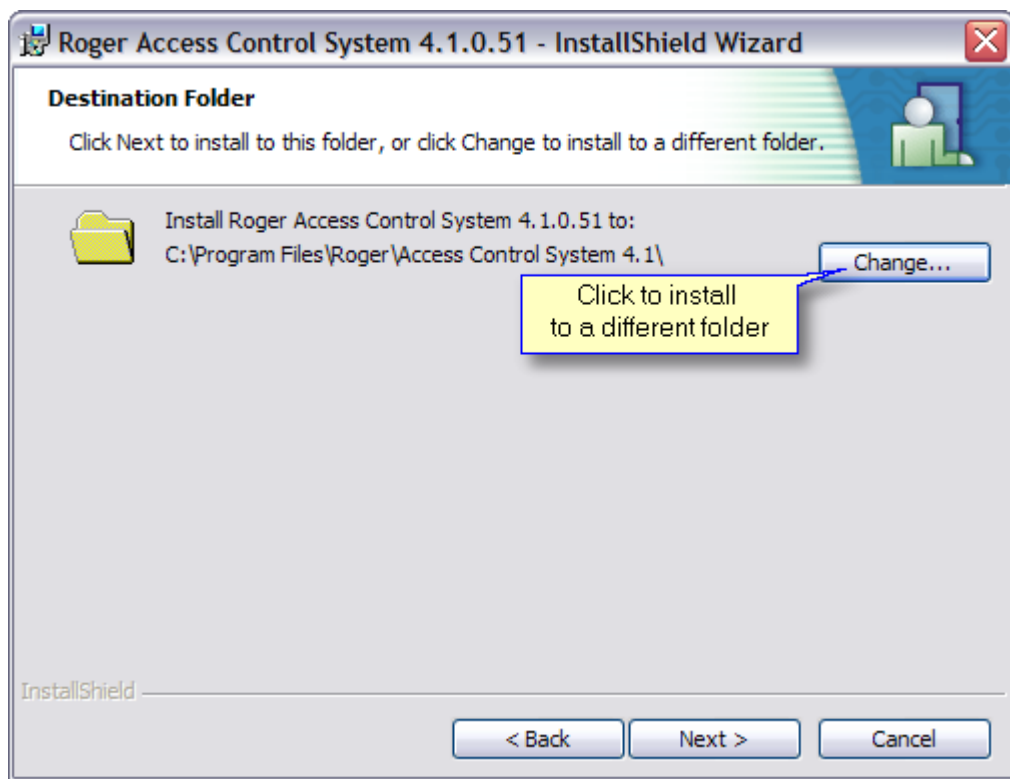
4.3 System requirements and installation tips

System requirements:

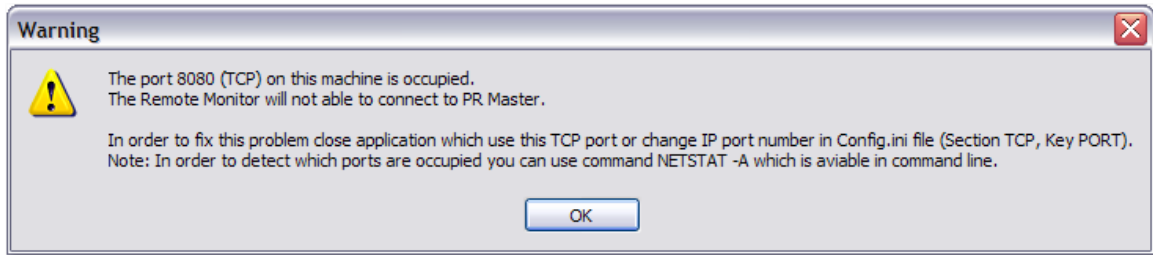
- Operating System: Windows XP, Windows® 2000 (recommended) or Windows NT, 98, 95
- processor: Pentium® II, 500 MHz or better
- 128 MB RAM (256 MB or more recommended)
- 100 MB of free disk space (250 MB or more required)

Installation tips

1. It's recommended to install PR Master using user account with administrator rights.
2. By default RACS software package is installed to **Program Files** directory, however you can choose another catalog. Click **Change** to install to different folder and **Next** to continue.



3. PR Master trying to open TCP ports for Remote Monitor applications during program starts. In case TCP port with default number: 64181 is occupied the Remote Monitor will not able to connect with PR Master. Following warning will appear:



To solve this problem open **Config.ini** which is located in the main directory of PR Master and change PORT=64181 to different PORT. You can easily check which of the ports are already occupied in your system using **netstat -a** command in CMD line.

4. If value of DPI resolution in your operating system exceeds 96, some problems with displaying windows may occur. Recommended resolution is **Normal size (96 dpi)**.

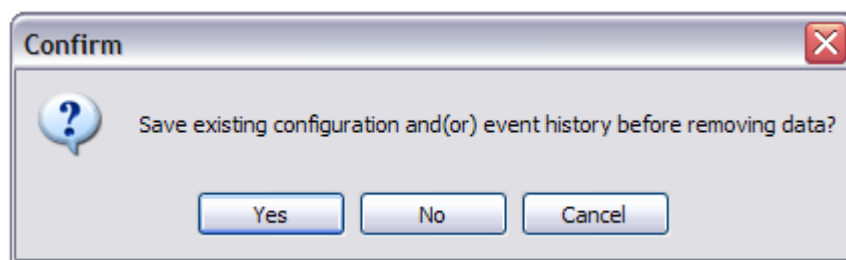
5 System database of RACS

All PR access system settings and events saved during ON-LINE operations PR Master retain in [system database](#). The events are appended to system database every time the **Read events buffer(s)** or **Monitoring** function is invoked. It's available to export and import system configuration, events or both to disk file with (*.xml) or (*.zip) extension. PR Master allows user to automatically backup ([backup configuration](#)) selected data (events, configuration) which can be used in case the database is crashed.

PR Master external files:

- **Config** file with extension *.xml
- **Events** file with extension *.xml
- **Backup** file with extension *.zip (configuration + events)

To create new system configuration file, choose **File -> New**, from main menu.



PR Master application enables user to work with:

- [Local system database](#) - locally on PC computer
- [Network system database](#) - shared in local network,

Local system database is located in the main directory of PR Master. Network system database is shared by computers connected to local network.

5.1 Local system database

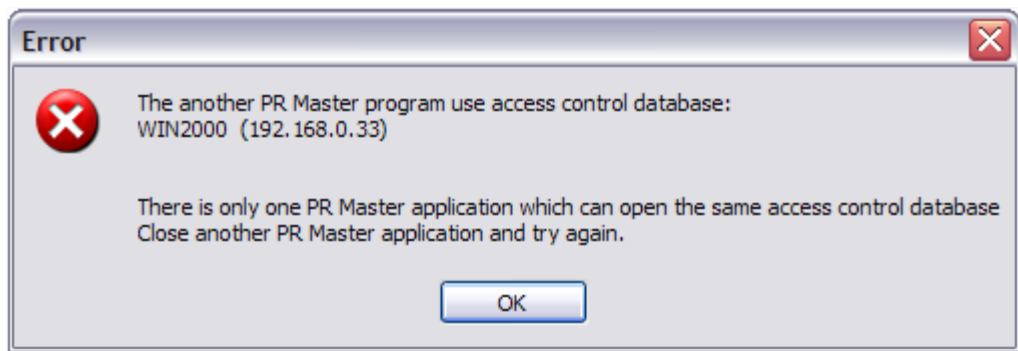
Local system database is used in simple installations on the one PC. It's the best solution, when you don't have to control and configure system from many computers.

5.2 Network system database

Networked database can be used only in case Access Control System is connected through UT-4 communication interface. Thanks to networked database it's available to configure and control system from many PC's with PR Master installed.

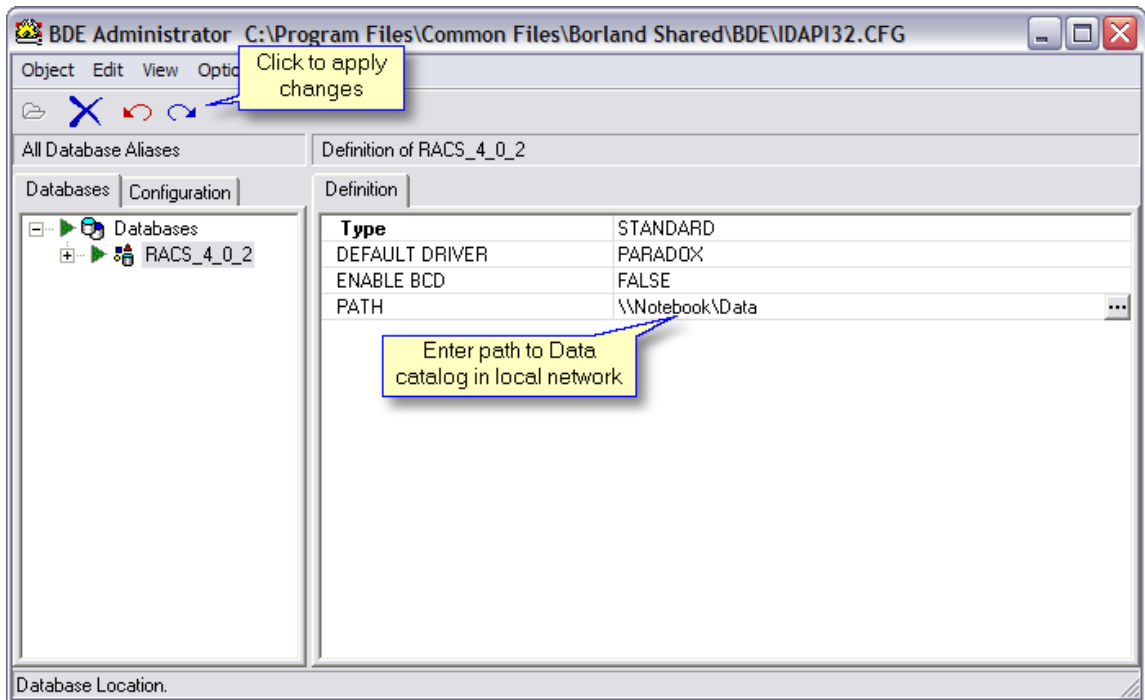
Feature is very useful, especially when many users on different PC's want to use RACS.

Remember that PR Master is not typical network application. Only one PR Master application can use database resources in the same time, therefore trying to run program on other PC will generate following communicate and close.



To configure RACS system to work with networked system database you should carry out the following steps:

- Copy **Data** catalog which is in *x:\Program Files\Roger\Access Control System 4.2*, where *x* is your system disc,
- Paste the catalog to a place in local network where it will be shared for other computers
- Share **Data** catalog in local network (Sharing and security)
- Set permissions to **change** and **read** for all or selected network users
- Open **Data/NET** catalog and delete files: **PDOXUSRS.NET**, **PARADOX.LCK**, **PDOXUSRS.LCK**
- Run **BDE Administrator** from Control Panel, following window will appear:



- Select **RACS_4_x_x** (depending on your RACS version) from list on left. Enter path to **Data** catalog in **PATH** field, and next apply changes by click on blue arrow in widow top menu
- Close BDE Administrator.

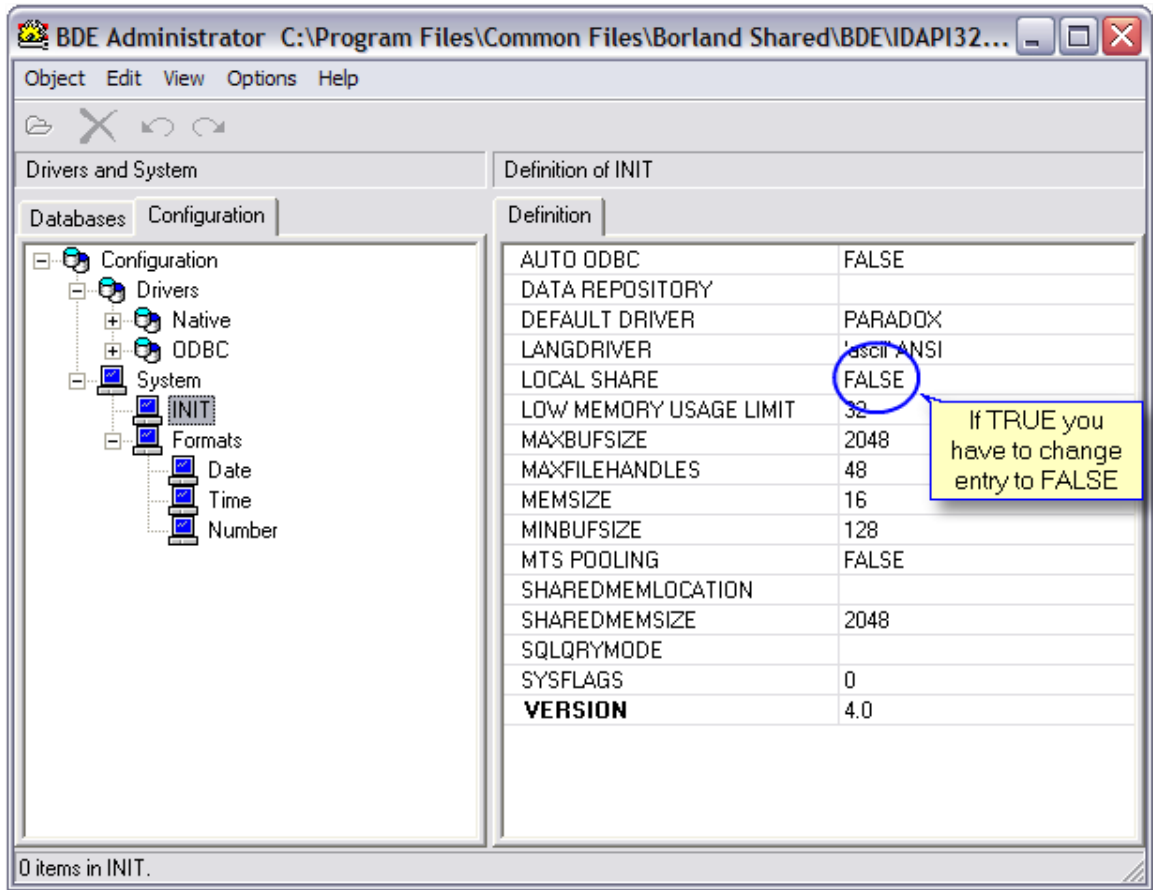


Note:

This configuration should be carried out on each computer with PR Master.

If problem with BDE Administrator will occur follow this steps:

- Run **BDE Administrator** from Control Panel
- Select **INIT** icon
- check if **LOCAL SHARE** entry is FALSE, if TRUE than change it to FALSE



6 Using program

6.1 Main window

Main window of the PR Master 4.2 consist of: [main menu](#), operator toolbar (on left side), list of access points, licence and operator information. Operator toolbar gives you the best way to access main system functions.



Note:

Usually a "hint" is displayed when you move the cursor close icon, field or button.

Access points

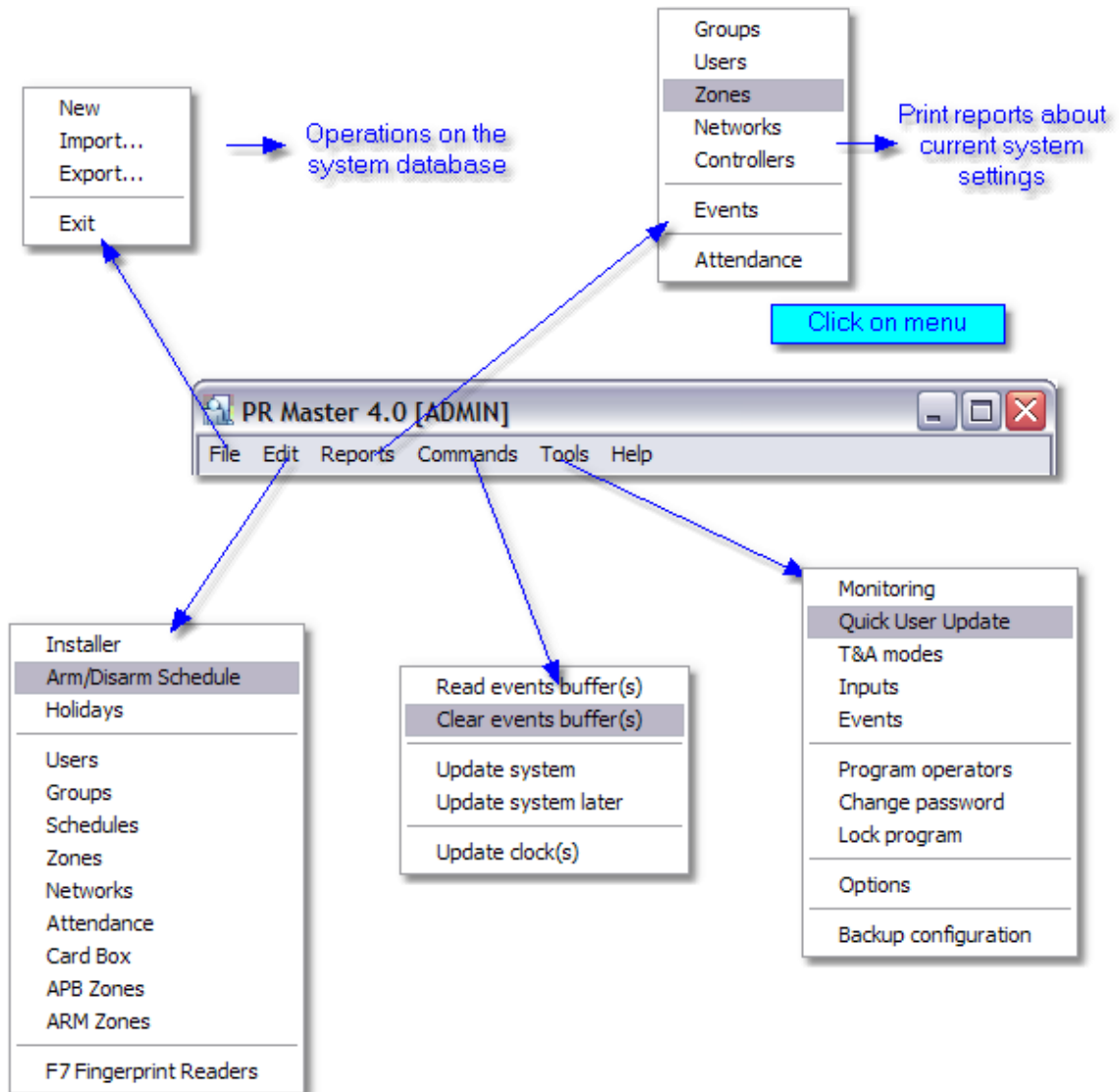
Access points	Zone
Demo PR301	New zone (4)
Demo PR402 - terminal 1	New zone (1)
Demo PR302	New zone (2)
Demo PR302LCD	New zone (1)
Demo PR402 - terminal 1	New zone (4)
Demo PR301 - terminal 0	New zone (4)
Demo PR402 - terminal 0	New zone (1)
Demo PR302LCD - terminal 0	New zone (4)
Demo PR402 - terminal 0	New zone (3)

Licence for: Roger Spółka Jawna
Gościszewo 59; roger@roger.pl
Maximum number of controllers: 32

Roger sp. j.
82-416 Gościszewo 59
tel: 055 272 0132
fax: 055 272 0133

6.2 Main menu

Main menu contain tools and options of the program.



6.2.1 Edit

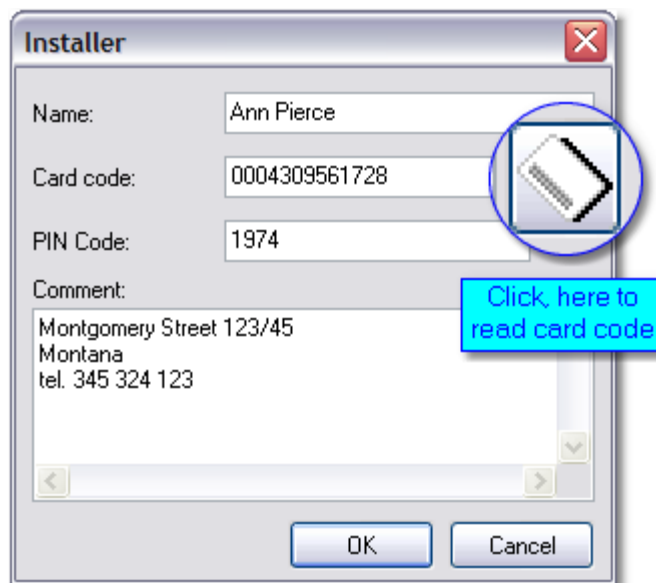
6.2.1.1 Installer

There is one user in PR system, who doesn't have ID number and is not authorised for door opening and other system features. He is called **INSTALLER**. Installer is only able to enter manually installer programming mode of the controller.

Programming **INSTALLER** user in PR system is not obligatory.

**Note:**

It is recommended to program RACS controllers from PR Master only. Making any changes in contents of controller memory in installer or user programming mode causes incompatibility with system database.



6.2.1.2 Arm/Disarm schedule

Access Controller has two working operating modes: Armed and Disarmed mode. The actual controller's operating mode is indicated on the dual color LED STATUS, which lights in red for Armed or green for Disarmed. Generally the Armed and Disarmed modes are dedicated for integration of the controller with the alarm system which protects the same room or area which is supervised by the access controller, nevertheless they can be used for any other control purpose which requires an On/Off control method. The integration with the alarm system (or another device or system) requires one output line to be configured to function no. 0 (Disarmed Mode) and one input line configured to input no. 13 function (Ready Status). The controller output line (function no. 0) indicates current operating mode of the controller, whereas the input line (function no. 13) verifies if the controlled system (or device) is ready to be armed (or set ON).

Note: When the installer doesn't define any controller's input to the function no. 13, the controller assumes that the alarm system is always ready for arming and switches to armed mode unconditionally.

Note: Upon powering on, the reader automatically returns to the Armed/Disarmed state it was in before powered off. Also, the reader returns to its original Armed/Disarmed state after exiting the programming mode. After Memory Reset the reader always enters the Armed mode.

Switching ARM/DISARM mode can be realised on the following methods:

- automatically, according to defined Arm/Disarm schedule
- locally with MASTER, SWITCHER or SWITCHER Limited identifiers
- locally with input line or [**F1 - F2**] key which is configured to one of following function:
 1. [**No.3: Arm/Disarm Steady Switch**]
 2. [**No.61: Arm/Disarm Momentary Switch**]
 3. [**No.78: Set Disarmed Mode**]
 4. [**No.79: Set Armed Mode**]

- locally trough the keypad command:
 1. [**No.11: Set Disarmed Mode**]
 2. [**No.12: Set Armed Mode**]
 3. [**No.13: Toggle Armed/Disarmed Mode**]

- remotely with interactive command from PC ([Commands to controller](#))

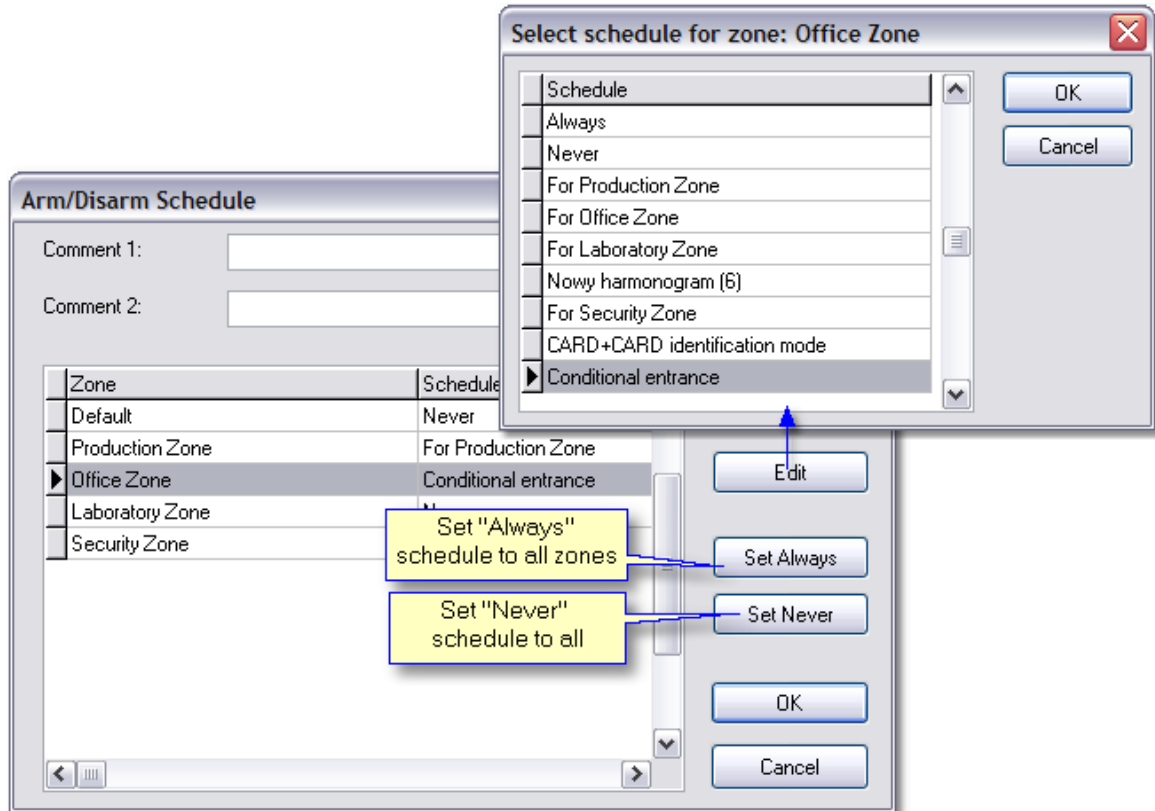
**Note:**

In case when Arm/Disarm mode control is realised trough: input line which is configured to function [**No 3, 78, 79**] or keypad command, then all other methods are automatically disabled

Controller Arm/Disarm modes can be switched automatically by defined time schedule. To enable it check [**Enable Arm/Disarm Schedule**] in **Options** tab in **Controller properties**. Auto-arming can be delayed trough the **Default Auto-arming Delay when alarm system not ready** option and additionally using manual triggering - Postponed Auto-arming Delay.

See also:

[Controller properties - options](#)



6.2.1.3 Holidays

Holidays - special days which are defined in one year period. This feature enables to assign time schedule from:

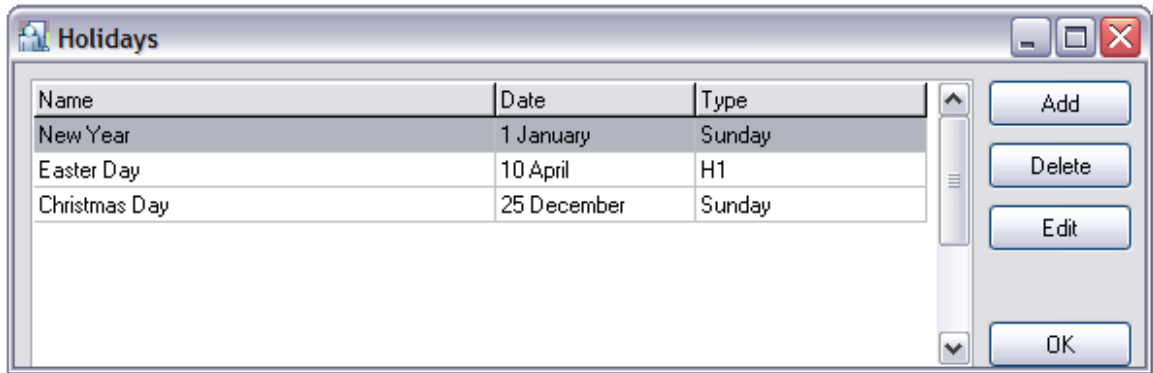
- selected day of week (Monday...Sunday)
- or defined H1 to H4 time schedule

to specified day in year.

To set up time period for H1 - H4:

- open **Schedules** -> **General purpose schedules**
- click on selected **H** tab
- click on **Add** to enter new time period

example: define "Easter" holiday that will be on 12 of April and system will use H1 time schedule settings in this day.



To define holidays:

- click **Add** button, following window will appear:

- type **Name** of holiday
- select **Day** and **Month** from menu
- select **Type** - time schedule (day of week or H1-H4)

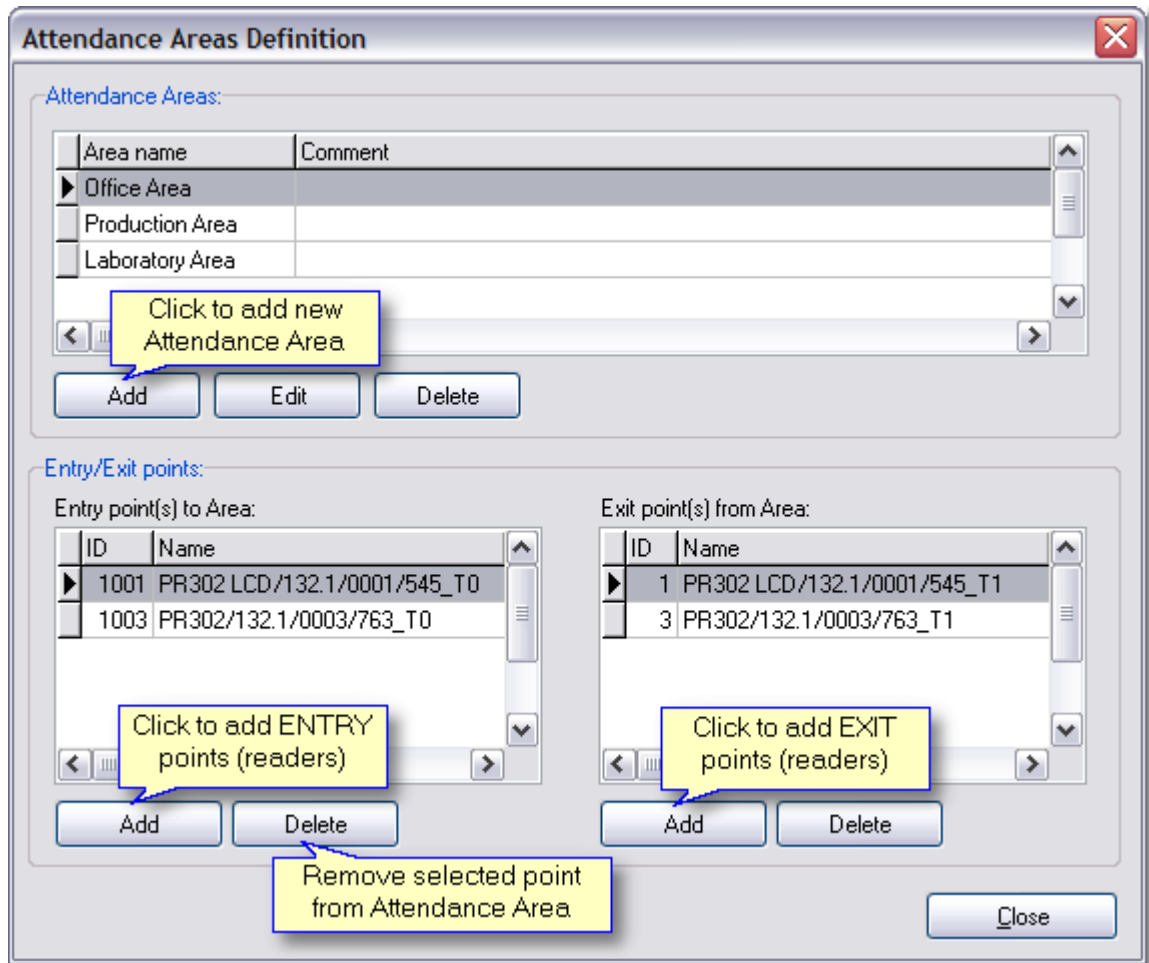


Note:

Older types of controllers (PRxx1) don't operate holidays.

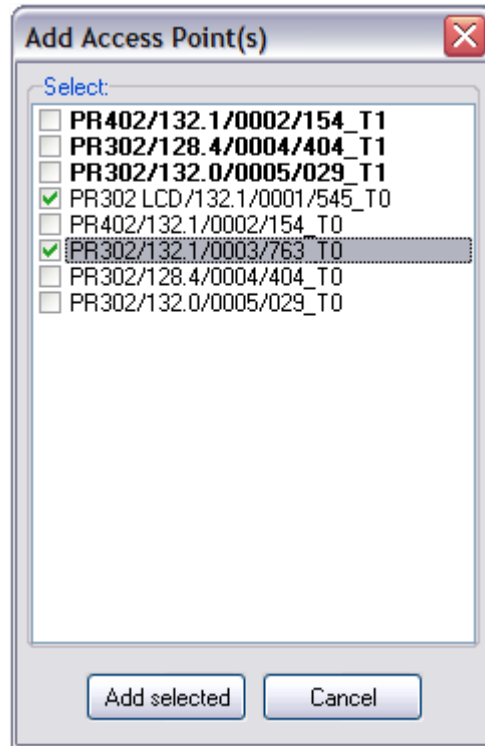
6.2.1.4 Attendance

Attendance areas are defined to generate T&A reports. Time marks of user ENTRY and EXIT included in T&A report are essential elements on which Total Time is counted. In special cases User Attendance report can be used to calculate effective user (employee) time attendance, e.g: in Production Area or Office Area. In difference of T&A reports, User Attendance reports do not include T&A modes.



To add new Attendance Area:

- Click on **Add** and type name of area
- click **OK** to confirm
- Click **Add** to define Entry point(s), where ENTRY events will be registered:



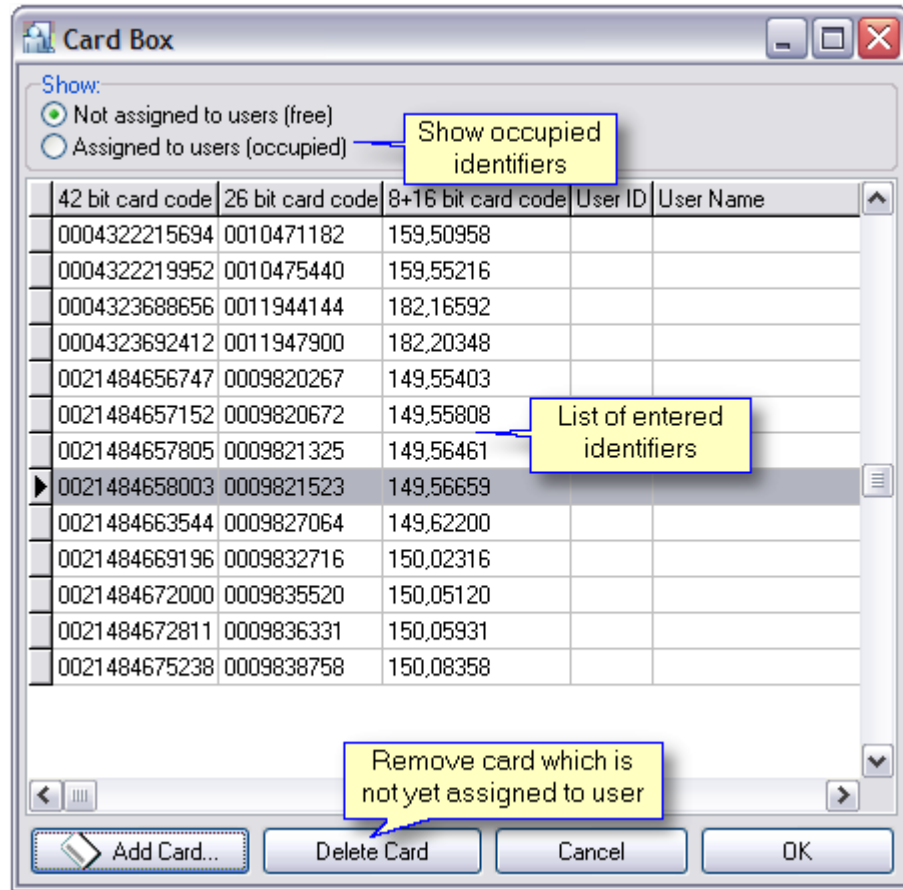
- select Entry points from the list and click **Add selected**
- Click **Add** to define Exit point(s), where EXIT events will be registered
- select Exit points from the list and click **Add selected**
- Click **Close**

6.2.1.5 Card Box

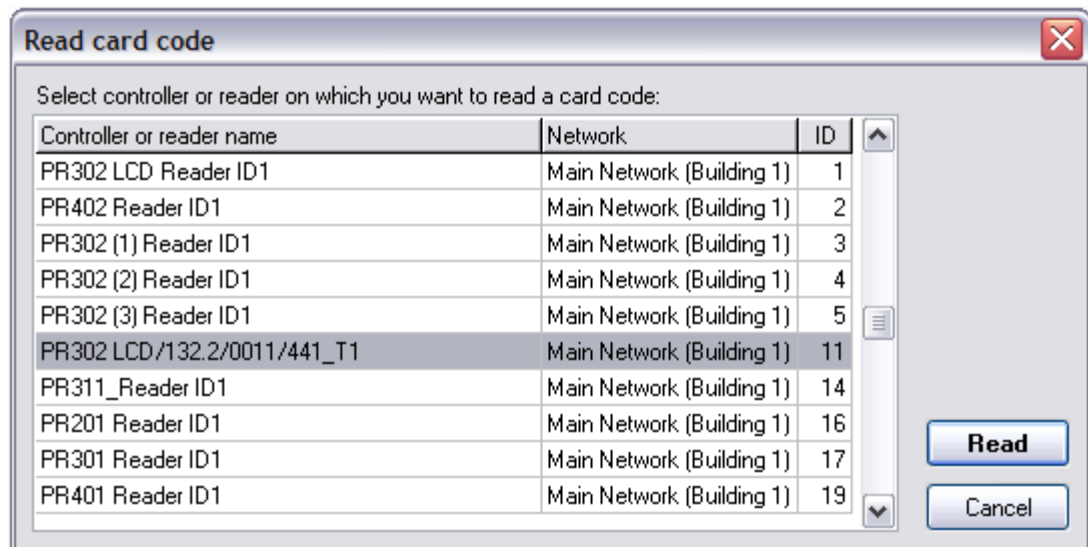
Card Box is a tool which enables to manage RACS identifiers. The main advantage of this feature is that identifiers are registered in system using method "one by one". It's the best solution when lot of new identification cards have to be registered.

To add new identifiers to the Card Box:

- click **Edit** -> **Card Box** from the main menu

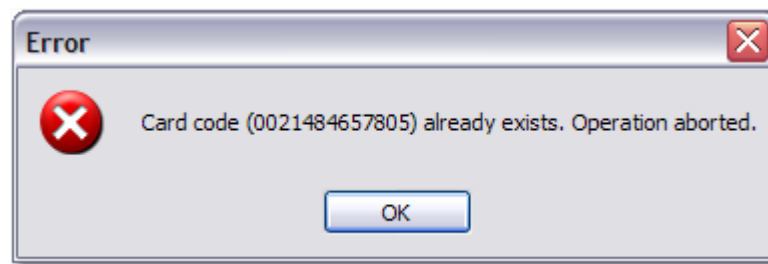


- click **Add Card** button, the following window will appear:



- select controller/reader on which you want to read card code
- click **Read**
- approach identifiers successively "one by one" making short breaks
- once entering identifiers is finished click **Cancel**.

In situation when identifier is already added to Card Box, the following error will occur:



After the registration of new identifiers is finished, user obtains list of free identifiers.

PR Master enables to display:

- Free identifiers - not assigned to users
- Occupied identifiers - already assigned to users, additionally show Name and i ID of user

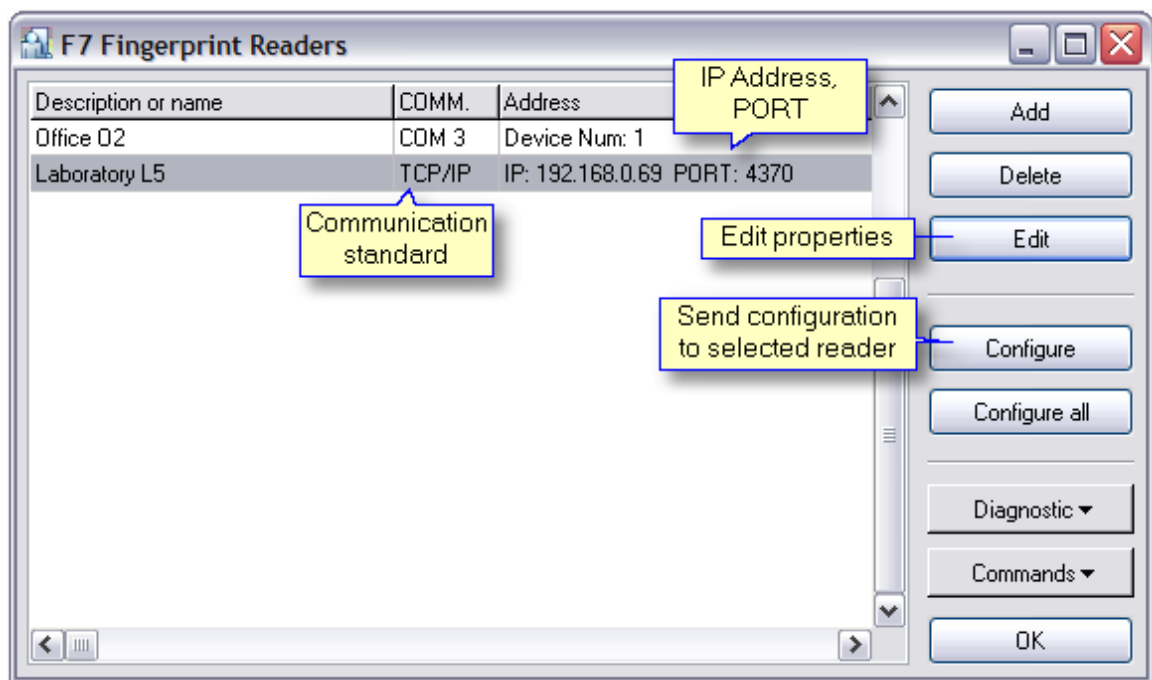


Note:

Registered card can't be removed in case it's assigned to a system user.

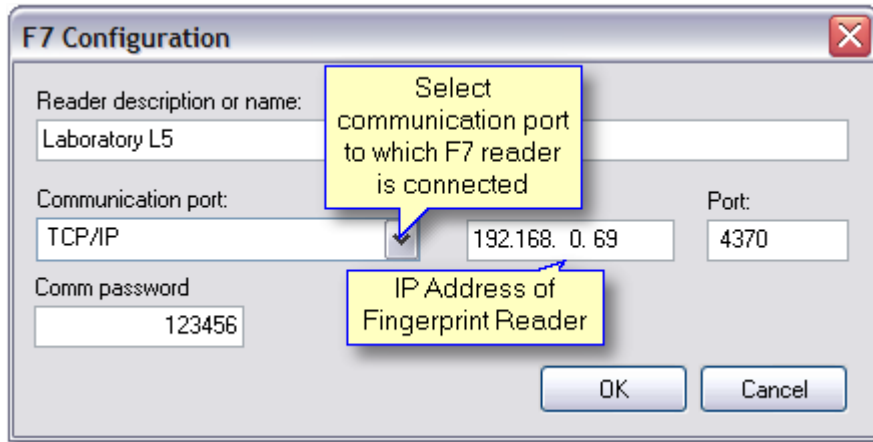
6.2.1.6 F7 Fingerprint Readers

This option allows to manage and configure Fingerprint Readers which are connected to Access Control System. F7 reader can be connected to UT-2 communication interface or directly to LAN network. If Fingerprint Reader is connected to the local network you have to enter F7's IP address.



To add new F7 Fingerprint Reader:

- choose **Edit** -> **F7 Fingerprint Readers** from the main menu
- click **Add** button, the following window will appear:



- type **Name** of reader
- select **Communication port** (COM or TCP/IP)
- if **TCP/IP** is selected you have to enter reader's **IP Address** and **Port** (default port: 4370, in most cases you don't have to change it)
- if **COM** port is selected you have to enter reader's ID address
- enter **Comm password** (by default 123456)
- click **OK**

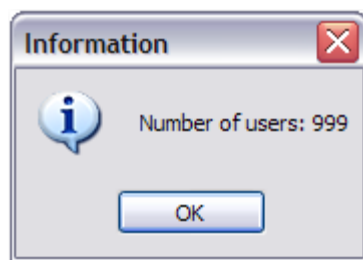


Note:

Comm password secures access to F7 reader's settings. If you change reader's default password you have to enter it in F7 configuration window.

Description of **Diagnostic** options:

- Firmware version - display version of reader's firmware
- Device MAC - display physical address of device
- Number of users in a reader

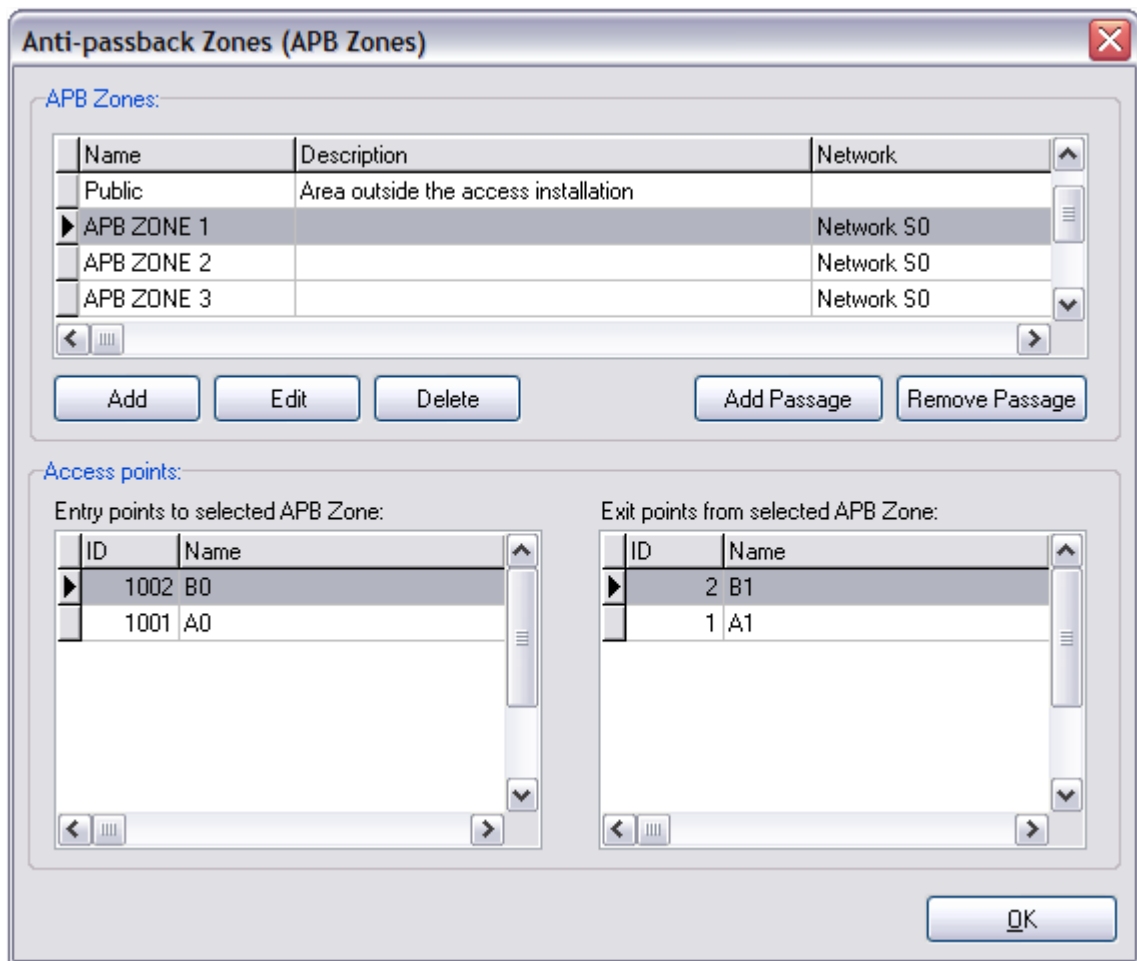


- Number of fingerprint templates in a reader
- Read date and time

Description of **Commands**:

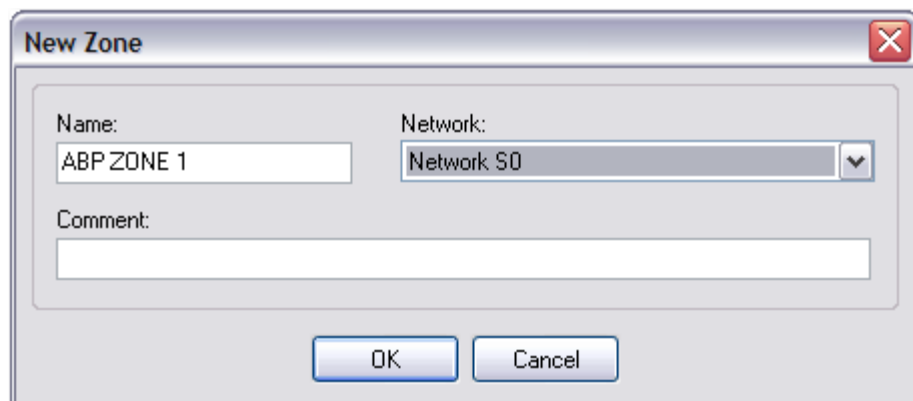
- Set date and time - set current date and time, synchronization with PC clock
- Restart - restart selected reader
- Delete all users - removes users from memory
- Update firmware - firmware upgrade

6.2.1.7 APB Zones



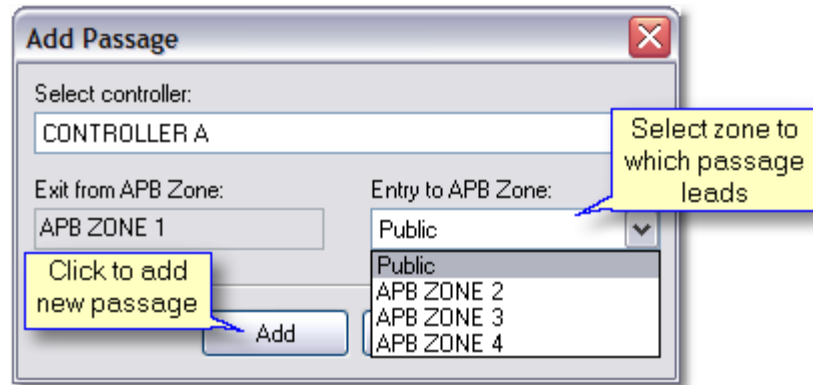
To define APB Zones:

- click **Add** button to define new APB zone, the following window will appear:



- type **Name** of APB zone
- select **Network**
- click **OK** to confirm
- once all zones are defined, you have to add Passage. Click **Add Passage**, the following

window will appear:



- select available controller from list
- select **Entry to APB zone** (zone to which passage leads)
- click **Add**



Note:

To operate APB zones CPR control panel is required.

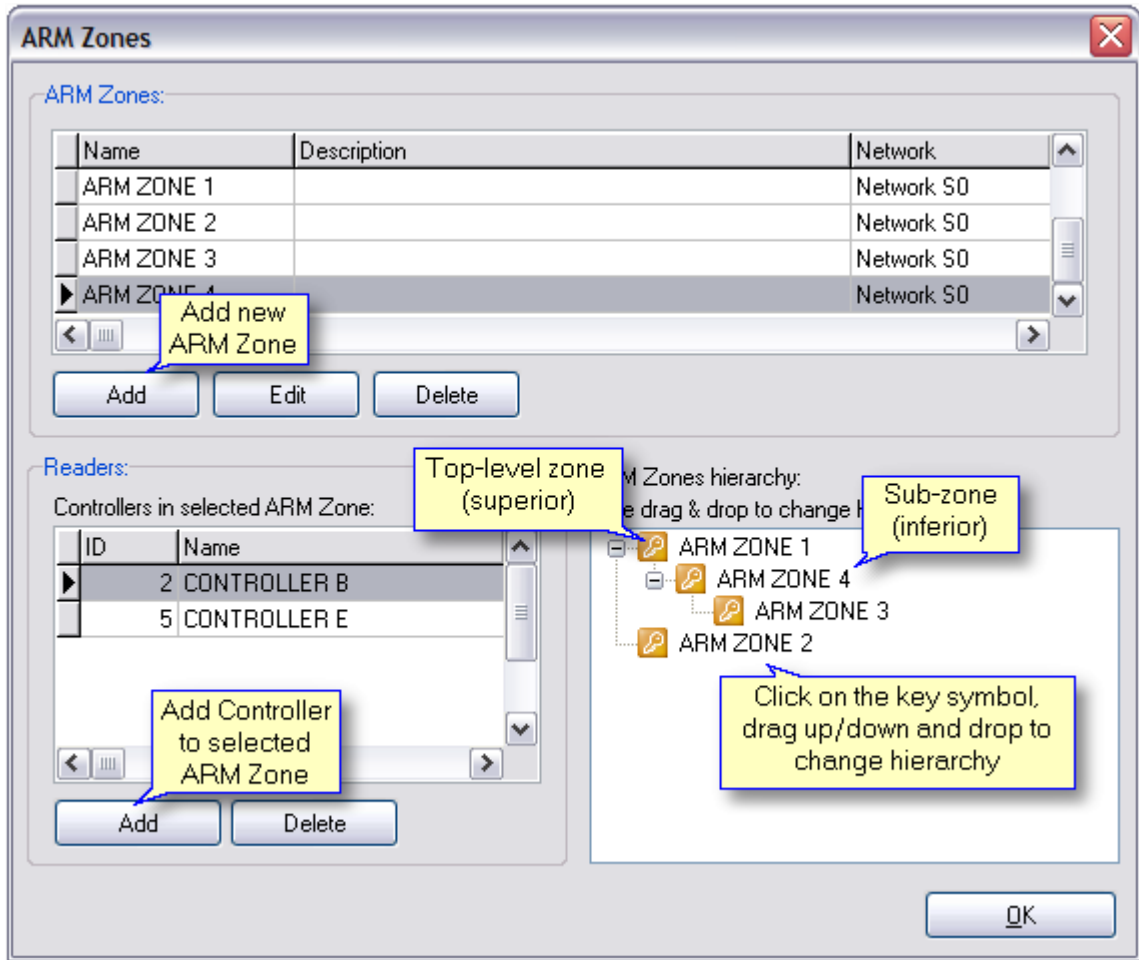
6.2.1.8 ARM Zones

ARM Zone is a defined group of controllers in which all devices can be simultaneously turned to ARMED or DISARMED mode. It means that switching controller to ARMED mode causes arming of all controllers which belong to the same ARM zone and similarly switching controller to DISARMED mode causes disarming of rest of controllers assigned to the ARM zone. **ARM Zones hierarchy** enables to arrange zones in appropriate order. For example some of the ARM Zones may be positioned lower, in this case they are armed simultaneously to superior zone. Turning to ARMED mode of higher positioned ARM Zone causes arming of all ARM sub-zones with lower level. Disarming of ARM Zone must be carried out individually for each zone.



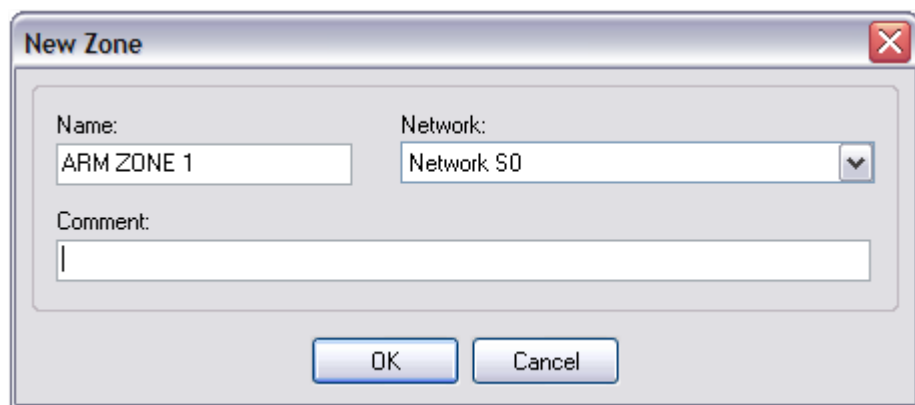
Note:

This feature requires CPR host controller.



To define ARM Zones:

- select **Edit** -> **ARM Zones** from the main menu
- click **Add** button to define new ARM Zone



- type **Name** of ARM Zone
- select **Network** from menu
- click **OK** to confirm
- next click **Add** to assign Controllers to selected ARM Zone

After the all required ARM Zones are defined, you can proceed to change zones hierarchy. Each of

new added ARM Zones is represented as yellow icon with key (watch the screenshot). Zones are arranged in one line which means that they are equal.
If you want to change hierarchy, e.g. one of ARM Zone have to be defined as a sub-zone relatively to another, you have to click on the key-icon and use drag & drop method.

6.2.2 Commands

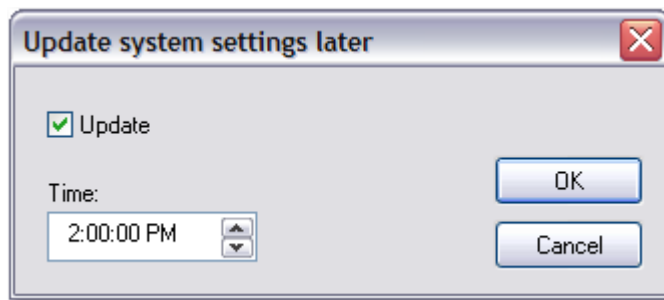
Commands from this menu concern entire RACS system (all networks).

- **Read event buffer(s)** - read events from all networks
- **Clear event buffer(s)** - clear events in all networks
- **Update system** - send configuration settings to all devices in system
- **Update system later** - send configuration settings to all devices in system at defined time
- **Update clock(s)** - set clocks in system according to PC system clock.



Note:

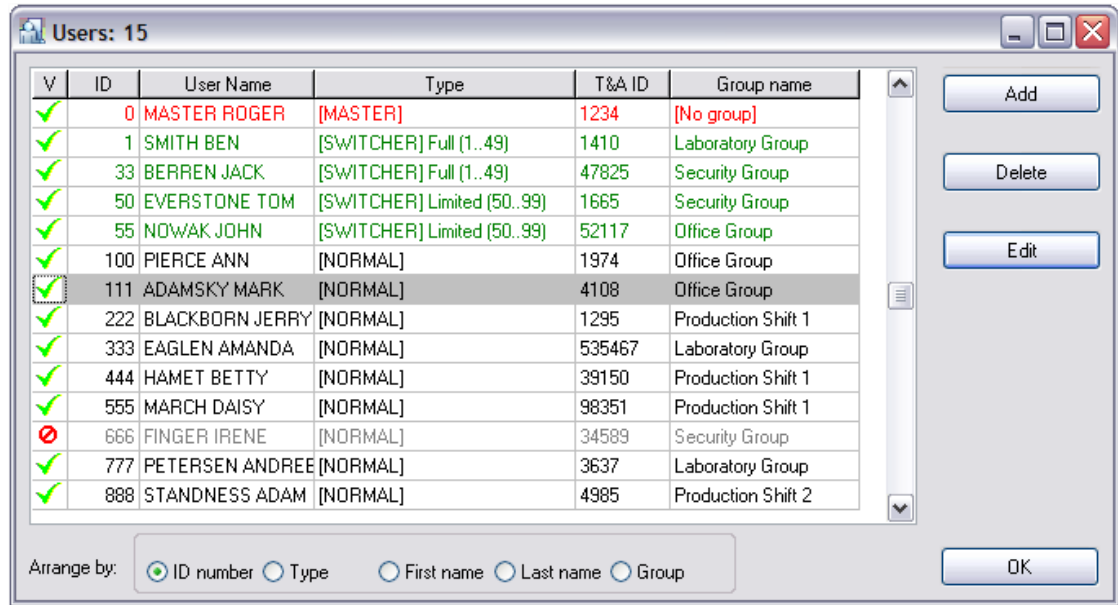
Option **Update system later** is useful especially in large systems, where sending configuration during users movement might cause problems, and difficulties in activity of object.



6.2.3 Tools

6.2.3.1 Quick user update

Quick user update feature enables to edit user settings and send changes to all system immediately. In difference of standard configuration sending the option sends settings of only one user, therefore data transfer is much faster.



6.2.3.2 T&A modes

Time & Attendance mode is an element which attach T&A mark (Entrance, Exit, On-duty exit) to the "Access granted" event. Each Access granted event which occur on controller has assigned a T&A Mark (T&A status) which specifies what kind of entry/exit has been registered. The actual type of registration for T&A purposes is determined by controller's T&A Mode. Each T&A Mode has its individual ID number from 0 to 255, numbers between 0 and 50 are reserved for predefined T&A Modes which can not be modified or changed.

Predefined T&A modes:

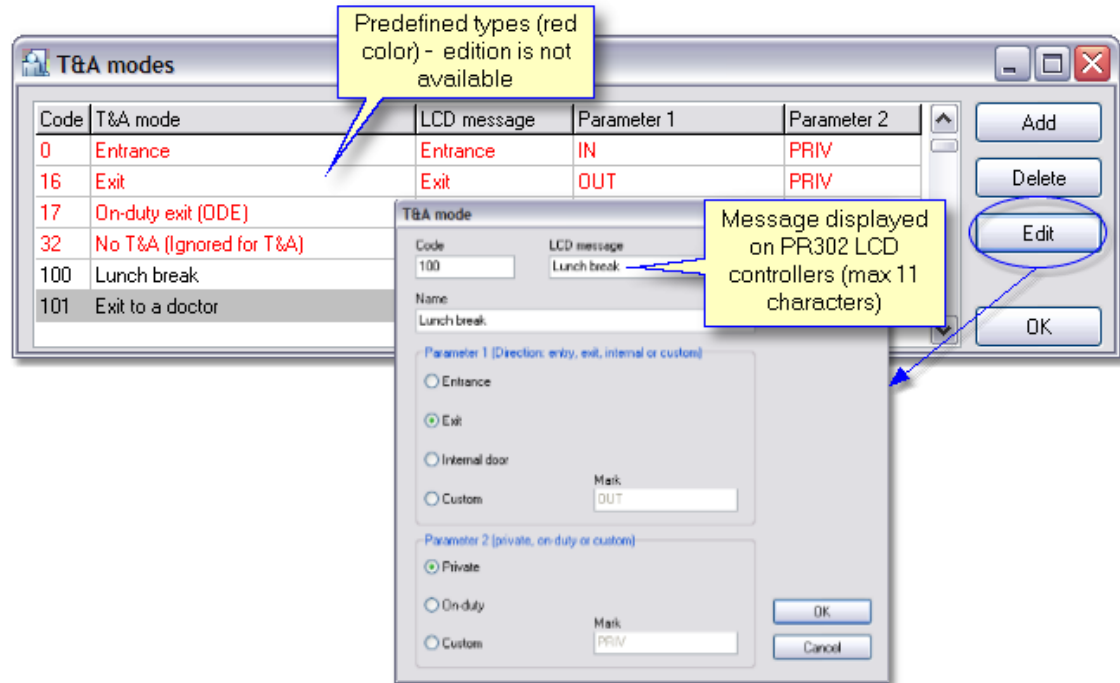
- Entry
- Exit
- On-duty exit (ODE)
- No T&A (Ignored for T&A)

When controller stay in **No T&A (Ignored for T&A)** mode it means that events which will occur during this mode will not play any rule in T&A reports or calculations.

The customer defined modes can be useful when new types of entry/exit are requested for detailed statistics of users attendance. It's available to define 204 T&A modes (codes from 50 - 254). In RACS system each access point (controller/terminal) may have its own Default T&A Mode. You can apply created T&A mode to Default T&A Mode option in Controller properties (**Controllers** -> **Properties** -> [Terminal ID0, ID1](#)). The T&A Mode of access terminal can not be dynamically changed during system activity except situation when option Terminals ID=0 and ID=1 have the same T&A Mode is set.

To add new T&A mode:

- click **Add** (and set all parameters)
- enter **Code** and **Name**
- type **LCD message** (controllers with LCD only)
- set **Direction** (select **Custom** to place your own Mark)
- set **P/D**

See also:[T&A Report](#)[Switching T&A mode](#)

6.2.3.2.1 Switching T&A Mode

The T&A Mode of controller can be dynamically changed in following methods:

- set T&A Mode from keypad
- set T&A Mode using **[F1 - F4]** Key
- set T&A Mode from input
- set T&A Mode automatically according to T&A Mode schedule
- set T&A Mode using **[*][#]** command on controller's keypad (PR302LCD)

Setting T&A Mode from keypad

Installer may enable/disable dynamic setting of T&A Mode from controller's keypad. The manual change of T&A Mode can be set for a limited period (momentary change) or for unlimited time (stable change). When using "momentary change" method the newly selected T&A Mode will be valid for nearest Access granted event only, when "stable method" is used all Access granted events which will occur during selected T&A Mode will have the same (new) T&A mark.

INPUTS:

Setting T&A Mode from input

Installer may define one or more input line to be used for setting required T&A Mode of controller. The input line can be used to set specified T&A Mode or to switch controller between different T&A modes. The input line which dynamically change T&A Mode is very useful especially when an external button(s) is required to select specified T&A Mode.

Stable T&A Mode setting input

When this type of input line is triggered controller move to next predefined T&A Mode and remain in this mode until next command comes and change it again.

Momentary T&A Mode setting input

When this type of input line is triggered controller move to next predefined T&A Mode and remain in this mode until next Card/PIN is entered, after this controller returns to previous T&A Mode. When no Car/PIN is entered during 8 seconds period controller will restore previous T&A Mode automatically.

Predefined T&A Mode setting input

When this type of input line is triggered controller move to dedicated T&A Mode and remain in that mode until next command comes and change it again. Each input line can be used for setting individual T&A Mode. For example IN1 can be used to set "Exit", IN2 can be used to set "Entry" and IN3 to set "On Duty Exit".

T&A Mode controlled by schedule

The T&A Mode Schedule enables automatic change of controller T&A Mode according to defined time schedule details. The T&A Mode Schedule specifies what T&A Mode will be set on controller in particular moments of day, week or holydays.

6.2.3.3 Types of Inputs

This feature allows user to add specific [types of Inputs](#) to the list. Predefined types of inputs (red font) are not editable. User may define new Input type to receive information about status of the other device equipment which is connected to controller (for example smoke detector)

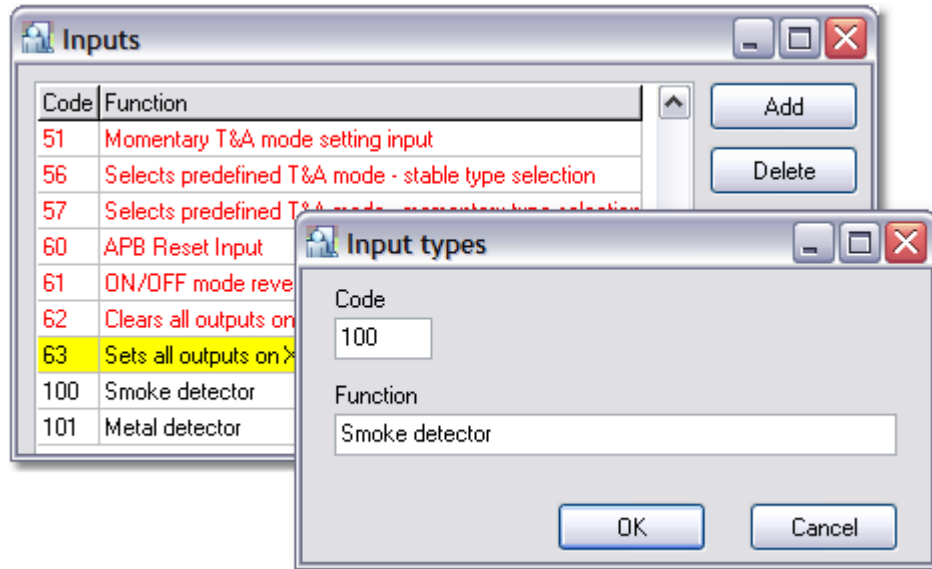


Note:

New defined type of input has default settings:

- activated - ALARM event
- return - NORMAL event

New input function can be assigned to one of four Input lines of controller (Inputs). Activity of all input lines can be controlled in order to defined General purpose schedule.



See also:

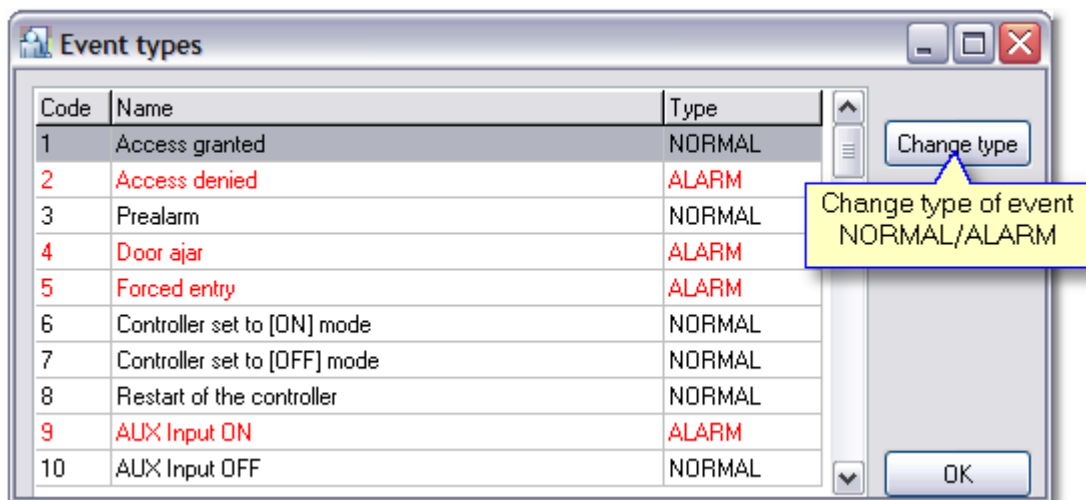
[Inputs](#)

[Outputs](#)

[General purpose schedules](#)

6.2.3.4 Types of events

This window contains list of all [events](#) which are registered by the system. Option enables user to specify NORMAL/ALARM events. To change type of event from NORMAL to ALARM or inversely click on **Change type** button.



Alarm states of controller:

- **Prealarm** - occur after three consecutive attempts of entering an unknown identifier repeated in a period shorter than 1 minute.
- **Door ajar** - occur after door remains opened longer than period of time defined by "Time for door closing"
[Controller properties - Access.](#)
- **Forced entry** - the state occur in consequence of forced opening door

Every alarm signalisation on access controller automatically disappears after 3 minutes. Alarm can be cleared earlier (before 3 minutes) by a valid identifier or interactive command.

System alarm can be cleared from PR Master in following ways:

- **Networks** -> **Commands** -> **Clear all alarms in network**
- **Networks** -> **Controllers** -> **Commands** -> **Clear alarm on controller** (selected controller only)
- **Monitoring** -> [Commands](#) (available: *clear all* or *selected alarm*)



Note:

1. Alarm event in monitoring mode is indicated additionally in "Alarm" window ("Alarm" belt blinks).
2. When two or more alarms occur on controller in the same time, alarm with the highest priority will be signalised only. However, every alarm is registered and indicated in monitoring window.

6.2.3.5 Program operators

This feature allows ADMIN operator to define new [program operators](#) and also enable or disable access to menu items of PR Master. It ensures that all actions performed on the PC can be attributed to a particular operator. Every account can be secured by password (max. 16 characters) which will be required when operator log in or application is locked. It's possible to change password in **Tools** -> [Change password](#).

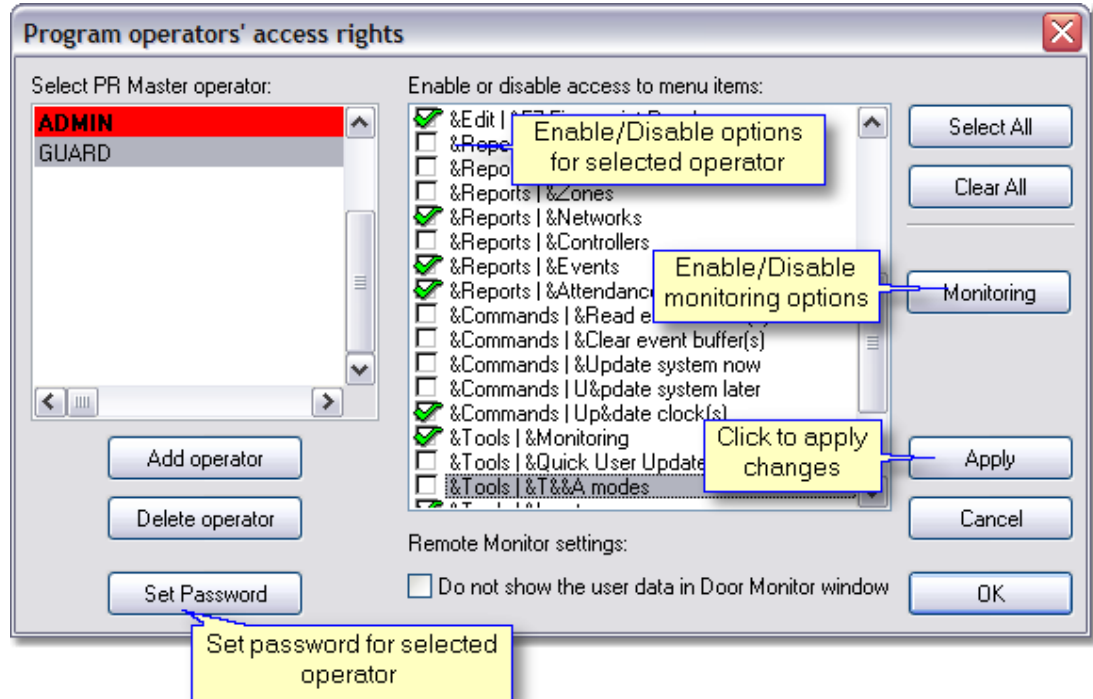
To define new program operator:

- Select from main menu: **Tools** -> **Program operators**
- Click on **Add**
- Enable/disable access to menu items by checking boxes
- Click on **Monitoring**
- Enable/disable access to Monitoring menu items by checking boxes
- Click **OK**
- Click on **Apply** to save changes



Note:

1. Password is case sensitive, watch on Caps Lock button
2. Password is not displayed nor printed, the system displays the password as asterisks.

**Note:**

By default ADMIN operator has no password.

See also:

[Access rights to monitoring window](#)

[Lock program](#)

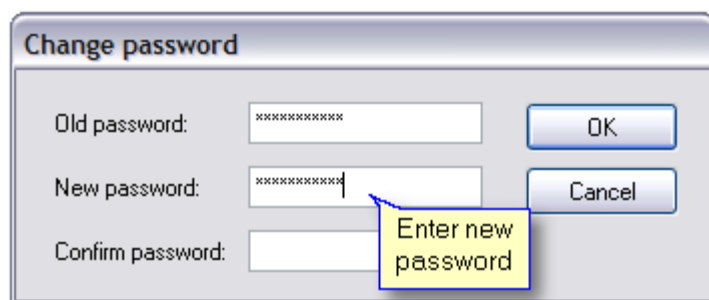
[Change password](#)

6.2.3.6 Change password

[Change password](#) of current operator. You should first enter **Old password**, next type **New password** and Confirm.

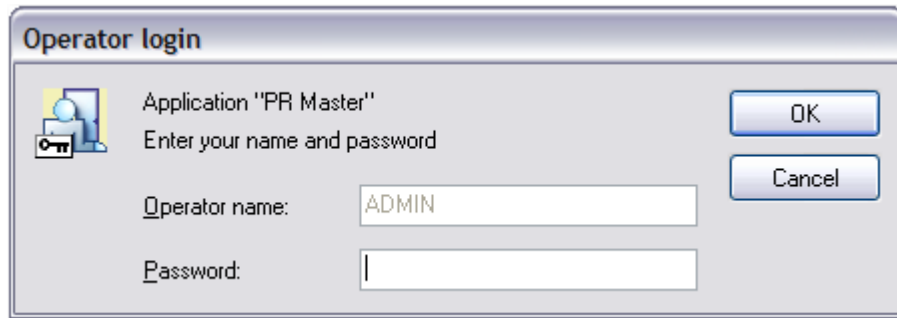
**Note:**

Watch on state of Caps Lock button, having Caps Lock on may cause you to enter your password incorrectly.



6.2.3.7 Lock program

Option allows to [Lock program](#) until password of current logged operator is entered. This protect from undesirable actions of others operators. When program is locked, the following window appears.



The image shows a dialog box titled "Operator login". It contains a small icon of a person at a computer on the left. The text inside the dialog box reads: "Application 'PR Master'", "Enter your name and password", "Operator name: ADMIN", and "Password:". There are two buttons on the right: "OK" and "Cancel".

To unlock program user must enter password of currently logged operator.

See also:

[Change password](#)

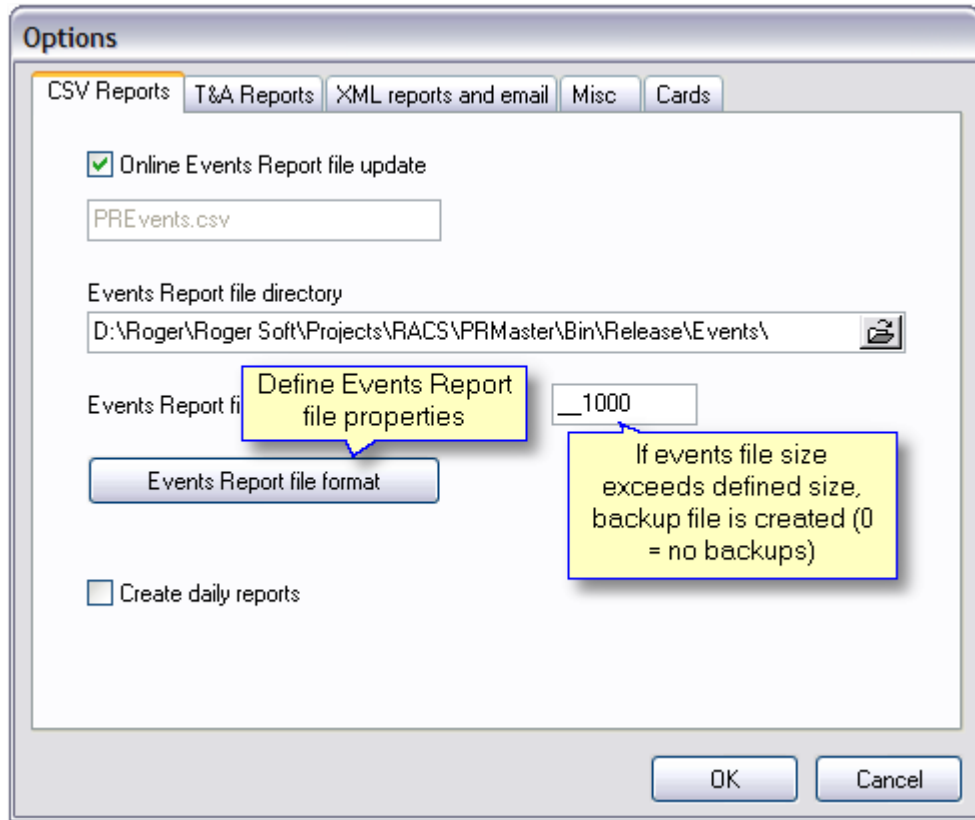
6.2.3.8 Options

6.2.3.8.1 Reports CSV

In case **Online Events Report file update** option is enabled events are continuously appended to CSV file in Monitoring mode. Every events buffer(s) read procedure causes actualisation of this file. User can select report contents in **Events Report filr format** and specify maximal size of CSV file. Create daily reports option enables to generate files with one-day events.

See also:

[CSV Reports](#)

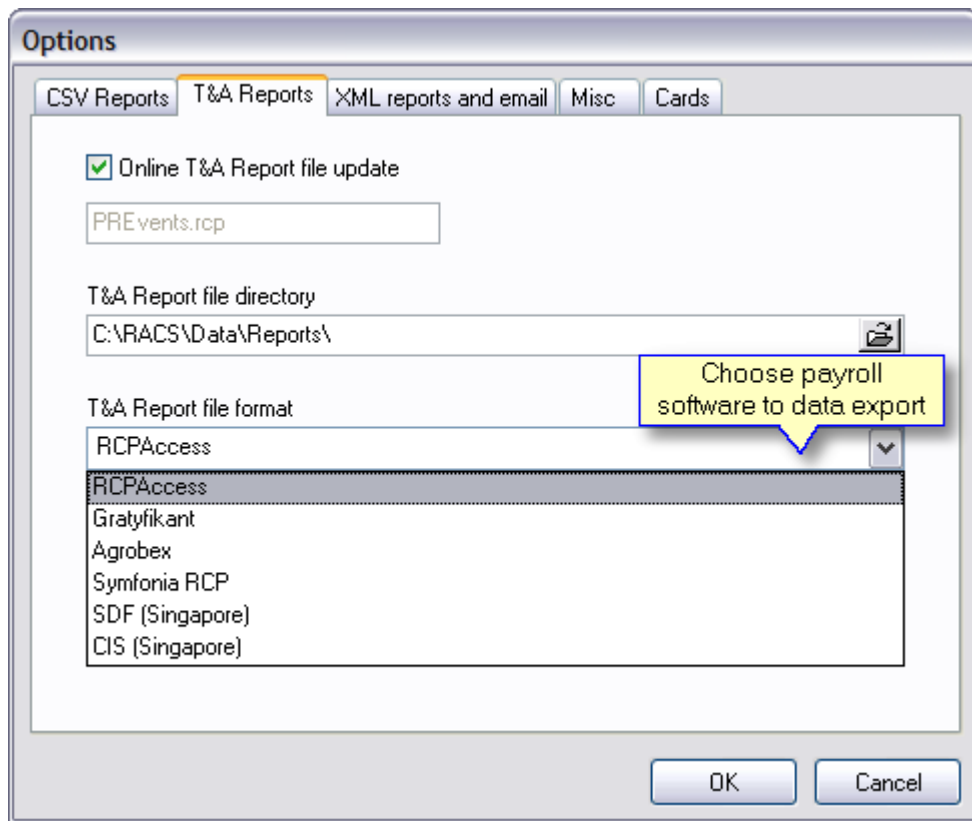


6.2.3.8.2 T&A Reports

When **Online T&A file update** option is enabled program continuously appends events to (*.rcp) file in Monitoring mode. PR Master enables to select appropriate file format, in order to used T&A software. Every events buffer(s) read procedure causes actualisation of this file.

See also:

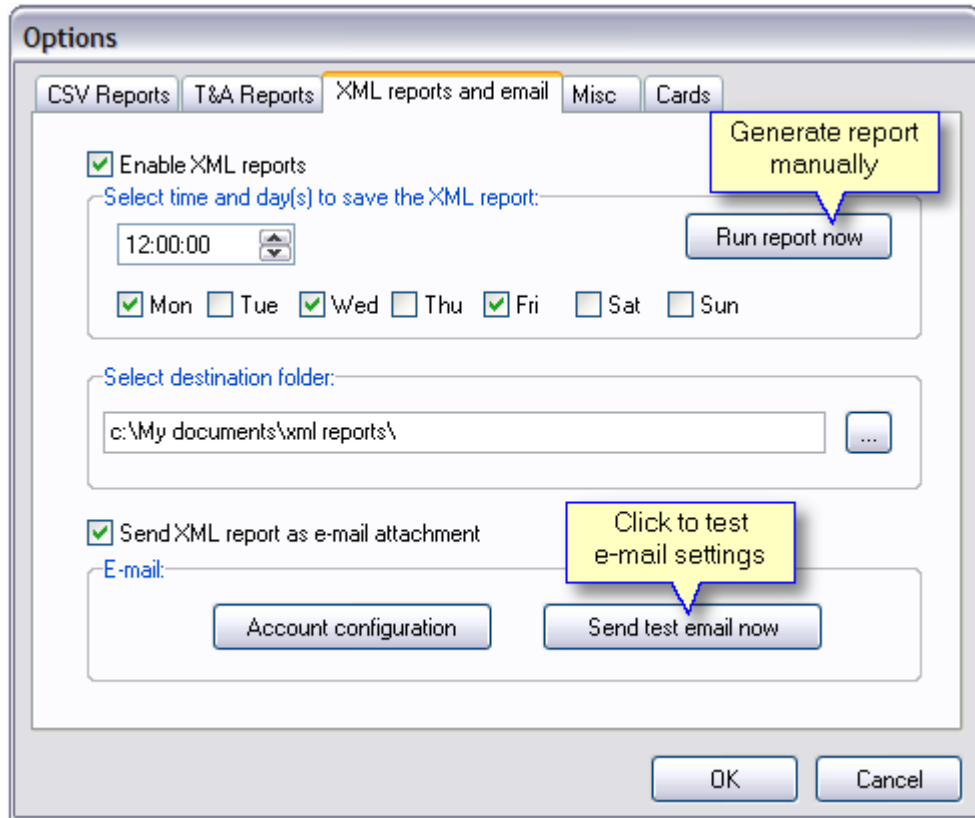
[T&A report](#)



6.2.3.8.3 XML reports and e-mail

PR Master enables user to generate [XML reports](#) according to defined time schedule. XML Report contains all events registered after the last report generation.

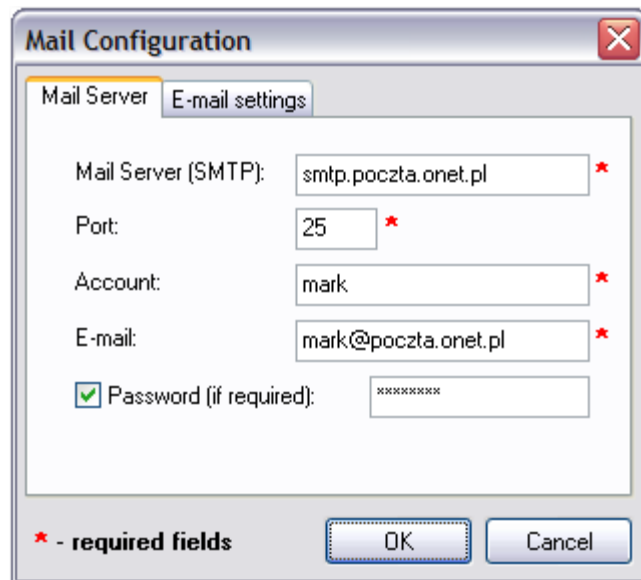
Files with date and time included in file name are saved into selected folder. It's available to generate file report immediately using **Run report now** function.



Reports can be sent by internet as e-mail attachment. To activate this function select **Send XML report as e-mail attachment** and configure e-mail account properly.

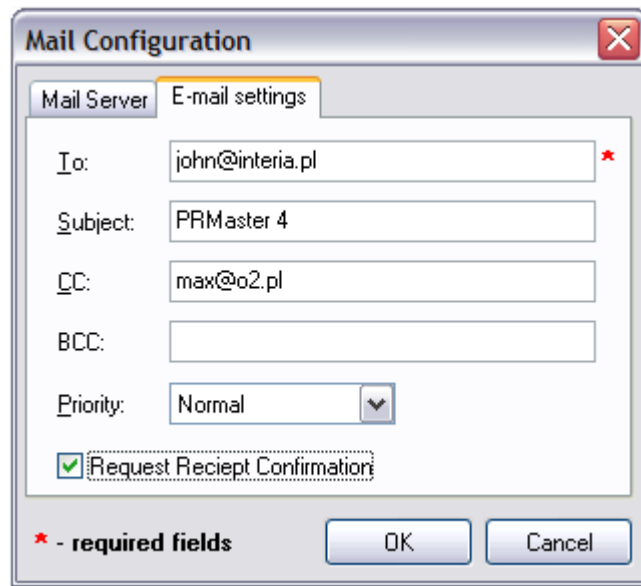
Follow these steps:

First enter data in the **Mail Server (SMTP)** tab.



Click on the **E-mail settings** tab.

Fill in gaps of recipients (**To:**, **CC:**, **BCC:**) and set up **Priority** of message. Once the **Return Receipt** box is checked a notice from receipt will be required.



The image shows a 'Mail Configuration' dialog box with two tabs: 'Mail Server' and 'E-mail settings'. The 'E-mail settings' tab is active. It contains several input fields: 'To:' with the value 'john@interia.pl' and a red asterisk; 'Subject:' with the value 'PRMaster 4'; 'CC:' with the value 'max@o2.pl'; 'BCC:' which is empty; and 'Priority:' with a dropdown menu set to 'Normal'. There is a checked checkbox for 'Request Receipt Confirmation'. At the bottom, there is a legend '* - required fields' and 'OK' and 'Cancel' buttons.

If e-mail account is configured properly, report is send to the selected recipients. Action follows XML file saving to a disc.

6.2.3.8.4 Misc

Miscellaneous program options allows to:

- **Disable DURESS codes**

If the user enters his/her PIN code, which differs from its original form by "one" (plus or minus), controller interprets it as a duress code entry.

When duress entry is recognized the DURESS event is generated and FORCED ENTRY alarm signalisation might occur on output line.

Example:

The original code is [4569], entering [4568][#] or [4560][#] is treated as a duress entry.

- **Events downloaded from networks only upon operator's request (command)**

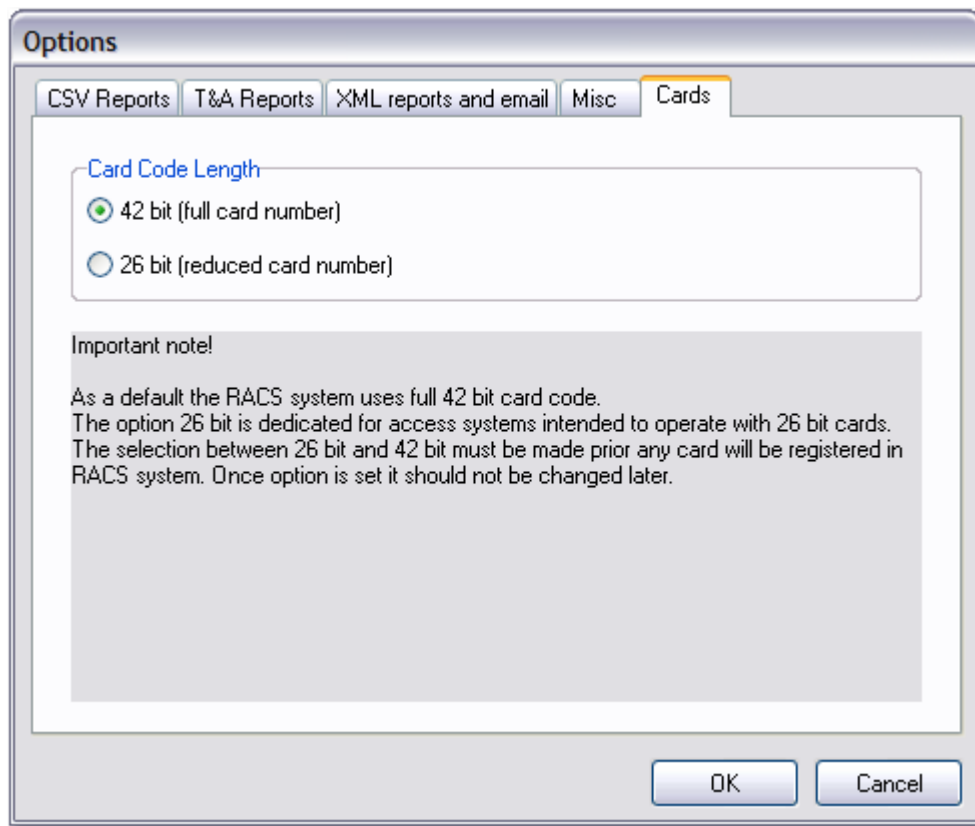
Once the option is enabled events are not automatically downloaded from buffer(s), events stored in controller must be downloaded manually by operator.

- **Disable APB Hierarchy**

See also:

[Controller properties - DURESS](#)

6.2.3.8.5 Cards



6.2.3.9 Backup configuration

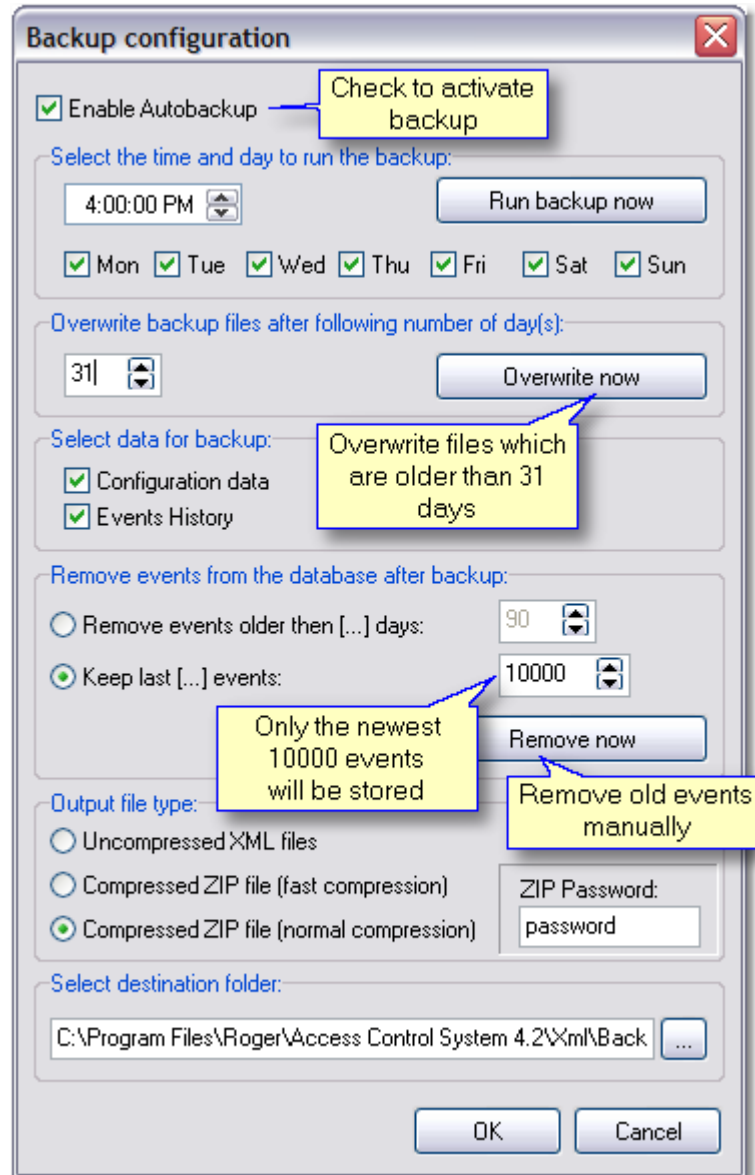
Function of PR Master allows user to configure [Autobackup](#). Generally it secures user from data lost or database crashing. The feature creates backups at defined time: day and hour, or now [**Run backup now**].

To enable Autobackup feature:

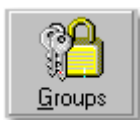
- check **Enable Autobackup** option
- enter time and choose days to run the backup
- select method of removing old events from database
- select data for backup (**Configuration data, Events History**)
- Select output file type and eventually enter password for ZIP file
- Select destination folder

PR Master enables to remove old events in two following ways:

- Remove events older than specified number of days
- Keep last defined number of events)



7 Groups



In RACS users may belong to 250 access [groups](#). Being member of access group determines user access rights in object. All users who belong to the same group have equal access rights to floors and zones. In special cases one group may include only one user. Group members gain access to a particular zones according to time schedules which are defined in a one-week period. Groups have also access rights to 16 floors, which are not controlled by any time schedule.

Every new registered system user belongs to none of defined system groups, he has full access (to all zones and floors) without any time restrictions and belong to group called [**No group**]. Every

7.2 Group properties

In Group properties you must define access rights to all system zones and eventually to 16 floors. To assign time schedule to access zone:

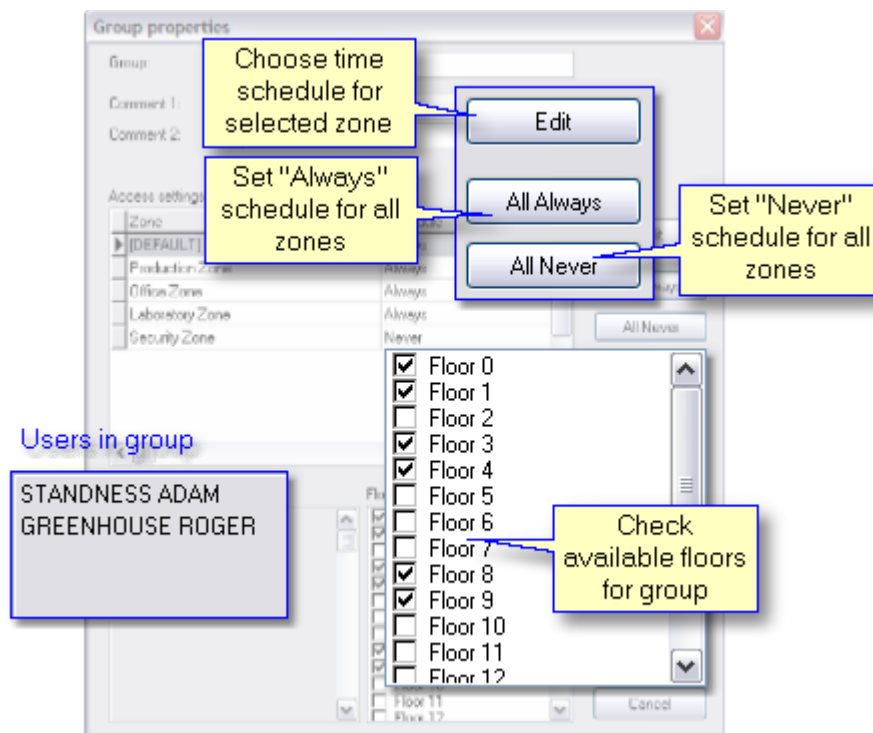
- select access zone
- click **Edit** button
- select time schedule
- click **OK**.

Define which of floors will be available for group by checking boxes in **Elevator Level Access settings**. You have to enable option **Enable XM-8 elevator control module(s)** in Controller properties window in [Options](#) tab.

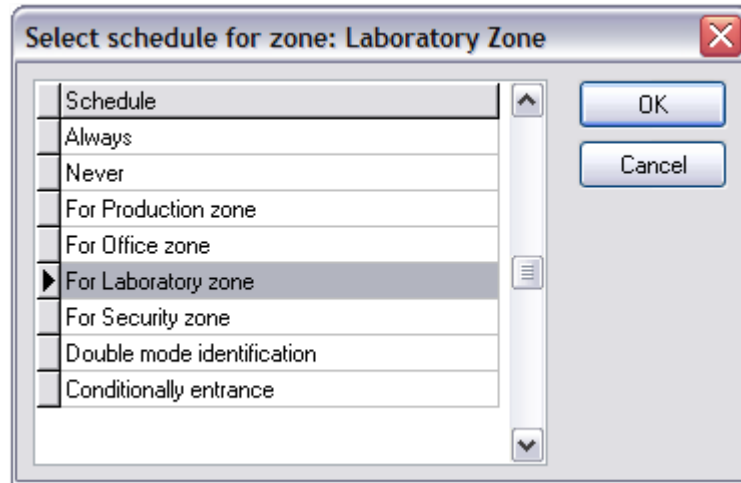


Note:

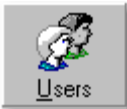
1. PR Master enables to operate with 16 floors (from 0 to 15). To use this feature XM-8 Input/Output expander connected to controller is required.
2. Access rights to floors are not changeable (not restricted by time schedules).



Time schedules: **Always** (access always granted) and **Never** (access never granted) are predefined in program. To select other time schedules you must define it in [Time schedules](#). Click on **All Always** and **All Never** buttons to change schedules for all zones.



8 Users



In Roger Access Control System can be registered up to 4000 users. Every user has his identification number (ID) and may be one of four predefined types of users. Access controllers identify users by their individual identifiers. In the Roger Access Control System identifier is a transponder (Proximity card) or PIN code. It's also available to set double identification mode (Card+PIN), which obligate users to use both method for identification. Sequence is no matter. Every identifier in system can be registered on unlimited time or time period limited to 12 months (from Start date to Expiry date) [Edit users](#). In addition it's possible to set Card usage limit. Defining card usage limits is carried out for each of controllers registered in system. When user activity time expired or card usage limits exceed, controller automatically removes the identifier from the list of valid identifiers. There is no possibility of further using the identifier.

The screenshot shows a user management window with a table of users and a sidebar of actions. Callouts provide the following information:

- V - user activity in system:** A green checkmark indicates the user is active, and a red circle with a slash indicates the user is not active.
- Type of user:** It determines user functions in the system. Various types are distinguished by different colors.
- Access group:** Access control according to defined schedules.
- T&A ID:** User evidence number, identifies user in T&A and Payroll report.
- ID number:** Unique user number.
- Export/Import:** Export/Import user list into csv file.
- Find user:** Find user by First or Last name.

V	ID	User Name	Type	T&A ID	Group name
✓	0	MASTER ROGER	[MASTER]	1234	[No group]
✓	1	SMITH BEN	[SWITCHER] Full (1..49)	1410	
✓	33	BERREN JACK	[SWITCHER] Full (1..49)	47825	
✓	50	EVERSTONE TOM	[SWITCHER] Limited (50..99)	1665	
✓	55	NOWAK JOHN	[SWITCHER] Limited (50..99)	52117	
✓	100	PIERCE ANN	[NORMAL]	1974	
✓	111	ADAMSKY MARK	[NORMAL]	4108	Office Group
✗	222	BLACKBORN JERRY	[NORMAL]	1295	Production Shift 1
✓	333	EAGLEN AMANDA	[NORMAL]	535467	Laboratory Group
✓	444	HAMET BETTY	[NORMAL]	39150	Production Shift 1
✓	555	MARCH DAISY	[NORMAL]	98351	Prod
✗	666	FINGER IRENE	[NORMAL]	34589	Secu
✓	777	PETERSEN ANDREE	[NORMAL]	3637	Laboratory Group
✓	888	STANDNESS ADAM	[NORMAL]		

Actions on the right: Add, Delete, Edit, Delete all, Change type, Change ID, Export, Import, Show deleted users (checkbox), OK.

Search options at the bottom: Arr, ID number, Type, First name, Last name, Group, Find..., OK.

Add - add new user (program allows registering up to 4000 users)

Delete - remove selected user from list

Edit - change user settings

Delete all - remove all users from list

Change type - change user type: MASTER, SWITCHER Full, SWITCHER Limited, NORMAL)

Change ID - change user ID number

Export - export users list to external csv file

Import - import users list from external csv file

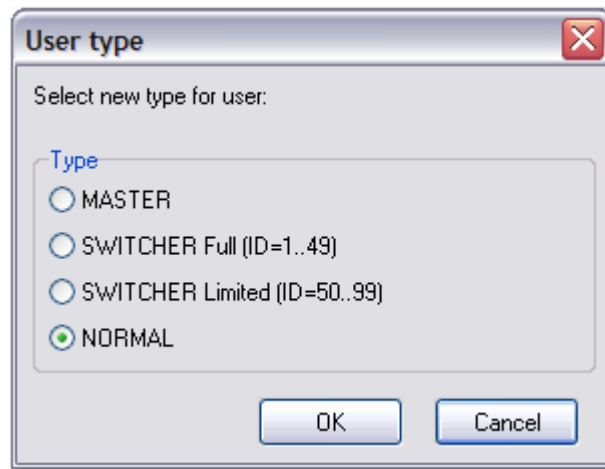


Note:

It's available to append users to existing user list through the **Import** option.

8.1 Add users

To add new system user choose **Add** from [Users](#) window



Select one of four types of users:

- MASTER – permission to door opening, switching to **ON/OFF** mode and enter manual programming mode (Identification number 0).
- SWITCHER Full - authorization for door opening, switching to **ON/OFF** mode (Identification number from 1 to 49).
- SWITCHER Limited - not allowed to door opening, permission to switching door mode only (Identification number from 50 to 99).
- NORMAL - permission to door opening only. This type of users has (Identification number from 100 to 3999).

Once the type of user is selected, click **OK**. User properties window will appear ([User properties](#)).



Note:

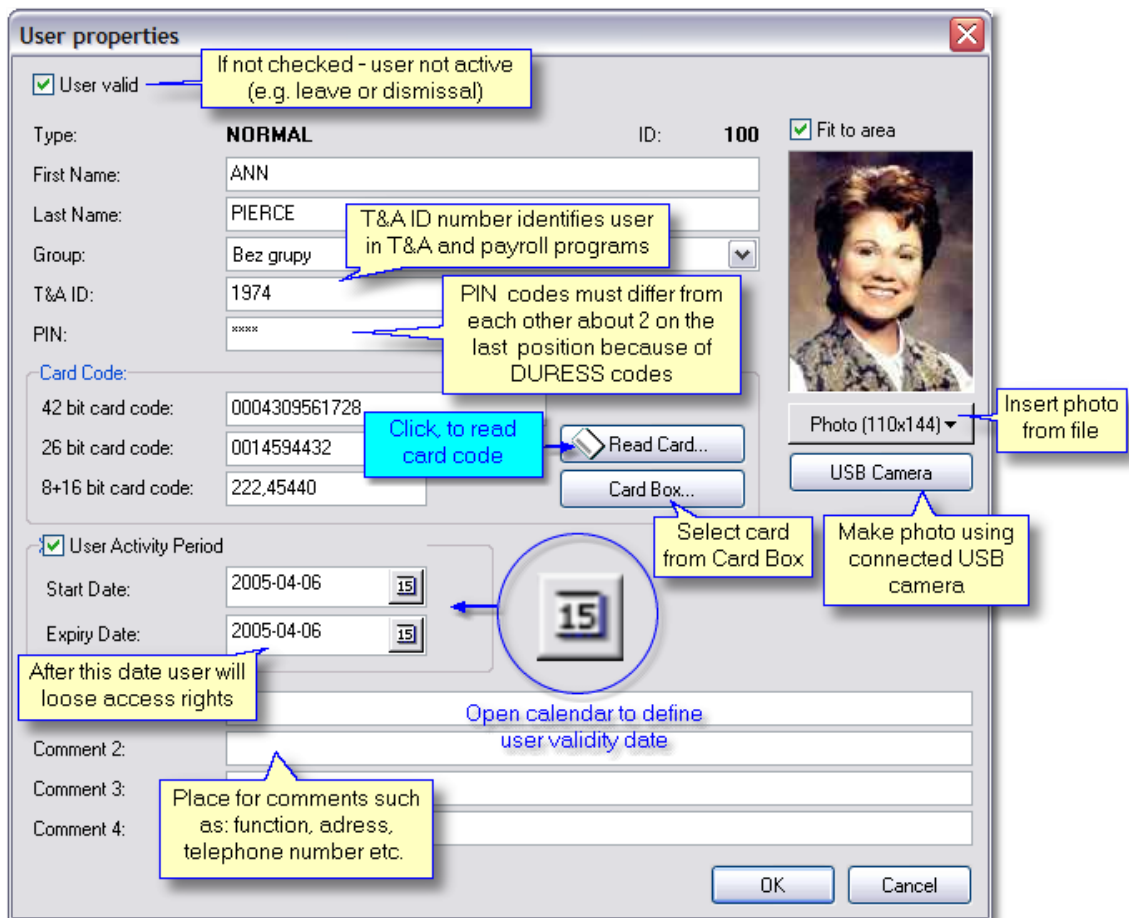
User with ID=1000 - 3999 (NORMAL) may be additionally defined as a Local SWITCHER on particular controller or controllers.

See also:

[Advanced](#)

8.2 User Properties

User properties window includes all information concerning system user.



To configure system user:

- Enable option **User valid**
- Fill gaps: **First Name**, **Last Name**
- Enrol system user into defined earlier access group by selecting position from **Group** menu
- Enter **PIN** code and confirm
- Assign Card Code to the user using one of methods described below

Optionally:

- Load user **Photo** from a file or make photo directly using USB camera
- Check **User Activity Period** and define Start date, Expiry date using calendar
- Place comments

Program enables two methods of assigning card to the system user:

- Automatically read card code on selected reader. Click on **Read Card** button, select name of controller and next approach Card to the reader. Once the card is properly read, program returns to the **User properties** window, card code should be displayed in the gaps.
- From **Card Box**. Click on Card Box and select appropriate card. Card Box includes collection of cards entered earlier. It gives you availability to Add, Remove or Review cards

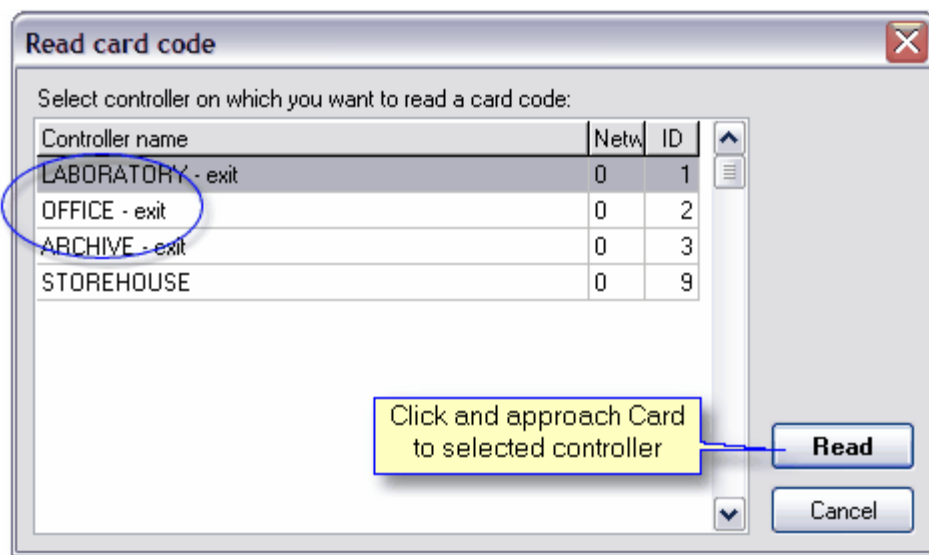
already occupied by users.



Note:

1. If user identifier(card) is registered for first time, it's necessary to read card code on reader.
2. Often there are numbers printed on cards provided from other companies, however, there aren't identification RACS codes.
3. Type of users SWITCHER Full and Limited can not be a local SWITCHER.

8.3 Read card code

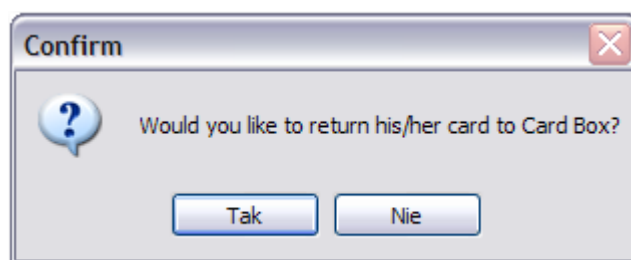


Before you start card code reading, first select controller on which you want to read a card code. Next click on **Read** button and approach transponder to the selected controller.

8.4 Delete users

To remove user from the list use one of methods listed below:

- open [User list](#)
- select user and click **Delete**
- click **Yes** to confirm
- return user card to Card Box, click **Yes** or **No**



- close User list and send configuration to the system (main menu: **Commands** -> [Update system](#))

Second method:

- open [Quick User Update](#)
- select user and click **Delete**
- click **Yes** to confirm
- return user card to Card Box, click **Yes** or **No**
- click **OK** to confirm system configuration update



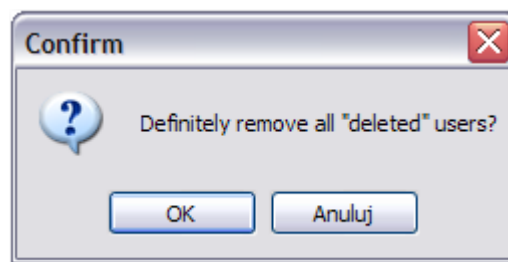
Note:

Removed user still remains in system database. It's possible to browse events in which he/she has participated.

To view removed users:

- choose **Edit** from main menu then select **Users**
- check option **Show deleted users**.

To permanently remove users from database check **Show deleted users**, click **Remove deleted** and **OK** to confirm.



9 Time schedules



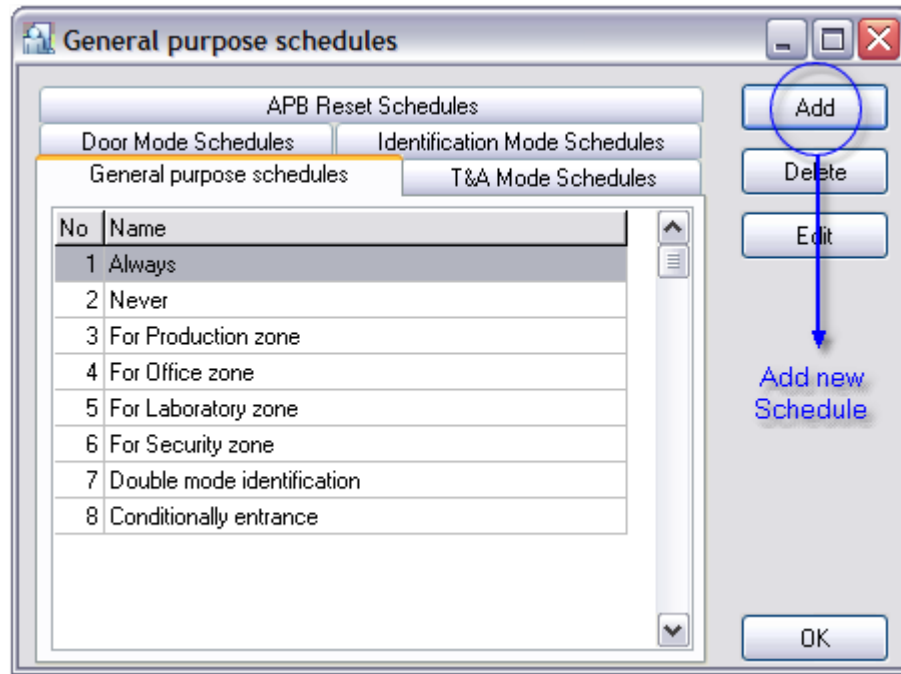
[Time schedule](#) is a set of defined time periods (From...To...) for every day of week (Monday to Sunday) and also for Holidays (H1, H2, H3, H4). Feature allows to perform specified actions by RACS in one-week period.

There are five types of Time Schedules:

- [APB reset schedules](#)
- [Door mode schedules](#)
- [Identification Mode Schedules](#)
- [General purpose schedule](#)
- [T&A mode schedules](#)

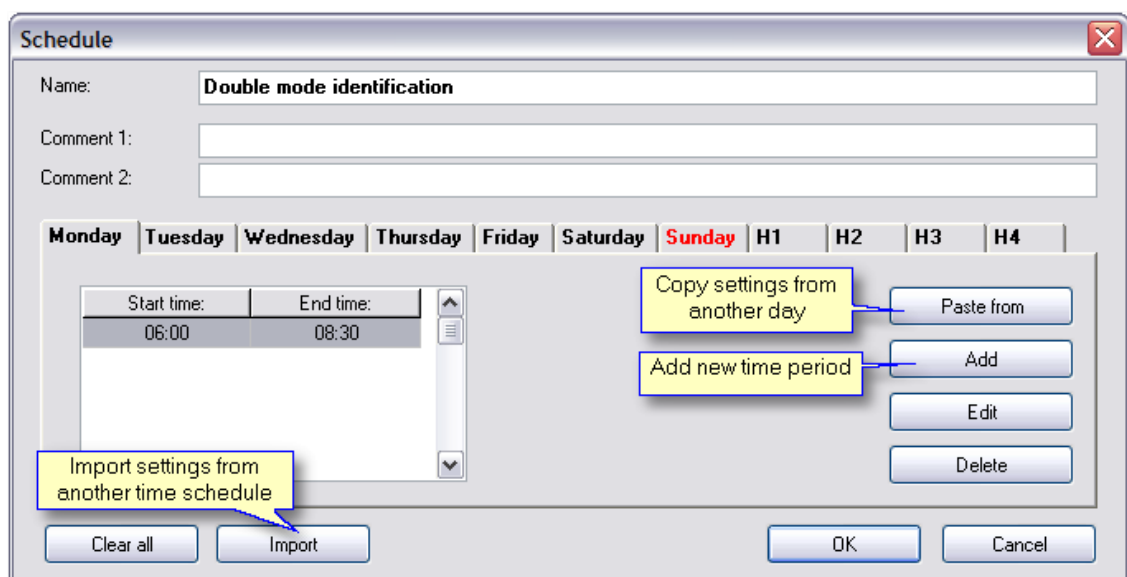
To define new Time Schedule:

- click on **Schedules** icon from operator tools or select **Edit** -> **Schedules** from the main menu
- click one of five available tabs
- click **Add** button



9.1 General purpose schedules

General purpose schedule may be dedicated to one or more functions of controller. For example, the same time schedule can be applied to control group access for defined zones, [#] Key options, input line and Conditional mode of controller simultaneously. PRxx2 type of controllers operate up to 99 this type of schedules. General purpose schedules haven't one specified purpose.



By default there are two types of schedules: **Always** and **Never**. To define new time schedule follow these steps:

- enter **Name** of time schedule
- choose day (Monday - Sunday) by clicking available tab
- click **Add**
- specify **Start time** and **End time**
- click **OK** to confirm.

General purpose schedules can be applied to control:

- group access to zones
- activity of input and output lines
- activity of [F1] - [F4] keys
- activity of Keypad Commands
- Arm/Disarm mode
- [#] key option
- activity of High Security option
- activity of Facility Code option
- activity of [Card+Card] option
- activity of SWITCHER Users
- APB Hard/APB Soft option
- activity of Conditional Access option

Paste from - copy time period definitions from other days

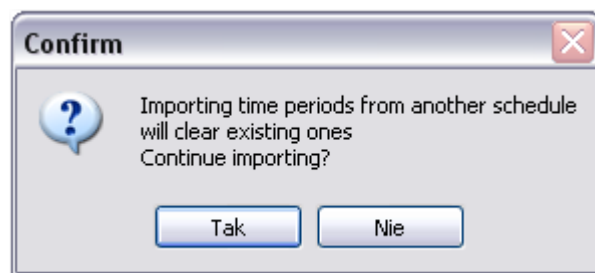
Clear all - reset all defined time periods in schedule

Import - import period definitions from existing time schedule. It's available to import settings only from time schedules of the same type. Importing time periods from another schedule will clear existing settings.



Note:

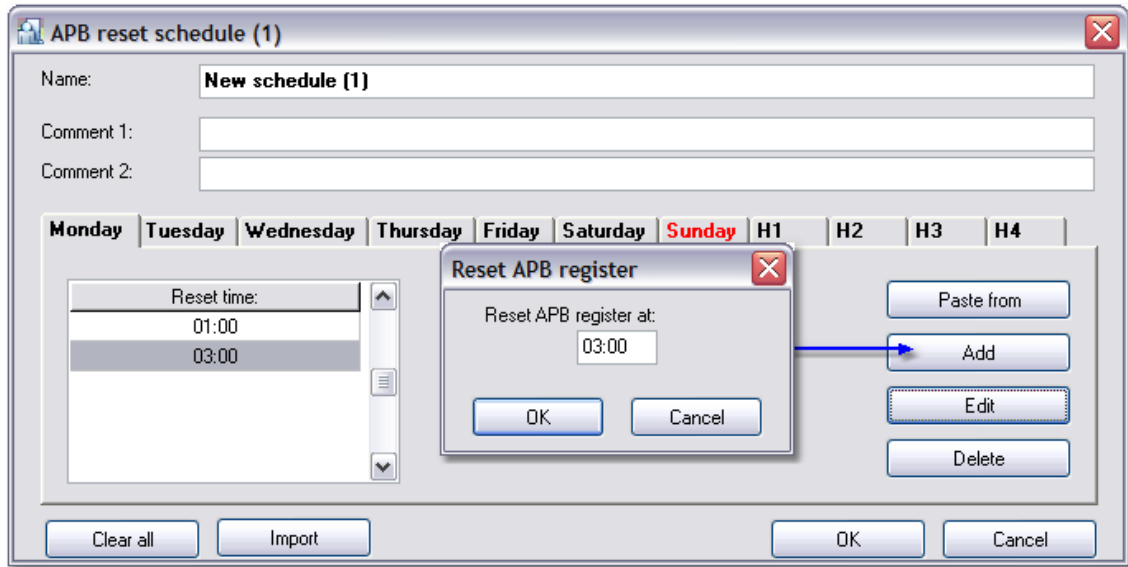
Importing time periods from another schedule will clear existing ones.



9.2 APB reset schedules

APB reset schedules are used to reset Anti-Passback registry. After the APB reset each of users in APB registry has undefined status (it's impossible to check, where the user was logged lastly, on entrance or exit). User with "clear" status is allowed to use identifier on entrance and exit as well. Once the first access is granted the controller starts to exact APB rules.

Defining this schedule is carrying out just like in case General purpose schedule except that time of ABP reset is set.



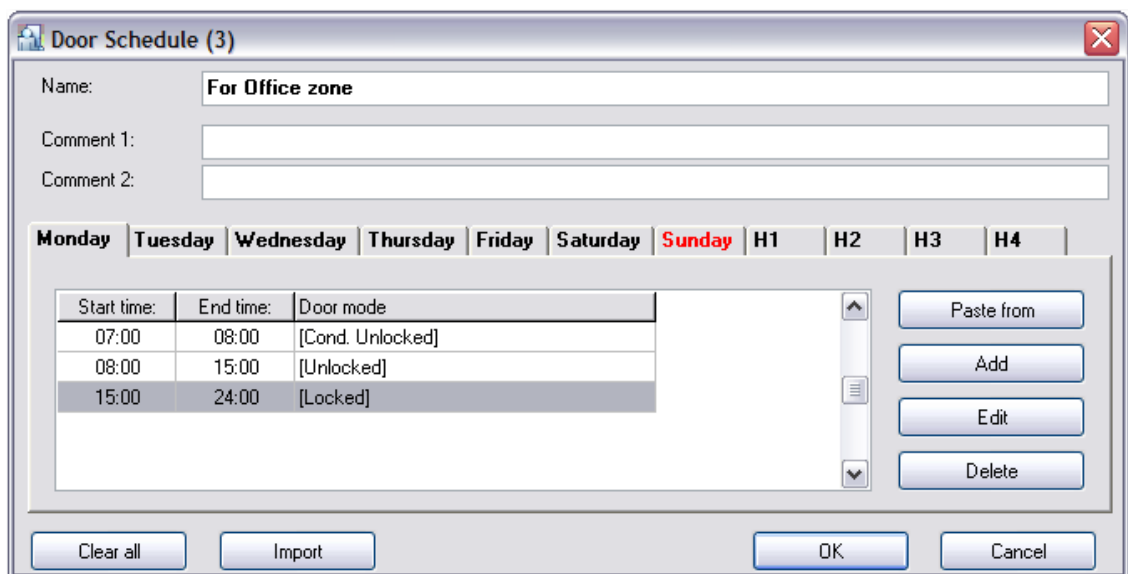
See also:

[Paste from](#), [Clear all](#), [Import](#)

9.3 Door mode schedules

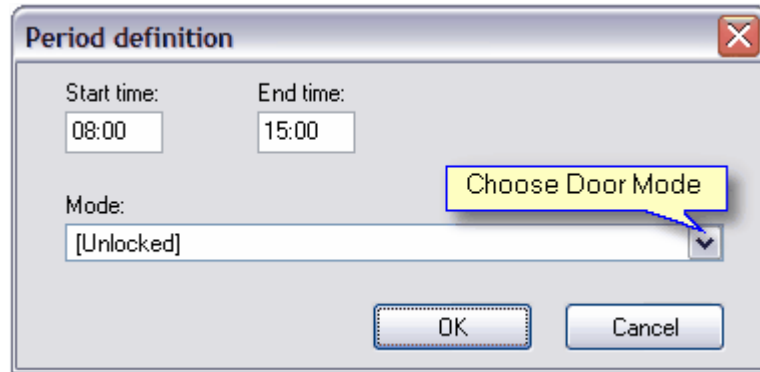
Door mode schedule allows to switch controller automatically between door modes. Door Mode determines how the controller will energize and de-energize door lock. Door lock can be set to few listed below modes of operation:

- **Normal** - Door lock is activated after controller decide to grant access.
- **Unlocked** - Door lock is continuously energized, door can be opened by any unauthorized person.
- **Conditional Unlocked** - Initially door lock is not energized, but when first authorized person come and use its identifier lock became energized and remain in this state until new door mode is set.
- **Locked** - Activation of door lock is permanently forbidden, no matter if some user has authorization for access or not, every attempt to open the lock will be rejected.



To define door mode schedule:

- enter **Name** of time schedule
- choose day (Monday - Sunday) by clicking available tab
- click **Add**



- specify Start time and End time
- select **Door mode** from menu: [Unlocked], [Locked], [Cond.Unlocked]
- click **OK** to confirm



Note:

In time between defined periods the controller automatically returns into **[Normal]** Door mode.

See also:

[Paste from](#), [Clear all](#), [Import](#)

9.4 Identification Mode Schedule

[Identification Mode Schedule](#) allows to switch controller automatically between Identification modes. Defining this schedule is carried out just like in case General purpose schedule except that identification modes are set. There are four identification modes available:

- Card and PIN
- Card or PIN
- Card only
- PIN only

Once you've specified all time periods you should assign time schedule to a selected reader. Open **Edit** -> **Networks** -> **Controllers** -> **Properties** -> **Terminal ID1/Terminal ID0** and select Identification mode from drop-down menu.

Identification Mode Schedule (1)

Name:

Custom 1:

Custom 2:

Monday Tuesday Wednesday Thursday Friday Saturday **Sunday** H1 H2 H3 H4

From time:	To time:	Identification Mode
00:00	06:59	Card and PIN
07:00	18:00	Card or PIN
18:01	23:59	Card and PIN

Buttons: Paste from, Add, Edit, Delete, Clear all, Import, OK, Cancel

**Note:**

In time between defined periods the controller automatically returns into default *identification mode*.

See also:

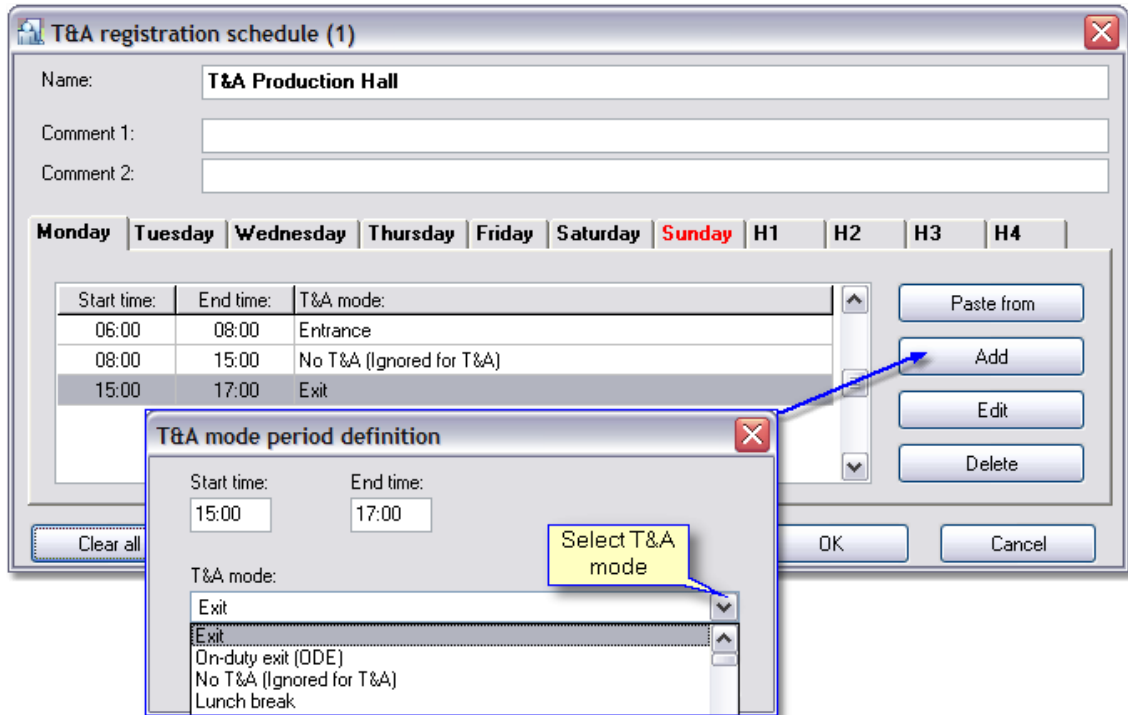
[Paste from](#), [Clear all](#), [Import](#)

9.5 T&A mode schedules

[T&A mode schedule](#) allows to switch controller automatically between T&A modes. Defining T&A mode schedule is carried out just like in case General purpose schedule except that T&A modes are set.

To define T&A mode schedule:

- enter **Name** of time schedule
- choose day (Monday - Sunday) by clicking available tab
- click **Add**
- specify **Start time** and **End time**
- Select **T&A mode** from drop-down menu
- click **OK** to confirm.



Once you've completed defining time periods:

- open **Edit** -> **Networks** -> **Controllers** -> **Properties** -> ([Options](#) tab)
- check **Enable T&A Schedule** to activate feature



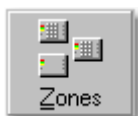
Note:

1. In time between defined periods the controller automatically returns into default **T&A mode**.
2. There are four predefined T&A modes: Entry, Exit, On-duty exit (ODE) and No T&A (Ignored). Additionally you can define your own T&A modes and assign them time periods. To add another T&A modes choose **Tools** -> [T&A modes](#) from main menu.

See also:

[Paste from](#), [Clear all](#), [Import](#)

10 Zones



Access Zone - set of selected identification points (controllers with built-in readers or access terminals) which are construed as a cohesive area in access control system. Examples of access zones: Production Hall, Office, Workshop, Warehouse, Floor etc.

Generally the main purpose of Zone concept is to make defining access rights operation more easy. Thanks to zones idea it's available to define access rights not only for one access point (single door) but for set of devices (controllers/terminals) which control access to specified area in object.

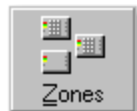
In special case each of access points (rooms) can compose single separated access zone. In this

situation access rights definition will be referred to individual door or passage. Every controller must be assigned to previously defined access zone. Each of new added controllers belongs to Default zone.

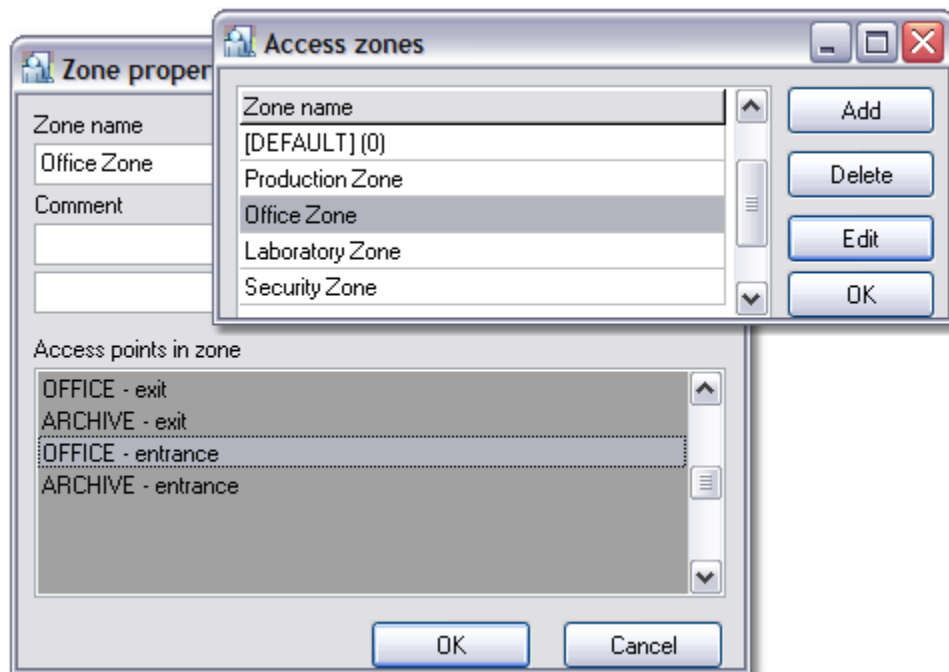
To add reader to access zone choose **Edit -> Network -> Controllers -> Properties -> Terminal ID1/Terminal ID0** and select **Access Zone** from menu.

10.1 Add access zone

To add new access zone:



- click on **Zones** from the operator tools or **Edit -> Zones** from main menu
- click **Add** button
- type **Name** of Zone
- click **OK**



Note:

[DEFAULT] (0) is a predefined zone which cannot be edited nor removed.

11 Networks



Roger Access Control System consists of control panels CPR (max 10), PR controllers and PRT terminals. All of control panels can operate up to 32 access controllers. Network called also Subsystem is composed of control panel with controllers and terminals.

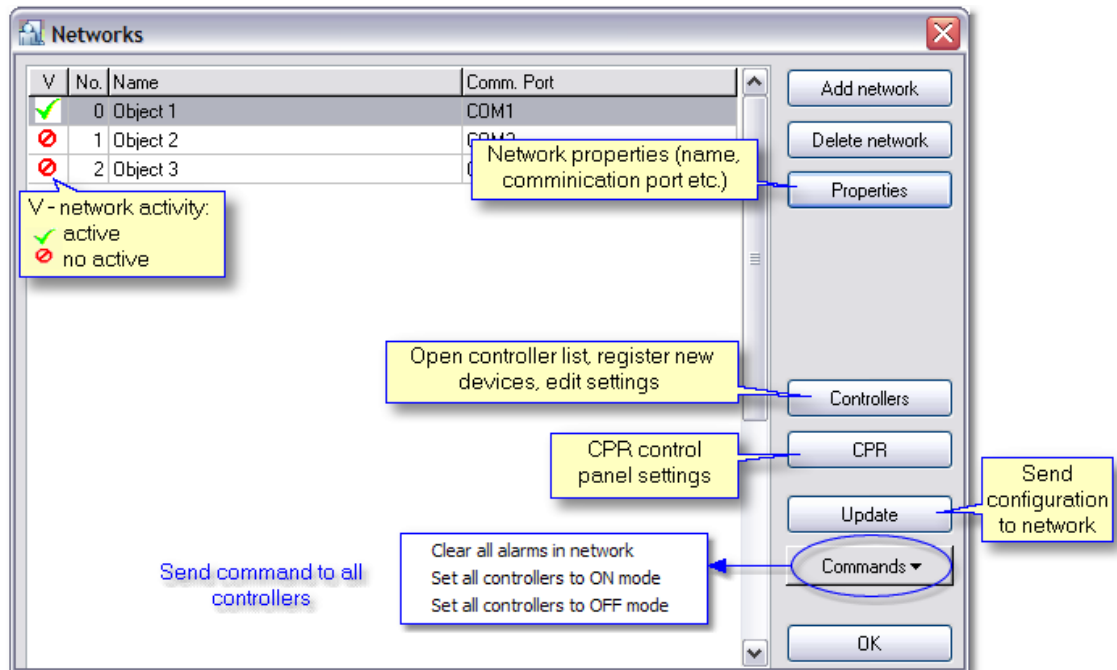
From this window you are able to configure all your networks, control panels, send commands and update system.

Description of available options:

- **Add network** - add new network (read [Add new network](#))
- **Delete network** - if network is not empty, you have to delete controllers first
- **Properties** - edit selected network (change communication port, port timeout)
- **Controllers** - open controllers list
- **CPR** - control panel options
- **Commands** - send command to all controllers

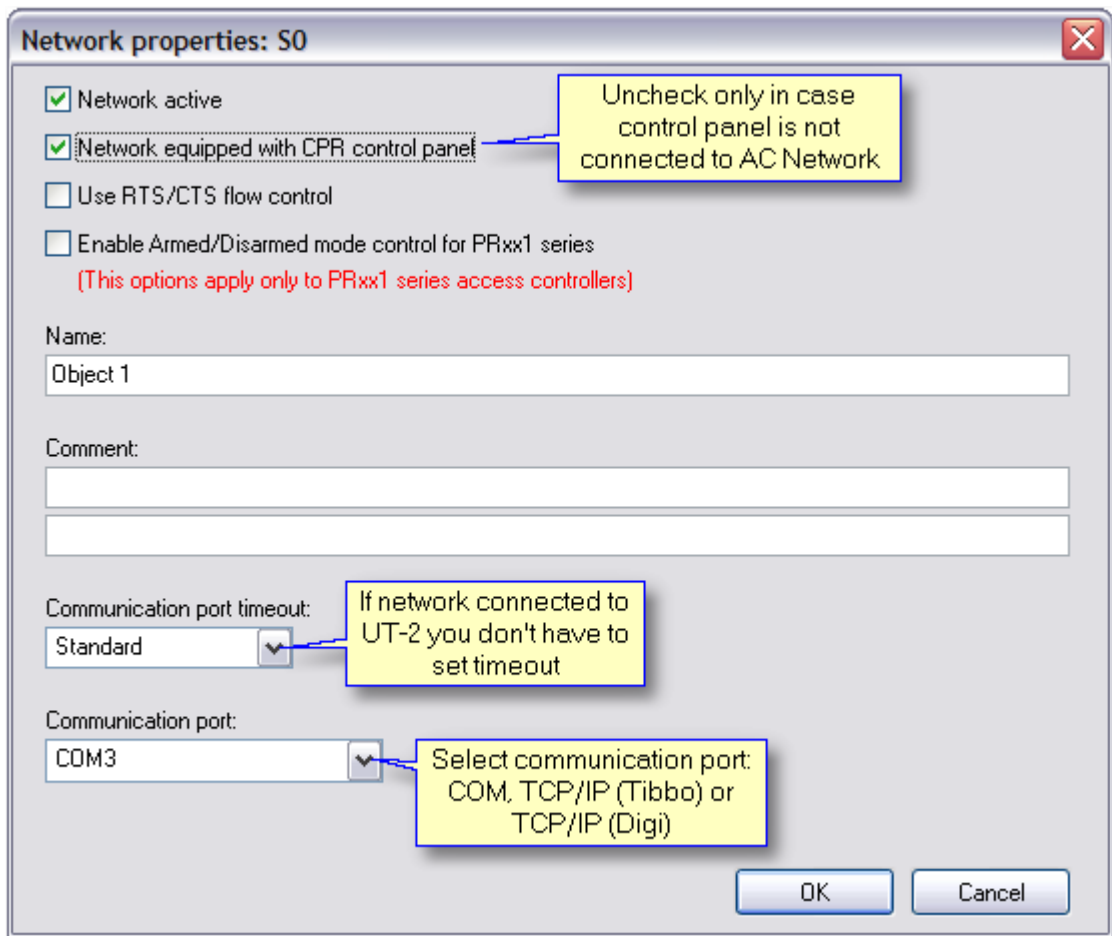
See also:

[Add new network](#)



11.1 Network properties

To add new network connected to **UT-2** interface:



- click on **Networks** from operator tools or **Edit -> Networks** from main menu
- click on **Add Network** button
- type **Name** of network
- select **Communication port** - COM
- enable **Network equipped with control panel** option if CPR device is connected
- click **OK**

Once the network configuration is finished you can click [Controllers](#) and proceed to search devices.

Description of available options:

- **Network active** - activate or inactivate network
- **Network equipped with control panel** - check if control panel is connected
- **Enable Armed/Disarmed mode control for PRxx1 series** - if PRxx1 type of controllers are connected

Network connected trough UT-4 communication interface expands RACS functionality. In this

configuration you are able to configure and supervise RACS system from remote place in local network (LAN) or (WAN). System with UT-4 allows also to share RACS database.

To add new network connected to **UT-4** interface:



- click on **Networks** from operator tools or **Edit -> Networks** from main menu
- click on **Add Network** button
- type **Name** of network
- enable **Network equipped with control panel** option if CPR device is connected
- select **Communication port** - TCP/IP
- choose **communication port timeout**
- click on **Find** button to search UT-4 devices (refer to [UT-4 configuration](#) chapter)

IP address of interface, should be compatible with address of network which is connected to. In case you enter IP address manually remember that default port of UT-4 is 1001. If you don't know the rules of IP addressing, you should contact with your network administrator.



Note:

Device address must differ from computer IP address with the last position after dot. For example if 192.168.0.100 is the IP address of PC then you should enter 192.168.0.xxx for device, where xxx is unique number in local network (in range from 0 to 255). It means that, any other device can't have this number.

See also:

[UT-4 configuration System without CPR](#)

11.1.1 UT-4 configuration

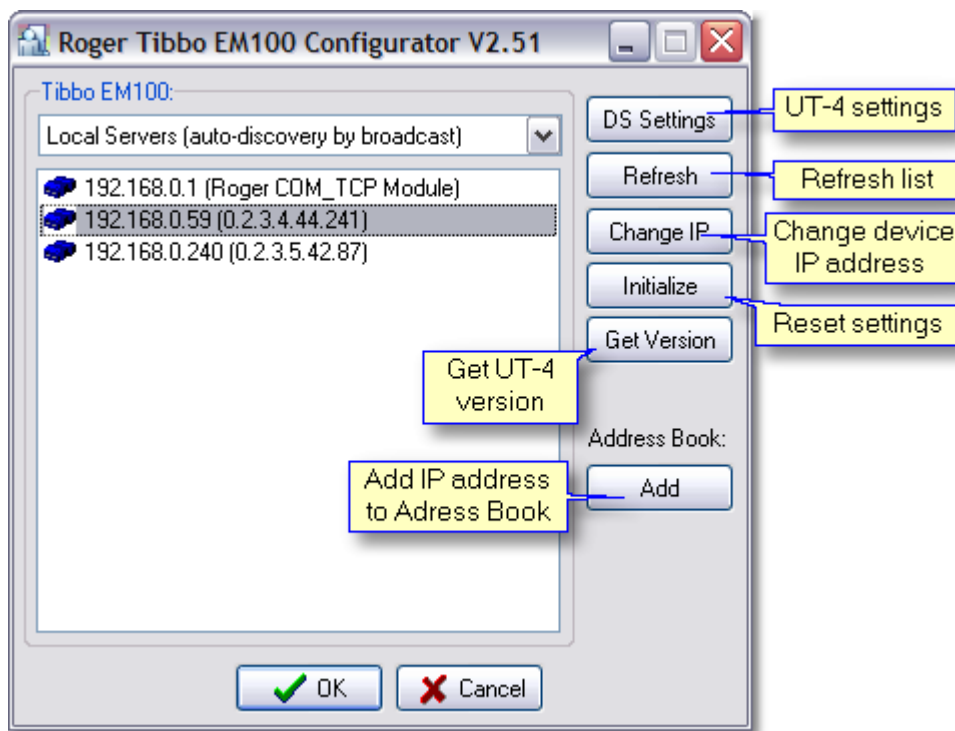
This tool allows to search local network (LAN) using **auto-discovery by broadcast** method or **(in WAN)** access IP address(es) added to Address Book.

In LAN network both methods are useful but you shouldn't use broadcast method when UT-4 is connected to WAN network.

There are two types of device searching:

- **auto-discovery by broadcast** (search LAN only)
- from the **Address book** (search LAN or WAN)

Once the search procedure is completed list of devices will display.

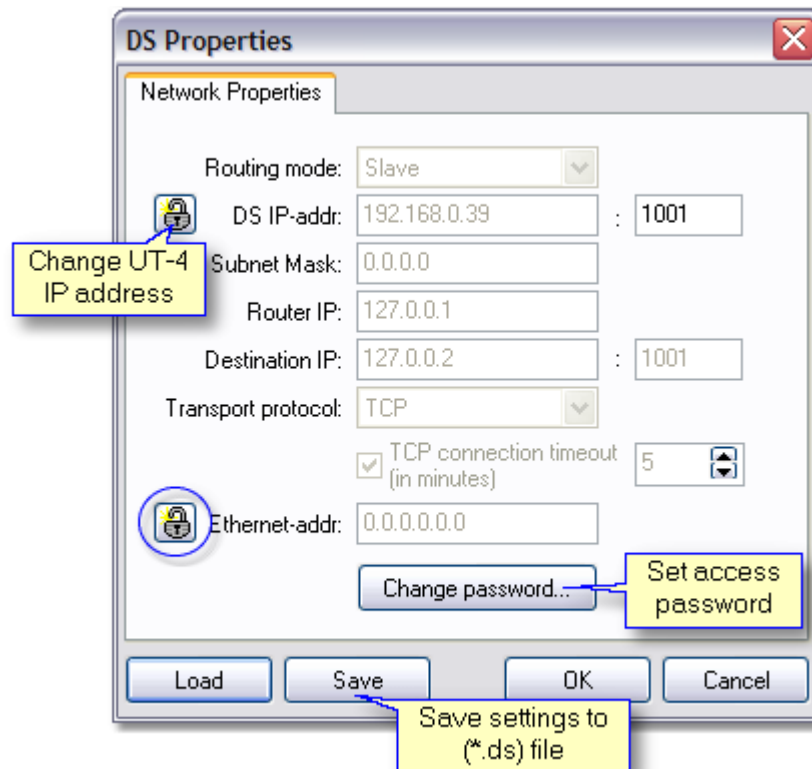


Description:

- **DS settings** - advanced settings of UT-4
- **Initialize** - reset settings, set all to default

11.1.1.1 Network properties

Feature enables to change [Network Properties](#). Access to UT-4 can be secured by password. It's available to **Save** and **Load** all settings from (*.ds) file. User can also change UT-4 interface IP-address and Ethernet address.

**Note:**

Changing IP address can cause communications problem and make device inaccessible. Changing the value of [**Ethernet-addr**] option is not recommended and almost never required.

11.1.2 DIGI configuration

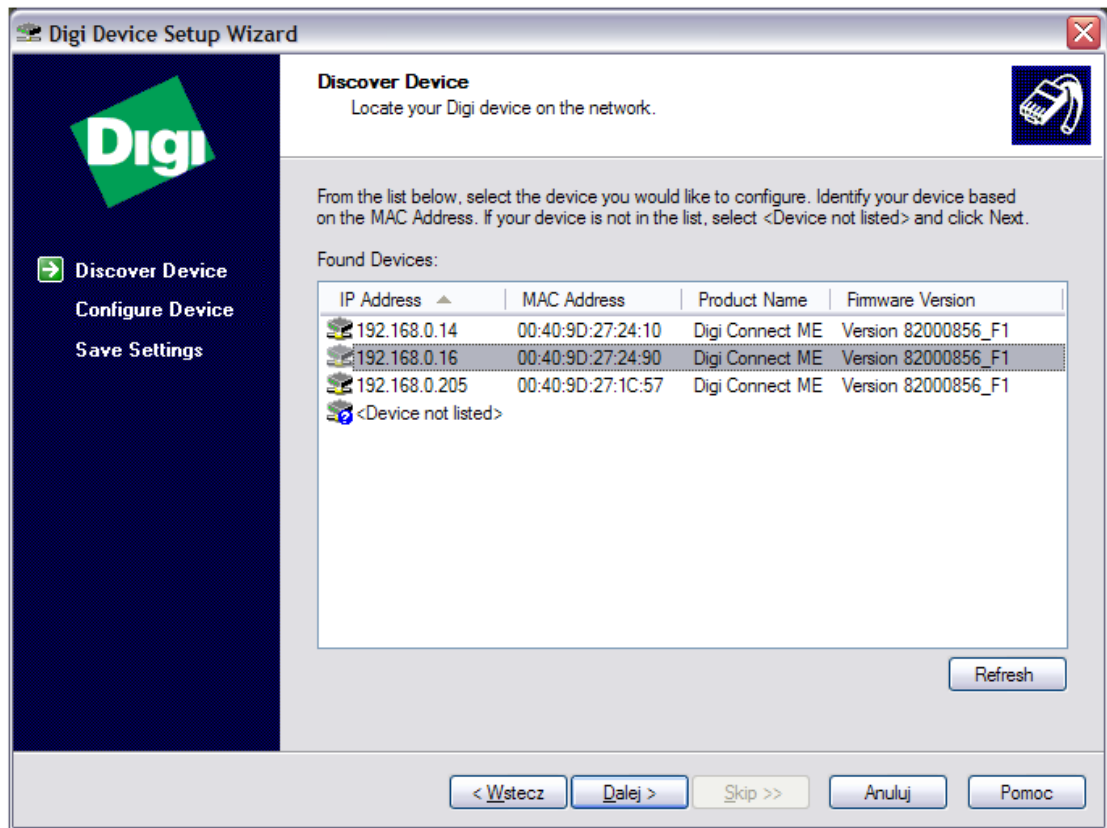
Installation on Microsoft XP

Digi Configurator is a component of RACS 4.2 software package. Using the Digi Device Setup Wizard (digi configurator) is the recommended and preferred method for configuration. It assigns an IP address for the device, configures the device based on your description of the device environment, and determines whether you need to install RealPort.

- to run Digi Configurator click menu **Start** -> **All programs** -> **Roger ACS 4.2** -> **Digi Configurator**.



- before beginning, ensure that you have:
 1. Connected the Digi Connect to the network and powered it on
 2. Recorded the Digi Connect MAC address, which is located on the bottom or back of the device. You will need this address to choose your device from the list of discovered devices that will appear during the next step.
- click **Next >** to continue, the following window will appear:

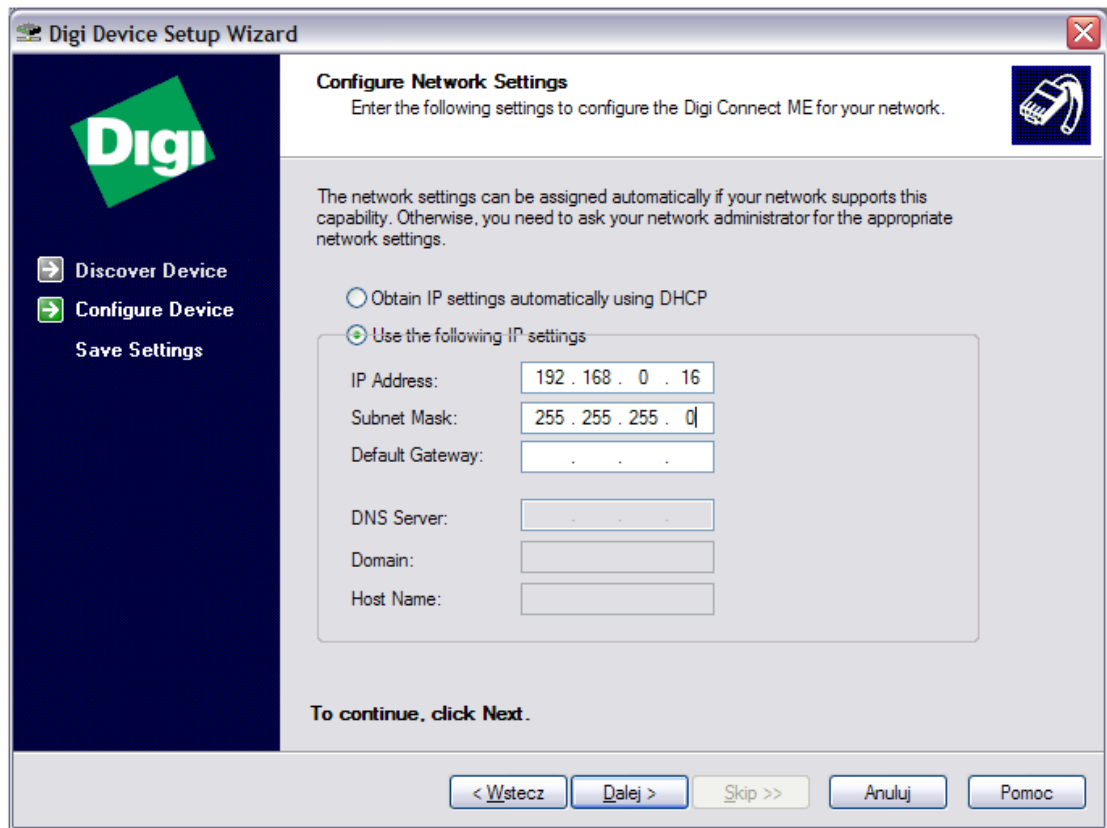


- select your device from the list. To rediscover devices, click **Refresh**.

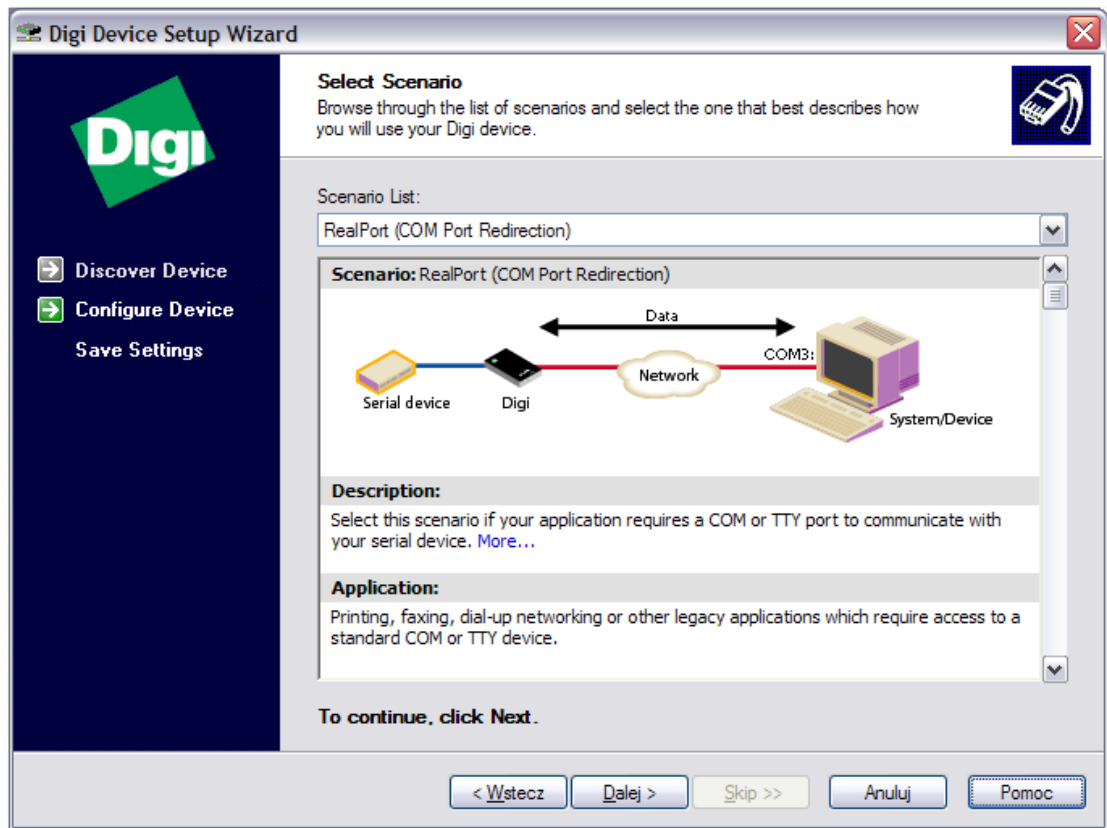
If your device is:

- Listed in black, the wizard fully supports it.
- Listed in gray, the IP address, subnet mask, and default gateway can be configured, but the wizard does not support configuration of other parameters.
- Listed in red with a label that says <unconfigured>, the DHCP client feature is on (the default) and there is no DHCP server on the network.
- Listed in red with a label that says <misconfigured>, the device has been configured before and the IP address settings do not work on the subnet the device is connected to.
- Not listed, the wizard could not locate it.

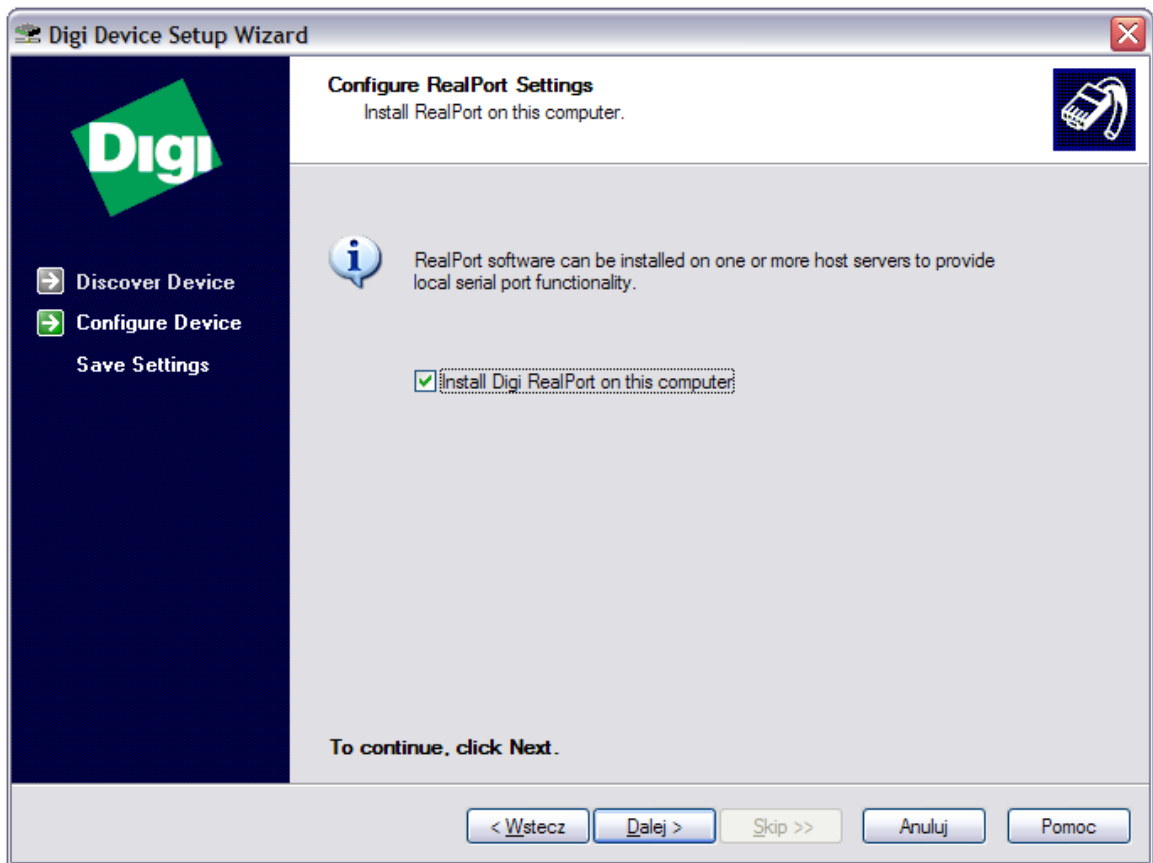
- click **Next >** to continue, the following window will appear:



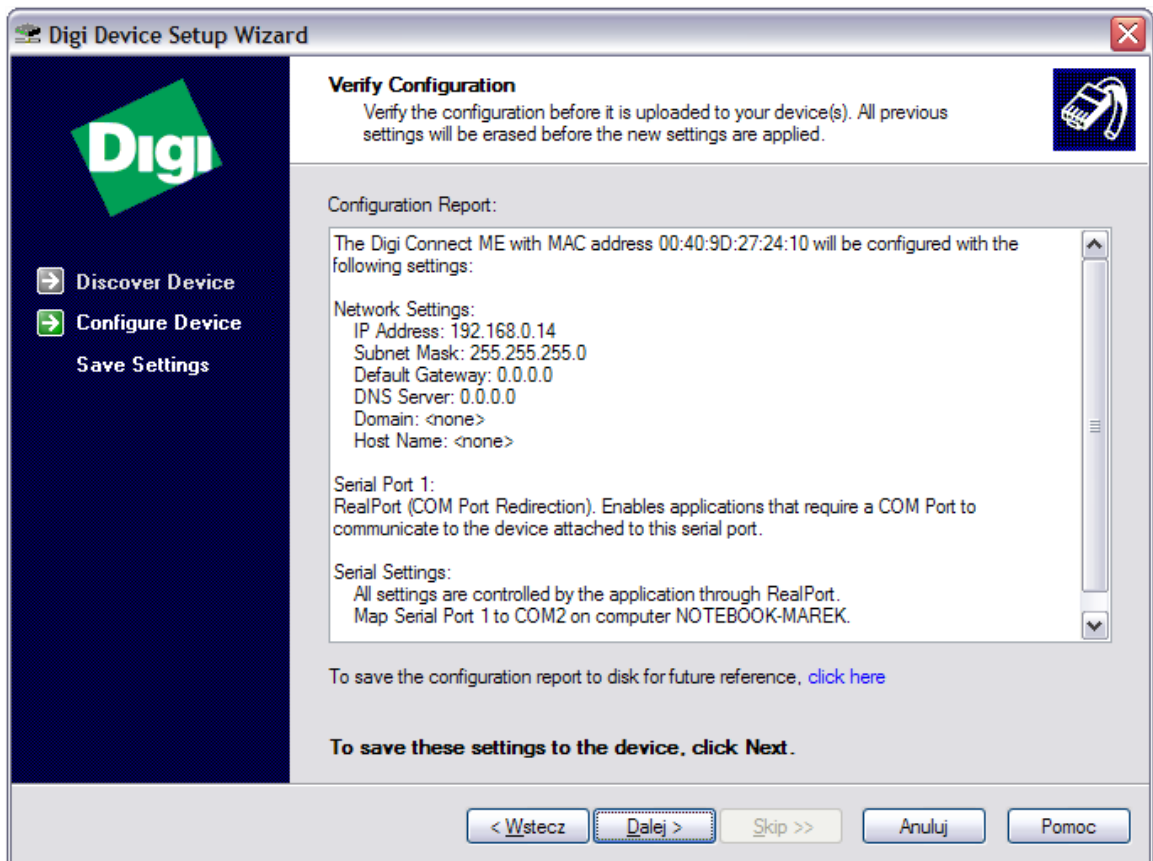
- select **Obtain IP Address settings automatically using DHCP** - this option requires a DHCP server to assign network settings. The Digi Connect ship with the DHCP client feature enabled. So if your site has a DHCP server, choose this setting and your Digi Connect will request network settings from the server.
- or select **Use the following IP settings** - this option requires that you gather network setting information from your network administrator and then input it on this wizard page. The IP address and subnet mask are required. Other fields are optional.
- click **Next >** to continue, the following window will appear:



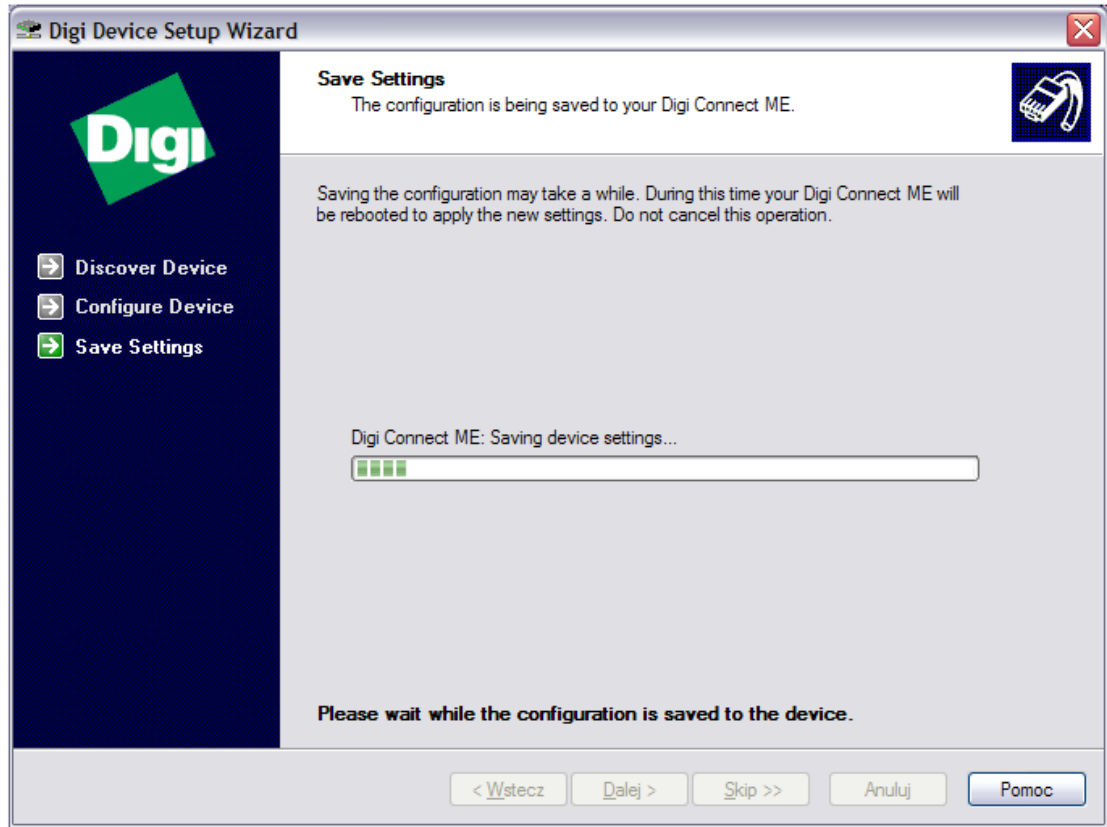
- select **RealPort (COM Port Redirection)** option. With the RealPort® technology, we emulate a serial port for RACS application. That means we work some magic in Windows (or other operating system) which allows the application to believe it is controlling a real serial port like COM1, and we redirect or send all information over the network to the device server. This is sometimes called Virtual Serial Port.
- click **Next >** to continue, the following window will appear:



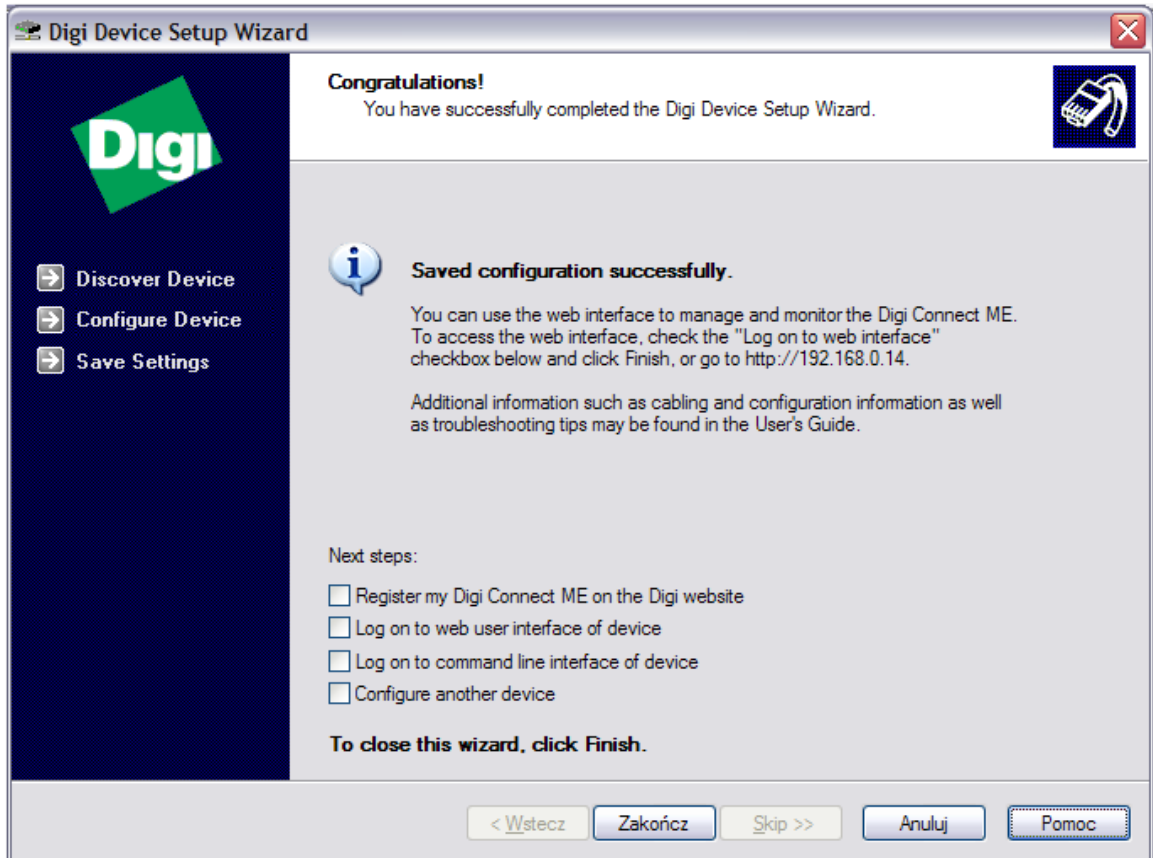
- check **Install Digi RealPort on this computer** option
- click **Next >** to continue, the following window will appear:



- Verify the configuration before you start to upload it to the device. All previous settings will be erased before the new settings are applied. You can save configuration report to disk for future reference.
- To save these settings to the device, click **Next >**, the following window will appear:



- This page displays the progress of applying the configuration settings to the device. Once the configuration is sent, the following window will appear:



- The configuration process is completed, click **Finish** to close Digi Device Setup Wizard. You can use web interface to enter Digi Connect ME configuration. To access the web interface, check the **Log on the web user interface of device** checkbox and click Finish or enter IP address in your web browser.

Installation on Microsoft Windows 98 or Microsoft Windows Me

Follow these steps to install RealPort:

- Click **Start**, click **Settings**, and then click **Control Panel**
- Double-click **Add New Hardware** to start the Add New Hardware Wizard. Click **Next** and then click **Next** again.
Note: The Add New Hardware Wizard is searching for new devices.
- If you see the message **Is the device that you want to install listed below?**, click **No, the device isn't in the list** and click **Next**.
- Click **No, I want to select the hardware from a list** and click **Next**.
- In the Hardware types list, select **Other** devices and click **Next**.
- Click **Have Disk**.
- Type the path to the RealPort files and click **OK**, or click **Browse** and locate the files.



Note:

You can obtain the newest drivers and firmware from manufacturer's site www.digi.com

- In the Models list, select the device you are installing: Digi Connect ME, click **Next**, and then click **Finish**.
- Follow the prompts on the screen to finish installing RealPort.

11.2 Configure CPR in network

Main function of the CPR is to operate and coordinate work of autonomic devices, which are components of Roger Access Control System.

CPR work modes

Control panel (CPR) can work in two main work modes; in [ON] mode or [OFF] mode. In the [ON] mode CPR works normally and controls all operating functions, in the [OFF] mode it suspends working and discharges system communication bus. [OFF] mode is indicated on control panel's LEDs. Generally suspended mode is used for tests or conservation, eg. when the controllers flashing procedure is being carried out.

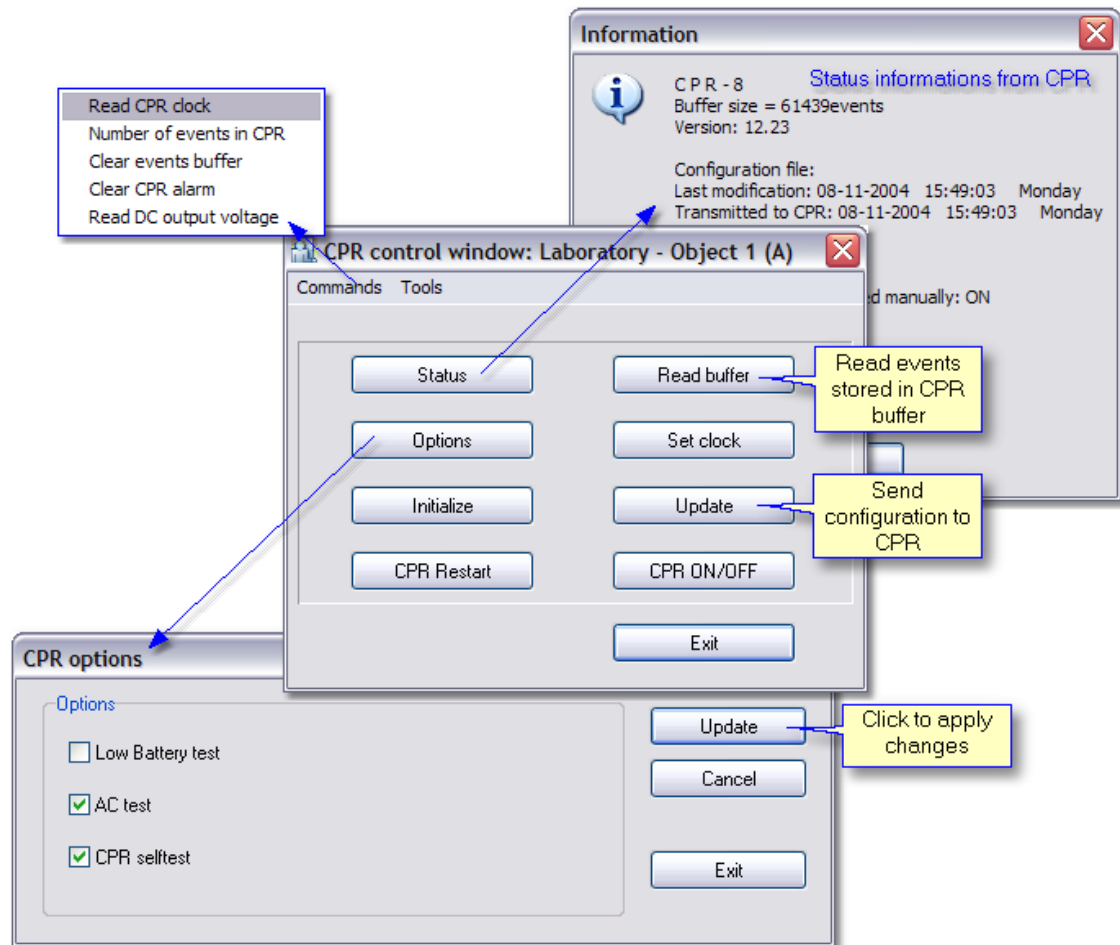
Available commands and functions:

- **Status** - information of control panel are showed (type, buffer size, config file name, last modification etc.)
- **Options** - enable/disable CPR tests
- **Initialize** - clear whole CPR memory, set clock and restart operation
- **CPR Restart** - cpr restart, used when CPR don't answer
- **Read buffer** - read events stored in CPR buffer
- **Set clock** - synchronize system clock according to the PC clock
- **Update** - send configuration to the CPR
- **CPR On/Off** - switch on/off mode



Note:

1. Initialize operation is usually carried out when CPR is completely deprogrammed or settings error occurred. Problems with CPR may happened in result of an AC lost or failure of battery, which sustain CPR memory. It's possible to initialize CPR manually.
2. In case control panel is in OFF mode for a long time, it's necessary to read events stored in controllers buffers. To do this send command from the controllers window [Check events buffer in controller](#)



Low battery test - Control panel periodically (in 10 minutes) tests battery charge level. In case as Voltage level decrease below to 12.0V alarm will occur.

AC (Accumulator) test - When CPR found that Accumulator voltage is missing [AC lost] event is indicated. Alarm decay when AC returns after 5 minutes.



Note:

Regarding work with PRxx1 controllers CPR performs also other functions - It supervises user access rights and collect events from controllers.

11.3 Send network configuration

To send configuration settings to whole subsystem (network):



- click on **Networks** from the operator tools or choose **Edit -> Networks** from main menu
- select appropriate network from the list
- click **Update**

Network must be active to send configuration. Performing this action causes configuration sending to control panel and all access controllers in selected network.

See also:
[Commands](#)

11.4 Update configuration of CPR

To perform [updating of CPR configuration](#):



- Click on **Networks** from the operator tools or **Edit -> Networks** from main menu
- Click on **CPR** button
- In CPR control window click **Update**

See also:
[Configure CPR in Network](#)

11.5 Controllers

General Description

Access Controller is an autonomic device, which controls single access point (one-way or two-way). In case two-way access point controller is connected with additional identification terminal. The controller is dedicated for use in Access Control and Time & Attendance systems. It may be configured to perform both function simultaneously or exclusively. Controller offers NO/NC Inputs, relay and transistor Outputs. [Inputs](#) and [Outputs](#) can be configured to several pre-defined functions. PRxx2 controller can register up to 4000 users, every user can be identified by Card, PIN or both method together (Card+PIN). Controller offers In Circuit Programming feature which enables firmware downloading into microprocessor memory. PRxx2 may operate with one or two external identification terminal(s) (PRT series terminal or Wiegand interface reader). Usually an remote identification terminal is used when door has to be controlled on both side or when controller has to be located in protected area (room) in order to avoid access of unauthorized person to controller's electronic circuit.

PRxx2 may activate door lock through internal relay output (REL1) or through relay output located on XM-2 remote I/O expander. Because an XM-2 module can be installed in remote, secure location the use of XM-2 expander increase overall controller's security level significantly. PRxx2 may operate in autonomic mode or in networked system equipped with CPR control panel or without it.

Due to complex and wide range of settings which can be defined in controller PRxx2 can not be programmed manually, it can be programmed from PC computer only. Programming from PC requires UT-2 communication interface.



Note:

1. In older types of controllers (PRxx1) maximal number of users is 1000. Once the configuration with number of users > 1000 will be send, users from ID=0 to ID=999 in will be programmed only.
2. PRxx2 controller can register up to 250 access groups, for older types of controllers (PRxx1) there are only 31.
3. In case absence of CPR or CPR in OFF mode, PRxx2 controllers are able to collect events automatically in non volatile 32 000 built-in buffers.

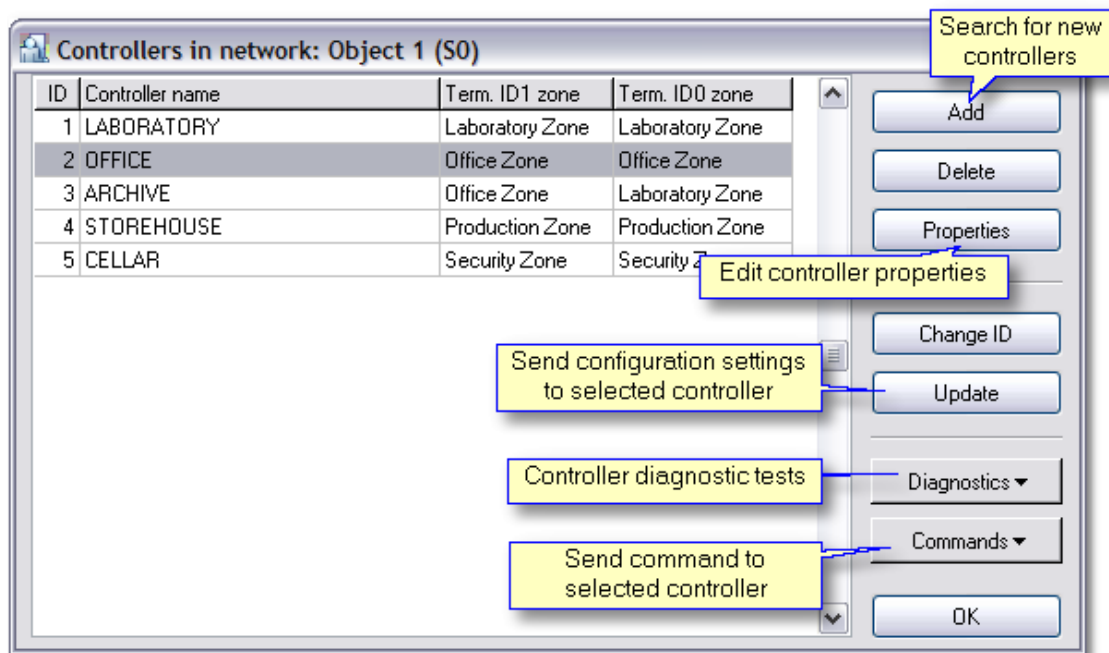
11.5.1 Add controllers

To add controllers connected to network:



- click on **Networks** from the operator tools or **Edit -> Networks** from main menu
- click **Controllers** button
- click **Add** button

After click on **Add** button program will start to search controllers connected to communication bus. Searching process ends with message "End of controllers searching", list of founded controllers will display:



Each of controllers has unique ID number (00..99). In case when program find device with the same ID, error message will appear! Therefore remember to set different IP numbers before adding new controllers.

Description of available options:

Add - search communication bus for new controllers

Delete - delete controller

Properties - enter controller properties

Change ID - select unique ID for controller

Update - send configuration settings to selected controller

Diagnostics - communication tests

Command - send command to selected controller

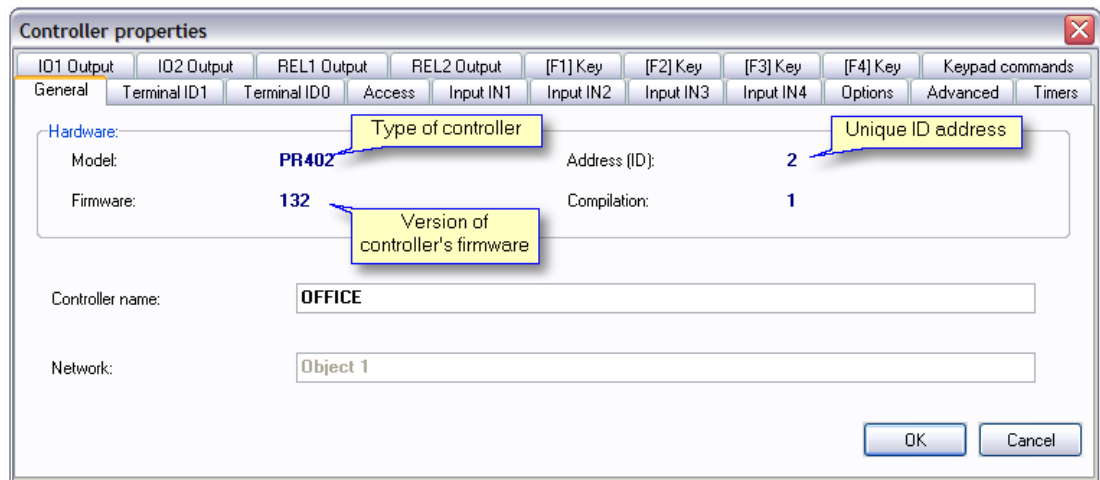
11.5.2 Controller properties

Controller properties consist of eighteen tabs:

- [General](#) - Hardware information, Controller Name, Network
- [Terminal ID1, ID0](#) - Location, Reader type, Access zone, Default T&A mode, [#] Key options, Identification mode, High Security
- [Access](#) - Door lock settings (REL1 output), Facility Code, Door Mode, Card+Card option
- [Inputs IN1, IN2, IN3, IN4](#) - input settings
- [IO1, IO2 Output](#) - output settings
- [REL1, REL2 Output](#) - output settings
- [Options](#) - T&A mode, External modules, Door Alarm options, Disable events
- [Advanced](#) - Anti-passback, Conditional Access, RTC test, List of Local SWITCHER users, Automatic arming, Quick disarm
- [Timers](#) - set flag timers
- [\[F1\] - \[F4\] Key](#) - Key settings
- [Keypad commands](#) - keypad commands settings

11.5.2.1 General

Here are information about: model, controller ID address, Firmware version and build, name of controller and network. Sometimes controller requires firmware upgrade e.g. when firmware version is not compatible with RACS version.

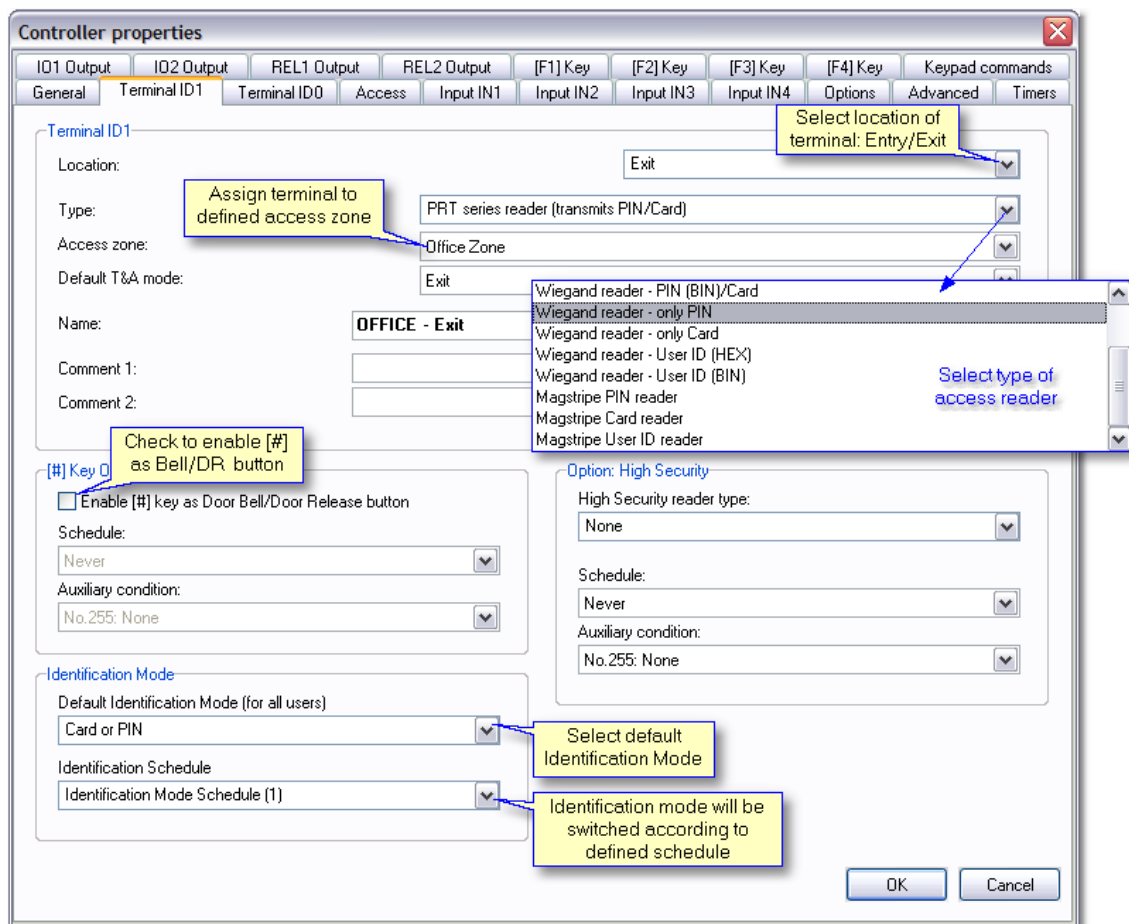


See also

[description of Firmware upgrade procedure](#)

11.5.2.2 Terminal ID1, ID0

In **Terminal ID1/ID0** tab you are able to give **Name** for terminal, specify **Default T&A mode** for Time&Attendance register etc.



Location - regarding **Max. number of users allowed to occupy the room** option location has significant meaning. Entry/Exit location refers also to **Conditional access** option of the controller. In this case first authorised person is obliged to identify on Entry reader. Location of the reader has no influence on T&A mode.

Type - select one of 12 available options. In case remote reader is not connected you should select **None** in ID0 tab. Thanks to this function can also disable built-in reader (integrated with controller).

- PRT series reader (transmits PIN/Card)
- PRT series reader (transmits user ID)
- Wiegand reader - PIN (HEX) / Card
- Wiegand reader - PIN (BIN) / Card
- Wiegand reader - PIN only
- Wiegand reader - PIN only
- Wiegand reader - User ID (HEX)
- Wiegand reader - User ID (BIN)
- Magstripe PIN reader
- Magstripe Card reader
- Magstripe User ID reader
- None

Wiegand reader is connected to Clock and Data lines instead of standard PRT terminal(s). When controller is configured for operation with Wiegand User ID reader it interprets transmitted digits as ID number of user which has performed identification, when is set to Wiegand PIN reader controller interprets transmitted digits as PIN number, when is set to Wiegand Card reader controller interprets transmitted digits as Card number. The Wiegand User ID mode is generally dedicated for biometric type readers which does not transmits PINs nor Cards codes but deliver ID number of user which has made successful identification. When controller is configured to Wiegand type reader no other extensions modules (XM-2, XM-8 or PSAM1) nor standard PRT reader can be connected simultaneously to controller's Clock and Data lines. By default Wiegand reader connected to Clock and Data lines is treated by controller as an ENTRY terminal.

Access zone - select access zone for terminal. Terminal ID1 and ID0 can be assigned to different access zones.

Default T&A mode - select mode from list which includes all defined T&A modes in system. Feel free to select T&A mode. You don't have to define Exit T&A mode on Exit reader because location of reader has no influence on T&A mode. There are four predefined T&A modes: **Entrance**, **Exit**, **On-duty exit (ODE)** and **no T&A (Ignored for T&A)**. Additionally program enables to add custom T&A modes adapted to own needs (Tools -> [T&A modes](#)).

[#] Key options - when checked [#] key on controller's keypad act as a Door Bell or Door Release button according to defined time schedule. If **Always** schedule is chosen then [#] key function as Door Release (DR), if Never [#] works as Door Bell button. In case different time schedule is selected then in defined time periods [#] function as DR button, and in time between defined periods act as Bell button.

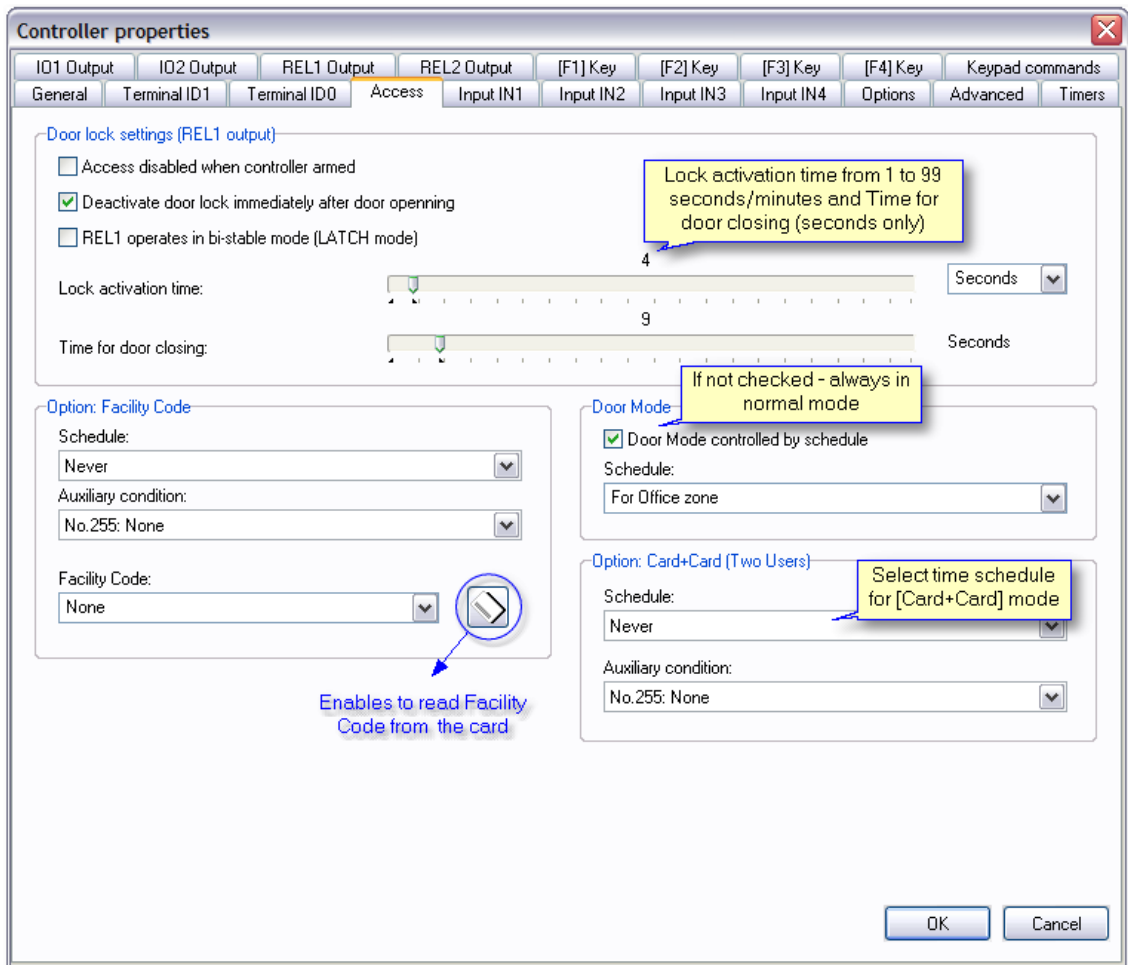
Identification mode - select **Default Identification Mode** of controller which specify normal identification method for each type of users (Master, Switcher and Normal)
Available options: Card or PIN, Card and PIN, Card only, PIN only. Additionally identification mode can be automatically switched between ident. modes due to defined schedule. You can define your own Identification mode schedule ([Identification Mode Schedule](#)).

High Security - When this mode is active users must perform two steps identification procedure, a standard identification (Card/PIN or Card+PIN depending on actual valid identification mode) plus an additional identification on High Security reader. The High Security reader can be connected to the same Clock & Data lines which are used for communication with ENTRY/EXIT access terminal and/or extension modules. Controller accept few types of High Security readers including Wiegand Card/PIN and Wiegand User ID. The Wiegand Card/PIN sends the code of entered PIN or Card, the Wiegand User ID sends ID number of user which has made identification. The High Security option can be activated separately for each side of the door and can be controlled by time schedule. Generally, the High Security option is dedicated for those doors which have to be protected with advanced identification method (e.g. biometric identification) .

See also:

[Glossary](#)
[T&A modes](#)

11.5.2.3 Access



Door lock settings (REL1 output) - door lock can be released:

- when authorised user enter identifier,
- by remote command from PC,
- by DR button which can be connected to controller input line or assigned to [#] button.


Door lock is activated for predefined period declared in **Lock activation time**. Lock activation time can be set from 1 to 99 seconds or minutes or for undefined period, in last case installer must select **Bistable mode** option. When it is selected each time door lock is triggered it moves to reverse condition (from on to off or inversely). When **Auto-relock** option is set, lock will be activated until door contact connected to controller input will indicate that door became open but not longer than predefined **Lock activation time**. Lock activation can be disabled when controller stay in **Armed** mode, this can be achieved by **Access disabled when controller armed** option. This feature is usually used when one of controller output line is dedicated to arm/disarm alarm zone or intruder sensor only. In this case switching controller to **Armed** mode will arm alarm system or alarm zone and automatically will disable access to premises for all users regardless of access settings.

Facility Code - In some installations all cards used is access system have a common part of card code, this part of card code is called Facility Code. The Facility Code consist of 8 data bits, those bits converted to decimal system may give the number from 0 to 255 range. If option is activated access is granted for those cards which belongs to the same "family" or another words have the same Facility Code. When Facility Code option is active controller verifies if the card presented

poses the common part of code which is declared as Facility Code and when yes the card is accepted without full card code verification. This option might be used in system with large number of users (e.g. student campuses) where access have to be granted for every card which have the same facility code. The Facility Option may have assigned time schedule and auxiliary control condition.

The Facility Code can be declared manually or can be retrieved automatically from card. To read Facility code:



- clicking on  button
- select controller or reader on which you want to read card code
- approach card to controller/reader

Door Mode - Door Mode determines how the controller will energize and de-energize door lock. As a default door lock stay in Normal Mode but it can be switch to another mode by [Door mode schedules](#) or by remote command. To enable switching due to time schedule check **Door Mode controlled by schedule** and select previously defined schedule from menu.

Door lock can be set to few listed below modes of operation:

- **Normal** - Door lock is activated after controller decide to grant access.
- **Unlocked** - Door lock is continuously energized, door can be opened by any unauthorized person.
- **Conditional Unlocked** - Initially door lock is not energized, but when first authorized person come and use its identifier lock became energized and remain in this state until new door mode is set.
- **Locked** - Activation of door lock is permanently forbidden, no matter if some user has authorization for access or not, every attempt to open the lock will be rejected.

Card + Card (Two users) - When this mode is active two authorized person must use his/her identifiers then controller will grant access to controlled door.

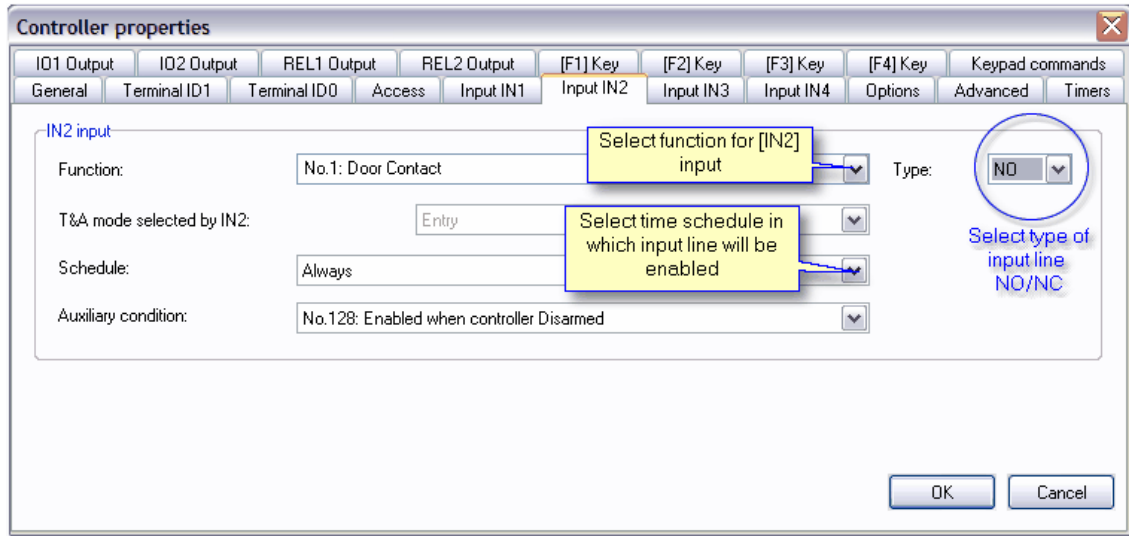
This mode can be controlled by [Card+Card] Schedule, selecting schedule Never will permanently disable this mode where schedule Always will permanently activate it. When together with this [Card+Card] option the [Card + PIN] mode is active both users must read his/her Cards and enter his/her PINs otherwise access will be denied.

See also:

[General purpose schedules](#)

11.5.2.4 Inputs IN1, IN2, IN3, IN4

Access controller has four [input lines](#). Each of controller inputs (IN1, IN2, IN3 and IN4) has the identical electrical structure. All inputs are NO/NC type with 5,6 k. resistor pulled up to supply plus. During setup process installer may configure each input independent as **NO or NC**. The NO type input is triggered when connecting it to supply minus. The NC input is normally shorted with supply minus, when disconnecting it from supply minus it became triggered. Controller ignore triggering impulses if they are shorter then 200 ms and accept signals that are longer then 500 ms. Detection of signals between 200 and 500 ms is not guaranteed. Each controller input can be programmed to different function and may be under control of time schedule. The following input functions are available:



The following input functions are available:

- **No.0: Input OFF (ignored)** - Selecting this function will disable decoding of this input, function can be used for temporary input deactivation without disconnecting it from triggering source.
- **No.1: Door Contact** - Input is dedicated for contact which will indicate that door is open. Input activation generate [Door opened] event, input deactivation generate [Door closed] event.
- **No.2: Exit Button** - Input is dedicated for operation with button which will be used to open the door without use of any identifier. Activation of this input will activate door lock for the same time period as after standard [Access granted] event, function is usually used for Request To Exit (REX) button connection. Activation/deactivation of input generate [Exit button ON]/[Exit button OFF event].
- **No.3: Arm/disarm Steady Switch** - Input is dedicated for operation with some button, switch or output line which will control actual [Arm/Disarm] mode of controller. Activation of this input force controller to [Disarmed] mode, as long as input is triggered controller will remain in [Disarmed] mode. Only one input on controller can be configured to this function. When such a function is selected any other methods of [Arm/Disarm] mode control will be forbidden.
- **No.5: AC Lost Input** - Input is dedicated to be connected to output line or contact which will indicate that AC supply of power supply unit is lost. Some brands of power supply are equipped with such a output line (e.g. PS20N from Roger). After input line is triggered controller generate [AC lost alarm ON] event, when line returns to normal condition controller generates [AC lost alarm OFF] event.
- **No.6: Low Battery Input** - Input is dedicated to be connected to output line or contact which will indicate that reserve battery is in low condition. Some brands of modern power supply are equipped with such a output line (e.g. PS20N from Roger). After input line is triggered controller generate [Low battery alarm input ON] event, when line returns to normal condition controller generates [Low battery alarm input OFF] event.
- **No.7: Bell Button Input** - Input is dedicated to be connected to button which will indicate that somebody want to enter premises. After input is triggered controller generate [BELL button ON] event and optionally may activate output line if configured as [BELL Output],

when line returns to normal condition controller generates [BELL button OFF] event and clears [BELL Output] line.

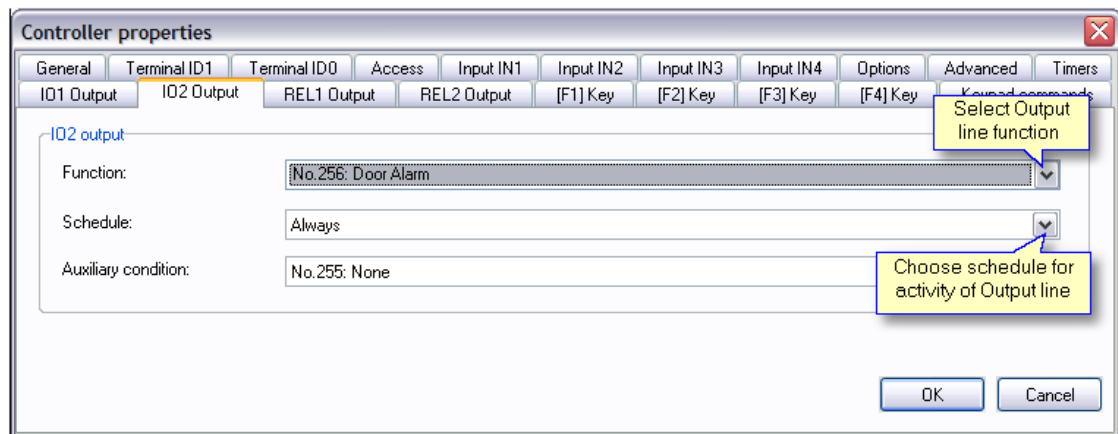
- **No.8: Tamper Loop Input** - Input is dedicated to be connected to tamper contact which will indicate that unauthorized person try to open controller/terminal case. After input is triggered controller generates [Tamper loop ON] event, when line returns to normal condition controller generates [Tamper loop OFF] event.
- **No.9: Intruder Detector Input** - Input is dedicated to be connected to some kind of intruder detector (e.g. PIR) which will indicate intruder's attendance in premises. After input is triggered controller generates [Intruder detector ON] event, when line returns to normal condition controller generates [Intruder detector OFF] event. The intruder detector input line can be bypassed in [ON] mode, this can be achieved selecting [Disable Intruder detector when controller in ON mode] option.
- **No.11: Access Disabled Input** - Input is dedicated to be connected to switch (or output) which when activated will disable access to controlled door, activation/deactivation of this input generate [Access disabled input ON]/ [Access disabled input OFF] event.
- **No.56: Selects Predefined T&A Mode – (steady change)** - Type Selection Input is dedicated to be connected to button which when pressed will turn controller to specified T&A Mode. The T&A Mode which will be set after input is triggered is declared by installer for every input line individually. The new T&A Mode is set for undefined time (until next command which will change T&A Mode of controller).
- **No.57: Selects Predefined T&A Mode – (mmomentary change)** - Type Selection Input is dedicated to be connected to button which when pressed will turn controller to specified T&A Mode. The T&A mode which will be set after input is triggered is declared by installer for each input line individually. The new T&A Mode is active till nearest user identification, if during next 8 seconds no identification was performed controller return to previously selected T&A Mode.
- **No.60: Reset APB register** - Input is dedicated to be connected to button which when pressed will reset APB Register of controller. Any time input is activated an internal APB Register of controller is initialized (cleared) and [APB Reset] event is generated.
- **No.62: Set XM-8 outputs OFF** - Input is dedicated to be connected to output line (contact) which when triggered will clear all outputs on XM-8 elevator control module(s).
- **No.63: Sets XM-8 outputs ON** - Input is dedicated to be connected to output line (contact) which when triggered will set all outputs on XM-8 elevator control module(s).

Besides those listed above functions input lines can be configured to customer defined input functions. Using PC software installer may define new input line functions, definition of input line function consist from function name and function code. Function name can be used to distinguish purpose of input e.g. [Guard Tour Button], [Alarm Button], [Assistance Request Button], each time input is activated system will register events which consist from function name and ON or OFF status which specify if the input line was activated or deactivated. The activity of each input can be controller by time schedule.

11.5.2.5 IO1, IO2 Output

IO1 and IO2 output lines

Both lines are open drain N-MOS transistor outputs. Each output can sink up to 1A DC current for unlimited time. In normal (not triggered) condition both outputs remain in high impedance state, when triggered they move to low resistance state which results that supply minus is observed on output. Both inputs are electronically protected from excessive currents and over-voltage. Each transistor output can be programmed to different function and can be controlled by individual time schedule.



Each output line may be configured to one of functions listed below:

- **No.0: Disarmed Mode** - output is activated when controller turns to [DISARMED] mode and remain active as long as controller remain in this mode.
- **No.256: Door Alarm** - middle double pulse every 2 seconds after door remains open in a period of time defined by "Time for door closing".
- **No.8: PC Command controlled** - output is activated/deactivated through interactive command from PC
- **No.9: Access Granted** - output is activated after controller grant access and remains in active state until door contact indicate that door became closed or lock activation time period has elapsed.
- **No.10: Door Open** - output is activated after controller detects that door became open and remains active as long as door is being open.
- **No.11: Access Denied** - output is activated for period about 2 seconds after controller denies access.
- **No.12: Schedule Controlled** - output is activated/deactivated according to selected schedule, no other method may change condition of output line.
- **No.13: Schedule or PC Command Controlled** - output is activated/deactivated according to selected schedule or interactive command from PC, both control methods have the same priority.
- **No.14: Entry/Exit Status** - Each time a successful identification is made on terminal ID0 output go to active condition and remains in this state till successful identification on terminal ID1 is performed. Usually this option is used when controller operates with TRIPOD type gate where lock must be set for clockwise or anticlockwise rotation depending on which terminals identification has been carried out.
- **No.15: Door Bell** - output dedicated to connect external door bell
- **No.16: Room Occupied** - output is activated when somebody occupy room, deactivated when nobody in room
- **No.17: Limit of Users Reached** - output is activated when defined maximal number of users allowed to occupy room is reached
- **No.18: Normal Door Mode** - output is activated when controller remains in Normal Door

Mode

- **No.19: Unlocked Door Mode** - output is activated when controller remains in Unlocked Door Mode
- **No.20: Conditional Unlocked Door Mode** - output is activated when controller remains in Conditional Unlocked Door Mode
- **No.21: Locked Door Mode** - output is activated when controller remains in Locked Door Mode
- **No.22: Postponed Auto-arming Delay in Progress** - output activated when delay of auto-arming command was sent to controller.
- **No.23: External buzzer** - output is activated/deactivated in parallel to internal buzzer of controller. Function may be used when connection of external buzzer is required eg. some type of Wiegand reader is connected.
- **No.24: Terminal Reset**
- **No.25: Pulse on disarming**
- **No.26: Pulse on arming**
- **No.27: Arm Request**
- **No.28: Forced Entry** - output Pulse/Pause 0.5/0.5 sec. after door opening without the use of controller.
- **No.29: Prealarm** - single pulse every 2 seconds after three consecutive attempts of entering an unknown identifier repeated in a period shorter than 1 minute.
- **No.30: Door Ajar** -
- **No.31: Door Chime**
- **No.32: APB Violation** - output is activated for period about 2 seconds after Anti-passback violation event occur.
- **No.64: Light**
- **No.65: Tamper Alarm**
- **No.66: AUX1**
- **No.67: AUX2**
- **No.68: Intruder Alarm**
- **No.84: Card or PIN mode for terminal ID0** - output is activated when Card or PIN mode on terminal ID0 is set
- **No.85: Card only for terminal ID0** - output is activated when Card only mode on terminal ID0 is set
- **No.86: PIN only for terminal ID0** - output is activated when PIN only mode on terminal ID0 is set
- **No.87: Card and PIN mode for terminal ID0** - output is activated when Card or PIN mode on terminal ID0 is set
- **No.88: Card or PIN mode for terminal ID1** - output is activated when Card or PIN mode on terminal ID1 is set
- **No.89: Card only for terminal ID1** - output is activated when Card only mode on terminal ID1 is set
- **No.90: PIN only for terminal ID1** - output is activated when PIN only mode on terminal ID1 is set
- **No.91: Card and PIN mode for terminal ID1** - output is activated when Card or PIN mode on terminal ID1 is set

11.5.2.6 REL1, REL2 Output

Controller offer two transistor outputs (IO1 and IO2) and two relay outputs (REL1 and REL2). The REL1 relay output is dedicated to control door lock, the functions of REL2, IO1 and IO2 can be assigned during controller's setup.

Relay output (REL1)

The relay output is dedicated to control electric door lock, it offers normally open and normally

closed contacts rating for 1.5A/24V DC or AC.

Both pair of relay contact are protected with over-voltage elements (MOV) which reduce sparks during switching inductive loads such electronic locks and thus extends relay contacts life significantly.

A relay output can be set to momentary or Bi-stable mode. When output is setup for momentary mode it becomes activated for limited period (from 1 second to 255 minutes) and after it returns to its normal condition. When output is set to Bi-stable mode relay output changes its state to opposite each time the triggering occurs.

REL1 output

Function:

Relay output (REL2)

This relay output can be assigned to different function, it offers normally open and normally closed contacts rating for 1.5A/24V DC or AC.

Both pair of relay contact are protected with over-voltage elements (MOV) which reduce sparks during switching inductive loads such electronic locks and thus extends relay contacts life significantly.

REL2 output

Function:

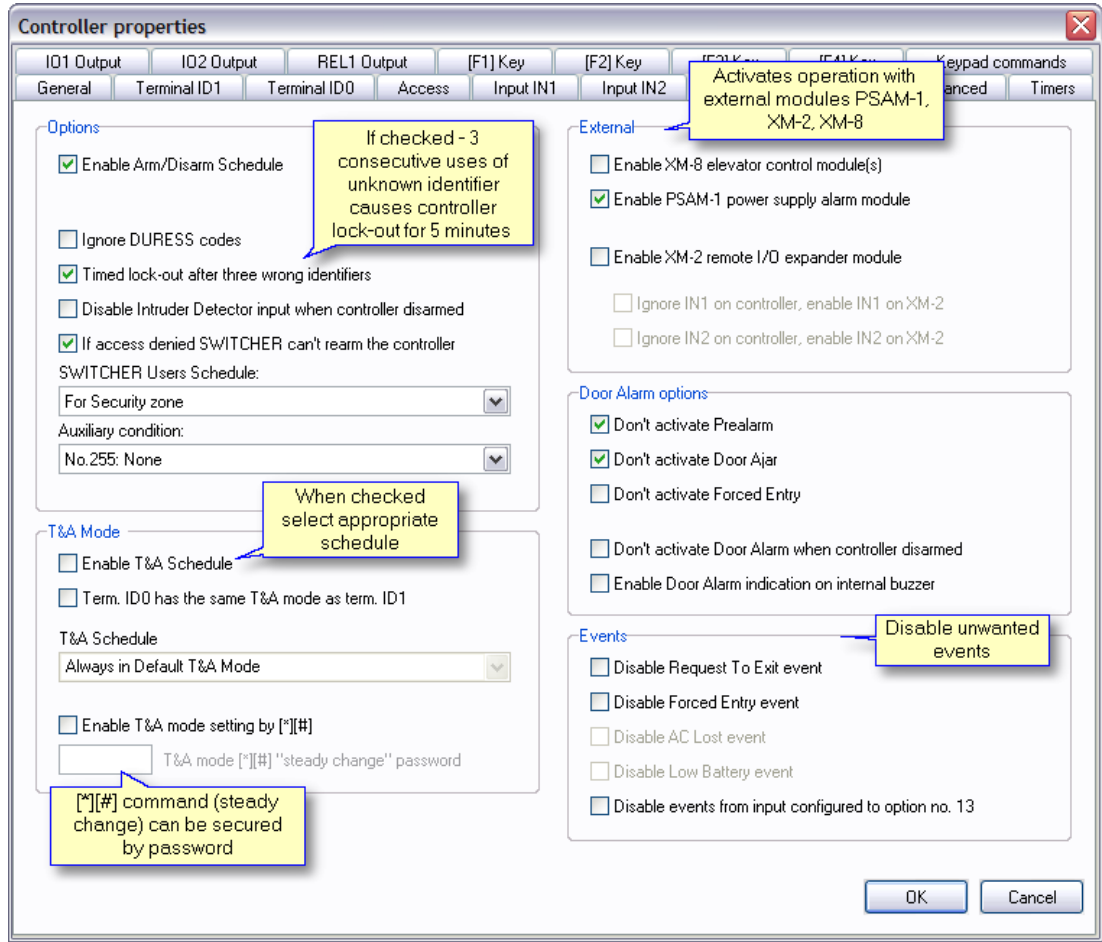
Schedule:

Auxiliary condition:

11.5.2.7 Options

Description of available options:

- **Enable Arm/Disarm Schedule** - when checked Arm/Disarm mode will be automatically switched according to time schedule. To define schedule open **Edit** -> **Arm/Disarm Schedule**
- **Ignore DURESS Codes** - if enabled controller will not generate alarm when DURESS code entered.
- **Timed lock-out after three wrong identifiers** - three consecutive attempts of entering an unknown identifier will cause controller lock-out for about 3 minutes. In this time any identifications on controller or terminal are not possible.
- **Disable Intruder detector input when controller disarmed** - the input is inactive when controller in disarmed mode
- **If access denied SWITCHER can't rearm the controller** - arm/disarm mode switching is available only when access is granted.



DURESS CODES - Duress entry - If the user enters his/her PIN code, which differs from its original form by "one" (plus or minus), controller interprets it as a duress code entry. When Duress entry occurs the [DURESS] event is generated and FORCED ENTRY alarm will occur.

Example:

The original code is [4569], entering [4568][#] or [4560][#] is treated as a duress entry.

Note: For proper recognition of duress entry, the PIN codes of individual users should differ one from each other at least by a value of +/- [2] on the last significant digit.

The Duress signalisation can be deactivated by PR Master software.

Terminals ID=0 and ID=1 have the same T&A Mode - If option is active events registered on terminal ID=0 have the same T&A status as events registered on terminal ID=1 (no matter if event was registered on terminal ID=1 or ID=0 they have assigned the same T&A status which is actually assigned for terminal ID=1). Generally, this option is dedicated to situation when controller is integrated into system which utilize another card standard (e.g. HID, Mifare), in such a configuration T&A Mode might be changed on controller (using keypad, input line or time schedule) but identification will be performed on remote Wiegand interface reader connected to Clock and Data lines.

External modules

- **XM-8 module**

Controller PRxx2 series may operate with one or two remote **XM-8 I/O modules** connected via Clock and Data lines. PRxx2 enable operation with XM-8 as elevator control interface. The first XM-8 module (address ID=8) is

dedicated to control access to floor 1-8, the second one (address ID=9) controls access to floors 9-16. Each time a successful identification is made controller determine to which floors has access particular user then activate some of XM-8's relays, relays remain active until input line assigned to option ***Clears all outputs on XM-8 elevator control module(s)*** is triggered or until next identification is accomplished and new set of outputs is activated. The operation with XM-8 module(s) is activated through option: ***Enable XM-8 elevator control module(s)***. All outputs of XM-8 can be alternatively activated by input line programmed to option: ***Sets all outputs on XM-8 elevator control module(s)***.

- **XM-2 module**

Controller may operate with one external **XM-2 I/O** module (address=5) connected to controller via Clock and Data lines. The XM-2 offers

two relay outputs (REL1 and REL2) and two NO/NC inputs (IN1 and IN2). The REL1 output on XM-2 is activated/deactivated simultaneously with REL1 output of controller, the second XM-2's output (REL2) is activated/deactivated simultaneously with controller's IO2 output. The XM-2's inputs are normally ignored but when allowed during controller's setup they can be used instead of IN1/IN2 inputs located on controller board. Installer may select which input(s) (local or remote) should be interpreted by controller. Generally XM-2 module is dedicated for PR302/PR302LCD controllers which normally activate door lock through internal relay, this relay can be easy accessed by non authorized person. When XM-2 is used, door lock may be activated not by internal controller's relay but by remote relay output located in secure location, this increase overall controller's security level significantly. The operation with XM-2 module is activated through option:

Enable XM-2 remote I/O expander module. The are two additional XM-2 options:

- ***Ignore IN1 on controller, enable IN1 on XM-2*** – controller will use remote (on XM-2) IN1 input instead of local (on controller) IN1, remote IN1 input will have the same function as assigned previously for local IN1 input, the electrical signals on controller's IN1 line will be ignored.
- ***Ignore IN2 on controller, enable IN2 on XM-2*** – controller will use remote (on XM-2) IN2 input instead of local (on controller) IN2, remote IN2 input will have the same function as assigned previously for local IN2 input, the electrical signals on controller's IN2 line will be ignored.

- **PSAM-1 module**

Controller may operate with one PSAM-1 power supply alarm module (address ID=4) connected to controller through Clock and Data lines.

The PSAM-1 is an optional part of power supplies offered by Roger, it delivers following data:

- actual DC output level
- low battery alert
- battery failure alert



Note:

PSAM-1 may operate in autonomic or networked mode, when connected to controller's Clock and Data lines it should be configured to networked mode with address ID=4.

The operation with PSAM-1 module is activated through option: ***Enable PSAM-1 power supply alarm module.***

11.5.2.8 Advanced

Anti-passback (APB)

When controller operates together with remote access terminal installer may activate anti-passback feature. When this feature is active, controller by default should be located on "exit" side and access terminal on "entry" side of door but this may be changed in **Terminal ID1, ID0** tab. During APB function activity users are obliged to use its identifiers on "entry" and "exit" side alternately.

There is two types of anti-passback:

- anti-passback hard, (APB Hard)
- anti-passback soft, (APB Soft)

APB Hard/APB soft mode can be switched according to defined time schedule. If the **Always** time schedule is selected then only APB hard will be activated, if **Never** - APB Soft. In case custom schedule is selected then in defined time periods APB hard will be active, beyond this periods APB will switch to Soft mode.

When anti-passback hard is set, the attempt to use the same identifier two consecutive times on the same entry or exit point will be rejected and **Anti-passback violation** event will occur, when anti-passback soft mode is set an attempt to use the same identifier on the same entry/exit point will be accepted but [Anti-passback violation] event will be generated. The activity of anti-passback can be reset (initialized) periodically according to [reset schedule](#) or manually (using dedicated input line, key or keypad command). Right after APB Reset each identifier can be used on entry or exit side, but after this first Card/PIN entry user must use its identifier alternatively on entry and exit point. Triggering input line, which is configured to Reset APB function, can do the manual reset of **APB** function.



Note:

Location: Entry/Exit of terminal in this case refer to anti-passback function and are not related to T&A modes.

List of LOCAL SWITCHER users

It's available to define list of **LOCAL SWITCHER** users (with ID numbers from 999 to 3999) on every particular controller. Users of this type are allowed to switch controller between Armed/Disarmed mode. SWITCHER Full and SWITCHER Limited users can not be a LOCAL SWITCHER, because functions which they perform concerns whole network.

To define Local SWITCHERS:

- click on the **Add/Remove Local SWITCHER**
- add them to the list using buttons: > and >>
- click **OK**

Option: Conditional Access

If Conditional Access option is activated then normally unauthorized users have access provided that somebody is already inside the room (it means that at least one user has status: Logged on Entry). Attendance of user in room authorize to enter. No matter who is inside, authorized person or user who has entered thanks to conditional access. To enable option select Always or defined time schedule. If Conditional Access will be realised on single access point then one of controller's input lines have to be configured as **No.60: Reset APB register**.

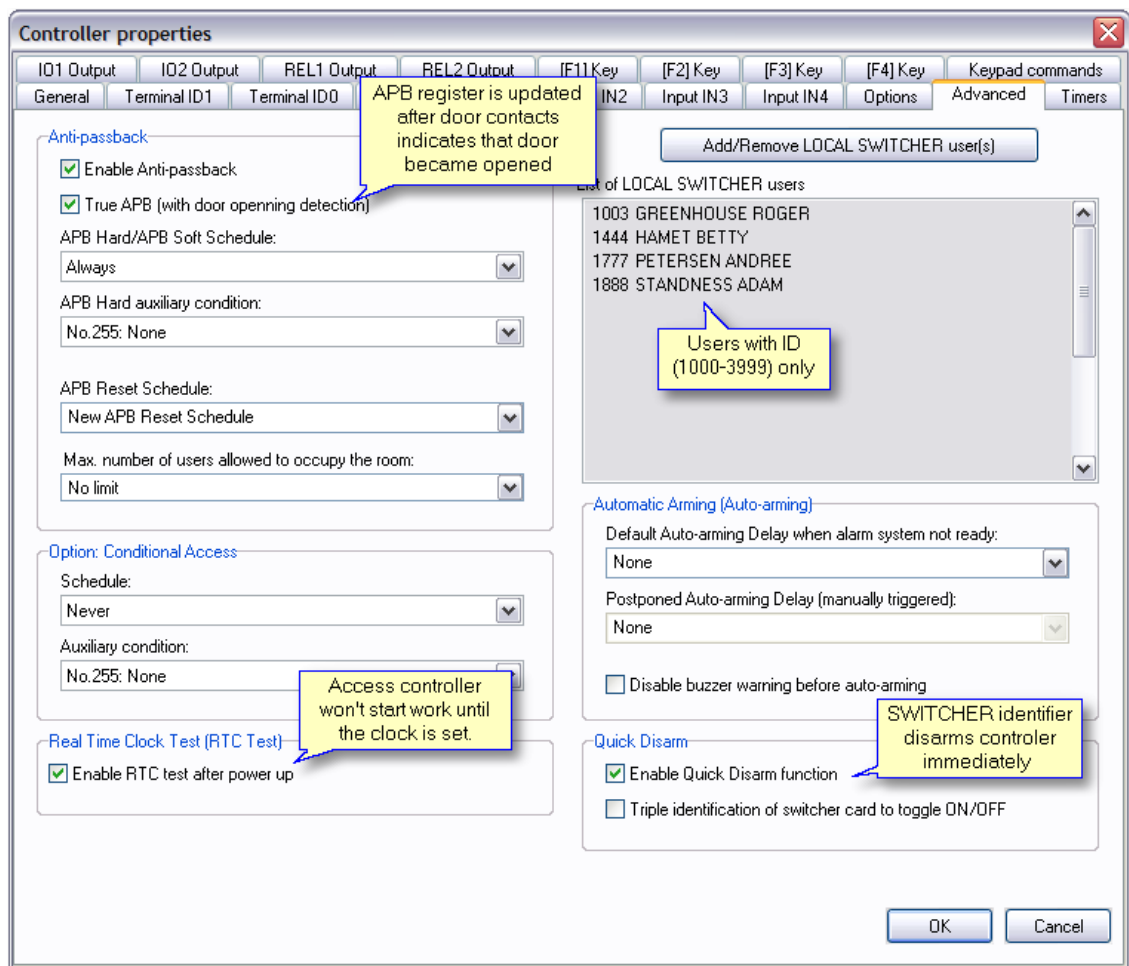
Real Time Clock Test

When controller is powered up, internal clock is not set. By default option **Enable RTC test after**

power up is enabled and controller won't start operation until internal clock is properly set. Clock can be updated automatically in case CPR Control Panel is connected to network or PR Master is running in Monitoring mode. It can be also carried out manually using command. If RTC test is disabled and controller's clock is not set device starts up with date: 01 January 2004. In this situation events are normally registered in buffer but event timestamps are incorrect. It's hardly recommend to update clock immediately.

Automatic Arming (Auto-arming)

Automatic arming option automatically switch controller to the ARMED mode according to defined time schedule. Feature allows to specify postponed Auto-arming Delay in case system is not ready (e.g. room not empty or door not closed), that is, state of appropriate output line indicate that system is not ready to arm. Postponed delay can be additionally triggered trough the input line or keypad command. 5 min before auto-arming controller generate acoustic signal, which informs about turning to Armed mode. It can be disabled by uncheck **Disable buzzer warning before auto-arming** option.



11.5.2.9 Timers

Timers option allows to define time period for activity of Flag. It's available to define time period from 1 sec. to 120 min. Flag can be permanently disabled when **Flag OFF** is selected. If Latch mode selected then Flag isn't set to ON for defined time period but until next switching.

Flag Timers

LIGHT Flag Timer	Latch mode
TAMPER Flag Timer	3 min.
AUX1 Flag Timer	Latch mode
AUX2 Flag Timer	Latch mode
INTRUDER Flag Timer	3 min.
Timeout of Break Alarm flag	3 min.
Timeout of Prealarm flag	3 min.
Timeout of Door Ajar alarm flag	3 min.

11.5.2.10 [F1] - [F4] Key

RACS enables to operate up to four **[F1] - [F4] keys**. Function activated according to defined time schedule can be assigned to each of them. Additionally auxiliary condition may control activity of keys. To disable key select **No.0: No function** from menu.

Controller properties

General Terminal ID1 Terminal ID0 Access Input IN1 **Input IN2** Input IN3 Input IN4 Options Advanced Timers

ID1 Output ID2 Output REL1 Output REL2 Output [F1] Key [F2] Key [F3] Key [F4] Key Keypad commands

Key [F1] on terminal ID0

Function: No.68: Set LIGHT flag on

T&A mode set by [F1] key on terminal ID0: Entry

Schedule: Always

Auxiliary condition: No.255: None

Key [F1] on terminal ID1

Function: No.255: Door Bell

T&A mode set by [F1] key on terminal ID1: Entry

Schedule: Always

Auxiliary condition: No.255: None

OK Cancel

Most of available functions to which [\[F1\] - \[F4\] keys](#) can be configured are the same like those in Input tab, so refer to [Inputs IN1, IN2, IN3, IN4](#) chapter to learn more about functions
Here are description of selected functions:

- **No.2:** Force Door Lock ON
- **No.4:** Key Pressed (event only)
- **No.58:** Set Postponed Auto-arming Delay ON
- **No.59:** Set Postponed Auto-arming Delay OFF
- **No.77:** Set INTRUDER+TAMPER flags OFF

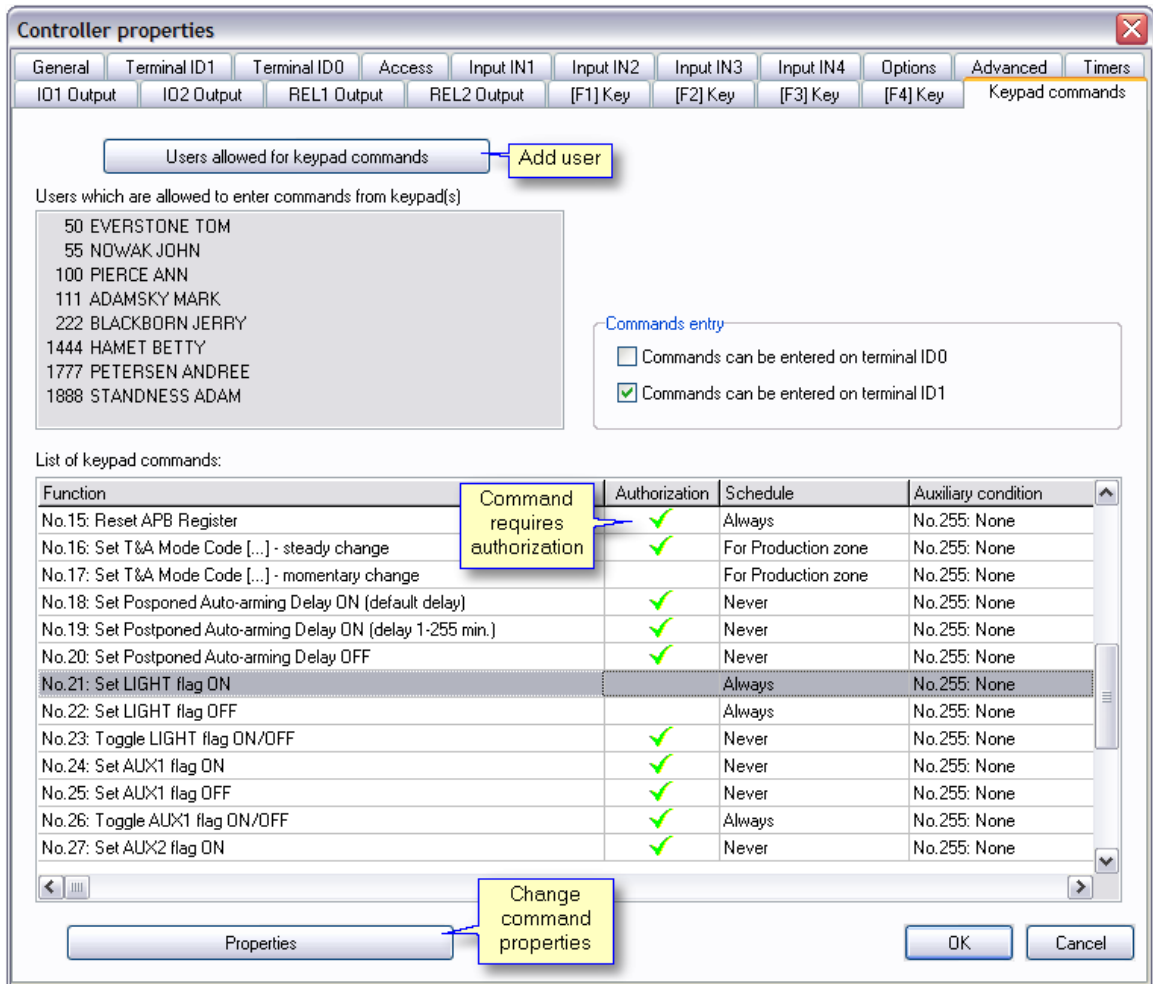
11.5.2.11 Keypad commands

RACS enables to enter [commands](#) directly on controller's keypad. It's available to select on which terminals commands will be accepted. Keypad commands may be allowed for previously defined list of users. Each of 33 available functions can be activated/deactivated according to selected time schedule, some of them may require user authorization. Additionally condition for command may be enabled.

To define Keypad command:

- click on **Users allowed for keypad commands**
- add users to the list using buttons: > and >>
- click **OK** to apply

- select keypad function from the list
- click **Properties**
- check/uncheck **User identifier required**
- choose time **Schedule** from list
- optionally choose Condition
- click **OK**



Most of available functions to which Keypad commands can be configured are the same like those in Input tab, so refer to [Inputs IN1, IN2, IN3, IN4](#) chapter to learn more about functions. Here are list of available keypad commands:

- **No.00:** Set controller ID - [*] [00] [#] [ID]
- **No.01:** Set Date - [*] [01] [#] [DDMMYW] [#] - where: **DD** - day, **MM** - month, **Y** - last digit of Year, **W** - day of week, 0 - Sunday, 1 - Monday, etc.
- **No.02:** Set Clock - [*] [02] [#] [HHMM] [#] - where: **HH** - hour, **MM** - minute
- **No.03:** Set Card and PIN mode on terminal ID1
- **No.04:** Clear Card and PIN mode on terminal ID1
- **No.05:** Set Card and PIN mode on terminal ID0
- **No.06:** Clear Card and PIN mode on terminal ID0
- **No.07:** Set Normal Door Mode
- **No.08:** Set Locked Door Mode
- **No.09:** Set Unlocked Door Mode
- **No.10:** Set Cond. Unlocked Door Mode

- **No.11:** Set Disarmed Mode
- **No.12:** Set Armed Mode
- **No.13:** Toggle Armed/Disarmed Mode - switch between the modes
- **No.14:** Restart Controller
- **No.15:** Reset APB Register - clear APB registry

- **No.16:** Set T&A Mode Code [...] - steady change - [*] [16] [#] [NNN] [#] - where: NNN is a T&A code, e.g. **017** - On-duty Exit (see [T&A modes](#)). When entered controller will turn to specified T&A Mode. The new T&A Mode is set for undefined time (until next command which will change T&A Mode of controller).

- **No.17:** Set T&A Mode Code [...] - momentary change - [*] [17] [#] [NNN] [#] - where: NNN is a T&A code. When entered controller will turn to specified T&A Mode. The new T&A Mode is active till nearest user identification, if during next 8 seconds no identification was performed controller return to previously selected T&A Mode.

- **No.18:** Set Postponed Auto-arming Delay ON (default delay)
- **No.19:** Set Postponed Auto-arming Delay ON (delay 1-255 min.)
- **No.20:** Set Postponed Auto-arming Delay OFF
- **No.21:** Set LIGHT flag ON
- **No.22:** Set LIGHT flag OFF
- **No.23:** Toggle LIGHT flag ON/OFF
- **No.24:** Set AUX1 flag ON
- **No.25:** Set AUX1 flag OFF
- **No.26:** Toggle AUX1 flag ON/OFF
- **No.27:** Set AUX2 flag ON
- **No.28:** Set AUX2 flag OFF
- **No.29:** Toggle AUX2 flag ON/OFF
- **No.30:** Set INTRUDER flag ON
- **No.31:** Set INTRUDER+TAMPER flags OFF
- **No.32:** Set Identification mode for terminal ID1
- **No.33:** Set Identification mode for terminal ID0

11.5.3 Send configuration settings to controller

It is recommended to [send configuration](#) to the controller after making any changes in controller's settings. To carry out configuration settings update:

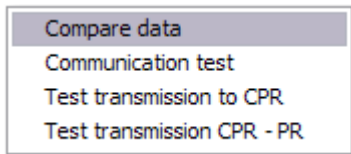
- Click on **Networks** button from operator tools or **Edit** -> **Networks** from main menu
- click **Update**

See also:

[Send network configuration](#)
[Commands to system](#)

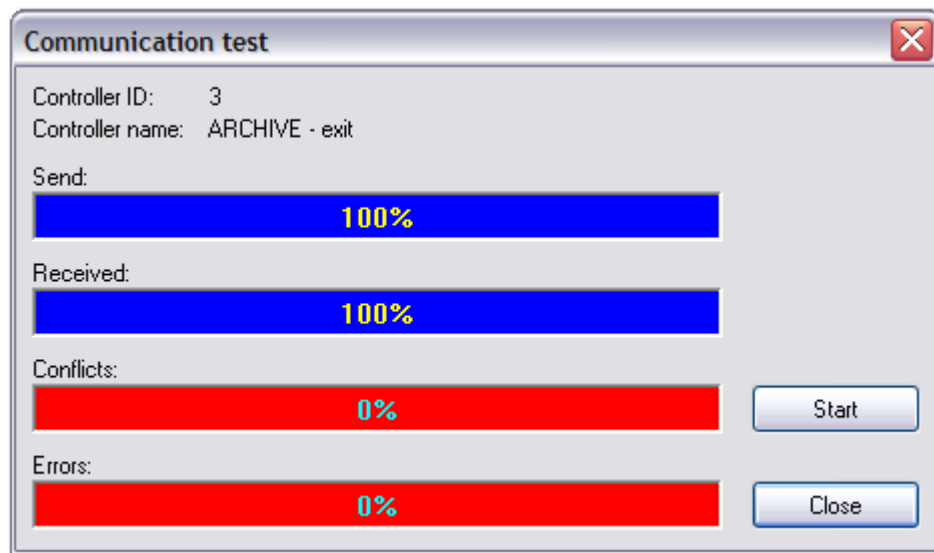
11.5.4 Diagnostics

Feature enables to perform diagnostics operations of controller. To send diagnostic command click on [[Diagnostics](#)] button in [Controllers](#). Menu box with options will appear:

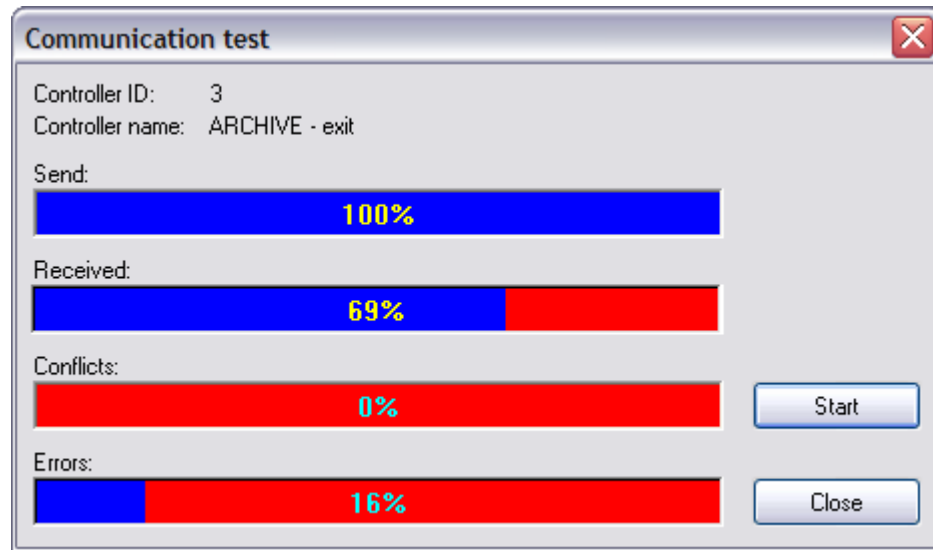


- **Compare data** - compares controller settings with configuration in program data base
- **Communication test** - test communication between PR Master and controller
- **Test transmission to CPR**
- **Test transmission CPR-PR**

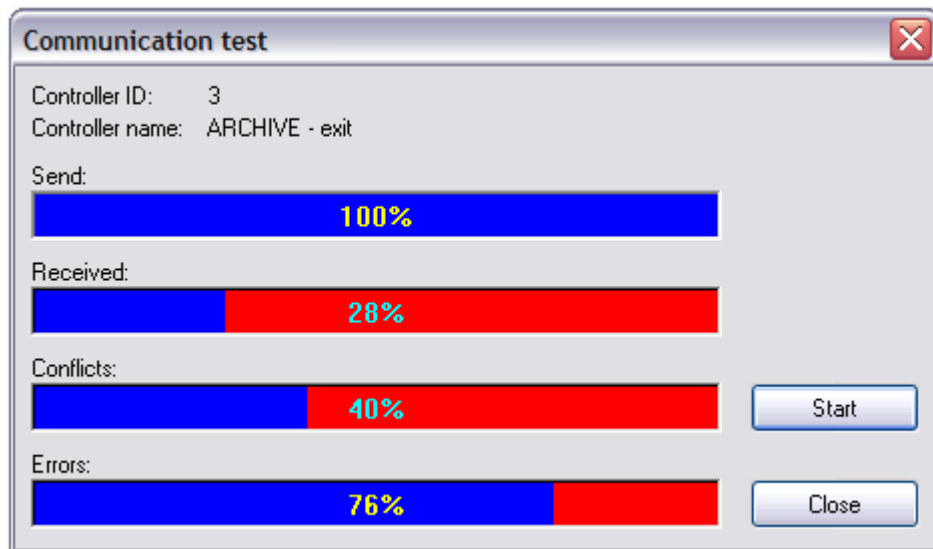
Results of Communication test:



results - very good, ideal communication, no conflicts nor errors



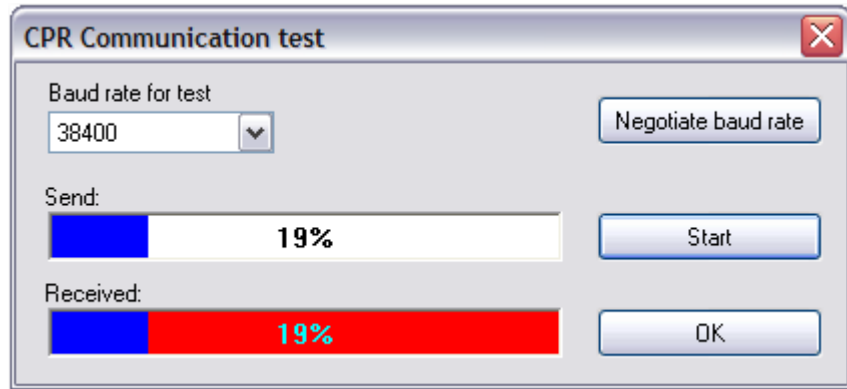
results - average, 60-80% answers may accept, however some conflicts and errors occurred



results - very bad, wrong communication, conflicts and many errors occurred. You should check controller connection to communication bus.

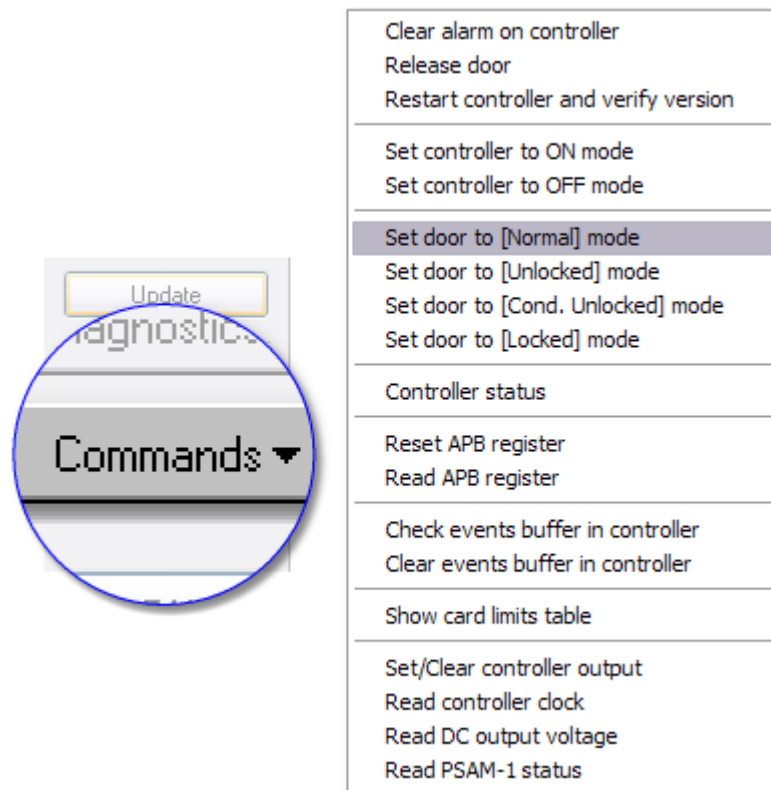
Transmission to CPR and **CPR-PR** are carried out in the similar method.

To execute transmission to CPR test you should first specify **Baud rate** for transmission. It's recommended to use **Negotiate** option, which offers appropriate baud rate.



11.5.5 Commands to controller

Once the controller is selected we can send a command to it. After click on [Commands] button menu with available commands (depend on controller type) will appear.

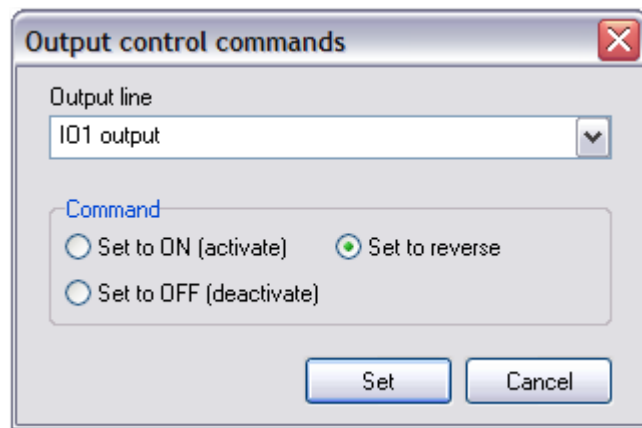


On the picture above we have commands for PR402 controller:

Commands:

- Clear alarm on controller - shut down controller alarm
- Release door
- Restart controller and verify version
- Set controller to [ON] mode
- Set controller to [OFF] mode

- Set door to [Normal] mode - door always locked, unlock after valid user authorization
- Set door to [Unlocked] - door always unlocked
- Set door to [Cond. Unlocked] mode - conditionally unlocked, door locked until first authorised access granted
- Set door to [Locked] - door always locked, no matter what access rights
- Controller status - shows controller information, terminal status, door and identification modes
- Reset APB register - causes reset of Anti-passback register
- Read APB register - display list of users who log on Exit terminal
- Check events buffer in controller - display number of buffered events
- Clear events buffer in controller
- Show card limits table - display status of limited users, add new limited identifiers
- Set/Clear controller output



- Read controller clock - shows current time in controllers chip
- Read DC output voltage - shows Direct Current output voltage
- Read PSAM-1 status

User ID	Name	Usage Limit
444	HAMET BETTY	3
1	SMITH BEN	4
333	EAGLEN AMANDA	5
555	MARCH DAISY	Exceed

11.5.6 Microprocessor Firmware upgrade

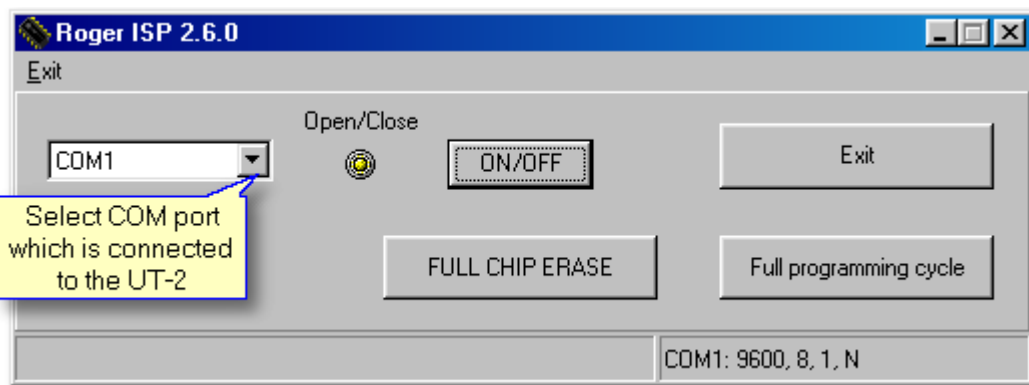
Upgrading control software of a device ([firmware downloading](#)) is an operation that sends new version of a control program to the memory of a microprocessor device. This operation is usually carried out when the device manufacturer releases a new, improved or enhanced version of firmware. When programming PRx2 or CPR32-SE new firmware is transmitted via a standard

communication lines (lines A and B of the RS485). The firmware downloading can be performed directly in the access system in which device runs without a necessity of removing it from installation place. It can be also de-installed and connected via the UT-2 interface to any other PC computer, in each cases the RogerISP program is required to transmit the new firmware to downloaded device.

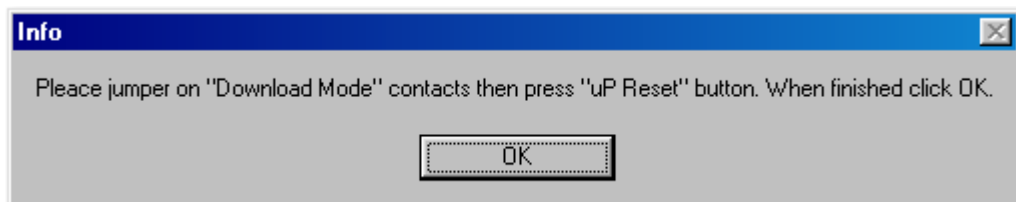
Downloading firmware

Below please find a description of successive steps of the downloading procedure assuming that the controller is an element of a functioning access control system and the new control software will be transmitted from the level of the same computer, which manages the access control system.

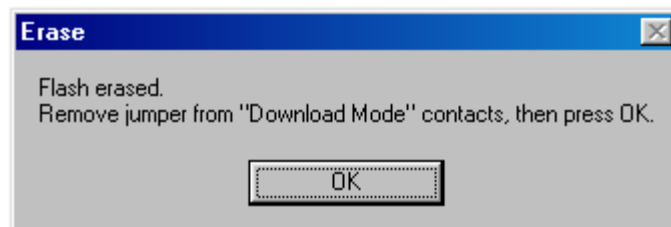
- Run the RogerISP program, select the appropriate communication port (the one to which the UT-2 interface is connected),



- Click on **Full Chip Erase**, the following communicate will appear:



- Place jumper on **FirmwareDownload Mode** contacts.
- Press **uP Reset** button.
- Click **OK**, after the chip memory erasing operation appropriate communicate will appear:

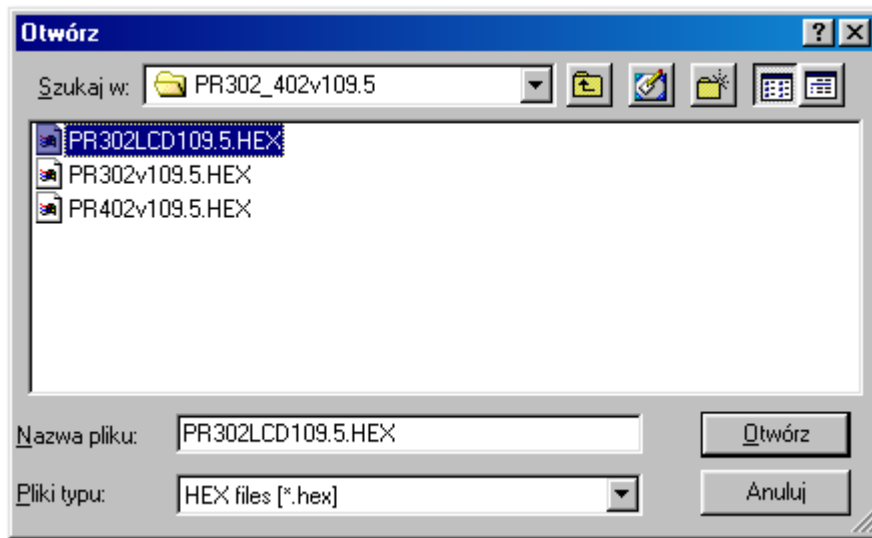


- should remove jumper from Firmware Download Mode contacts and observe a reaction of the controller. In case when "device is dead" it means that operation is successful and can continue with procedure. However when device resume it's work and respond (just like before erasing) you should repeat erasing operation

- Click on **Full programming cycle**, following message will appear:



- Place jumper on **Firmware Download Mode** contacts again.
- Press **uP Reset** button, then click **OK**.
- Program will ask you to select HEX type file with new firmware, when selected click on **Open**,



- The programming process will begin. On the bottom of the Roger ISP window progress of sending records will show.
- When transmission is finished the following message will appear:



- Remove jumper from **FirmwareDownload Mode** contacts and click on **OK**, if controller does not resume work, it means that programming operation is failed and you should repeat steps from erasing procedure. However if device resume it's work you can finish flashing process and exit RogerISP program.
- After new firmware transmitting should configure the device from PRMaster software.



Notes

1. Transmission of new software can be carried out to one or more controllers simultaneously. However, should remember to realize verifying steps for each device individually.
2. If successive attempts to flash the device directly in the access system are not successful (which may result from some disturbances which exists on communication bus), you should remove the device(s) and connect it directly to the programming computer.

12 Monitoring

Generally **Monitoring** is a working mode of PR Master in which events are automatically downloaded from buffers and displayed in Monitoring window. It means that all events (access granted, alarm, communication lost etc.) which occur on controllers are illustrated in real time in PR Master window. Program operator is able to observe situation in whole RACS system and additionally supervise devices. When PR Master remains in a Monitoring mode, all occurred events are immediately appended to the system database. Each type of events are distinguished with different icon and color. Alarm events are additionally indicated in Alarms window.

By default before execute Monitoring mode all events are downloaded from system buffers and are appended to the database. In some cases operator may want to review in monitoring window previously occurred events. To realise it: select **Tools** from main menu of PR Master -> **Options** -> **Misc** -> check option **Events downloaded from networks only upon operator's request (command)**.

Blinking belt and data missing means communication with network lost

Alarm states of CPR: Tamper, CPR OFF, Low Batt., AC, Buffer

18-05-2004 10:51:29 Tuesday

Events

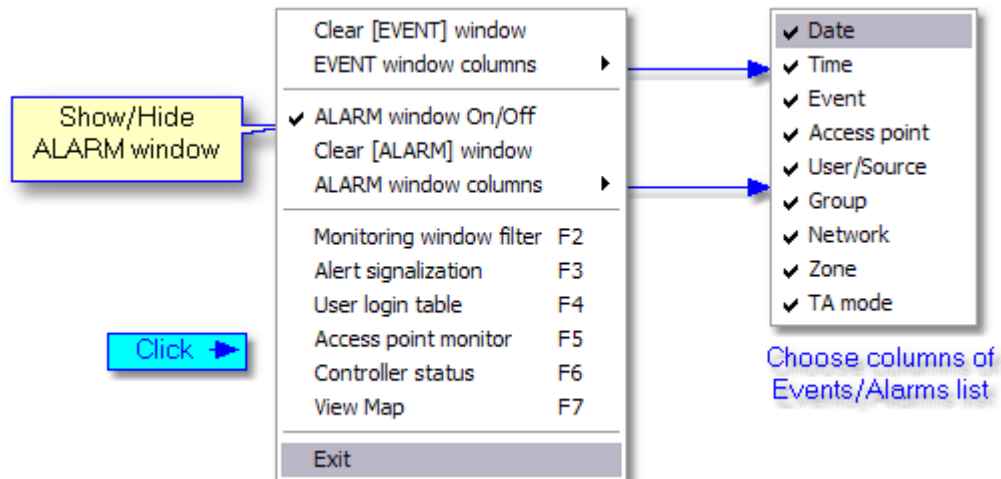
Date	Time	Event	Access point	User/Source	Group	Network	Zone	TIA mode
18-05-2004	10:47:50	Access denied	LABORATORY - exit	PETERSEN ANDREE				
18-05-2004	10:48:00	CPR: Communication with coSTOREHOUSE						
18-05-2004	10:48:00	Restart of the controller						
18-05-2004	10:48:00	[Card+Card] mode turned off						
18-05-2004	10:48:10	Access granted	STOREHOUSE	STANDNESS ADAM				
18-05-2004	10:48:10	Access granted	STOREHOUSE	GREENHOUSE ROGER				

Alarms

Date	Time	Event	Access point	User/Source	Group	Network	Zone
18-05-2004	10:47:50	Access denied	LABORATORY - exit				
18-05-2004	10:48:20	Forced entry	OFFICE - exit				
18-05-2004	10:48:50	Communication with Terminal ID=0 lost	ARCHIVE - exit				
18-05-2004	10:49:30	Access denied	STOREHOUSE				

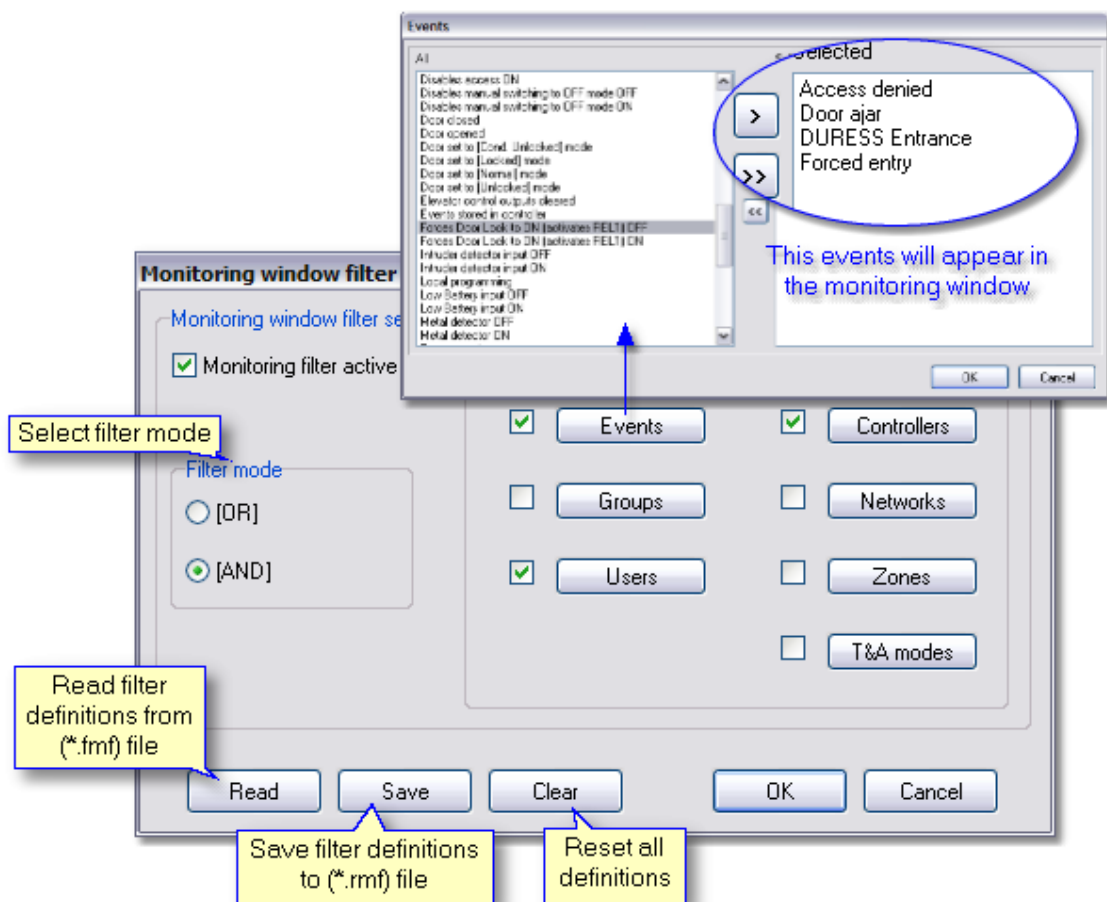
12.1 View

This menu allows to change **view** of Monitoring window and run additional options (keyboard shortcuts F2-F7). Monitoring window consists of two parts: "Events" and "Alarms". Here you can select columns, which will be displayed in the window.



12.1.1 Monitoring filter

Monitoring filter option allows to select only this events, which will be displayed in monitoring window. By selecting **AND/OR** filter mode it's possible to specify type of condition(s). **AND mode** - is used when all selected conditions must be realized, whereas **OR mode** - when one of selected condition must be realized.



Options description:

- **Read** - read filter definitions from external (*.rmf) file
- **Save** - save filter definitions to external (*.rmf) file
- **Clear** - reset all settings and disable filter

To define Monitoring window filter:

- check **Monitoring filter active**
- select **filter mode (type of condition)** by clicking radio button
- click on one of **Active subfilters**: Events, Groups, Users, Controllers etc.
- add elements to the list using buttons: > and >>
- click **OK**
- check box located next to the subfilter button to activate it.
- add another subfilter following four previously listed points



Example:

- select filter mode **AND/OR**
- specify **Active subfilters**
- click **Events** and select: Forced entry, Prealarm, DURESS Entrance and Door ajar
- click **Zones** and select: e.g. Zone X and Zone Y
- leave date checkbox unchecked

Description:

1. AND mode selected

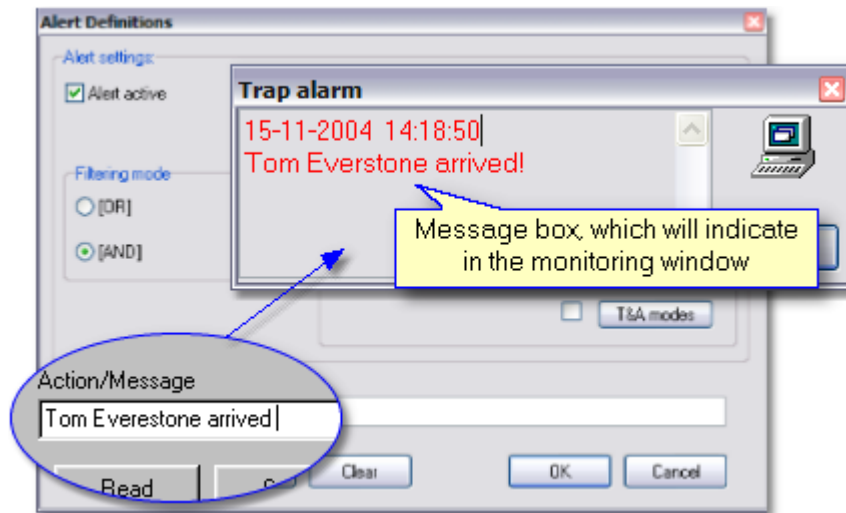
Monitoring window will display only this events which fulfill **AND** condition. It means that event will be shown in case at least one element from each of active subfilters will be met. If filter set like in the example Monitoring window will display e.g. Prealarm in Zone X or Door Ajar in Zone Y.

2. OR mode selected

Monitoring window will display only this events which fulfill **OR** condition. It means that event will be shown in case one of defined element in active subfilter is fulfilled. If filter set like in the example Monitoring window will display all Prealarms, DURESS Entries, Forced entries, Door ajar and all events in Zone X and Zone Y.

12.1.2 Events Alert

[Events Alert](#) feature enables to specify monitoring pop-up messages which inform about occurrence of defined events. To specify what kind of events should be alerted define filter (method of defining is the same like in [Monitoring filter](#)).



To define event alert:

- run **Monitoring** Mode
- select **Events Alert (F3)** from **View** menu
- check **Alert Active** option
- define **Filtering criteria**
- in **Alert Action** field type short message, which will inform about occurred event.

To define more detailed Alert message you can utilize following variables:

- %u - user
- %g - group
- %e - event
- %c - controller
- %s - subsystem
- %n - go to new line

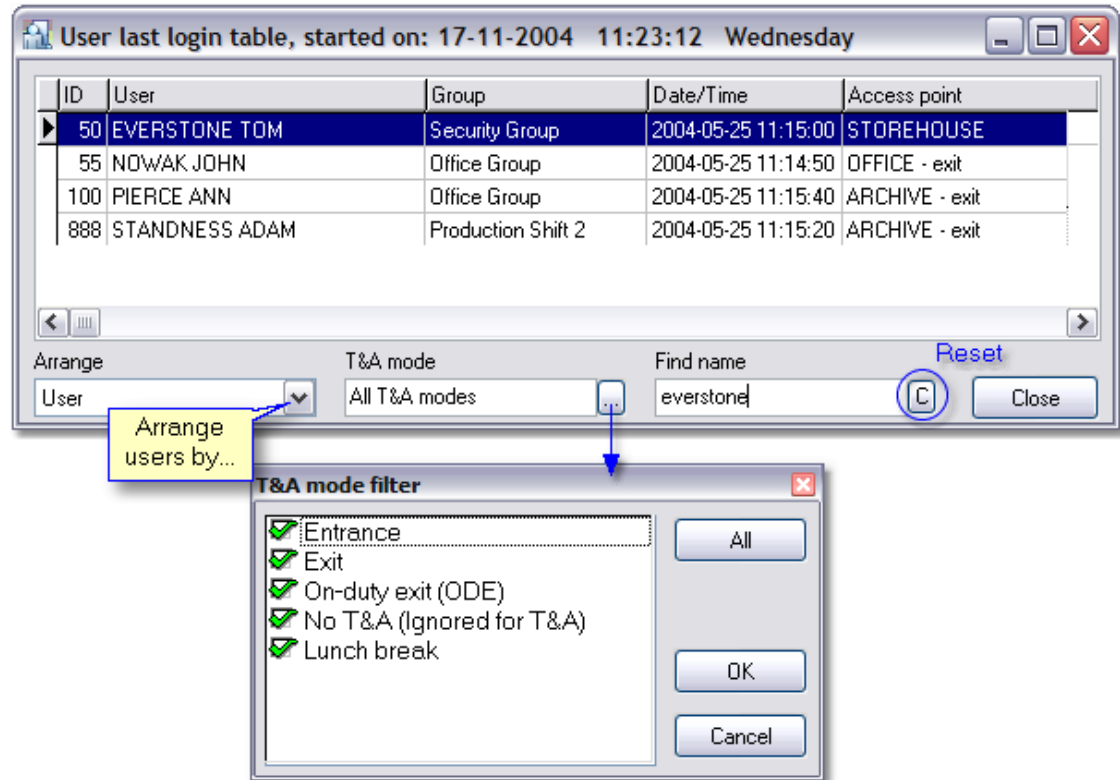


Note:

Use variables if you want to make messages more precisely. It's especially useful when many filter conditions are defined.

12.1.3 User login table

User login table shows, on which of controllers user was logged lastly. Feature is helpful especially when you need to find current user location and you don't want to browse long event list in monitoring window. It's possible to arrange logins list in defined order, and additionally enable T&A mode filter.

**Note:**

1. If the list of users is very long you can enter name of user in Find option.
2. To quick open User login table use F4 key in Monitoring mode.

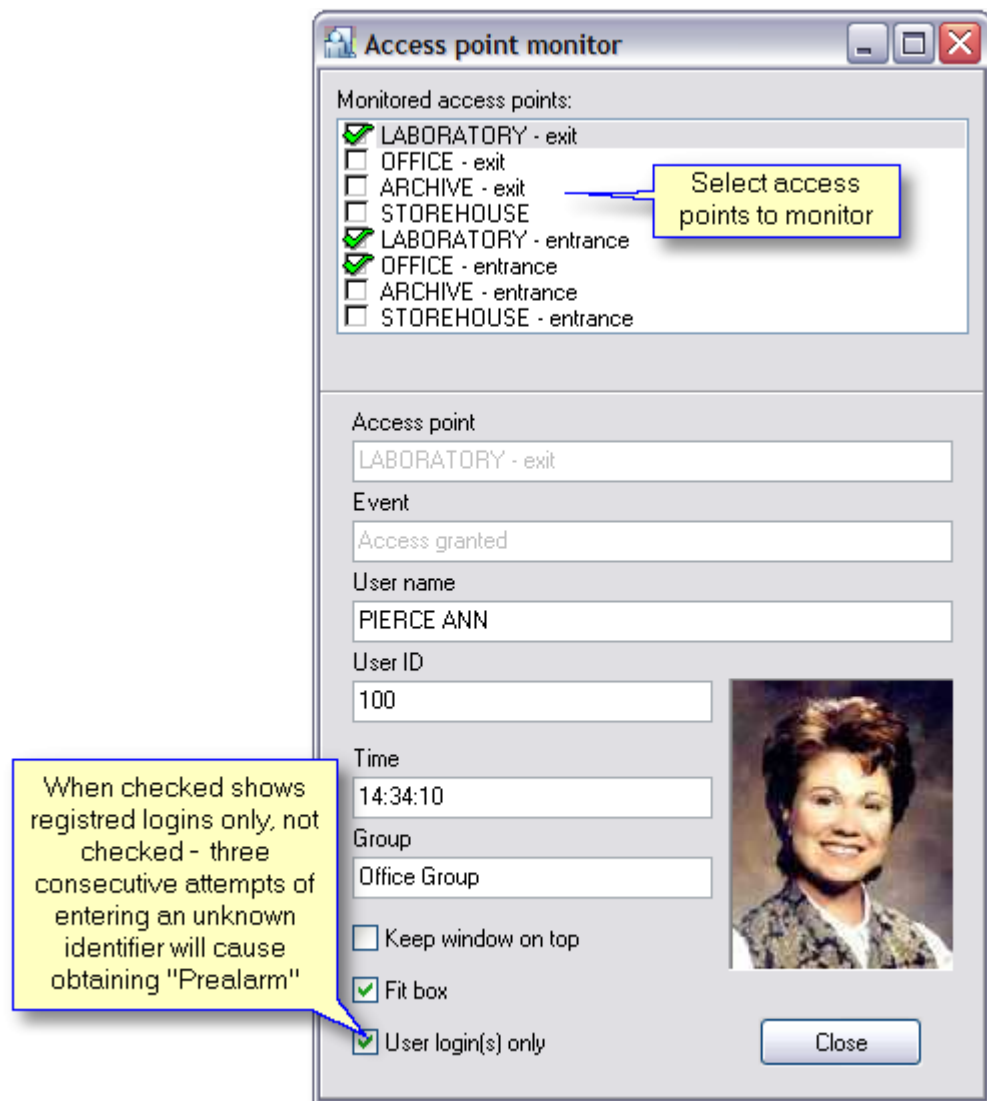
See also:

[Monitoring filter](#)
[Define trap](#)

12.1.4 Access point monitor

[Access point monitor](#) allows to observe movement of users on selected access points. When option is enabled user identification on selected access point(s) causes displaying information of system user (watch the screenshot below). Person who monitors access point(s) is able to compare user on the passage with photo which is displayed in the window. In case [**Only users login**] option is checked, information about registered users will be showed only, whereas unchecked, three consecutive attempts of entering an unknown identifier on one of controllers will cause obtaining "Prealarm" event.

1. The feature may be used in systems where some group of users has no access rights to enter and door are opened after verification carried out by other person. It means that other authorised person release door for user after he compare his/her face with assigned photo.
2. Feature can be also utilized in Access Systems where cameras are installed. It gives ability to monitor many remotely located access points. In this case images from cameras which are installed on the passages are displayed on the separated display(monitor) and can be compared with user's data.



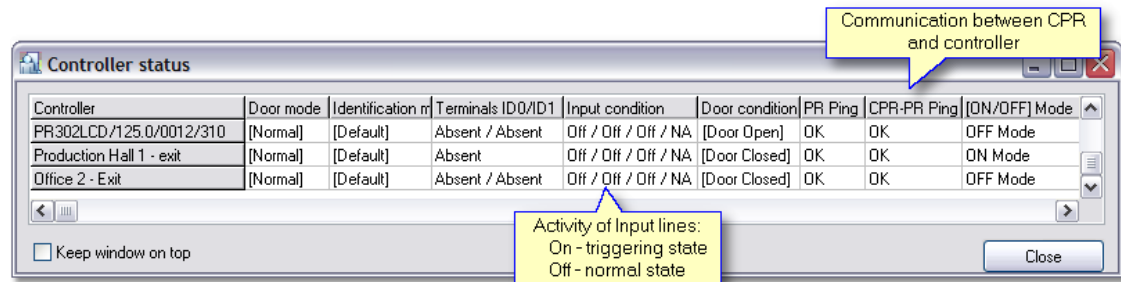
12.1.5 Controller status

Controller status feature enables to observe controller's states, such as Door mode, Identification mode, Input and Output lines states. From this level you are only able to monitor, sending commands or changing appearance are not allowed.



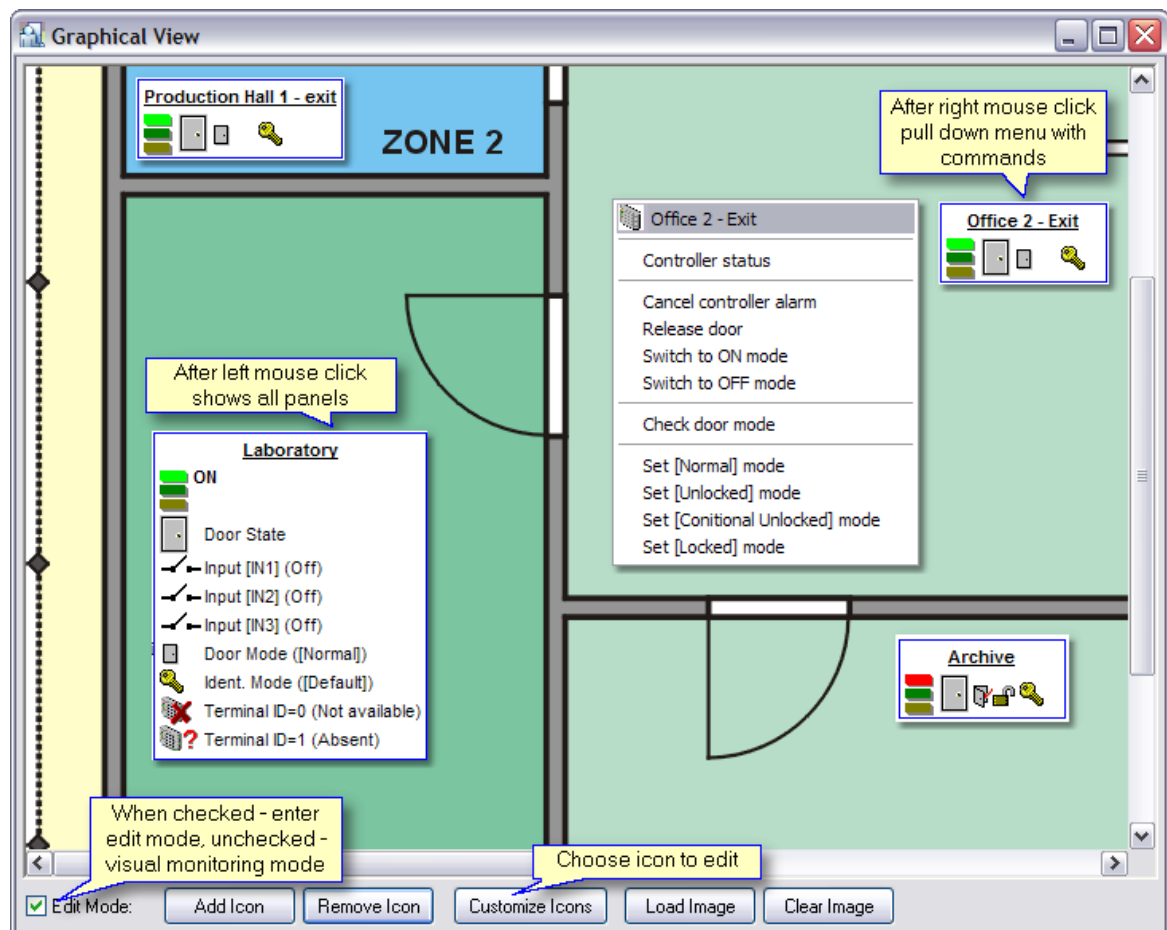
Note:

Data in the table is refreshed every 6 seconds. Occurrence of BD, means NO DATA.



12.1.6 View map (Graphical View)

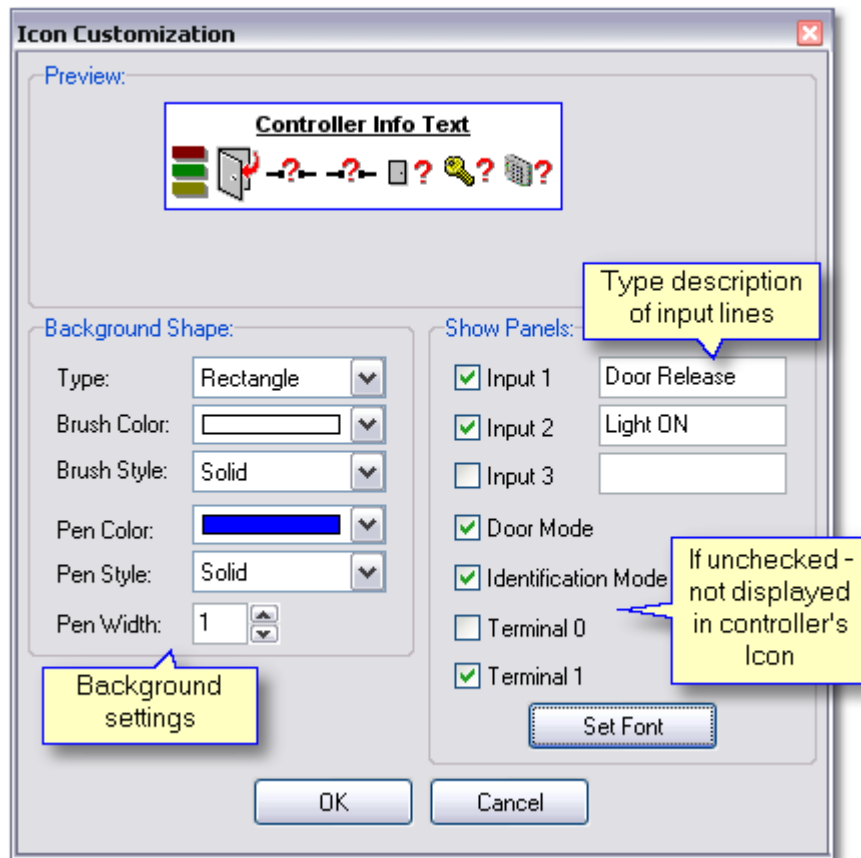
Graphical View feature enables to monitor status of selected controllers on the custom background image. Thanks to this option devices which are represented by icons may be positioned in specified places of loaded image (object scheme or building map). It helps to identify and for example immediately send command to a particular controller.



To carry out Graphical View configuration:

- check **Edit mode** box
- click **Add icon**
- in the next window select controllers which you want to monitor by checking boxes
- click **Add selected**
- click on **Load image** to set background

You may as well finish configuration and uncheck **Edit mode** to start monitor. But sometimes it's necessary to customize controller's icons. To carry out customization of icons you have to enter Edit mode. To edit Icons click on **Customize Icon** button, the following window will appear:



To run monitoring mode uncheck **Edit mode**.

- To view expanded mode of icon with all panels click left-mouse on it
- To send command to controller click right-mouse on icon and select command from menu

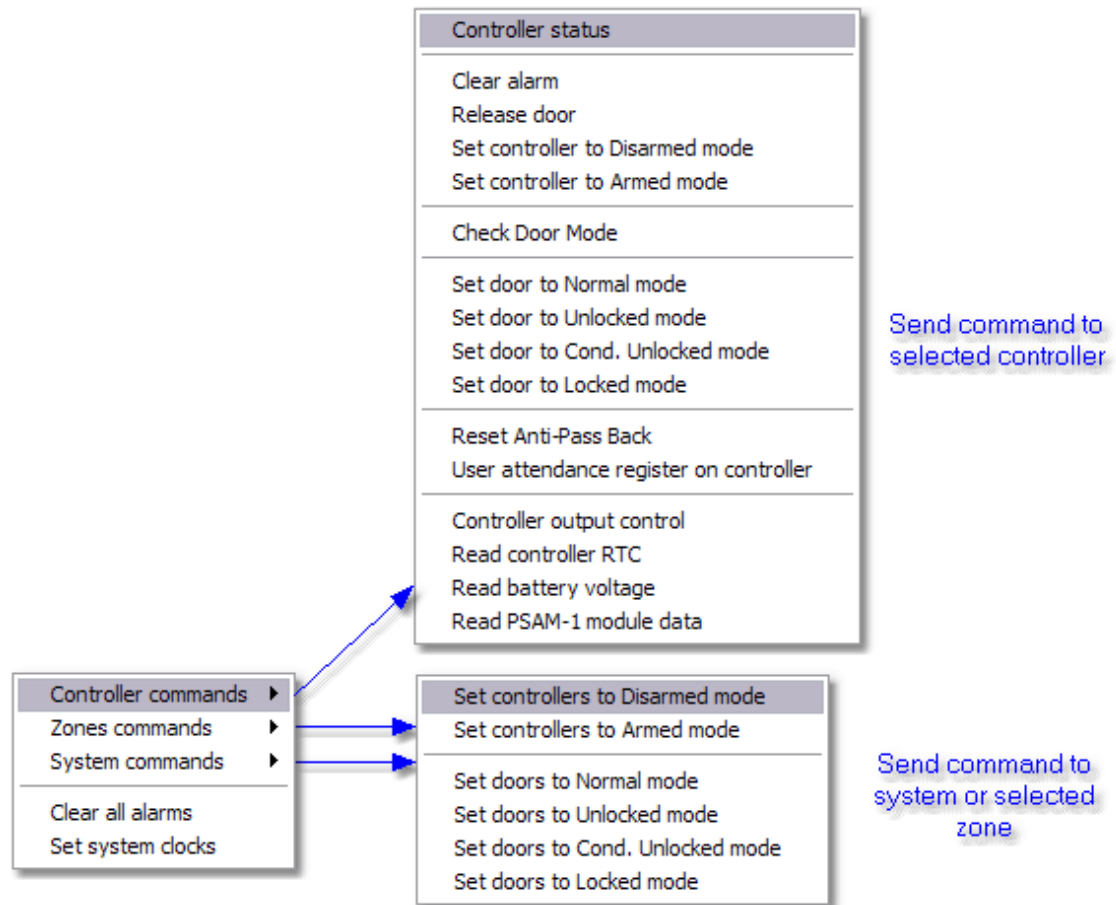
See also:

[Controller status](#)

12.2 Commands

To execute **command** in monitoring mode:

- select category: **Controller commands**, **Zones commands** or **System commands**
- select appropriate controller or zone in the next window (if command send to system click **OK** to confirm)
- click on the button with a name of the command



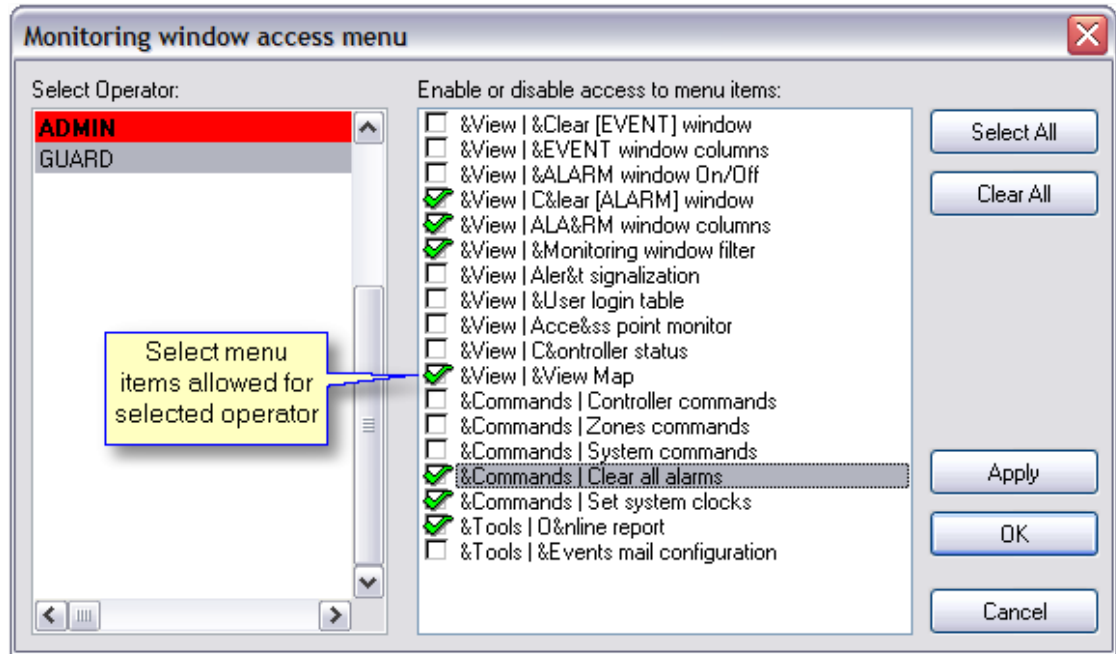
12.3 Tools

12.3.1 Operator rights

This feature allows to define access rights to the monitoring window menu for selected program operator. Configuration consist in checking boxes which means menu items of monitoring window. When finished click **Apply** to save changes.

In case only **ADMIN** is defined, you have to add new operator:

- close this window,
- close monitoring window
- Select **Tools** from main menu and -> [Program operators](#)
- Click **add** button



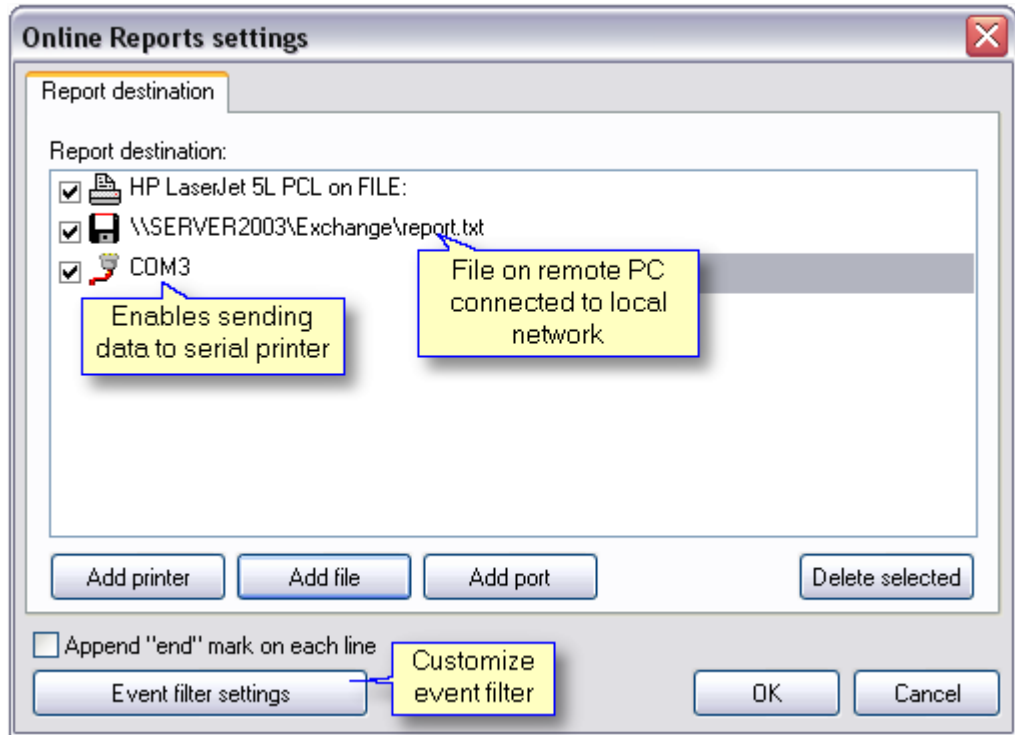
12.3.2 Online reports

This function enables to generate [online reports](#). When option is activated events are immediately send from RACS system to all defined destinations. It's possible to specify filter settings for each of defined destinations. Configuration of filter is carried out the same like in [Monitoring filter](#).

To activate filter you should:

- click on **Report Filter** tab
- check **Online Report Filter active** box
- set filter **mode** and **criteria**

Feature is very useful especially when operator wants to print all or particular events, or to save events in remote directories. It's possible to define many printers, files and ports if needed.



See also:

[Monitoring filter](#)

12.3.3 Events mail configuration

The option allows to send all or filtrated events in e-mail message. To enable this feature:

- check **Output filter active**
- define events in **Active subfilters** field
- click on Account configuration button
- configure account (e-mail account configuration is carried out the same like in [XML reports and e-mail](#) function)

Once finished you can test your settings by click on **Send test e-mail now**.

Events mailing configuration ✖

Output mail filter settings:

Output filter active

Filter mode:

OR mode

AND mode

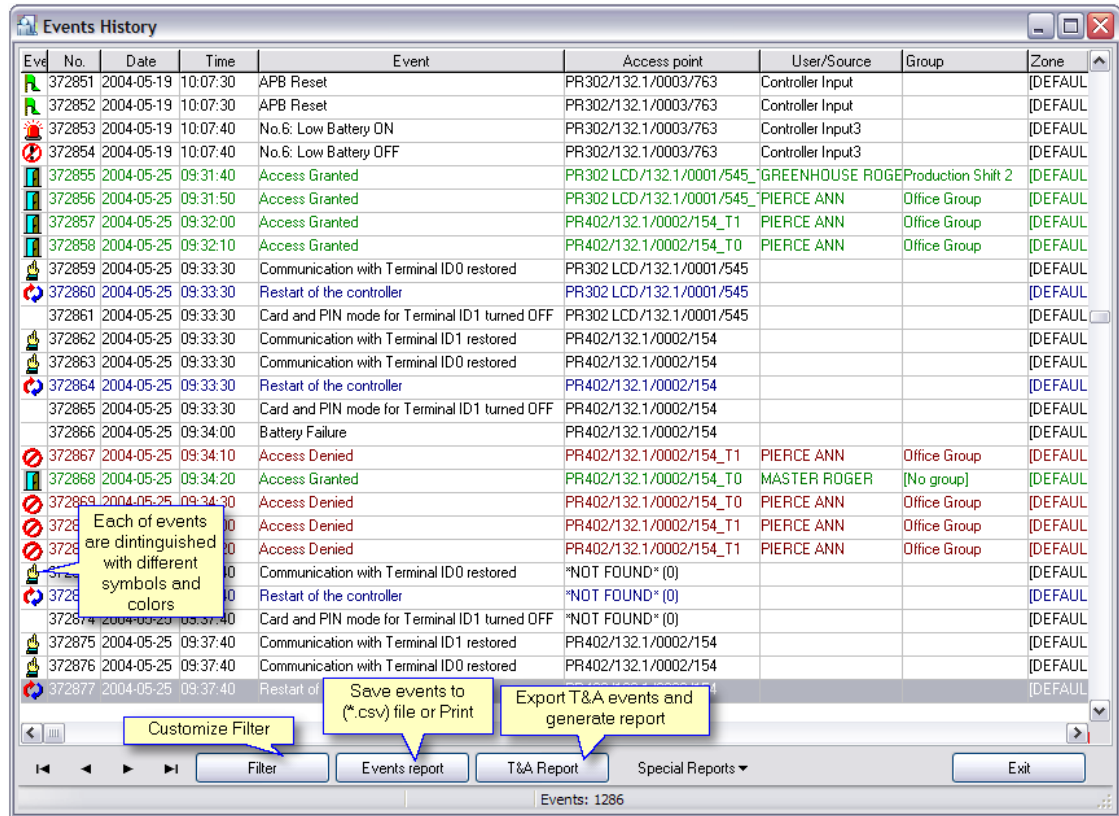
Active subfilters:

<input checked="" type="checkbox"/>	Events	<input checked="" type="checkbox"/>	Controllers
<input type="checkbox"/>	Groups	<input type="checkbox"/>	Subsystems
<input checked="" type="checkbox"/>	Users	<input type="checkbox"/>	Zones
		<input type="checkbox"/>	Door types

E-mail:

13 Events

Events history (or events registry) feature displays filtered or all events stored in system database. From this window events may be directly exported to CSV or T&A report.



See also:

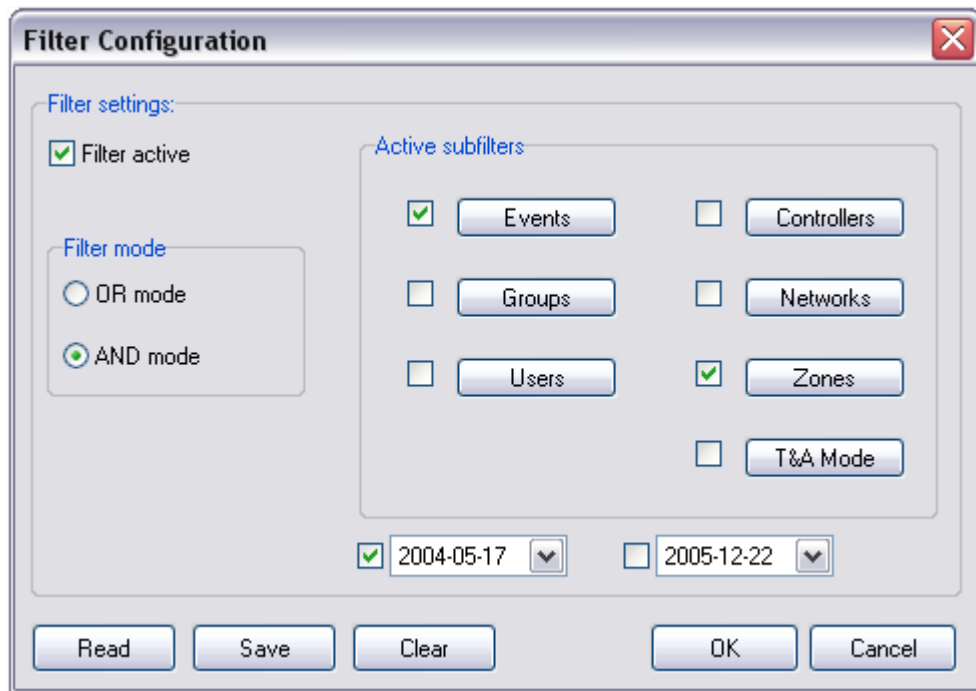
[CSV Report](#)

[T&A Report](#)

[Attendance in area report](#)

13.1 Filter configuration

Filter configuration feature enables to specify which of events stored in RACS database you want to review. Once **Filter active** option is disabled and you click **OK** button, Events history window with all registered events will appear. By selecting **AND/OR** filter mode it's possible to specify type of condition(s). **AND mode** - is used when all selected conditions must be realized, whereas **OR mode** - when one of selected condition must be realized.

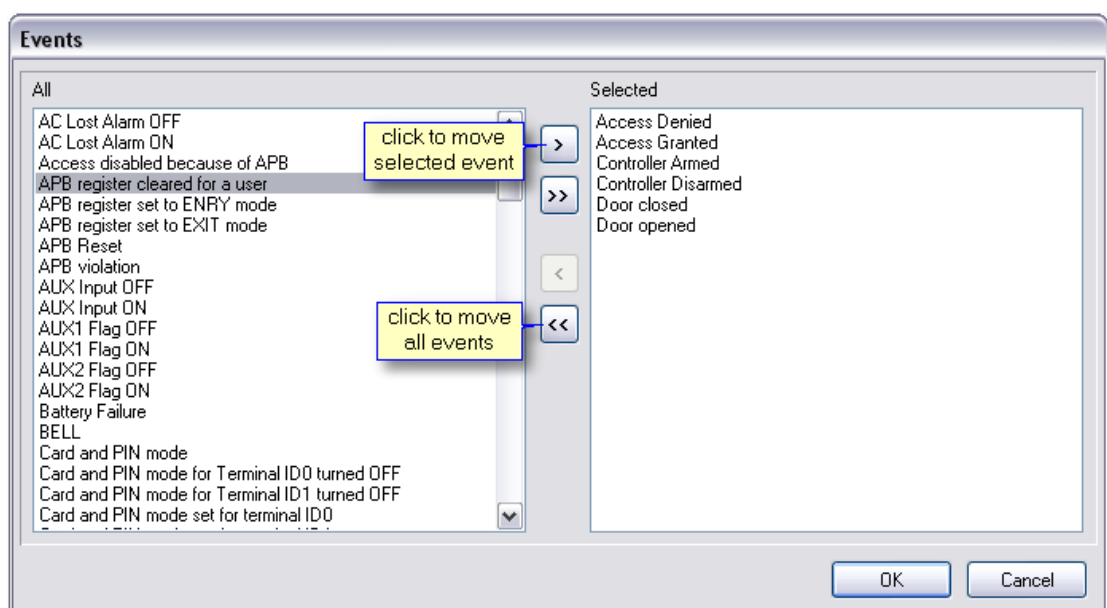


Options description:

- **Read** - read filter definitions from external (*.rmf) file
- **Save** - save filter definitions to external (*.rmf) file
- **Clear** - reset all settings and disable filter

To define Monitoring window filter:

- check **Monitoring filter active**
- select **filter mode (type of condition)** by clicking radio button **OR/AND** mode
- click on one of **Active subfilters**: Events, Groups, Users, Controllers etc. Similar window will appear:



- add elements to the list using buttons: > and >>
- click **OK**
- check box located next to the subfilter button to activate it.
- add another subfilter following four previously listed points

Optionally it's possible to set **start date** and **end date**. This option allows to review events which happened later than defined start date and also review events which happened earlier than defined end date. If both checked then list of events of time period from start date to end date is displayed. You don't have to activate subfilters when only date settings are required, option works separately.



Example:

- select filter mode **AND/OR**
- specify **Active subfilters**
- click **Events** and select: Forced entry, Prealarm, DURESS Entrance and Door ajar
- click **Zones** and select: e.g. Zone X and Zone Y
- leave date checkbox unchecked

Description:

1. AND mode selected

Events history window will display only this events which fulfill **AND** condition. It means that event will be shown in case at least one element from each of active subfilters will be met. If filter set like in the example Events history will list e.g. Prealarm in Zone X or Door Ajar in Zone Y events.

2. OR mode selected

Events history window will display only this events which fulfill **OR** condition. It means that event will be listed in case one of defined element in active subfilter is fulfilled. If filter set like in the example, Events history will list all Prealarms, DURESS Entries, Forced entries, Door ajar and all events in Zone X and Zone Y events.

13.2 CSV Report

This option allows to generate (*.csv) events reports which consist of all or filtrated events. CSV reports can be reviewed in MS Excel software.

To configure events report:

- select report columns by clicking boxes,
- choose **columns' separator**
- select **location** and type name of file
- click **OK**

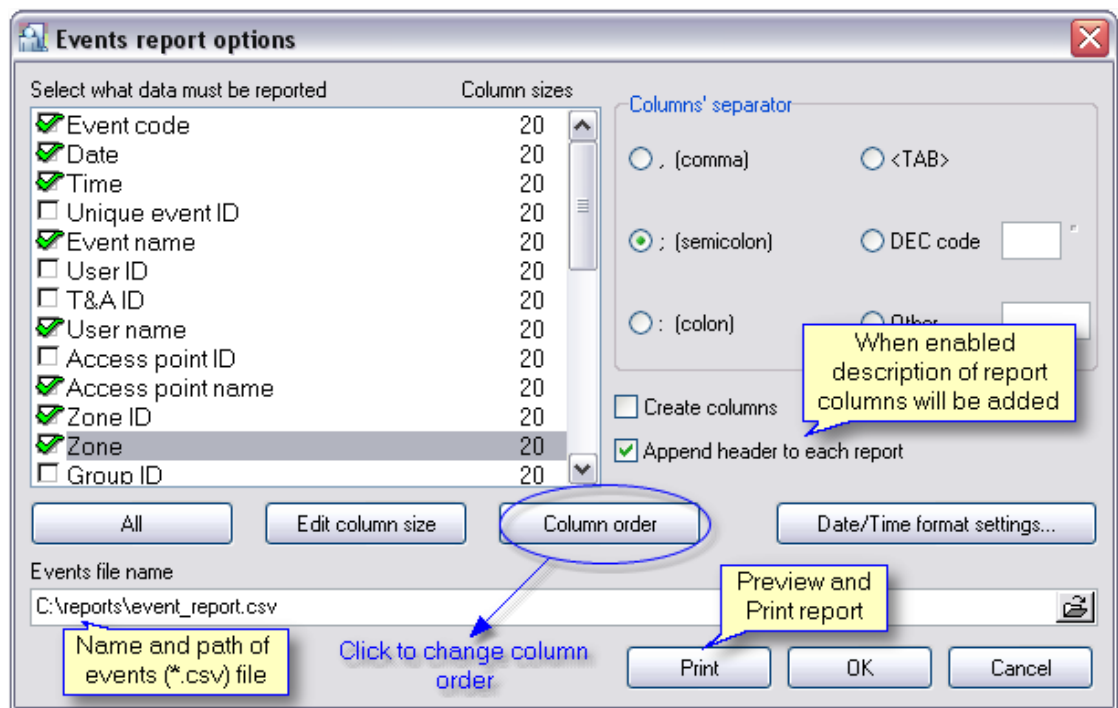


Note:

1. By default all columns are unchecked, so remember to select appropriate boxes before generating report.

2. To open CSV report in **MS Excel** it's recommended to follow these steps:

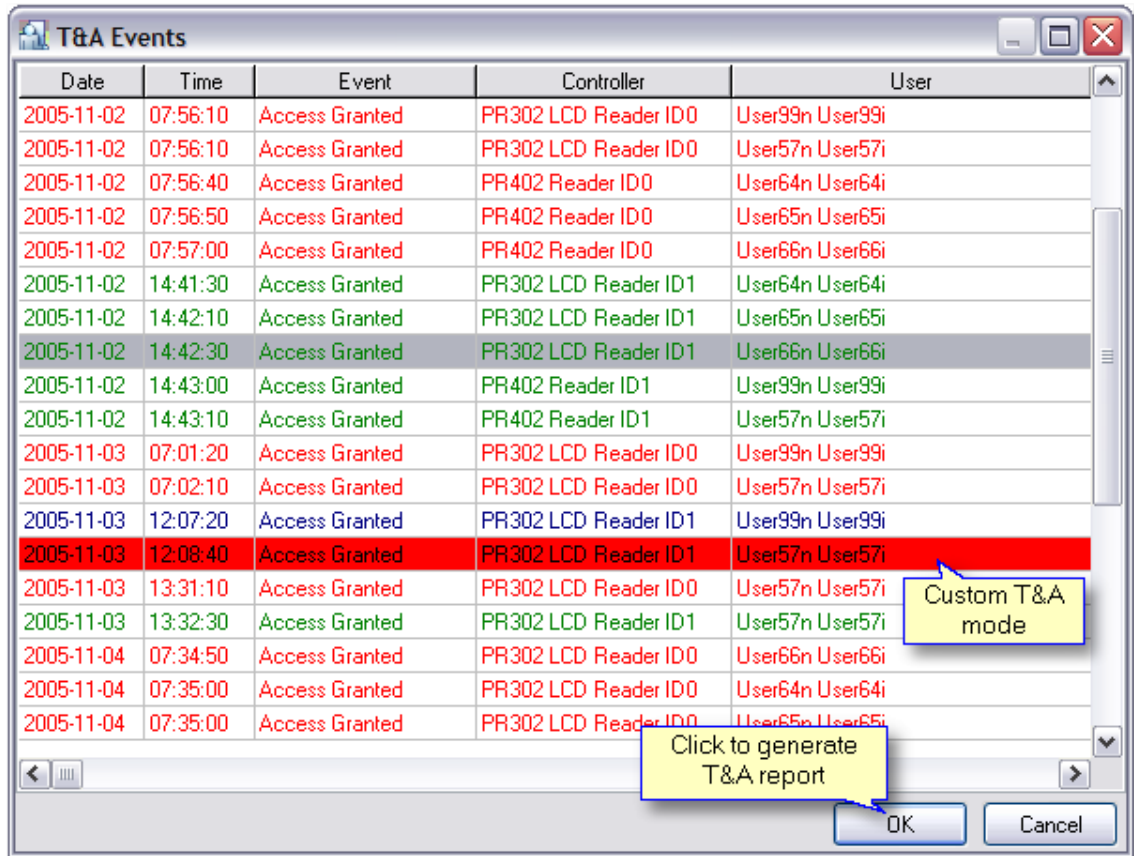
- click **File** -> **Open** from menu
- select file type: text files (*.prn, *.txt, *.csv)
- select CSV file and click **OK**



13.3 T&A report

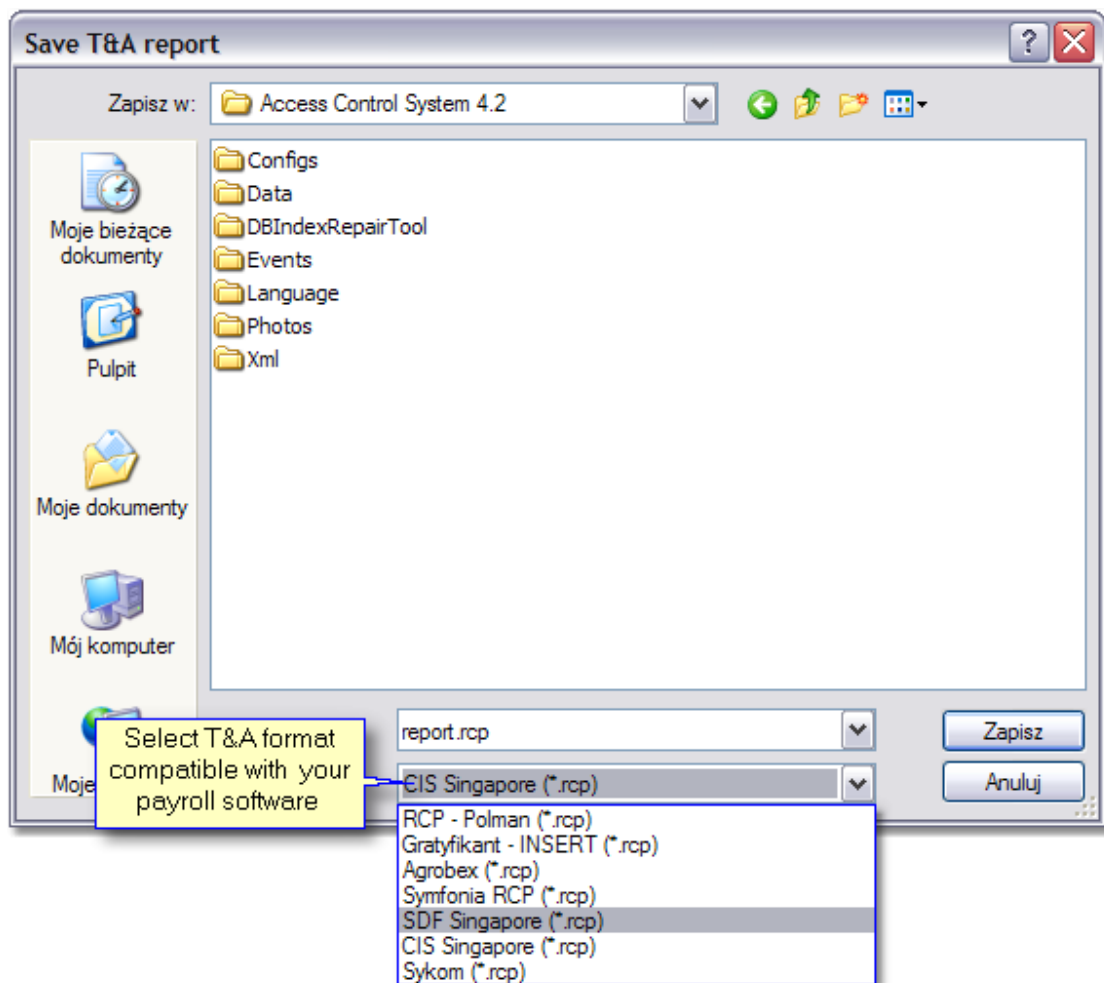
This feature allows to generate RCP report which enables to export data from PR Master to external payroll software. Report includes only these events, which have influence on T&A registering. All Access Granted events with **No T&A** mark are ignored and excluded from the list. Listed events are distinguished in varied colors, it helps to review T&A events. Here is description of T&A events:

- red font - Entrance
- green font - Exit
- blue font - On-duty exit (ODE)
- black font, red background - custom T&A mode (codes with ID from 50 to 254)



To generate T&A report:

- Click **OK**, the following window will appear:



- select destination folder and type a **Name** of file
- Select format of T&A report,
- click **Save**

RACS enables to generate report files in following formats:

- RCP - Polman (RcpAccess Pro+, Net+)
- Gatyfikant - INSERT
- Agrobex
- Symfonia RCP
- SDF Singapore
- CIS Singapore
- Sykom

See also:
[T&A Modes](#)

13.4 Attendance in area report

Attendance in area report is used for calculation of total job hours in defined area. Total attendance time is calculated on base **Entrance** (access granted registered on Entry point) and **Exit** (access granted registered on Exit point) events.

To generate attendance report:

- choose from the main menu **Reports -> Attendance**
- specify time range **From/To** (date and hour)
- select **User group**
- select T&A area (defined by user **-Edit -> Attendance**)
- specify maximal acceptable attendance period (do not set 00:00)
- click on **Refresh** to see applied settings

Attendance report can be printed - **Print** or saved into formatted (*.rtf) file - **Save**. It's available to select type of rtf report:

- **Normal (summary attendance in area)** - report contains only total attendance time of users
- **Detail (summary and detail users attendance in area)** - report contains total and detailed attendance time of users

Enter a time range for attendance report:

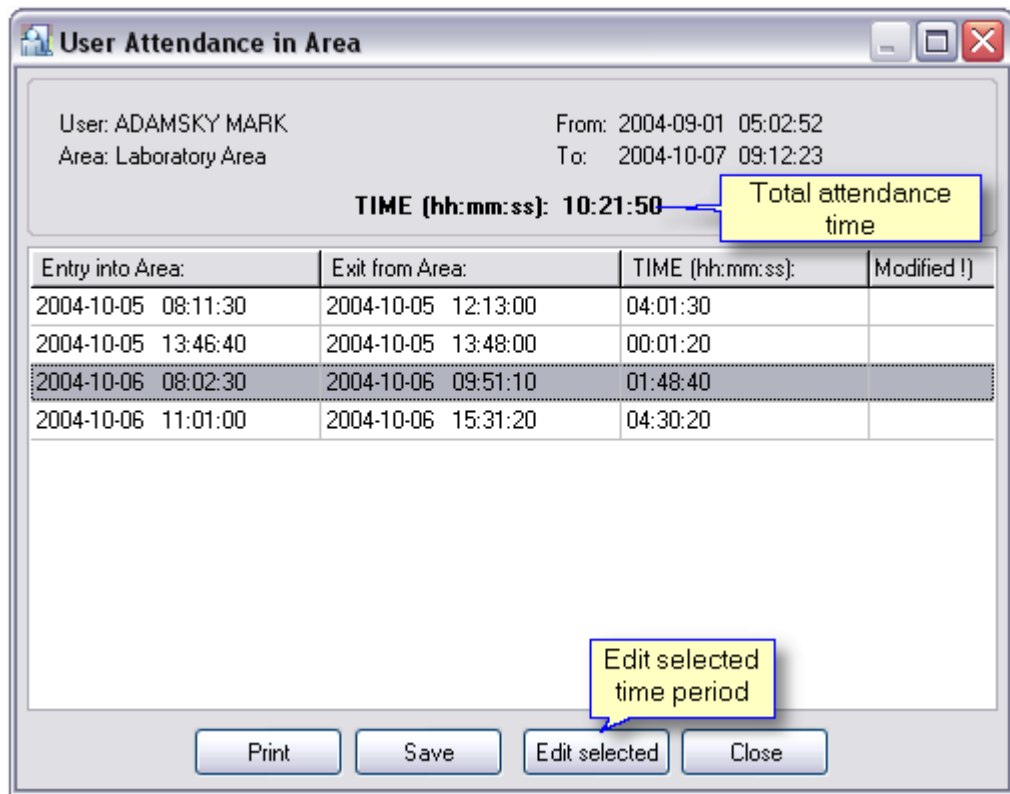
From: 2004-05-25 00:00:00 To: 2004-05-25 19:49:31

Select Attendance Area: Name: Laboratory Area Max. acceptable attendance period: Max. time: 19:00:00 Refresh

User ID	User Name	T&A ID	Time (hh:mm:ss)	M
333	EAGLEN AMANDA	535467	06:24:50	yes
444	HAMET BETTY	39150	06:26:30	
555	MARCH DAISY	98351	05:50:50	
777	PETERSEN ANDREE	3637	04:07:10	

Print Save View selected Close

In case in the **Time (hh:mm:ss)** field ? sign occurred it means that program hasn't received Entrance or Exit event. It's recommended to modify it by **[View selected]** button and enter missing date and hour.



You can disable incomplete time periods, by checking **Ignore incomplete data** option. In this case only completed time periods will be taken into consideration.

13.5 Reports

This feature allow to generate "ready to print" [reports](#). Reports concern all system domains (Groups, Users, Zones, Networks, Controllers). They cannot be edited nor saved. It's only available to preview just before printing.

14 System with/without CPR

Networked operation with CPR

When PRxx2 type of controller operates in networked system together with other controllers and CPR control panel, events are continuously transferred from all controllers to CPR internal buffer. When connection with CPR is broken controllers automatically move to autonomic mode and store events in theirs internal memory banks, after communication with CPR is restored controllers return automatically to networked, in both cases controllers retain their full functionality (no functionality is lost or reduced). During normal system operation CPR synchronize real time clocks of all controllers and stores events which occurred in system. Events stored in CPR and eventually in controllers' buffers can be manually downloaded to PC database or will be downloaded automatically anytime monitoring from PC is started. Older types of controllers PRxx1 series don't have ability to store events. Devices of this type must operate with control panel. CPR manages access rights on the PRxx1 controllers and store system events.

The main advantage of networked system equipped with CPR is that events which have been

occurred on controllers are instantly transferred to remote “secure” buffer in CPR and that CPR continuously synchronize clocks on all controllers so even after long time period controllers’ clocks have the same time.

Networked operation without CPR

When computer is connected to access control system and monitoring window of PR Master is active, events are continuously transferred from controllers to PC database. When PR Master operate with monitoring window deactivated, events are stored in controllers’ internal buffers and can be later transferred to PC using interactive command or will be downloaded automatically anytime monitoring window is started.

Main advantages of networked operation with CPR:

- CPR continuously collect events and stores in a safe buffer (256 tys. events)
- CPR continuously synchronize real time clocks of all controllers (even after long operating time controllers’ clocks have the same time set)

Disadvantages of networked operation without CPR:

- if network is connected trough UT-4 interface, CPR causes additional communication time delays
- when many access controllers with internal buffers (more than 8) are connected to network, control panel’s buffer is filled much faster.



Note:

1. When controller (PRxx2) detects activity of CPR control panel or PR Master is running in monitoring mode it moves automatically to networked mode and vice versa, when no CPR exist in access network or monitoring mode disabled controller moves to autonomic mode.

2. Utilisation of CPR control panel is optional and depends on system requirements.