User Manual

preliminary document

roger®

ROGER ACCESS CONTROL SYSTEM

Table of Contents

1 Introduction to PR Master 4.0

PR Master 4.0 is a program 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 neccesary. Detailed update procedure description is on www.roger.pl site.
- The most stable work of RACS software can be achieved with systems Microsoft Windows XP and 2000.

Main features of PR Master 4.0:

- 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 guide, 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.

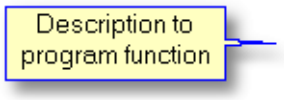
The most important concepts related to RACS:

- **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 precints 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.

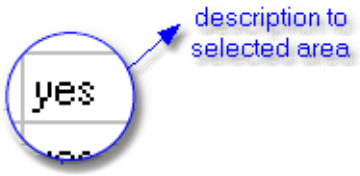
3 Using Help

To better understand this instruction 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 shaddow decribes zoom or selected regions of windows

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

Describes interactive links

Notice:

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 Install and register program

Software package is delivered on ROGER CD-ROM and available to download on www site www.roger.pl.

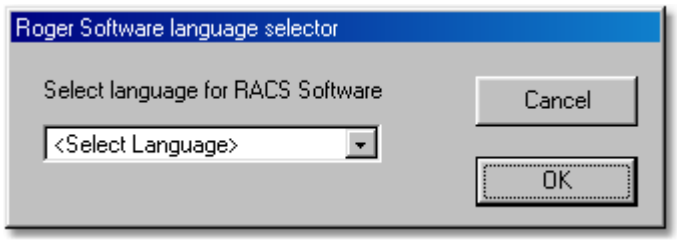
To install RACS software from CD-ROM click on ***start.exe***

PR Master package consist from programs:

- PR Master
- Language Selector
- Remote Monitor

Program is installing in English language version. To change language you should:

- Choose from menu ***Start*** -> ***Programs*** -> ***Roger ACS 4.0*** - > ***Select language***.
- And then select language

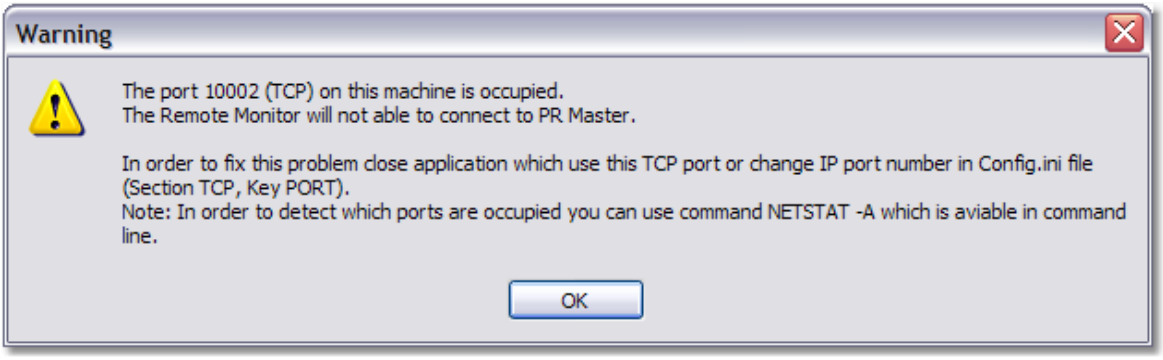


First start of PR Master

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

During the PR Master start, program trying to open ports to listen and communicate with Remote Monitor applications.

In case when port with default number TCP:64181 and UDP:6789 is already occupied by other system application following window will appear:



In this situation you should edit Config.ini file, which is in main directory of PR Master program and change PORT=64181 to another number e.g. PORT=5555.

Note:
Type "netstat -a" command in the command line to check which ports are already used.

To make login procedure more easy, user can apply autologin function. It allows on automatic user login to program.

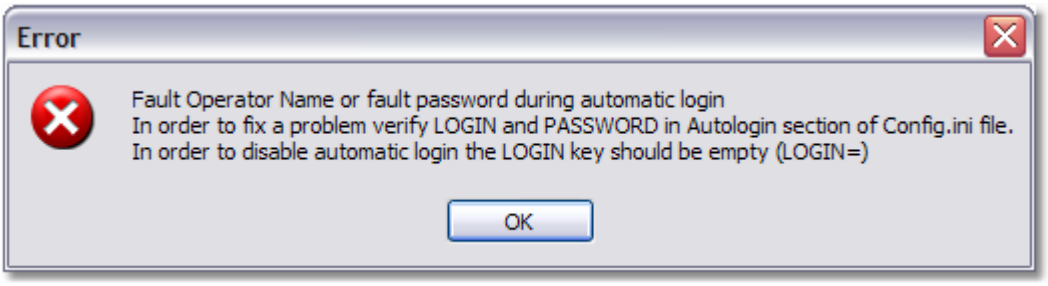
To use this function you should make some changes in Config.ini file:

- open Config.ini file e.g. in Notepad
- find section:

[Autologin]
LOGIN=ADMIN
PASSWORD=

- type your LOGIN and PASSWORD

When PR Master start, it check autologin section and next try to login with defined keys LOGIN and PASSWORD. If login procedure fail, the following communicate will appear and close the application.



To register program, copy licence file "PRlicence.ini" into directory ..\Program Files\Roger\Access Control System 4.0.
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.

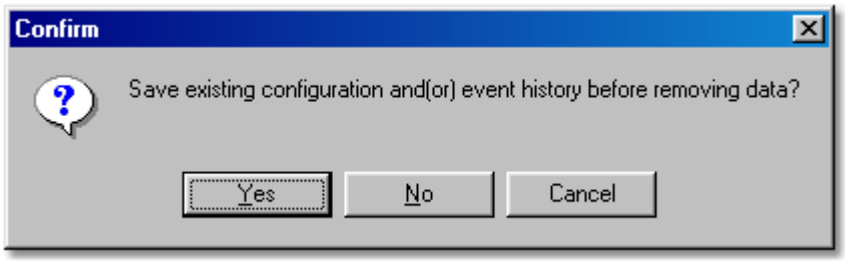
5 System database of RACS

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. PRMaster allows user to autobackup (backup configuration) selected data (events, configuration) which can be used in case the database is crashed.

PRMaster 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.



Note:
It's very risky operation, should be careful and save file before creating new database.

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 in main catalog of PR Master program. Network system database is shared for many computers in local network by setting permissions for users.

5.1 Local system database

Local system database is used in installations on the one PC computer. It's the best solution, when there is no need to control and configure system from many computers.

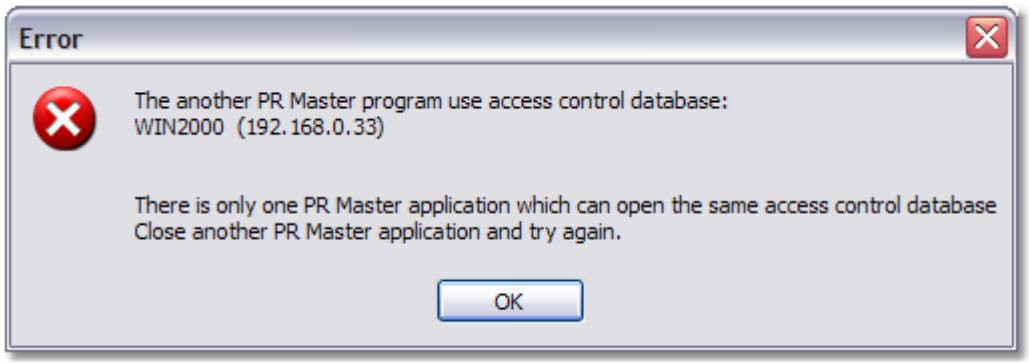
5.2 Network system database

Operation with network system database enables to configure and control RACS system from many places in local network. System database is shared with all or selected network users by setting permissions. PC computer which connect with network database requires PR Master applications installed.

This system feature is very useful, especially when many users utilize system database resources. It's also good solution in companies which own wide LAN network and there is a need to full system control not only from the one computer.

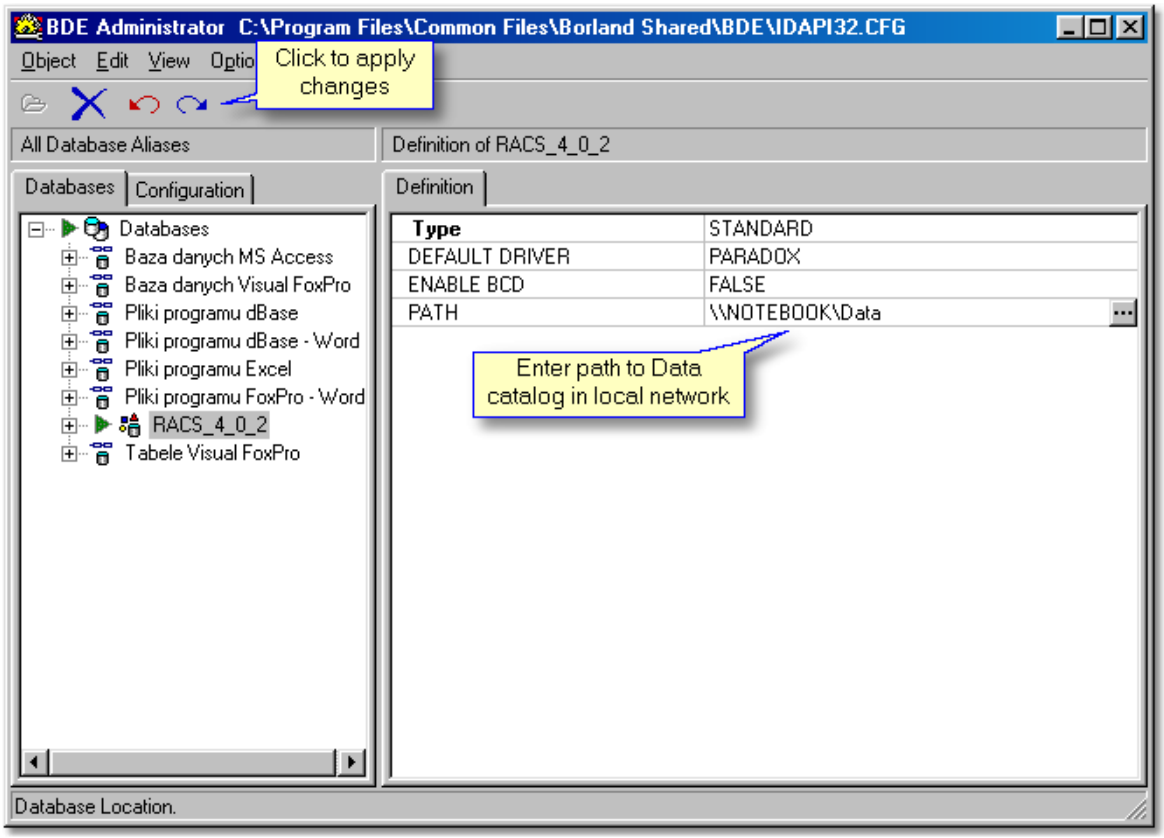
Full RACS system control from many computers in LAN network is available only in case when communication bus is connected by UT-4 communication interface and works on TCP channel. Thanks to defined IP address of UT-4 computers communicate with system from every place in LAN network.

Note:
In the same time one PR Master application which use database resources can be executed only, therefore trying to run application on other PC will generate following communicate and close the program.



To prepare RACS system to work with network system database you should do the following steps:

- Copy ***Data*** catalog which founds in ***x:\Program Files\Roger\Access Control System 4.0,*** 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 change and read permissions for all or selected network users
- Open ***Data*** catalog and delete this files: PARADOX.LCK, PDOXUSRS.LCK, PDOXUSRS.NET
- Run ***BDE Administrator*** from Control Panel on computer which will connect with system network database.
  Following window will appear:



- Select ***RACS_4_0_2*** 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 application.

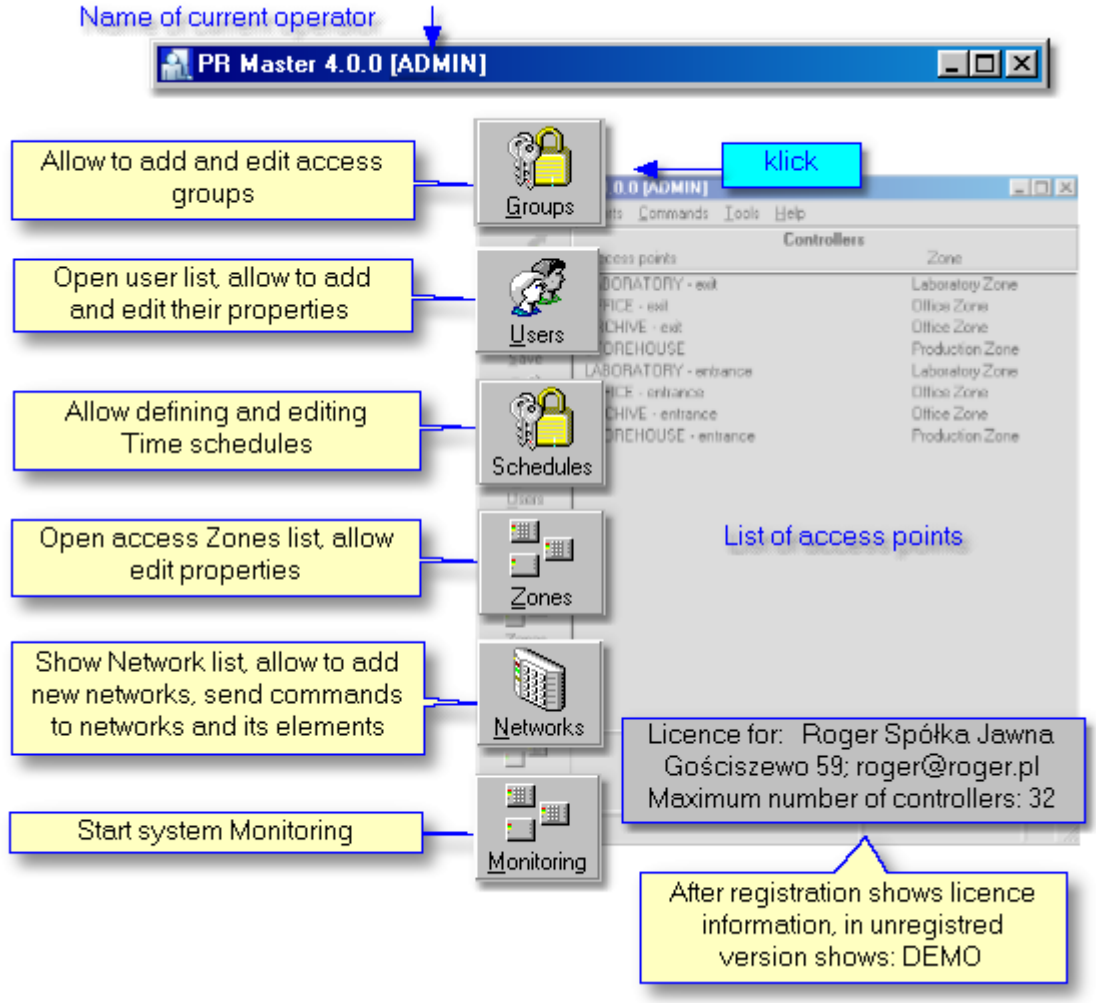
Note:
PATH changes should be done on every computer, which connect with network database

System is configured now, and enables to operate with network database.

6 Using program

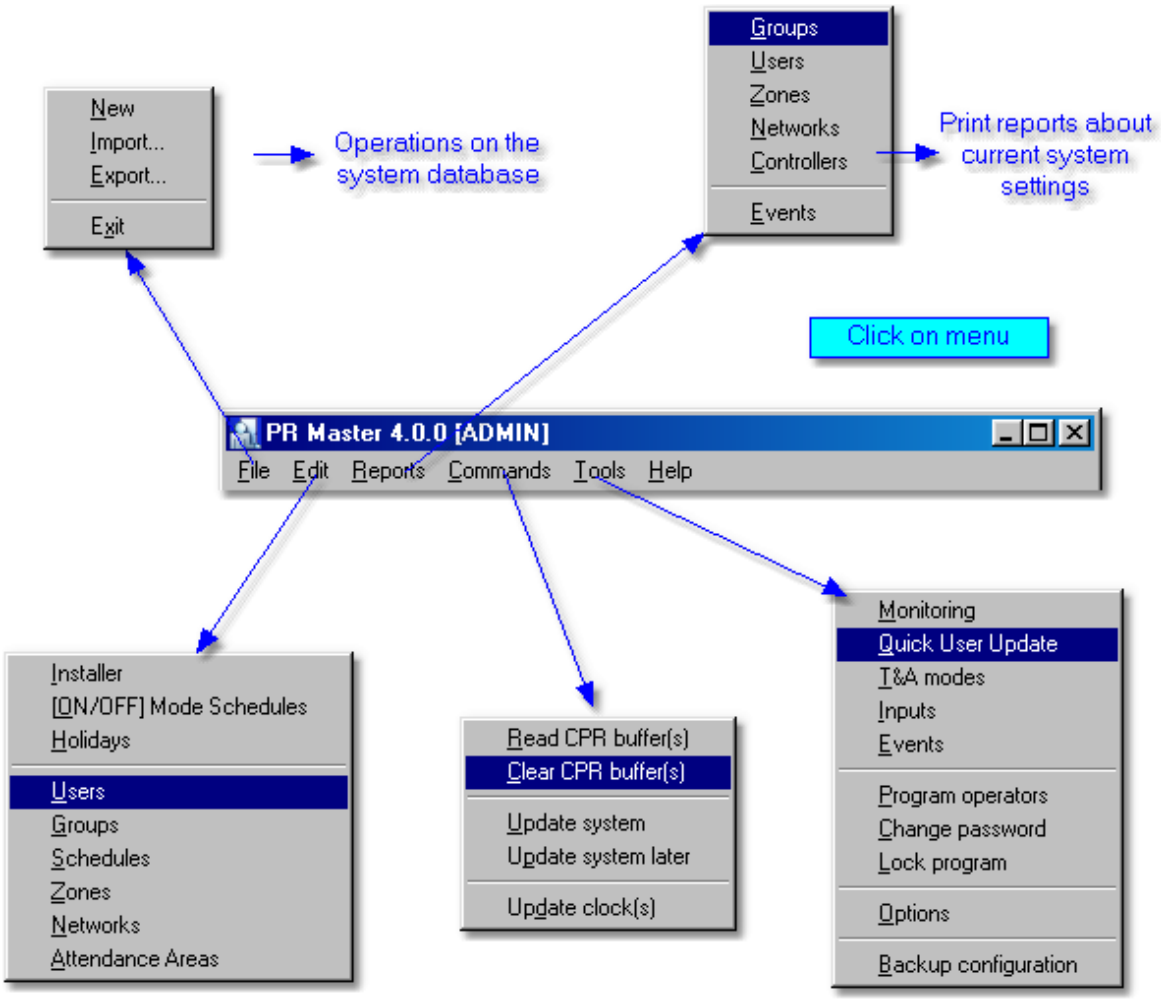
6.1 Main window

Main window of the program PR Master 4.0 consist of: main menu, operator toolbar, list of access points and licence information. Operator toolbar is an easier way to access the system functions. Usually a "hint" is displayed when you move the cursor close icon, field or button.



6.2 Main menu

Main menu contains tools and options of the program.



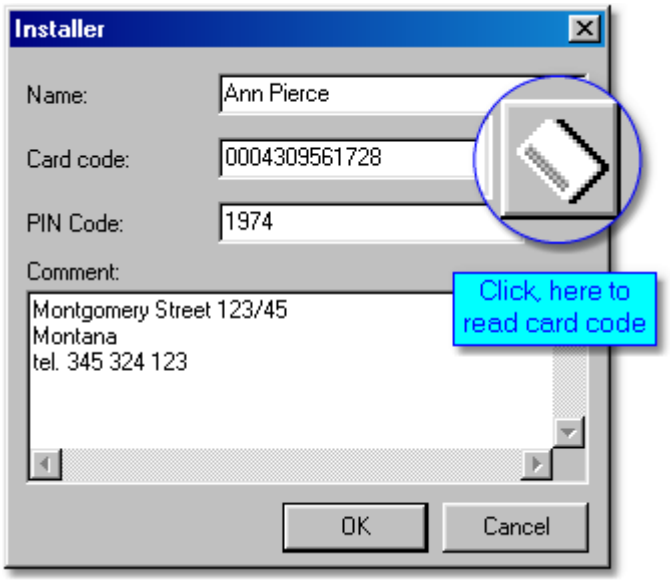
6.2.1 Edit

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 only from PR Master. Making any changes in contents of controller memory in installer or user programming mode causes incompatibility with program database.



6.2.1.2 [On/Off] Mode Schedules

Controller has two work modes: On mode and OFF mode.

Switching the mode [ON/OFF] can be realised:

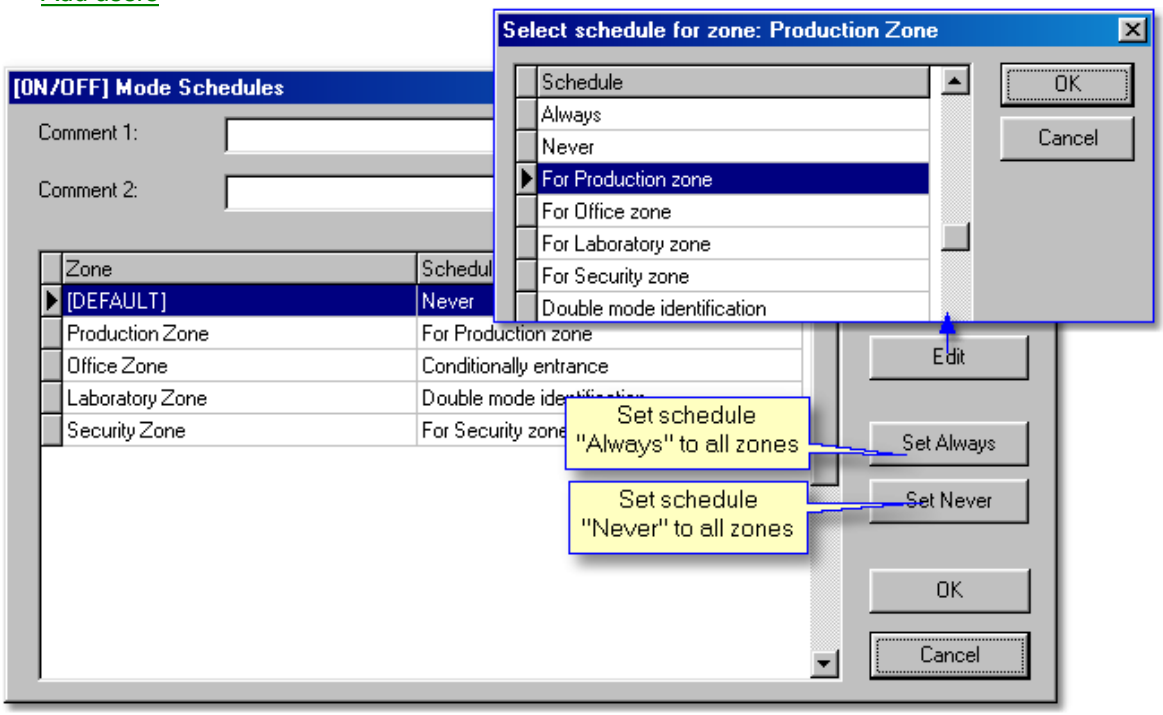
- local with MASTER or SWITCHER identifiers
- local with input line configured to function [ON/OFF Mode Control Input]
- local with input line configured to function [ON/OFF Mode Reversing Input]
- using interactive command (Commands to controller)
- automatic according to defined [ON/OFF] mode schedule

Note:
In case we choose function (local with input line configured to function [ON/OFF Mode Control

Input]), all other methods are automatically disabled.

See also:

Controller properties - options
Add users



6.2.1.3 Holidays

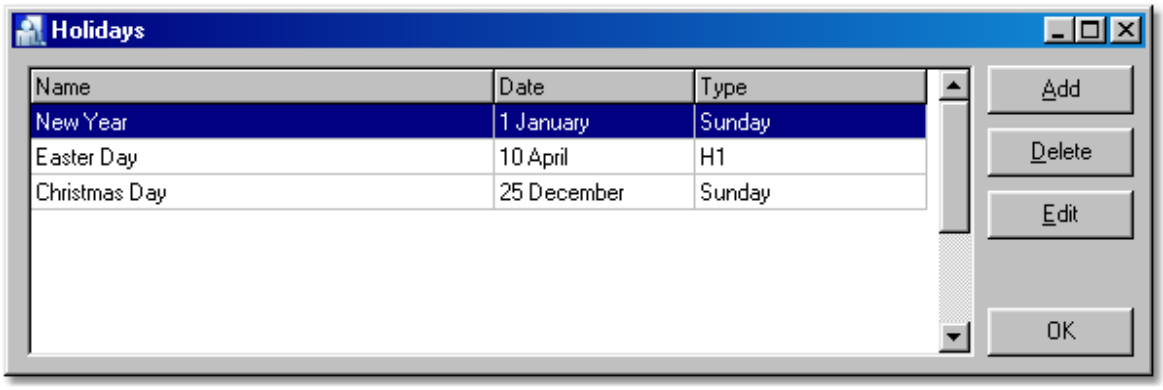
Holidays definition specify some days during year period in which controller behaviour is different as usual. Installer can define some special rules for holidays, PR Master software enables four types of holidays settings to be defined, H1, H2, H3 and H4.

The holiday definition consist from:

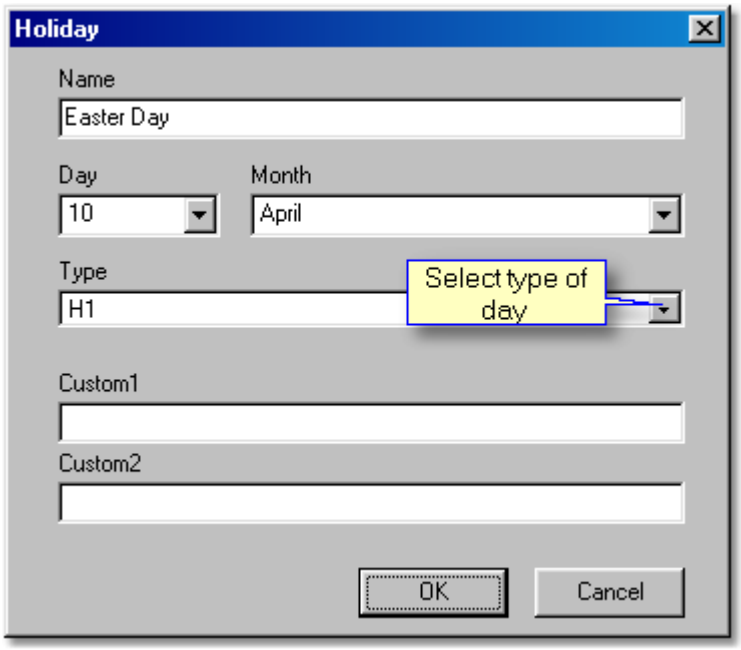
- name of holiday day, (e.g. Easter)
- date of holiday, (e.g. 10 of April)
- detail settings of holiday (e.g. H1)

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

Defining time schedules (including access rights), is realised in one-week period (from Monday to Sunday).



In the window [Holiday] choose ***Day***, and then select ***Type*** of the day (schedule).
We have days of week and days H1-H4 at choice. Days H1-H4 are utilized to define holidays, for which different (from defined days) time schedules will be valid.



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

6.2.1.4 T&A Areas

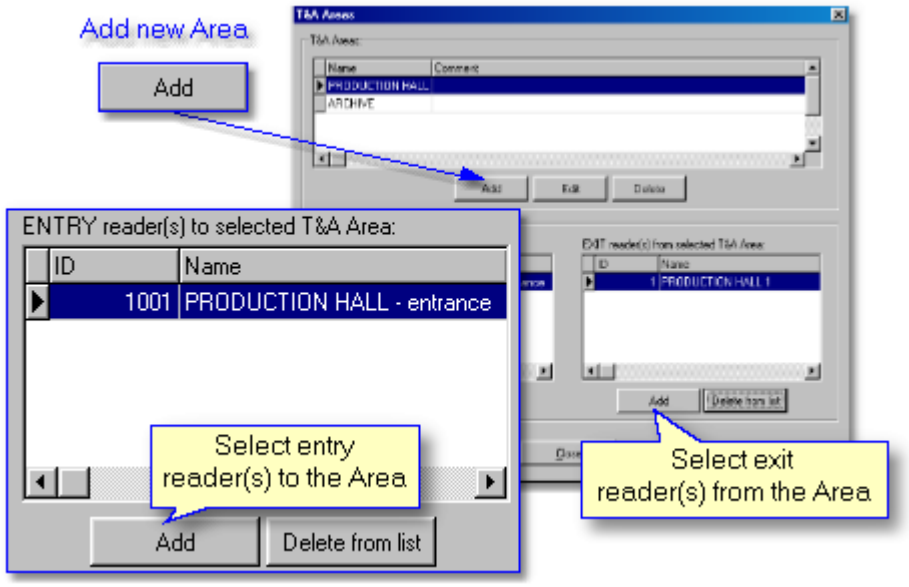
T&A Areas are defined to generate User Attendance reports. User attendance report shows time of user entry/exit and stay time in interesting us Area as well.
Time user spending in Area is counted on base entrance/exit from area register.

In difference of T&A reports, User Attendance reports don't consist in defining T&A modes. To generate User Attendance in Area report should define ENTRY and EXIT readers to/from Area. On base User Attendance report can count effective user (employee) time attendance, for example: in

Production Zone or Canteen.

To add new Area:

- Click on ***Add*** and type name of area
- Define ***Entry*** and ***Exit*** points (readers) of area

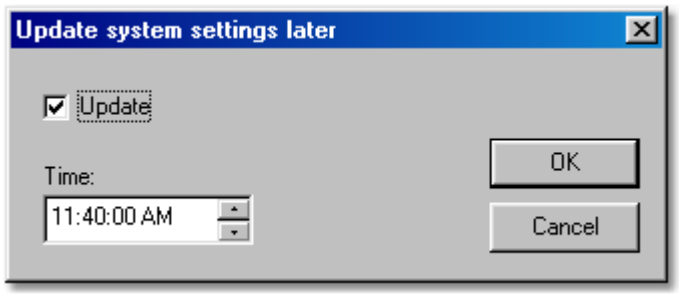


6.2.2 Commands

Commands sending from this menu concern whole system (all networks).

- **Read CPR buffer(s)** - read events from all networks
- **Clear CPR buffer(s)** - delete buffers of 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.

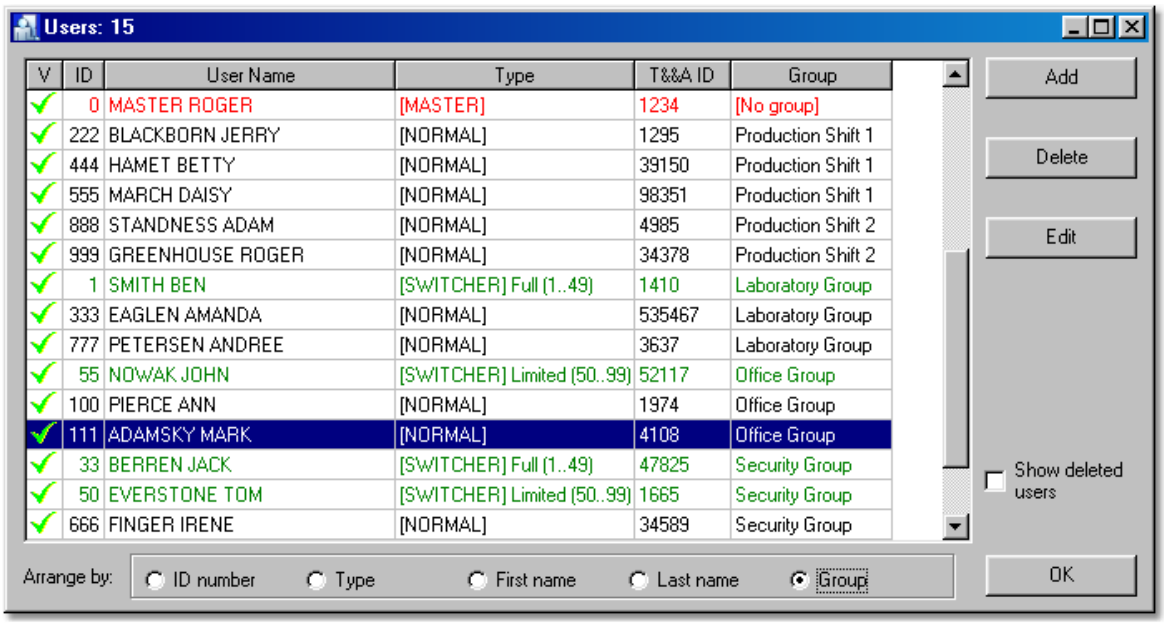
Note:
Option ***Update system later*** is useful especially in big systems, where sending configuration during users movement might cause problems, and difficulties in object functioning.



6.2.3 Tools

6.2.3.1 Quick user update

Quick user update is a very useful tool, which enables to edit, selected or add new user and send configuration to all controllers immediately.
In difference of normal configuration sending to controller tool ***Quick user update*** sends settings of only one user. Therefore data transfer is much faster.



6.2.3.2 T&A modes

This tool is used to define own T&A (Time & Attendance) modes:

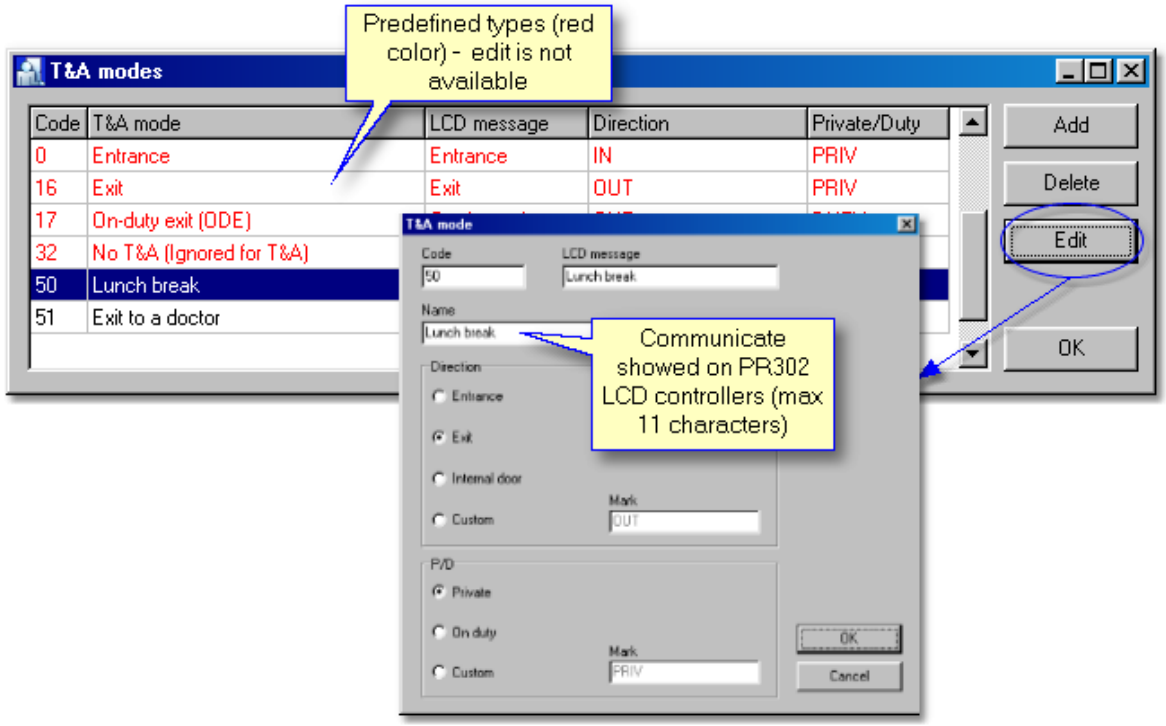
To add new T&A mode:

- 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***

We can apply Created T&A modes to Default T&A option in Controller properties (***Controllers*** -> ***Edit*** -> Terminal)

Note:
T&A codes in range from 0 to 49 are reserved to predefined types, which can't be edited.

See also:
T&A Report



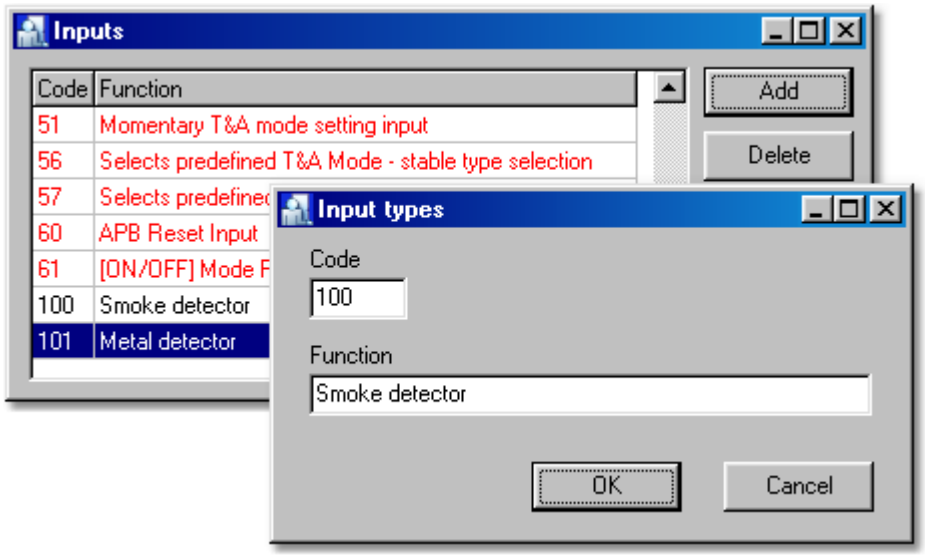
6.2.3.3 Types of Inputs

This tool allows adding own types of Inputs to the list. Predefined types of inputs (red font) are not editable.
If you want to receive information from controller about status of the other device equipments (for example smoke detector) define your own type of input.

Note:

Every new defined type of input has default settings:
- arm is ALARM event
- and disarm (return) is NORMAL event

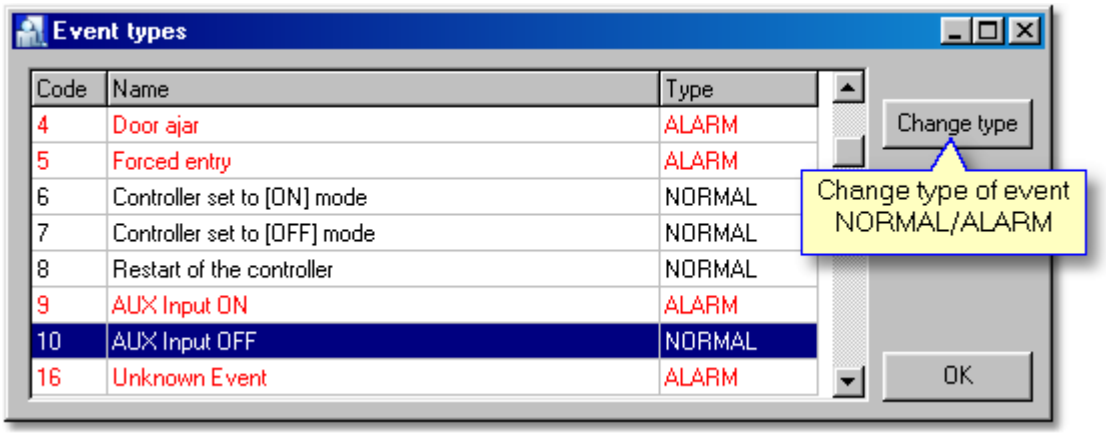
New type of input can be applied to one of four Input lines of controller (Inputs). Activity of input lines can be controlled in order to defined General purpose schedule.



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. Tool allows selecting from the list ALARM and NORMAL type of event. To change type of event from normal to alarm or inversely click on ***Change type***.
Alarm event in monitoring mode is also indicated in "Alarm" window, and causes "Alarms" belt blinking.



Alarm states of controller:

- ***Prealarm*** - the alarm occurs after three consecutive attempts of entering an unknown identifier repeated in a period shorter than 1 minute.
- ***Door ajar*** - the alarm occurs after door remains opened longer than period of time defined by "Time for door closing" Controller properties - Access.
- ***Forced entry*** - the state occurs in consequence of opening door without using controller

Every alarm signalisation on access controller automatically disappears after 3 minutes. Alarm may be deleted earlier (before 3 minutes) by a valid identifier registered in controller 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*** (concern selected controller)
- ***Monitoring*** -> Commands (available clear all or selected alarm)

Note:
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 indicated in monitoring window and registered in events history.

6.2.3.5 Program operators

This tool allows user to define new program operators with various access rights to a menu items. The feature is available for Administer only. It is possible to set password for operator, it will be required at the start of PR Master (login). Nevertheless normal logged operator of the program can change his password.

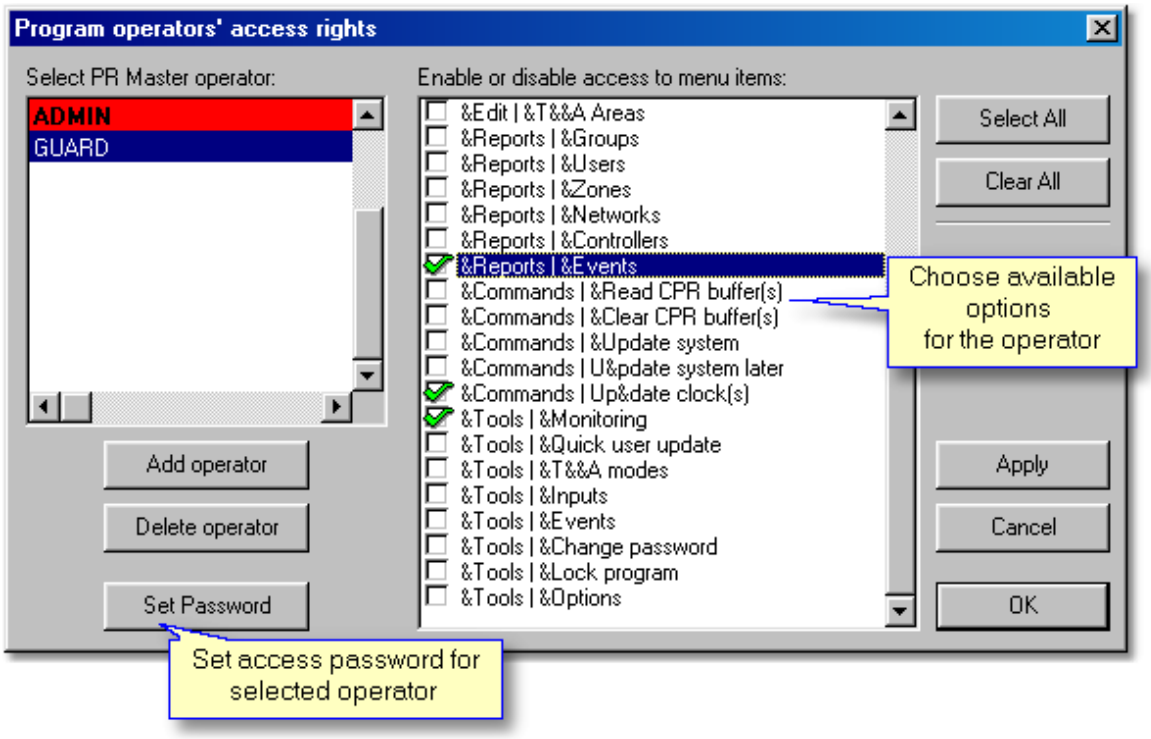
Feature ensures that all actions performed on the PC can be attributed to a particular operator.

Note:

1. The password is not displayed nor printed, the system displays the password as asterisks.
2. In Password up to 16 characters is available.

To define new operator should:

- Choose from main menu: ***Tools*** -> ***Program operators***
- Click on ***Add***
- Enable or disable access to menu items
- Click on ***Apply*** to save changes

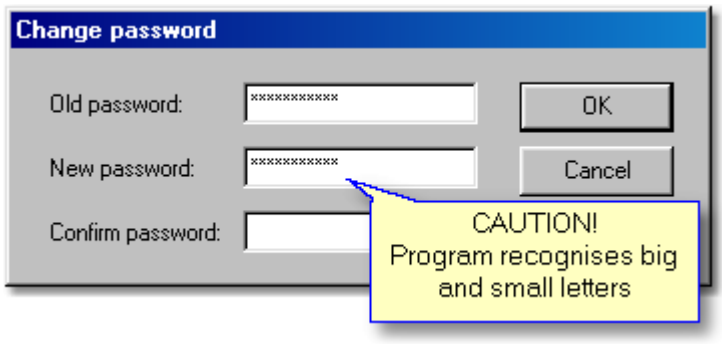


See also:
Lock program
Change password

6.2.3.6 Change password

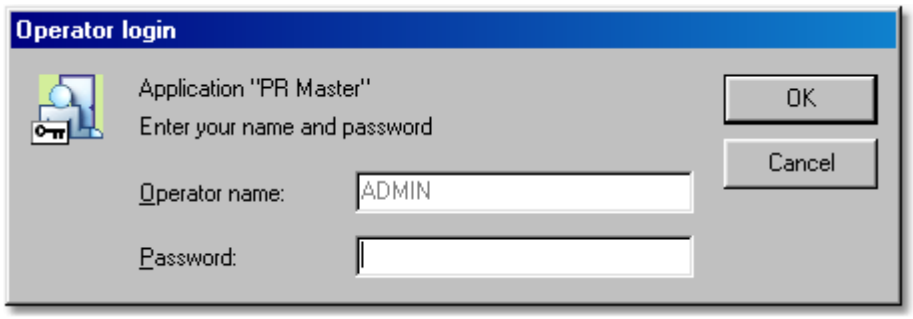
Tool enables to change password of currently logged program operator. You should first enter ***Old password,*** next type ***New password*** and Confirm.

Note:
Watch on state of "Caps Lock" button, because program recognises small and big characters.



6.2.3.7 Lock program

Tool allows to lock program and protect from others operators. When program is locked, its minimalised and following window appears.



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

See also:
Change password

6.2.3.8 Options

Additional program options:

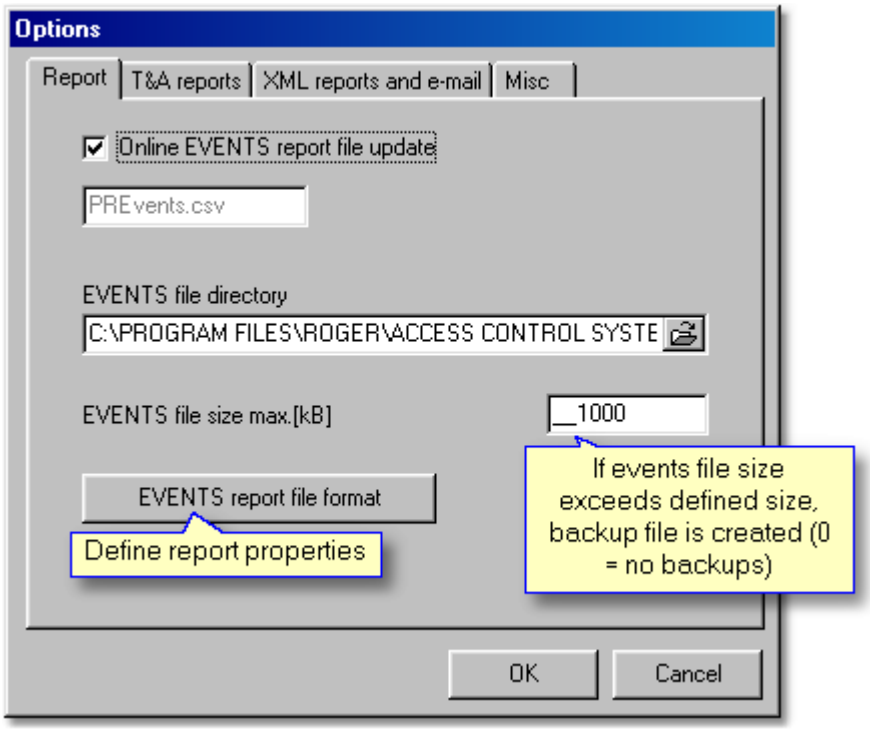
- Report
- T&A Reports
- Misc

6.2.3.8.1 Reports CSV

In case as ***Online EVENTS file update*** option is activated program PRMaster 4.0 in Monitoring mode continuously appends events to defined CSV file.When Monitoring window isn't opened, every events receiving from system buffer(s) causes actualisation of this file.
User can select report contents and define properties as well. It's also possible to specify maximal

size of CSV file.

See also:
CSV Reports

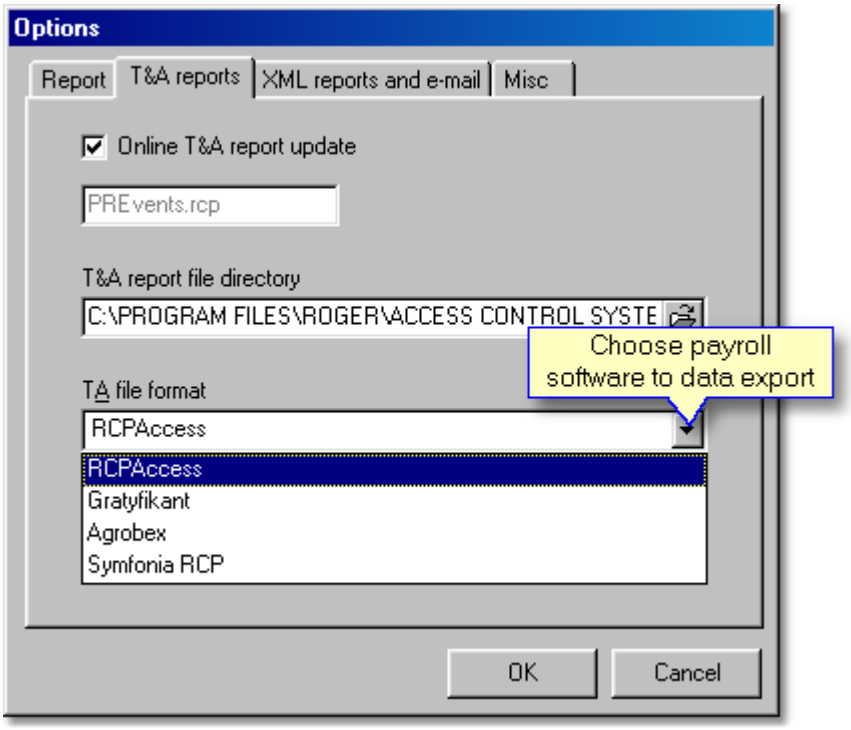


6.2.3.8.2 Reports RCP

When ***Online T&A file update*** option is activated program PRMaster 4.0 in Monitoring mode continuously appends events to defined (*.rcp) file. PR Master enables to select appropriate file format, according to used T&A software.

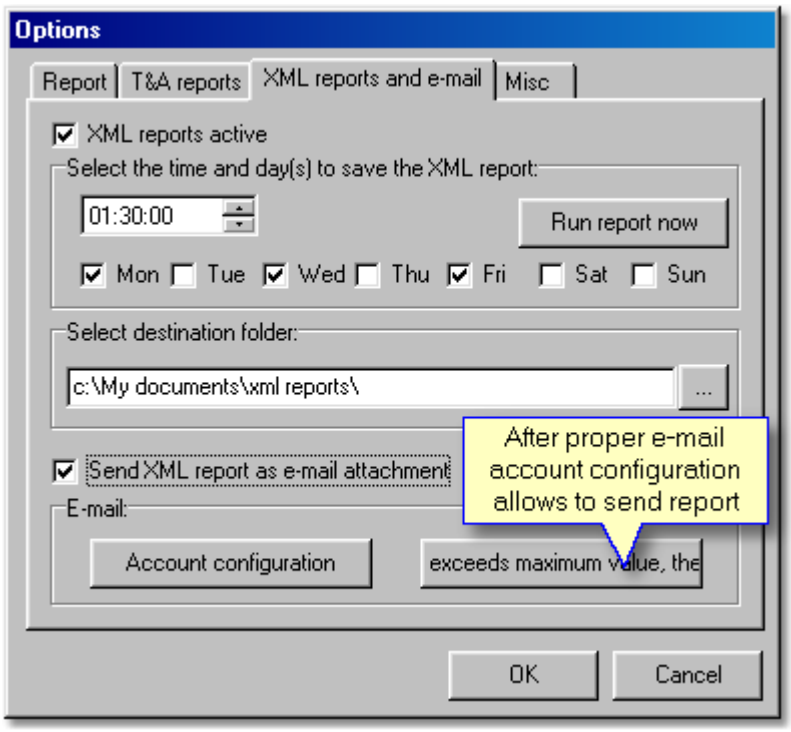
When Monitoring window isn't opened, every events buffer(s) reading causes actualisation of this file

See also:
T&A report

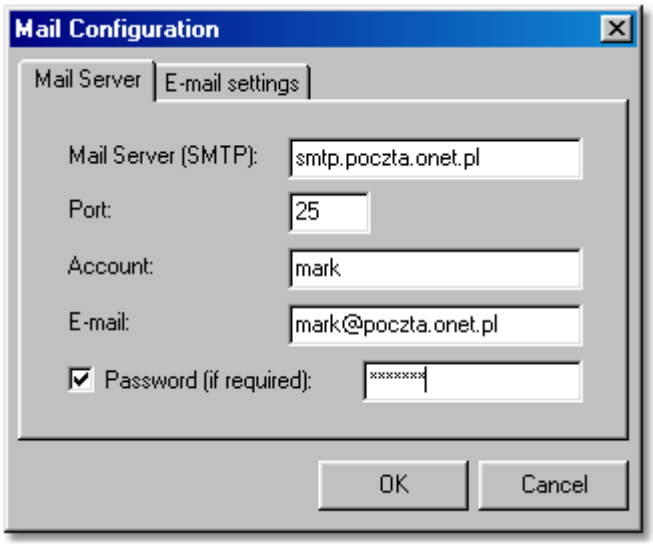


6.2.3.8.3 XML reports and e-mail

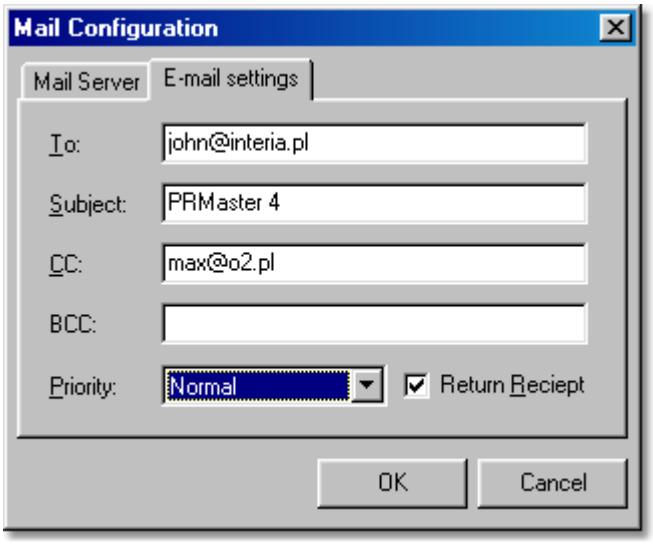
PR Master application allows XML reports generating according to schedule defined by user. Report contains all events, which took place after the last report generation. Files with precisely date and time included in file name are saved into selected folder. It's available to generate file report immediately using ***Run report now*** function.



User has availability to send reports by internet. To activate this function activate ***Send XML report as e-mail attachment*** function and configure e-mail account properly. You should enter data in the ***Mail Server*** tab. Information about e-mail server is often sending just after account set up. Enter password only if server requires it.



In the ***E-mail settings*** tab should fill in gaps of recipients (***To:***, ***CC:***, ***BCC:***) and set up ***Priority*** of message. Once the ***Return Reciept*** box is checked a notice from receipt will be required.

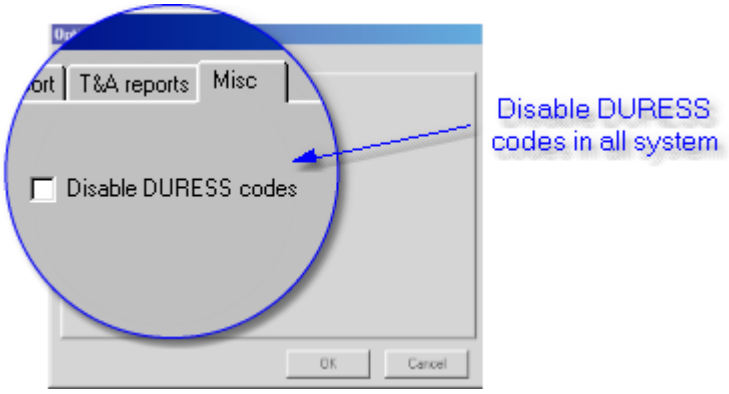


If e-mail account is configured properly, report is send to the selected recipients. Action follows XML file saving to a disc.

6.2.3.8.4 Misc

Miscellaneous program options allows to:

- Disable ***DURESS codes*** in all system



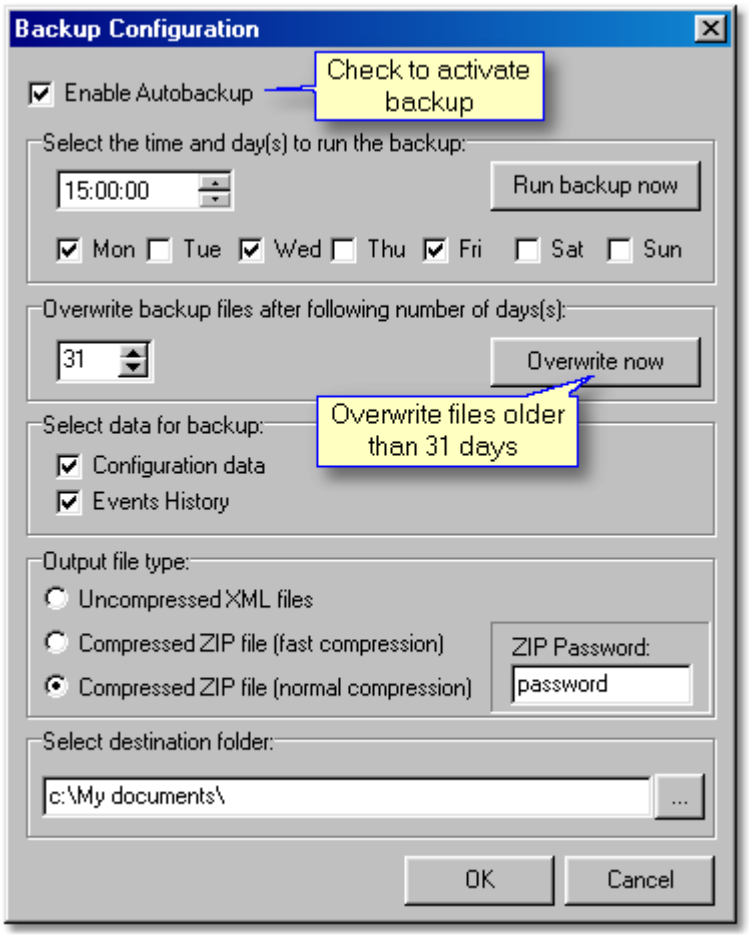
See also:
Controller properties - DURESS

6.2.3.9 Backup configuration

Function of PR Master allows user to define autobackup. It secures user from any database crashings.

The basic feature creates backups at the specified time: day and hour, or now [***Run backup now***]. Backup files are overwrought after number of days defined by user. Should select data for backup:

Configuration settings or ***Events History*** and destination folder.



Note:
Once Compressed ZIP file is selected can also enter security ZIP password.

7 Groups

In Roger Access Control System users may belong to a various access groups. Being member of access group determines user access rights in object. All users who belong to the same group have equal authorization for door opening. Eventually one user may be one group.
Program operator can define time schedules which are defined in a one-week period. According to it users will gain access to a particular zones. Groups have also access rights to 16 floors, which are not controlled by any of time schedule.
Every new registered system user belongs to none of defined system groups, he has full access (all rooms and floors) without any time restrictions and belong to group called [***No group***].
Every user may be registered to different group. So it is available to specify access rights for more than one system user.

System users loose access rights only in case:

- input line configured to Access disabled is activated
- door mode is set to locked mode
- controller is in OFF mode and option ***Access disabled in [OFF] mode*** is enabled

Note:
PR Master has one predefined access group called [***No group***], which has full access.
For older types of controllers (PRxx1) only 31 access groups can be defined.

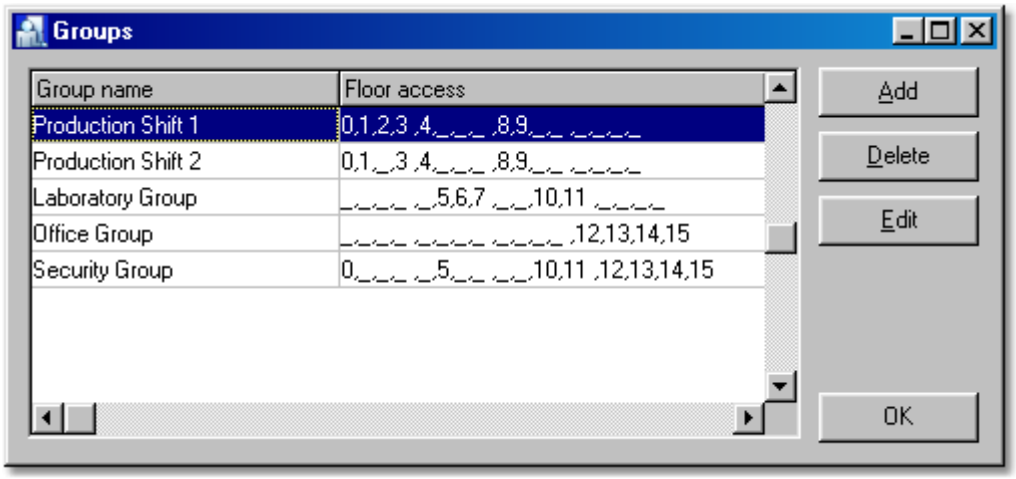
See also:
Add access groups
Group properties

7.1 Add access groups

New group can be created in two ways:

- Click on 

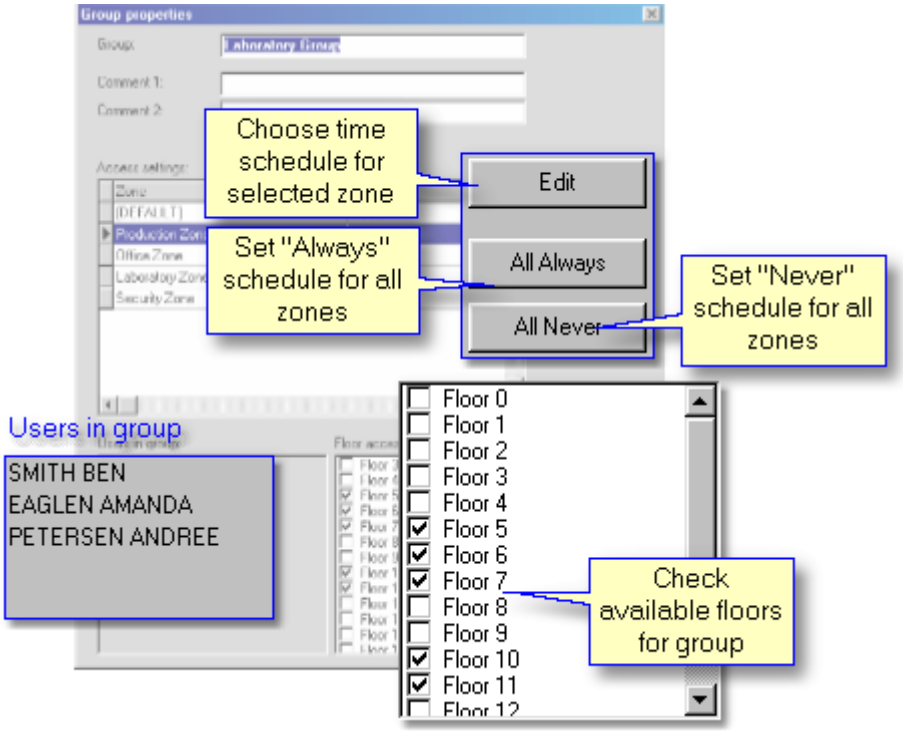
from operator tools in the main window or select from menu ***Edit*** -> ***Groups***
- Click ***Add*** button



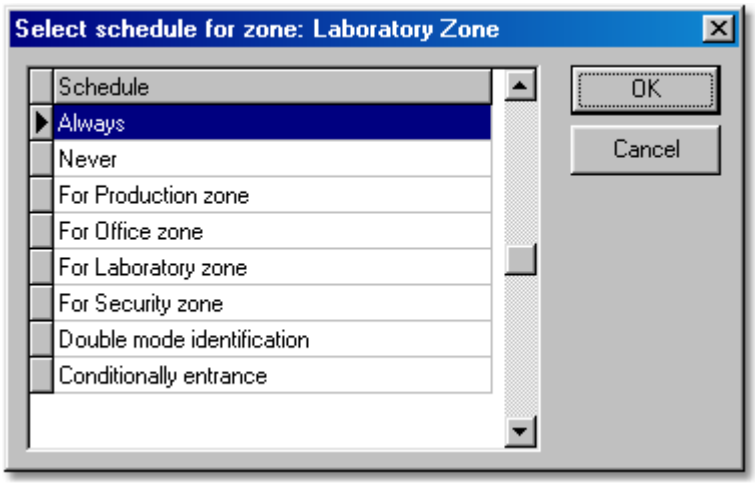
After adding new group should set properties.
Group properties

7.2 Group properties

Each group should have a specified time schedules for all zones and access rights to 16 floors.
To attribute defined schedules click on ***Edit*** in Group properties window and select time schedule.
Here the time schedules concerns group access to zones only.
PR Master enables operating with 16 floors (from 0 to 15). Floor access rights are not changeable.
Select available floors in a field below in the ***Group properties*** window to assign floor access rights for group



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

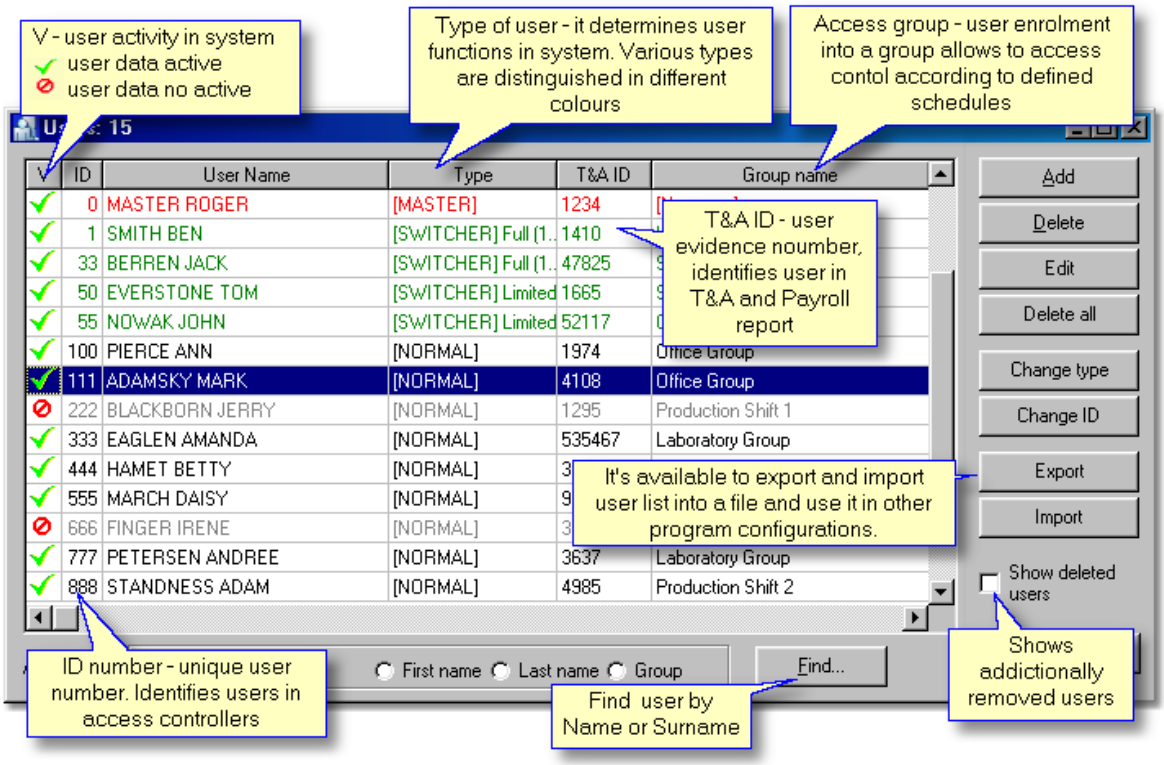


8 Users

In Roger Access Control System can be registered up to 4000 users. Every user owns 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 addiction to User Activity Period defining 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.
Commands to controller

To open list of users:

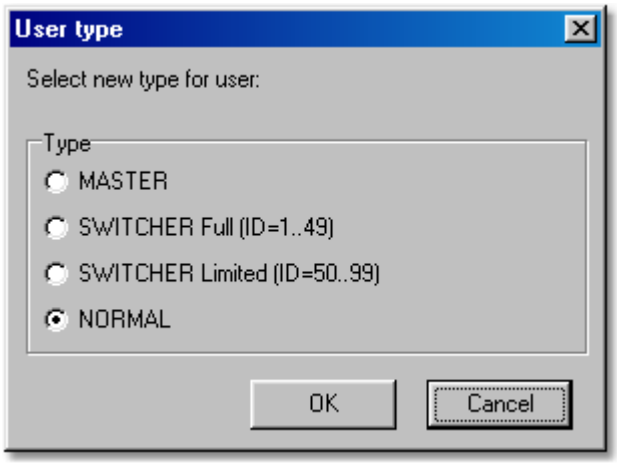
- select from main menu: ***Edit*** -> ***Users***
- or click on ***Users*** icon from operator tools



Note:
We can always change user settings using buttons: ***Edit***, ***Change type*** or ***Change ID***. Very useful feature of the program is ***Import*** and ***Export*** user table to a file. To do it click on Export or Import button on the right side. Program allows registering up to 4000 users.

8.1 Add users

To add new system user choose ***Add*** from Users window



Should select one of four types of users:

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

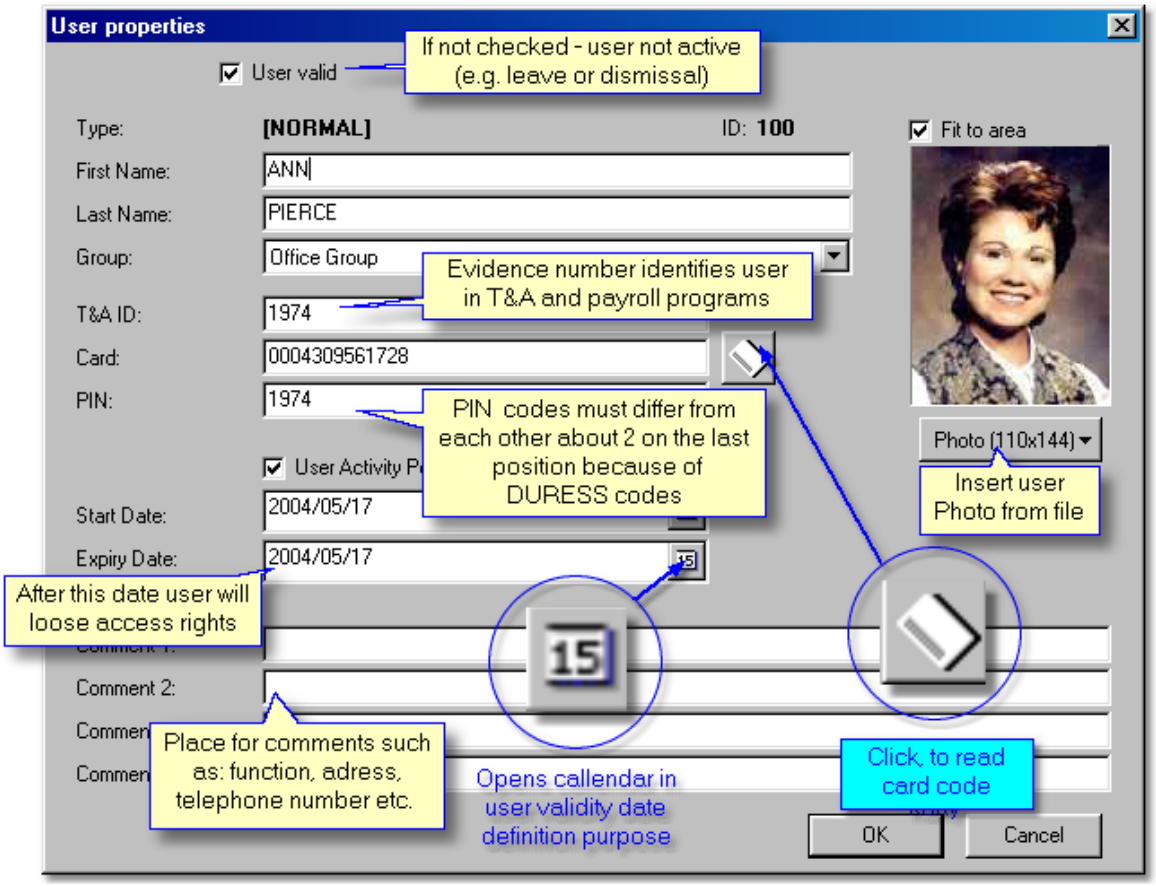
Note:
User with ID=1000 - 3999 (NORMAL) may be additionally defined as a Local SWITCHER on particular controller or controllers.

Once the type of user is selected, click ***OK***. User properties window will appear. User properties
Next, enter all necessary user data into gaps.

See also:
Advanced

8.2 Edit users

In User properties window fill all necessary information about user.



It's possible to enrol the user into defined access group now. In T&A ID, Card and PIN gaps enter data, which identifies user access card. Program enables to automatic read transponder code and write it into a Card gap.

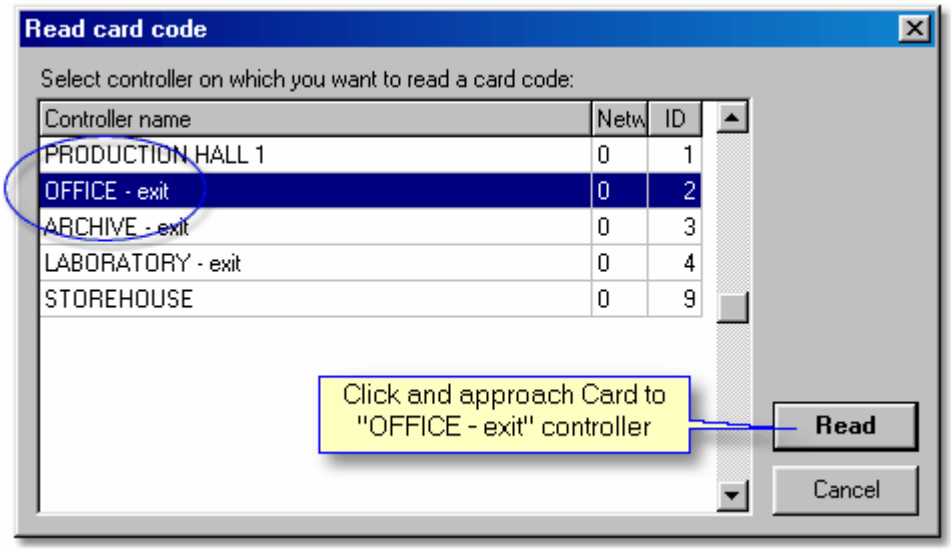
To read card code:

- Click on icon next to Card gap
- Select controller, which will be used to register the card Read card code
- Click ***Read*** button and then approach transponder to controller

Once, the card code is read properly, program returns to ***User properties*** window with filled gap. Optionally operator can insert identifiable photo for every user. To activate user in system assign ***User valid*** check box.

Note:
1. If user identifier is register for first time, carry out reading card code operation is necessary. Available transponders from other companies have printed numbers. However, there are not identification RACS codes.
2. Type of users SWITCHER Full and Limited can not be a local SWITCHER.

8.3 Read card code



Before you start card code reading operation, 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

In user removing from database it's recommended to follow these steps:

- read events stored in CPR buffer (main menu: ***Events*** -> ***Read CPR buffer(s)***)
- delete selected user from User list
- send configuration to the system (main menu: ***Commands*** -> Update system)

Note:
User removing from user list don't causes delete him from system database. It's possible to browse events in which he participate.

To view user removed from list should:
- choose ***Edit*** from main menu then select ***Uses***
- check option ***Show deleted users.***

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 performing specified actions by RACS in one-week period.

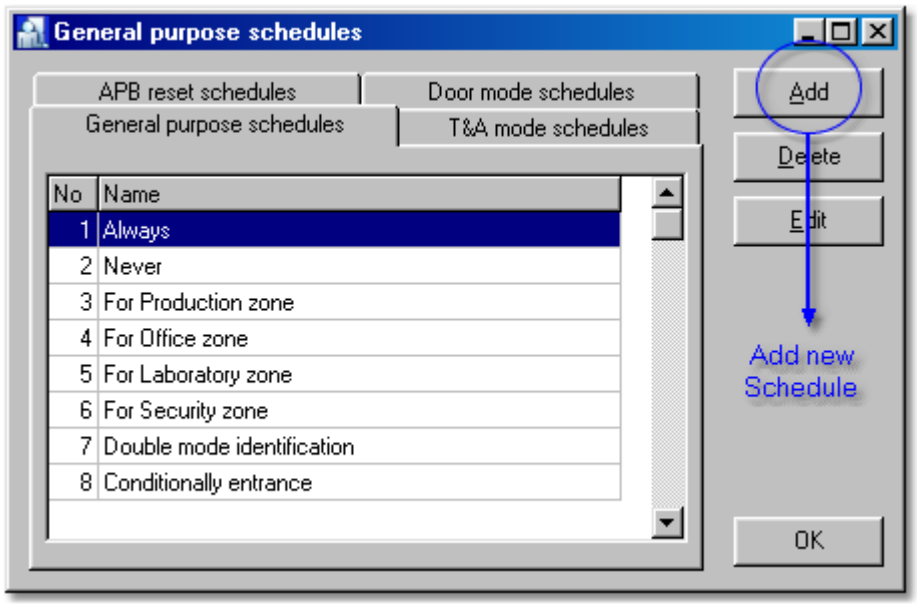
In PR Master are four types of Time Schedules:

- General purpose schedule
- Door mode schedules
- APB reset schedules
- T&A mode schedules

To define new time schedule should:

- click on ***Schedules*** icon from operator tools
- or select from main menu: ***Edit*** -> ***Schedules***

New window with four available tabs will appear, click one of them and click on ***Add*** button.



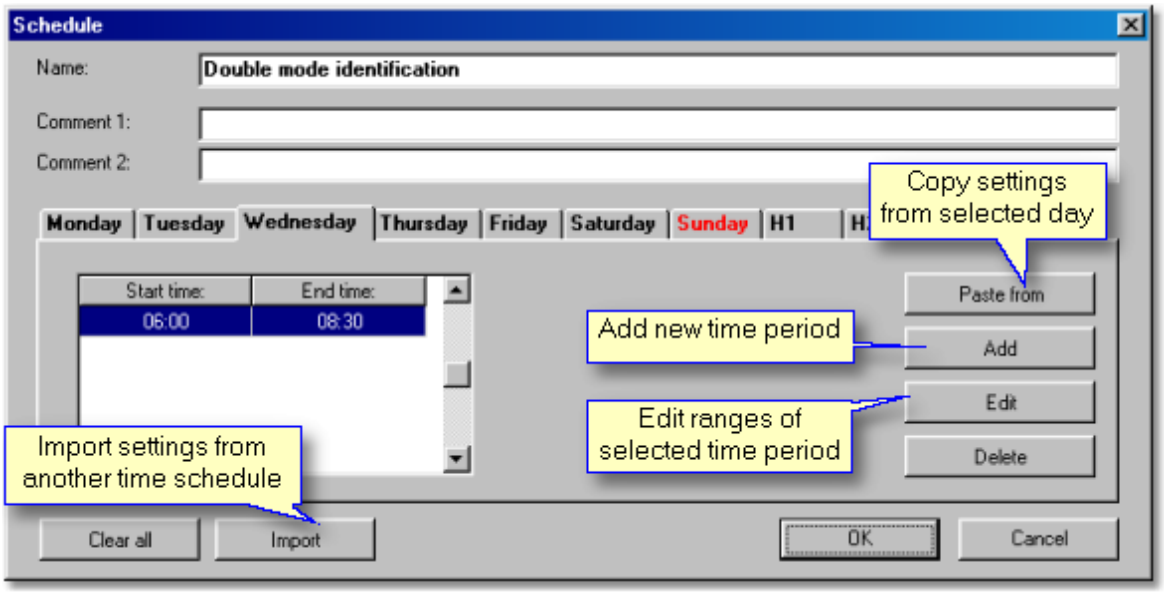
9.1 General purpose schedules

General purpose schedule may be dedicated to one or more functions of controller. For example, the same time schedule can be applied to control access, control output line or disable input line. In PRxx2 controllers is available to define 99 this type of schedules.
These schedules have not one specified purpose.

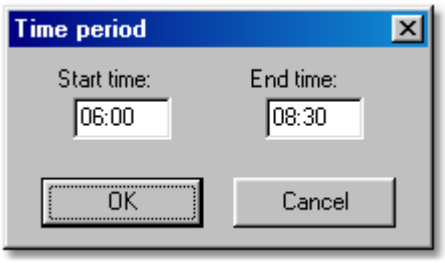
They can be applied to:

- Group access for defined zones
- Card+Card mode
- Card+PIN mode (double identification mode)
- Arm and unarm input lines
- Arm and unarm output lines
- SWITHERS access
- Conditional mode

By default there are two types of schedules: ***Always*** and ***Never***. To define new time schedule first enter a name.



Choose appropriate day of week, click on ***Add*** button to specify time period(s).



Once we want to utilize the same period for another days or holidays (H1-H4) we can use ***Paste*** from button panel. Click on ***Paste*** from and choose day you want to repeat. We can also import time periods definitions from existing time schedule, but of the same type only (in this case General purpose schedule). It's always possible to edit or delete time schedule.

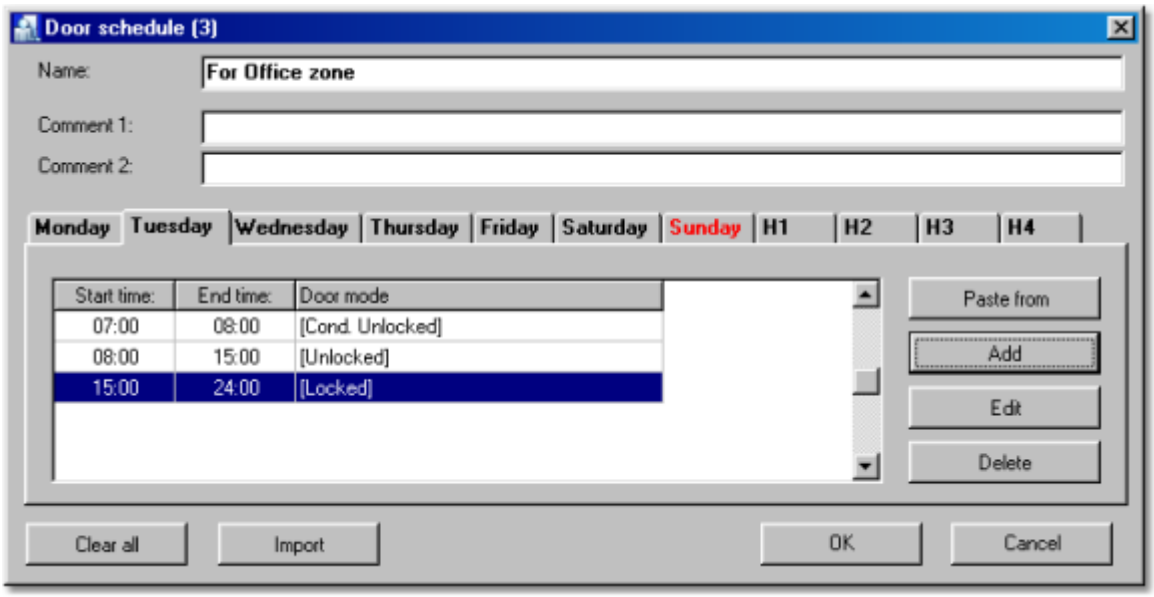
9.2 Door mode schedules

Door mode schedule allows to automatic controller switching between door modes. To define door mode schedule first choose day, specify a time period, then select an appropriate door mode for it. In time between defined periods a controller automatically returns into ***[Normal]*** Door mode.

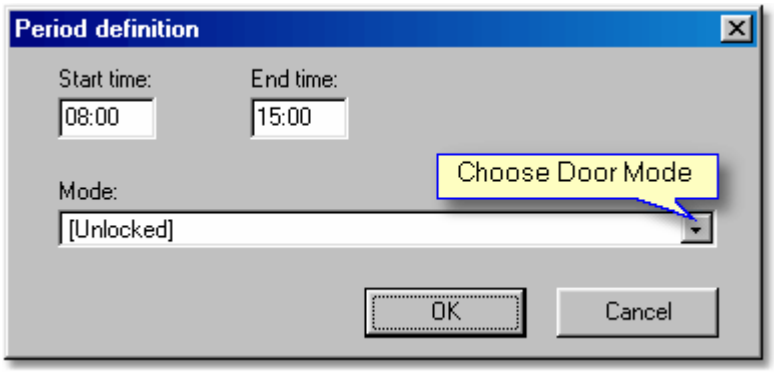
Defining this schedule is carrying out almost just like in case General purpose schedule.

For each time period can specify Door mode:

- ***[Unlocked]*** – during time schedule door always unlocked
- ***[Locked]*** – during time schedule door always locked
- ***[Cond.Unlocked]*** – conditionally unlocked, door locked until first authorised access granted



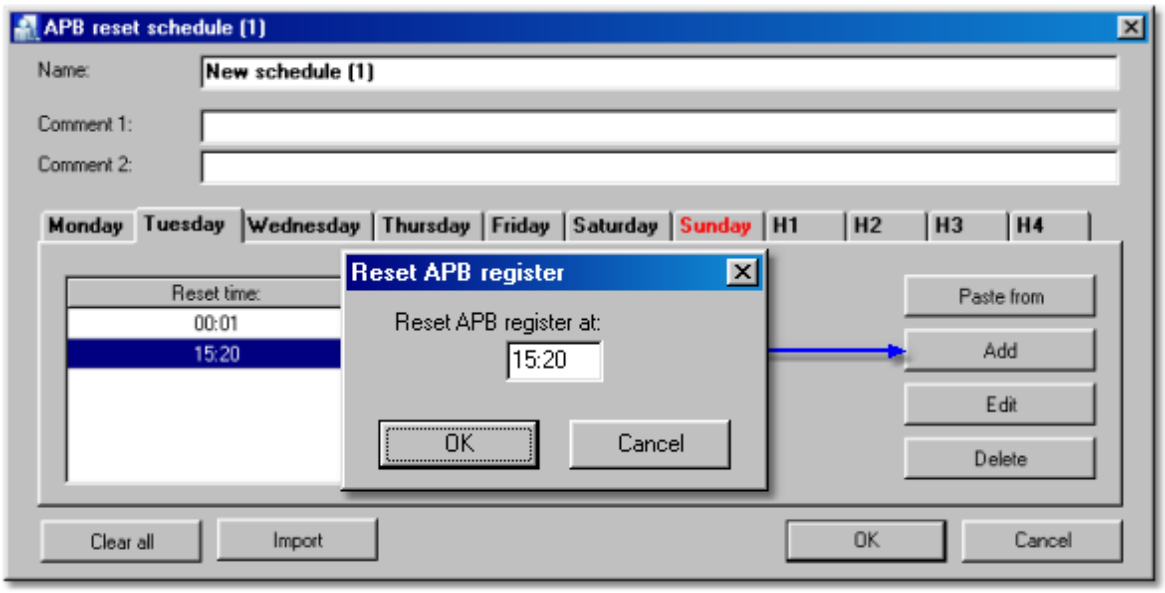
Note:
In undefined time period door are in [Normal mode] - door locked, unlock after valid user authorization.



9.3 APB reset schedules

APB reset schedules are used for Anti-Passback registration reset. Just after APB reset each of users registered in controller owns undefined status in APB registry (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 first access is granted the controller starts to exact APB rules.

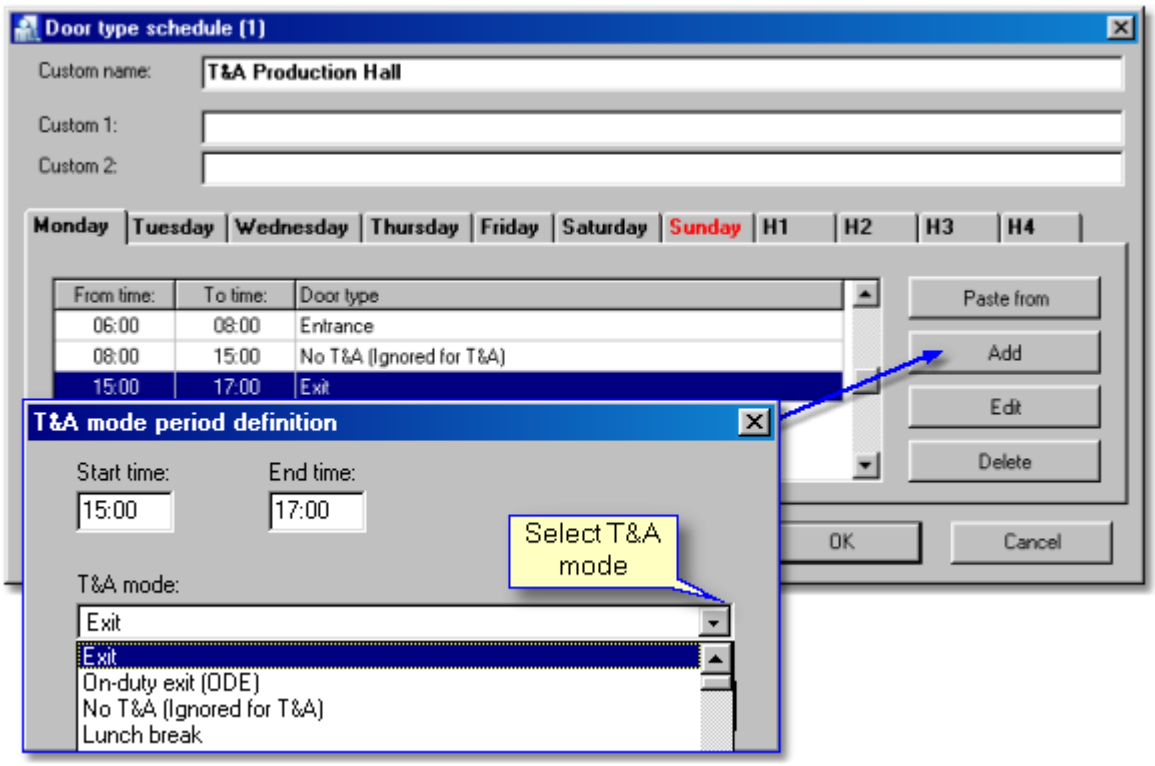
Defining this schedule is carrying out almost just like in case General purpose schedule but only Reset Time is set.



9.4 T&A mode schedules

T&A mode schedule allows to automatic controller switching between T&A modes. Time schedule consist of time periods definitions and related T&A modes.
It's available to use one identification point to varied types of T&A registration. In case when T&A mode is switched from the controller keypad or Input line it's possible to secure this feature with password. To set password choose Options in Controller properties window.
User is allowed to define password for "momentary" T&A mode and "stable" T&A mode as well.

Defining this schedule is carrying out almost just like in case Door mode schedule but T&A modes (Entrance, Exit, On- duty exit etc.) are set.



Note:
Program PRMaster enables defining other T&A registration types adjusted to own necessities. To define other T&A registration mode choose Tools -> T&A modes.
Tools [T&A modes]

10 Zones

Zone - area of network, in which are controllers. All system is divided on zones. Every controller should be related to defined Zone. After adding new controller to the system its zone is default.

To add the controller to selected zone:
choose ***Network*** from the operator tools -> ***Edit*** -> General

Note:
"Zone" concept is not equal with "Area" concept.

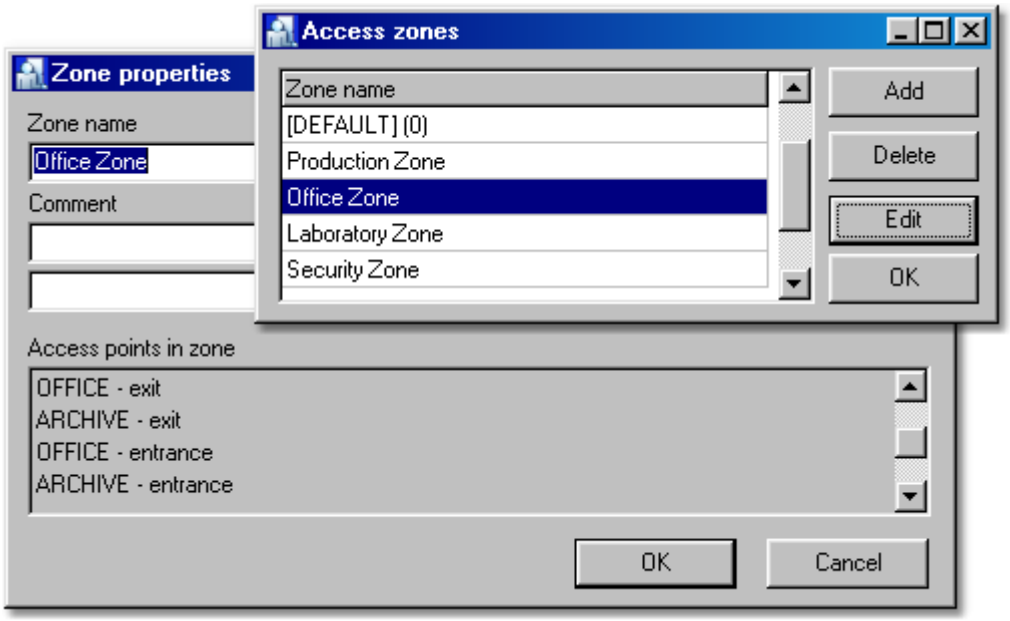
See also:
Add access zone
T&A Areas

10.1 Add access zone

Program enables access zones defining, which are associated with appropriated controllers. ***Default (0)*** is a predefined zone, it's not editable and removable.

To add new zone click on 

from the operator tools or from main menu ***Edit*** -> ***Zones***.



See also:

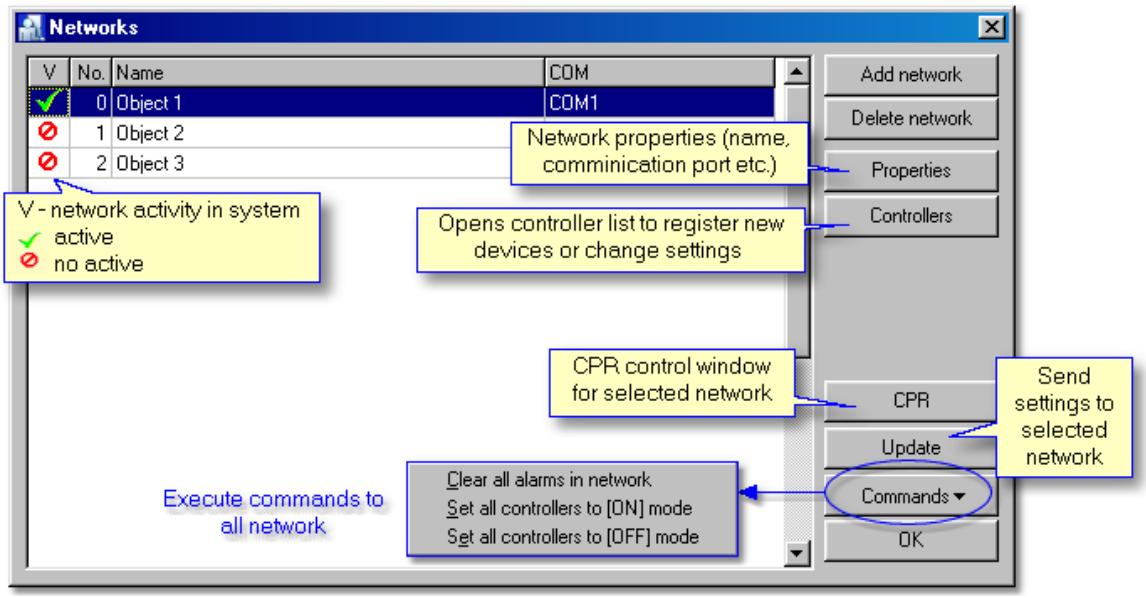
Zones

11 Networks

Roger Access Control System consists of control panels (max 10), PRxxx controllers and PRT terminals. All of control panels can operate 32 access controllers. Network called also Subsystem is composed of control panel with controllers and terminals. System includes all networks (subsystems) with communication interfaces (UT-2, UT-3, UT-4) and PR Master 4.0 software on PC.

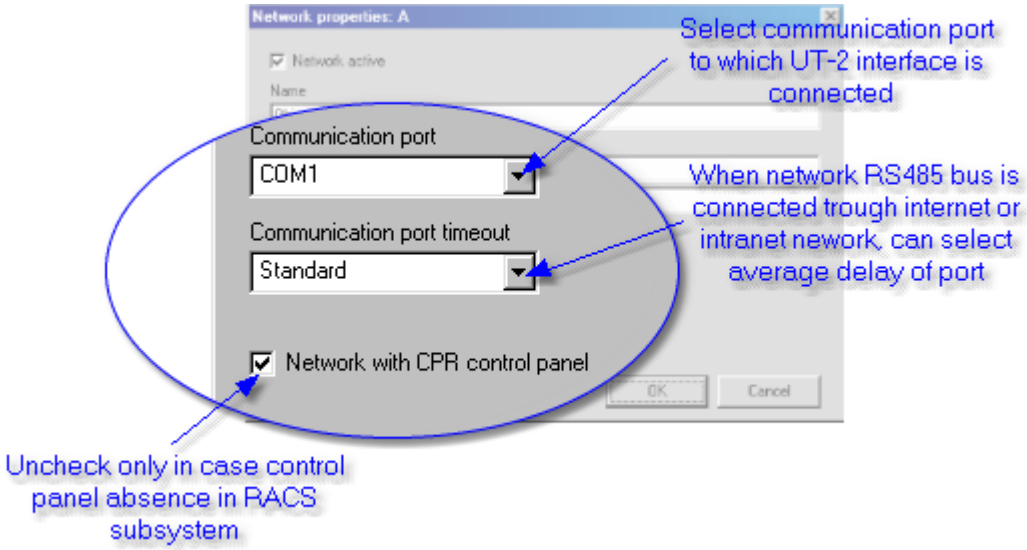
See also:

Adding new network



11.1 Network properties

To create new subsystem click on from operator tools or choose from main menu ***Edit*** -> ***Networks***. Next should add new Subsystem. To do it click on ***Add Network*** button and type name of network. Select ***Communication port*** (COM) where network is connected to RACS communication bus. Every subsystem requires own free communication port and communication interface UT-2.

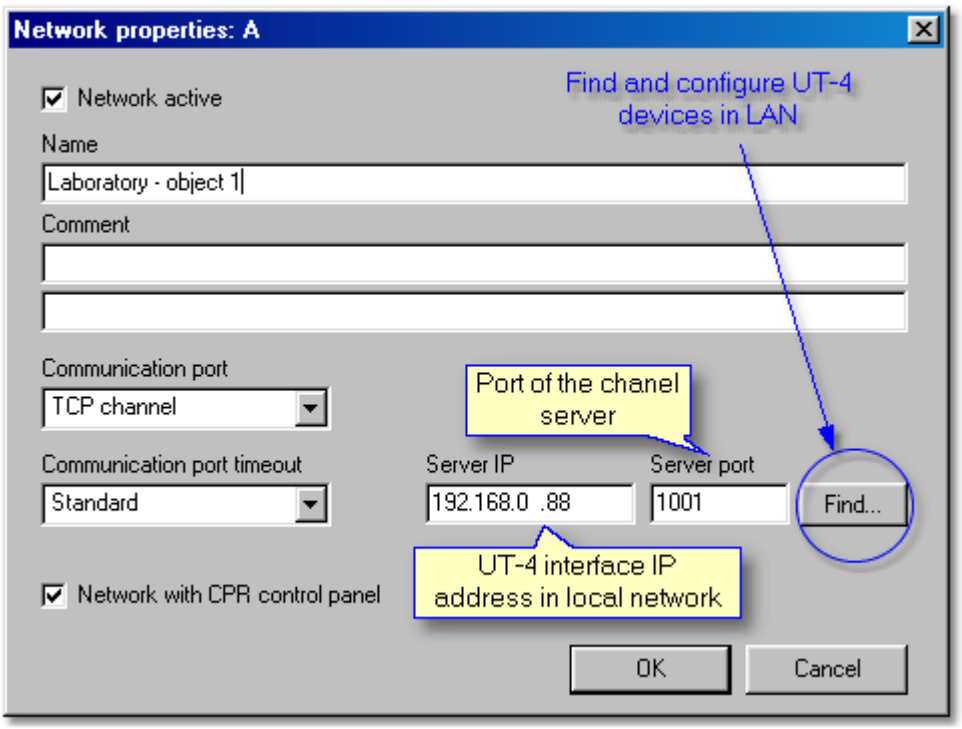


Should remember to uncheck box ***Network without CPR control panel*** in case absence of this device.

In special case we can apply UT-4 communication interface. Device enables to connect RS485 bus to computer local network (LAN). When UT-4 is supported should select TCP channel from ***Communication port*** dropped down menu. Next should specify average delay of COM port in milliseconds.
Now enter IP address of UT-4 interface, which identifies it in local network and ***Server port***. If you don't know the rules of IP device addressing, should read IP address of computer with installed PR Master 3.9.3 software.

To read IP address of the computer should:

- open ***Network properties*** or ***Network*** window
- select TCP/IP protocol from network components (network card)
- click on ***Properties***



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:
UT4 configuration
System without CPR

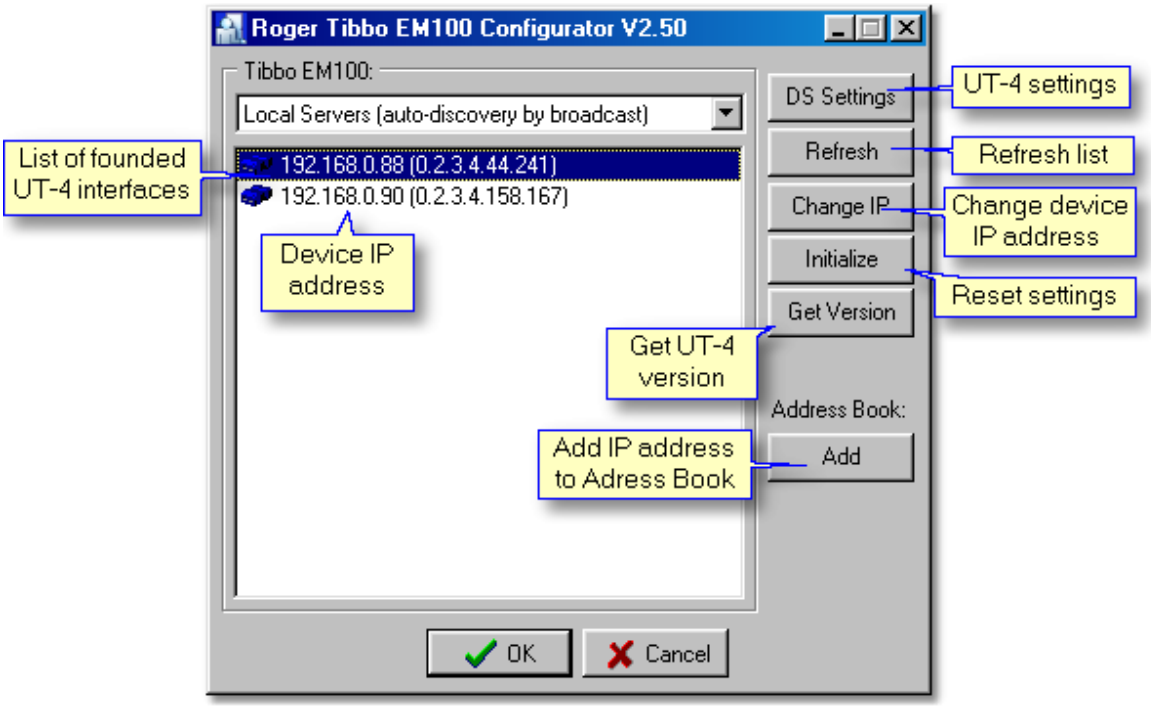
11.1.1 UT-4 configuration

In UT-4 configuration window operator is allowed to change interface settings. In case when IP address will be the same like other IP address should change it immediately.

There are two types of device searching:

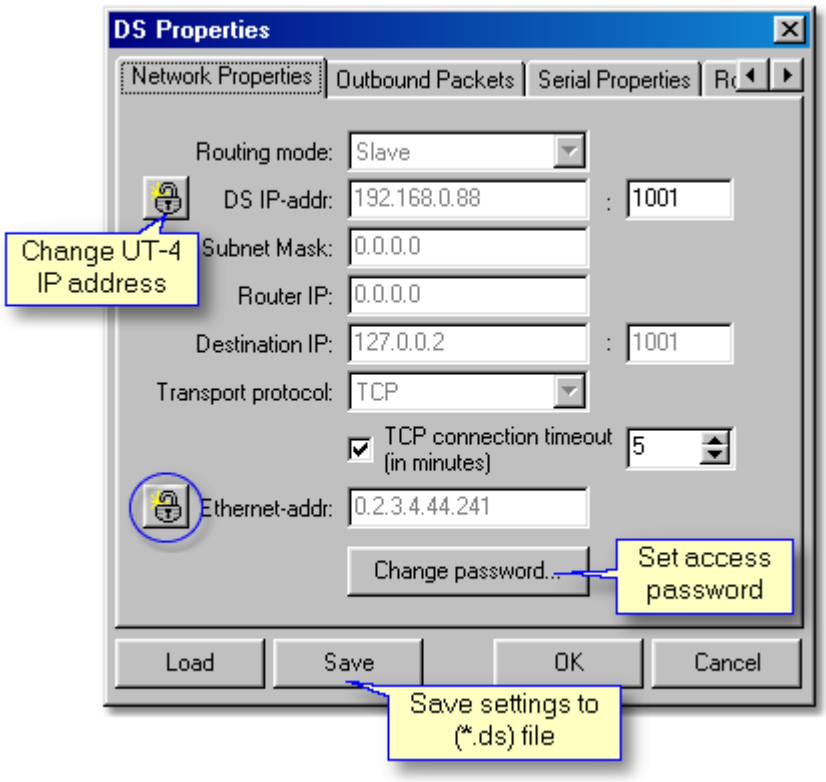
- ***auto-discovery by broadcast***
- from the ***Address book*** (should add IP addresses firstly)

Initialize option resets settings and sets all to default.



11.1.1.1 Network properties

Feature enables to change Network Properties. Access to UT-4 settings 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.

11.2 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. Suspended mode is mainly used to tests or for conservation purposes, for example when the controllers flashing operation is being carried out.

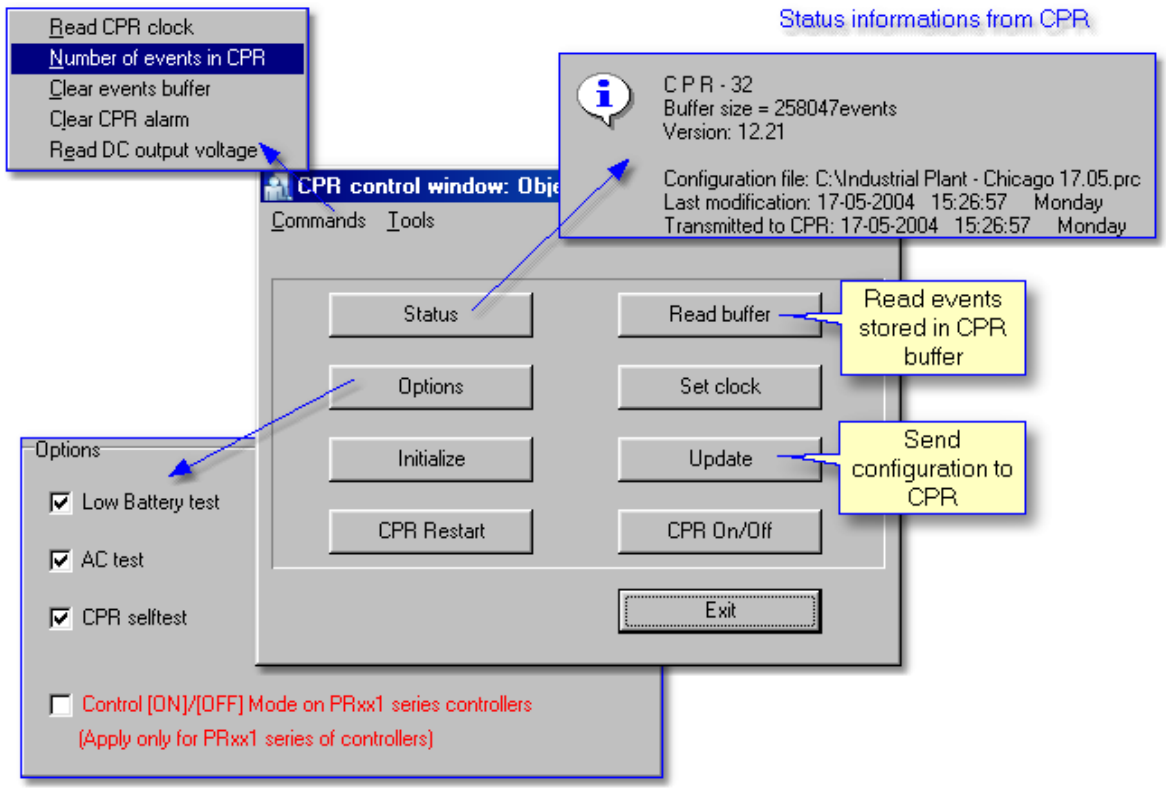
In CPR control window are available commands and functions:

- Status - information of control panel are showed (type, buffer size, config file name, last modification etc.)
- Options - allows to switch on/off varied CPR tests which are active during CPR's work
- 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 and append it to the system file
- Set clock - synchronize system clock according to the PC clock
- Update - send configuration to the CPR
- CPR On/Off - switch to on/off mode

Note:
1. Initialize operation is usually carried out when CPR is completely deprogrammed or settings error occurred. Problems with CPR may happen in result of an AC lost or failure of battery, which sustain CPR memory. It's possible to initialize CPR manually.

2. In case when control panel is in OFF mode for a long time, it's necessary to read events stored in controllers buffers. To do this execute 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.

Accumulator test

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

Note:

Refer to PRxx1 access controllers CPR perform also other functions. It controls user system rights and registers events from controllers of this type.

11.3 Send network configuration

To send configuration settings to whole subsystem (network) should:

- Click on 

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

Subsystem must be active. Performing this operation causes configuration sending to control panel and all access controllers in selected network. We use this command, when we change controller(s) settings and want to transmit it only to selected subsystem.

Here are commands, which are sending to all the system: Commands

11.4 Update configuration of CPR

To perform updating of CPR configuration should:

- Click on 

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

Configure CPR in Network

11.5 Controllers

Controller is an autonomic device, which controls one access point (one-way or two-way). In case two-way access point controller is connected with additional identification terminal.
In PRxx2 is available to register up to 4000 users. In older types of controllers (PRxx1) maximal number of users is 1000. Once the configuration settings with users list which exceeds 1000 are send, users from ID=0 to ID=999 in controllers memory will be exist only.

Controller reads card or PIN-code and realizes identification. In controllers with keypads it's possible

to apply double identification mode (Access) Card+PIN, which obligate users to use both method for identification. Sequence is no matter.

Controller's memory includes also access groups' information. In system is available to register 127 access groups (PRxx2). For older types of controllers (PRxx1) there are only 31.
In case no CPR or it's OFF mode, PRxx2 controllers can record all events. PR302 devices have memory buffer which can collect 48000 events, PR402 - 32000 events.

Access controller owns its default T&A mode (Time and Attendance). Every access granted event is registered with appropriate T&A mark code. You can change T&A mode in Options.

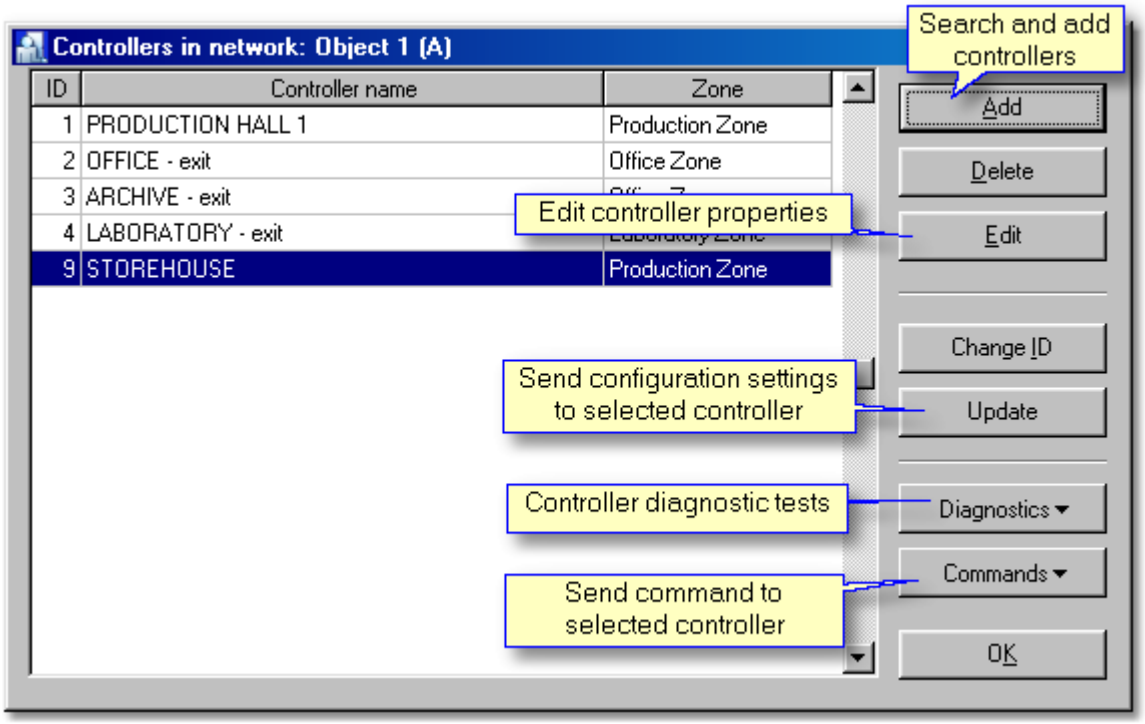
Controllers is equipped with four input lines (IN1, IN2, IN3) and three output lines (IO1, IO2, REL2).

See also:
Add controllers

11.5.1 Add controllers

Add controllers connected to one subsystem using ***Add*** button.

Window with controllers in network:



When you click on ***Add*** button program begins to search controllers connected to subsystem communication bus.
Searching process ends with message "End of controllers searching".

Every controller has individual ID number (00..99). In case when program find device with the same

ID, error message will appear!
Therefore, before adding new controllers to the program database, you should set different ID numbers for devices.

After successful searching process it's possible to change ID (***Change ID*** button).

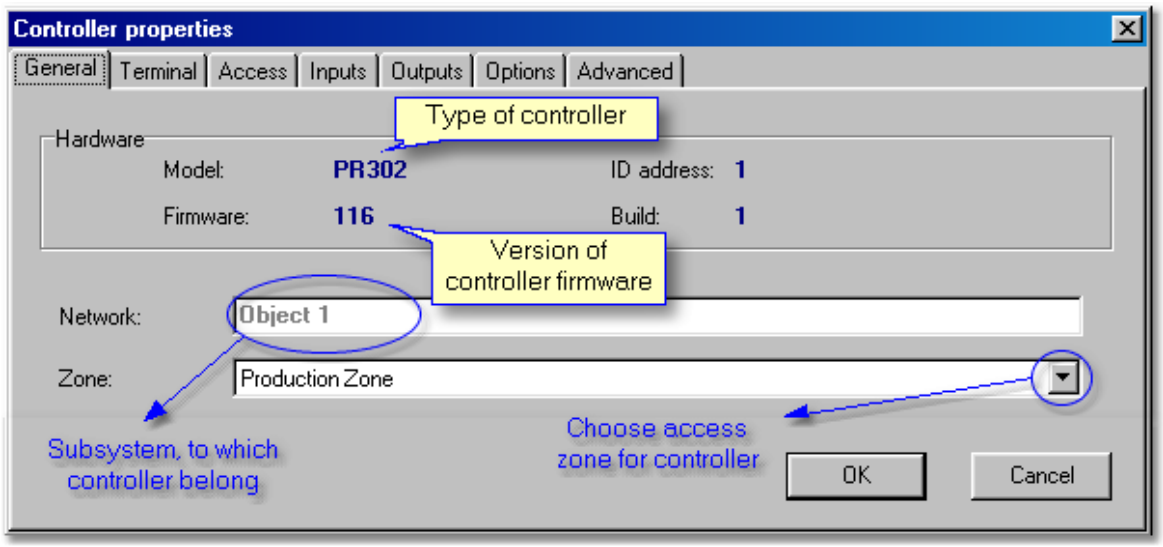
11.5.2 Controller properties

To open controller edit mode click on ***Edit*** button from menu in Controllers window.
Controllers in network.
In controller properties window are available six tabs to choose.

- General
- Terminal
- Access
- Inputs
- Outputs
- Options
- Advanced

11.5.2.1 General

Here are information about: model, controller ID address, Firmware version and build, name of network and Access Zone. In this window you should select zone to which controller belongs.



11.5.2.2 Terminal

In Terminal window you are able to give ***Names*** for terminals, and specify ***Default T&A mode*** for Time&Attendance registering. Moreover PR Master allows to choose type of terminal which is connected to logical device.
Select one of 15 available options in the ***terminal type*** tab:

- PRT series reader (PIN/Card) or (User ID),
- Wiegand 26bit, 34bit, 42bit, 66bit (PIN reader), (Card reader) or (User ID reader),
- None.

Operation with Wiegand readers

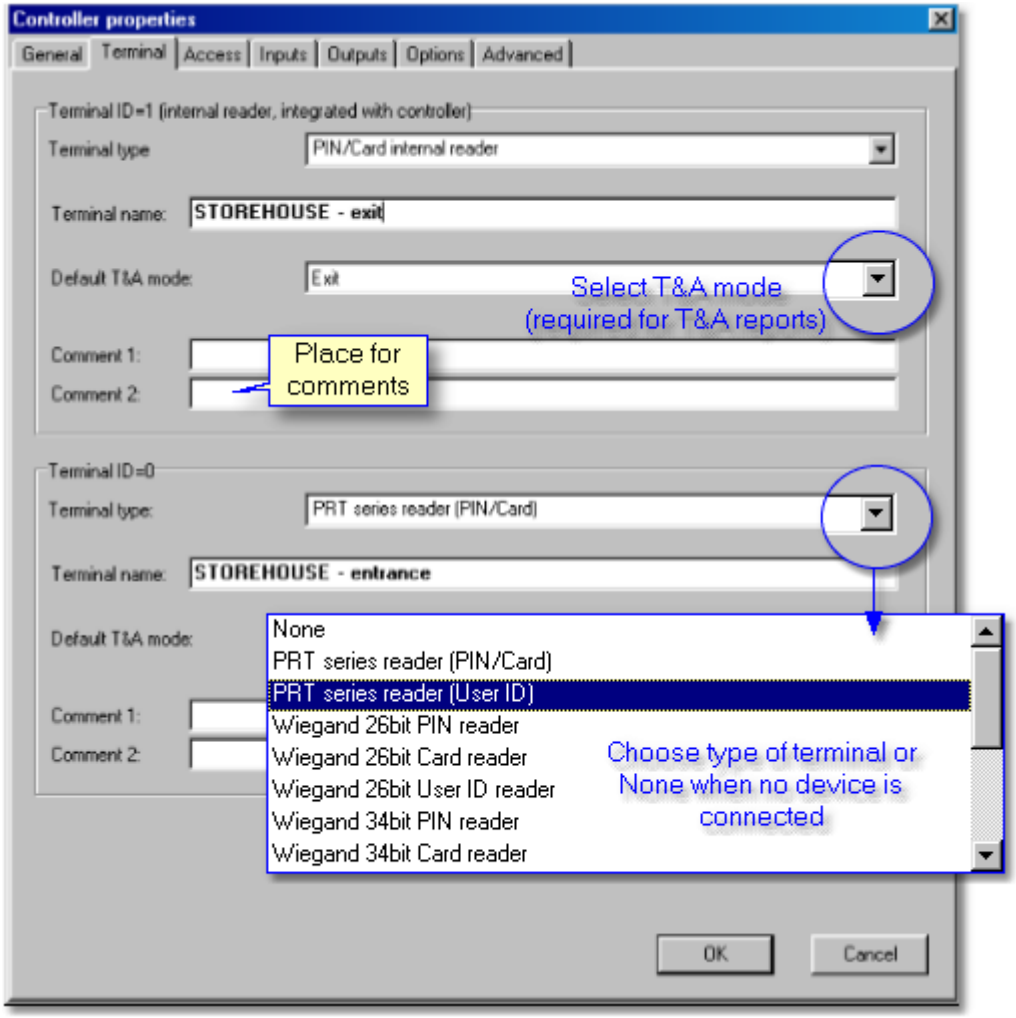
Wiegand reader is connected to Clock and Data lines instead of standard PRT terminal(s). When controller is configured for operation with Wiegand User ID reader it interprets transmitted digits as ID number of user which has performed identification, when is set to Wiegand PIN reader controller interprets 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.

In case the terminal is not connected you should select ***None,*** using this function can also disable internal reader (integrated with controller).

Predefined (often used) T&A registering modes:

- Entrance
- Exit
- On-duty exit(ODE)
- no T&A (Ignored for T&A)

Program enables defining specified T&A modes adapted to own needs.



See also:
Glossary
T&A modes

11.5.2.3 Access

In Access tab specify door rely mode, default user identification mode and choose schedule for door mode, Card+Card and Card+PIN. It's allowed to select own specified schedules.

Door Rely

Door lock can be released when authorized:

- when user enter its identifier,
- by remote command from PC,
- by exit button which can be connected to controller input line.

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 ***OFF*** mode, this can be achieved by
Access disabled in [OFF] mode 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 [OFF] mode will arm alarm system or alarm
zone and automatically will disable access to premises for all users regardless of access settings.

Additional schedules:

Door mode schedules

Controller may be set to few modes (Door Modes) which determine what manner door lock is controlled:

- **Normal Door** lock is activated after each successful identification.
- **Unlocked Door** lock is continuously energized, door is continuously open.
- **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.

 **Note:**
As a default door lock stay in Normal Mode but it can be switch to another mode by Door Mode Schedule or by remote command from PC software.

Identification Modes

Controller enables user identification in two different modes:

- **[Card/PIN]** Controller requires Card or PIN to be entered for successful identification.
- **[Card + PIN]** Controller require Card and PIN to be entered for successful identification, no matter what
  sequence Card then PIN or PIN then Card.

Installer may define Default Identification Mode of controller which specify normal identification method for each type of users
(Master, Switcher and Normal). For example installer may define that default identification mode as follows:

- for Master user: [Card+PIN]
- for Switcher users: [Card/PIN]
- for Normal users: [Card/PIN]

Normally, only Master user will be obliged to use Card and PIN, other types of users may use only one method (Card or PIN). In

some periods of day or week controller can be switched to [Card+PIN] mode according to [Card+PIN] Schedule. This schedule
specify time periods when all types of users must use Cards and PINs together. There are two predefined schedules, which can be
set for [Card+PIN] Schedule: Always and Never. When Always schedule is selected controller will always require Card and PIN,
when Never schedule is selected, controller will always stay in Default Identification Mode.

[Card + Card] Mode

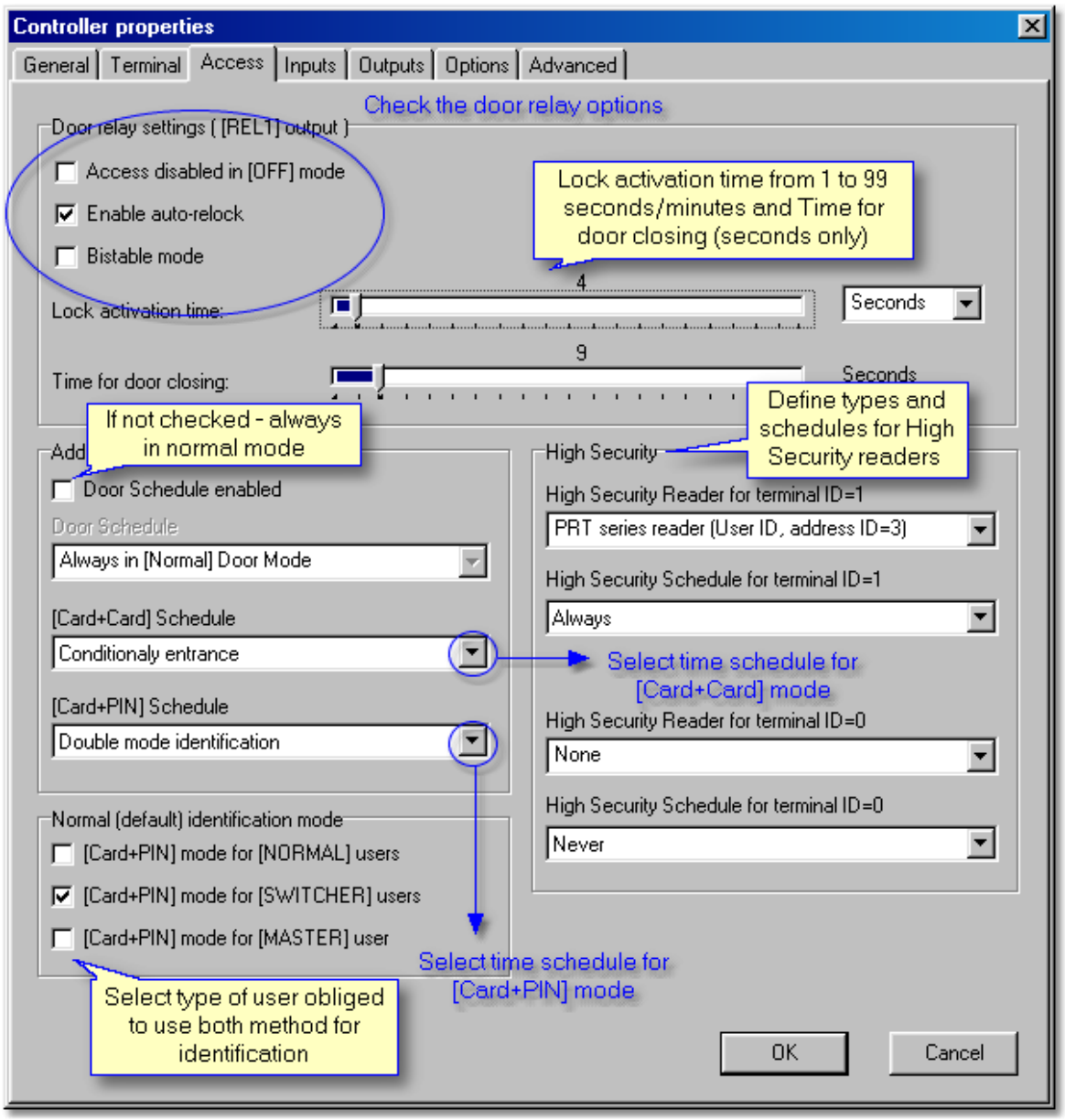
When this mode is active two authorized person must use his/her identifiers then controller will grant access to controlled door.
This mode can be controlled by [Card+Card] Schedule, selecting schedule Never will permanently disable this mode where
schedule Always will permanently activate it. When together 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.

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) .

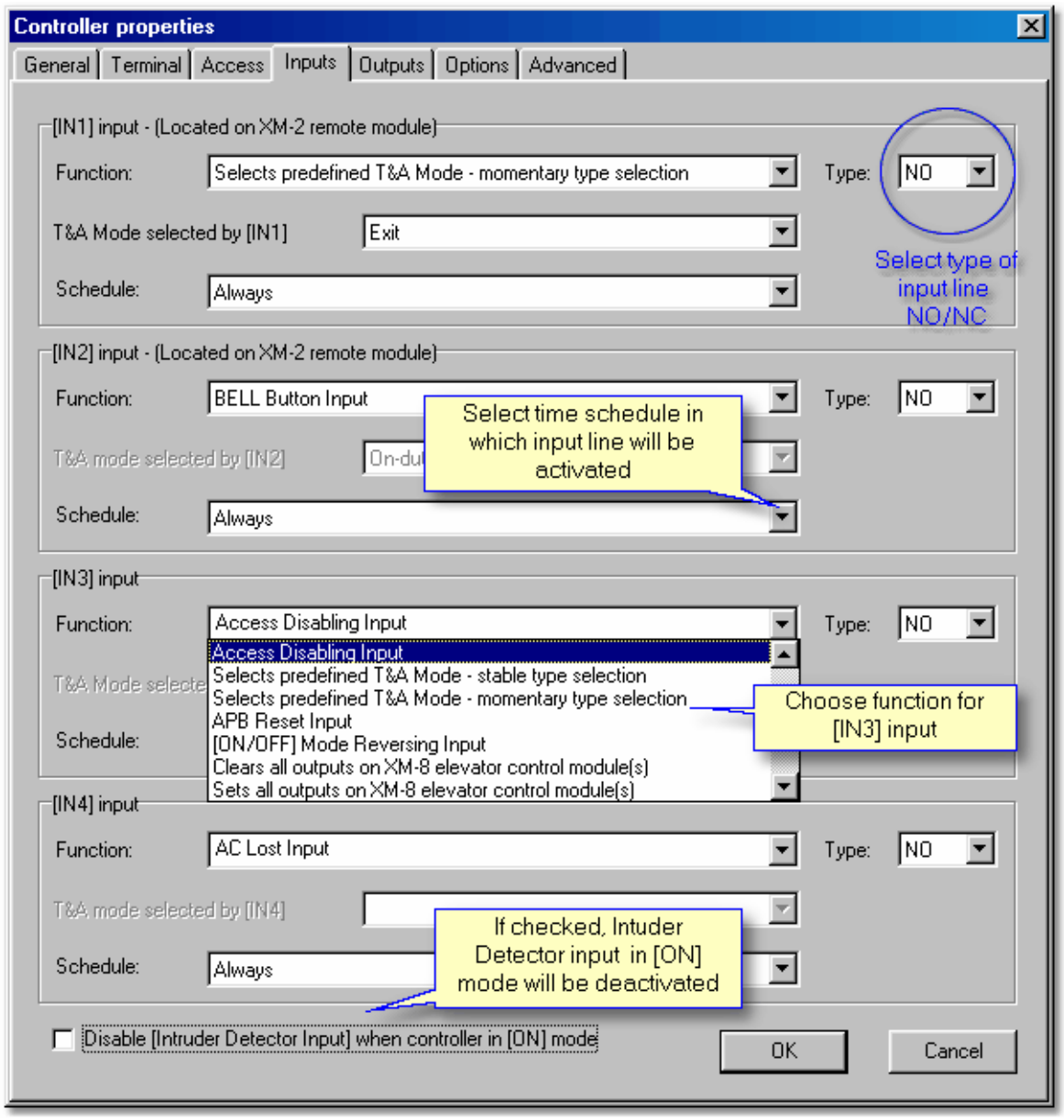
See also:

General purpose schedules



11.5.2.4 Inputs

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:

- **Input ignored** - selecting this function will disable decoding of this input, function can be used for temporary
  input deactivation without disconnecting it from triggering source.

- **Door contact input** - input is dedicated for contact that will indicate that door is open. Input activation generate
  [Door opened] event, input deactivation generate [Door closed] event.

- **Exit button input** - 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 button connection.

Activation/deactivation of input generate [Exit button ON]/ [Exit button OFF] event.

- **[On] mode reversing input -** every activation of this input causes switching [ON/OFF] mode of controller. When this function is selected other methods of [ON/OFF] mode control will not be forbidden. Input activation generates [Switch controller to ON/OFF mode] event.

- **[ON] mode control input** - activation of this input will force controller to [ON] mode, as long as input is triggered controller will remain in [ON] mode. Only one input on controller can be configured to this function. When such a function is selected any other methods of [ON/OFF] mode control will be forbidden.

- **AC lost alarm input** - input is dedicated to be connected to output line which will indicate that AC supply of power
  supply unit is lost. Some brands of power supply are equipped with such an 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.

- **Low battery alarm input** - input is dedicated to be connected to output line which will indicate that reserve battery is in
  low condition. Some brands of modern power supply are equipped with such an 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.

- **Bell button input** - input is dedicated to be connected to contact which will indicate that somebody want to enter premises. After input is triggered controller generate [BELL button ON] event, when line returns to normal condition controller generates [BELL button OFF] event.

- **Tamper loop input** - input is dedicated to be connected to tamper contact that 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.

- **Intruder detector input** - input is dedicated to be connected to some kind of intruder detector (e.g. PIR), which will indicate intruder 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 by bypassed in [ON] mode, this can be achieved selecting [Disable Intruder detector in [ON] mode] option.

- **[ON/OFF] mode reversing input** - input is dedicated to be connected to pushbutton which when pressed will alternate ON/OFF mode of controller to opposite condition (from [ON] to [OFF] or reversibly).

- **Access disabled input** - input is dedicated to be connected to some kind of switch which when activated will disable access to controlled door, besides this activation/deactivation of input result in generation of [Access disabled input ON]/ [Access disabled input OFF] event.

- **T&A mode setting input** - input is dedicated to be connected to some kind of pushbutton which when pressed will switch controller to specified T&A mode. Installer for every input line declares the T&A mode, which will be set after input is triggered, individually. The new T&A mode is set for undefined time, till next input activation or till relevant schedule will force new T&A mode.

- **APB reset input** - input is dedicated to be connected to some kind of pushbutton which when pressed will reset
  APB register of controller. Any time input is activated an internal APB function register of controller is initialized (cleared) and [APB reset] event is generated.

- **Clears all outputs on XM-8 elevator control module** - Input is dedicated to be connected to output line (contact) which when triggered will clear all outputs on XM-8 elevator control module(s).

- **Sets all outputs on XM-8 elevator control module** - 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 of function name and function code. Function name can
be used to distinguish purpose of input e.g. Guard Tour Button, Alarm button, Rescue button, each time input is activated system
will register events which consist from function name and ON or OFF mark which specify whether the input line was activated or
deactivated.

11.5.2.5 Outputs

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 nad IO2 can be assigned during controller's setup.

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.

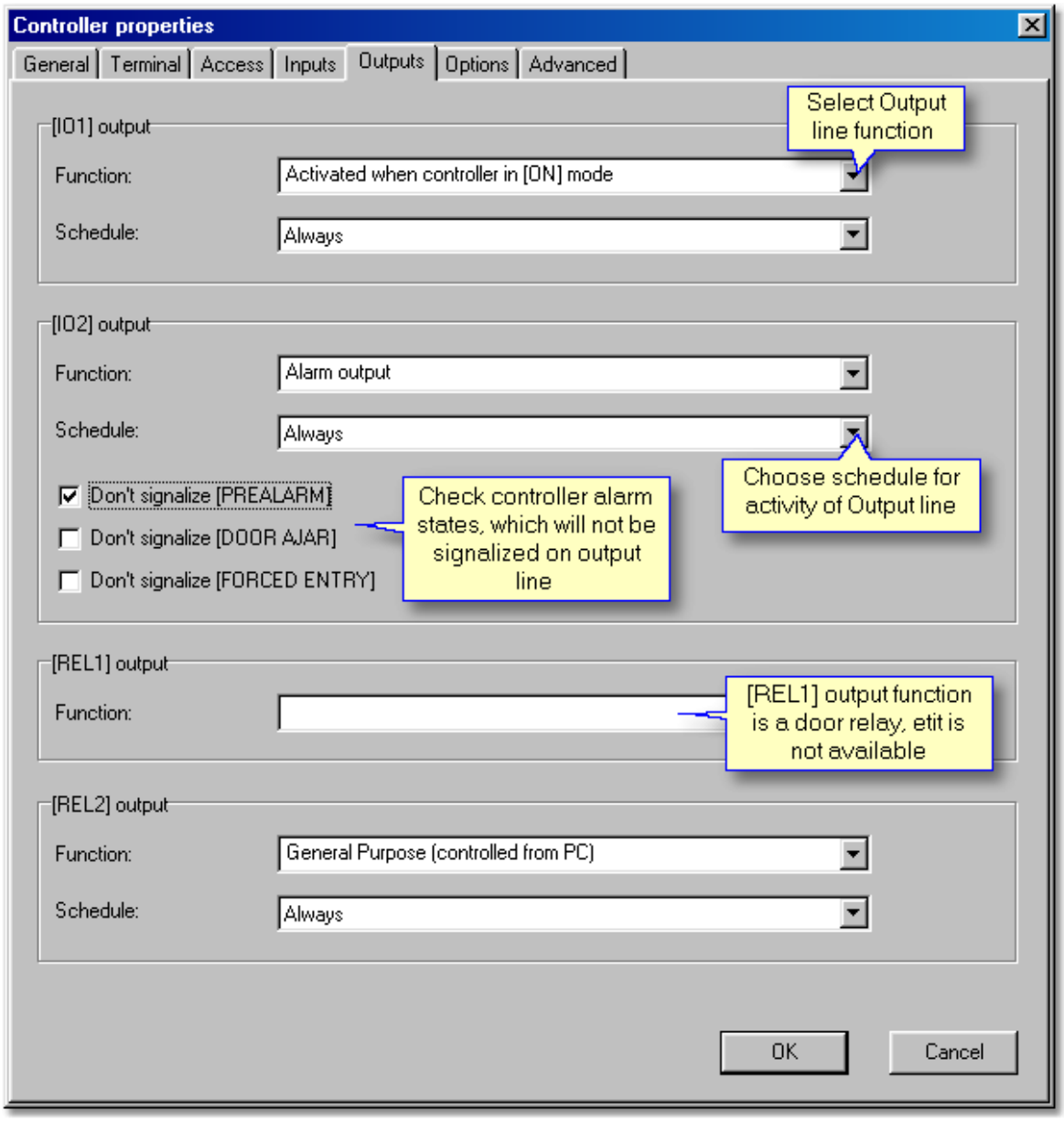
Relay output (REL1)

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.

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.



Each output line may be configured to some function listed below:

- **Alarm output** - output is activated when at least one alarm situation occur. There are three different alarm situations that can be signalized on this output: [PREALARM], [DOOR ALARM] and [FORCED ENTRY]. Installer may select which alarm output should output line signalize.
- **General purpose output** - output is activated/deactivated through interactive command, which can be sending from PC.
- **Activated when controller in [ON] mode** - output is activated when controller turns to [ON]

mode and remain active as long as controller remain in this mode.

- **Activated on [Access granted] event** - 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.

- **Activated on [Door open] event** - output is activated after controller detects that door became open and remains active as long as door is being open.

- **Activated on [Access denied] event** - output is activated for period about 2 seconds after controller denies access.

- **Activated by schedule** - output is activated/deactivated according to selected schedule, no other method may change
condition of output line.

- **Activated by schedule or PC command** - output is activated/deactivated according to selected schedule or interactive command from PC, both control methods have the same priority.

- **Activated when identification on terminal ID=1** - output is activated when controller grant access on terminal ID=0, output line remains in active mode until identification on terminal id=0. This type of output is used to operate "Tripod" gates, where two-way control is necessary.

- **Clears all outputs on XM-8 elevator control module** - Input is dedicated to be connected to output line (contact) which when triggered will clear all outputs on XM-8 elevator control module(s).

- **Sets all outputs on XM-8 elevator control module** - Input is dedicated to be connected to output line (contact) which when triggered will set all outputs on XM-8 elevator control module(s).

11.5.2.6 Options

Controller can enable/disable following options:

- **ON and OFF Mode schedule** - according to defined time schedule: ***Edit*** -> ***[ON/OFF] Mode Schedules***
- **Disable DURESS Codes -** using Duress codes on controller or terminal keypad is not available.
- **Bad card timed lock-out -** 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.
- **Switcher under control of group schedule -** allows using SWITCHERS identifiers only where his group has access rights.

ON and OFF Mode of Controller

PRxx2 controller may stay in [ON] or [OFF] mode, both modes are signalized on bi-colour LED marked ON/OFF. The current mode
(ON or OFF) of controller may be optionally signalized on dedicated output line, when controller is switched from ON to OFF mode

(or reverse direction) output line will follow these changes.

Generally the ON/OFF modes are dedicated for auxiliary control purpose e.g. light control, copy machine control etc. but in most cases they are used for integration of access control system with intruder alarm system. Connecting output line which follows ON/OFF mode to adequate input line of Intruder Alarm Panel user may arm or disarm alarm system in required room or zone, in this case when controller goes to OFF mode (ON/OFF LED set to red) this will automatically arm adequate alarm zone and vice verso when controller goes to ON mode (ON/OFF LED set to green) this will automatically disarm adequate alarm zone. The access to room/zone can be temporary blocked when controller stay in OFF mode, this can be achieved by option [Access disabled in OFF mode].

An [ON/OFF] mode of controller can be controlled in few listed below ways:

- manually, by use of SWITCHER or MASTER card/PIN,
- by external input line - ON/OFF Mode Reversing Input,
- by external input line - ON/OFF Mode Control Input,
- by time schedule (see [ON/OFF] Mode Schedule),
- remotely by interactive command from PC.

Note:
Combining different method of [ON/OFF] mode control together with some other options installer may obtain few additional
effects.

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 signalization can be deactivated by PR Master software.

Note:

To disable DURESS codes in system choose from main menu: ***Tools*** -> ***Options*** -> ***Misc*** -> [***Disable DURESS codes***].
Misc

Events

- Disable [RTE] event - disables generation of [Request to exit] event
- Disable [Forced entry event] - disables generation of [Forced entry] event

T&A Registration

Access controller offers T&A registration, which further can be used for calculation of total job hours. Each "Access granted" event, which occurs on controller, has a "T&A mark" which specifies what kind of entry/exit has been registered. Controller „T&A Mode" determines the actual type of

registration for T&A purposes. Entry, Exit, On Duty Exit or Ignored for T&A are predefined "T&A Modes". In RACS system each access point (controller/terminal) may have its own default T&A Mode.
The T&A mode of access terminal cannot by dynamically changed during system activity.

The T&A Mode of controller can be dynamically changed in few manners that are listed below:

- by adequate Time Schedule (T&A Mode Schedule),
- by manual command entered from controller's keypad,
- by activation input line - select predefined T&A mode

In case last two manners are available two options of changing T&A mode: stable type selection (on unlimited time) and momentary type selection (until first identification). It's possible to set password (3..6 digits) for stable and momentary type selection. It will be indispensable to change T&A mode.

Remote modules

Controller extends its functions and abilities with additional remote modules. To activate operation with modules should set options in **Remote modules** field.

- **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.

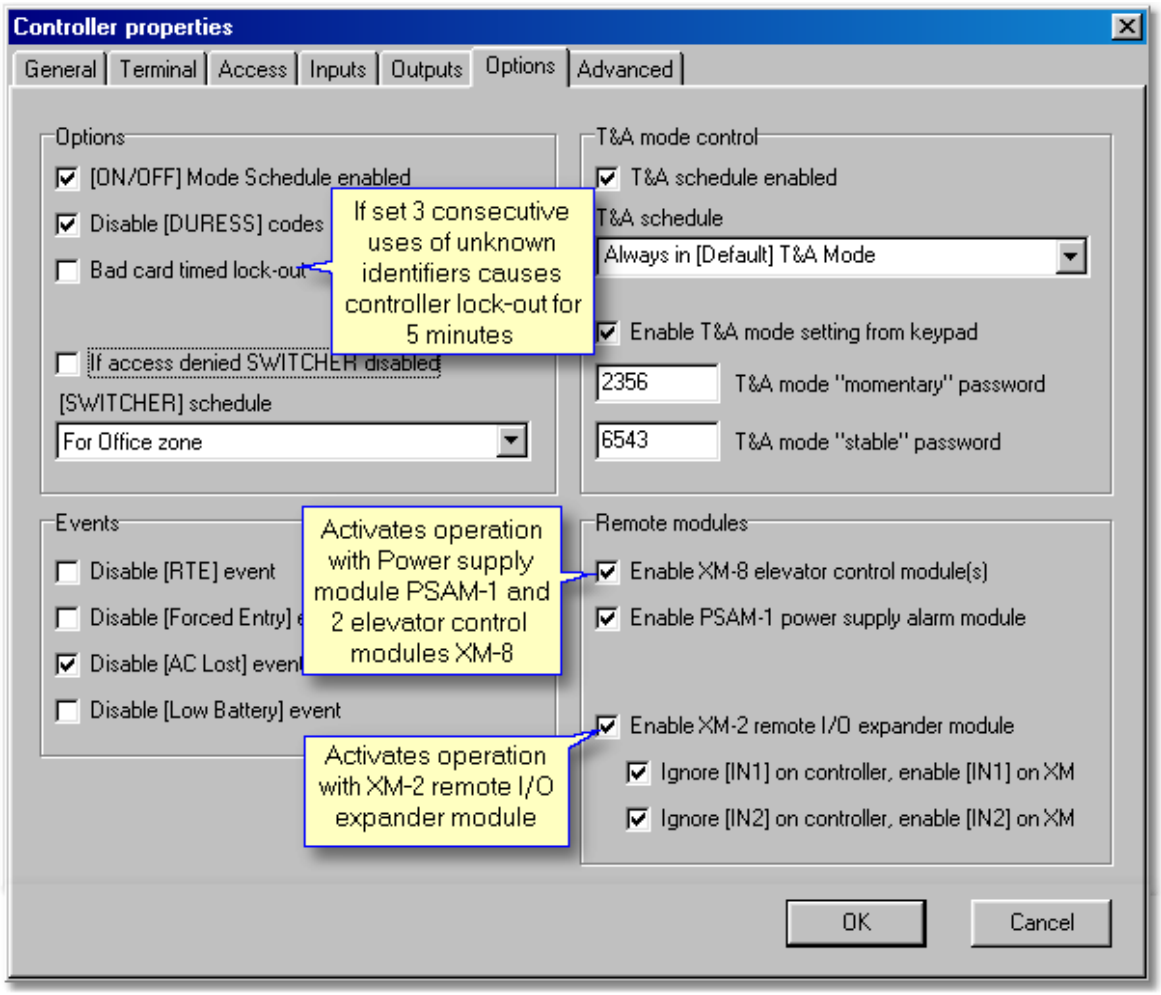
- **PSAM-1 module**
  Controller may operate with one PSAM-1 power supply alarm module (address ID=4) connected to controller through Clock and Data lines.
  The PSAM-1 is an optional part of power supplies offered by Roger, it delivers following data:

  - 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***.



11.5.2.7 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
by option ***Terminal ID=1 on "entry" side*** which is available in controller's settings. During APB function activity users are
obliged to use its identifiers on "entry" and "exit" side alternately.

The anti-passback can be used in two variants:

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

When anti-pasback 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 APB Reset Schedule or manually (using dedicated input line). 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:**

Concepts: Entry terminal and Exit terminal in this case refer to anti-passback function and are not related to T&A modes.
Term [Entry] /[Exit] in T&A is not equal with Entry/Exit terminal. It means that Exit terminal may be set to the Entrance T&A mode.

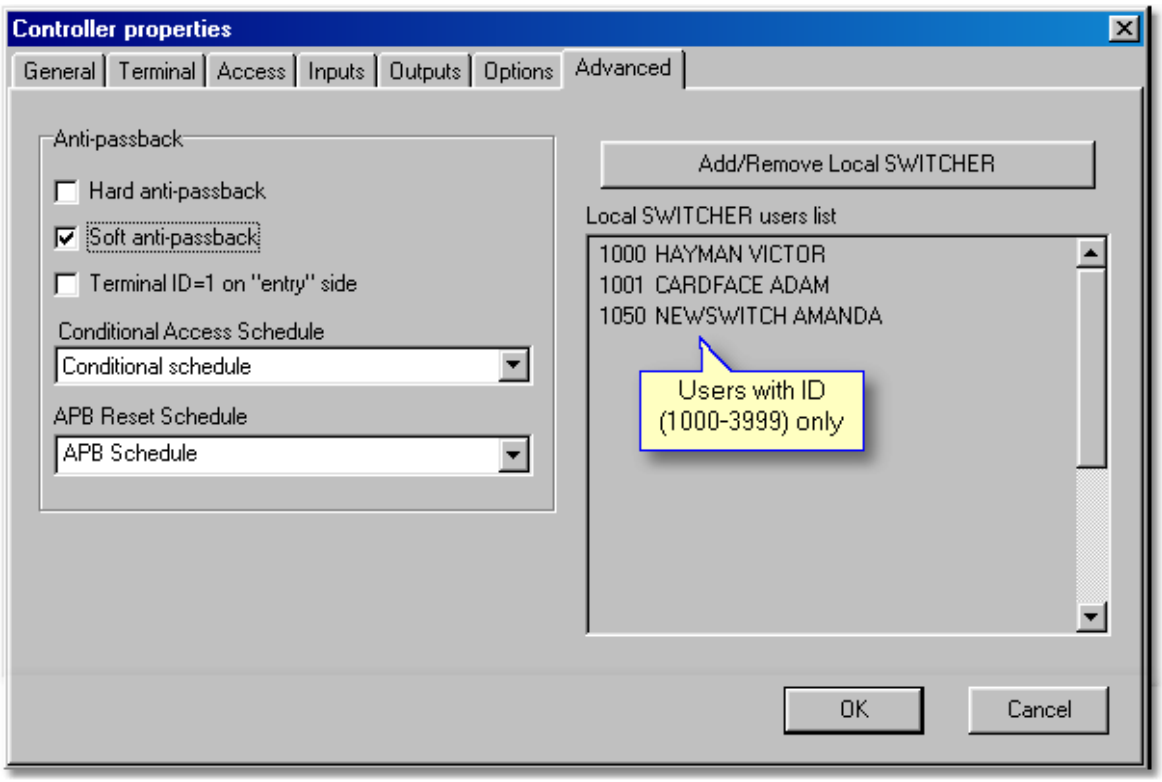
This feature allows inspecting users movement on the one access point so it's local type. By this function it's possible to control amount of logged users within selected zone.

In the controller memory is an array called ABP register, which consist of information about users and their APB status.
When user owns undefined status in APB registry (it's impossible to check, where the user was logged lastly, on entrance or exit) is allowed to use identifier on entrance and exit as well. Once first access is granted user loose undefined status and the controller starts to exact APB rules on him.

Controller enables APB reset function according to defined APB reset schedule, and by triggering external input line configured to [APB Reset] function.

We can utilize ABP to enable conditionally entrance function which reference to defined time schedule.
If feature works only on terminal ID=0 should check box ***Terminal ID=1 on "entry" side***. Once function is enabled configure one of external input line as: ***ABP reset***.

Each of controllers owns Local SWITCHER (users with ID numbers from 999 to 3999) list. These users are allowed to switch controller to ON/OFF mode. To define Local SWITCHERS you should click on the ***Add/Remove Local SWITCHER*** and then add them to the list using buttons: **>** and **>>**. Type of users SWITCHER Full and Limited can't be a local SWITCHER, its function concerns all system controllers .



11.5.3 Send configuration settings to controller

It is recommended to send configuration to the controller after making any changes of the controller settings.
Program offers it after each click on ***OK*** button. Other way is to choose ***Update*** from Controllers window.

To carry out configuration settings update:

- Click on 

from operator tools -> ***Controllers*** -> ***Update***
- or ***Edit*** from main menu -> ***Networks*** -> ***Controllers*** -> ***Update***

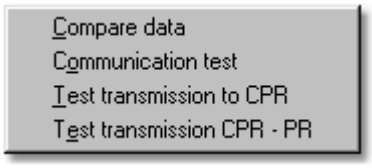
Note:
Remember that command causes transfer to selected controller only.

See also:
Send network configuration
Commands to system

11.5.4 Diagnostics

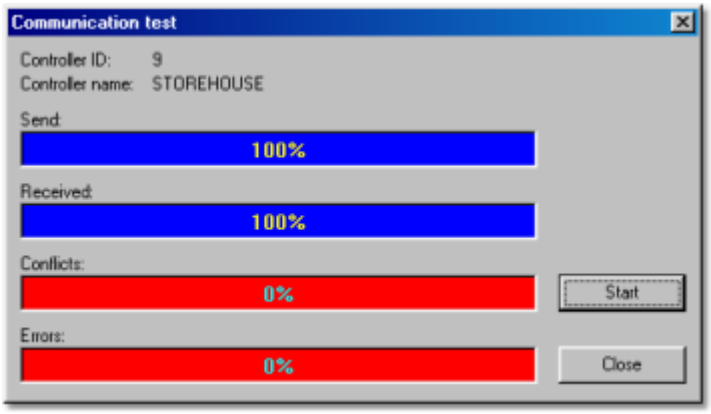
Feature enables to perform diagnostics operations of controller.

To send diagnostic command click on [Diagnostics] button in Controllers. Menu box with options will appear:

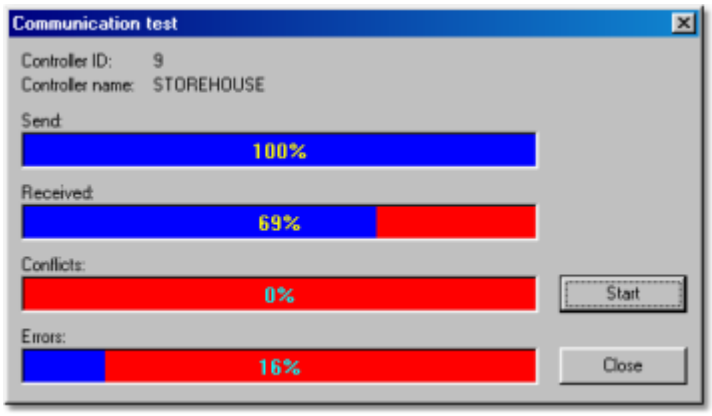


- ***Compare data*** - compares controller settings with configuration in program data base
- ***Communication test*** - test communication between PR Master and controller
- ***Test transmission to CPR***
- ***Test transmission CPR-PR***

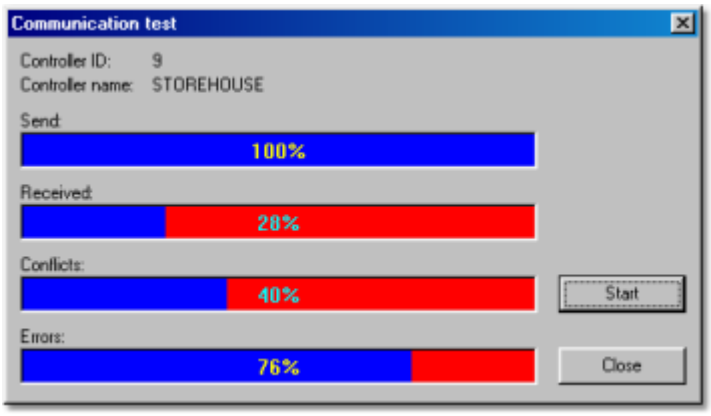
Results of Communication test:



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



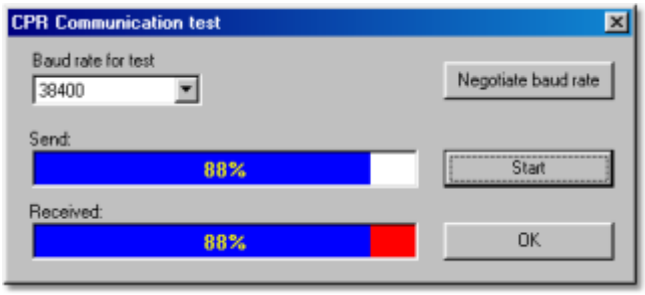
results - average, 60-80% answers may accept, however some conflicts and errors occurred



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

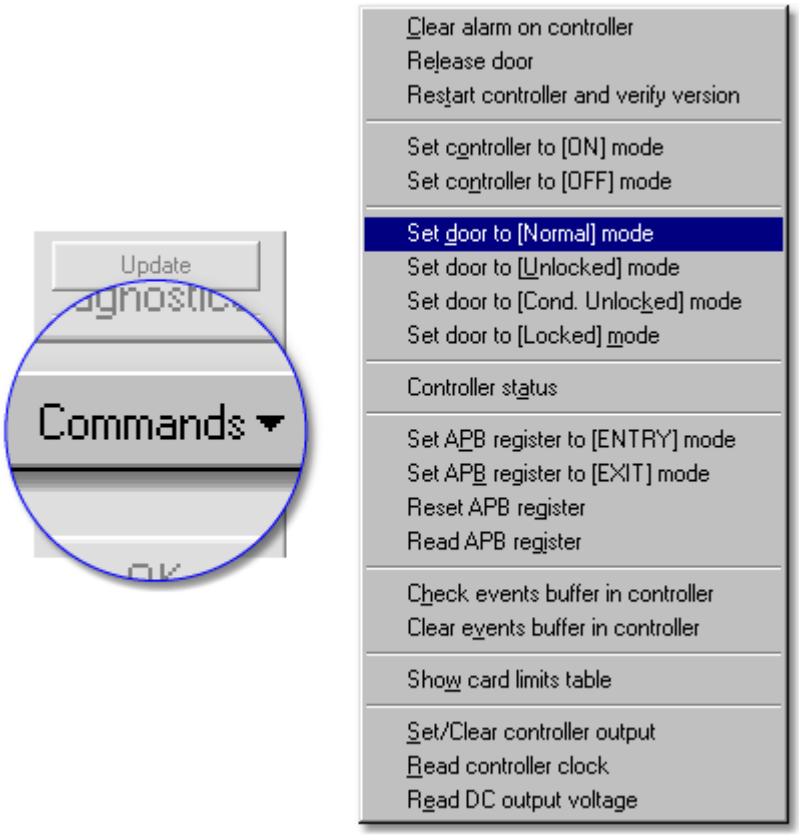
Transmission to CPR and ***CPR-PR*** are carried out in the similar method.

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

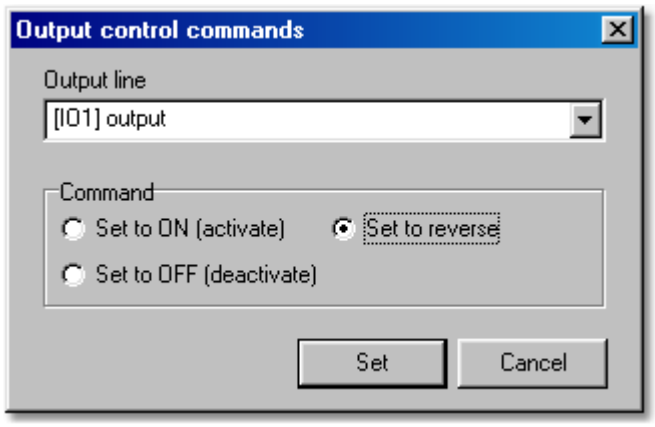
Once the controller is selected we can send a command to it. After click on [Commands] button menu with available commands (depend on controller type) will appear.



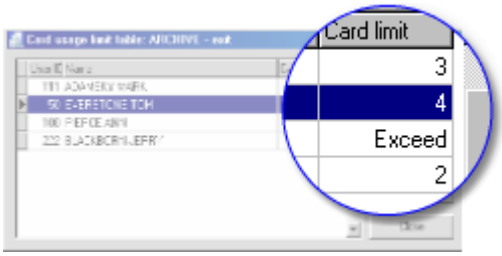
On the picture above we have commands for PR402 controller:

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
- Set APB register to [ENTRY] mode - sets mode in which user should first log on entrance terminal
- Set APB register to [EXIT] mode - sets mode in which user should first log on exit terminal
- Reset APB register
- Read APB register
- Check events buffer in controller - shows number of buffered events
- Clear events buffer in controller
- Show card limits table - allows defining new limited identifiers
- Set/Clear controller output



- Read controller clock - shows current time in controller chip
- Read DC output voltage - shows Direct Current output voltage



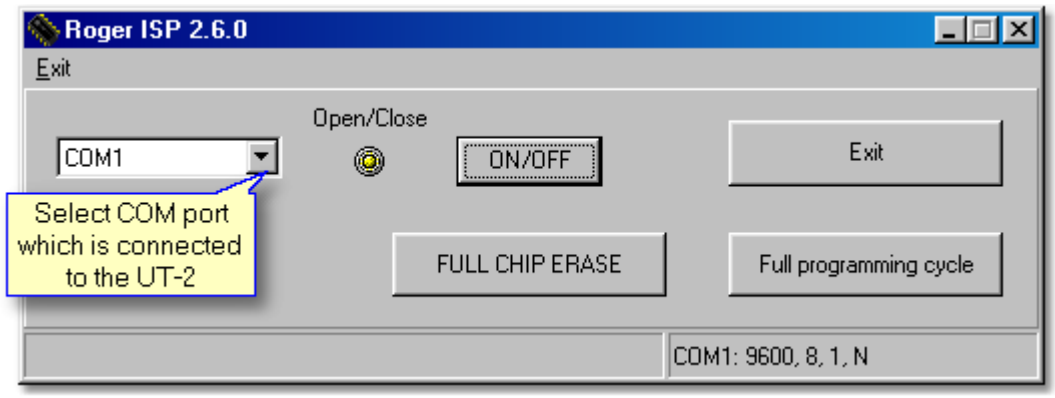
11.5.6 Microprocessor Firmware upgrade

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 PRxx2 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),



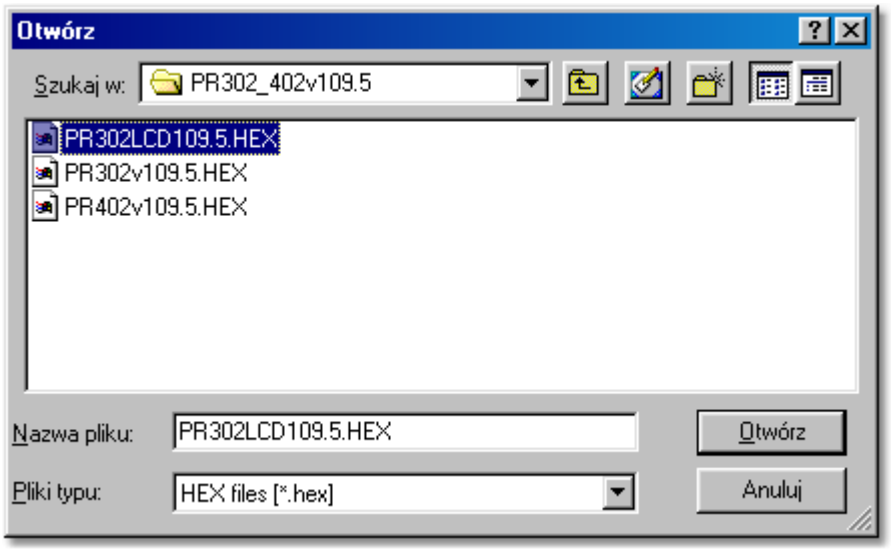
- Click on ***Full Chip Erase***, the following communicate will appear:

- 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 by carried out to one or more controllers simultaneously. However, should remember to realize weryfing 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

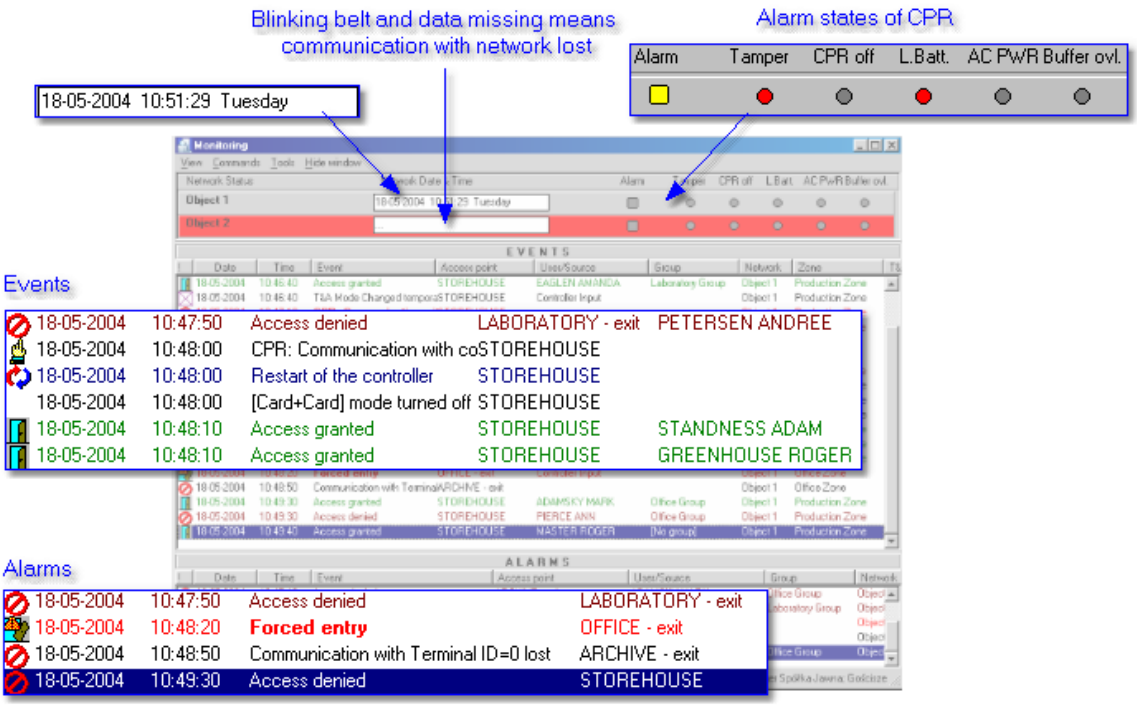
Monitoring Mode is a working mode of PR Master, which consist in events visualization in a real mode. When PR Master remains in a Monitoring mode, occurred events are immediately appended to system database and are available to export and report generating.

PR Master enables monitoring on computers in local network by Remote Monitor software.

You can turn on monitoring mode when you:

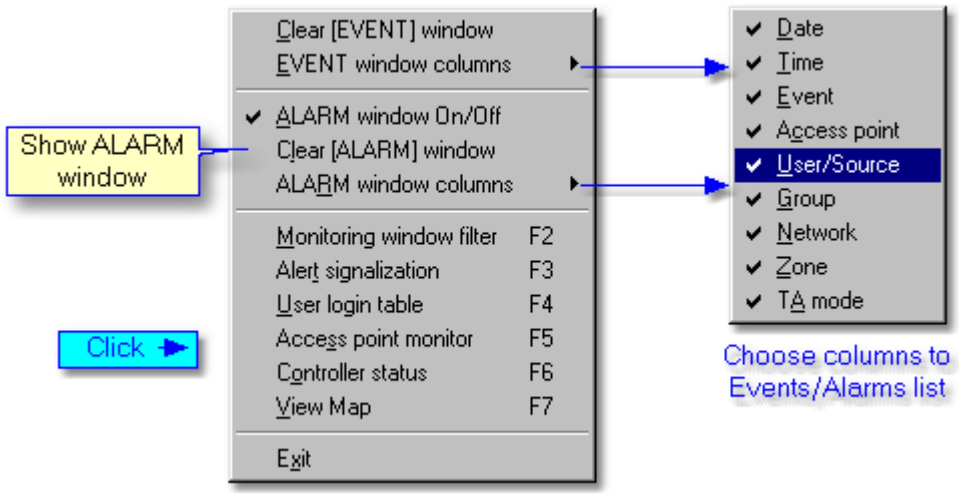
- click on from operator tools
- or choose ***Tools*** -> ***Monitoring from main menu***

Note:
Before the monitoring window opens, all events are received from system buffers and appended to database.



12.1 View

This menu allows to change windows view and execute additional options (keyboard shortcuts F2-F7).
Monitoring window consists of two sub windows: "Events" and "Alarms". From this level can select columns, which will be, figure in the window. Optionally can disable "Alarms" sub window or clear it.



Note:
Send ***Clear [EVENT] window*** command don't clear "Alarms" sub window.

12.1.1 Monitoring filter

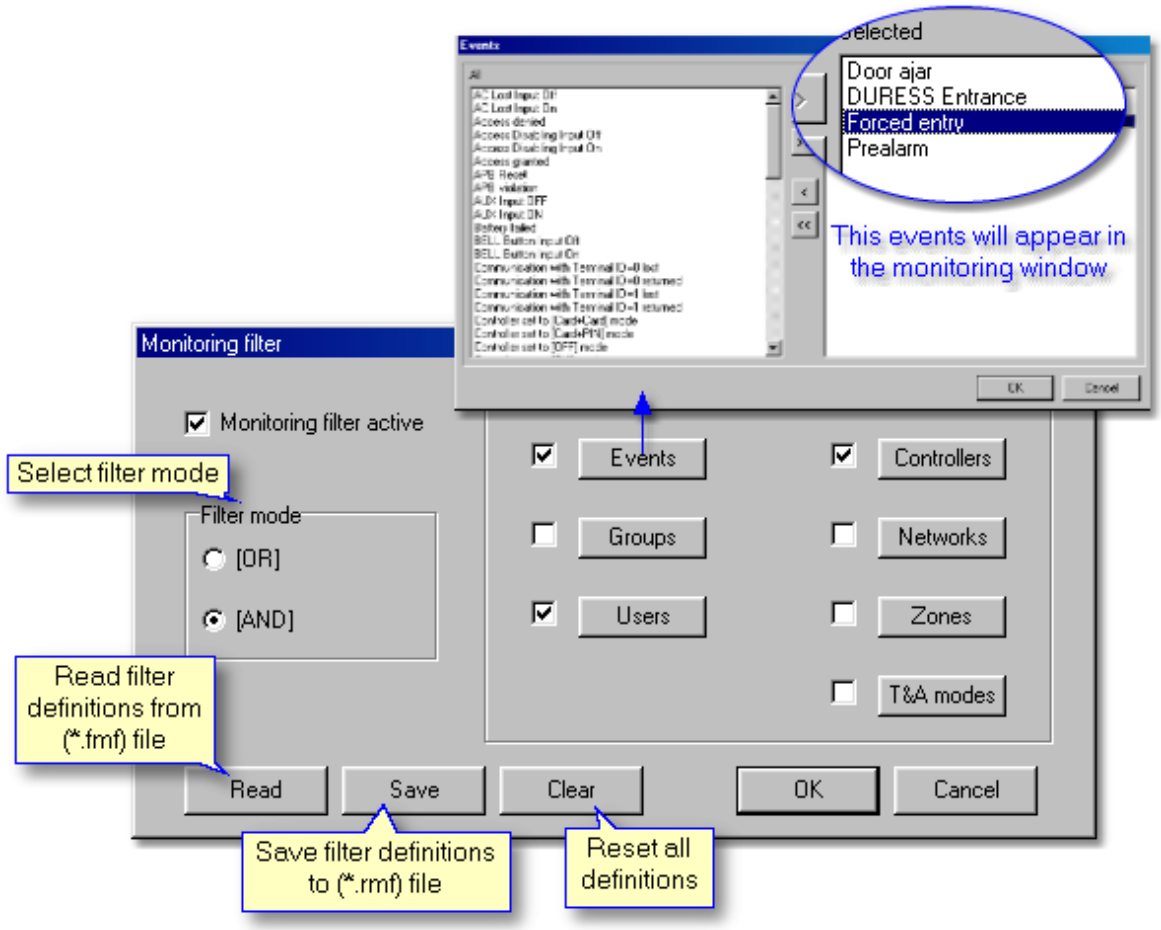
Option Monitoring filter allows selecting only this events, which will be showed in monitoring window. By selecting ***AND/OR*** filter mode it's possible to specify kind of condition. ***AND mode*** - when all selected conditions will be realized, ***OR mode*** - when one of selected condition will be realized.

Example:
- Select filter mode
- Specify filter rules:
- Events: Forced entry, Prealarm, DURESS Entrance and Door ajar
- Zones: Office Zone and Production Zone

Note:

1. In the example, events will be showed in case fulfilment of all conditions (AND mode). Condition fulfilment: Prealarm in Office Zone.

2. When we change filter mode on (OR mode) in the monitoring window will occur all of events: Prealarms, DURESS Entries, Forced entries, Door ajar and all events in Office and Production Zone.

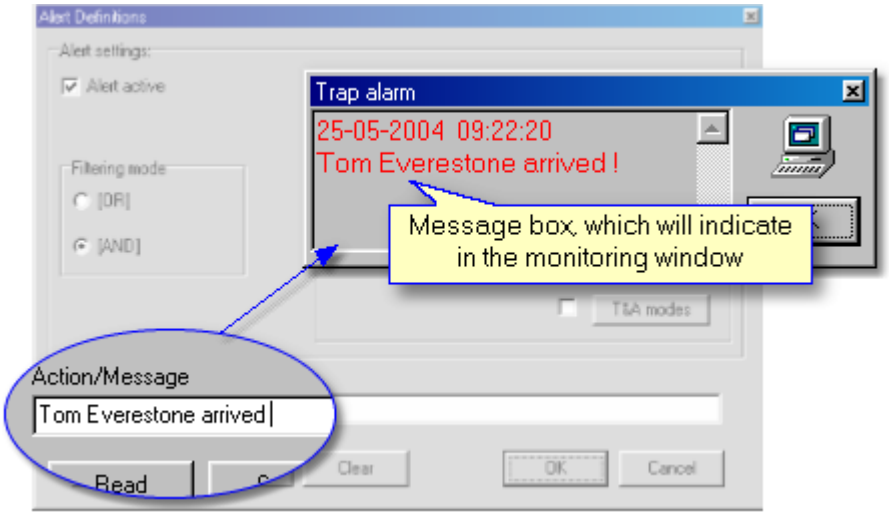


Can save and read filter definitions from (*.rmf) file. Clear option resets all settings.

Note:
Open Monitoring filter more quickly by pressing F2 on keyboard.

12.1.2 Alert signalization

Alert signalization feature enables to specify monitoring messages. Events selecting method is the same like in Monitoring filter. The message is a kind of "alarm window". To define message select ***Alert signalization*** (F3) from ***View*** menu in monitoring window.



In Action/Message gap enter short text, which inform about occurred event.

We can also specify the manner of reaction utilizing following variables:

Here are variables to use in the message:

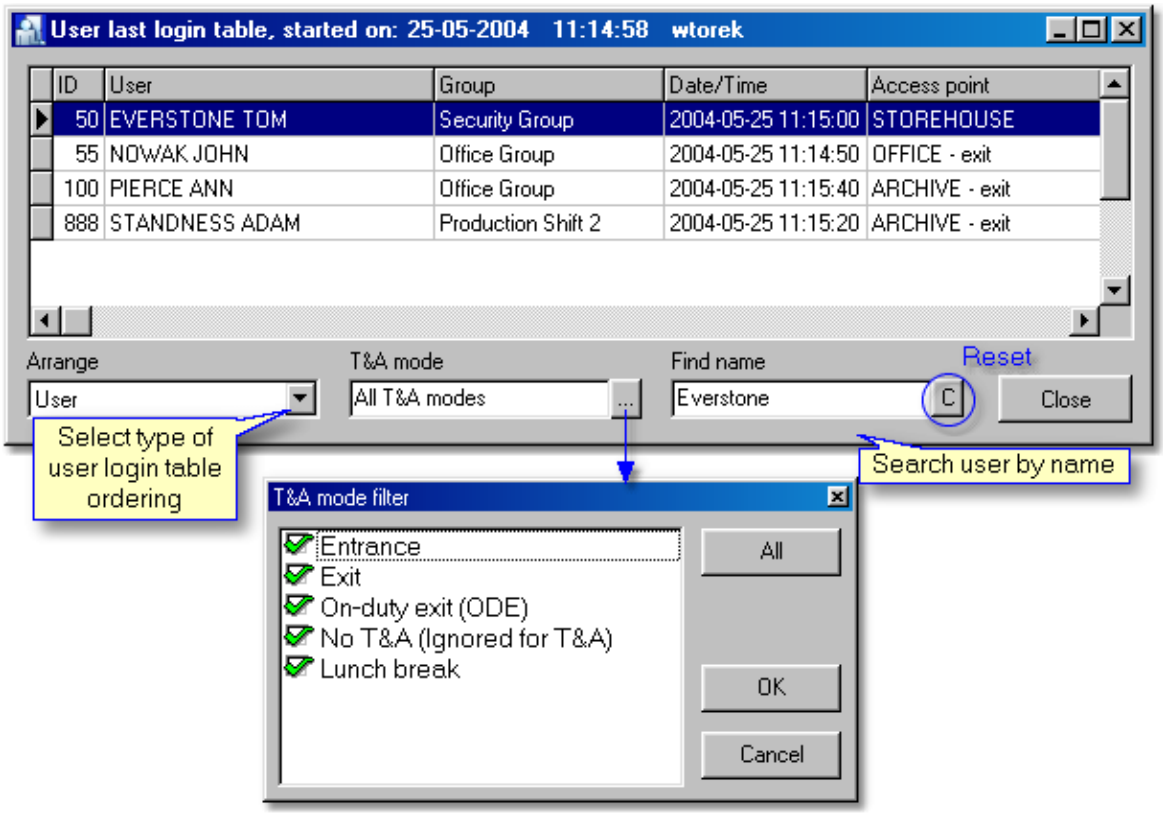
- %u - user
- %g - group
- %e - event
- %c - controller
- %s - subsystem
- %n - go to new line

Note:

1. Use variables when you want to define more precisely manner of action. It's useful when many conditions are defined.
2. Message is always showed under event date and hour.

12.1.3 User login table

This option allows to quick and efficient system user searching. User login table shows, on which of controllers user was logged lastly. Feature is helpful especially when you need to find information about current user location and you don't want to browse long event list in monitoring window.
In the table it's possible to order logins by selected criterion, and additionally enable T&A mode filter.



Note:

1. In case long list of users we can enter a name of searching user in Find name gap.
2. To quick open User login table use F4 on keyboard.

See also:

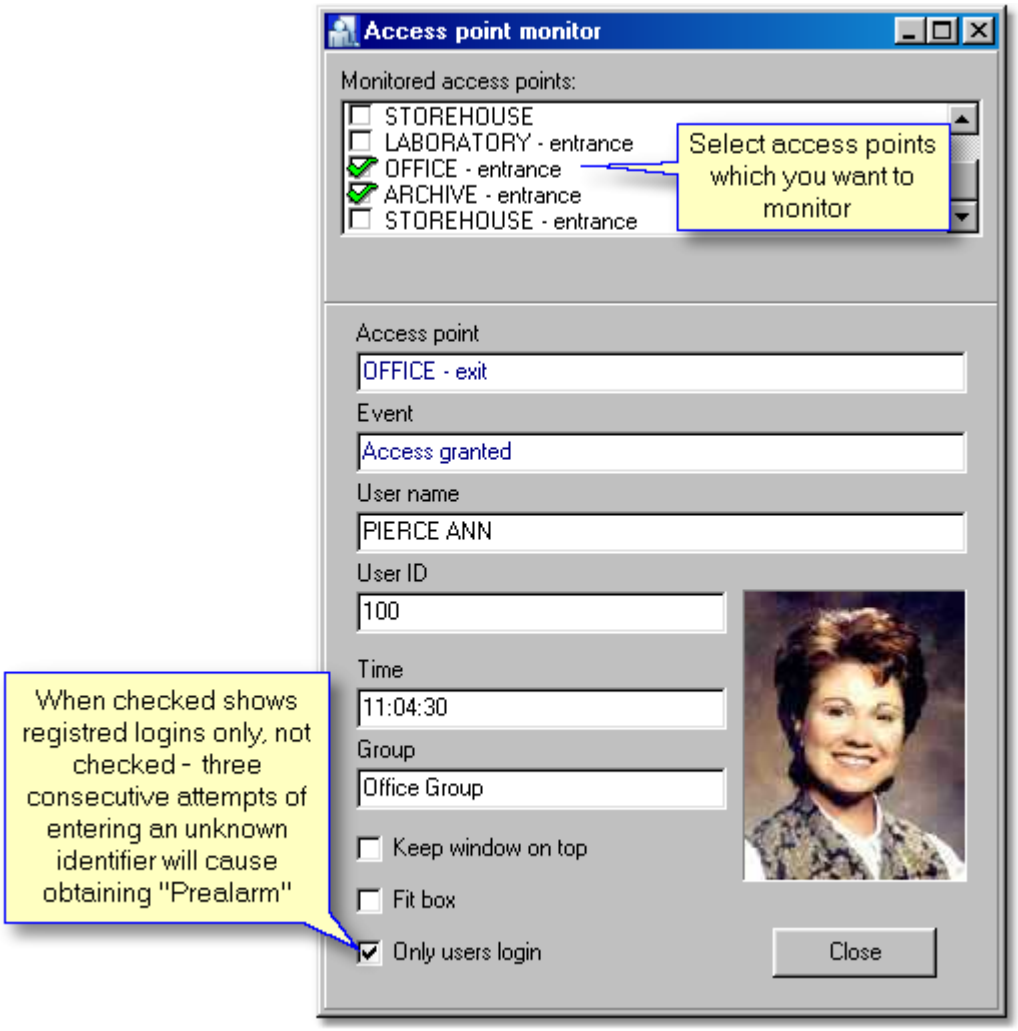
Monitoring filter

Define trap

12.1.4 Access point monitor

Access point monitor enables to show visual information about system user on selected access point(s). Activation Access point monitor option consist in selecting monitored access points. When user identification on one of chosen points is done program shows information about system user and assigned photo. It's possible to verify person who uses identifier, especially in big system with lots of users.

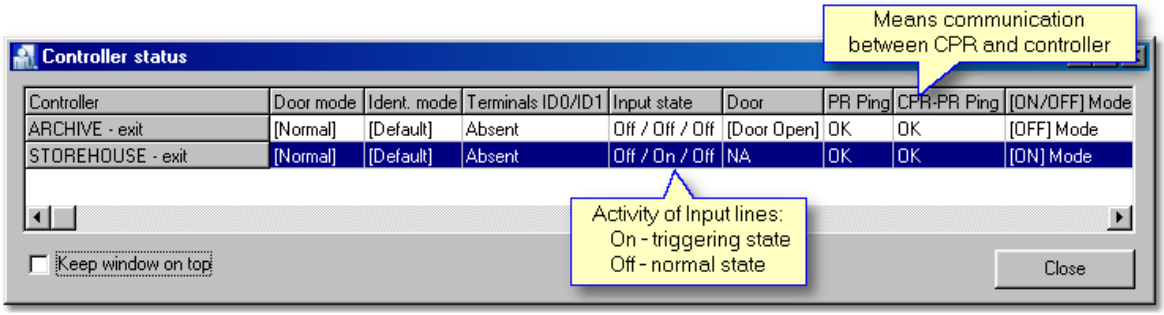
In case the [***Only users login***] option is checked, in window logins of registered users will be showed only. Whereas the option is unchecked, three consecutive attempts of entering an unknown identifier on one of controllers will cause obtaining "Prealarm" event in ***Event*** field.



12.1.5 Controller status

Controller status enables to observe controller states, such as Door mode, Identification mode, Input and Output lines states.
From this window level we are only able to watch, sending commands, selecting category, or changing appearance of window are not allowed. However it's available in View map option.

Note:
Data in the table is refreshed in 6 seconds periods. BD occurring means NO DATA.



See also:
Diagnostics

12.1.6 View map

View map enables visual system monitoring with object map utilization. User can load object scheme or building map, which want to monitor and put controller icons in appropriate places. Each of icons can be modified according to own needs. From controller icon can send commands to the device.

Icon edition can be carried out in two following ways:

- Click right mouse button on the controller icon
- Once menu appeared select [***Edit icon***]

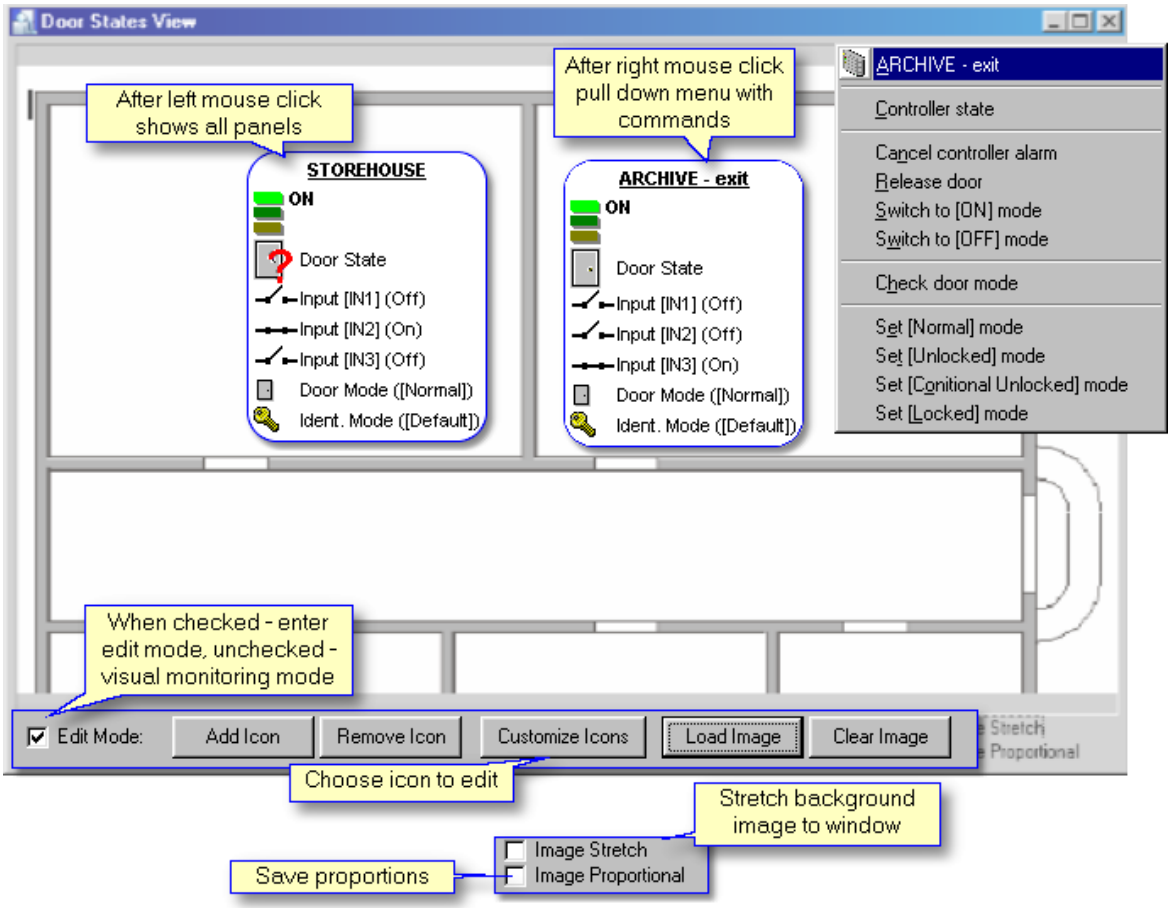
or

- Click on [***Customize Icons***] button from belt on the bottom
- Select controller to edit

In controller icon edition we have panels to choose, which will be showed in the icon during the monitoring and also appearance settings such as font, background etc.

Visual monitoring mode

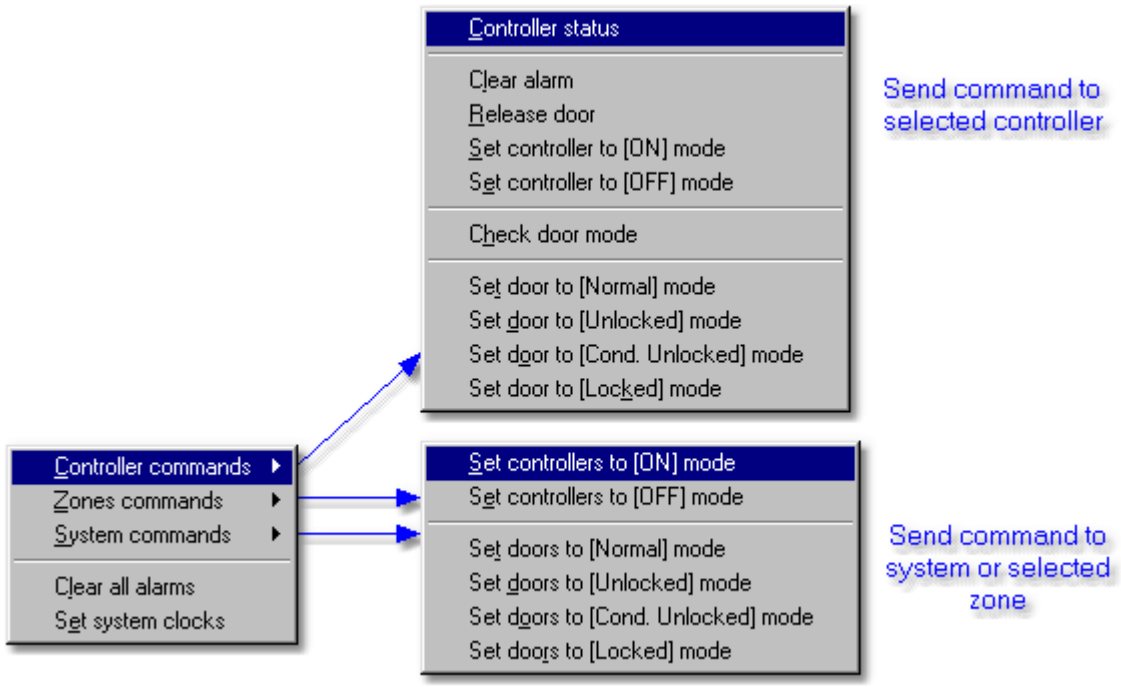
To enter visual monitoring mode should uncheck box [***Edit mode***]. We can observe controller states in a real mode now, and also send commands to devices. To pull down menu with commands click right mouse button on controller's icon.



See also:
Controller status

12.2 Commands

Set of system monitoring commands. Once command to controller is selected, window with available devices will appear. Click on one of them. Sending commands to zone looks similar.



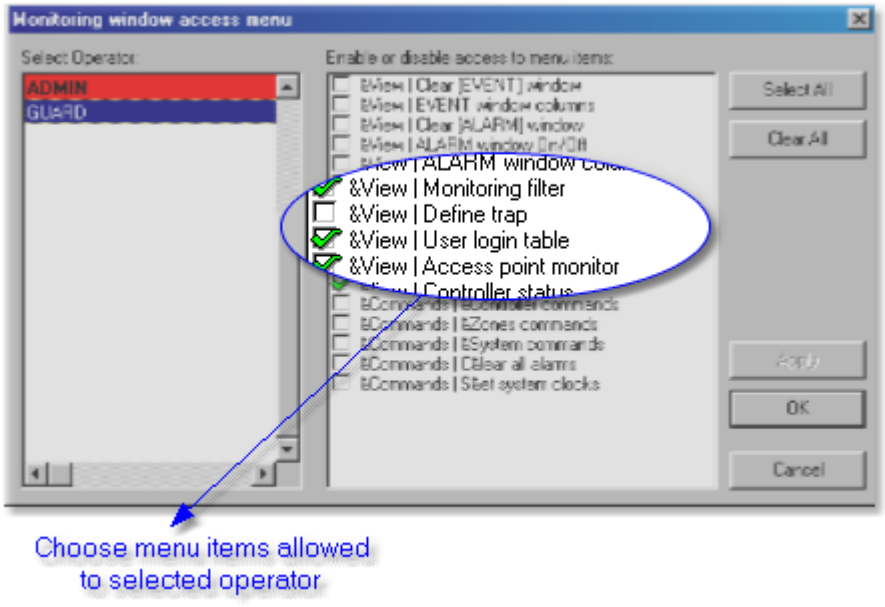
12.3 Tools

12.3.1 Operator rights

This feature allows defining access rights to the monitoring window menu for selected program operator. When existing only one operator (ADMIN), close monitoring window and define new program operators.

To add new program operator:

- Select ***Tools*** from main menu and -> Program operators
- Click ***add*** button



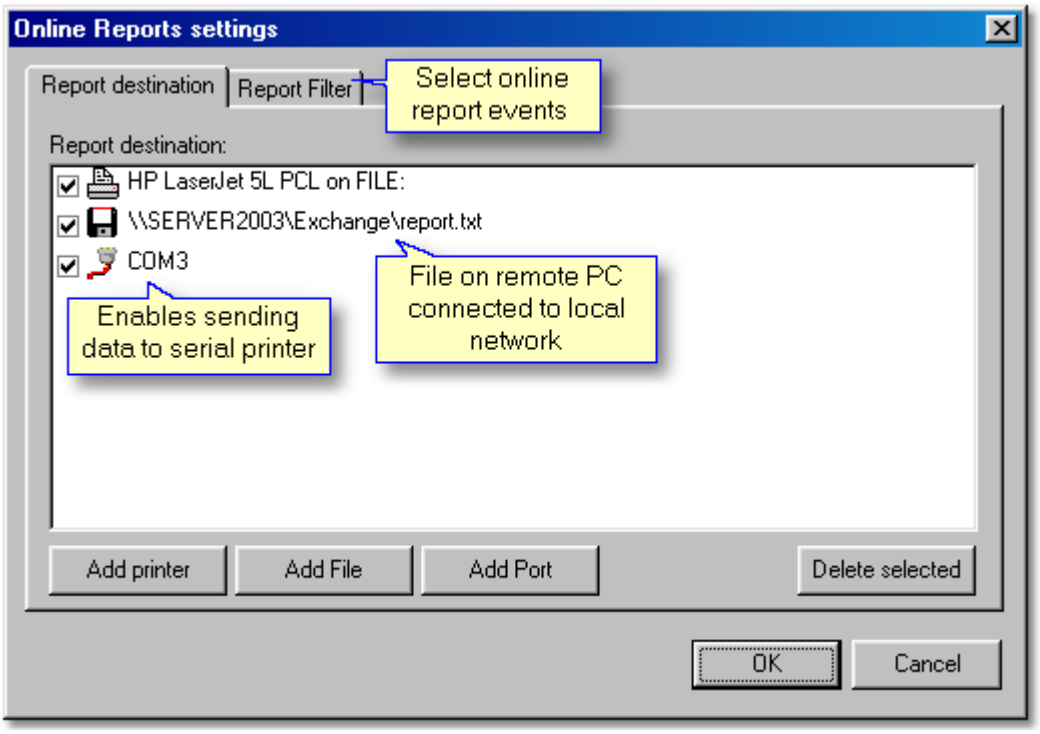
12.3.2 Online reports

This function enables online reports generating. When it's activated events are immediately send from RACS system to all defined destinations. By using report filter can specify report events.

To activate filter you should:

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

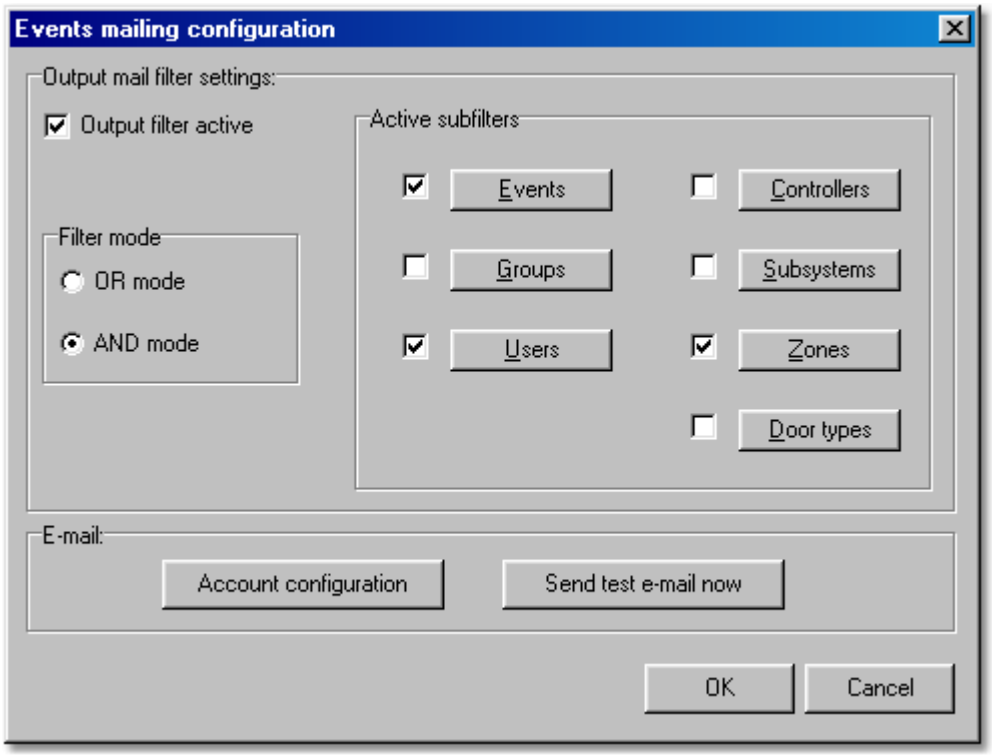
Optionally can define many printers, files and ports. Feature is very useful especially when operator wants to store files in a safe place or to print particular events.



12.3.3 Events mail configuration

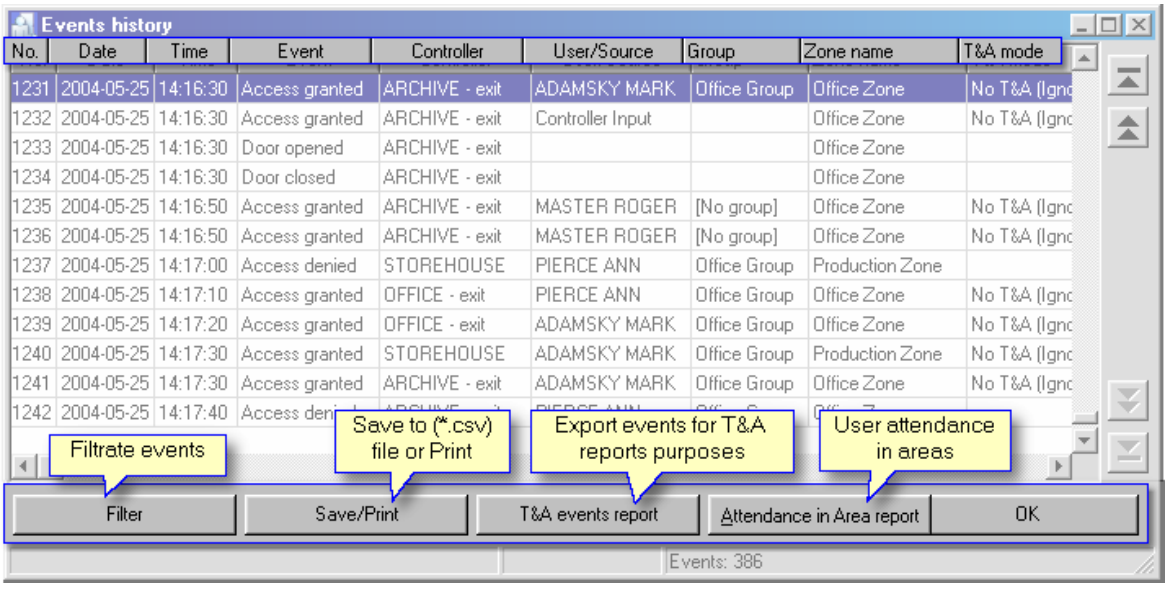
The option allows e-mail sending with filtrated events. To enable feature you should check ***Output filter active*** and define events in ***Active subfilters*** field. The next step is an Account configuration, which is carried out the same like in XML reports and e-mail function. To check configuration can send test e-mail.

If user has an e-mail box which enables SMS messages sending, then he can always have a contact with the access system.



13 Events

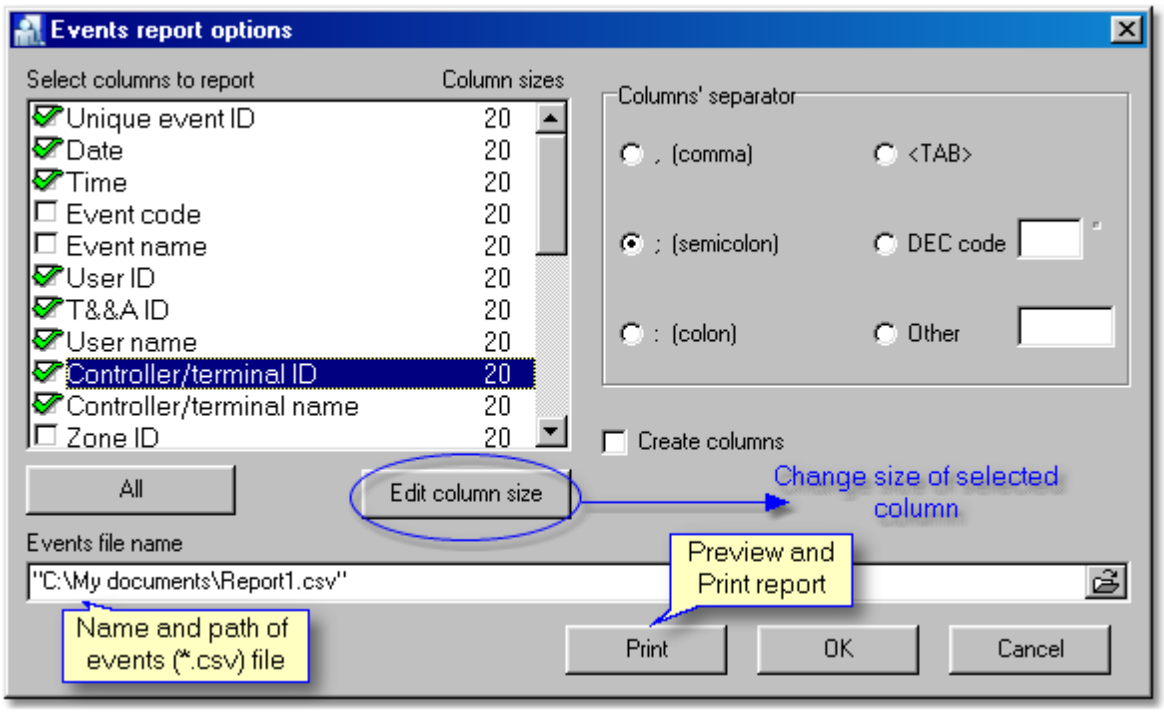
Events history (or events registry) contains all read events from the system database. To make events review more easily can activate Filter. Filtrated events can be exported to text file (*.csv) or printed. There is also possibility to export all events or events from defined range to the file with (*.rcp) extension.



See also:
CSV Report
T&A Report
Attendance in area report

13.1 CSV Report

This option allows user to generate report in (*.csv) text file form. Report can be generated from all or filtrated events. Components of csv report are selected by box checking. If an information in generated report table is not all visible, it's recommended to change column sizes.
User is able to completely remove columns or separate them with one of predefined column separators. Can also define own separator, by checking ***Other*** and filing gap.



13.2 T&A report

By this feature can generate T&A reports in file form with *.rcp extension. RCP file includes only these events, which have influence on T&A registering. It allows exchanging data between PR Master application and external payroll software.

Program generates files in following formats:

- RcpAccess Pro+

- Gatyfikant
- Agrobex
- Symfonia

13.3 Attendance in area report

Attendance in area report is used for calculation of total job hours in specified area. Spending time is counted on base Entrance and Exit from area registering.

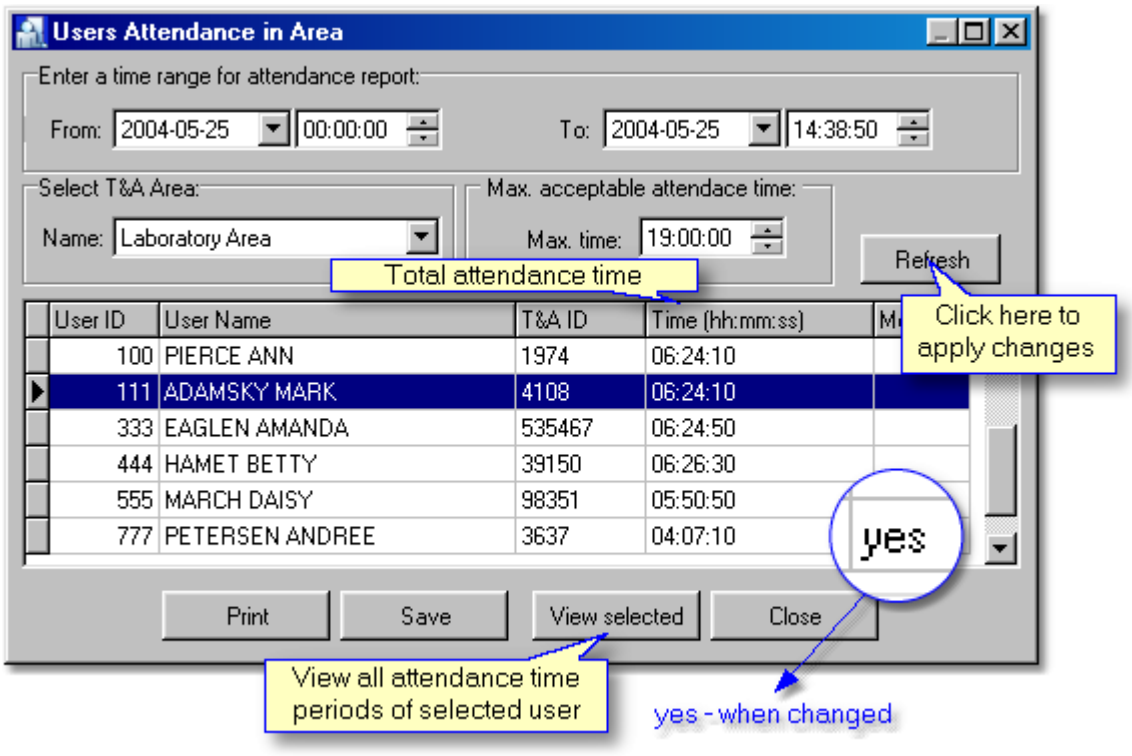
To open Users Attendance in Area window:

- choose from main menu ***Report*** -> ***Events***,
- in Events history window click on ***Attendance in Area report*** button

To generate user attendance in selected area report:

- Enter a time range From/To (date and hour)
- Select T&A area (defined by user - T&A Areas)
- Specify maximal acceptable attendance time (do no set 00:00)
- Click on ***Refresh***

We can save attendance report into formatted file (*.rtf) - [Save], or Print it.



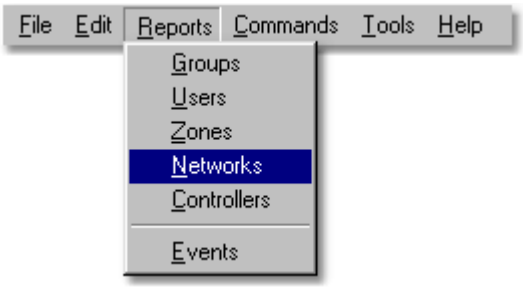
Note:
In case when in some way in the ***Time*** (hh:mm:ss) field question tag will occur it means that

program hasn't received information about T&A Entrance or Exit event. It's recommended to modify it by click on [***View selected***] button and enter missing date and hour.

See also:
Events history

13.4 Reports

This feature generates reports, which are ready to print. Reports concern all system domains (Groups, Users, Zones, Networks, Controllers). It's no available to edit nor save reports. Document is only adapted to preview just before printing.



14 System with/without CPR

Networked operation with CPR

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. 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.

When ***controller PRxx2*** series 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 PRxx2 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 theirs full functionality (no functionality is lost or reduced).

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.

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 (PRxx2 only) and can be later transferred to PC using interactive command or will be downloaded automatically anytime monitoring window is started.

To enable Network without CPR option you should select: ***Edit*** -> ***Networks*** and uncheck box: ***Network with CPR control panel.*** Network properties

It's recommended to send configuration settings to each controller in system separately.