APS mini

APS Home

APS mini Plus system administration program

User's guide

techfass®

(Released on 2020/05/18, valid for build 1.0.7443.12414)

1 Content

2 Program and installation

2.1 Description

APS Home is a software product designed for offline management of *APS mini Plus* access control system by *TECH FASS s.r.o.*; the product is usually used to manage access control in applications like block of flats, etc. The product is designed for single-user management of the system.

The connection to APS mini Plus system lines can be done using *COM, USB, or TCP/IP* (with appropriate communication line converters). The communication interface types can also be mixed in a single application.

Note: If you want to manage the system by multiple users or want to run the system 24/7, use *APS Administrator* software product for the system management.

2.2 Installation

The program can be installed on *Microsoft Windows 7, 8 and 10. MS .NET Framework 4.0* is required to run the program.

The program can use two types of data storage:

- *MS SQL Server*, including Express edition, version 2005 and newer.
- MS SQL Server Compact Edition 3.5, which is obsolete at the time and its further development is not planned. We do not recommend to use this option. The support of this option remains in the program to secure backward compatibility.

2.3 APS Home program installation

The program is installed by running its installer. The program is installed in *TechFass\APSminiPlus.Home* folder in Program Files folder of your computer.

2.4 MS SQL Server (Express) installation

- Run the MS SQL Server installer (can be downloaded at MS website)
- Install the program following the instructions in the guide. If necessary, you can install the server as a named instance (not recommended)

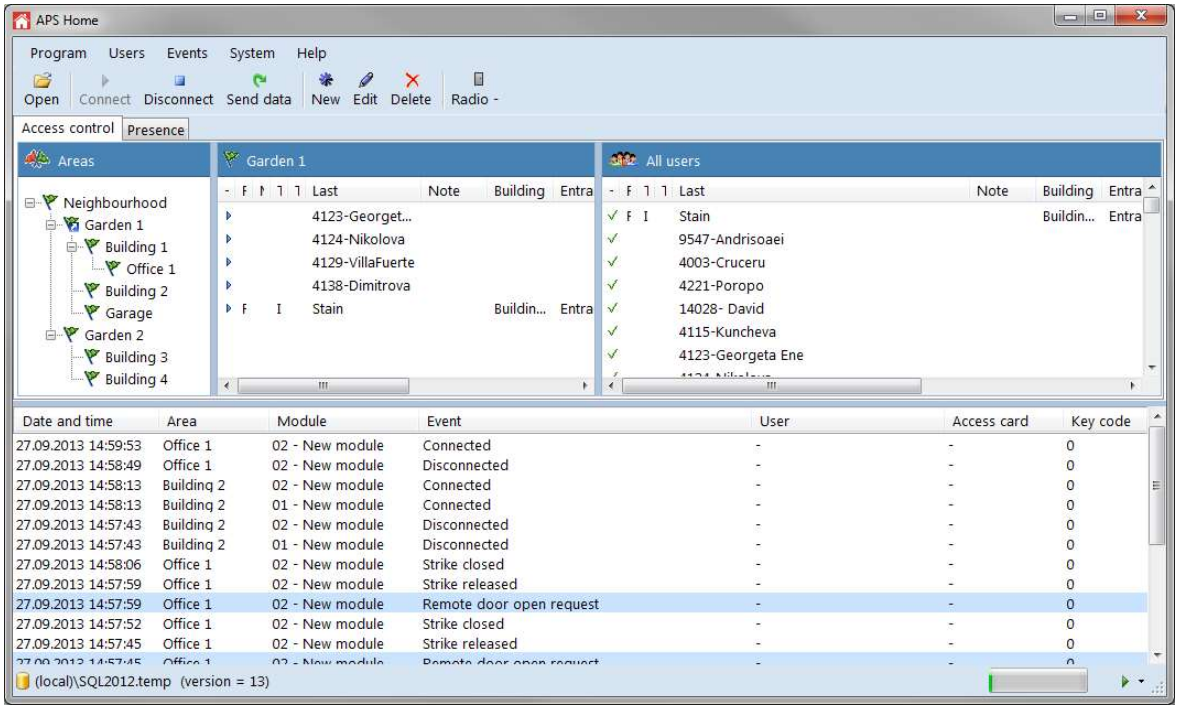
Note: In this guide we assume, that the server is installed as unnamed instance.

techfass®

3 User interface and general program options

3.1 User interface

The program main window (*pic. 1*) consists of several parts. In the upper part you can find the main menu containing *Program*, *Users*, *Events*, *System* and *Help* options. Below the menu you can find a panel containing buttons for communication control, system programming and users administration.



Pic. 1: APS Home program

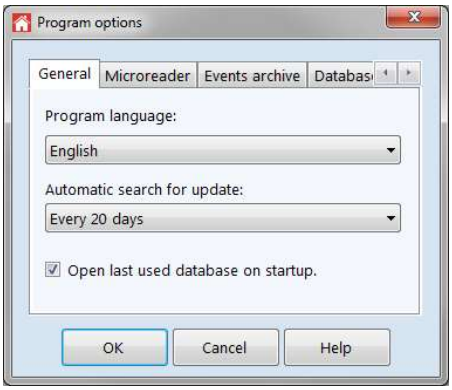
The window is divided into 3 vertically separated parts in the middle at the first tab (*Access control*). In the left part you can find a list of areas, in the middle one you can find a list of users with an access right to the selected area, in the right part you can find a list of all users.

The second tab (*Presence*) is used for the time spent in selected areas evaluation, which can be used for the simplest T&A evidence.

The bottom part of the window is reserved for events of the system, which are actually being read. The events read earlier are at disposal in the event archive. Under the area there is a panel with information about connection to the server and database on the left, in the right part there is a progress bar indicating data transfer status and communication lines status button (detailed info is available after left-clicking the mouse).

3.2 Program options

The program options are available after choosing *Program* > *Options* (*pic. 2*).



Pic. 2: Program Options

At the *General* tab you can choose one of the available program languages. The program offers an option of automatic control of the actualizations, the interval of the search for new versions is set in the *Automatically find update* list. If you want the program to open the last used database on startup automatically, select the appropriate option.

At the *Microreader* tab you can set the parameters for a microreader connection. First of all, it is necessary to check the *Use microreader* checkbox and set *Server IP address*, *Server IP port* and *Card ID length [bit]* (usually you can keep the default values if the server with a microreader runs at the same computer as the program). The microreader server with a user's guide can be found at http://techfass.com site.

At the *Events archive* tab you can set how old (in days) events shall be displayed maximally and a maximal number of events displayed at a single page.

The *Database* tab offers an option to set up the maximum timeout of database maintenance operations (timeout for long-lasting database operation like deleting records from the events archive).

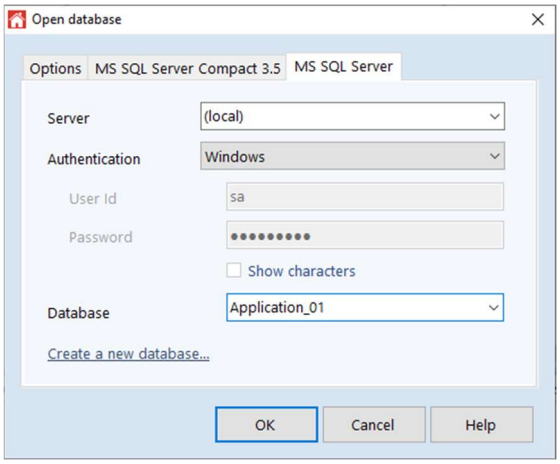
The *Log Files* tab allows setting the maximal time, after which the program automatically deletes the log files; it is set individually for the *system communication log* and *IP camera communication log*. By selecting the *Open folder* link, you can access the appropriate log files.

4 APS mini Plus application

The APS mini Plus application (physical installation of the APS mini Plus system) is in the APS Home program represented by the database, which contains all the data needed for configuration of the hardware modules and management of the users.

It is recommended to create a new database for each application. To create the database, open the *Open database* dialog (*pic. 3*) by clicking the *Open* button. The next steps are different for MS SQL CE and MS SQL Server.

We do not recommend the use of the MS SQL Server CE due to the end of its development. Description of the database creation procedure is retained here only for completeness.



Pic. 3: Open / Create database

4.1 Creating database – MS SQL Server Compact

- Select the *MS SQL Server Compact 3.5* tab
- Select the *Create a new database file…* link
- Enter the name of the file you wish to create in the *Database File* field – database will be stored in this file; path can be set by selecting the *Browse* link.
- The *Sort order* can be usually left at its default value
- Click the *Next* button and check your parameters; By selecting the *Create Database*… link create the database
- After the database is created, press the *Close* button
- After returning to the *Database Selection* dialog press *OK*.

4.1.1 Creating database – MS SQL Server

Enter the *Database selection* dialog by pressing the *Open* button.

- Choose the *MS SQL Server* tab
- Select the *Create a new database…* link
- In the Server field select a name of the computer with your SQL server installed, if it is not listed in the list, fill in *(local)*
- By pressing the *Test connection…* link verify you can access the SQL server and continue by pressing the *Next* button
- In the next dialog you can change the *Database name* and use another *Collation* (strings sort order), then click the *Next* button.
- Click the *Create database…* link
- After creating the database press the *Close* button
- Press the *OK* button and connect to the database

4.2 Connecting to database

To open an existing database, press the *Open* button. In the Select / Open database dialog (*pic. 3*) choose the tab according to the selected SQL server, enter the name of the database (or the database file) you want to open and press the *OK* button. If you want let the program to open the last used database on startup automatically, select the appropriate option at the *General* tab in the *Program options* dialog, which is available after selecting *Program* > *Options* in the main menu.

4.3 Database backup and restore

The program is able to perform database *backup* and *restore* operations. The operations are available only for the *SQL Server* databases. Both actions can be performed only by a user with administration privileges. The program can use the maintenance operations only when using a local SQL server.

Both operations can take a pretty long time. Therefore, in the *APS Home* program there you can set the maximal time of their duration. The option is available int the *Program options* dialog at the *Database* tab, which is available after selecting *Program* > *Options*. The default value of the *Maintenance commands timeout* parameter is *600 s*. A detailed description of both operations can be found in the *Supplement 3*.

The tools for database backup and restore are available in the *System settings* dialog at the *Database* tab, which is available after selecting *System* > *General*.

Note: The dialog for database operations can be protected by *configuration password*.

4.3.1 Database backup

For creating a database backup press the *Backup* button. In the first step select the *SQL server* and the *authentication method*; then select the *database* for backup operation. Continue by pressing the *Next* button. In the next dialog page select the *file name* and *location*. Continue by pressing the *Next* button. In the last step verify the correctness of entered parameters and run the database backup operation by selecting the *Backup database* link. After the process is finished, an information window about the operation result is shown.

Note: We recommend performing the database backup regularly. If for any reason the actual database file becomes damaged, you will prevent yourself from possible data loss.

4.3.2 Database restore

Before performing a database restore operation be aware of following facts:

- The operation is performed with *REPLACE* and even *MOVE* (when needed) flags. Therefore, it is possible to overwrite ant database with any backup!
- After a database is restored the former data stored in the database are *irreversibly lost*!
- The database can be restored only into an existing database. If you want to restore a database backup in a new database, you have to create a new one first.
- When restoring a database, no user can be connected to it and the APS Home communication must be stopped.

For restoring a database from a backup file press the *Restore* button. In the first step select the *SQL server* and the *authentication method*; then select the *database* for the restore operation. Continue by pressing the *Next* button. In the next dialog page select the *backup file name* and *location*. Continue by pressing the *Next* button. In the last step verify the correctness of entered parameters and run the database restore operation by selecting the *Restore database* link. After the process is finished, an information window about the operation result is shown.

4.3.3 SQL console

The last option of the *Database* dialog is an *Open SQL console* link, which opens a new dialog window for entering and executing the SQL scripts.

- *Open*: Opens a file with an SQL script.
- *Execute*: Executes an entered script.

In the lower part of the dialog, there are two tabs:

- *Data*: Displays the data result of the script.
- *Output*: Displays the information about successful execution of the script or error message.

The SQL console is a tool for direct work with the database and it is intended for advanced and experienced users only!

4.3.4 Summer time adjustment

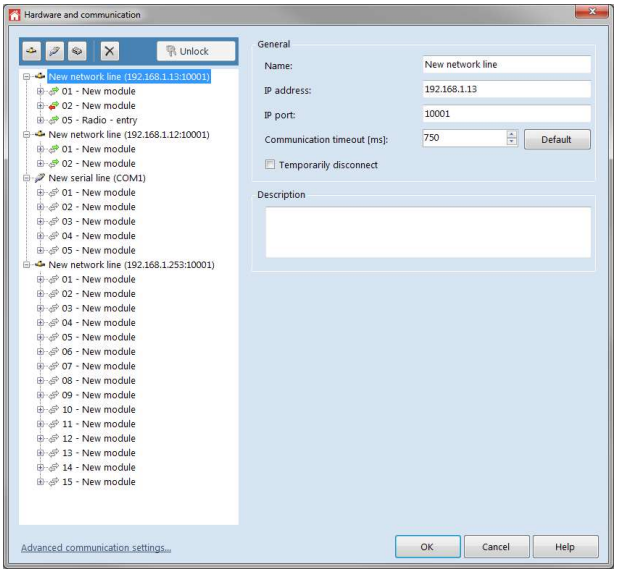
If you are located in a zone, where the summer time adjustment is not used, you can globally suppress this feature in the modules in the *System setting* dialog at the *General* tab. The dialog is available after selecting *System* > *General*. The summer time adjustment is enabled by default.

4.3.5 Application security

The application enables to set up passwords for two levels of access – a *user password*, which is required for the connection to the database itself when set, and a *master password*, which is required for advance settings (changing values in the *Hardware and communication* dialog) when set. The passwords are not used by default; the setting can be done at the *Passwords* tab in the *System setting* dialog available by selecting *System* > *General* in the main menu.

5 Hardware and communication

The communication with the APS mini Plus modules is done in the *Hardware and communication* dialog (*pic. 4*), which is available after selecting *System* > *Hardware and communication*.



Pic. 4: Hardware and communication

In case of a connection with a poor quality, it is sometimes necessary to change the basic reaction of the program on communication timeouts – this can be done after selecting *Advanced communication settings* link in the lower left corner of the dialog. Following options can be set:

- Communication line restart delay [s]
- Number of communication errors or timeouts before requesting restart
- Maximum number of attempts to send a packet

In most cases you can use the default values (reset with the anchor buttons).

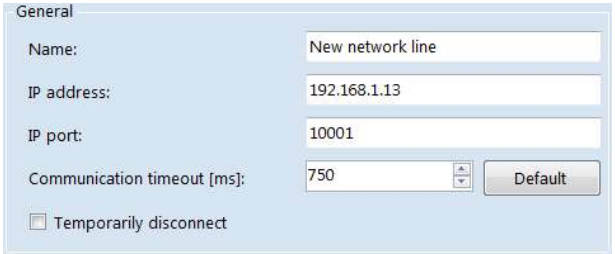
Furthermore you can enable the detailed communication log – if this choice is selected, each sent and received packet is logged in the program's communication log – in such case the program operation is quite demanding, therefore we recommend using this option only in case you need to discover errors in the communication.

5.1 Communication lines

To set the communication with modules it is necessary to set parameters of communication lines, which they are connected to. The setting is done in the *Hardware and communication* dialog (*pic. 4*), which is available after selecting *System* in the main program menu.

5.1.1 Network line

To add a new network line, open the *Hardware and communication* dialog and select the *New network line* button. Fill in the parameters of the network line (*pic. 5*) – *IP address* and *IP port* (according to the converter settings).



Pic. 5: Network line

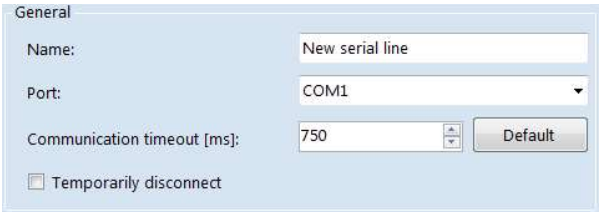
For verifying the converter is able to communicate, use the *ping* command from the context menu. We recommend filling in a unique *Description* of the line, if you intend to use more than a single line. As long as all required parameters are not set properly, the status is signalized by a little red sign in the line icon.

The *Communication timeout* parameter defines the response timeout of the devices bound to the communication line. It is meaningful to change the parameter when using remote connection to the converter (e.g. using GPRS, VPN, etc.). The default value is 750 ms.

The communication with the modules at the line can be disabled by using the option *Temporarily disconnect*. In that case the communication with modules bound to the line is not established at all.

5.1.2 Serial line

For adding a new serial line, open the *Hardware and communication* dialog. Fill in the *Port* parameter (*pic. 6*) – if you use an *USB > RS 232* converter, you can find the name of the port in *My computer* > *Manage* > *Device manager* > *Ports (COM and LPT).* We recommend filling in a unique *Description* of the line, if you intend to use more than a single line. As long as all required parameters are not set properly, the status is signalized by a little red sign in the line icon.



Pic. 6: Serial line

The *Communication timeout* parameter defines the response timeout of the devices bound to the communication line. The default value is 750 ms.

The communication with the modules at the line can be disabled by using the option *Temporarily disconnect*. In that case the communication with modules bound to the line is not established at all.

After creating communication lines, it is possible to bind the APS mini Plus modules to them.

Note: If the master password is set, it is not possible to change the values until the dialog is unlocked by pressing the *Unlock* button and entering the password.

5.1.3 RS 485 line testing

The connection of the modules at the RS 485 BUS can be tested with a broadcast sent by choosing the *Test 485* command in the communication line context menu. After sending the broadcast all modules should start blinking with red and green diode.

Note: The *test 485* function is supported by modules with FW version 5.1 or newer.

5.2 Module HW address

Each module on the communication line needs to have a *unique HW address* set to work properly. The address is set either by the configuration of address jumpers on the module or by the *APS Reader* program (according to the HW type, see *tab. 1*).

HW address setting	Product line	Type
	xRIF 32, xREx 53, xREM 55, xREM 57, xREM 57U, xREM 58, xREM 59, xREM 63, xREM 64, xREM 65, xREx 73, xREP 78, xREM 79, xREM 80, xREM 81, xREM 82[2)]	SW
	xREM 54, xREM 56, xREM 76, xWGD 46[6)], xABA 46[6)], xRRF 12, xRIF 232	HW
	xDEM 31	SW or via the terminal screen configuration

Table 1: Type of HW address setting procedure

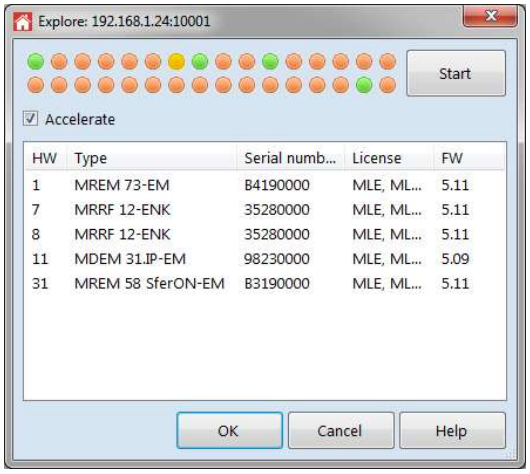
[1)] These modules occupy two (or more) addresses; the first one is set by the HW jumpers' configuration, the second (and other) one is greater by one.
[2)] The MREM 82 MTMBOX-MF can occupy 1-32 successive addresses (first address and the count of them are user configurable).

An easy search for all modules connected to the communication line can be performed by pressing selecting the *Explore communication line* option in the context menu of a line.

In the dialog (*pic. 7*) you can select the *Accelerate* option to speed up the line search. Press the *Start* button to begin the search. Following information is displayed in the result:

- *HW address*
- *HW types*
- *Serial number*
- *Licenses*
- *FW*

If there is any HW address conflict on a line, no module can be found on the address or the parameters read can be incomplete or wrong.



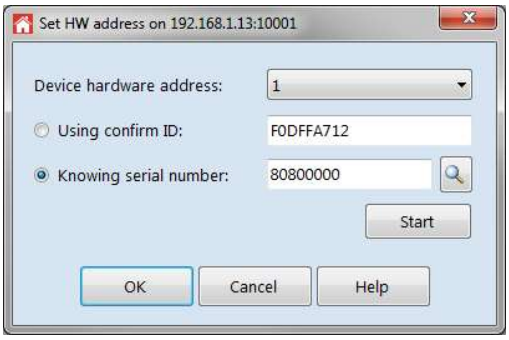
Pic. 7: Searching the communication line

5.2.1 Software setting of the module HW address

The software setting of the module HW address is available in the *Set HW address* dialog available from the context menu of the line.

5.2.2 Setting HW address of a module with a known serial number

If you know the serial number of a module (the simplest way to set the address), select *Knowing serial number* at the *Device* tab and fill it in the adjacent input field (*pic. 8*). Choose required *HW address* then (within range *1 ÷ 32*) and press the *Connect* button. After pressing the *Set address* button, the required module HW address is set.



Picture 8: HW address setting

5.2.3 Setting HW address with a "confirmation ID"

The second way of setting the HW address (less comfortable, but not requiring the knowledge of the module's serial number) is reading a confirmation ID in the HW address setting mode. Fill in a known ID of an identification medium in the field adjacent to the *Using confirmation ID* option in the Set HW address dialog; the medium will be used for setting the module HW address (*pic. 8*). Choose required HW address then and press the *Connect* button. Do not forget the address must not be occupied by another module! Press the *Start* button, modules at the communication line will be brought to the HW address setting mode, in which the module awaits reading the confirmation ID (this mode is indicated by flashing of green and red LED at the modules). Read the confirmation ID at required module, the HW address will be set and the communication with the module will start (at the moment the HW address setting mode is terminated).

The HW address setting procedure must be repeated for every module, where the HW address is set with the software, until all HW addresses are unique.

Note: The confirmation ID can be created from any common card (*except for programming cards*) by connecting a single module to a communication line (its HW address can be easily found with searching the line then), and reading a card at the reader. The card ID can be found for example in the events archive then.

Once the modules connected to a communication line have their unique HW addresses set, they can be added en masse with the *Explore communication line* option in the context menu (*pic. 7*). After the line is explored, press *OK* to bind all found devices to the communication line.

For adding a single module, choose the *New module* button.

5.3 Module parameters setting

5.3.1 Available functional parameters setting according to module's FW version

Once a successful communication between the program and an APS mini Plus module is established, information about the module firmware version is read. Basis this information only meaningful parameters setting is enabled, other parameters setting is disabled.

The module function change list (according to its HW type and FW version) is displayed in *table 2*.

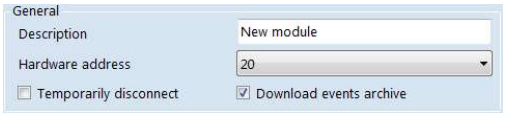
Available function	FW version	Available functions
	until 4.06	WIEGAND output configuration, Keypad function configuration, Door control, HW address setting using a confirmation ID, Alarm and its acoustic signalization setting
	since 4.07	HW address setting using serial number of the module, Events archive saving setting, Summer time adjustment setting, ID keypad block time setting, WIEGAND input configuration[6)]
	since 4.10	User configuration of EM Marin IDs reading[7)], door lock relay function – standard / toggle, permanent lock release according to a time schedule, PIN code demand suppression according to a time schedule[3)], Door lock indication with yellow LED, Module advanced function[4)]
	since 4.11	Supporting ABLOY APERIO wireless locks (xWGD 46 modules)
	since 4.13	Standard operating mode with IDS control setting [5)]
	since 4.14	Firmware upgrade using bootloader function
	since 5.00	Antipassback, ID with alarm flag, Access rights expiration functions
	Since 5.01	RS 485 BUS testing broadcast
	Since 5.04	Suppress PIN request when disarming IDS according to a time schedule [5)]
	Since 5.08	Setting of the 2nd and 3rd input as blocking; configurable function of ignoring Mifare sector data read at the Aperio reader [4)]
	Since 5.09	Reading synchronization setting (using IO port 3 or Wiegand interface)
	Since 5.10	Configuration of the 1st input, Release lock with REX button while tamper is active function
	Since 5.11	Setting of Online authorization of access rights function parameters
	Since 7.00	Configuration for dual readers 125 kHz and 13,56 MHz, possibility to enable / disable reading of individual ID technologies
	Since 7.01	Configuration of blanking filters for outputs of selected module types
	Since 7.02	Configuration of HW addresses count for modules MREM 82 MTMBOX-MF

Table 2: Available configuration of APS mini Plus module function

[3)] This setting is only available for modules with keypad and xWGD 46.
[4)] This setting is only available for xWGD 46, xABA 46.
[5)] This setting is only available for xREP 73 and xREP 78 modules.
[6)] This setting is only available for modules with Wiegand input.
[7)] This setting is only available for modules with 125 kHz RFID readers.

5.3.2 Module general parameters

After inserting a module in the Hardware and communication dialog set up the general parameters (*pic. 9*).



Pic. 9: General parameters

- *Description* – a description text, which will be used in the events archive – we recommend to fill it in meaningfully
- *Hardware address* – a HW address of the module set either by the SW settings or by the module's address jumpers' configuration (see *table 1*).

Other parameters setting will be enabled after the device information is read from the device (for connecting to the device close the *Hardware and communication* dialog and press the *Connect* button at the top toolbar).

The communication with the module can be disabled by using the option *Temporarily disconnect*. In that case the communication with the module is not established at all. The events archive downloading can be switched on/off by changing the status of the *Download events archive* checkbox.

5.3.3 Door control

The *door control* options enable to set the door lock behavior, the beeper, maximal door open time and the second input function (*pic. 10*). All parameters detailed description can be found in *table 3*.

Picture 10: Door control

Door control	Parameter	Default value	Value range
	Strike time [seconds]	7 s	0 ÷ 255
	Ajar time [seconds]	20 s	0 ÷ 255
	Strike control	Direct	Direct / Reverse
	Door lock relay function	Standard	Standard / Toggle / Pulse
	Permanent door lock release	Never	Never / Time schedule
	Beep type (copy strike release)	YES	YES / NO
	Input 1 function	Door contact	Door contact / REX button
	Input 2 function	Request to exit button	Request to exit button / Handle / Tamper / Disabling
	Input / Output 3 function	Tamper	Tamper / Disabling / Signal for external buzzer / IDS status monitoring / Reading synchronization

Table 3: Configurable parameters

- *Strike time* sets the maximal time of the strike release (unless the door is opened before the time expires)
- *Ajar time* sets the time, after which the “Door ajar alarm“ occurs, if the door stays opened any longer
- *Strike control* defines the state of the output when the strike is released or closed. When direct control is set, the output is activated on strike release and deactivated on strike close. When reverse control is set, the strike control is vice versa.
- *Door lock relay function* defines module behavior when door open command is performed. In the *standard* mode the door lock is released for preset time and locked again, in the *toggle* mode the door lock relay status is changed. In the *pulse* mode the Door open function makes an impulse with the door lock output for a defined time given by a configurable *Pulse width* parameter (with a 10 ms step)
- *Permanent door lock release according to a time schedule* – if set, the door lock is permanently released when the time schedule is valid
- *Beep type* sets whether the strike release is announced by a beeper (*Copy strike release*) or the module remains silent (*Silent*).
- *Input 1 function* defines the function of the first input of the module. When set to *Door contact*, the contact monitoring the door status should be connected to the input. When set to *Request to exit button*, the *Open door* function is performed when the button is pressed.
- *Input 2 function* defines the function of the second input of the module. When set to *Handle*, the door can be opened without triggering a Forced Door alarm when the handle is pressed. When set to *Request to exit button*, the *Open door* function is performed when the button is pressed. When the *tamper* value is set, the module expects connecting an external tamper contact. *Disabling* configuration enables to block access of the users with access defined by time schedule or block remote door open function by setting relevant status at the input.
- The *Input / output 3 function* defines the function of the third IO port. The setting is bound to the operating mode of the module. If the module works in mode with entry reader, the function is always *Signal for external reader buzzer control*; When IDS control operating mode is set, the function is *IDS status monitoring*. In other cases, the function is configurable to *Tamper* or *Disabling* function (same as above). Since the FW version 5.09 it is possible to set the *Reading synchronization* driven by *IO port 3* status. The function can operate in *MASTER* or *SLAVE* mode.

5.3.4 Alarms setting

Module recognizes 6 types of alarm states (*pic. 11*): *Tamper*, *Forced door*, *Door ajar*, *Antipassback*, *ID with Alarm flag* and *Output overload*. If you do not want to evaluate any of the states, set the value to zero. If the value is greater than zero, module activates its alarm output if the alarm condition is met and announces the alarm status for the time period set by the value. The alarm parameters overview is described in *table 4*.

Picture 11: Alarms etting

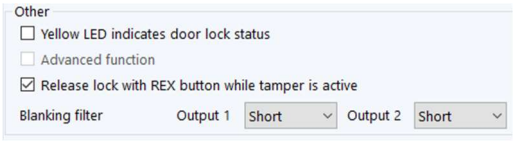
Alarms setting	Parameter	Default value	Value range	Beep on alarm	Set alarm output
	Tamper	30 s	0 ÷ 255	Yes	Yes
	Forced door	30 s	0 ÷ 255	Yes	Yes
	Door ajar	0 s	0 ÷ 255	Yes	Yes
	Antipassback	0 s	0 ÷ 255	Yes	No
	ID with Alarm flag	30 s	0 ÷ 255	No	Yes
	Output overload	30 s	0 ÷ 255	Yes	Yes

Table 4: Alarms setting

- *Door ajar alarm* sets the time the Door ajar status is signalized
- *Tamper alarm* sets the time the Tamper alarm status is signalized
- *Forced Door alarm* sets the time the Forced Door status is signalized
- *Antipassback alarm* sets the time the Antipassback alarm is signalized
- *ID with Alarm flag* sets the time the ID with Alarm flag alarm is signalized
- *Output overload* sets the time the Output overload alarm is signalized

5.3.5 Other options

These settings affect general behavior of a module (*pic. 12*).



Picture 12: Other configuration options

To allow *indication of door lock status by yellow LED*, check the appropriate checkbox. If the option is set, the LED flashes when the door lock is released.

Selected modules can be configured for operating in *advanced function mode*. The modules exact function in advanced mode is described in appropriate data sheets.

Furthermore, the function *Release lock with REX button while tamper is active* can be enabled or disabled.

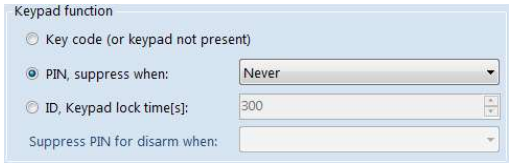
Note: When setting the advanced function or summer time adjustment at dual address modules (*see tab. 1*) the setting is automatically applied to both addresses of a module.

The outputs of selected module types are equipped with *current short-circuit protection* with a current value of 1 A. This current protection is enabled by default. In case of capacitive load, the current limit can be reached and the output will be disabled. If it is a short peak current pulse, it is possible to turn on the "blanking time" filter. This function disables the current protection for a short time so that this peak can be bypassed. Then the current protection is activated again.

The setting can be made in the range Off - Short - Medium - Long (the setting corresponds approximately to the values 0 µs – 60 µs - 80 µs – 100 µs). To protect the el. circuits of the module, it is recommended to choose the shortest possible value of disabling the current protection.

5.3.6 Keypad function

The keypad function can be set after selecting the *Keypad function and ID format* node belonging to a module. Setting up the keypad function is only enabled where it is meaningful. Available options for a module with a keypad can be seen in *pic. 13*.



Picture 13: Keypad function

The keypad function setting can be set to one of the following options:

- *Key code (or keypad not present)* – this option is used when a module without any keypad is used or when a keypad is used for entering a reason for exit.
- *PIN* – with this option selected the keypad is used for entering PIN codes, a correct PIN is required for valid identification when this option is selected; furthermore you can select a time schedule, which will cause the module to suppress PIN code requirement for a valid identification, when the time schedule is valid.
- *ID* – this option enables entering a code at the keypad which is used as a user's read ID medium; the time for locking up the keypad when an unknown ID is entered 5 times in a row can be set there as well, the setting range is from 0 to 2550s with a 10s step.

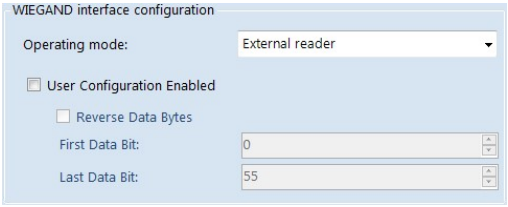
Since the *FW version 5.4* the *Suppress PIN for disarm function* is supported. In case the Wiegand interface is configured to IDS control function, it is possible to select a time schedule, which suppresses the PIN demand for IDS disarm function, when valid. Moreover, it can be set to suppress: always / never.

5.3.7 WIEGAND interface configuration

The *WIEGAND interface* of a module can be always configured to the operating modes, which are meaningful for the given module type.

In the *Standard operating mode,* the interface is used for remote control of the *WIO 22 relay module* (the WIO 22 module outputs copy the status of the module door lock control and alarm outputs).

Some modules feature a *WIEGAND input*, which allows connecting a *reader with WIEGAND output*. Setting up the operation mode determines the function of connected reader (*pic. 14*).



Pic. 14: WIEGAND input configuration

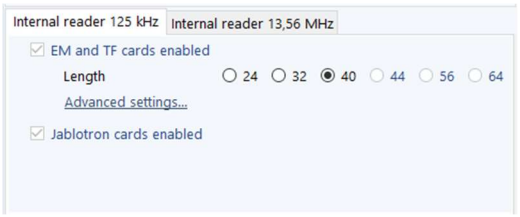
If the operating mode is set to *Standard*, the external reader is not involved; if set to *Entry reader*, the identification events raised at the reader have a reason code 255 assigned; if set to *External reader*, the internal reader of the module is turned off and the chosen reasons are assigned to the identification events raised at the external reader. Furthermore, it is possible to use the *user configuration of WIEGAND* input. By default, the user configuration is not used. To enable user configuration, check the appropriate checkbox. Set the indexes of the first and the last data bit. If required, choose the *Reverse data bytes* option.

Note: User configuration of *WIEGAND input* requires a deeper knowledge of the issue; we recommend leaving the setting to an installation company.

The *xREP 78* modules can be configured to the *Standard with IDS control* operating mode. In this mode the WIEGAND interface is used for controlling a WIO 22 module used for control of the IDS. It is necessary to define the way of controlling the IDS – the module can either use the *Status control* or *Pulse control* – in the second case it is possible to set up the width of the pulse in the range of 0 ÷ 25500 ms with a 100 ms step.

5.3.8 Read ID interpretation

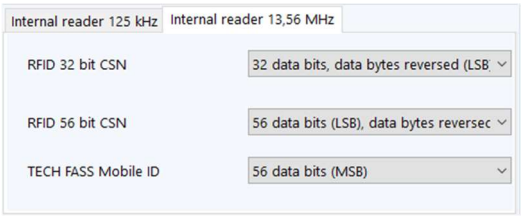
A *standard reader module with an integrated 125 kHz reader* can read *EM Marin and Jablotron*. When reading an ID the code is formatted first (*pic. 15*) and the module hereafter works with the code in the new format. Reading of individual types of ID media can be enabled/disabled.



Pic. 15: Read ID125 kHz interpretation

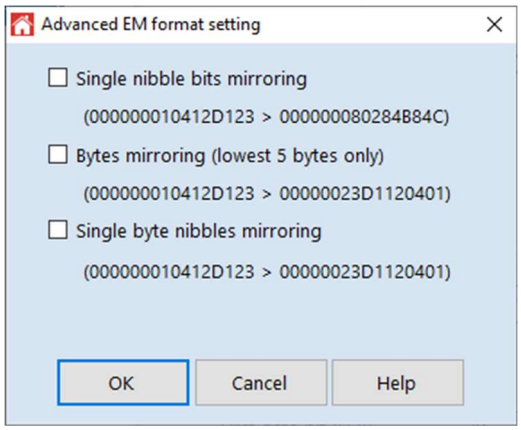
The ID codes of the *EM Marin* technology media can be formatted to *24*, *32*, *40* or *44 bits* format. The default value is *40 bits*, in this configuration the ID code is not changed.

If the reader module has integrated *13,56 MHz antenna*, you can also configure the length and orientation of *32bit* and *56bit CSN* and mobile application *TECH FASS Mobile ID* (*pic. 16*).



Pic. 16: Read ID 13,56 MHz interpretation

If there is further need to change the interpretation of the EM Marin media code, press the *Advanced settings* link. In the displayed dialog (*pic. 17*) you can change any combination of changes in the code interpretation.

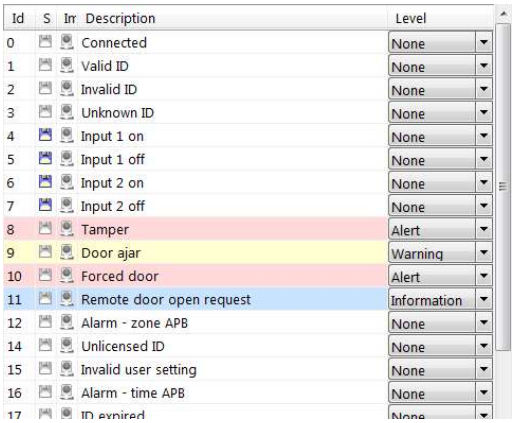


Pic. 17: Advanced EM Marin format setting

Note: User configuration of *Advanced settings of the EM Marin code interpretation* requires a deeper knowledge of the issue. Therefore, we recommend leaving the setting to an installation company.

5.3.9 Events description and saving

The module events description can be set after choosing the *Events description* node in the tree of the *Hardware and communication* dialog. In the right part you can find a list of every possible event (*pic. 18*), that can occur in the system. After a module is added to a communication line the descriptions are set to default descriptions of the selected program language. The descriptions can be altered after double-clicking the description text. Furthermore, it is possible to set a *Level* of attention to every event type. The levels of attention are distinguished in color in the events archive and online events view – the information level is blue; the warning level is yellow and the alert level is red.



Id	S	In	Description	Level
0			Connected	None
1			Valid ID	None
2			Invalid ID	None
3			Unknown ID	None
4			Input 1 on	None
5			Input 1 off	None
6			Input 2 on	None
7			Input 2 off	None
8			Tamper	Alert
9			Door ajar	Warning
10			Forced door	Alert
11			Remote door open request	Information
12			Alarm - zone APB	None
14			Unlicensed ID	None
15			Invalid user setting	None
16			Alarm - time APB	None
17			ID expired	None

Pic. 18: Events Description

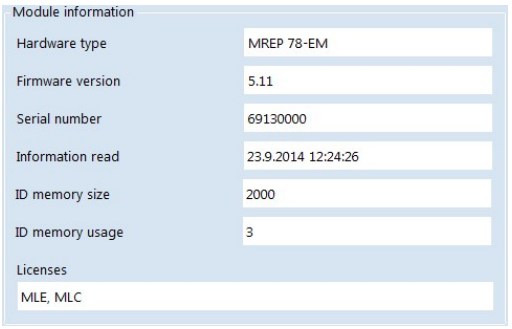
Furthermore, it is possible to *suppress saving of certain events*, which leads to a saving of the module's memory in the events archive when the module goes offline. Suppressing and enabling of the event saving is realized by clicking the diskette icon of the appropriate event (codes 4, 5, 6, 7, 64, 65).

5.3.10 Aperio – autodetection of Mifare sector reading

The older version of *Aperio* wireless locks FW occasionally misinterprets *Mifare DESFIRE* IDs as Mifare sector data IDs. This error can be compensated from the ACS side by selecting *Disable auto detection of Mifare sector data*.

5.3.11 Module Information

Module information (*pic. 19*) is available after choosing the *Module information* node in the tree of the *Hardware and communication* dialog. In the right part of the window you can find the newest read information about the *Hardware type*, *Firmware version*, *Serial number*, the *date* of the last information update, *ID memory capacity* and *usage*, and present *Licenses* (older FW version modules).

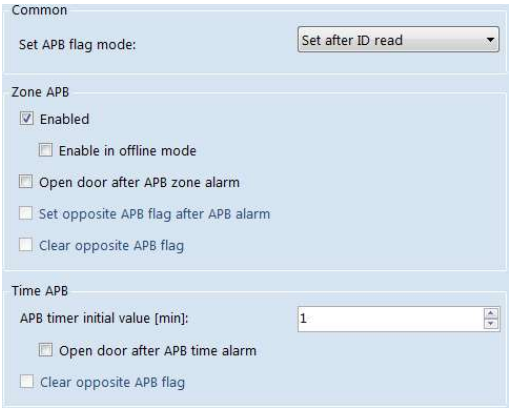


Pic. 19: Module information

5.3.12 Antipassback

The Antipassback function is in the APS mini Plus modules implemented in two types:

- *Time APB* – user cannot repeatedly use his ID for defined time
- *Zone APB* – user cannot repeatedly enter an area, where he is already present



Pic. 20: Antipassback options

The Antipassback function is used *only for the users*, whose access is driven by a *time schedule*. The users with access always granted are not affected by the Antipassback function. *All Antipassback flags* are *reset* whenever new *access rights data are downloaded* from the program.

The setting of the parameters affecting the Antipassback function evaluation is available at the Antipassback tab (*pic. 20*).

Both Zone and Time Antipassback flags are written either immediately *after an ID is read*, or after relevant *door is opened* (relevant input is disconnected).

5.3.13 Time Antipassback

The *Time Antipassback* is defined by the *ABP timer initial value* (in minutes), which is set to the ID after passing at the relevant address. If the users uses the ID at the address during the timer for the ID is running, the Time APB alarm is raised. Following parameters affect the Time APB function:

- *APB timer initial value* – defines the Time APB flag (timer) value set to the ID after passing at the relevant address. If a user uses the ID again before the timer elapses, Time APB alarm is raised.
- *Open door after APB time alarm* – if the option is enabled, the Door open function is performed after the Time APB alarm is raised.
- *Clear opposite APB flag* – if the option is enabled, passing at the relevant address causes a reset of the APB timer flag at the opposite side of the module.

5.3.14 Zone Antipassback

The *Zone Antipassback* is defined by *enabling the option* for the relevant address. The Zone APB flag is set for the ID when passing at the relevant address. If a user uses the ID again when the Zone APB flag is set, the Zone APB alarm is raised. Following parameters affect the Zone APB function:

- *Enabled* – enable/disable general Zone APB flag setting.
- *Enable in offline mode* – if the option is not set, the module operates in offline mode like if the APB function was not implemented.
- *Open door after APB Zone alarm* – if the option is enabled, the Door open function is performed after the Zone APB alarm is raised.
- *Set opposite APB flag after APB alarm* – if the Zone APB alarm is raised, the Zone APB alarm flag is set for both sides of the module.

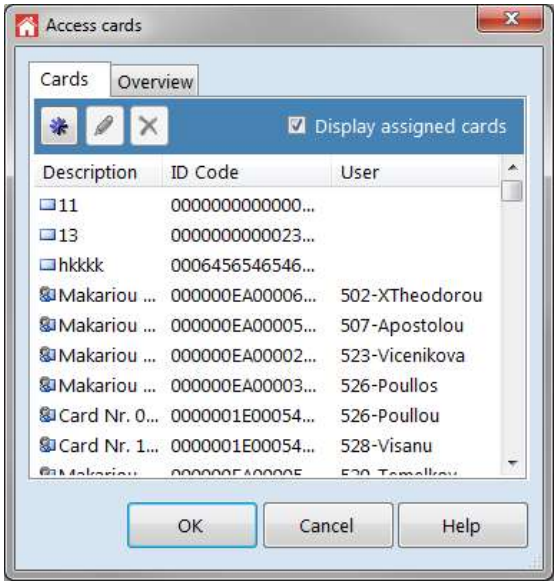
Clear opposite APB flag – if the option is enabled, passing at the relevant address causes a reset of the Zone APB alarm flag at the opposite side of the module. Note: Controlling zone antipassback by the door controller locally is obsolete and it is not supported by the system management software. Use APS Administrator with online authorization to ensure full control of the antipassback function across the entire system.

6 Access cards

Inserting cards into the database can be done in several ways – via a *microreader*, by *reading cards on any reader in the system* of from the *events archive*.

6.1 Access cards administration

The access cards overview is available after choosing System > Access Cards in the main menu of the program (*pic. 21*).



Pic. 21: Access cards administration

The *Cards* tab contains a list of cards with card *Description*, *ID Code* and eventually assigned *User* name. Icon meanings are described in *table 5*. The cards assigned to users can be hidden/displayed by changing the *Display assigned cards* option.

A new card can be created in the tab by selecting the *New card* button; *Card description* can be edited by choosing the *Edit* button. When editing the ID properties, the *Alarm – ID flag* can be *set*. After using such ID in the system, the *Alarm – ID* alarm is raised. *ID Code* of the card can be also inserted in the *Edit card* dialog by using a *microreader*. Press the *Delete* button to delete selected cards.

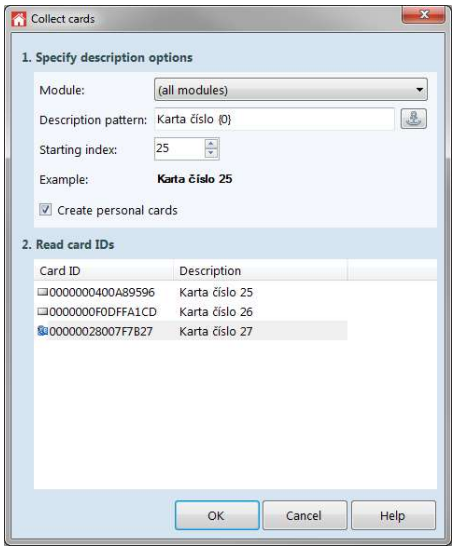
The *Overview* tab offers an overview of assign, unassigned and a total number of cards saved in the database.

techfass®

6.2 Colleting cards by online reading in the system

Choose *System* > *Collect cards* in the main menu of the program. Set the parameters displayed in the dialog (*pic. 22*).

- In the *Module* option select module(s) you wish to use for the cards collecting (including a microreader)
- *Description pattern* indicates a name assigned to collected card (string {0} is replaced by an ordinal number of a card)
- *Start index* parameter indicates the starting ordinal number
- *Example* shows a name of the first collected card.
- Check the *Create personal cards* checkbox if you intend to create personal cards to collected cards



Pic. 22: Collecting access cards

By reading cards at selected modules, the cards are inserted in the list of collected cards in the bottom part of the dialog. Icons in the *Card ID* column indicate if the card was already found in the database. The icon meanings are displayed in *table 5*.

Icon Meanings	Icon	Meaning
		Unknown card
		Deleted card formerly present in the database
		Known unassigned card
		Known card assigned to a user
		Known card with Alarm – ID flag assigned to a user
		Known unassigned card with Alarm – ID flag

Table 5: Card icons meaning

If you want to remove some cards from the *Collected cards* list, select *Delete* in the context menu. You can change the order of the cards in the list in the context menu. If there are existing cards present in the selection, their descriptions will be altered only.

After collecting all required cards, setting their order and removing unwanted cards, choose *OK* to insert cards into the database. For canceling the action press the *Cancel* button.

6.3 Inserting cards from the events archive

Choose *Events* > *Open archive* from the program main menu. After selecting all events with the card IDs you want to collect, press the *Collect cards* button. A dialog similar to the one in chapter 5.2 (*pic. 20*) is displayed; all parameters and icons meanings are identical. After selecting all required parameters and cards press the *OK* button to insert the cards, or press the *Cancel* button to cancel the action.

7 User administration

All users list is displayed in the right part of the main program window (*pic. 1*). Users can be sorted by any of available columns. The sorting column can be selected in the context menu opened from the All users list. You can also change displayed columns selection in the context menu. The meaning of the icons displayed in the All users list is described in *table 6*.

Icons	Icon	Meaning
		A user with a temporarily denied access to all modules in the system
		A user with no access card assigned
		A user with an access card assigned and access granted
		A user with an assigned card, access granted and set expiration date
		A user with an assigned card access granted and already expired

Table 6: Meaning of icons in all users list

7.1 Working with users

A new user can be created by pressing the *New* button in the main program window or by choosing *Users* > *New* in the main program menu, or by selecting *New* in the *All users* context menu. The simplest way to create users is by collecting cards and their inserting with *Create personal cards* checkbox checked (chapters *5.2*, *5.3*). The changes of users' parameters can be done after selecting the user and choosing *Edit* in the *Users* menu or by pressing the *Edit* button. Users can be deleted by pressing the *Delete* button. When deleted the user is displayed in *Users > Deleted users…*

You can also assign a user to selected area or choose to display events archive of the user in the selected user's context menu.

Since version *1.0.3982.19080* the program supports the search function in all users' list. To run the function, select *Users* > *Find*, or use the shortcut *CTRL + F*. After entering the text and pressing ENTER, the rows containing at least one field with the text or its part are highlighted. The buttons *Find next* or *Find previous* can be used to move among the records. The function is closed by pressing the *Close panel* button or by pressing the *ESC* key.

Since version 1.0.6698.27427 the program supports renewing deleted user, *Anonymize* function and exporting digital footprint due to the GDPR policy.
To export digital footprint, select *Export footprint…* in the context menu of a user.
To renew a deleted user open *Users > Deleted users…* and select *Renew* in the context menu of selected user. The user is renewed withou acces cards and areas.
To anonymize a user delete him first. Then open *Users > Deleted users…* and select *Anonymize* in the context menu of selected user. The user and all personal data are deleted from the program including events archive.

techfass®

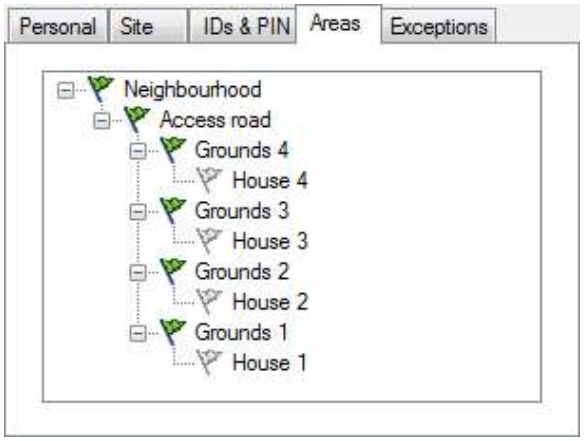
7.2 Personal card

Personal card of every user contains five tabs (*pics. 23-28*).

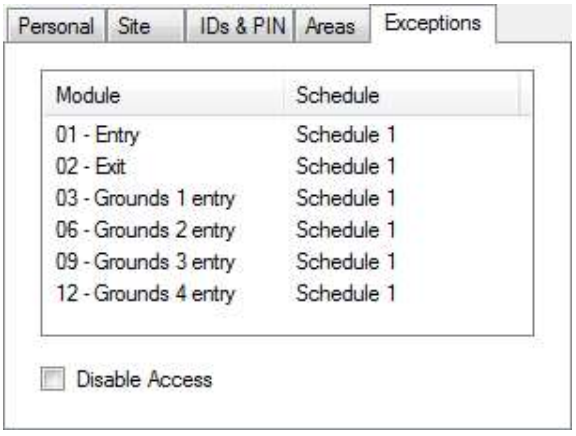
Pic. 23: Personal tab

Pic. 24: Site tab

Pic. 25: IDs & PIN tab



Pic. 26: Areas tab



Pic. 27: Exceptions tab

Pic. 28: Images tab

The *Personal* tab (*pic. 23)* is used to enter the personal data of a user: *Title*, *First* name, *Middle* name, *Last* name, *2nd Title*, *Phone* and *E-Mail*. The *Last* name is the only mandatory parameter.

The *Site* tab (*pic. 24*) enables you to fill in data about the user housing. Available parameters are: *Building*, *Entrance*, *Flat* and *Note*. These parameters can be also set en mass by selecting a group of users and choosing *Site Properties* in the context menu.

The *IDs & PIN* tab (*pic. 25*) enables you to assign *access cards* to a user and set his *PIN*. Only a value from 0 to 65535 is assumed as a *valid PIN*. After selecting the *Assign* button a dialog similar to *chapter 5.1* is displayed. The meanings of all buttons and symbols are identical. A microreader can be also used for collecting card IDs here. The last button at the *IDs & PIN* tab (*Release*) releases selected cards of the user. When the *Use expiration* option is set, an *Expiration date* can be set. When that date occurs, user's access rights expire. If the expiration date already occurred, the user's access rights are downloaded to the module as already expired.

The *Areas* tab (*pic. 26*) contains a tree of areas. The access level of a user is indicated by each symbol and its color. Symbols and their colors meaning overview is displayed in *table 7*.

Icon Meaning	Icon	Meaning
		The user is not assigned to the area, the access is denied
		The user is assigned to the area, the access is granted
		The user is assigned to the area, the access is denied
		The user is assigned to the area, the access is driven by a time schedule
		The user is assigned to the area, an exception is present

Table 7: The icon meaning in the Areas tab

The *Exceptions* tab (*pic. 27*) displays a list of access rights exceptions. If there is an exception set for a module, it has a *greater priority* than a default access for an area and therefore it is used for the user at the module. At the tab you can also globally disable access to every module in the system for the user by checking the *Disable Access* checkbox (appropriate for a temporal disabling of the access).

At the *Images* tab (*pic. 28*) you can assign a picture or a group of pictures to a user. To add a new image, press the + (plus) button; to remove selected picture press the – (minus) button. To save a selected image on disk, press the button with *diskette symbol*. If you want to change the order of images in the list, select appropriate image and use the buttons with *up* and *down* arrows.

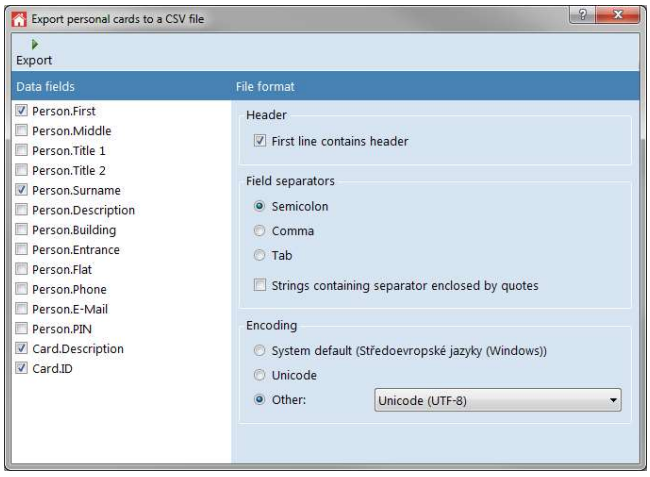
7.3 Data import and export

The program offers an option to import and export users' personal cards with their assigned cards. To *export* data select *Program* > Data import / export > *Export personal cards data to a CSV file*. To import data select *Program* > *Data import / export* > *Import personal cards data from a CSV file*.

Also there is a possibility to *Import lost events*. If the SQL Server gets temporarily unavailable while the events are being read from connected HW, the events cannot be saved in the database. Therefore such read events are saved in a *CSV file* directly on the computer disk. When the connection is reestablished, you can import them into the database using *Program* > *Data import / export* > *Import lost events* dialog.

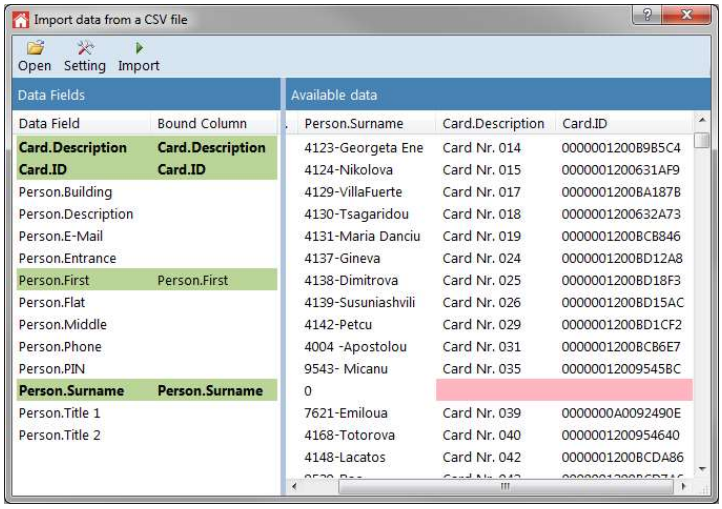
7.3.1 Personal cards data export

In the *Export personal cards to a CSV file dialog* (*pic. 29*) choose columns of the persons and cards tables you wish to export to a CSV file in the *Data fields* area. In the File format area choose the *First line contains header* option, if you wish the first row to contain a header with the exported columns description. Select the *field separators* and *encoding* of the file then. If you intend to use the exported file for inserting it in another *APS Home* database, it is necessary to export *Person.Surname*, *Card.ID* and *Card.Description* columns at least, since the columns are mandatory for import. After pressing the *Export* button select the path and filename of the exported file.



Pic. 29: Personal cards data export

7.3.2 Personal cards data import



Pic. 30: Personal cards data import

In the *Import data from a CSV file* dialog (*pic. 30*) open a CSV file with required data first by pressing the *Open* button. The next step is setting up the import options, which are available in a dialog opened by pressing the *Setting* button. Check the *First line contains header*, if the first row contains a header with columns description. Then choose the options of field separators and file encoding. After setting up the parameters, save the options by pressing the *OK* button. The next step is assigning the columns of the opened file to the data fields of the database. The assignment is done by *dragging* the selected *data field* with mouse *and dropping* it in desired column of the imported file (*Available data* area). The import requires to assign fields *Person.Surname*, *Card.ID* and *Card.Description*, other fields are optional. For data import press the *Import* button. If there are no data in one of the mandatory columns in the file, the row cannot be imported. After attempting to import such rows, the program designates relevant cells with *red background*. For a successful import it is necessary to remove such rows (by selecting the row and choosing *Remove* from the context menu) or fill in the missing data in an external program and reopen the file then. If you import a person with a card, which is already stored in the database, the card is removed from the original person and assigned to the imported one.

7.3.3 Lost events import

Open the import dialog using *Program* > *Data import / export* > *Import lost events* option. Select the proper CSV file, the events will be imported at once. The file extension will be changed in order to avoid importing duplicate events.

techfass®

8 Access rights

The access rights model is designed for easing access rights administration in objects like blocks of flats and others. Modules in the system are bound to a defined area, the access right of a user is defined by assigning him to an area – by this action the user gains the default access rights to every entry module of the area.

8.1 Areas

The *areas* are hierarchically sorted in a tree. A user assigned to an area automatically gains access rights to every parent areas of the given area. After selecting a user in the All Users list in the program main window, areas, which the user can access, are highlighted in *green*.

8.1.1 Area tree

The meanings of icons in the tree (*pic. 1*) are given by the *default access* to the area and by settings of the *modules* as entry or exit ones for the given area. The meaning of the icons is described in *table 8*.

Icons Meaning	Icon	Meaning
		Default access level in the area: Access granted
		Default access level in the area: Access denied
		Default access level in the area: Access driven by a time schedule
		Entry module of the area
		Exit module of the area

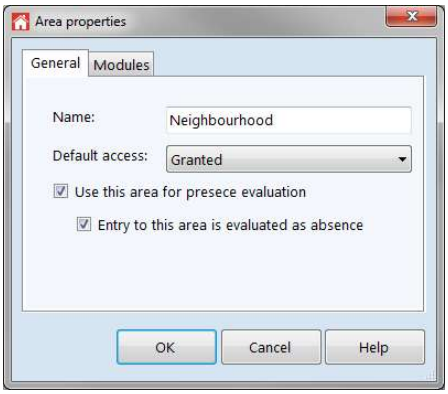
Table 8: The icon meaning in the Area tree

For creating a new area select a *new Root* area in the context menu of the Area tree, or create a *new Child* area of the selected area. Parameters of the area can be set in the *Area Properties* dialog, which is displayed after it is created.

8.1.2 Area properties

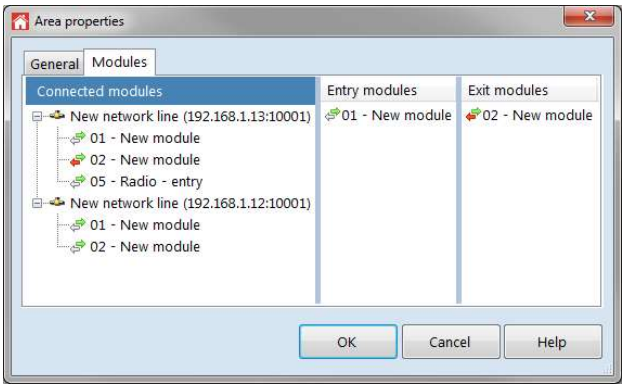
At the *Properties* tab (*pic. 31*) select a *Name* of the area and its *Default access* to the area. The access level will be assigned as a default access to all users, which will be assigned to the area. If there is a demand to set another access level for certain users or modules in the area, it can be done in the *examples* settings.

If you want to file the presence of users in selected area, choose *Use this area for presence evaluation*. If you want to count the time spent in the area as absence, choose *Entry to this area is evaluated as absence*.



Pic. 31: Area properties - General

At the *Modules* tab (*pic. 32*) assign *Entry* and *Exit* modules to the area. The settings is done by dragging a module from the left part and dropping it in the *Entry* or *Exit modules* area. In the left column there is a list of all Connected Modules. The meanings of icons are given in *table 9*.



Pic. 32: Area properties - Modules

Icon meaning	Icon	Meaning
		Network communication line, not configured
		Network communication line
		Network communication line, temporarily disconnected
		Network communication line, not configured, temporarily disconnected
		Serial communication line, not configured
		Serial communication line
		Serial communication line, temporarily disconnected
		Serial communication line, not configured, temporarily disconnected
		Module is not assigned to any area
		Module is not assigned to any area, temporarily disconnected
		Module is assigned to some area as an entry one
		Module is assigned to some area as an entry one, temporarily disconnected
		Module is assigned to some area as an exit one
		Module is assigned to some area as an exit one, temporarily disconnected
		Module is assigned as both an entry and an exit one to some area
		Module is assigned as both an entry and an exit one, temporarily disconnected
		Number of IDs assigned to a module exceeds its capacity!
		tf hit system module; such modules are incompatible with APS Home program.

Table 9: The icon meanings in Area properties and Hardware and communication dialogs

Assigning a module to an area as an *exit* one is only appropriate when the module does not lead from an area, which is a *parent* area of the area the module leads to. If a module is assigned to some area as an *exit* one, a user is allowed to access the module only if he is a member of *both* module's *entry* and *exit* areas.

If it is necessary to edit the area settings, choose *Change* in the area's context menu. The areas can be shifted up or down in the area tree by selecting *Move Up* or *Move Down* in the context menu. If you want not to display modules in the area tree, select *Hide Modules* option from the context menu. To display the modules again, choose *Show Modules*. To display events for selected module or area, choose *Show Events* in the context menu. It is possible to remotely open any door in the system by selecting *Open Door* from the context menu, when the communication is running. If you wish to display the door status in the buttons area, check the *Show* option in the module's context menu.

8.1.3 Double-sided door control

Some types of the APS mini Plus reader modules with integrated door controller are equipped with *Wiegand interface* able to operate as *Wiegand input*. Such modules are ready for connecting a *simple Wiegand output reader from the other side of the door* and thus perform very effective double-sided door control.

In case the double-sided access control (entry/exit) is used, it is necessary to *correctly assign the module functioning as the controller as entry module to given area*. If the *Wiegand output reader* (connected from the other side of the door) *does not lead from the area*, which is *direct superior* of the *entry area of the controller*, it is *essential to correctly assign the area, from where the Wiegand output reader leads* (assign the *controller as exit module from the area*)! With these settings correctly set the *proper distribution of access rights* and *proper evaluation of users' presence* at *Presence tab* is secured.

8.2 Access rights settings

Users' access rights settings are done simply – In the left column select an area; in the right column select users. By *dragging and dropping* the users from to the *middle part* you will set the *default access rights* to the selected users to the given area.

When any area or any module is selected, a list of users assigned to the selected object is displayed. The meanings of icons in the users list is described in *table 10*.

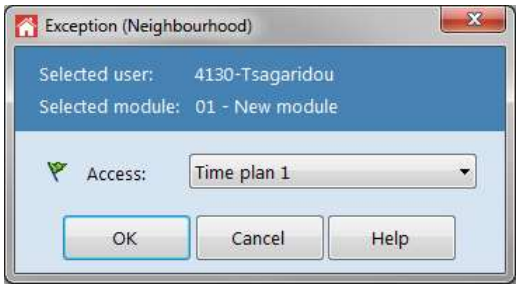
Icon Meanings	Icons	Meanings
		A user is not allowed to access the module, because he is not a member of the modules exit area
		An exception is set for the user and selected area or module
		User's access to all modules in the system is temporarily denied (see *chapter 6*)
		A user with a default access for selected area or module

Table 10: The meanings of icons in assigned users list

The user access rights setting can be copied to a clipboard and pasted to other users. After a source user is selected, choose the *Copy access rights* option from the context menu. Choose destination users and select *Paste access rights* option from the context menu. In the displayed copy options dialog select required type of the copy method.

8.3 Exceptions

If it is necessary to set a different access level than the default one to a user for an area or a module, create an *exception*. First assign demanded users to the area. Then choose either entire area or module and select demanded users in the middle area. In the context menu choose *Exceptions*. In the Exceptions dialog (*pic. 33*) check if your selection contains demanded users and modules, select demanded access level and save the exception by pressing *OK*.



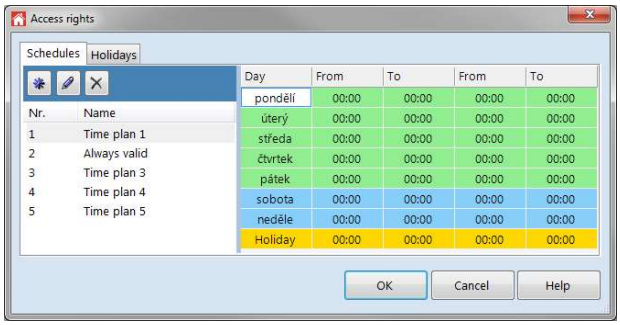
Pic. 33: Exceptions

8.4 Time schedules and holidays

It is necessary to define a time schedule before you can set it as an access level to an area or a module. The setting is done in the *Time schedules and holidays* dialog, which is available after choosing *Schedules and Holidays* option from the *System* menu.

8.4.1 Time schedules

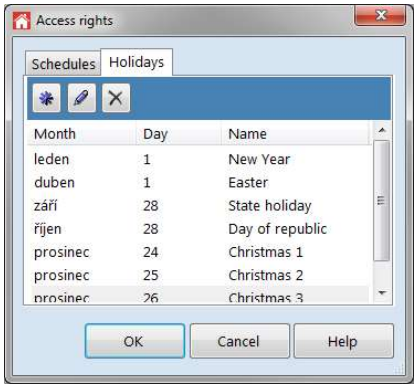
For creating a new time schedule, select the *New* button at the *Schedules* tab (*pic. 34*). Choose a *Number* and a *Name* of the schedule and save it by pressing *OK*. In the right part of the dialog you can define two time intervals for every day of a week and for holidays. The access is granted within the intervals, denied outside of them. Only days listed in the table of *Holidays* is considered as a holiday. If a user accesses a module in a time he is not allowed to, he raises an *Invalid ID* event. For altering a name or a number of a time plan, press the *Edit* button, for deleting press the *Delete* button. The time schedules can be copied and pasted via clipboard; pasted time schedules have the same time intervals definitions as the time schedules copied to the clipboard. The program offers an option to set a time schedule, which is always valid, by selecting the time schedule in the list and using the *Always valid* option (such time schedule can be handy for Antipassback function).



Pic. 34: Time Schedules

8.4.2 Holidays

For creating a new holiday press the *New* button at the *Holidays* tab (*pic. 35*). Enter a *Name* of the holiday and select a *day in a year* you wish to be considered as holiday. If you intend to set the *Easter* holiday, it can be automatically calculated and inserted from the context menu (do not forget to set the holiday after the New Year). For deleting holidays select demanded holidays and press the *Delete* button.



Pic. 35: Holidays

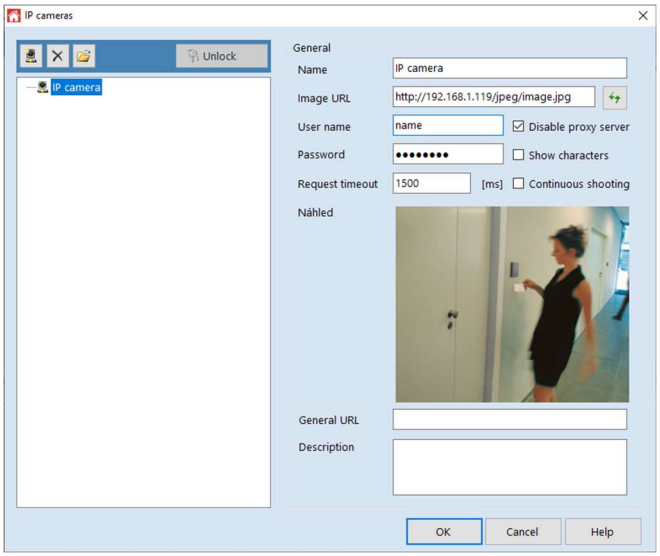
techfass®

9 IP cameras

The *IP camera support* is implemented since the program version 1.0.3779.19201. The option was introduced mainly for visual check of the user's identity basis an operating event in the system. Any IP camera with the option to download the *JPEG image* via the *HTTP GET request* is usable.

9.1 IP cameras setting

The IP cameras setting is done in the IP cameras dialog, which can be entered by selecting System > IP cameras (*pic. 36*).



Pic. 36: IP cameras dialog

For inserting a new camera, press the *New IP camera* button or select the command from the context menu. If you intend to delete a camera, do it by pressing the *Delete selected object* button or select the command from the context menu.

9.1.1 IP camera properties

After selecting an IP camera, it is necessary to set up its properties first:

- *Name* – an identifier of the camera in the APS Home program
- *Image URL* – http address, where the image from the camera in the JEPG format is available to download
- *Disable proxy server* – when processing the GET request, the automatic detection of the proxy server setting is bypassed (recommended setting)
- *User name* and *Password* – username and password for accessing the camera image, when it is required
- *Request timeout* – maximal time (in ms) of waiting for the camera response – if the camera does not respond to an image request in specified time, it is considered unavailable and the image is not saved
- *Continuous shooting* – if the feature is not used, a picture from camera is shot after the program sends a request to the camera (when this mode is used, the program automatically uses a higher communication rate to reduce the response timeout). If the feature is used, the camera sends snaps to the program continuously, then a request for image saving comes, the program saves the closest snap.
- *General URL* – for future use
- *Description* – IP camera description in APS Home program

Recommendations for *request timeout* setting:

- Set the camera with a response timeout about *5000 ms*.
- Set a rule for taking pictures and let it work.
- Open the cameras operation log (for opening the folder with logs use a new button in the *IP cameras* dialog) and use the average response timeout value multiplied by 2-3.

Relevant record in the log looks like this:

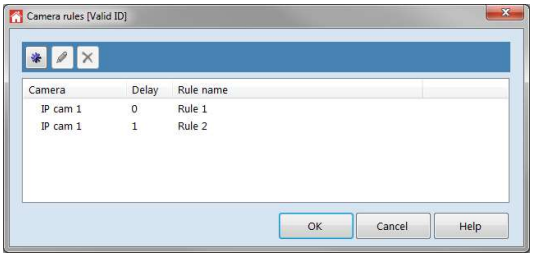
```
9.7.2010 8:38:53;Information;CameraThread;Cached image - Camera "Camera_Name" (IdCamera = 4, ImageURL = http://85.70.42.29/cgi-bin/video.jpg), dt = 828ms, response statistics = (avg: 738ms, min: 703ms, max: 781ms
```

The average response time (*avg*) is given in the camera response statistics.

If you want to display the content of the *Password* field, select the *Show* option. For verifying the picture accessibility press the *Refresh* button (next to the Image URL field), the picture appears in the *Preview* area when configured correctly. Before saving the configuration, it is appropriate to perform one test at least.

9.2 IP camera rules

The IP camera images saving is defined by a set of rules, which can be set by following procedure.



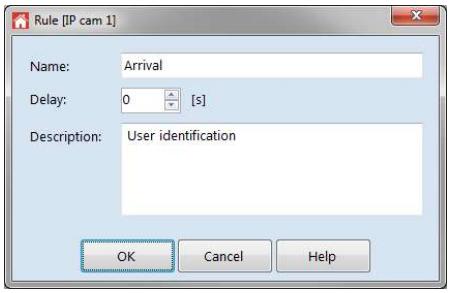
Pic. 37: Camera rules

The setting is available in the *Camera rules* dialog. The dialog can be entered from the *Hardware and Communication* dialog, when you select a module and its *Events description* settings. After double the *camera symbol* of the relevant event or selecting appropriate command from the context menu, the dialog is displayed (pic. 37).

For creating a new rule press the *New rule* button and select desired camera. For deleting a rule press the *Delete* button, for editing the rule press the *Edit* button. All commands are also available in the context menu.

9.2.1 Rule setting

In the *Rule* dialog (pic. 38) it is possible to set the IP camera rule. The *Name* parameter defines the rule name in APS Home program, *Description* is a n optional text description of the rule. The *Delay* parameter sets a time period between the event occurrence and taking the picture (in seconds). It is possible to take multiple pictures from a single camera and event by adding rules with different delay parameter.



Pic. 38: Camera rule setting

A negative delay can be set to the cameras using the continuous shooting mode; if the camera does not use this mode, the program displayes a warning.

techfass®

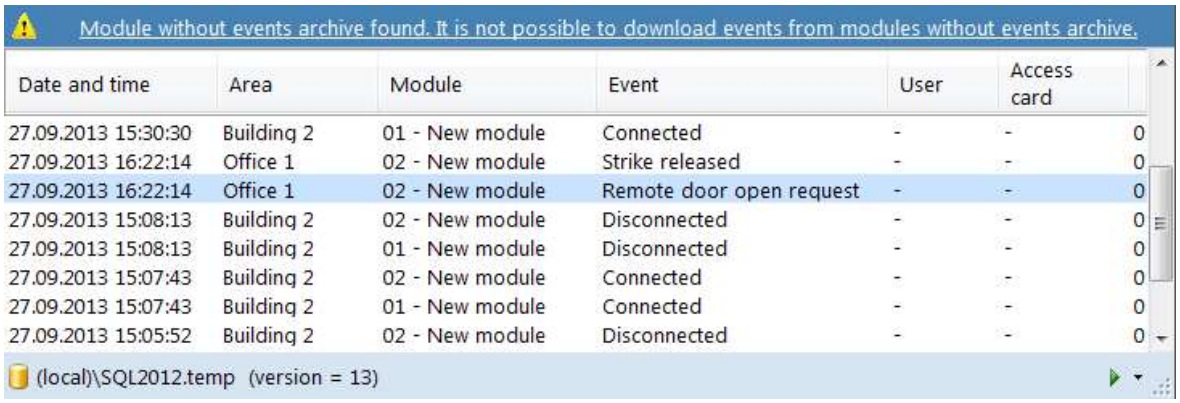
10 Events

In the lower part of the program main window you can find a list of events, which are being online read from the modules in the system. The events are being stored in the database immediately and are available in the *Events Archive* later.

Note: Do not forget, that only *APS mini Plus* modules (containing the *MLE* license) enable reading events from the system. Events from the modules without *MLE* license cannot be displayed in the program.

10.1 Online events reading

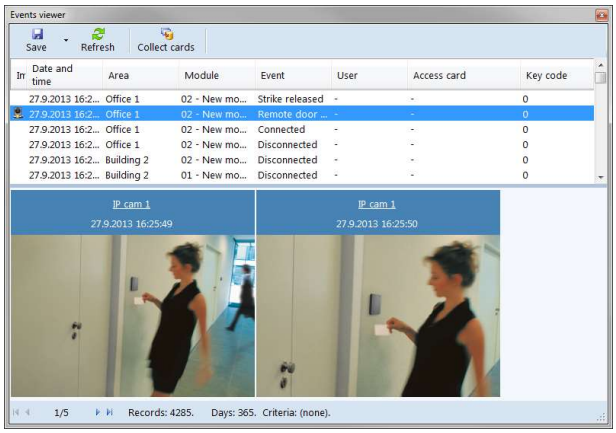
After connecting the program to the *APS mini Plus* system the events archives of connected modules are read (if the events archive reading is enabled). The events are displayed in the *lower part* of the *program main window* (*pic. 39*) in the order they are read from the system. Every event contains data about *Date and Time* of its occurrence, an *Area*, which is the module assigned to, a *Module*, which the event occurred on, a *User* if meaningful, an *Access Card* if meaningful, and a *Key Code* pressed as the event occurred. If there is any alert level set for the event, the record is highlighted by the corresponding background color. If the program detects a module without the *MLE* license, an attention with a link to a list of the modules is displayed.



Pic. 39: Online Events Reading

10.2 Events archive

The *Events Archive* is available after choosing the *Open archive* from the *Events* menu in the main program window (*pic. 40*).



Pic. 40: Events Archive

The *events* are sorted by the *Date and Time*; the same columns as mentioned in the previous chapter are displayed. In the upper part of the window you can press the *Save* button to save displayed events in a file in *.csv* format. You can insert cards in the database from the events archive by selecting relevant events and pressing the *Collect Cards* button. After pressing the *Refresh* button, the events archive is reread – therefore if there are new events happening in the system, they are displayed after pressing the button.

Since the program version 1.0.3779.19201 the IP cameras are supported. Every event archive record containing a picture is designated with a camera symbol in the *Im* row. When the record is selected, all pictures assigned to the record are displayed.

In the lower part of the window there is a list containing navigation buttons displayed. You can display older and newer pages of the archive by pressing the arrow buttons if the total number of events is higher than the maximal number of records displayed per page. The age of displayed events is maximally even to the number days set in the *Days* parameter. The number of days and number of records per page setting can be done in the program options dialog.

10.2.1 Filters

The program offers an option to display only events bound to a specific module, area or a user. If you want to display such events, select corresponding object and choose *Show events* in the context menu. Control elements and the button meanings are the same as in the previous description.

The events are stored in the database at the moment of their reading from the modules' event archives. If you change an area of a module, the events of the module in the archive will keep their formerly set area in their area column.

10.2.2 Events archive maintenance

Because the database size is limited (depending of the used server version), the program offers a comfort option to delete older events from the events archive and thereby save the database memory. The commands can be found in the *Events archive statistics and maintenance* dialog available by selecting *Events* > *Statistics and maintenance* in the main menu. Choose desired time period and select one of the options in the context menu. You can save the events in a *CSV* file or delete events in selected periods.

The archive maintenance operation can take a pretty long time. Therefore, in the *APS Home* program there you can set the maximal time of its duration. The option is available int the *Program options* dialog at the *Database* tab, which is available after selecting *Program* > *Options*. The default value of the *Maintenance commands timeout* parameter is *600 s*.

10.3 Event type meanings

Event types

##	Default description	Meaning
0	Connected	Communication with a PC has started
1	Valid ID	A valid card, access granted
2	Invalid ID	A known card without proper permission, access denied
3	Unknown ID	An unknown card (from the module's sight)
4	Input 1 on	Input 1 on
5	Input 1 off	Input 1 off
6	Input 2 on	Input 2 on
7	Input 2 off	Input 2 off
8	Tamper	Tamper alarm
9	Door Ajar	Maximal time for door staying opened was exceeded
10	Forced Door	Door forced
11	Remote Door Open Request	Opening door from a PC
12	Alarm – zone APB	Read ID which is already present
13	Power on (reset)	Device turned on / restarted
14	Unlicensed ID	Read ID is not an original TECHFASS ID
15	Invalid user setting	User setting is invalid, default setting used
16	Alarm – time APB	ID read while APB timer active
17	ID expired	ID expired (according to the expiration date)
18	Invalid ID (expired)	Read expired ID
19	Alarm – ID	Alarm – ID with Alarm flag read
20	Strike control – pulse	Door lock relay pulse performed
21	Identification with ID from a PC	Identification from a PC with user ID
62	Keypad unlocked	Keypad unlocked after lock time expiration
63	Keypad locked	Keypad locked after entering 5 unknown codes
64	Strike Released	Unlocked
65	Strike Closed	Locked
68	Armed	Signal from IDS – armed
69	Disarmed	Signal from IDS – disarmed
70	IDS control – pulse	Pulse for IDS status change

71	IDS control – disarm	IDS control output in disarmed status
72	IDS control – arm	IDS control output in armed status
73	IDS control – warning	IDS control warning status
74	Input 3 on	Input status changed in disabling mode
75	Input 3 off	Input status changed in disabling mode
76	Disabled	Module function disabled by input status
77	Enabled	Module function enabled by input status
78	Invalid (disabled)	Identification invalid, module disabled st.
79	Denied (tamper)	Function denied due to module tamper st.
80	Denied (disabled)	Function denied, module in disabled st.
81	Invalid (rolling code error)	Unexpected value of ID rolling code
82	Output 1 overload	Output 1 current limit was reached
83	Output 2 overload	Output 2 current limit was reached
84	Output 1 overload alarm	Output 1 overload alarm was activated
85	Output 2 overload alarm	Output 2 overload alarm was activated
86	Denied media read (125 kHz TF / EM)	ID media of the denied type was read
87	Denied media read (Jablotron)	
88	Denied media read (125 kHz)	
89	Denied media read (13.56MHz 32bit UID)	
90	Denied media read (13.56MHz 56bit UID)	
91	Denied media read (TECH FASS Mobile ID)	
206	Diagnostic information	Reserved for the manufacturer
207	Battery low	Reserved for APS Key
208	Automatic configuration correction	
209	Permanent door lock release started by time plan	
210	Permanent door lock release stopped by time plan	
211	Cancellation of permanent door lock release after repeated card read rejected	
212	Invalid ID - validity index low	
213	Permanent door lock release after repeated card read rejected	
214	Permanent door lock release after repeated card read	
215	Cancellation of permanent door lock release after repeated card read	
216	Programmer successfully authorized	
217	Invalid - before permission validity	
218	Cannot read from sector	The sector number is written in the “Key code” field
219	Invalid key for reading from sector	
220	Cannot write to sector	
221	Invalid key for writing to sector	

222	Foreign card (customer ID)	Reserved for APS Key
223	Foreign card (installation ID)	
224	Foreign programmer (customer ID)	
225	Foreign programmer (installation ID)	
226	Communication enabled after connecting foreign programmer	
227	Online authorization - unsupported result	Response type for online authorization request is not supported
228	Online authorization - unexpected result	Received a response for authorization request when no request sent
229	Online authorization - timed out	Response type for online authorization request was not received in time
230	Online authorization - waiting for previous result	New ID read while waiting for response for previous online authorization request
231	Online authorization - missing license	Online authorization request was not sent, the device does not contain proper license
232	Events archive overflow	Some events lost due to archive overflow
233	PIN duress	Duress PIN code entered
234	FW initialized	New firmware first run, configuration reset
235	Aperio events	Event of Aperio wireless lock
236	RTC power lost	Clock reset due to RTC power loss
237	Single ID Added	ID inserted in a server process
238	Single ID Deleted	ID deleted in a server process
239	Hardware Address Changed	Module HW Address was changed
240	Remote Configuration Downloaded	Configuration data downloaded from a PC
241	Remote Access Rights Downloaded	Access rights data downloaded from a PC
242	Remote Access Rights Deleted	Access rights data deleted from a PC
243	Service Mode Started – Insert ID	Service mode entered for inserting IDs
244	Service Mode Started – Delete ID	Service mode entered for deleting IDs
245	Service Mode – Delete All IDs	All IDs deleted in service mode
246	Service Mode Stopped	Service mode left
247	Service Mode – ID Inserted	A card inserted in service mode
248	Service Mode – ID Deleted	A card deleted in service mode
249	Tamper OK	End of tamper alarm
250	PIN Alarm	Alarm – invalid PIN entered 5 times in a row
251	PIN Changed	PIN changed
252	Invalid PIN	Invalid PIN entered
253	Door OK	End of door ajar or forced door alarm
255	Disconnected	Communication with a PC lost

Table 11: Event type meanings

11 Communication and data transfer

After setting up all parameters required for communication with the modules at the communication lines, connect to the system by pressing the *Connect* button. Program starts to communicate with all modules bound – first it reads general info available in the *Module information* info later. At the same time reading of the events archive is performed (on modules containing the event archive). When all events are read, the communication progress bar (in the right bottom corner) finishes.

11.1 Configuration download

The module configuration is uploaded to the modules immediately after pressing *OK* in the *Hardware and communication* dialog, if the communication is running. Otherwise the configuration is uploaded after connecting to the system and pressing the *Send data* button (the user data is sent as well). The finish of the downloaded is indicated by reading the *Remote configuration downloaded* event.

11.2 Sending all data

For uploading all parameters and access rights connect to the system and press the *Send Data* button. As soon as the access rights are downloaded to the system, *Remote Access Rights* Downloaded event is read from the events archive.

11.3 Communication status

The communication status is indicated by an icon displayed in the bottom right corner of the program main window. After clicking the icon all communication lines status icons are displayed separately. To display all details of the errors, select the specific communication line. The icon meanings are described in *table 12*.

Icon Meanings	Icon	Meaning
		The communication with all bound modules is successful
		The communication is stopped
		Communication error – probably a communication converter settings error
		Communication error – probably could not establish connection to one of the modules bound

Table 12: The communication icon meanings

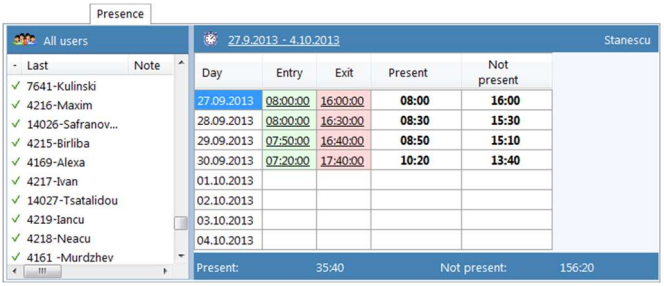
For the errors correction we recommend stopping the communication by pressing the *Disconnect* button and try to find and solve the problem in the configuration tool *APS Reader*.

techfass®

12 Presence overview

12.1 Displaying presence overview

To display a *presence overview* in selected areas, select the *Presence* tab in the main program window (*pic. 41*). Setting of areas for presence overview is described in chapter *Area properties*.

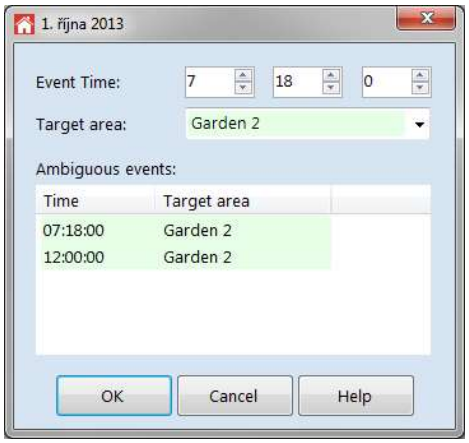


Pic. 41: Presence overview

A list of all users is displayed in the left part of the window. The list can be sorted by a column selected in the context menu, from which you can also hide or display other available columns. After a user is selected, an overview of his entries to and exits from the selected area for the selected time period is displayed. The time period is indicated by two dates displayed in the upper part of the window. In the overview there is a date is displayed in the first column followed by all entries to and exits from the area for current day, last two columns display total time spent inside and outside the area for the day. In the lower part there is a total sum of time spent inside and outside the area for the entire time period.

The program supports the search function in the users' list. To run the function, use the shortcut *CTRL + F*. After entering the text and pressing ENTER, the rows containing at least one field with the text or its part are highlighted. The buttons *Find next* or *Find previous* can be used to move among the records. The function is closed by pressing the *Close panel* button or by pressing the *ESC* key.

The *time period* can be set by the link indicating the time period borders in the upper part of the window. If an entry or exit event occurs twice in a row without any supplementary event interruption, a *choice of valid event* is enabled after clicking at the link (*pic. 42*).



Pic. 42: Ambiguous event

Events in the overview can be also changed, deleted or inserted. A change is performed in a dialog, which is available after clicking at the event. You can change the time of the event in the dialog. Inserting a new event is available by selecting appropriate command from the context menu of selected field. An option to delete an event is also available in the context menu.

12.2 Overview printing

The presence overview can be saved in a printable *html* format. Saving options are available in the context menu of selected users in the *Reports* option. A report can content either selected or all users and their entries or exits for selected area, or total sums of presence and absence of all users.

13 Supplements

13.1 Automatic IP address setting for TCP/IP – RS 485 converters

The function is available since the program version *4.0.3793.20575*. It is usable for devices: *APSLAN*, *MDEM 31.IP* and *MWGD 46.IP*. For using the function, it is necessary to know the *MAC address* of the device (printed at a label of each device) and connect the computer with the device by TCP/IP without using any active routing device.

Select the *Device* tab and open the *TCP/IP tools* menu in the *Communication* area. Select the *Set IP address* option in the menu.

The first step is filling in the *MAC address* of the device. Continue by pressing the Next button.

In the next step it is necessary to select an *IP address* you wish to set. The IP address must be located in the same subnet as the IP address of the used network interface of your computer. After pressing the *Find* button the network is set for the first unoccupied IP address in the relevant subnet. Continue by pressing the *Next* button.

In the last step verify all parameters. The *Configuration password* option enables setting of the password used for accessing the converter setting, the default value is *1234*. After pressing the *Assign* button, the program tries to assign selected IP address to the device with selected MAC address.

Note: In the Windows Vista and newer operating systems, you will be several times asked for UAC elevation. Without allowing this the setting IP address process will fail.

13.2 Manual TCP/IP – RS 485 converters setting

For setting the *TCP/IP – RS 485* converters it is necessary to know the actual *IP address* of the converter. If the address is not known, it can be *temporarily* set by following procedure. Do not forget to *set the IP address again* in the converter's setting itself!

Note: You can reset the *APSLAN* converter, the embedded converter of the *MWGD 46.IP* or *MDEM 31.IP* terminal to its factory defaults (IP address *192.168.1.253*, IP port *10001*, password *1234*) by pressing the reset button for more than 5 seconds.

Temporary IP address setting in Windows NT, 2000 and XP

- Connect the device to the computer network.
- Open a *command line* by executing the *cmd* command.
- Delete the *ARP Table* with the command *arp –d*.
- Insert a record into the *ARP Table* with the command *arp –s IP_address MAC_address*. The device *IP address* must be in the same subnet as the computer used for configuration. The device *MAC address* is printed at the device's factory label.
- Run the command *telnet IP_Address 1* to insert the desired IP address into the ARP table of the converter (Telnet shows an error after a while).

Temporary IP address setting in Windows Vista and higher

- Connect the device to the computer network.
- Run the command line terminal as the Administrator.
- Run the command *netsh interface ipv4 show addresses*, the available network interfaces will be displayed. Choose the network interface to connect the device (IP address must be in the same subnet) and copy its name to the clipboard (or remember it).
- Run the command *netsh interface ipv4 delete neighbors* to delete the ARP table content.
  Run the command *netsh interface ipv4 add neighbors "interface_name" "required_IP_address" "device_MAC_address"* to add static entry to the ARP table.
- Run the command *telnet IP_Address 1* to insert the desired IP address into the ARP table of the converter (Telnet shows an error after a while).

Note: The procedure described above requires the telnet client program, which is an optional Windows feature. It can be enabled in the section Enable or disable Windows features of the Windows configuration.

Device configuration

After executing the commands above, the device is *temporarily* available at the IP address set and it is necessary to proceed the standard configuration:

- In the *APS Reader* program choose the *Device* tab and fill in the *IP address* of the converter.
- Press the *Configure* button.
- Press the *Enter* key to advance to the converter setting itself

Following procedures differ for individual converter types:

13.2.1 APSLAN, the embedded converter of the MWGD 46.IP controller or MDEM31.IP terminal

- Enter the password – its default value is *1234*.
- Enter required IP address after selecting *1 Set IP*.
- Enter required IP port after selecting *2 Set port* (we recommend to preserve the default value *10001*).
- Check the function mode of the converter after selecting 4 Set function mode – it must be set to *0 – RS485/Ethernet* (APSLAN converter only).
- Save the settings by selecting 9 Save & Exit.

The converter is ready to operate at the address *IP_address:IP_port* now.

13.2.2 GNOME 485

- Choose the option *0 Server* and fill in the required *IP address*. You can leave the other parameters intact.
- Choose the option *1 Channel 1* and set the parameter *BaudRate* to the value *19200* and the parameter *I/F Mode* to the value *7F*. We recommend leaving other parameters intact.
- Save the settings by choosing *9 Save and exit*.

The converter is now ready to communicate at *IP_Address:10001*.

13.3 APS mini Plus module upgrade

For upgrading the module, connect to the module first. Then choose *Upgrade device (MPL)* or *Upgrade device (TFFW)* from a context menu displayed after right-clicking in the *Device information* area (at bottom right). Select the upgrade file for a module with corresponding serial number; the program uploads the new configuration in the module's memory.

Note 1: The procedure of device upgrade (MPL) is available since FW version 4.9. This type of upgrade does not allow upgrading the firmware. Note 2: The procedure of device upgrade (TFFW) is available since FW version 4.14. This type of upgrade does allow upgrading the firmware. Note 3: If a device occupies multiple addresses at the communication line, it is necessary to upgrade the firmware at the lowest assigned HW address. Note 4: If a device occupies multiple addresses at the communication line, it is necessary to upgrade the licenses and configuration at each of the assigned address.

13.4 Database restore and backup operation notes

The database backup and restore functions are available since the program version *1.0.3861.19359*.

The database backup and restore operations can be performed only at a local SQL server (the backup itself is performed by the SQL server, not by the APS Home program). For both operations the Administration privilege is required (run the program as Administrator). Furthermore, when restoring the database, no users can be connected to the given database (meaning the system communication in the APS Home program must be stopped as well).

Both operations can take a long time, therefore the maximal timeout of the maintenance operations is configurable in the APS Home program.

13.4.1 Database backup operation process

The backup operation is run at the SQL server; the backup file contains a single (actual) backup of the database (INIT flag). The backup file is saved to the default folder for backup files, the backup file name is random. After the backup operations is finished, the file is copied to the user-defined location named according to the user selections. The temporary file is deleted afterwards.

13.4.2 Database restore operation

The file with the database backup is copied to the standard folder with database backups (with a random filename) and acquires corresponding permissions (SQL server usually runs under NETWORK SERVICE account, not under the logged user account). After performing the database restore the temporary file is deleted.

Note: The restore operation is run with the REPLACE and even MOVE (when necessary) flags. Therefore, it is possible to overwrite any database with any database backup.

After the database restore is completed, the restored database is opened in the APS Home program.