APS Reader

Configuration program for APS mini Plus system

User's guide

(release date: 2024/01/18; valid for build 4.0.8696.14566)

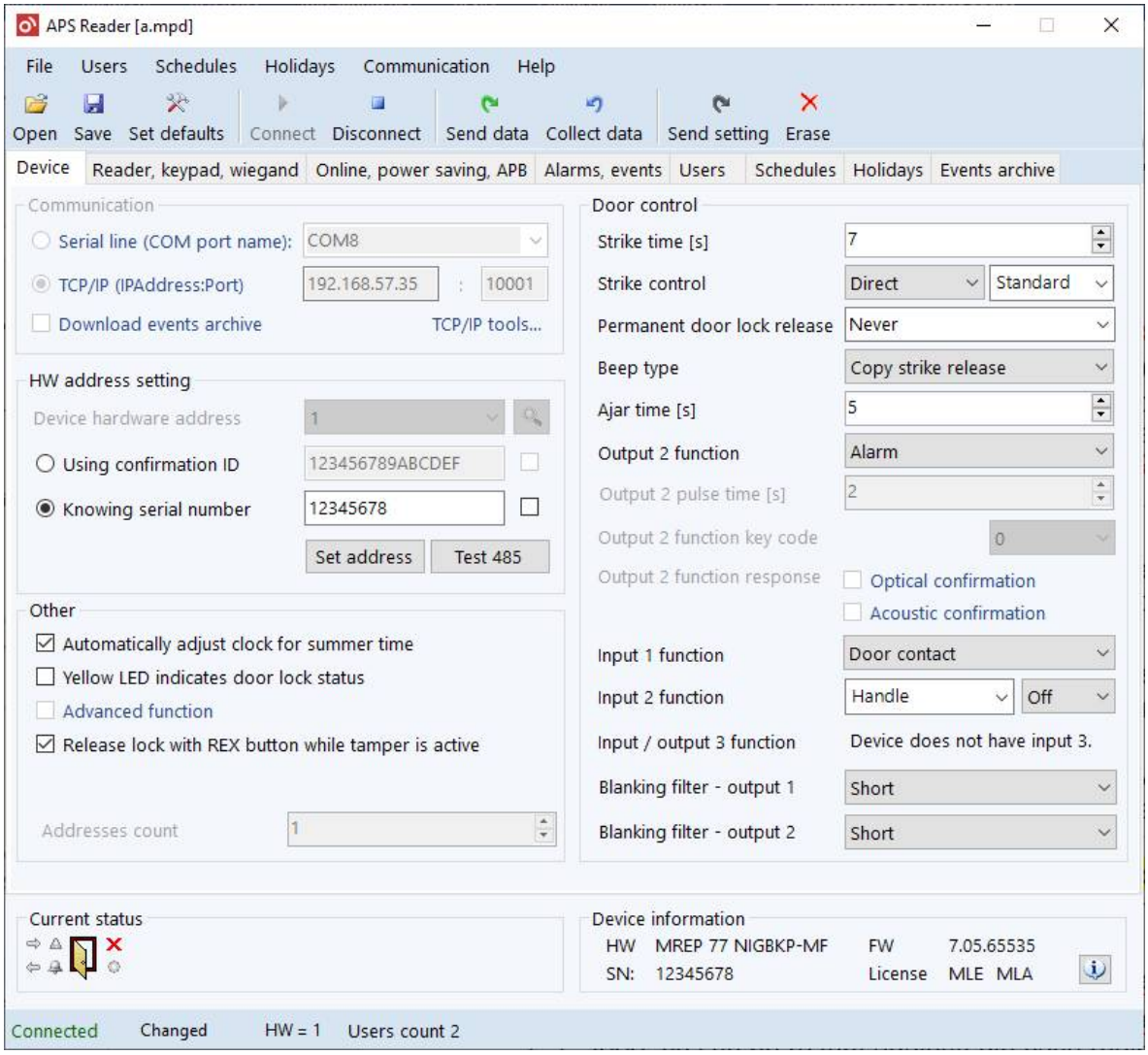
1 Content

2 Product description

The software product *APS Reader* (*pic. 1*) is a basic configuration tool for setting up the parameters of APS mini Plus system modules. In the simplest application with single or few autonomous modules it can be also used for administration of users and their access rights.

Note: It is recommended to use *APS HiT* software for offline administration. For large and / or online systems *APS Administrator* (with a large amount of extending program modules) is recommended. Since 2020, the *cloud solution* for APS mini Plus systems administration can be used. For more information see techfass.com.

The communication with modules connected to an RS 485 communication line is provided via COM, USB or TCP/IP interfaces (with proper communication converters).



Picture 1: APS Reader program

techfass®

3 Installation and program maintenance

3.1 System requirements

The program requires a PC with OS *Windows 10* and *MS .NET Framework 4.6.1* installed to run.

3.2 Installation

The program installation is performed by its installer, which is available for download at the web pages techfass.com. The program is installed in *Program Files\TechFass\APS mini Plus.Reader* folder and there are shortcuts for its executable file and documentation (PDF format) created in the *Start* menu.

3.3 Program update

The *APS Reader* program searches for an automatic update on its start in a regular period, which can be set in a dialog available after opening the menu *File* > *Options* at the *Update* tab. For an instant update press the *Search now* button or select *Help* > *Check for updates* in the main menu.

3.4 Program and module versions compatibility

Once a successful communication between the program and an APS mini Plus module is established, information about the 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 1*.

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[1)].
	since 4.10	User configuration of EM Marin IDs reading[2)], 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.
	Since 7.04	Configuration of entry reader keypad function and power saving options.
	Since 7.05	Configuration of the 2nd output function, support for door with holding magnet, configurable logic of 2nd input, new function of the I/O port 3 – REX button.
	Since 7.06	Improved RTC operation.

Table 1: Available configuration of the APS mini Plus module function

[1)] This setting is only available for modules with Wiegand input.
[2)] This setting is only available for modules with 125 kHz RFID readers.
[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.

techfass®

4 Setting parameters of the APS mini Plus module

4.1 Communication settings

Communication between the *APS Reader* program and the APS mini Plus modules is realized via an RS 485 communication line. The PC can be connected to this line with one of the ways further described. Since the program version *4.0.4086.17084* it is possible to adjust the maximal device response timeout. The setting is available in the context menu of the Communication area. The minimal value is 250 ms, the maximal value is 2500 ms with a step of 50 ms.

Tip: See typical APS mini Plus lines wiring diagrams at techfass.com in the "*Wiring diagrams*" section. Recommended communication converters can be found in the "*Product catalogue*" section.

4.1.1 Communication via a serial port

To connect a PC via serial port you will need an *RS 232 / RS 485* converter with an automatic direction switching (e.g. 232TO485DA).

In the *APS Reader* program select the *Device* tab, choose *Serial line (COM port name)* and insert *COM#*, where # is the number of the COM port. When configuring the converter (usually carried out by the jumpers' configuration) do not forget to set the communication rate to 19200 bd.

4.1.2 Communication via USB

To connect a PC via USB you will need a *USB / RS 485 converter* (e.g. APSUSB).

After connecting the converter to a PC and installing converter drivers, the system creates a virtual serial port – its name can be found in *Computer Management* > *Device Manager* > *Ports (COM & LPT)*. In *APS Reader* program select the *Device* tab, choose *Serial line (COM port name)* and insert *COM#*, where # is the number of the virtual COM port.

4.1.3 Communication via TCP/IP

To connect a PC via TCP/IP (recommended) you will need a *TCP/IP / RS 485* converter (e.g. *APSLAN*, *GNOME 485*, or embedded converter of the door controller *MWGD 46.IP*). Instructions for recommended converter parameters setting can be found in *supplements 1 and 2*, which can be found at the end of this guide.

4.2 Searching the line, HW address settings

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. 2*).

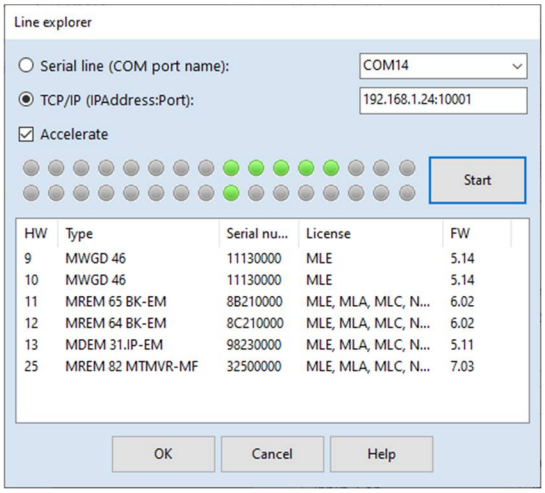
HW address setting	Product line	Type
	xRIF 32, xREx 53, xREM 55, xREM 57, xREM 57U, xREM 58, xREM 59, xREM 63, xREM 64, xREM 65, xREx 73, xREM 77, xREP 78, xREM 79, xREM 81, xREM 82[7)]	SW
	xREM 54, xREM 56, xREM 76, xWGD 46[6)], xABA 46[6)], xRRF 12, xRIF 232	HW
	xDEM 31	SW or via the terminal screen configuration

Table 2: Type of HW address setting procedure

[6)] These modules occupy two addresses; the first one is set by the HW jumpers configuration, the second one is greater by one. In the LIFT and XT versions the modules occupy 4 successive addresses.
[7)] 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 the button with a *magnifying glass* picture next to the Device HW address setting field.

Select a type of communication line and its parameters in the opened dialog (*pic.2*). To speed up the search, select the *Accelerate* option. Press the *Start* button to begin the search. The line is searched for all connected modules. When the search is completed, following information is shown for each module found:



Pic. 2: Searching the communication line

- *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.

techfass®

4.3 RS 485 line testing

The correct connection of the modules at the RS 485 BUS can be tested with a broadcast sent by pressing the *Test 485* button (*pic. 3*). After sending the broadcast all modules should signal acquiring "test 485" command and start blinking with red and green diode. By this function you can test both modules, where the HW address is set by SW and modules, where the HW address is set by configuration jumpers.

Picture 3: HW address setting

The *test 485* function is supported only by modules with FW version 5.1 or newer!

4.4 HW address setting with APS Reader

4.4.1 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. 3*). 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.

Tip: If you know current module HW address (and the address is not in a conflict with another module), the serial number can be read and inserted in the input field by checking the box next to the input field.

4.4.2 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. Select the *Device* tab and fill in a known ID of an identification medium in the field adjacent to the *Using confirmation ID* option; the medium will be used for setting the module's HW address (*pic. 3*). Choose required HW address then and press the *Connect* button. You will see a red label "*Timed out*" in the status bar (if you see a green label "*Connected*", the HW address is already occupied and you need to use another one). Press the *Set address* button now, 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. There will be a green label "*Connected*" shown in the status bar.

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

Tip: 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), checking the box placed next to the text box for Confirmation ID entering and reading the card at the reader.

4.4.3 Setting count of HW addresses

On special modules for controlling a large number of outputs with one reader (for example, MREM 82 MTMBOX-MF modules) it is also possible to set the number of addresses that the module occupies on the communication line and controls corresponding number of outputs (*pic. 1*). If the first address is set to 1, the maximum number of addresses is 32, if it is set to 2, the maximum number of addresses is 31, and so on.

5 Module functional parameters setting

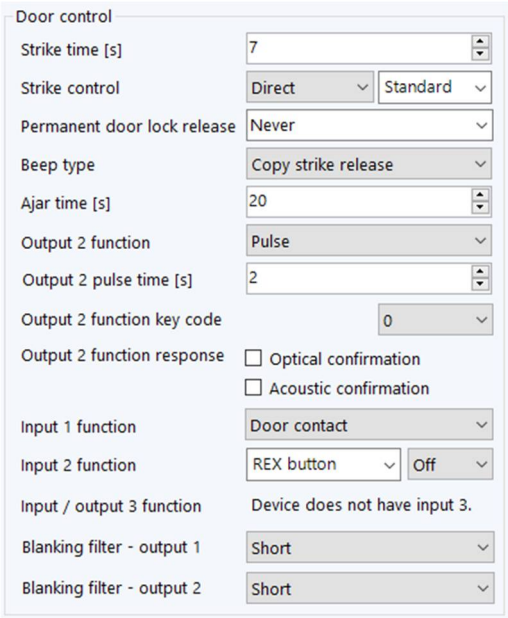
After connecting the program to an APS mini Plus module (*Connect* button), all information about the HW type, serial number, licenses and functional parameters of the module is read. You can adjust the values of all required functional parameters at the *Device* and *Reader, keypad, …* tabs.

5.1 Device

At the *Device tab* you can configure all operational parameters of a module. The program allows configuring parameters which are meaningful for the module HW type and FW version.

5.1.1 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. 4*). All parameters detailed description can be found in *table 3*.



Picture 4: Door control

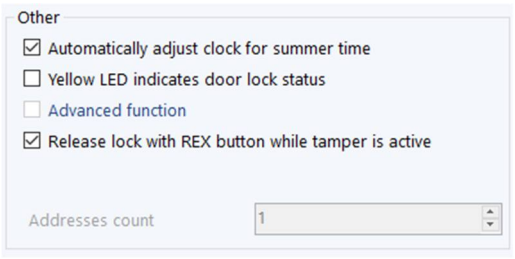
Door control	Parameter	Default value	Value range
	Strike time [seconds]	7 s	0 ÷ 255
	Ajar time [seconds]	20 s	0 ÷ 255
	Strike control	Direct	Direct / Reverse
	Door lock relay function	Standard	Standard / Toggle / Pulse / Holding magnet
	Permanent door lock release	Never	Never / Time schedule
	Beep type (copy strike release)	Yes	Yes / No
	Output 2 function	Alarm	Alarm / Pulse / Toggle
	Output 2 pulse time	2 s	0 ÷ 255
	Output 2 function key code	0	0 ÷ 255
	Output 2 function optic response	Yes	Yes / No
	Output 2 function acoustic response	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	Request to exit button / Tamper / Disabling / Signal for external buzzer / IDS status monitoring / Reading synchronization
	Blanking filter – output 1	Extra-long	Off / Short / Medium / Long / Extra-long
	Blanking filter – output 2	Extra-long	Off / Short / Medium / Long / Extra-long

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) and finally, in the *holding magnet* mode, the locking output is set to on after the door is closed.
- *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*).
- Parameter *Output 2 function* defines the behavior of the second output: *Alarm*, *Pulse*, or *Toggle*. The *output 2 pulse time* can be s set in [s].
- *Output 2 function key code* … defines which key is to be used to activate the output 2 function.
- The method of signaling the activation of the output 2 function can be set by the checkboxes *Optical* and *Acoustic confirmation of the output 2 function*.
- *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. Since the FW version 7.05 also the *REX button*.
- 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* – *Extra-long* (the setting corresponds approximately to the values 0 µs – 60 µs - 80 µs – 100 µs – 800 µs). To protect the el. circuits of the module, it is recommended to choose the shortest possible value of disabling the current protection.

5.1.2 Other options

These settings affect general behavior of a module (*pic. 5*)



Picture 5: 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.

For denying the automatic summer/winter time adjustment, uncheck the checkbox *Automatically adjust clock for summer time*. The option is enabled by default.

The *xABA 46* and *xWGD 46* 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. 2*) the setting is automatically applied to both addresses of a module.

The last element in this part is setting of the count of addresses on special modules with an adjustable number of addresses. This setting has already been described in chapter 4. 4. 3: Setting count of HW addresses.

5.1.3 Default values

To set the default functional parameters of the module press the *Set defaults* button at the top toolbar of the program.

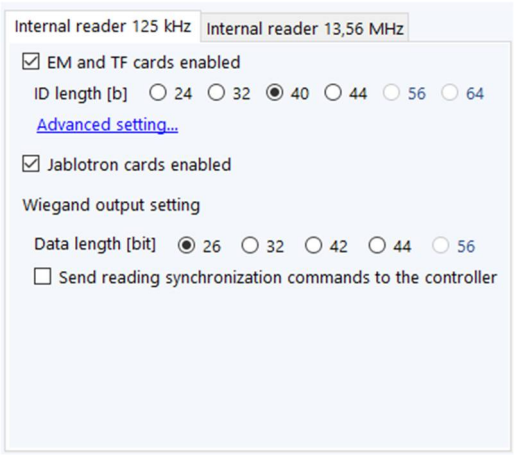
techfass®

5.2 Reader, keypad, …

On this tab it is possible to configure the *operating mode* of the module, the *formatting of the IDs* of the read ID media, the *wiegand input and output formats*, the *function of the internal keypad*, resp. the keybpad of the connected external reader and *function of the keypad of the entry wiegand reade*r. The program allows you to set only those parameters that are supported by the connected module.

5.2.1 Internal reader 125 kHz

A *standard reader module with an integrated 125 kHz reader* can read *EM Marin and Jablotron* technology media. When reading an ID the code is formatted first (*pic. 6*) and the module hereafter works with the code in the new format.

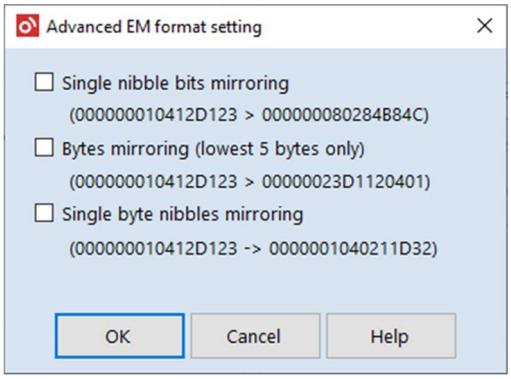


Picture 6: Internal reader 125 kHz

Since FW version 7.0 reading of individual types of ID media can be enabled / disabled.

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 there is further need to change the interpretation of the EM Marin media code, press the *Advanced settings* link. In the displayed dialog (*pic. 7*) you can change any combination of changes in the code interpretation.



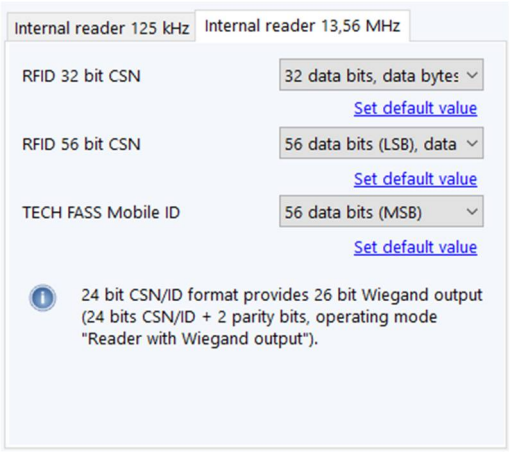
Picture 7: Advanced settings

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.

5.2.2 Internal reader 13,56 MHz

When configurating modules that operate on frequency 13,56 MHz you can set the length of ID media with *32 bit CSN* and *56 bit CSN* and also mobile application *TECH FASS® Mobile ID* (*pic. 8*).

Since FW version 7.0 reading of individual types of ID media can be enabled / disabled.



Picture 8: Internal reader 13,56 MHz

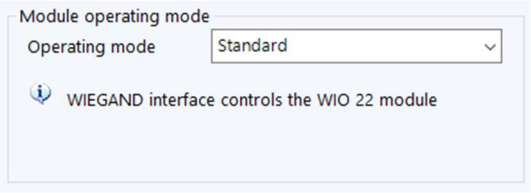
ID format setting	ID technology	Available formats
	RFID 32 bit CSN	Disabled 32 data bits (MSB) 32 data bits, data bytes reserved (LSB) 24 data bits (MSB) Facility code 0x01 + 16 data bits (MSB)
	RFID 56 bit CSN	Disabled 32 data bits (MSB) 32 data bits, data bytes reserved (LSB) 24 data bits (MSB) Facility code 0x01 + 16 data bits (MSB) 56 data bits (MSB) 56 data bits, data bytes reserved (LSB)
	TECH FASS® Mobile ID	Disabled 32 data bits (MSB) 32 data bits, data bytes reserved (LSB) 24 data bits (MSB) 56 data bits (MSB) 56 data bits, data bytes reserved (LSB)

Table 4: ID length and orientation setting

techfass®

5.2.3 Module operating mode

The operating mode of the modules providing own IDs reading determines the overall function of a module (*pic. 9*).



Picture 9: Module operating mode

If a module is intended to work as a *standard APS mini Plus module*, it is necessary to use the *Standard* operating mode. 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).

Modules providing own IDs reading can also be configured in the *WIEGAND reader* mode, in which the code of read ID is sent in one of selected formats. Since the *FW* version *5.09* it is furthermore possible to turn on the *Send reading synchronization commands to the controller* option. This function can be used to cancel mutual disturbance of a pair of TECHFASS readers – module can operate in the *Wiegand reading synchronization – MASTER mode*. The function can be applied after connecting the module to properly configured reader module supporting the *Wiegand reading synchronization - SLAVE mode*.

WIEGAND	ID technology	IDs sending
	EM Marin	Formatted with internal reader format configuration first, then sent with standard WIEGAND output – 26, 32, 42, or 44 bit format
	Other media	Standard WIEGAND output – 26, 32, 42 or 44 bits

Table 5: IDs format in WIEGAND operation mode

If the module features a keypad, the key code is sent immediately after a key press as a 4-bit burst; the highest bit comes first, the values are binary encoded. The key codes sent differ in accordance to the keypad function setting (*tab. 6*).

Wiegand output keys encoding	Reason keypad				PIN or ID keypad			
	Title	Code	Title	Code	Title	Code	Title	Code
	1	1	9	9	1	1	8	8
	2	2	10	10	2	2	9	9
	3	3	ESC	0	3	3	0	0
	4	4	ENTER	11	4	4	ESC	10
	5	5	F1	12	5	5	↵	11
	6	6	F2	13	6	6	F ↑	14
	7	7	F3	14	7	7	A ↓	15
	8	8	F4	15				

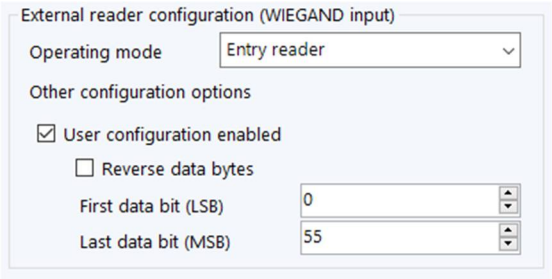
Table 6: Key code encoded in WIEGAND output configuration

The *WIEGAND interface* of the module can be always configured only into modes, which are meaningful for given module.

The *xREP 78* modules (FW version 4.13 – 5.10) 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.

5.2.4 WIEGAND input (external reader)

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. 10*).



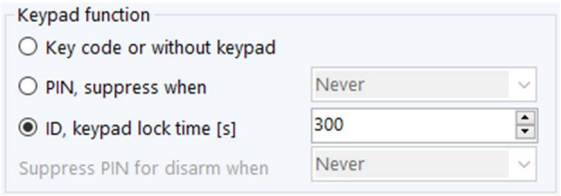
Pic. 10: WIEGAND input configuration

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.

5.2.5 Keypad function

Setting up the keypad function is only enabled where it is meaningful (*pic. 11*). The keypad function setting can be set to one of the following options:



Picture 11: Keypad function

- *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.

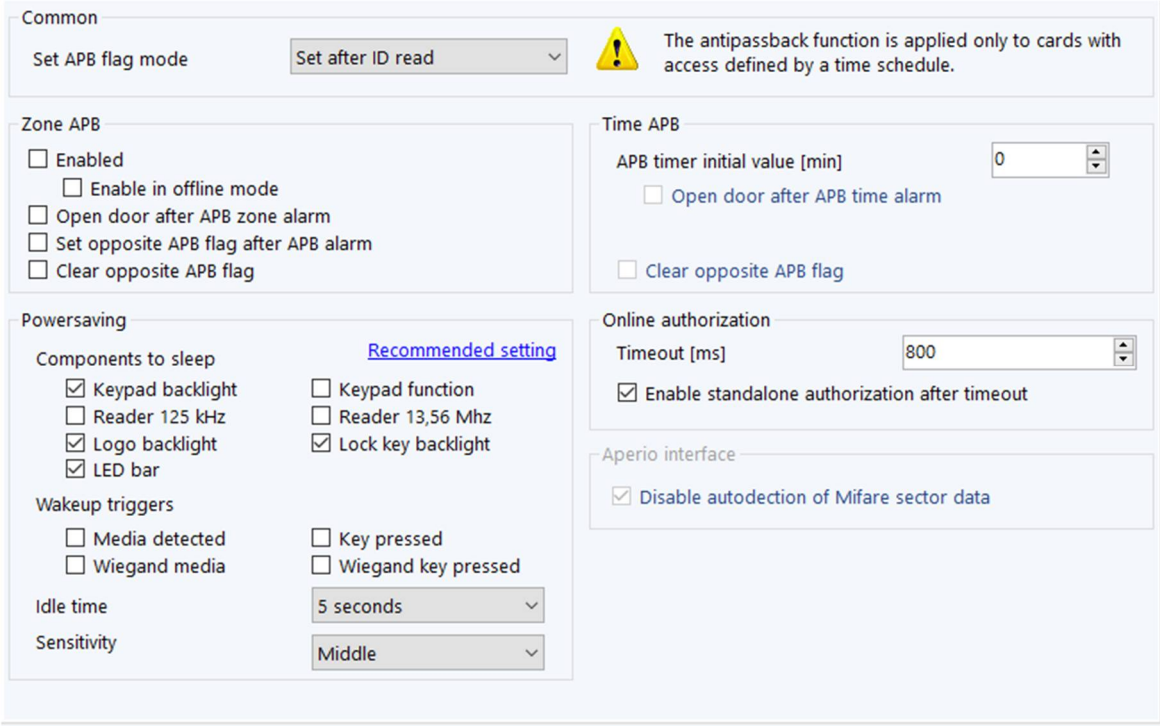
Since the *FW version 5.4* the *Suppress PIN for disarm function* is supported. In case the Wiegand interface is configured to IDS control function, it is possible to select a time schedule, which suppresses the PIN demand for IDS disarm function, when valid. Moreover it, can be set to suppress: always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

techfass®

5.3 Online, power saving, APB, …

Parameters of the following functions can be configured on this tab (*pic. 12*):

- Antipassback
- Power saving
- Online authorization
- Aperio



Pic. 12: Page Online, power saving, APB, …

5.3.1 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 by setting the flag *Disable auto detection of Mifare sector data*.

5.3.2 Online authorization

The Online authorization function has been implemented in APS mini Plus modules since *firmware version 5.11*. In this mode, the authorization of the read ID is evaluated by the master system (eg. APS Server). This feature requires an MLO license for each address where it is to be used. The *APS Reader* program is used for setting following parameters:

- *Timeout [ms]* … defines maximal time for the module to wait for authorization response from the master system after an ID is read.
- *Enable standalone authorization after timeout* … defines the module behavior after authorization timeout – if set, the standard standalone authorization of ID will be performed after timeout; otherwise the module saves the "Authorization timeout" event and the ID will not be authorized to pass.

5.3.3 Antipassback

The Antipassback function is defined in two ways:

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

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. 14*). 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).

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.

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.

techfass®

5.3.4 Power saving

Configurable parameters

- *Components to sleep* … contains check boxes for selecting components which will be turned off after the device goes to the sleep mode:
  - Keypad backlight.
  - Keypad function.
  - Reader 125 kHz.
  - Reader 13,56 MHz.
  - Logo backlight.
  - Lock key backlight.
  - LED bar.
- *Wakeup triggers* … contains check boxes for selecting resources that the device wakes from sleep mode:
  - Media detected … reading ID.
  - Key pressed … key pressed on the internal keypad.
  - Wiegand media …reading ID by the reader connected via Wiegand interface.
  - Wiegand key pressed …key pressed on the reader connected vie Wiegand interface.
- *Power save idle time*.
- *Ambient light sensor sensitivity*.

Power saving effect

Access system components generally have relatively low energy consumption (negligible compared to heating or air conditioning). Nevertheless, it is appropriate to reduce their energy consumption where possible. The following table shows the approximate reduction of the energy consumption of the single components of the dual frequency TECH FASS reader with integrated keypad.

Power saving	Component	Savings (full backlight) [%]	Savings (default backlight) [%]
	Keypad backlight*	22	12
	Keypad function	0	0
	Reader 125 kHz	3	6
	Reader 13,56 MHz	7	12
	Logo backlight*	9	6
	Lock key backlight*	8	4
	LED bar*	28	14
	Total (* with recommended setting)	77 (*67)	54 (*36)

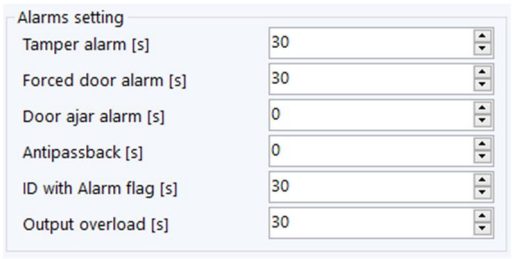
Table 7: Approximate energy savings of single reader components

Only the components with * are turned off when recommended setting is applied.
The energy saving data is based on measurements performed on the MREP 82 MTM product, at 12 V power supply and full and default (approx. ½ full) backlight intensity of the keypad, LED bar, etc. Full backlight intensity is only available when the "Ambient light sensitivity" function is enabled.

5.4 Alarms, events

5.4.1 Alarms

Module recognizes 6 types of alarm states (*pic. 13*): *Forced door*, *door ajar* and *tamper*, *antipassback*, *ID with alarm flag* and *Output overload* alarms. 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/or announces the alarm status for the time period set by the value. The alarm parameters overview is described in *table 8*.



Picture 13: Alarms setting

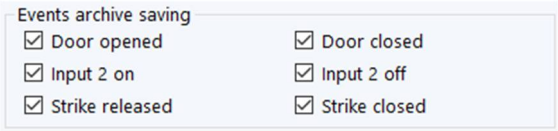
Alarms setting	Parameter	Default value	Value range	Beep on alarm	Set alarm output
	Tamper	30 s	0 ÷ 255	Yes	Yes
	Forced door	30 s	0 ÷ 255	Yes	Yes
	Door ajar	0 s	0 ÷ 255	Yes	Yes
	Antipassback	0 s	0 ÷ 255	Yes	No
	ID with Alarm flag	30 s	0 ÷ 255	No	Yes
	Output overload	30 s	0 ÷ 255	Yes	Yes

Table 8: 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

5.4.2 Events saving

The firmware enables to deny saving of some events in the events archive in order to save the memory of the module. To deny saving of a specific event, check the according box (*pic. 14*).



Picture 14: Events archive saving

techfass®

6 Program operation

6.1 Environment

Language settings is available in the menu *File* > *Options*. In the following dialog choose the desired language and click *OK*.

6.2 Access password

A password required for program operation can be set in the *Program options* dialog (*File* > *Options*). Once the password is set, it is required for all users on each program start.

6.3 File management

The connection parameters and permissions setting (cards, schedules, holidays) can be saved in an *APS mini Plus data file* (*.mpd*) by clicking the button *Save* in the upper part of the program; the command is also available in the menu *File* > *Save* and *File* > *Save as*. The default location for the files is set to "*…\User's Profile\Documents\APS mini Plus.Reader*". If the data is edited after loading them from a file or reading them from a module, a black sign *Changed* is displayed in the lower part of the program.

To create a new file, select *File* > *New* in the menu. If you want to open an existing file, use the button *Open* or select *File* > *Open* in the menu. For closing the program select *File* > *Exit*.

If you intend the program to open the last opened file at startup, check the option at the *General* tab at the dialog available by choosing *File* > *Options*.

6.4 Communication

For connecting to the APS mini Plus module, press the *Connect* button in the upper part of the program; the command Is also available in the menu *Communication* > *Connect*. For stopping the communication, press the *Disconnect* button or choose *Communication* > *Disconnect* in the menu.

The communication state is indicated in the lower left part of the program:

- *Disconnected* (black) … module is disconnected.
- *Connected* (green) … communication with the module is running.
- *Error* (red) … communication cannot be established.
- *Timed out* (red) … communication failed.

Note: The program is not designed for online system management. Therefore, if there is no event read from the module in 10 minutes, the communication is automatically terminated.

To display the basic information of the modules at the communication line, follow the steps in *chapter 4.2: Searching the line, HW address setting*.

6.5 Data transfer

6.5.1 Programming the module's memory

This action is done by pressing the *Send data* button in the upper part of the program. The command is also available by selecting *Communication* > *Upload* in the menu. By executing this command all configured parameters, users and their access rights, time schedules and holidays are transferred in the module's memory.

6.5.2 Reading data from the module's memory

This action is done by pressing the *Collect data* button in the upper part of the program. The command is also available by selecting *Communication* > *Download*. By executing this command all configured parameters, users and their access rights, time schedules and holidays are read from the module's memory. The names assigned to the read data are restored if they were previously set, new data are named as a generic string with an ordinal number.

6.5.3 Programming the module configuration

For a fast programming of the functional parameters from the tabs Device and Reader, keypad, …, press the Send setting button. With this action only the functional parameters of the module are transferred, user data are not transferred at all.

6.5.4 Deleting the module's memory

This action is done by pressing the *Erase* button. The command is also available by selecting *Communication* > *Erase* in the menu.

Note: Data transfer between the module and the PC is displayed in the in the program status bar. The data transfer can be interrupted by disconnecting.

techfass®

6.6 Module status indication

Pic. 15: Module status

The current status of inputs, outputs, alarm states and a buzzer can be found in *Current status area* on the *Device* tab (pic. 15). If a card is read at a module, information about the card's ID validity and assigned user (if any) are displayed. Remote door opening is enabled by clicking the door icon with left mouse button (the same action as if a valid ID were read or an exit button pressed). The meaning of the icons indicating the status of the module is described in *tab. 9*.

After right-clicking the door icon a context menu is raised, where remote ID code and reason key code can be sent to the module, thus simulate reading an ID at the module.

The PIN code cannot be remotely sent to the module, the function is meaningless when the module keypad is configured as PIN keypad.

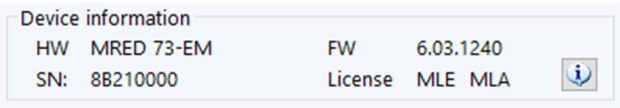
Reader module current status indication	Part	Icon	Meaning
	Door		Module not connected, door status unknown
			Door closed
			Door opened
			Door ajar time exceeded (Door ajar alarm status)
			Forced door (Forced Door alarm status)
	Strike		Module not connected, strike status unknown
			Strike closed
			Strike released
	2nd input		Second input Off
			Second input On
	3rd input / output		Third input Off / Third output Off
			Third input On / Third output On
	Tamper		Tamper OK
			Tamper alarm (Tamper alarm status)
	Buzzer		Buzzer inactive
			Buzzer active
	Alarm output		Alarm output not active
			Alarm output active

Table 9: Module status indication

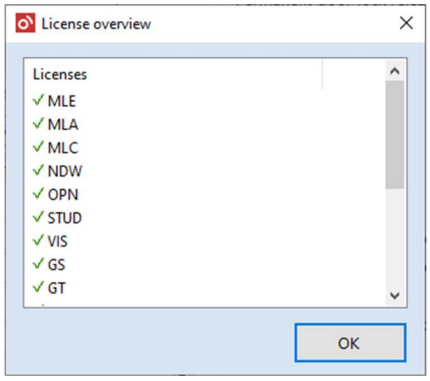
6.7 Module information and license overview

On the right next to the status visualization you can find information about connected module's *HW type*, *FW version* and *serial number* (*pic. 16*).

A list of present licenses can be displayed by selecting Full license list from the context menu (pic. 17). The meaning of the licenses is described in *table 10*. If a license is present in the module, it is marked with a *green check mark*; if it is not present, it is marked with a *red cross*.



Picture 16: Connected module information



Picture 17: License overview

Licenses	License	Meaning
	MLE	Enables reading the events archive.
	MLA	Enables usage of the module in the APS T&A SW extension.
	MLC	Internal reader can read both factory (TF) and other (EM) EM Marin technology IDs.
	NDW	Enables usage of APS T&A.WEB SW extension in the system (single license is required for system/server, not required by current versions of SW).
	OPN	Enables usage of APS Administrator.OPN SW extension in the system (single license is required for system/server).
	STUD	Enables usage of APS Administrator.ST SW extension in the system (single license is required for system/server).
	VIS	Enables usage of APS Administrator.VIS SW extension in the system (single license is required for system/server).
	GS	Module can be visualized in APS Administrator.GS visualization.
	GT	Module can be used for guard duty monitoring in APS Administrator.GT sw extension.
	MLO	Module can be used in the online authorization mode.
	HIT	Licenses uses by modules from the GO product line (canceled).
	HTP	
	HEA	
	DV	Module can be used for system management division in APS Administrator (not required by current versions of SW).
	PM	Enables usage of the module in the APS Administrator.PM SW extension.
	CR	Enables usage of the module in the APS Administrator.CR SW extension.
	EHS	Enables usage of the module in the APS Administrator.EHS SW extension.

Table 10: Module licenses

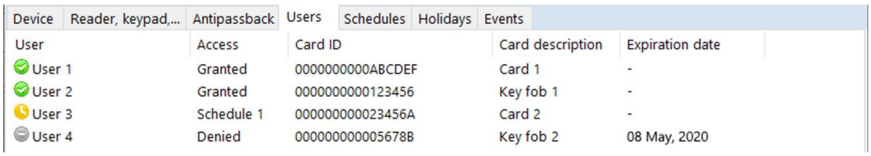
techfass®

7 Access rights administration

The *access permission* of a user to the APS mini Plus module is defined by the setting of *access rights* for each HW address and user's card or other ID medium. The access can be *always granted*, *always denied* or it can be driven by a *time schedule*.

7.1 User administration

In the APS Reader program, the users and their access rights can be managed at the *Users* tab (*pic.18*).



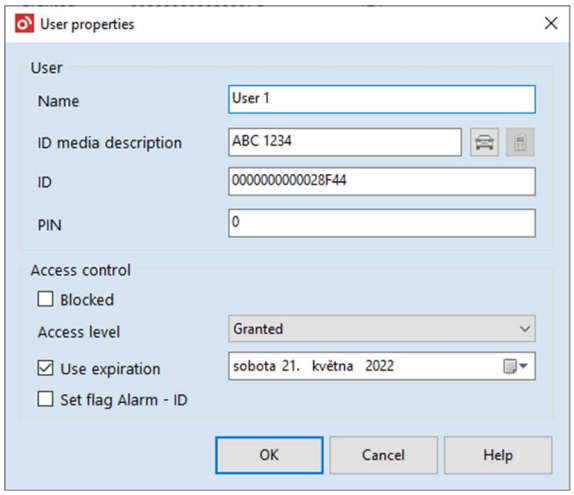
Picture 18: Users tab

Symbols displayed next to the users are indicating their access rights levels. The meaning of the symbols is described in *tab.10.*

	Symbol meaning at the Users tab
Icon	Meaning
	No ID assigned to the user
	No ID assigned to the user, ID alarm flag set
	User is blocked
	User is blocked, ID alarm flag set
	User with access always denied
	User with access always denied, ID alarm flag set
	User with access always denied, expired
	User with access always denied, ID alarm flag set, expired
	User with access driven by a time schedule
	User with access driven by a time schedule, ID alarm flag set
	User with access driven by a time schedule, expired
	User with access driven by a time schedule, ID alarm flag set, expired
	User with access always granted
	User with access always granted, ID alarm flag set
	User with access always granted, expired
	User with access always granted, ID alarm flag set, expired

Table 11: Symbol meaning at the Users tab

You can add a new or edit an existing user by right-clicking in the users list at the *Users* tab. *Picture 19* shows the *User properties* dialog. Meaning of the *User parameters* is following:



Picture 19: User properties

- *Name* – a name of the user; it is recommended to enter the name in the format *<<surname> <first name>>* for sorting reasons.
- *ID* – the code of the ID media, or an ID code for modules with ID keypad.
- *ID media description* – any possible description of the ID media.
- *PIN* – PIN code of the user, set to zero by default; required for valid identification on modules with a PIN keypad. The PIN code must not be a zero value; otherwise the identification on PIN modules will be automatically invalid.
- When clicking the button *with the car symbol*, value of the *ID media description* box will be calculated to the 24bit ID using the ANPR algorithm and set to the *ID* box.
- When clicking the button *with the mobile phone symbol,* value of the *ID media description* box (where the phone number with the international area code is expected) will be calculated to the 32bit ID and set to the *ID* box.

Access control settings:

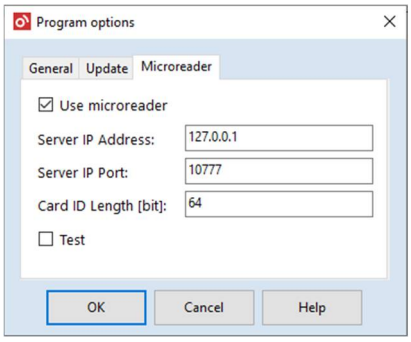
- *Blocked* – if this box is checked, the user's data are not uploaded to the module and the user cannot access the module.
- *Access level* – the access level can be always *Granted*, always *Denied* or it can be driven by a *Time schedule*; individual *time schedule* selection is available after the defining at the *Schedules* tab (*chapter 7.4*).
- *Use expiration* – option to select a date, when the user's access rights expire
- *Set flag – Alarm ID* – Sets the Alarm flag to the user's ID – when such ID is read at the reader, the ID with Alarm flag alarm is raised.

The access level and the user blocking can be set en masse in the context menu after selecting a group of users on the *Users* tab.

7.2 Microreader and it's using

7.2.1 Microreader parameters setting

The microreader parameters setting is available in the *Program options* dialog, which is available after selecting *File* > *Options*. At the *Microreader* tab (*pic. 20*) 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 techfass.com website.



Pic. 20: Microreader settings

For testing the functionality of the microreader select the *Test* option and read a card at the microreader. If the configuration is set correctly, the card ID is shortly shown in the area next to the *Test* option.

7.2.2 Using microreader

The microreader can be used for inserting new users or for a search for existing users. In the main program window select the *Users* tab and read the card at a microreader. If a user with relevant card ID exists, it is selected. Otherwise a dialog for inserting a new user is shown, where the card ID code is already inserted from the information acquired from the microreader. After editing all desired parameters press the *OK* button to save the user.

7.3 User list import and export

A list of users can be imported from and exported to *.csv* files. Necessary commands are available in the main menu after choosing *File* > *Import* / *export*. When exporting, only user's name, ID and card description parameters are saved. When importing, an incomplete file can be used as well, missing parameters are replaced by default values then.

7.4 Schedules

At the *Schedules* tab you can create up to 64 time schedules, which can determine the user's access rights to a module. *Picture 21* shows an example of a time schedule. You can create a new or edit an existing time schedule by right-clicking at the *Schedules* tab. The command is also available in the menu *Schedules* > *New* / *Edit*.

Description
Schedule 1
Schedule 2
Schedule 3
Schedule 4
Schedule 5
Schedule 6

Day	From	To	From	To
Monday	08:00	18:00	00:00	00:00
Tuesday	08:00	18:00	00:00	00:00
Wednesday	09:00	15:00	20:00	22:00
Thursday	07:30	19:00	00:00	00:00
Friday	06:15	15:00	00:00	00:00
Saturday	07:00	12:00	13:00	22:00
Sunday	00:00	00:00	00:00	00:00
Holiday	10:00	18:00	00:00	00:00

Picture 21: Time schedules

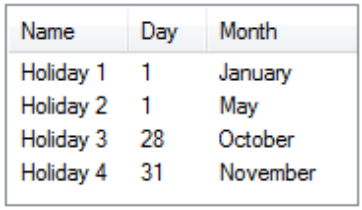
Every time schedule allows setting up two time intervals defining a time period, in which the user has access granted. These intervals are set separately for every day of a week and for holidays. After creating a time schedule you will be able to assign it to a user by setting the *Access level* parameter at the *Users* tab. Days considered as holiday are defined at the *Holidays* tab (*chapter 7.5*).

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).

7.5 Holidays

The days considered as holidays are defined at the *Holidays* tab (*pic. 22*). You can create a new or edit an existing holiday by right-clicking at the *Holidays* tab. The command is also available in the menu *Holidays* > *New* / *Edit*.

The program also offers an option of inserting the *Easter* holiday. The command is available both in the context menu and in the main menu in *Holiday* > *Easter*.



Name	Day	Month
Holiday 1	1	January
Holiday 2	1	May
Holiday 3	28	October
Holiday 4	31	November

Picture 22: Holidays

techfass®

8 Events archive

The online read events archive is placed at the *Events* tab. Events archive is downloaded only if the option *Download events archive* at the *Device* tab is selected. Events are read online and sorted by time (the newest on top). Every event carries information about *Date & Time*, *Event Type*, *ID* of a card, which caused the event (if meaningful), *Key Code* pressed on the reader's keypad and *User Name*, if it is assigned to the related ID (*pic. 23*).

Date & Time	Event Type	ID	Key Code	User Name
21.2.2008 14:09:38	Valid ID	0000000F0DFFA6B7	0	Smith John
21.2.2008 14:09:32	Forced Door		0	-
21.2.2008 14:09:32	Door Opened		0	-
21.2.2008 14:09:31	Door Closed		0	-
21.2.2008 14:09:26	Strike Closed		0	-
21.2.2008 14:09:19	Strike Released		0	-
21.2.2008 14:09:19	Remote Open Door Request		0	-
21.2.2008 14:09:12	Strike Closed		0	-
21.2.2008 14:09:11	Invalid ID	0000000F0DFFA721	0	Green Richard
21.2.2008 14:09:09	Unknown ID	0000000F00970A97	0	not found
21.2.2008 14:09:05	Strike Released		0	-
21.2.2008 14:09:05	Valid ID	0000000F0DFFA6B7	0	Smith John
21.2.2008 14:08:57	Connected		0	-
21.2.2008 14:08:49	Disconnected		0	-

Picture 23: Events overview

Note: Only modules with the *MLE* license contain the events archive! This license is

8.1 Obtaining user data

New users can be easily created in the user's list by following procedure:

- Read new cards at a reader (will be displayed as unknown cards in the archive).
- Select related events at the *Events* tab.
- Select *Create new user* in the context menu

Tip: If only the ID of a card is requested for some reason, select the event in the archive and choose *Copy ID to clipboard* in the context menu.

8.2 Event types

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
66	Output 2 on	Output 2 on
67	Output 2 off	Output 2 off
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)	
92	RTC failed	RTC failed
93	RTC restored	RTC restored
202	Execute output 2 function requested	Execute output 2 function requested (by the selected key)
203	Execute output 2 function denied	Execute output 2 function denied
204	Remote execute output 2 function requested	Remote execute output 2 function requested (by the communication line)
205	Remote execute output 2 function denied	Remote execute output 2 function denied
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 12: Event type meanings

techfass®

8.3 Events archive and log saving

After disconnecting the communication program, or after reading 5.000 events from the archive, the program automatically saves a document in .xml format in the location "*…\User's Profile\Documents\APS mini Plus.Reader\Events*". The name of a file consists of ordinal number, serial number of the reader module and the date and time at which the file was saved. The file contains all events read in the same format as they are displayed in the events archive of the program; additionally, the file contains information about the module – serial number, HW type, licenses present, time of connecting to and disconnecting from the module and the name of a profile used when downloading the events archive (windows login name).

A quick link to the folder containing events archive files is available in the menu *File* > *Open Folder With Archives*.

Events archive browser can be opened by the command *File* > *Open events archive browser*.

9 Supplements

9.1 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.

techfass®

9.2 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:

9.2.1 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.

9.2.2 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*.

techfass®

9.3 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.