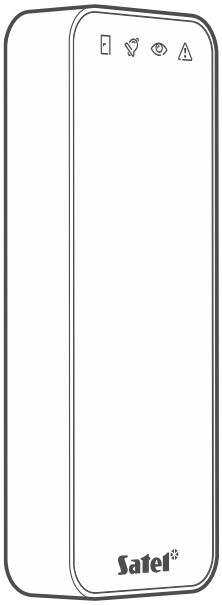
MIFARE proximity card reader

SO-MF3

Firmware version 1.00

EN



CE

so-mf3_en 08/24

SATEL sp. z o.o. • ul. Budowlanych 66 • 80-298 Gdańsk • POLAND
tel. +48 58 320 94 00
www.satel.pl

IMPORTANT

The device should be installed by qualified personnel.

Prior to installation, please read carefully this manual.

Changes, modifications or repairs not authorized by the manufacturer shall void your rights under the warranty.

SATEL aims to continually improve the quality of its products, which may result in changes in their technical specifications and software. Current information about the changes being introduced is available on our website.
Please visit us at:
https://support.satel.pl

Hereby, SATEL sp. z o.o. declares that the radio equipment type SO-MF3 is in compliance with Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: www.satel.pl/ce

The following symbols may be used in this manual:

 - note,

 - caution.

CONTENTS

The SO-MF3 reader can operate as:

- proximity card reader in the INTEGRA alarm system,
- proximity card reader in the ACCO access control system,
- proximity card reader in systems of other manufacturers,
- standalone door control module.

Before you install the reader, program the settings required for the selected operating mode in the CR SOFT program. The exception is a reader that is to operate in the ACCO NET system and is to be connected to the ACCO-KP2 controller using the RS-485 bus (OSDP protocol). The OSDP protocol is supported by the ACCO-KP2 controllers with firmware version 1.01 (or newer). In that case, you can program the required settings in the ACCO Soft program (version 1.9 or newer).

1. Features

- User identification by MIFARE® proximity card.
- Support for 13.56 MHz MIFARE proximity cards:
  - Ultralight,
  - Classic,
  - DESFire (EV1 / EV2 / EV3).
- Supported OSDP protocol (RS-485 bus).
- Additional communication interface:
  - EM-Marine (in the INTEGRA or ACCO system),
  - Wiegand.
- Programming in the CR SOFT program.
- LED indicators.
- Relay output for controlling an electric strike, electromagnetic lock or other door actuator (in the standalone door control module mode).
- Door status input (in the standalone door control module mode).
- Request-to-exit input (in the standalone door control module mode).
- Built-in sounder.
- Tamper protection against enclosure opening and removal from the wall.

The reader supports version 2.2 of the OSDP protocol.

To program MIFARE® cards, the SO-PRG programmer is required.

2. Description

2.1 LED indicators

LED	Color
	blue
	red
	green
	yellow

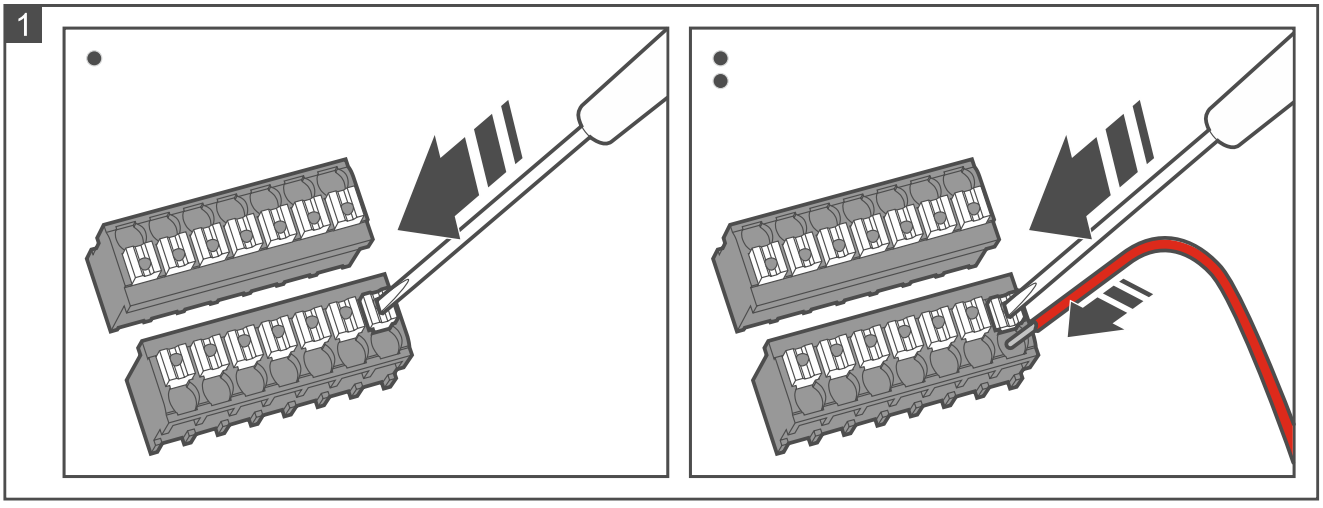
Flashing of the LEDs successively from left to right indicates no connection with the control panel / controller (e.g. connection made incorrectly).

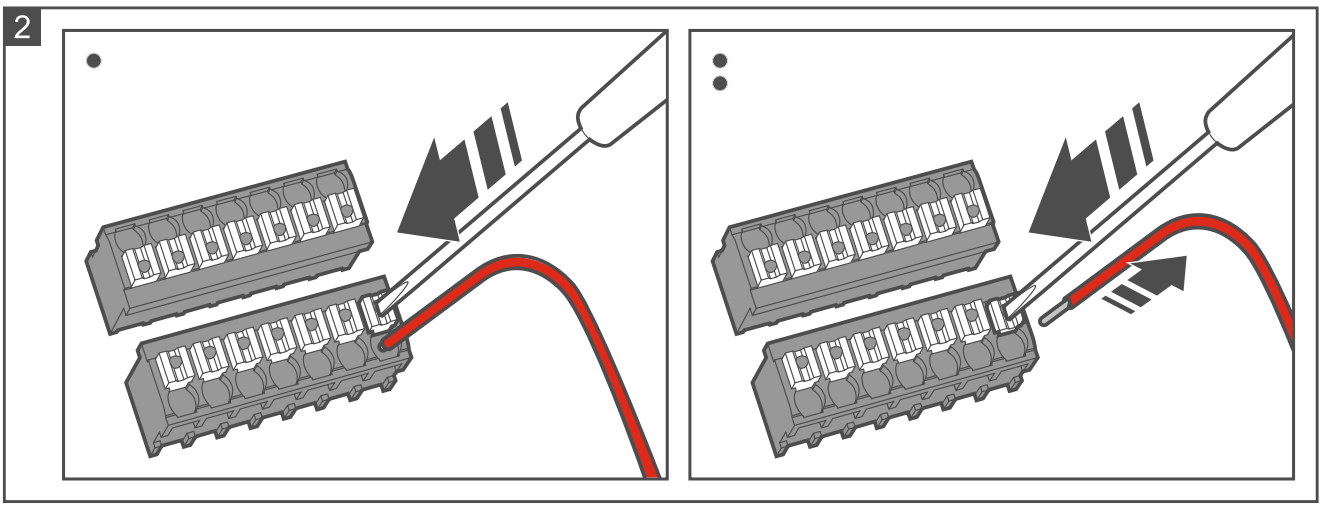
Flashing of the LEDs successively from right to left indicates no communication with the control panel / controller (connection made correctly but the device has not been identified).

2.2 PUSH IN terminals

The terminals used in the reader are PUSH IN type. Figure 1 shows how to connect a wire to the terminal. Figure 2 shows how to disconnect the wire. You can use a wire with a cross-section up to 1.5 mm^2.

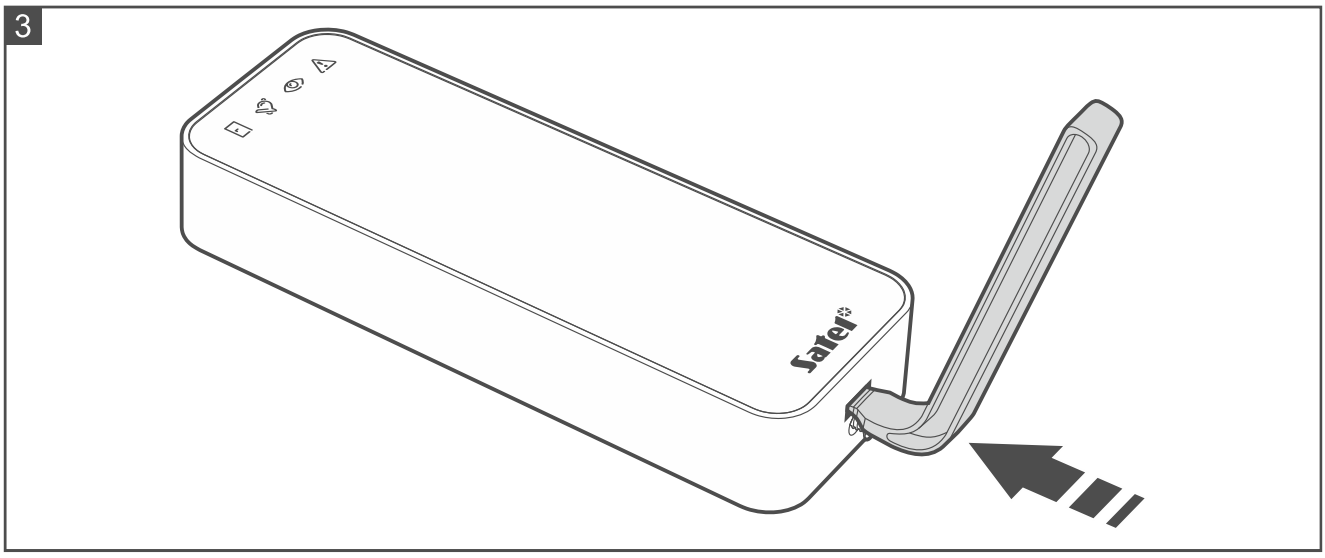
1





2.3 Enclosure opening tool

A tool for opening the enclosure is delivered with the keypad. Figure 3 shows how to open the enclosure using the tool. The screw must be loose.



3. Connecting the reader to the computer

If you are planning to install the reader in the ACCO NET system and use the OSDP protocol, you can skip this section. The ACCO Soft program in version 1.9 (or newer) enables programming of all the required settings.

Before you mount the reader, program its settings. Connecting the reader to the computer is required. To connect the reader to the computer, use the USB / RS-485 converter (e.g. ACCO-USB by SATEL). Follow the instructions in the converter manual.

Do not connect more than 24 access control devices provided with the MIFARE card reader (SO-MF5, SO-MF3, CR-MF5 and CR-MF3) to the converter. The CR SOFT program may not be able to support more devices correctly.

4. CR SOFT program

If you are planning to install the reader in the ACCO NET system and use the OSDP protocol, you can skip this section. The ACCO Soft program in version 1.9 (or newer) enables programming of all the required settings.

The program is used to program the settings of access control devices provided with the MIFARE card reader (SO-MF5, SO-MF3, CR-MF5 and CR-MF3) and to program MIFARE cards (the SO-PRG programmer is required). You can download it from www.satel.pl. Required program version: 1.1 (or newer).

The program requires Windows 10 operating system (or newer).

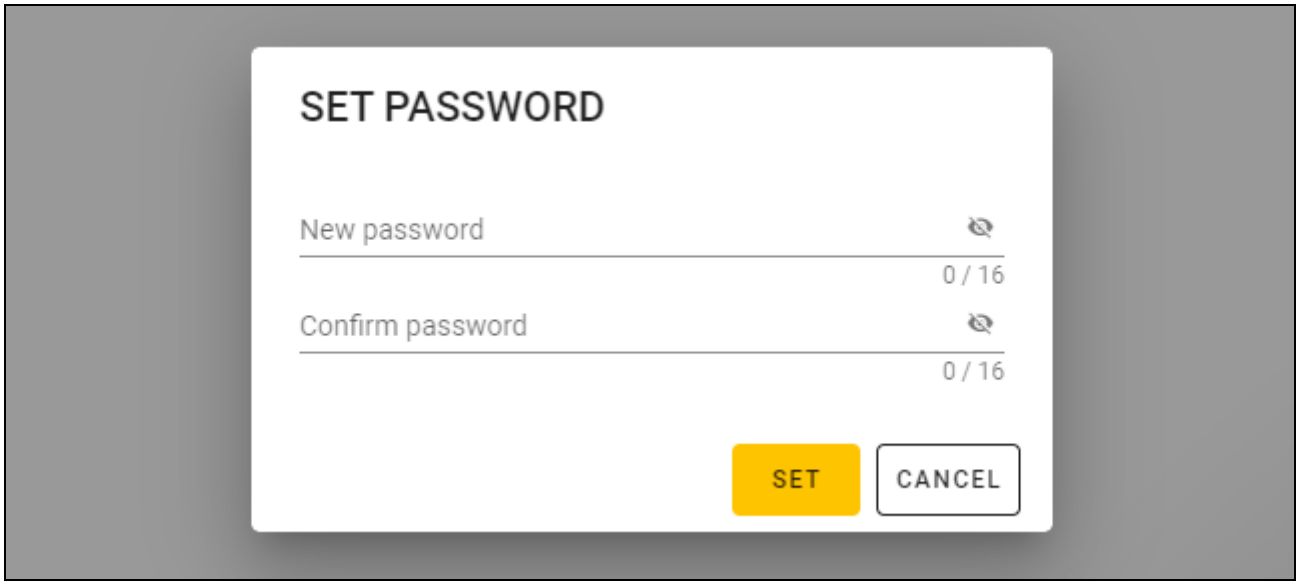
The screenshots in this manual show sample settings.

4.1 Starting out

4.1.1 Setting the administrator password

When the program is started for the first time, the “SET PASSWORD” window will be displayed. Set the administrator password there. The administrator has access to all projects created in the program.

If you do not set the password, the “SET PASSWORD” window will be displayed each time the program is started. No administrator password means no protection against unauthorized access to projects and their data.

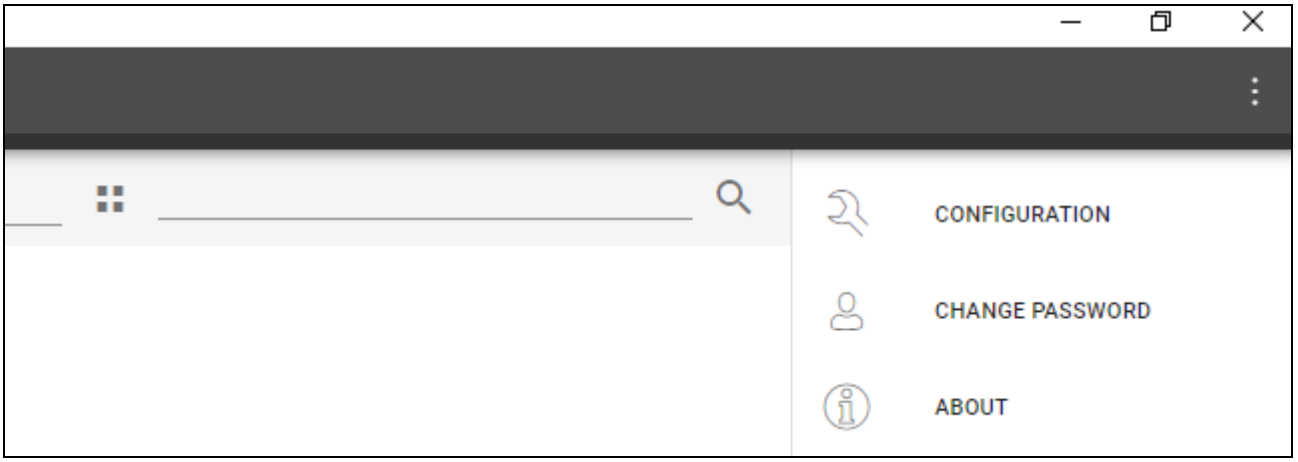


1. In the “New password” field, enter a password (1-16 digits, letters or special characters).
2. In the “Confirm password” field, enter the same password.
3. Click “Set”. The “SET PASSWORD” window will be closed. A message will confirm that the password has been set. You will access the program window (see: “Program window with the list of projects” p. 8).

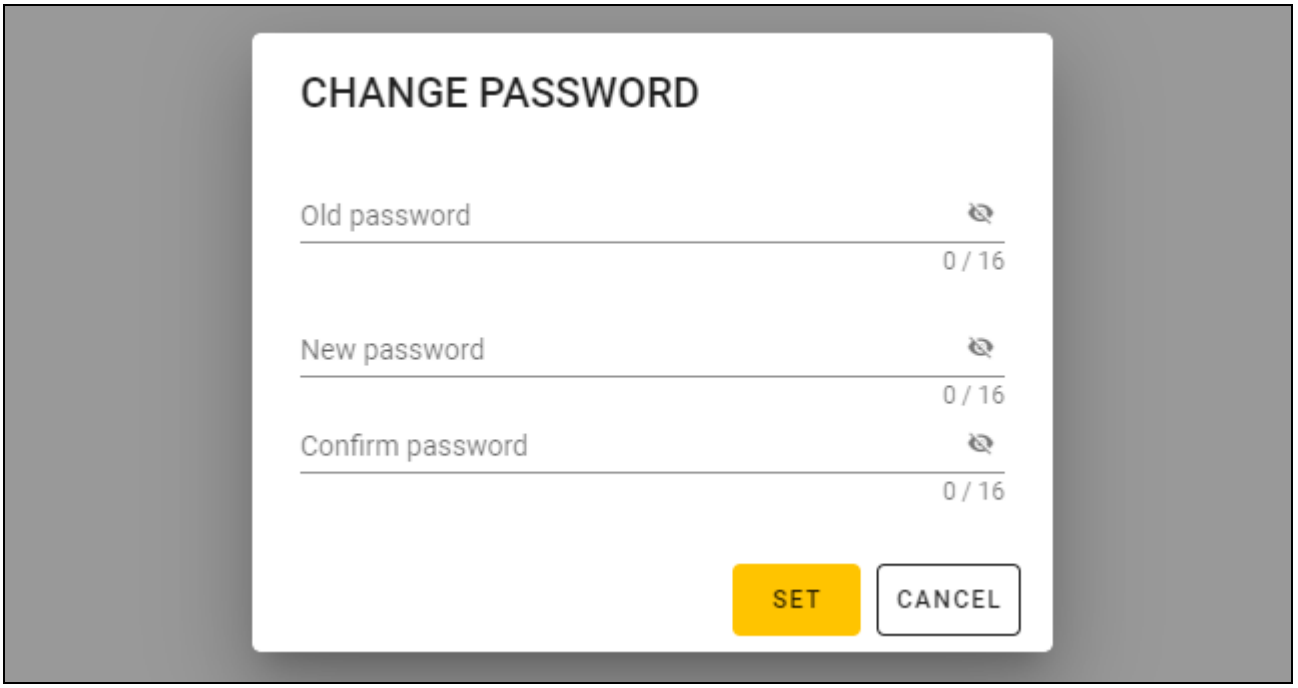
Next time you start the program, you will have to log in to access the program window.

4.1.2 Code changing

1. Click  on the menu bar. The menu will be displayed.



2. Click “CHANGE PASSWORD”. The “CHANGE PASSWORD” window will be displayed.

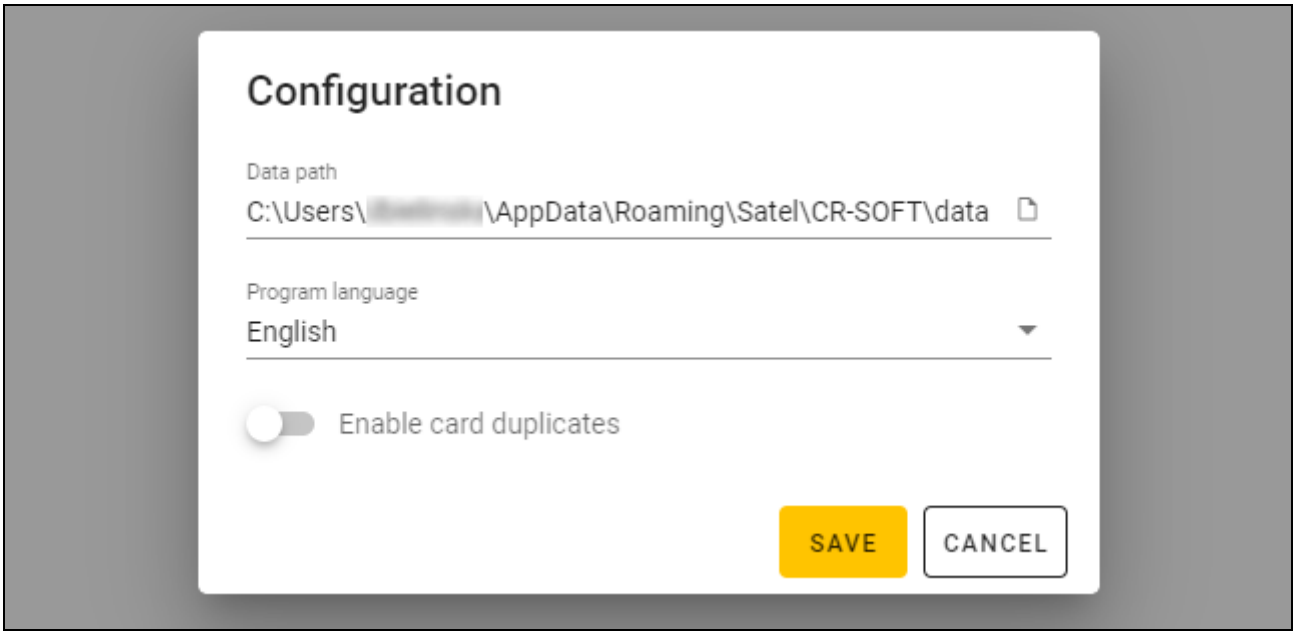


3. In the “Old password” field, enter the current password.
4. In the “New password” field, enter the new password (1-16 digits, letters or special characters).
5. In the “Confirm password” field, re-enter the new password.
6. Click “Set”. The “CHANGE PASSWORD” window will be closed. A message will confirm that the password has been changed.

4.1.3 Changing the program language

1. Click  on the menu bar. The menu will be displayed.

2. Click “CONFIGURATION”. The “Configuration” window will be displayed.

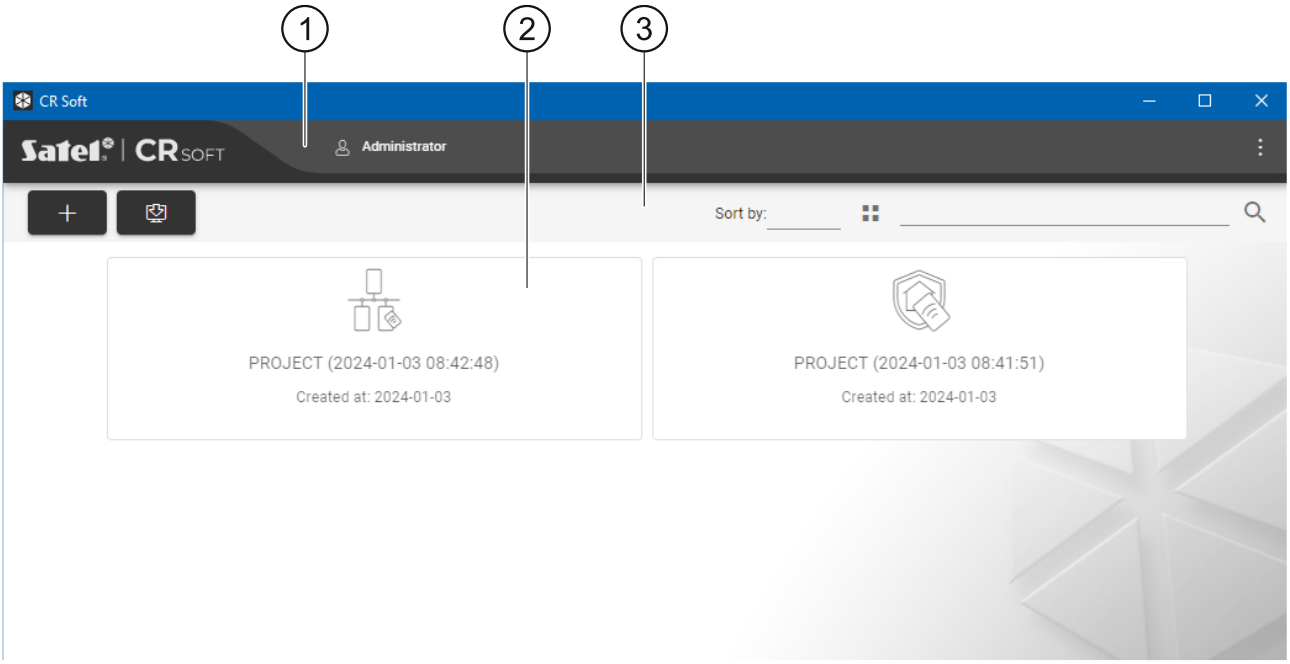


3. Click the “Program language” field. The list of languages will be displayed.
4. Click the language to be used.
5. Click “SAVE”. The “CONFIGURATION” window will be closed.

4.2 Program window

4.2.1 Program window with the list of projects

After logging in, the list of projects will be displayed in the program window.



(1) menu bar (see: “Menu bar” p. 10).

(2) list of projects.

(3) tool bar for the list of projects.

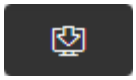
List of projects

All projects to which you have access are displayed on the list. Click a project to open it.

Tool bar for the list of projects

Project-related buttons and functions are displayed on the tool bar.

 - click to create a new project (see: “Creating a project” p. 12).

 - click to import a project (see: “Importing a project” p. 13).

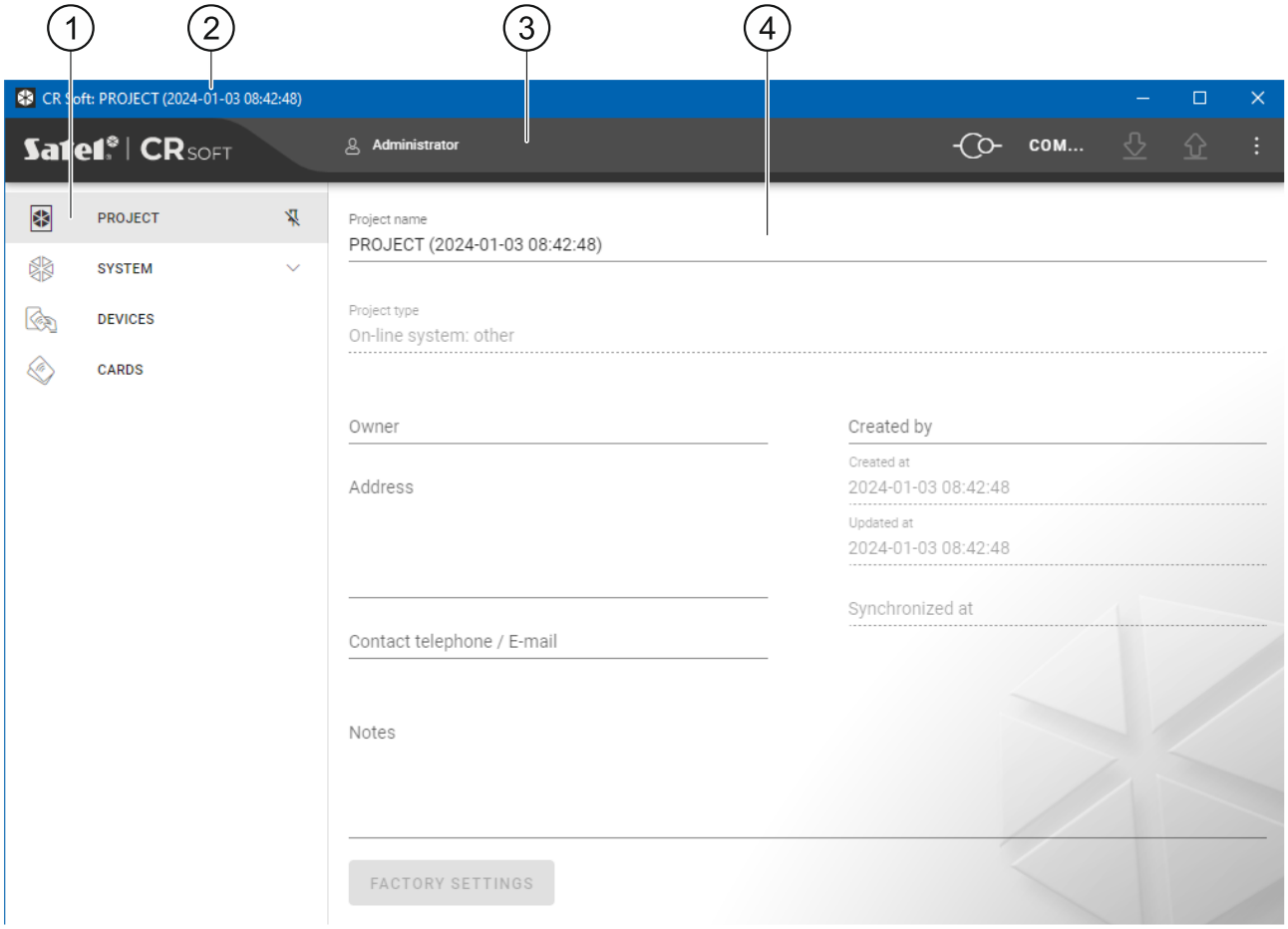
Sort by – you can select how the projects are sorted on the list (by name or creation date).

 - click to change the view mode of the project list to a table.

 - click to change the view mode of the project list to tiles.

Filter – enter a string of characters and click  to display the projects whose name or settings in the “PROJECT” tab contain this string of characters.

4.2.2 Program window after opening a project



(1) tabs.

(2) title bar.

(3) menu bar (see: “Menu bar” p. 10).

(4) settings available in the tab.

Tabs

Click a tab to display the settings available in the tab.

PROJECT – project details.

SYSTEM – system settings:

INTERFACES – communication interfaces settings.

TOKEN SETTINGS – MIFARE cards settings.

DEVICES – list of access control devices in the project and their settings.

CARDS – list of MIFARE cards in the project.

USERS – list of users in the project and their settings. This tab is only available in a *Standalone system* type project.

After connection is established with the SO-PRG programmer, only these tabs are available: "PROJECT", "TOKEN SETTINGS", "CARDS" and "USERS" .

- click to enable the auto-hide of tab labels.

- click to disable the auto-hide of tab labels.

Title bar

The name of the open project is displayed on the title bar.

4.2.3 Menu bar

Buttons and information are displayed on the menu bar. The appearance of the menu bar depends on the program window size, content displayed in the program window, etc.

 - click to display the tabs. This button is displayed when the tabs are not displayed due to the window size.

 - click to log out. The name of the logged in user is displayed next to the button.

 - click to establish connection with the access control devices / programmer. This button is displayed when a project is open and the program is not connected with the access control devices / programmer.

If no COM port for communication has been selected, when you click the button, the "Connection" window will be displayed.

 - click to disconnect from the access control devices / programmer. This button is displayed when a project is open and the program is connected with the access control devices / programmer. Information on whether the program is connected with the access control devices or the programmer is displayed on the left of the button.

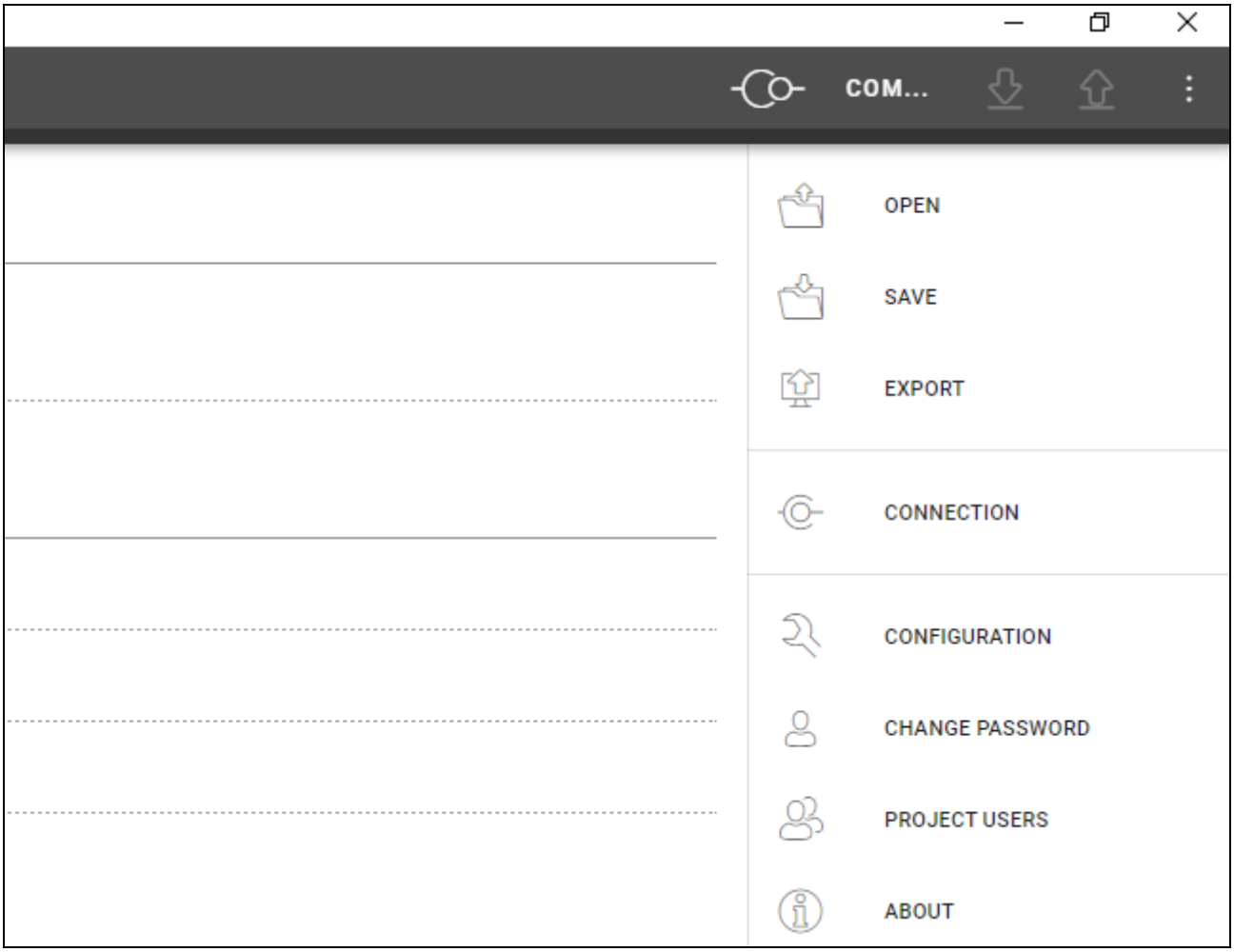
- click to select the COM port for communication with the access control devices / programmer. When the COM port is selected, the port number will be displayed instead of the three dots. You can also select the COM port in the "Connection" window. This button is displayed when a project is open.

 - click to read data from the access control devices. This button is displayed when a project is open and the program is connected with the access control devices.

- click to write data to the access control devices or the programmer. This button is displayed when a project is open and the program is connected with the access control devices / programmer.

- click to display the menu.

4.2.4 Menu



The following commands are available in the menu:

OPEN – click to close the project and return to the list of projects.

SAVE – click to save changes in the project (see: “Saving changes in the project” p. 26).

EXPORT – click to export the project (see: “Exporting a project” p. 26).

CONNECTION – click to open the “Connection” window.

CONFIGURATION – click to open the “Configuration” window.

CHANGE PASSWORD – click to change the password (see: “Code changing” p. 7).

PROJECT USERS – click to open the “PROJECT USERS” window.

ABOUT – click to display information about the program.

When the list of projects is displayed, only the following commands are available in the menu: ”CONFIGURATION”, “CHANGE PASSWORD” and “ABOUT”.

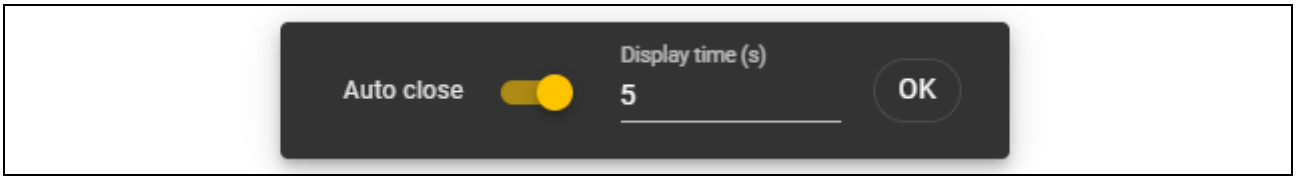
4.2.5 Message window

The message window is displayed on the bottom of the program window. It notifies the user about the actions performed by the program.

 - click to go to the message window settings.

 - click to close the message window.

Message window settings



Auto close – if this option is enabled, the message window will close automatically.

Display time (s) – time after which the message window will close when the *Auto close* option is enabled.

OK – click to close the message window settings.

4.3 Using the program

4.3.1 Creating a project

This function is available when the list of projects is displayed.

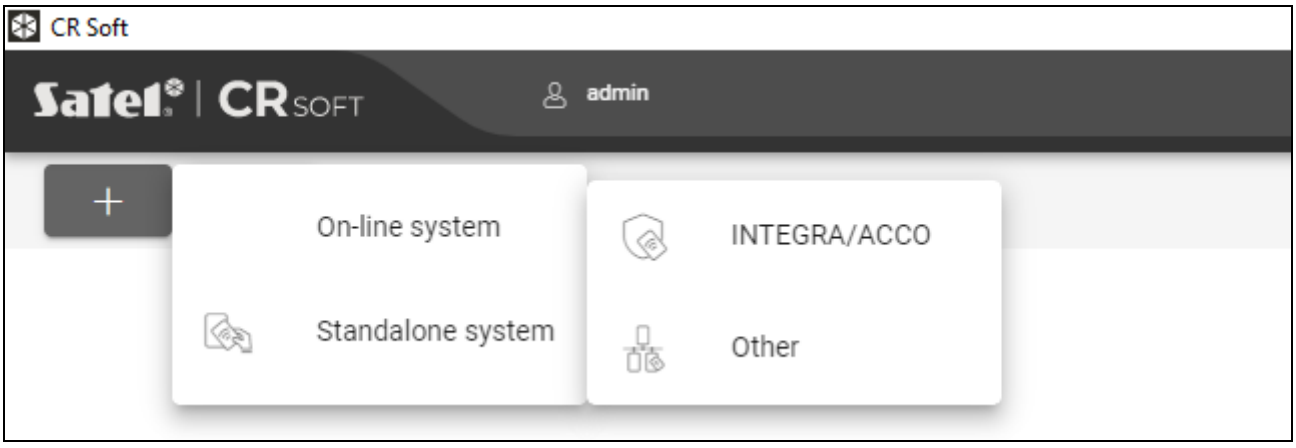
1. Click  . The menu of available project types will be displayed:

   On-line system – system in which the access control device is connected to another device (e.g. controller or control panel) which decides whether to grant access or not. You can select:

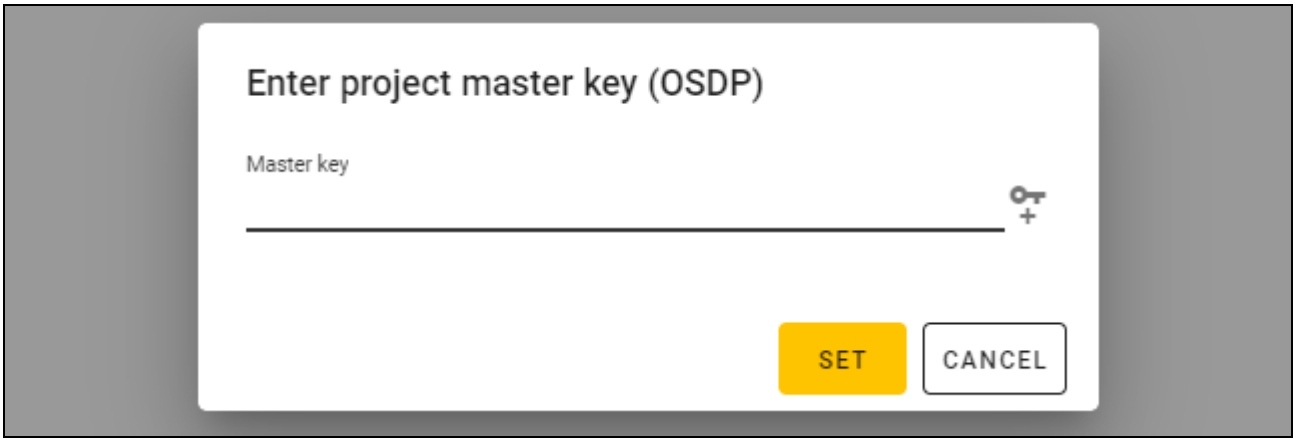
   INTEGRA/ACCO – access control devices and cards will be used in one of the SATEL systems: INTEGRA alarm system or ACCO access control system.

   Other – access control devices and cards will be used in other manufacturer's system.

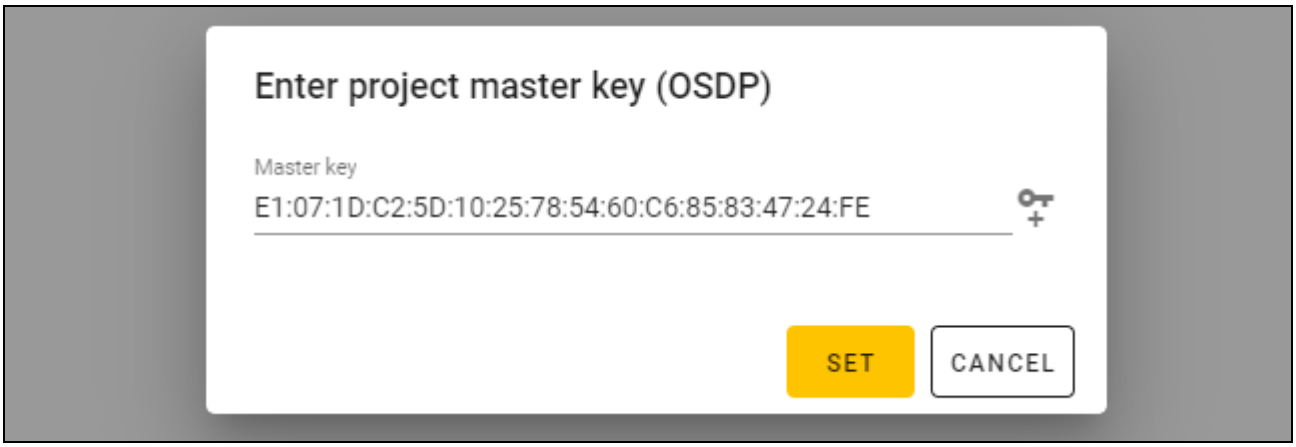
   Standalone system – system in which the access control device decides on its own whether to grant access to a single door or not (it operates as a standalone door control module).



2. Click the type of project you want to create. The “Enter project master key (OSDP)” window will be displayed.



3. Enter the master key (32 hexadecimal characters) or click to generate a random master key.

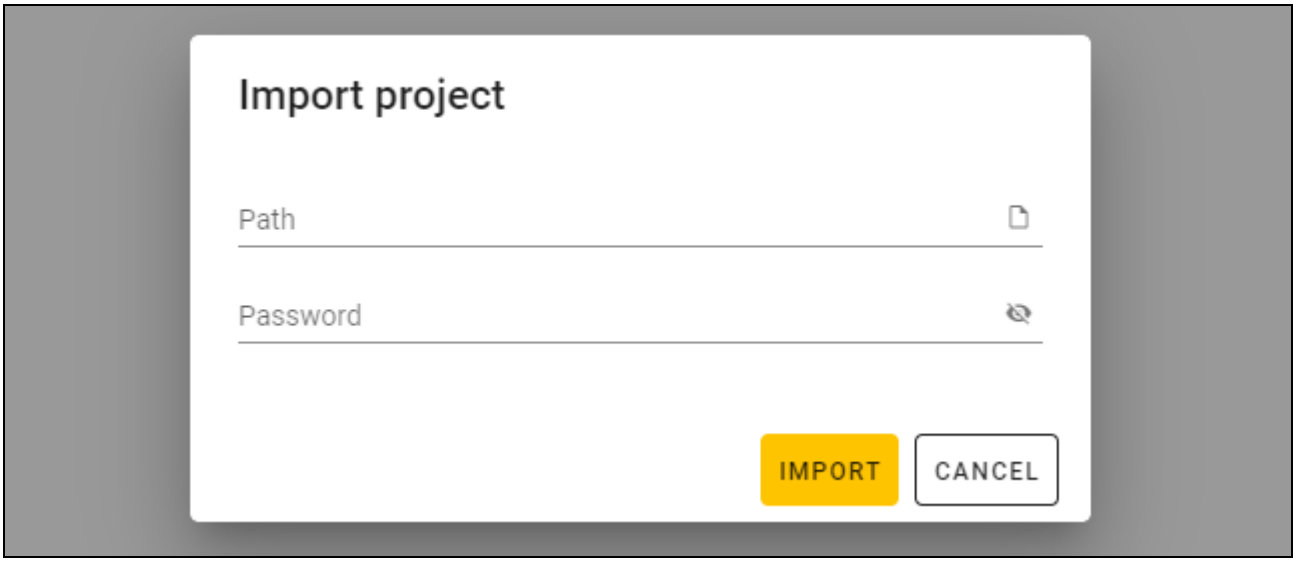


4. Click “SET”. The “Enter project master key (OSDP)” window will be closed. The “PROJECT” tab for the newly created project will be displayed.

4.3.2 Importing a project

This function is available when the list of projects is displayed.

1. Click . The “Import project” window will be displayed.



2. In the “Path” field, enter the file path or click to indicate the file location in the system window.
3. In the “Password” field, enter the password for the file you are importing.
4. Click “IMPORT”. The project successfully imported will be displayed on the list of projects.

4.3.3 Deleting a project

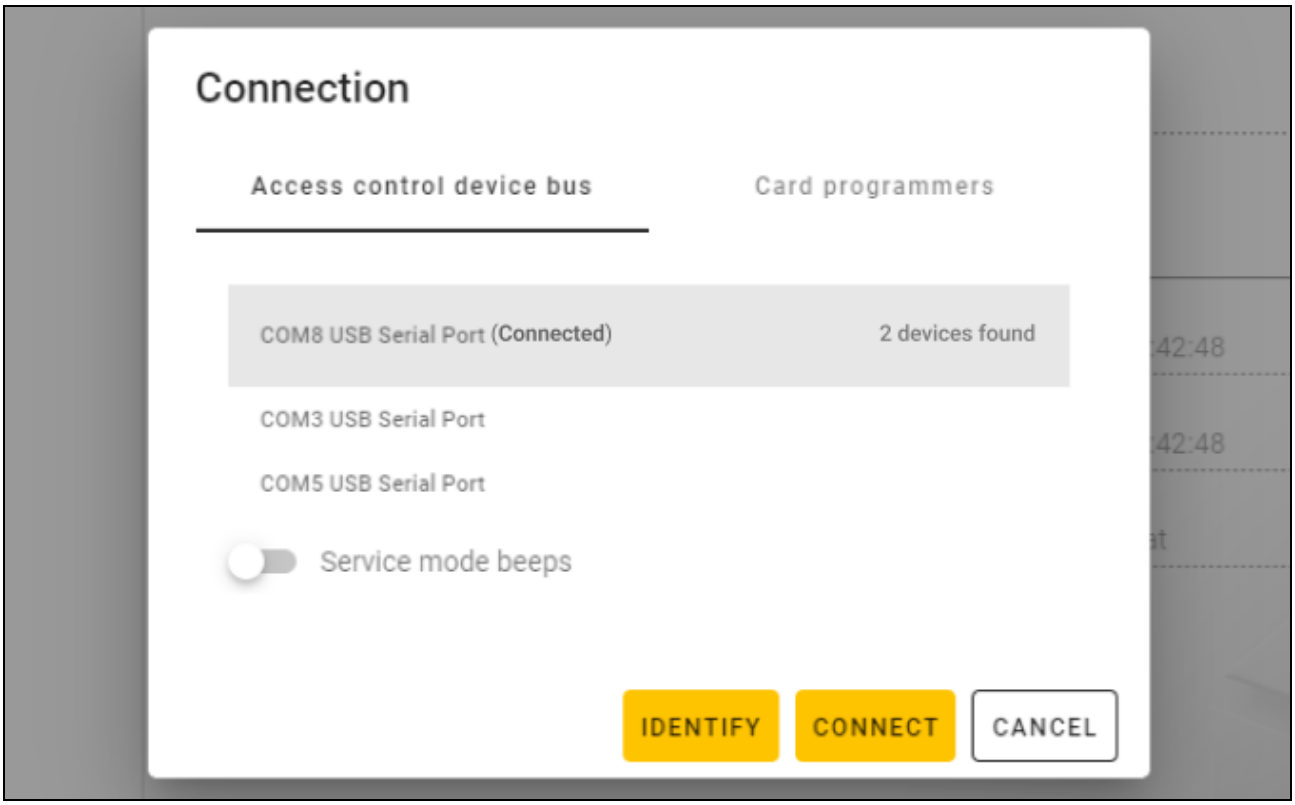
This function is available when the list of projects is displayed.

1. Hover the mouse over the project. The button will be displayed.
2. Click . A deletion confirmation window will be displayed.
3. Click “OK”. A message will confirm that the project has been deleted.

4.3.4 Establishing connection with access control devices

This function is available after opening a project.

1. Click on the menu bar. The menu will be displayed.
2. Click “CONNECTION”. The “Connection” window will be displayed.



3. Click the COM port assigned to the converter to which the access control devices that you want the program to connect with are connected.
4. If devices with factory settings are connected to the converter, click “IDENTIFY”. The program will assign unique addresses to the devices.

The address of devices with factory settings is 0.

If several devices have the same address, it is impossible to establish connection with the devices.

The identification function assigns addresses only to devices with the address 0. If several devices have the same address, but other than 0, do not connect them to the

converter at the same time. Connect them separately and give them unique addresses.

If the Service mode beeps *option is enabled, the devices beep when they are connected with the program.*

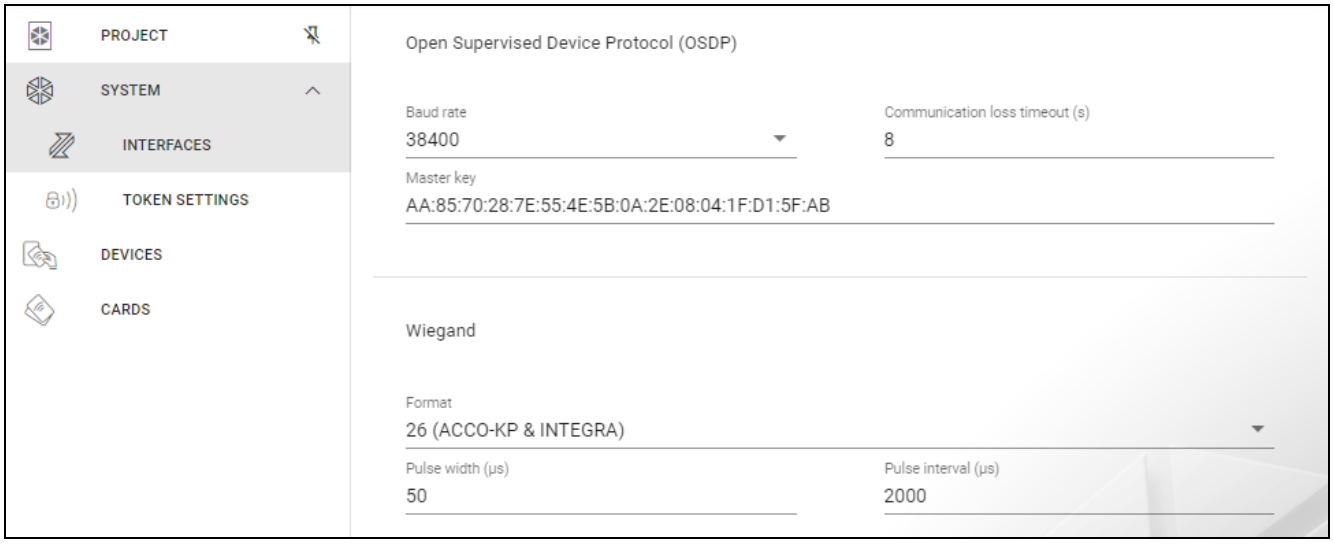
5. Click “CONNECT”. The program will connect with the devices. If the devices are new to the project, they will be added to the project (“DEVICES” tab).

4.3.5 Programming the interface settings

This function is available after opening a project.

1. Click the “INTERFACES” tab.
2. Program the communication interfaces settings that are to be used by the access control devices.
3. Click  on the menu bar to upload the interfaces settings to the devices.

Interfaces settings



Open Supervised Device Protocol (OSDP)

The protocol used for communication via the RS-485 bus. The bus is used to connect access control devices provided with the MIFARE reader to the computer. It can also be used to make connections in the ACCO NET system or systems of other manufacturers. It is a two-way, encrypted communication.

Baud rate – OSDP baud rate used by the devices in the system. Factory rate: 38400.

Communication loss timeout (s) – time after which the device’s LEDs start to indicate a loss of communication. By factory: 8 s.

Master key – key used to encrypt communication. It is set when the project is created. It can be changed. You can enter 32 hexadecimal characters (16 bytes).

The key should be unique for each project.

Wiegand

Additional interface. It is a one-way, unencrypted communication.

Format – Wiegand transmission format used by the devices. See: “Supported Wiegand transmission formats”.

Pulse width (µs) – duration of a pulse corresponding to 1 bit. By factory: 50 µs.

Pulse interval (µs) – duration of a gap between two pulses. By factory: 2000 µs.

Supported Wiegand transmission formats

26 (ACCO-KP & INTEGRA) – even parity bit + 24 data bits + odd parity bit; byte order: from MSB to LSB;

32 MSB (ACCO-KP) – 32 data bits without parity check; byte order: from MSB to LSB;

32 LSB – 32 data bits without parity check; byte order: from LSB to MSB;

33 – even parity bit + 31 data bits + odd parity bit; byte order: from MSB to LSB;

34 (ACCO-KP & INTEGRA) – even parity bit + 32 data bits + odd parity bit; byte order: from MSB to LSB;

35 – parity bit (even) + card number (33 bits) + parity bit (odd); byte order: from MSB to LSB;

36 (ACCO-KP) – even parity bit + 34 data bits + odd parity bit; byte order: from MSB to LSB;

36 XOR – 32 data bits + 4 parity check bits (XOR);

37 – parity bit (even) + card number (35 bits) + parity bit (odd); byte order: from MSB to LSB;

40 (ACCO-KP) – 40 data bits without parity check; byte order: from MSB to LSB;

42 (ACCO-KP & INTEGRA) – even parity bit + 40 data bits + odd parity bit; byte order: from MSB to LSB;

44 XOR – 40 data bits + 4 parity check bits (XOR);

56 MSB – 56 data bits without parity check; byte order: from MSB to LSB;

56 LSB (ACCO-KP & INTEGRA) – 56 data bits without parity check; byte order: from LSB to MSB;

58 – even parity bit + 56 data bits + odd parity bit; byte order: from MSB to LSB;

64 – 64 data bits without parity check; byte order: from MSB to LSB;

66 – even parity bit + 64 data bits + odd parity bit; byte order: from MSB to LSB.

Custom – you can program your own transmission format settings.

4.3.6 Programming the card settings

This function is available after opening a project.

1. Click the “TOKEN SETTINGS” tab.
2. Program the token settings.
3. Click  on the menu bar to upload the card settings to the devices.

Token settings for the INTEGRA/ACCO on-line system

SATEL token key – card number access key for all types of cards. After a project has been created, it is the same as the *Master key*. You can change it.

The key should be unique for each project.

No encryption – if this option is enabled, the card's factory serial number (CSN) is used as the card number. There is no need to program the cards.

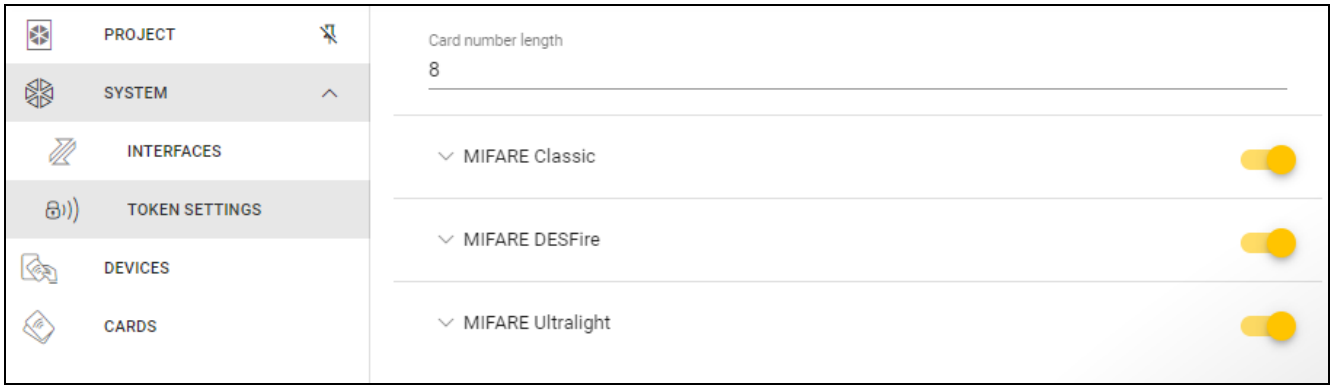
The card number length in the INTEGRA/ACCO system is 5 bytes.

For the MIFARE Classic card types, only the key's 6 lower bytes are used.

If you enable the No encryption *option, the* SATEL token key *will be cleared.*

Program the same settings in the INTEGRA alarm system / ACCO access control system.

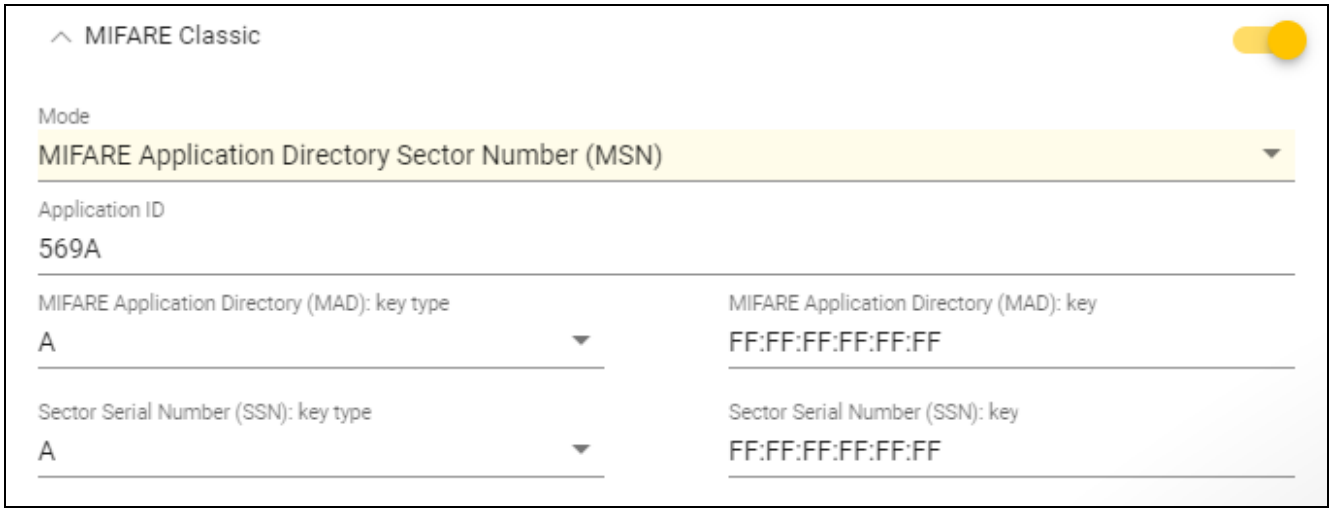
Token settings for other on-line system or standalone system



Card number length – number of bytes used for the card number. You can enter a number from 5 to 8.

The settings for each card type are available if support of these card types is enabled.

MIFARE Classic



Mode – card operating mode:

Chip Serial Number (CSN) – card's factory serial number is used as the card number. There is no need to program the cards. No additional settings are available for this mode.

Sector Serial Number (SSN) – card number can be programmed and written in the selected card memory sector.

MIFARE Application Directory Serial Number (MSN) – card number can be programmed and written in the card memory sector identified by the *Application ID* (AID).

Sector number – number of the data sector in which the card number is to be written. You can enter a number from 0 to 16. This parameter applies to the *Sector Serial Number (SSN)* mode.

Block – number of the block in the sector in which the card number is to be written. You can enter a number from 0 to 2. This parameter applies to the *Sector Serial Number (SSN)* mode.

Offset – card number's first byte position in the block. You can enter a number from 0 to 15. This parameter applies to the *Sector Serial Number (SSN)* mode.

Application ID – application identifier that indicates the sector containing the card number (AID). You can enter 4 hexadecimal characters (2 bytes). This parameter applies to the *MIFARE Application Directory Serial Number (MSN)* mode.

MIFARE Application Directory (MAD): key type – type of access key to the sector with application ID. You can select A or B. This parameter applies to the *MIFARE Application Directory Serial Number (MSN)* mode.

MIFARE Application Directory (MAD): key – access key to the sector with application ID. You can enter 12 hexadecimal characters (6 bytes). This parameter applies to the *MIFARE Application Directory Serial Number (MSN)* mode.

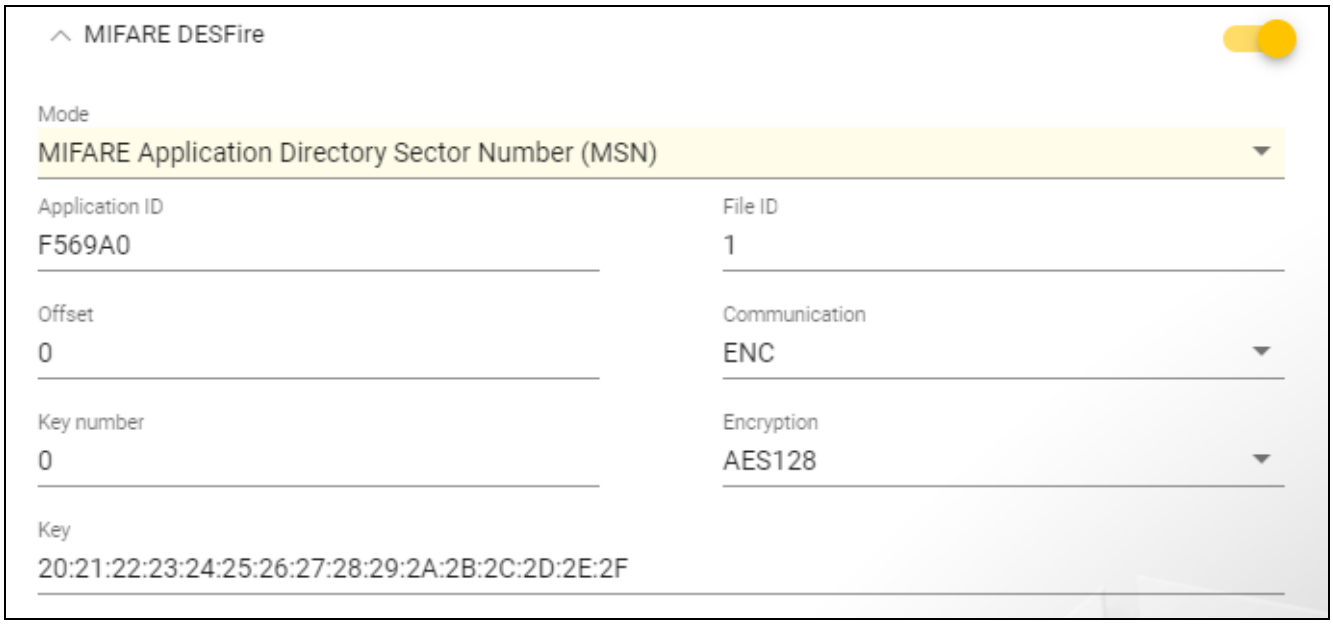
The key should be unique for each project.

Sector Serial Number (SSN): key type – type of access key to the sector containing the card number. You can select A or B.

Sector Serial Number (SSN): key – access key to the sector containing the card number. You can enter 12 hexadecimal characters (6 bytes).

The key should be unique for each project.

MIFARE DESFire



Mode – card operating mode:

Chip Serial Number (CSN) – card's factory serial number is used as the card number. There is no need to program the cards. No additional settings are available for this mode.

MIFARE Application Directory Serial Number (MSN) – card number can be programmed and written to the card.

Application ID – application identifier that indicates the directory containing the card number file. You can enter 6 hexadecimal characters (3 bytes).

File ID – number of the file with card number.

Offset – card number's first byte position in the file. You can enter a number from 0 to 99.

Communication – type of encryption used for communication:

PLAIN – communication is not encrypted.

MAC – communication is not encrypted but it is digitally authenticated.

ENC – communication is encrypted.

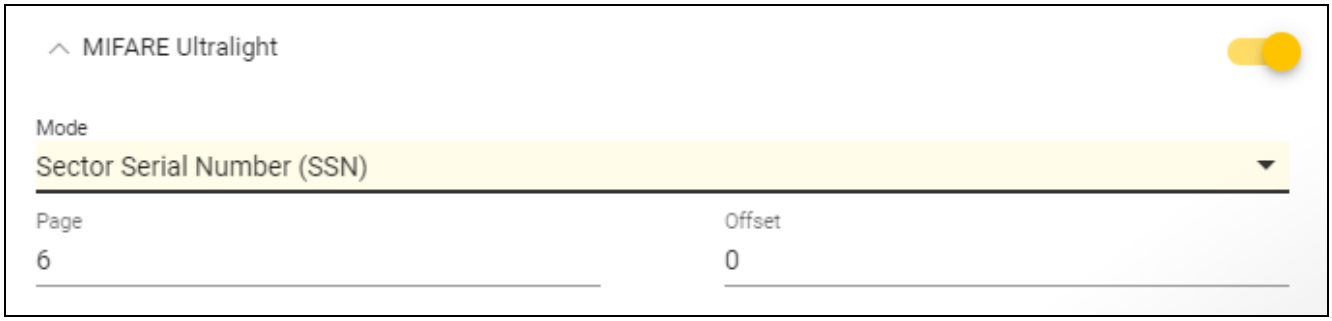
Key number – number of the key used to encrypt the card number file. This parameter applies to digitally signed communication (MAC) and encrypted communication (ENC).

Encryption – type of encryption key. You can select *DES*, *2K3DES* or *AES128*. This parameter applies to digitally signed communication (MAC) and encrypted communication (ENC).

Key – access key to the card number. This parameter applies to digitally signed communication (MAC) and encrypted communication (ENC).

The key should be unique for each project.

MIFARE Ultralight



Mode – card operating mode:

Chip Serial Number (CSN) – card's factory serial number is used as the card number. There is no need to program the cards. No additional settings are available for this mode.

Sector Serial Number (SSN) – card number can be programmed and written to the card.

Page – number of the page containing the card number. You can enter a number from 0 to 100.

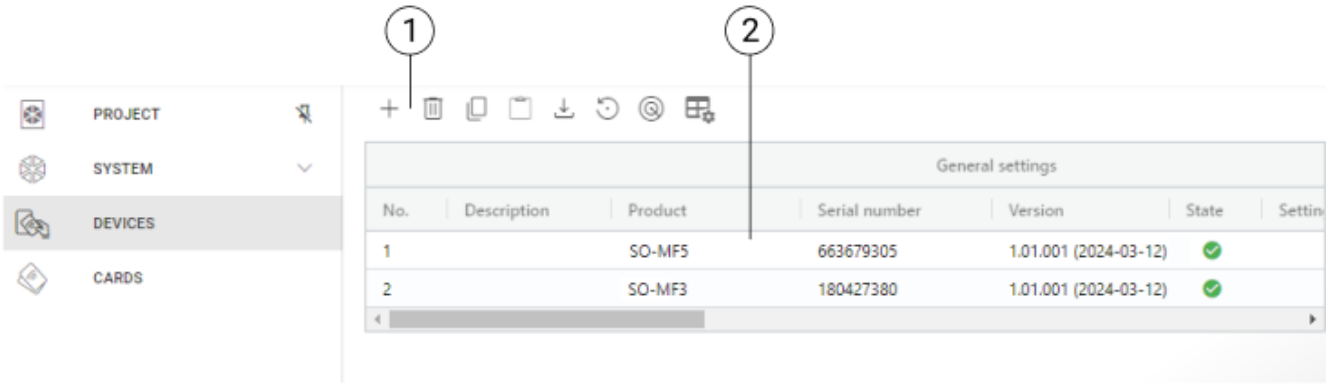
Offset – card number's first byte position on the page. You can enter a number from 0 to 3.

4.3.7 Programming the access control device settings

This function is available after opening a project.

1. Click the "DEVICES" tab.
2. Program the devices settings.
3. Click  on the menu bar to upload the settings to the devices.

Description of the “DEVICES” tab



(1) tool bar for the list of devices.

(2) list of devices.

Tool bar for the list of devices

Device-related buttons and functions are displayed on the tool bar.

- click to add a device to the project without connecting with the device (see: “Adding to the project a device not connected to the computer”).

- click to delete device(s) from the project (see: “Deleting a device from the project”). This button is available if at least one device is selected.

- click to copy the device settings. This button is available when the device is selected.

- click to paste the settings to the selected device(s). This button is available if you had copied the settings.

- click to copy the system settings from the device (communication interfaces and token settings). This button is displayed when the program is connected with the devices and the device is selected.

- click to restore the factory settings of the device(s). This button is displayed when the program is connected with the devices and at least one device is selected.

- click to find a device (the device’s LED indicators will start to flash rapidly). Click again to end the function. This button is displayed when the program is connected with the devices and the device is selected.

- click to edit the settings of the table with the list of devices.

List of devices

The devices added to the project are displayed on the list.

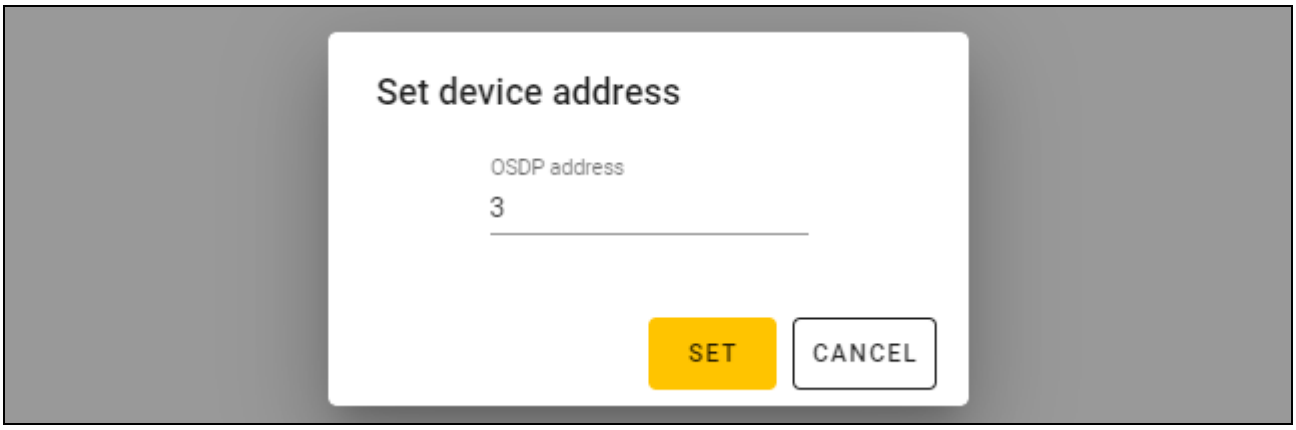
Adding a device to the project

Adding to the project a device connected to the computer

If the access control device is connected to the computer, it will be automatically added to the project when communication is established with the device (see: “Establishing connection with access control devices” p. 14).

Adding to the project a device not connected to the computer

1. Click + . The “Set device address” window will be displayed.



2. In the “OSDP address” field, enter the OSDP address you want to assign to the device. You can enter a number from 1 to 126.
3. Click “SET”. The “Set device address” window will be closed. The new device will be added to the list of devices.

Reader settings

General settings

Description – additional description of the device.

Product – type of access control device.

Serial number – serial number of the device. It is read after connection is established with the device. You will find it on the label inside the device enclosure (marked as Satel MNI).

Version – firmware version of the device.

State – the icon indicates the connection status of the device. Hover the mouse over the icon to see its description.

Settings problem – the icon indicates the status of the device settings. Hover the mouse over the icon to see its description.

OSDP address – the device’s OSDP address. Each device must have a unique address. The factory address of each device is 0. The address is assigned automatically to devices (see: “Establishing connection with access control devices” p. 14). You can set a different address in the range from 1 to 126 (see: “Changing the device’s OSDP address” p. 23).

Additional interface

The settings are not available in a *Standalone system* type project.

Type – type of additional interface used by the reader:

Not used – additional interface is not used.

EM-Marine – interface used in the INTEGRA and ACCO systems.

Wiegand – interface used in the INTEGRA and ACCO systems as well as other manufacturers’ systems.

NFC

Send the card ID – way of sending the card ID:

According to system – the card ID is sent according to the settings of the system in which the device operates.

After presenting the card – the card ID is sent immediately after it is read.

After moving the card away – the card ID is sent after the card has been moved away from the reader.

Signal identifier sending – way of signaling the card ID sending:

According to system – the card ID sending is signaled according to the settings of the system in which the device operates (recommended for the INTEGRA system).

Disable – device does not signal the card ID sending.

Enable – device signals the card ID sending with a short beep.

Inputs

The settings are available when the Wiegand interface (additional interface) is used.

Input operating mode – input activation mode:

High level sensitive – input is controlled by high level.

Low level sensitive – input is controlled by low level.

IN1 input – IN1 input function:

Disable – input is not used.

Sounder – sounder control.

LED: green – green LED control.

LED: red – red LED control.

LED: yellow – yellow LED control.

LED: blue – blue LED control.

IN1 input type – type of circuit:

NC – normally closed.

NO – normally open.

IN2 input – IN2 input function:

Disable – input is not used.

Sounder – sounder control.

LED: green – green LED control.

LED: red – red LED control.

LED: yellow – yellow LED control.

LED: blue – blue LED control.

IN2 input type – type of circuit:

NC – normally closed.

NO – normally open.

IN3 input – IN3 input function:

Disable – input is not used.

Sounder – sounder control.

LED: green – green LED control.

LED: red – red LED control.

LED: yellow – yellow LED control.

LED: blue – blue LED control.

IN3 input type – type of circuit:

NC – normally closed.

NO – normally open.

Standalone settings

The settings are available in a *Standalone system* type project.

Door status input – settings of the input that controls the door status (IN1):

Unused – input is not used.

NC – input supports a detector provided with the NC (normally closed) type output.

NO – input supports a detector provided with the NO (normally open) type output.

Request-to-exit input – request-to-exit input settings (IN2):

Unused – input is not used.

NC – input supports the NC (normally closed) type button.

NO – input supports the NO (normally open) type button.

Request-to-exit button – used type of request-to-exit button:

Monostable – button has one stable state.

Bistable – button has two stable states.

Door unlock time – time for which the relay remains active after gaining access. You can enter 1-255 seconds. When this time is counted down, you can open the door.

Shorten the door unlock time – operating mode of the function to shorten the door unlock time:

Disable – function to shorten the door unlock time is not used.

After opening the door – opening the door will stop the countdown of the door unlock time (relay will be turned off).

After closing the door – closing the door will stop the countdown of the door unlock time (relay will be turned off).

For the Shorten the door unlock time *function to work, the door status control must be controlled (a detector must be connected to the door status input)*.

Door open time – maximum time for which the door can be open after gaining access. If the door is open longer, the device will indicate long open door. You can enter 0-255 seconds. If you enter 0, the function will be disabled. This feature requires the door status control (a detector must be connected to the door status input).

Additional settings

Beep volume – volume of sounds emitted by the reader.

Tamper – if this option is enabled, the device controls the status of tamper protection.

Changing the device's OSDP address

1. Double-click a field in the "OSDP address" column. The "Set device address" window will be displayed.
2. In the "OSDP address" field, enter the OSDP address you want to assign to the device. You can enter a number from 1 to 126.
3. Click "SET". The "Set device address" window will be closed. A message will confirm that the address has been changed.

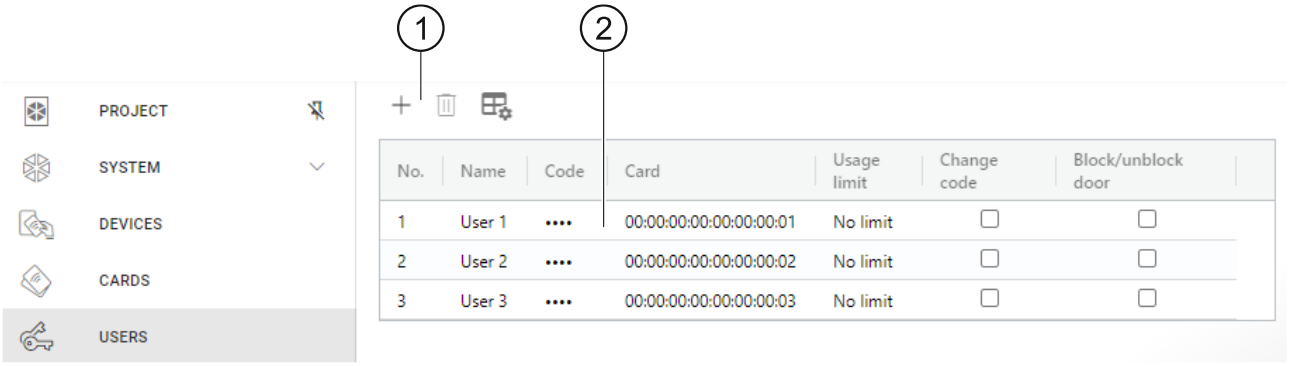
Deleting a device from the project

1. Click a device on the list to select it.
2. Click . The device will be deleted.

4.3.8 Managing users

This function is available after opening a *Standalone system* type project. You can manage the users in the "USERS" tab.

Description of the “USERS” tab



(1) tool bar for the list of users.

(2) list of users.

Tool bar for the list of users

Users-related buttons and functions are displayed on the tool bar.

- click to add a user to the project (see: “Adding a user to the project”).

- click to delete user(s) from the project (see: “Deleting a user from the project”). This button is available if at least one user is selected.

- click to edit the settings of the table with the list of users.

List of users

The users added to the project are displayed on the list.

Adding a user to the project

1. Click . The new user will be added to the list of users.
2. Add a card to the user (see: “Adding a card to the user”).

A user who has no code or card cannot be written to devices. The user will be automatically deleted after the project is closed.

3. Program the remaining user settings.
4. Click on the menu bar to write the user to the devices.

User settings

Name – user name.

Code – *does not apply to the SO-MF3 reader*.

Card – if the user has no card, the button is displayed in the field – click to add a card to the user (see: “Adding a card to the user”). If the user has a card, the card’s number is displayed in the field – click to change the user’s card (see: “Changing the user’s card”) or delete the card (see: “Deleting the user’s card”).

Usage limit – number of times the card can be used until the user loses access to the device.

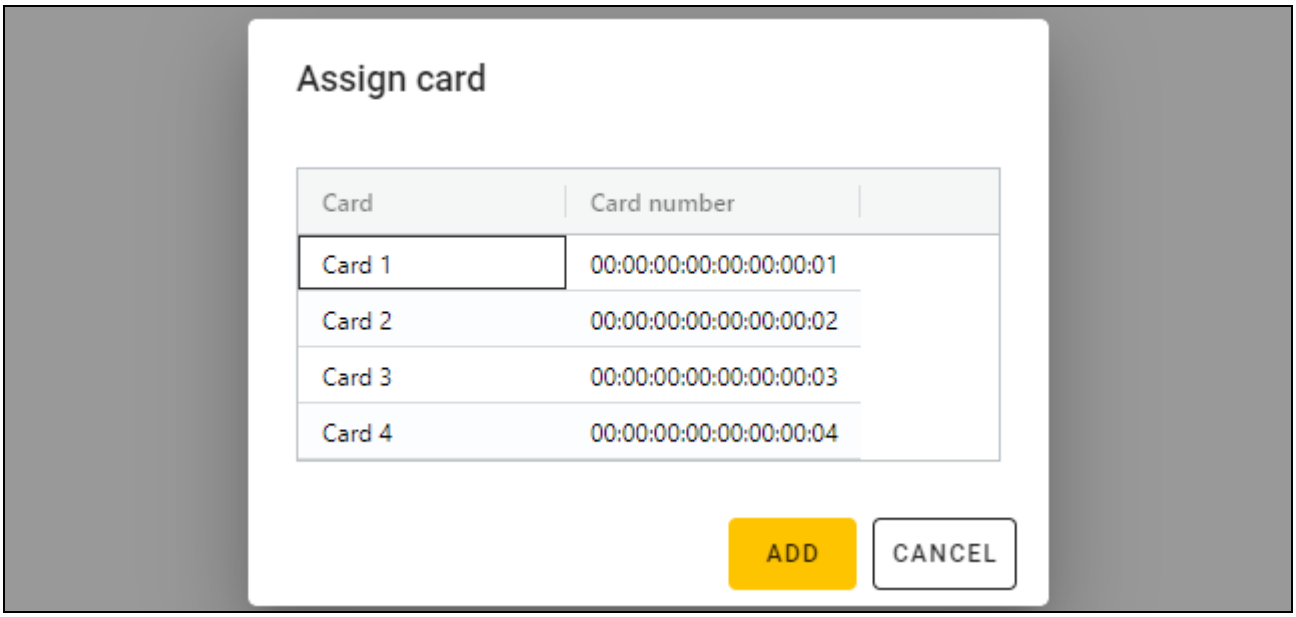
Change code – *does not apply to the SO-MF3 reader*.

Block/unblock door – if this option is enabled, the user can block / unblock the door.

Adding a card to the user

1. Click ⊞ in the “Card” column. The “Assign card” window will be displayed.

The cards that can be assigned to the user are displayed in the “Assign card” window. These are the cards that have been added in the “CARDS” tab but have not yet been assigned to any users. For instructions on how to add and program cards, please refer to the SO-PRG programmer manual.

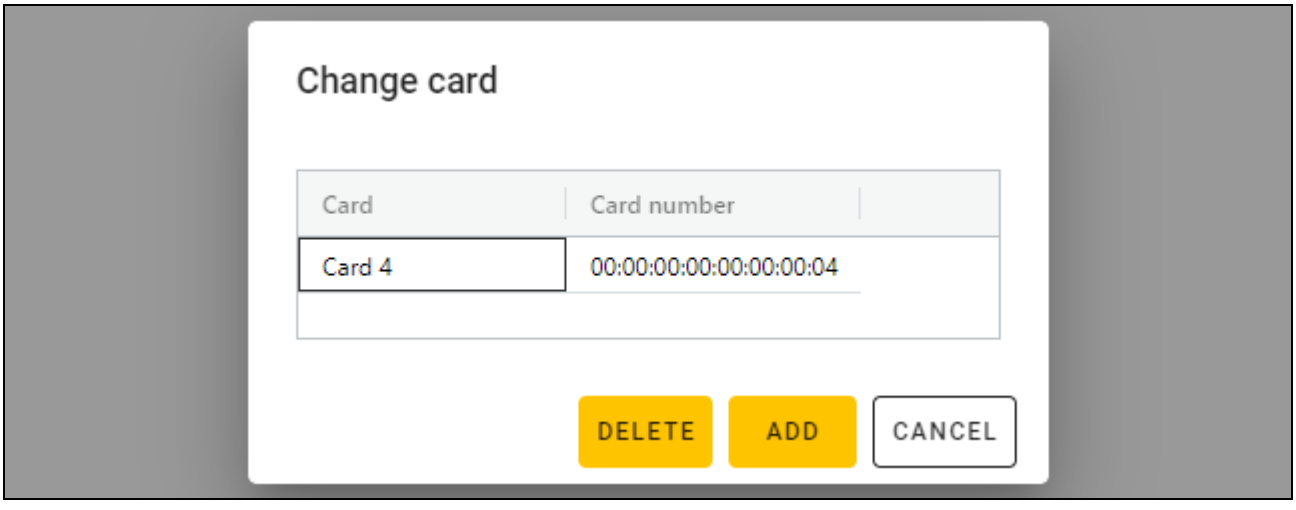


2. Click the card that you want to add to the user.
3. Click “ADD”. The “Assign card” window will be closed. In the “Card” column, the card number will be displayed.

Changing the user’s card

1. Click the user’s card number. The “Change card” window will be displayed.

The cards that can be assigned to the user are displayed in the “Change card” window. These are the cards that have been added in the “CARDS” tab but have not yet been assigned to any users. For instructions on how to add and program cards, please refer to the SO-PRG programmer manual.



2. Click the card that you want to add to the user.
3. Click “ADD”. The “Change card” window will be closed. In the “Card” column, the number of the new card will be displayed.

Deleting the user's card

1. Click the user's card number. The "Change card" window will be displayed.
2. Click „DELETE". The "Change card" window will be closed. The button will be displayed in the "Card" column.

Deleting a user from the project

1. To select the user, click the user on the list.
2. Click . The user will be deleted.
3. Click on the menu bar to save the changes to the devices.

4.3.9 Saving changes in the project

This function is available after opening a project.

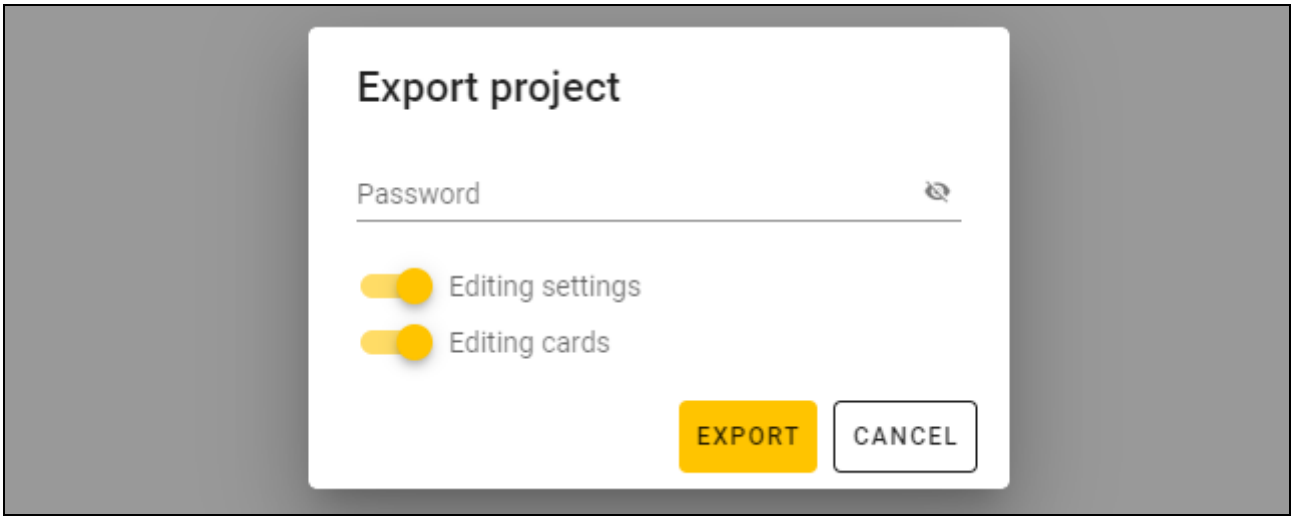
1. Click on the menu bar. The menu will be displayed.
2. Click "SAVE". A saving window will be displayed.
3. Click "SAVE" if you do not want to rename the project or click "SAVE AS" if you want to rename the project.

You can use the Ctrl + S shortcut to skip the first two steps and open the saving window right away.

4.3.10 Exporting a project

This function is available after opening a project.

1. Click on the menu bar. The menu will be displayed.
2. Click "EXPORT". The "Export project" window will be displayed.



3. In the "Password" field, enter the password to secure the file you are exporting (1-16 digits, letters or special characters).
4. Disable the *Editing settings* option if the system settings are to be unavailable after the file is imported (the "System" and "Devices" tabs will not be displayed).
5. Disable the *Editing cards* option if card editing is to be unavailable after the file is imported (the "Cards" tab will be displayed but you will not be able to manage the cards).
6. Click "EXPORT". A system window will be displayed in which you should indicate where the exported file is to be saved.

5. Reader in the INTEGRA system

5.1 Installation in the INTEGRA system

The device should be installed indoors, in spaces with normal air humidity.

The reader must be connected to the INT-R expander for card / ibutton readers.

Disconnect power before making any electrical connections.

5.1.1 Installation in short

1. Open the reader enclosure (see “Enclosure opening tool” p. 5).
2. Connect the reader to the computer (p. 9).
3. Program the reader in the CR SOFT program.
   3.1. Create a new *On-line system: INTEGRA/ACCO* type project (p. 12) or open an existing project.
   3.2. Establish connection between the program and the device (p. 14).
   3.3. If the Wiegand interface is to be used, program its settings (p. 15).
   3.4. Program the cards settings (p. 16).
   3.5. Program the reader settings (p. 19):
   - select *EM-Marin* or *Wiegand* as the type of additional interface (select interface supported by the INT-R expander that the reader is to be connected to – see the INT-R expander for card / ibutton readers manual),
   - program the remaining settings.

The Wiegand interface readers do not support the feature of holding the card.

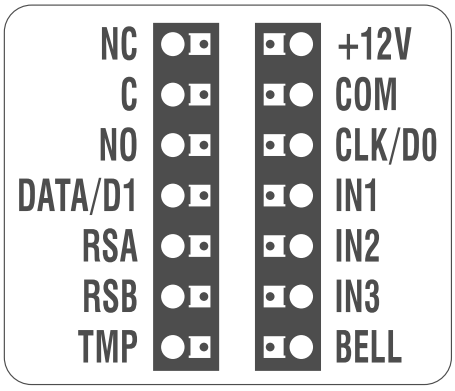
4. Disconnect the reader from the computer.
5. Run the cables to where you want to install the reader. Use unshielded straight-through cables.

The length of cable connecting the reader with the INT-R expander should not exceed 30 m.

6. Mount the reader and start it (p. 28).

5.1.2 Description of terminals for reader in the INTEGRA system

4



Terminal	Description
NC	*not used*
C	*not used*
NO	*not used*
DATA/D1	*not used* [EM-Marin interface] / data (1) [Wiegand interface]
RSA	RS-485 bus terminal [OSDP]
RSB	RS-485 bus terminal [OSDP]
TMP	tamper output
+12V	+12 VDC power input
COM	common ground
CLK/D0	data [EM-Marin interface] / data (0) [Wiegand interface]
IN1	programmable input [EM-Marin / Wiegand interface]
IN2	programmable input [EM-Marin / Wiegand interface]
IN3	programmable input [EM-Marin / Wiegand interface]
BELL	*not used*

5.1.3 Mounting the reader in the INTEGRA system

1. Place the enclosure base against the wall and mark the location of mounting holes.
2. Drill the holes in the wall for wall plugs (anchors).
3. Run wires through the opening in the enclosure base.
4. Use wall plugs and screws to secure the enclosure base to the wall. Select wall plugs specifically intended for the mounting surface (different for concrete or brick wall, different for plaster wall, etc.).
5. Connect the reader terminals with the INT-R expander terminals (see: “Connecting using the EM-Marin interface” or “Connecting using the Wiegand interface”).
6. Close the reader enclosure.
7. Power on the reader.

Connecting using the EM-Marin interface

SO-MF3 reader terminals	INT-R expander terminals	
	Reader A	Reader B
TMP	TMPA	TMPB
+12V	+GA	+GB
COM	COM	COM
CLK/D0	SIG1A	SIG1B
IN1 [program as *LED: red*]	LD2A	LD2B
IN2 [program as *LED: green*]	LD1A	LD1B
IN3 [program as *Sounder*]	BPA	BPB

If you program functions other than the ones recommended in the table for the IN1...IN3 inputs, the LED indicators or the sounder will operate differently from what is described in the INT-R expander manual. Inform the users about the changes.

Connecting using the Wiegand interface

SO-MF3 reader terminals	INT-R expander terminals	
	Reader A	Reader B
DATA/D1	SIG2A	SIG2B
TMP	TMPA	TMPB
+12V	+GA	+GB
COM	COM	COM
CLK/D0	SIG1A	SIG1B
IN1 [program as *LED: red*]	LD2A	LD2B
IN2 [program as *LED: green*]	LD1A	LD1B
IN3 [program as *Sounder*]	BPA	BPB

If you program functions other than the ones recommended in the table for the IN1...IN3 inputs, the LED indicators or the sounder will operate differently from what is described in the INT-R expander manual. Inform the users about the changes.

5.2 Using the reader in the INTEGRA system

For information on how to use the reader, please refer to the INT-R expander manual.

If the EM-Marin interface is used, the reader distinguishes between presenting and holding the card (the card must be presented to the reader and held for 3 seconds). The Wiegand interface reader only reacts to presenting the card.

6. Reader in the ACCO system

6.1 Installation in the ACCO system

The device should be installed indoors, in spaces with normal air humidity.

The reader must be connected to one of the access control modules: ACCO-KP2, ACCO-KP-PS, ACCO-KP, ACCO-KPWG-PS or ACCO-KPWG.

Disconnect power before making any electrical connections.

6.1.1 Installation in short

Connecting using the EM-Marin / Wiegand interface

The EM-Marin interface enables the reader to be connected to any of the above access control modules. The Wiegand interface is only supported by the ACCO-KP2, ACCO-KPWG-PS and ACCO-KPWG modules.

1. Open the reader enclosure (see “Enclosure opening tool” p. 5).
2. Connect the reader to the computer (p. 5).

3. Program the reader in the CR SOFT program.
   3.1. Create a new *On-line system: INTEGRA/ACCO* type project (p. 12) or open an existing project.
   3.2. Establish connection between the program and the device (p. 14).
   3.3. If the Wiegand interface is to be used, program its settings (p. 15).
   3.4. Program the cards settings (p. 16).
   3.5. Program the reader settings (p. 19):
      – select *EM-Marin* or *Wiegand* as the type of additional interface (select interface supported by the access control module that the reader is to be connected to),
      – program the remaining settings.
4. Disconnect the reader from the computer.
5. Run the cables to where you want to install the reader. Use unshielded straight-through cables.

The length of cable connecting the reader with the access control module should not exceed 30 m.

6. Mount the reader and start it (p. 31).

Connecting using the RS-485 bus (OSDP)

The RS-485 bus enables the reader to be connected to the ACCO-KP2 access control module (firmware version required: 1.01 or newer).

1. Open the reader enclosure (see “Enclosure opening tool” p. 5).
2. Connect the reader to the computer (p. 5).
3. Program the reader in the CR SOFT program.
   3.1. Create a new *On-line system: INTEGRA/ACCO* type project (p. 12) or open an existing project.
   3.2. Establish connection between the program and the device (p. 14).
   3.3. Program the OSDP protocol settings (p. 15).
   3.4. Program the cards settings (p. 16).
   3.5. Program the reader settings (p. 19):
      – select *Not used* as the additional interface type.
      – program the remaining settings.
4. Disconnect the reader from the computer.
5. Run the cables to where you want to install the reader. For the RS-485 bus, we recommend using a UTP cable (unshielded twisted pair). To make other connections, use unshielded straight-through cables.

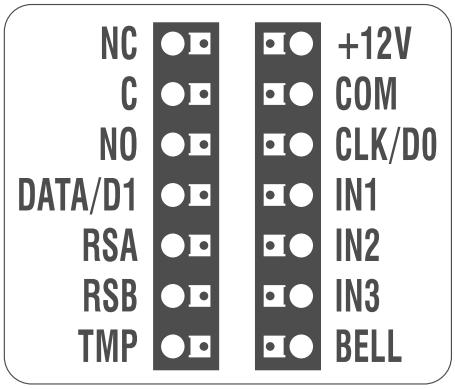
The RS-485 bus may be up to 1200 m long.

6. Mount the reader and start it (p. 31).

The ACCO Soft program in version 1.9 (or newer) enables programming of all the required settings (ACCO NET system). If it is to be used, you can skip the steps 2-4.

6.1.2 Description of terminals for reader in the ACCO system

5



Terminal	Description
NC	*not used*
C	*not used*
NO	*not used*
DATA/D1	*not used* [EM-Marin interface] / data (1) [Wiegand interface]
RSA	RS-485 bus terminal [OSDP]
RSB	RS-485 bus terminal [OSDP]
TMP	tamper output
+12V	+12 VDC power input
COM	common ground
CLK/D0	data [EM-Marin interface] / data (0) [Wiegand interface]
IN1	programmable input [EM-Marin / Wiegand interface]
IN2	programmable input [EM-Marin / Wiegand interface]
IN3	programmable input [EM-Marin / Wiegand interface]
BELL	*not used*

6.1.3 Mounting the reader in the ACCO system

1. Place the enclosure base against the wall and mark the location of mounting holes.
2. Drill the holes in the wall for wall plugs (anchors).
3. Run wires through the opening in the enclosure base.
4. Use wall plugs and screws to secure the enclosure base to the wall. Select wall plugs specifically intended for the mounting surface (different for concrete or brick wall, different for plaster wall, etc.).
5. Connect the reader terminals with the controller terminals (see: “Connecting using the EM-Marin interface”, “Connecting using the Wiegand interface” or “Connecting using the RS-485 bus (OSDP)”).
6. Close the reader enclosure.
7. Power on the reader.

Connecting using the EM-Marin interface

Connecting to the ACCO-KP-PS / ACCO-KP controller

SO-MF3 reader terminals	ACCO-KP-PS / ACCO-KP controller terminals	
	Reader A	Reader B
TMP	TMPA	TMPB
+12V	+GA	+GB
COM	COM	COM
CLK/D0	SIGA	SIGB
IN1 [program as *LED: red*]	LD2A	LD2B
IN2 [program as *LED: green*]	LD1A	LD1B
IN3 [program as *Sounder*]	BPA	BPB

If you program functions other than the ones recommended in the table for the IN1...IN3 inputs, the LED indicators or the sounder will operate differently from what is described in the ACCO-KP-PS / ACCO-KP controller manual. Inform the users about the changes.

Connecting to the ACCO-KPWG-PS / ACCO-KPWG controller

SO-MF3 reader terminals	ACCO-KPWG-PS / ACCO-KPWG controller terminals	
	Reader A	Reader B
TMP	TMPA	TMPB
+12V	+G	
COM	COM	COM
CLK/D0	SIG1A	SIG1B
IN1 [program as *LED: red*]	LD2A	LD2B
IN2 [program as *LED: green*]	LD1A	LD1B
IN3 [program as *Sounder*]	BPA	BPB

If you program functions other than the ones recommended in the table for the IN1...IN3 inputs, the LED indicators or the sounder will operate differently from what is described in the ACCO-KPWG-PS / ACCO-KPWG controller manual. Inform the users about the changes.

Connecting to the ACCO-KP2 controller

SO-MF3 reader terminals	ACCO-KP2 controller terminals	
	Reader A	Reader B
TMP	IN3	IN7
+12V	+G1…+G4	
COM	COM	
CLK/D0	IN1	IN5
IN1 [program as *LED: red*]	OUT3	OUT7
IN2 [program as *LED: green*]	OUT2	OUT6
IN3 [program as *Sounder*]	OUT1	OUT5

If you program functions other than the ones recommended in the table for the IN1...IN3 inputs, the LED indicators or the sounder will operate differently from what is described in the ACCO-KP2 controller manual. Inform the users about the changes.

Connecting using the Wiegand interface

Connecting to the ACCO-KPWG-PS / ACCO-KPWG controller

SO-MF3 reader terminals	ACCO-KPWG-PS / ACCO-KPWG controller terminals	
	Reader A	Reader B
DATA/D1	SIG2A	SIG2B
TMP	TMPA	TMPB
+12V	+G	
COM	COM	COM
CLK/D0	SIG1A	SIG1B
IN1 [program as *LED: red*]	LD2A	LD2B
IN2 [program as *LED: green*]	LD1A	LD1B
IN3 [program as *Sounder*]	BPA	BPB

If you program functions other than the ones recommended in the table for the IN1...IN3 inputs, the LED indicators or the sounder will operate differently from what is described in the ACCO-KPWG-PS / ACCO-KPWG controller manual. Inform the users about the changes.

Connecting to the ACCO-KP2 controller

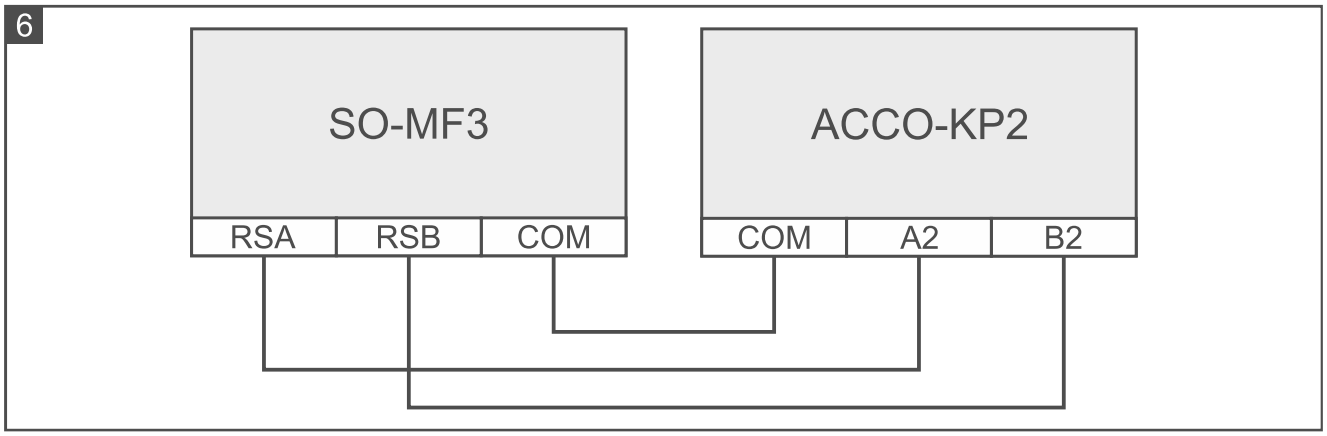
SO-MF3 reader terminals	ACCO-KP2 controller terminals	
	Reader A	Reader B
DATA/D1	IN2	IN6
TMP	IN3	IN7
+12V	+G1…+G4	
COM	COM	
CLK/D0	IN1	IN5
IN1 [program as *LED: red*]	OUT3	OUT7
IN2 [program as *LED: green*]	OUT2	OUT6
IN3 [program as *Sounder*]	OUT1	OUT5

If you program functions other than the ones recommended in the table for the IN1...IN3 inputs, the LED indicators or the sounder will operate differently from what is described in the ACCO-KP2 controller manual. Inform the users about the changes.

Connecting using the RS-485 bus (OSDP)

Connect the reader's RSA terminal with the controller's A2 terminal, and the RSB terminal – with the controller's B2 terminal. Also, connect the reader's and the controller's COM terminals together.

6



6.2 Using the reader in the ACCO system

For information on how to use the reader, please refer to the controller or the ACCO NET system manuals. Note that the LED indicators operate differently when the SO-MF3 reader uses the OSDP communication (it is connected via the RS-485 bus).

6.2.1 LED indicators (OSDP communication)

LED	Color	Description
	blue	**ON** – door unblocked (permanently unlocked) **flashing slowly** – door unblocked (permanently unlocked) after the "Fire – unblock door" type of input is activated **flashing rapidly** – door unlocked (user gained access)
	red	**ON** – alarm **flashing** – alarm memory
	green	**ON** – door blocked (permanently locked) **flashing slowly** – door blocked (permanently locked) after the "Alarm – block door" type of input is activated
	yellow	not used

Flashing of the LEDs successively from left to right indicates no connection with the controller (e.g. connection made incorrectly).

7. Reader in other manufacturer's system

7.1 Installation in other manufacturer's system

The device should be installed indoors, in spaces with normal air humidity.

The reader must be connected to a device that supports the OSDP protocol or the Wiegand interface.

Disconnect power before making any electrical connections.

7.1.1 Installation in short

1. Open the reader enclosure (see "Enclosure opening tool" p. 5).
2. Connect the reader to the computer (p. 5).
3. Program the reader in the CR SOFT program.
   3.1. Create a new *On-line system: Other* type project (p. 12) or open an existing project.
   3.2. Establish connection between the program and the device (p. 14).
   3.3. Program the OSDP or Wiegand protocol settings (p. 15).
   3.4. Program the cards settings (p. 16).
   3.5. Program the reader settings (p. 19):
   - select *Not used* as the additional interface type if the RS-485 bus is to be used for connecting the reader, or *Wiegand* if the Wiegand interface is to be used for connecting.
   - program the remaining settings.
4. Disconnect the reader from the computer.
5. Run the cables to where you want to install the reader. For the RS-485 bus, we recommend using a UTP cable (unshielded twisted pair). To make other connections, use unshielded straight-through cables.

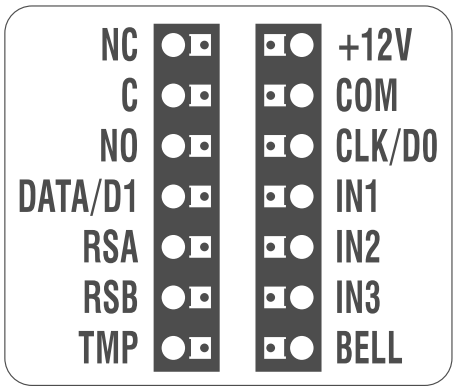
The RS-485 bus may be up to 1200 m long.

In the case of the Wiegand interface, the length of cable connecting the reader with the device should not exceed 30 m.

6. Mount the reader and start it (p. 31).

7.1.2 Description of terminals for reader in other manufacturer's system

7



Terminal	Description
NC	*not used*
C	*not used*
NO	*not used*
DATA/D1	data (1) [Wiegand interface]
RSA	RS-485 bus terminal [OSDP]
RSB	RS-485 bus terminal [OSDP]
TMP	tamper output
+12V	+12 VDC power input
COM	common ground
CLK/D0	data (0) [Wiegand interface]
IN1	programmable input [Wiegand interface]
IN2	programmable input [Wiegand interface]
IN3	programmable input [Wiegand interface]
BELL	*not used*

7.1.3 Mounting the reader in other manufacturer's system

1. Place the enclosure base against the wall and mark the location of mounting holes.
2. Drill the holes in the wall for wall plugs (anchors).
3. Run wires through the opening in the enclosure base.
4. Use wall plugs and screws to secure the enclosure base to the wall. Select wall plugs specifically intended for the mounting surface (different for concrete or brick wall, different for plaster wall, etc.).
5. Connect the reader as required by the system in which the reader is to operate.
6. Close the reader enclosure.
7. Power on the reader.

8. Standalone door control module

8.1 Features

- Support for up to 128 proximity cards.
- Functions started using the proximity card:
  – unlocking the door,
  – blocking / unblocking the door.
- Ability to specify the number of the card use.

8.2 Installation of the standalone door control module

The device should be installed indoors, in spaces with normal air humidity.

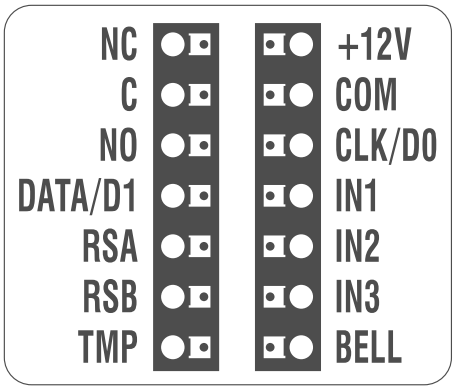
Disconnect power before making any electrical connections.

8.2.1 Installation in short

1. Open the reader enclosure (see “Enclosure opening tool” p. 5).
2. Connect the reader to the computer (p. 5).
3. Program the reader in the CR SOFT program.
   3.1. Create a new *Standalone system* type project (p. 12) or open an existing project.
   3.2. Establish connection between the program and the device (p. 14).
   3.3. Program the cards settings (p. 16).
   3.4. Program the reader settings (p. 19).
   3.5. Add users (p. 23).
4. Disconnect the reader from the computer.
5. Run the cables to where you want to install the reader. Use unshielded straight-through cables.
6. Mount the reader and start it (p. 31).

8.2.2 Description of terminals for the standalone door control module

8



Terminal	Description
NC	relay output normally closed contact
C	relay output common contact
NO	relay output normally open contact

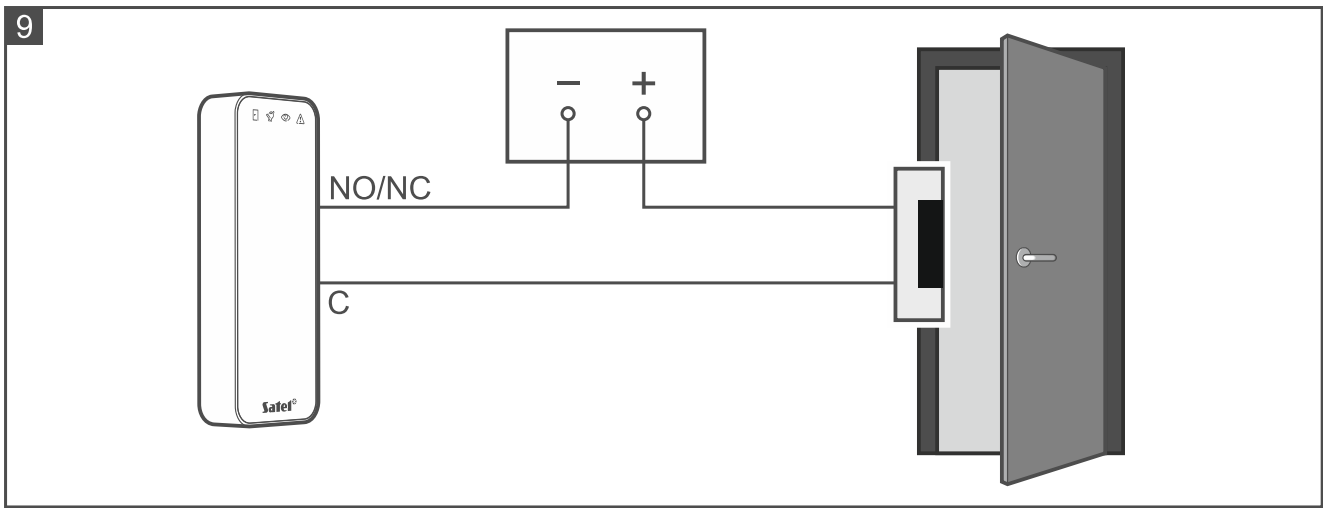
Terminal	Description
DATA/D1	*not used*
RSA	RS-485 bus terminal [OSDP]
RSB	RS-485 bus terminal [OSDP]
TMP	tamper output
+12V	+12 VDC power input
COM	common ground
CLK/D0	*not used*
IN1	door status input
IN2	request-to-exit input
IN3	*not used*
BELL	*not used*

8.2.3 Mounting the standalone door control module

1. Open the reader enclosure.
2. Place the enclosure base against the wall and mark the location of mounting holes.
3. Drill the holes in the wall for wall plugs (anchors).
4. Run wires through the opening in the enclosure base.
5. Use wall plugs and screws to secure the enclosure base to the wall. Select wall plugs specifically intended for the mounting surface (different for concrete or brick wall, different for plaster wall, etc.).
6. Connect the electric strike, electromagnetic lock or other door actuator to the relay output as shown in Fig. 9. Depending on the device type, use the following terminals:
   - NC: NC and C,
   - NO: NO and C.

It is not recommended that the door actuator be powered from the same source as the reader.

9



7. If the reader is to control the door status, connect the detector controlling the door status to the IN1 and COM terminals. If the reader is not to control the door status, program the IN1 input as *Not used* (CR SOFT program).

8. If the request-to-exit button is to be used, connect it to the IN2 and COM terminals. If the request-to-exit button is not to be used, program the IN2 input as *Not used* (CR SOFT program).
9. Connect the power to the +12V and COM terminals.
10. Close the reader enclosure.
11. Power on the reader.

8.3 Using the standalone door control module

The features are available on using the proximity card by the user. Managing users and adding proximity cards to the users can be done in the CR SOFT program (see: “Managing users” p. 23).

The reader distinguishes between presenting and holding the card (the card must be presented to the reader and held for 3 seconds).

8.3.1 Alarms

The reader indicates alarm in the following cases:

- forced entry (if the door status is controlled – see: “Reader settings” p. 21),
- 3 attempts to get access using an unknown card,
- module tamper (if the *Tamper* option is enabled – see: “Reader settings” p. 21).

After alarm is triggered, the LED is turned on and a continuous sound is emitted. The signaling goes on for 10 seconds. Then the alarm memory is signaled (the LED flashing). Using the card by any user clears the alarm / alarm memory.

8.3.2 LED indicators

LED	Color	Description
	blue	**ON** – door unblocked (permanently unlocked) **flashing** – door unlocked (user gained access)
	red	**ON** – alarm **flashing** – alarm memory
	green	*indicates no state*
	yellow	**flashing** – door blocked (permanently locked)

8.3.3 Sound signaling

The installer can disable the sound signaling.

1 short beep – door unlocked (access gained).

2 short beeps – door blocked / door unblocked / door restored to normal operation mode.

2 long beeps – access denied (card unknown / door blocked) / refusal to execute function.

Long beep lasting 10 seconds – alarm.

Intermittent sound – long open door.

8.3.4 Available functions

Unlocking the door

The door will unlock when you are granted access. When the door is unlocked, you will be able to open the door. Ask the installer how much time you have to open the door after you were granted access and how much time you have to close the door after you opened it.

1. Present the card to the reader.
2. When the LED starts flashing, open the door.

If the door status is controlled and the door is not closed within the specified time, the reader will start emitting an intermittent sound. The long open door signaling will continue until the door is closed.

Blocking the door

The door can be blocked if the door status is controlled.

1. Make sure that the door operates in the normal mode and that the door is closed.
2. Present the card to the reader and hold it. When the door is blocked, the LED will be turned on.

Unblocking the door

The door can be unblocked if the door status is controlled.

1. Present the card to the reader.
2. When the LED starts flashing, open the door.
3. Present the card to the reader and hold it. When the door is unblocked, the LED will be turned on.

Restoring the door to normal operation mode

If the LED (door blocked) or the LED (door unblocked) is turned on, present the card to the reader and hold it. The door will be restored to normal operation mode. The LED will be turned off.

9. Firmware update

1. Download the device firmware update program from the support.satel.pl website.
2. Start the downloaded program.
3. Click  .
4. In the window that will be displayed, indicate the COM port through which communication with the device is to take place, then click “OK”.
5. When the window with the list of devices detected by the program is displayed, select the device(s) whose firmware you want to update, then click “OK”.
6. The firmware of the device(s) will be updated.

10. Specifications

Supply voltage ..... 12 VDC ±15%

Standby current consumption .....63 mA

Maximum current consumption	112 mA
Reader transmit frequency	13.553...13.567 MHz
Read range of MC-DF3-2 encrypted card	up to 55 mm
Relay output (resistive load)	1 A / 30 VDC
Operating temperature range	-25°C...+55°C
Maximum humidity	93±3%
Dimensions	45 x 128 x 21 mm
Weight	87 g