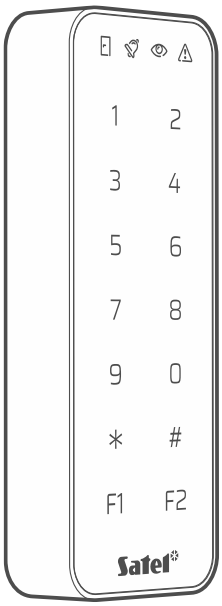
Keypad with MIFARE proximity card reader

SO-MF5

EN

Firmware version 1.01



CE

so-mf5_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-MF5 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

1. Features 4
2. Description 5
2.1 Function keys 5
2.2 PUSH IN terminals 5
2.3 Enclosure opening tool 6
3. Connecting the keypad to the computer 7
4. CR SOFT program 7
4.1 Starting out 7
4.1.1 Setting the administrator password 7
4.1.2 Changing the password 8
4.1.3 Changing the program language 9
4.2 Program window 10
4.2.1 Program window with the list of projects 10
List of projects 10
Tool bar for the list of projects 10
4.2.2 Program window after opening a project 11
Tabs 11
Title bar 12
4.2.3 Menu bar 12
4.2.4 Menu 13
4.2.5 Message window 13
Message window settings 14
4.3 Using the program 14
4.3.1 Creating a project 14
4.3.2 Importing a project 15
4.3.3 Deleting a project 16
4.3.4 Establishing connection with access control devices 16
4.3.5 Programming the interface settings 17
Interfaces settings 17
4.3.6 Programming the card settings 18
Token settings for the INTEGRA/ACCO on-line system 18
Token settings for other on-line system or standalone system 19
4.3.7 Programming the access control device settings 21
Description of the “DEVICES” tab 22
Adding a device to the project 22
Keypad settings 23
Changing the device’s OSDP address 25
Deleting a device from the project 26
4.3.8 Managing users 26
Description of the “USERS” tab 26
Adding a user to the project 26
User settings 26
Deleting a user from the project 29
4.3.9 Saving changes in the project 29
4.3.10 Exporting a project 29
5. The INT-SCR keypad in the INTEGRA system 30
5.1 Features 30
5.2 Installation in the INTEGRA system 30

5.2.1 Installation in short 31
5.2.2 Description of terminals for keypad in the INTEGRA system 31
5.2.3 Mounting the keypad in the INTEGRA system 32
5.2.4 Programming the keypad in the INTEGRA system 33
Programming in the DLOADX program 33
Programming in the LCD keypad 33
Keypad settings 33
5.3 Using the INT-SCR keypad 37
5.3.1 LED indicators 37
5.3.2 Sound signaling 38
Beeps generated when operating 38
Event signaling 38
5.3.3 Available functions 38
[Code] ✳ / presenting the card 38
[Code] # / holding the card 39
Quick arming 39
Generating the alarm from the keypad 40
Silencing the alarm sound at the keypad 40
Code changing 40
Impact of the EN 50131 standard on keypad use 40
6. The ACCO-SCR keypad in the ACCO system 40
6.1 Features 40
6.2 Installation in the ACCO system 40
6.2.1 Installation in short 41
Connecting using the ACCO-SCR interface 41
Connecting using the RS-485 bus (OSDP) 41
6.2.2 Description of terminals for keypad in the ACCO system 42
6.2.3 Mounting the keypad in the ACCO system 42
Connecting using the ACCO-SCR interface 43
Connecting using the RS-485 bus (OSDP) 43
6.2.4 Programming the keypad in the ACCO system 43
6.3 Using the ACCO-SCR keypad 44
6.3.1 LED indicators 44
7. The keypad in other manufacturer's system 44
7.1 Installation in other manufacturer's system 44
7.1.1 Installation in short 44
7.1.2 Description of terminals for keypad in other manufacturer's system 45
7.1.3 Mounting the keypad in other manufacturer's system 45
8. Standalone door control module 46
8.1 Features 46
8.2 Installation of the standalone door control module 46
8.2.1 Installation in short 46
8.2.2 Description of terminals for the standalone door control module 47
8.2.3 Mounting the standalone door control module 47
8.3 Using the standalone door control module 48
8.3.1 Alarms 48
8.3.2 LED indicators 49
8.3.3 Sound signaling 49
8.3.4 Available functions 49
Unlocking the door 49

Blocking the door 49
Unblocking the door 49
Restoring the door to normal operation mode 50
Changing the code 50
9. Firmware update 50
10. Specifications 50

The SO-MF5 keypad can operate as:

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

Before you install the keypad, program the settings required for the selected operating mode in the CR SOFT program. The exception is a keypad 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

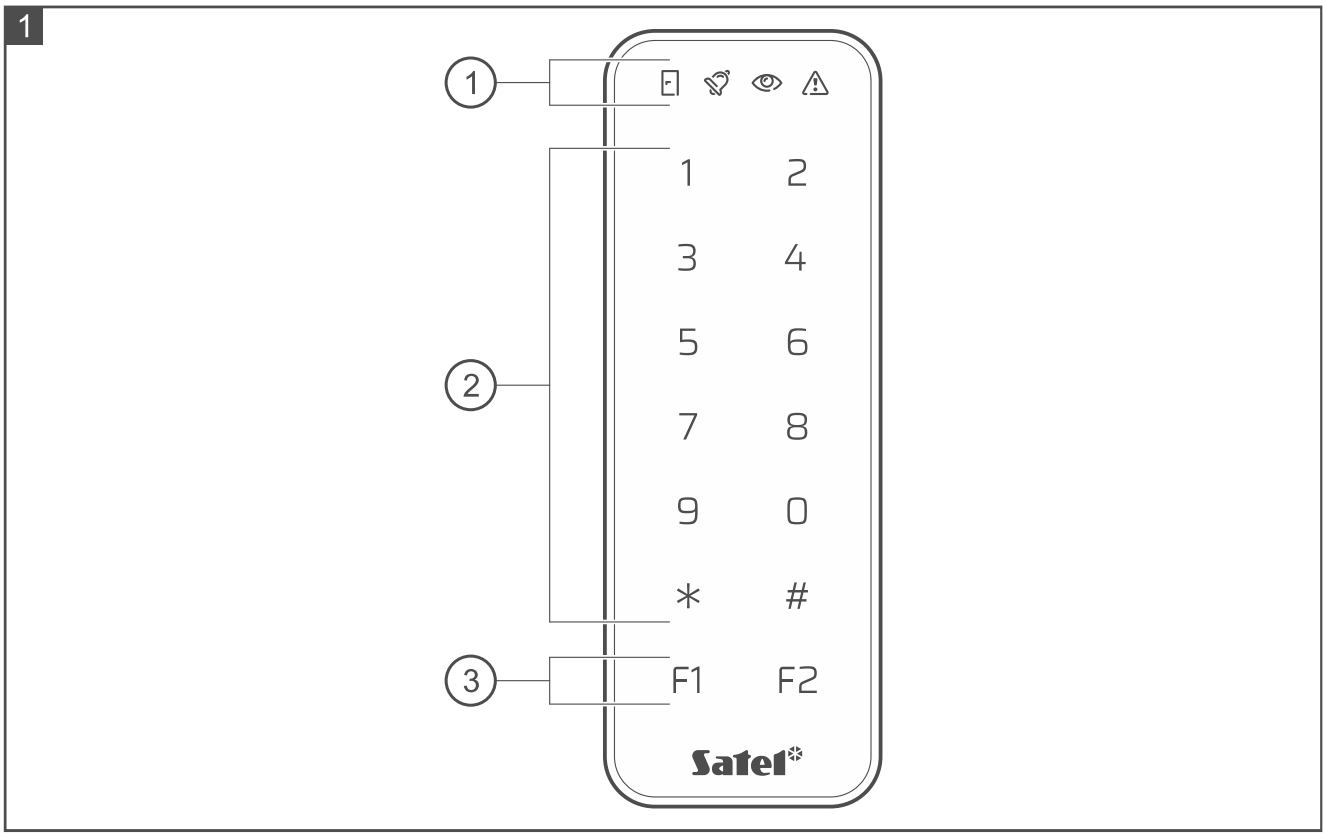
- User identification by code and/or MIFARE® proximity card.
- Touch keypad with backlight:
  - 12 keys for entering the code,
  - 2 function keys (when touched, the information is sent using the OSDP protocol).
- Built-in 13.56 MHz MIFARE proximity card reader:
  - Ultralight,
  - Classic,
  - DESFire (EV1 / EV2 / EV3).
- Supported OSDP protocol (RS-485 bus).
- Additional communication interface:
  - INT-SCR (in the INTEGRA system),
  - ACCO-SCR (in the ACCO system),
  - Wiegand (in other manufacturer's system).
- Programming in the CR SOFT program.
- LED indicators.
- OC type output (BELL) controlled by the F1 function key.
- Relay output for controlling an electric strike, electromagnetic lock or other door actuator (in the INT-SCR keypad mode or standalone door control module mode).
- Door status input (in the INT-SCR keypad mode or standalone door control module mode).
- Request-to-exit input (in the INT-SCR keypad mode or standalone door control module mode).
- Built-in sounder.
- Tamper protection against enclosure opening and removal from the wall.

The keypad supports version 2.2 of the OSDP protocol.

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

2. Description

1



(1) LED indicators.

(2) keys for entering the code.

(3) function keys.

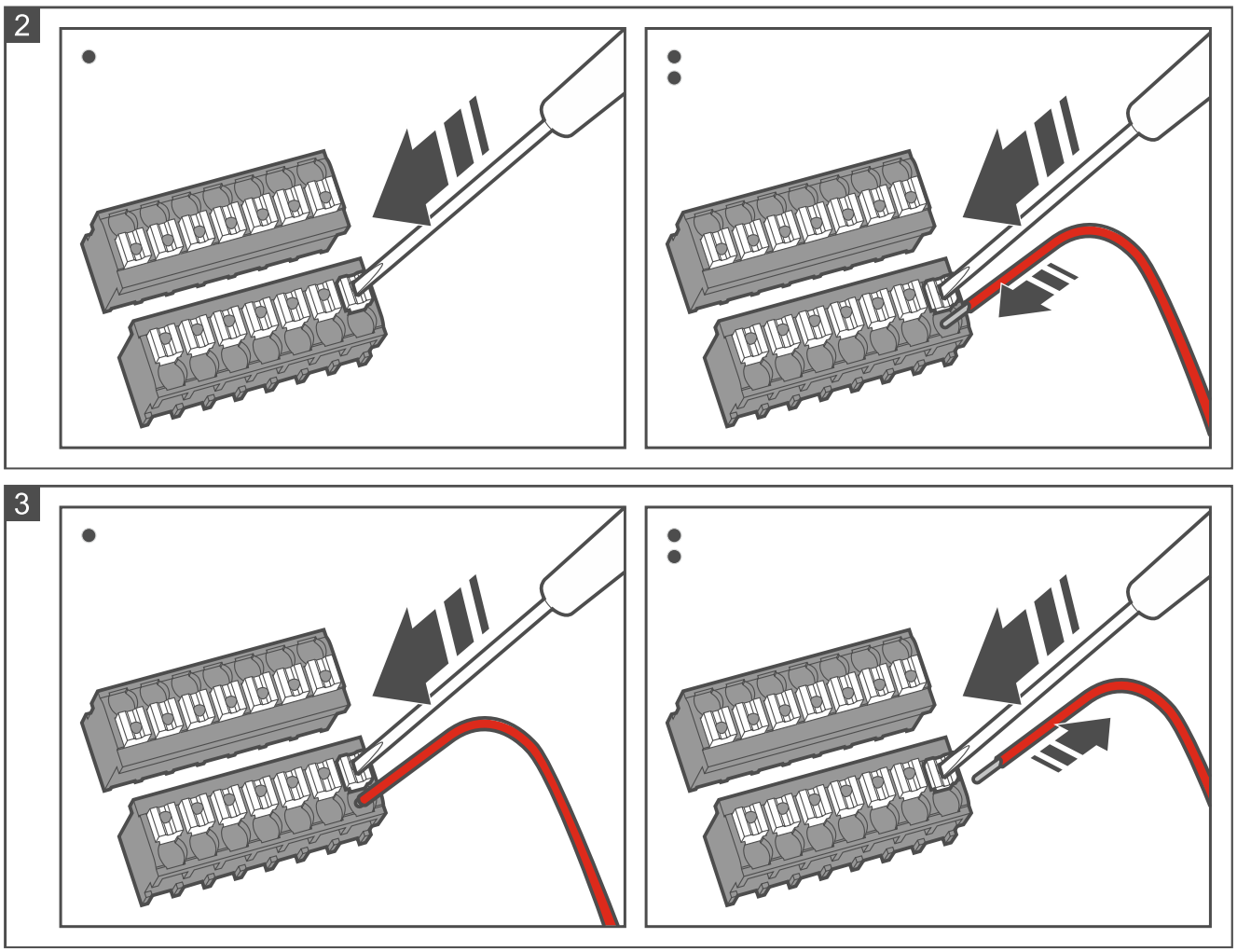
2.1 Function keys

The F1 function key is used to directly control the keypad's BELL output. The BELL output is a low-current OC type output. When you touch the key, the output is shorted to common ground.

When you touch the F1 or the F2 key, the information about it is sent using the OSDP protocol.

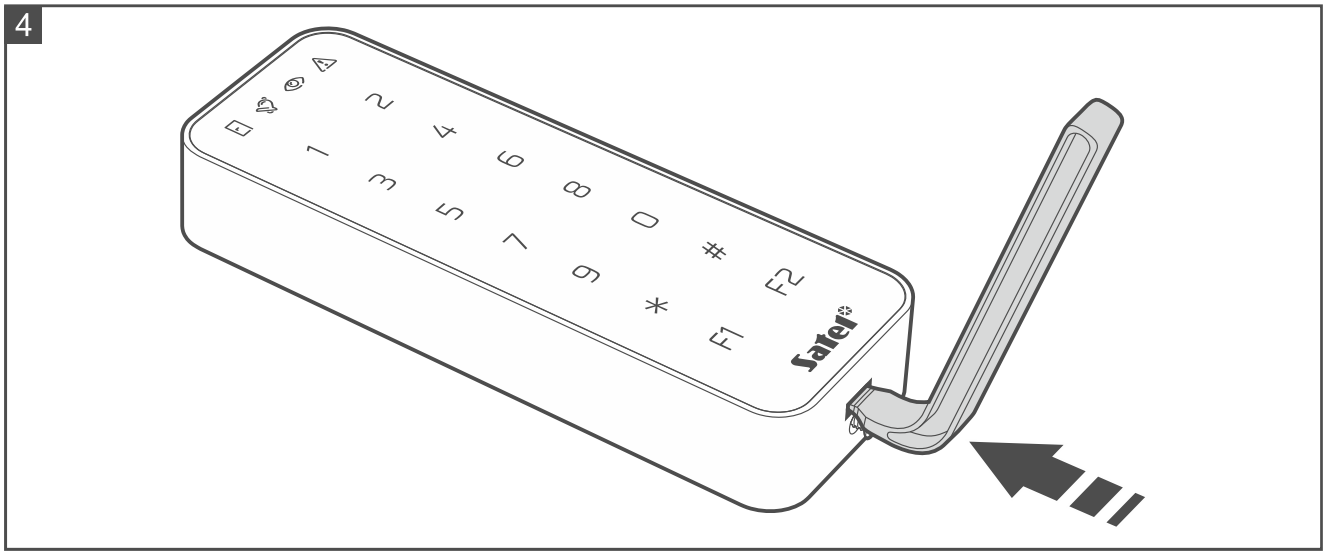
2.2 PUSH IN terminals

The terminals used in the keypad are PUSH IN type. Figure 2 shows how to connect a wire to the terminal. Figure 3 shows how to disconnect the wire. You can use a wire with a cross-section up to 1.5 mm^2.



2.3 Enclosure opening tool

A tool for opening the enclosure is delivered with the keypad. Figure 4 shows how to open the enclosure using the tool. The screw must be loose.



3. Connecting the keypad to the computer

If you are planning to install the keypad 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 keypad, program its settings. Connecting the keypad to the computer is required. To connect the keypad 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 keypad 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).

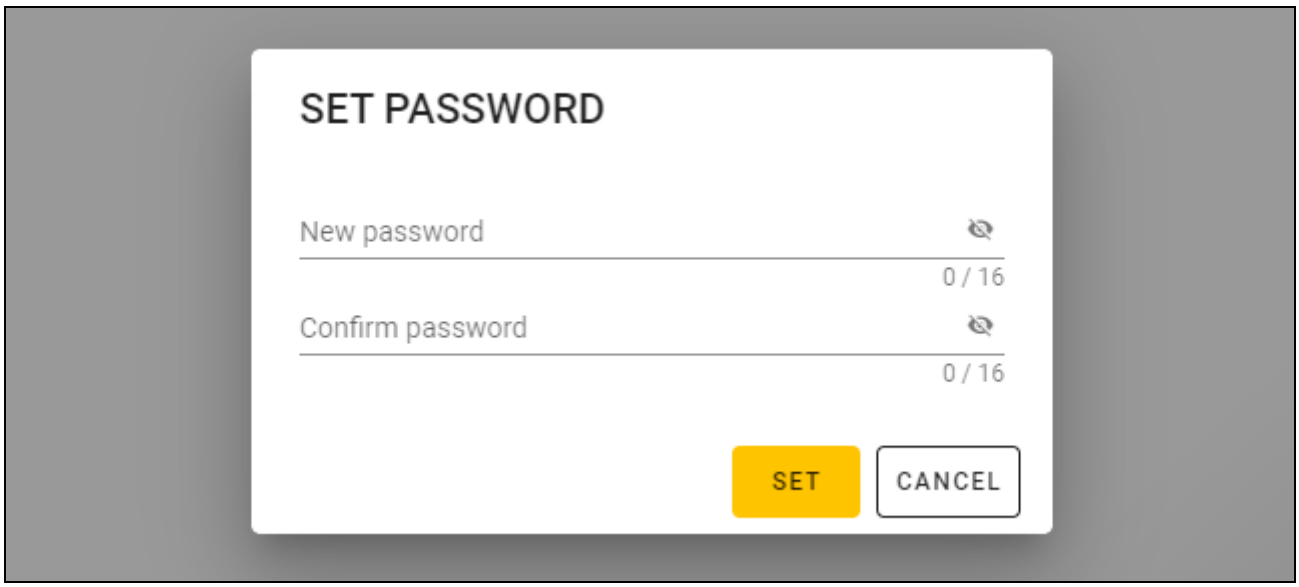
The screenshots in this manual show sample settings.

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.

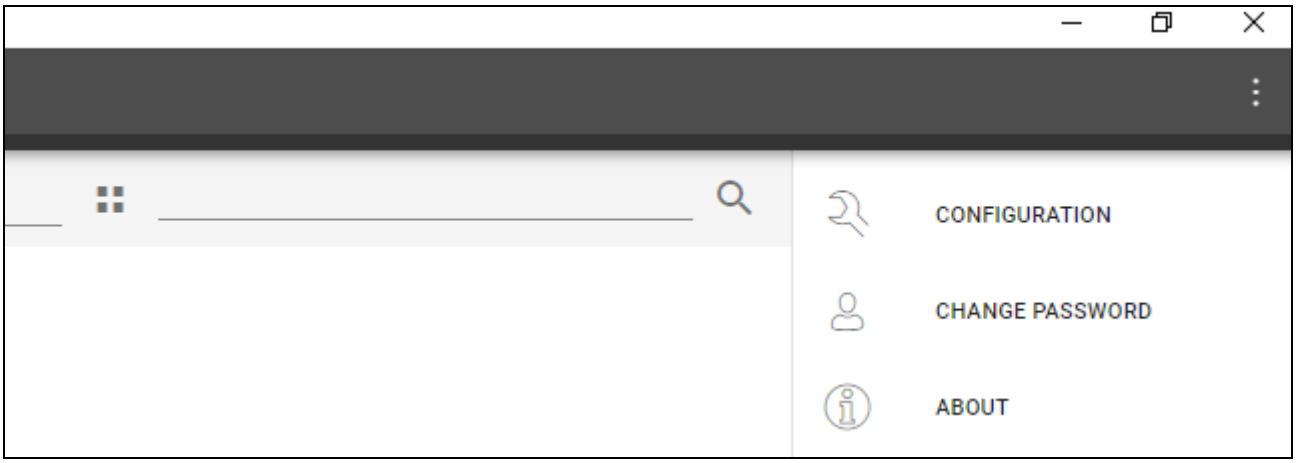


1. In the “New password” field, enter a password (1-16 digits, letters or special characters).
2. In the “Confirm password” field, enter the same password.
3. Click “Set”. The “SET PASSWORD” window will be closed. A message will confirm that the password has been set. You will access the program window (see: “Program window with the list of projects” p. 10).

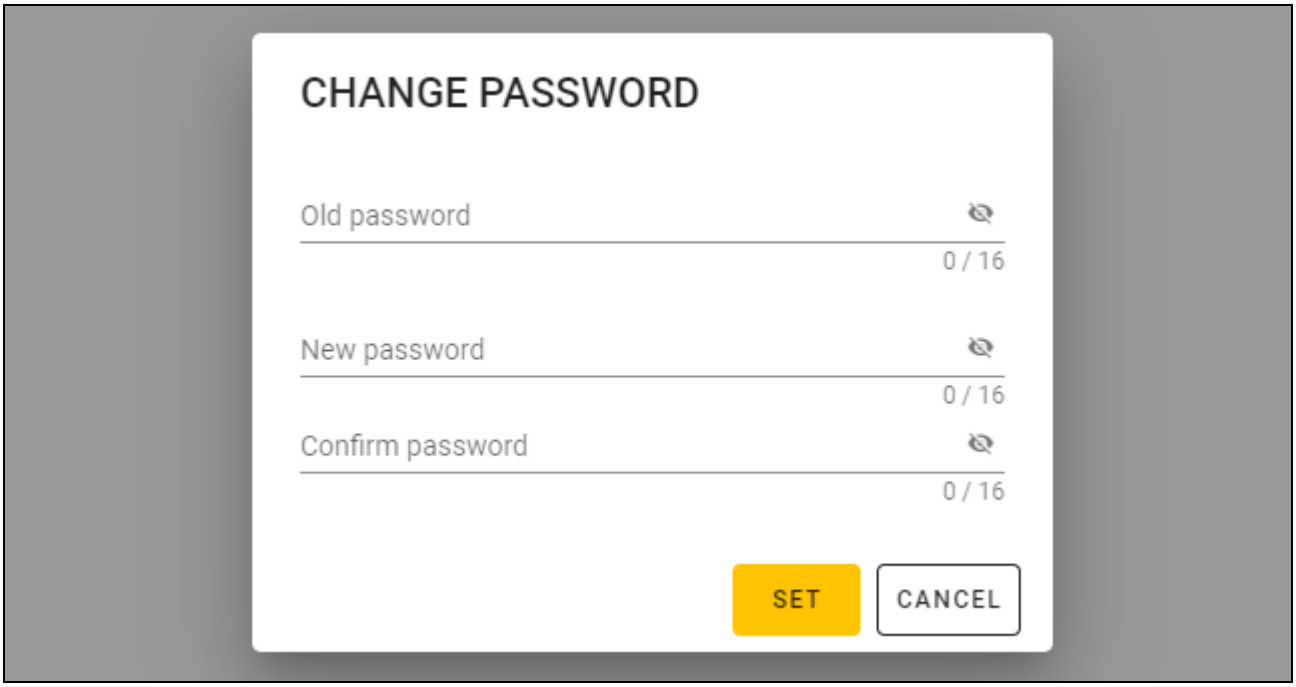
Next time you start the program, you will have to log in to access the program window.

4.1.2 Changing the password

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



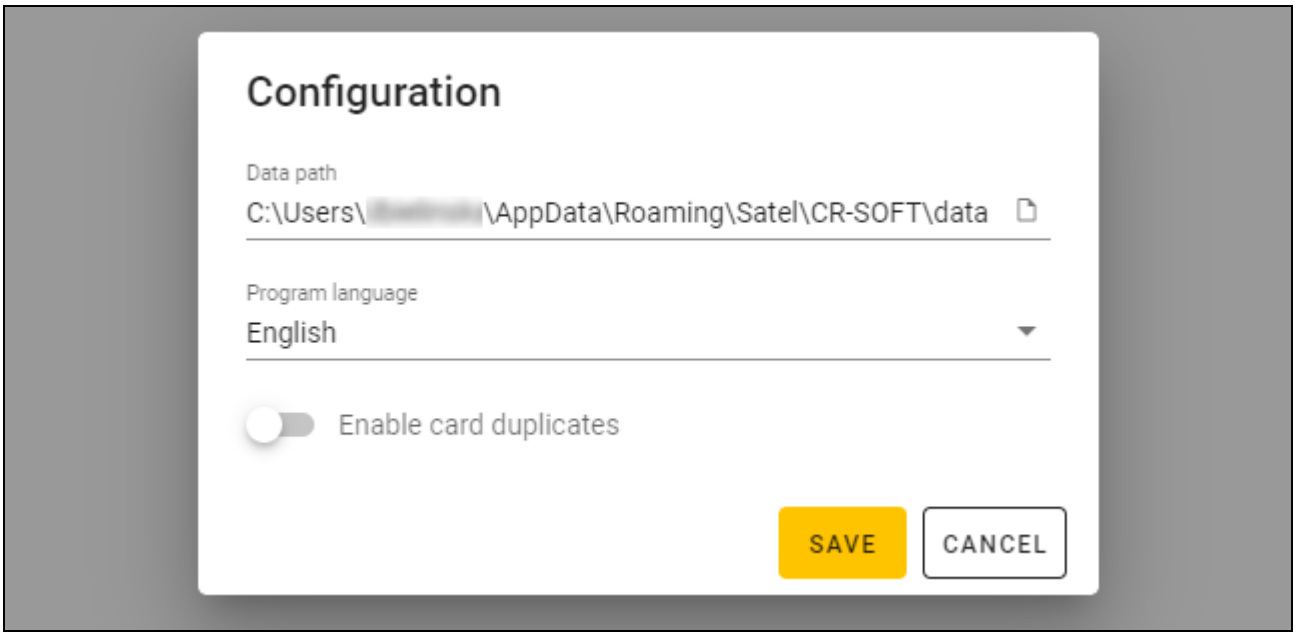
2. Click “CHANGE PASSWORD”. The “CHANGE PASSWORD” window will be displayed.



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.



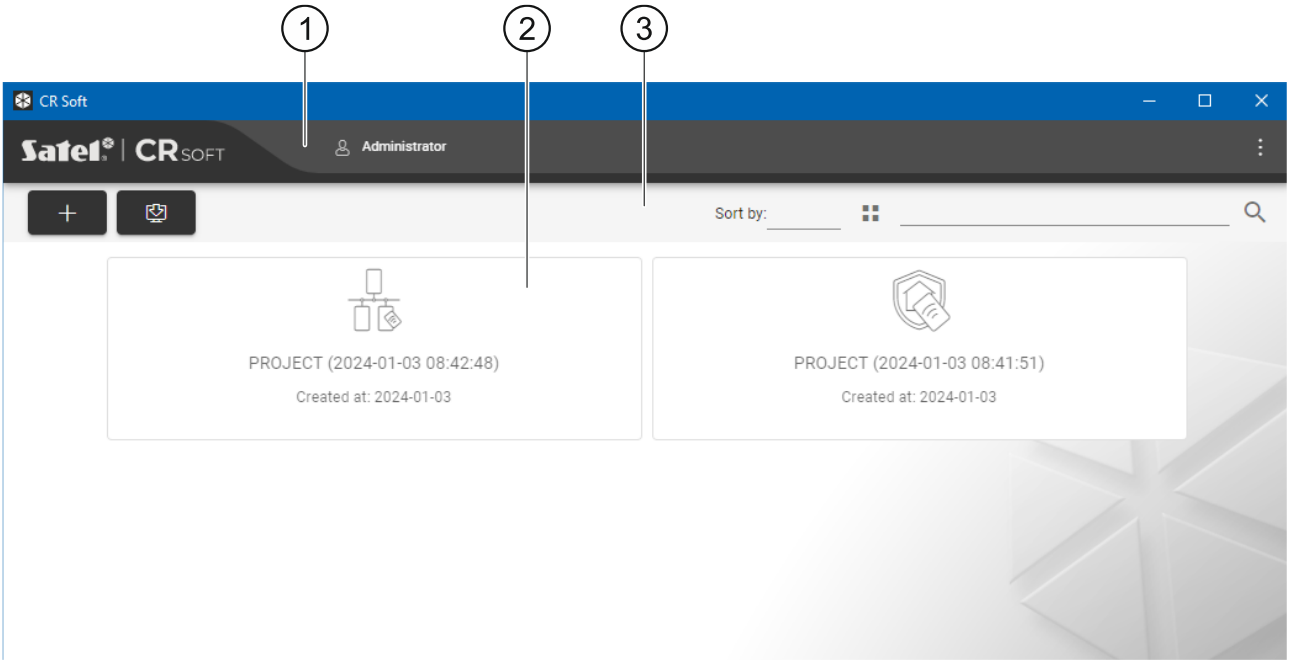
3. Click the “Program language” field. The list of languages will be displayed.
4. Click the language to be used.

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. 12).

(2) list of projects.

(3) tool bar for the list of projects.

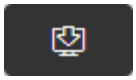
List of projects

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. 14).

 - click to import a project (see: “Importing a project” p. 15).

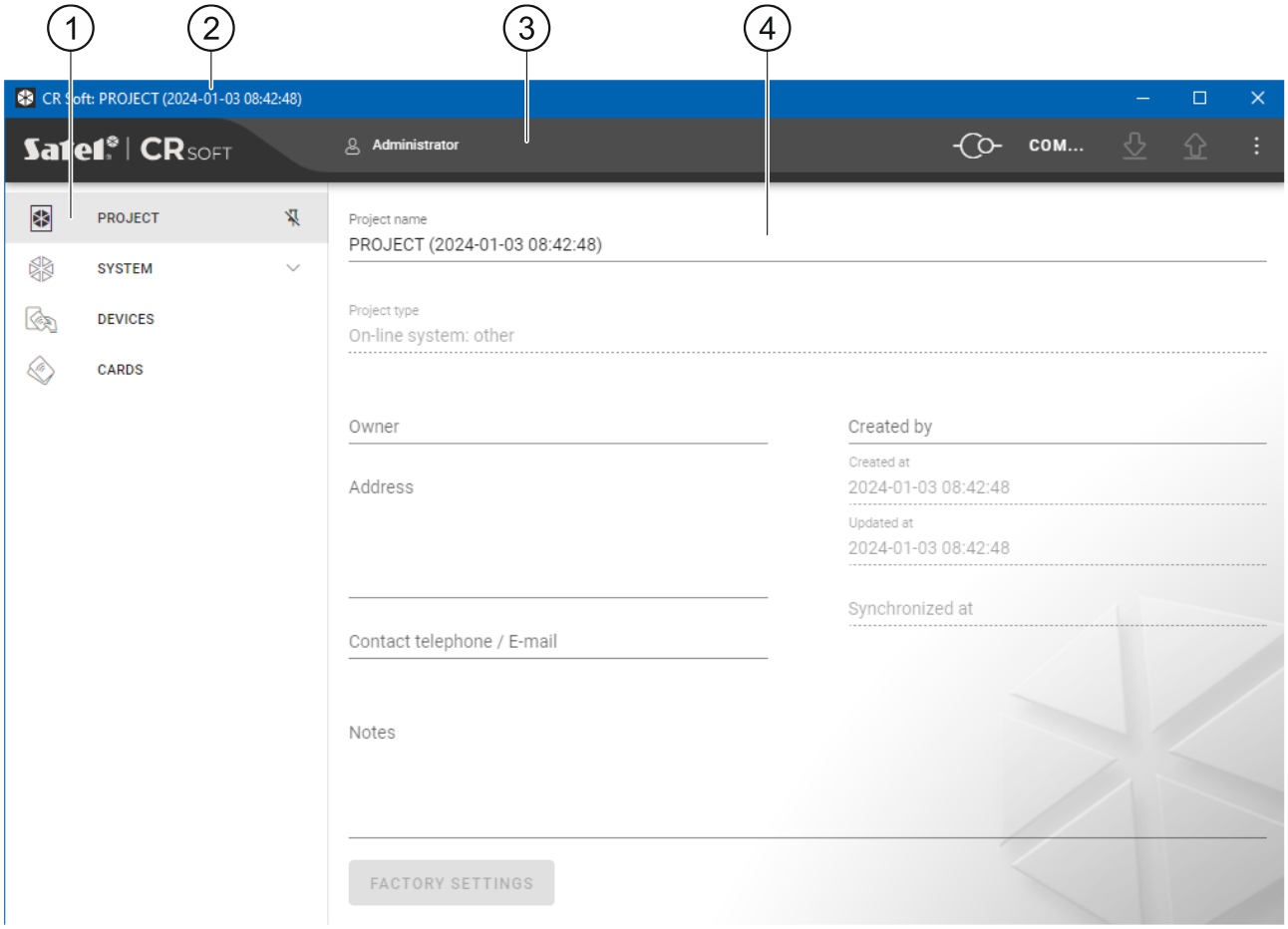
Sort by – you can select how the projects are sorted on the list (by name or creation date).

 - 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. 12).

(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.

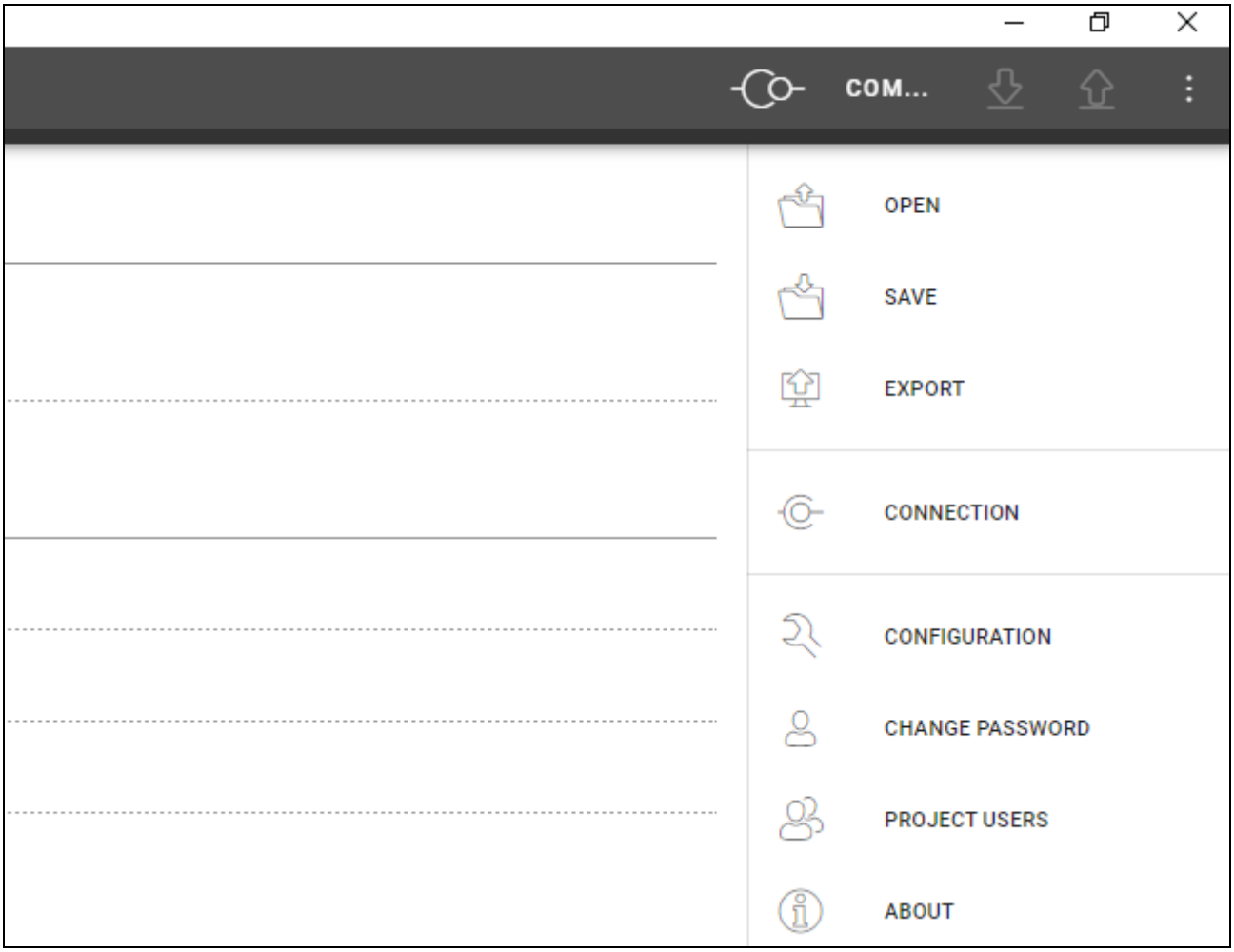
- click to select the COM port for communication with the access control devices / programmer. When the COM port is selected, the port number will be displayed instead of the three dots. You can also select the COM port in the "Connection" window. This button is displayed when a project is open.

 - 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. 29).

EXPORT – click to export the project (see: “Exporting a project” p. 29).

CONNECTION – click to open the “Connection” window.

CONFIGURATION – click to open the “Configuration” window.

CHANGE PASSWORD – click to change the password (see: “Changing the password” p. 8).

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”.

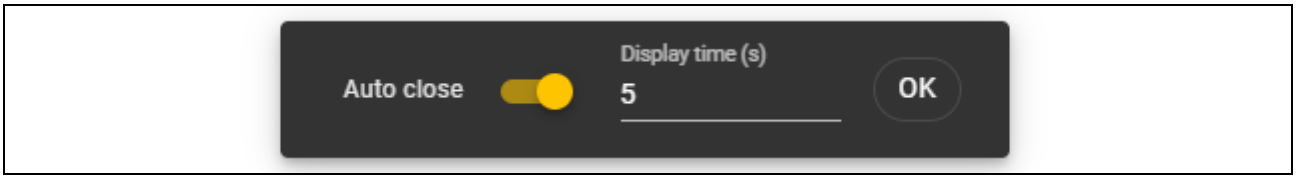
4.2.5 Message window

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.

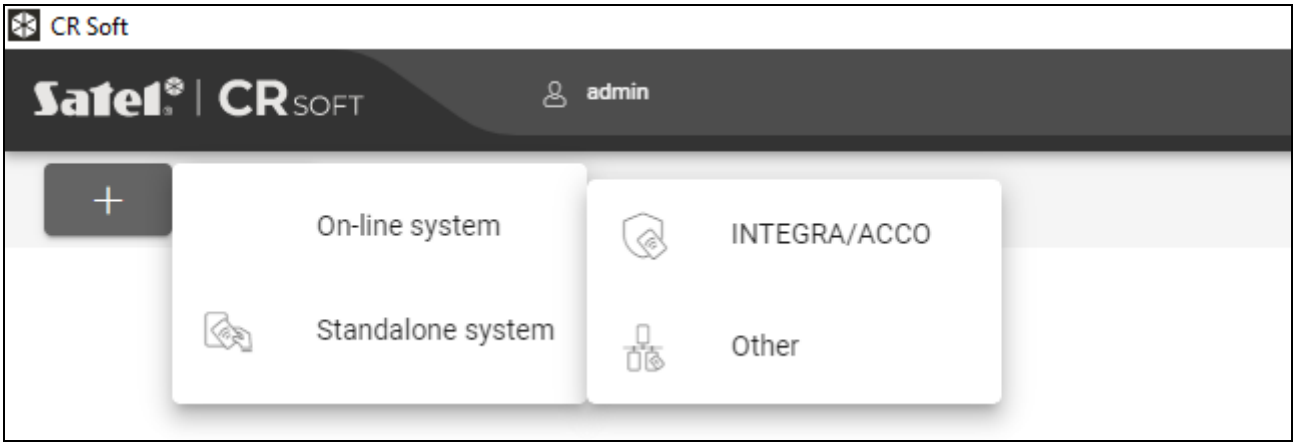
1. Click  . The menu of available project types will be displayed:

   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:

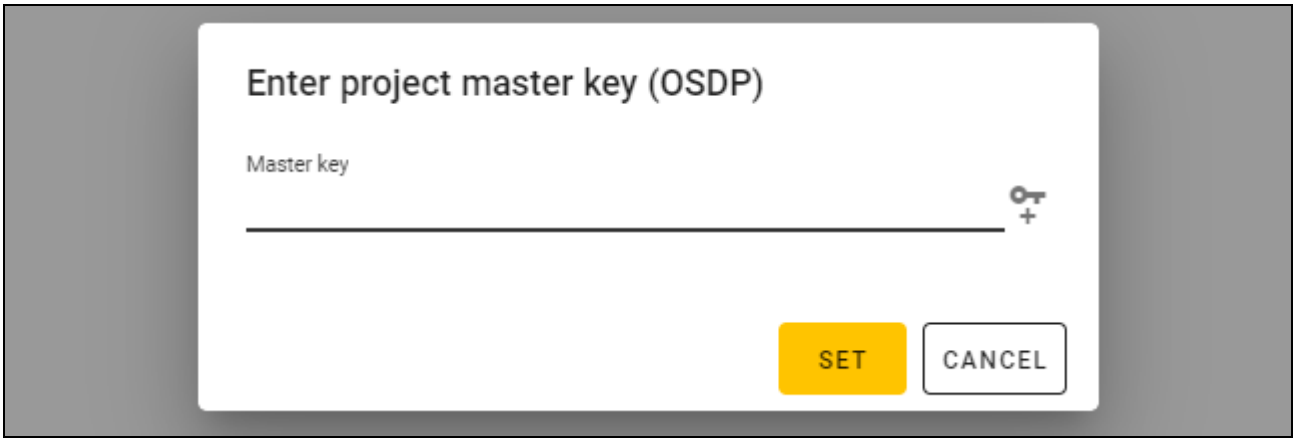
   INTEGRA/ACCO – access control devices and cards will be used in one of the SATEL systems: INTEGRA alarm system or ACCO access control system.

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

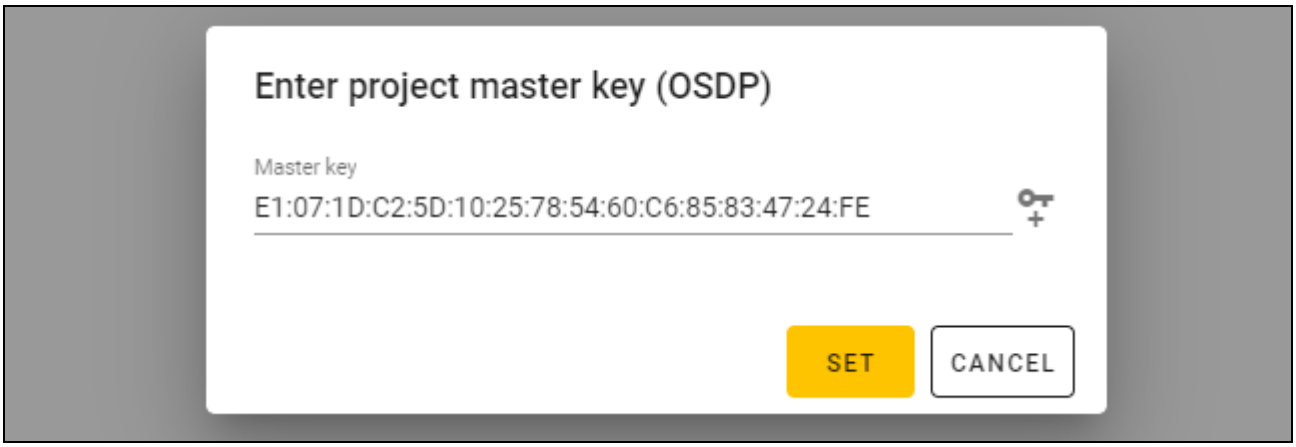
   Standalone system – system in which the access control device decides on its own whether to grant access to a single door or not (it operates as a standalone door control module).



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.

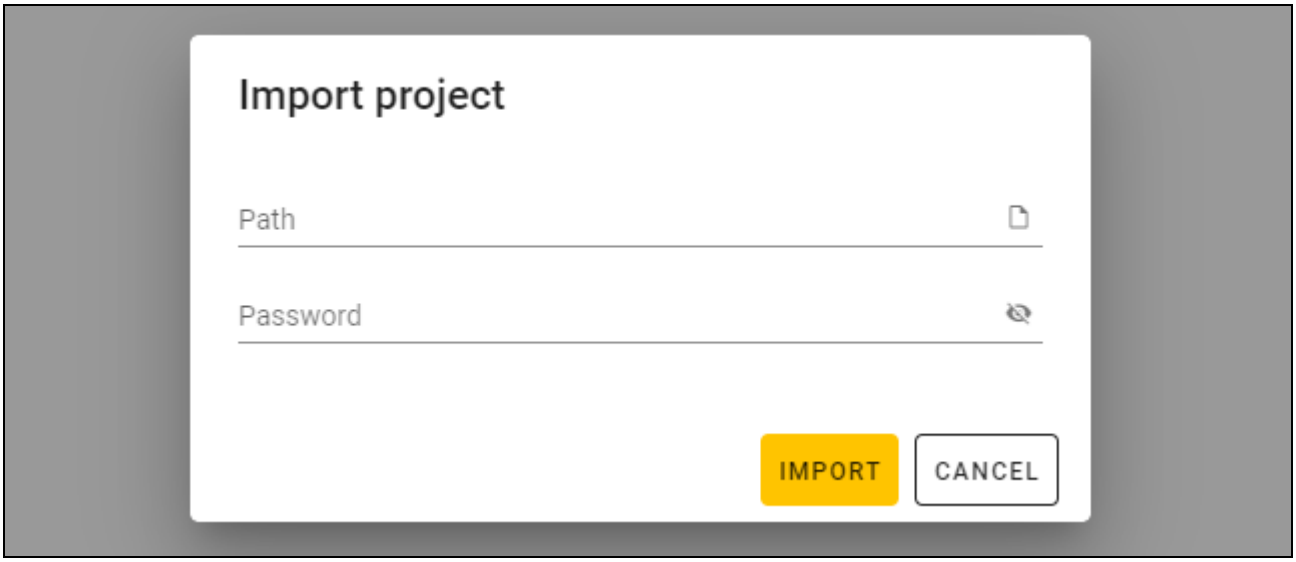


4. Click “SET”. The “Enter project master key (OSDP)” window will be closed. The “PROJECT” tab for the newly created project will be displayed.

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

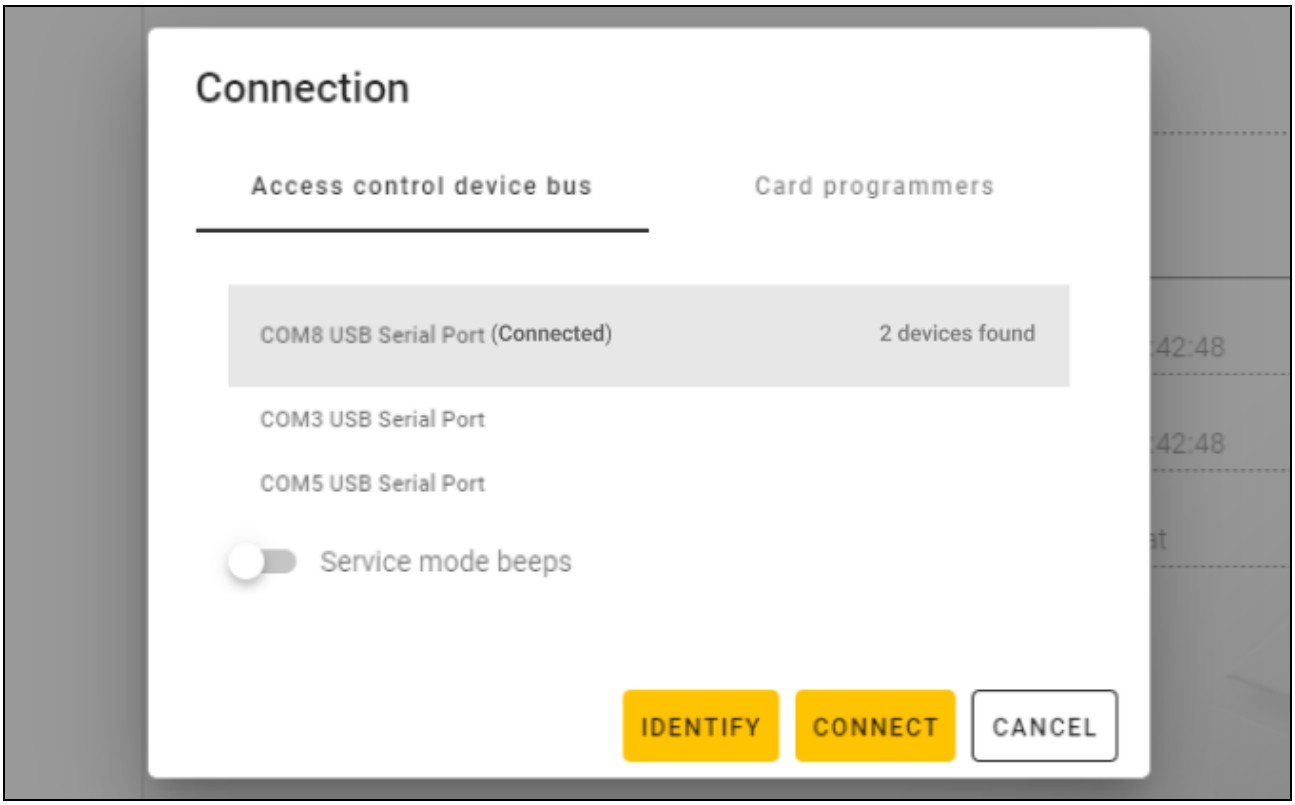
This function is available when the list of projects is displayed.

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 OSDP addresses to the devices.

The OSDP address of devices with factory settings is 0.

The identification function assigns OSDP addresses only to devices with the address 0. If several devices have the same OSDP 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 several devices have the same OSDP address, it is impossible to establish connection with the devices.

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

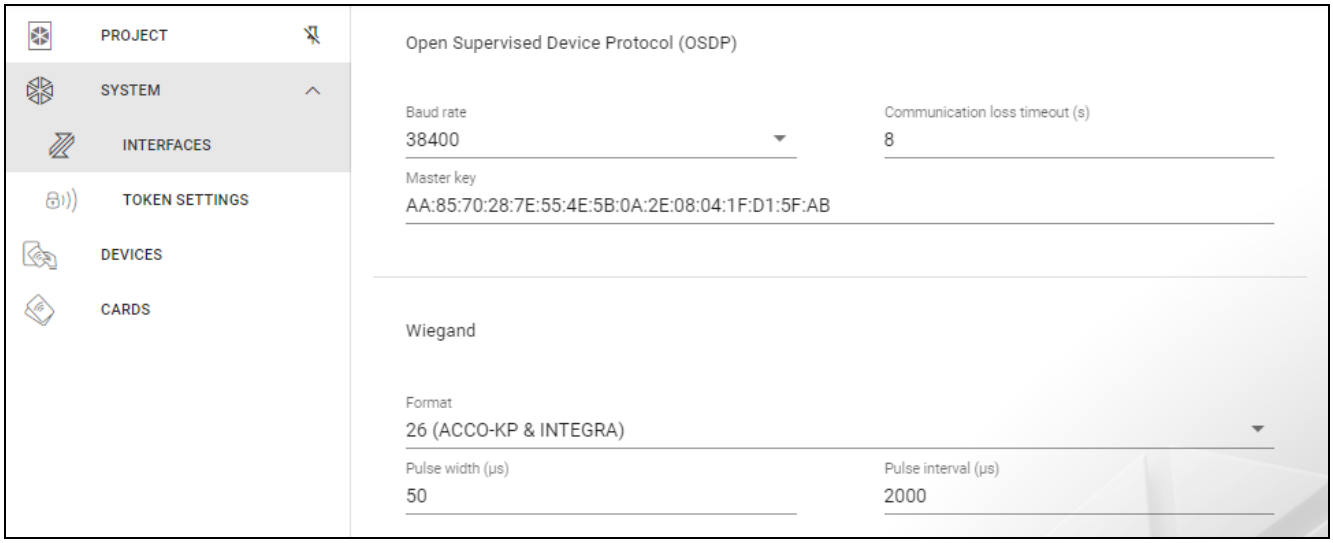
5. Click “CONNECT”. The program will connect with the devices. If the devices are new to the project, they will be added to the project (“DEVICES” tab).

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. Default rate: 38400.

Communication loss timeout (s) – time after which the device’s LEDs start to indicate a loss of communication. By default: 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 can be used by the keypad for communication in systems of other manufacturers. 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 default: 50 µs.

Pulse interval (µs) – duration of a gap between two pulses. By default: 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 – even parity bit + 33 data bits + odd parity bit; 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 – even parity bit + 35 data bits + odd parity bit; 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.

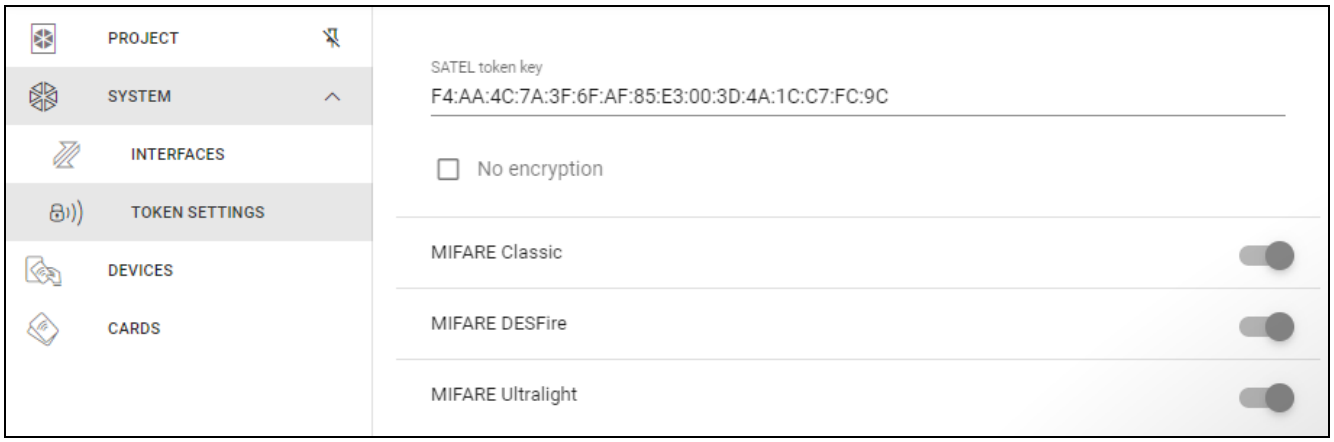
Custom – you can program your own transmission format settings.

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.

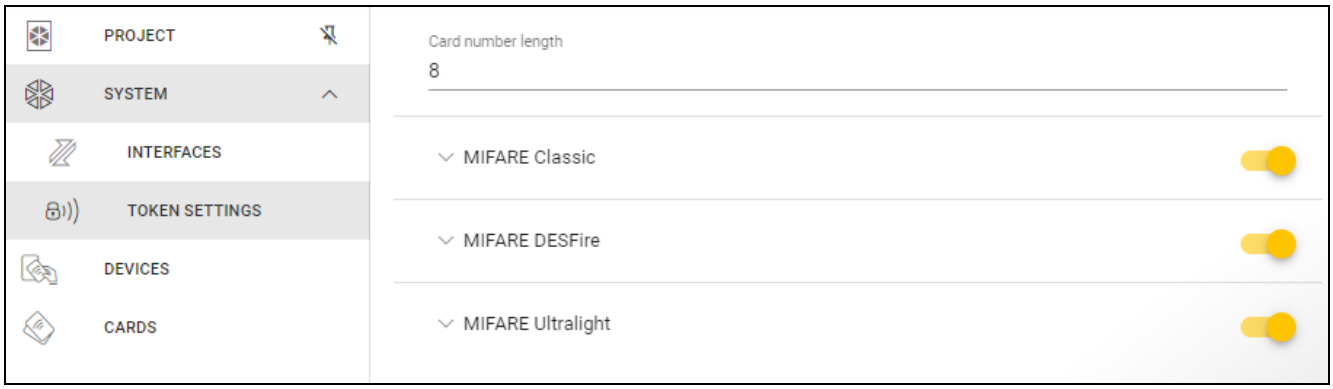
The card number length in the INTEGRA/ACCO system is 5 bytes.

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.

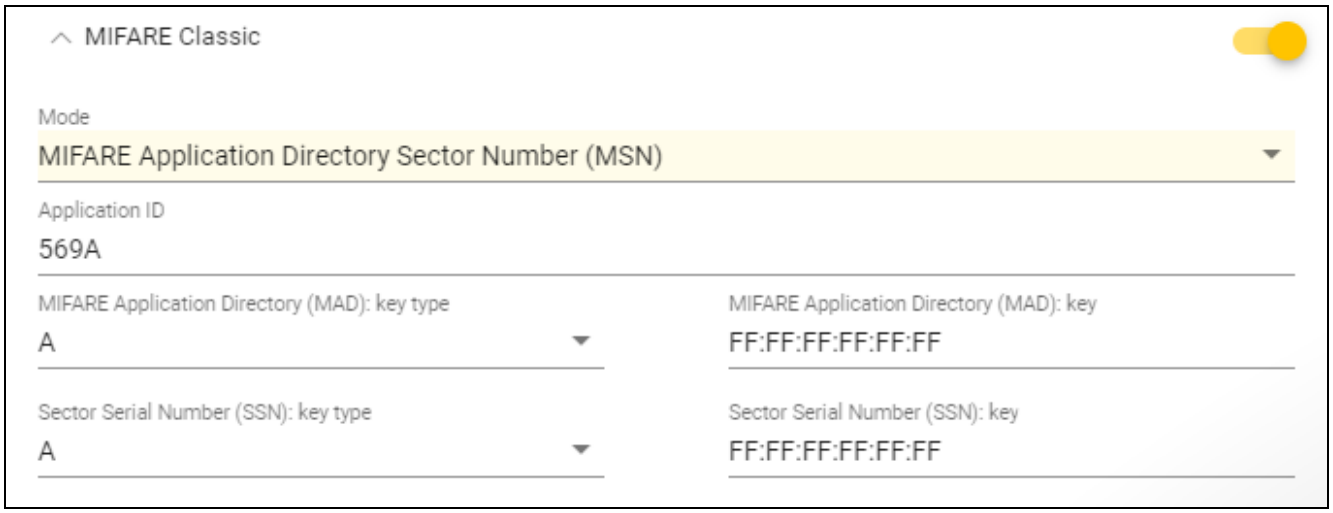
Token settings for other on-line system or standalone system



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.

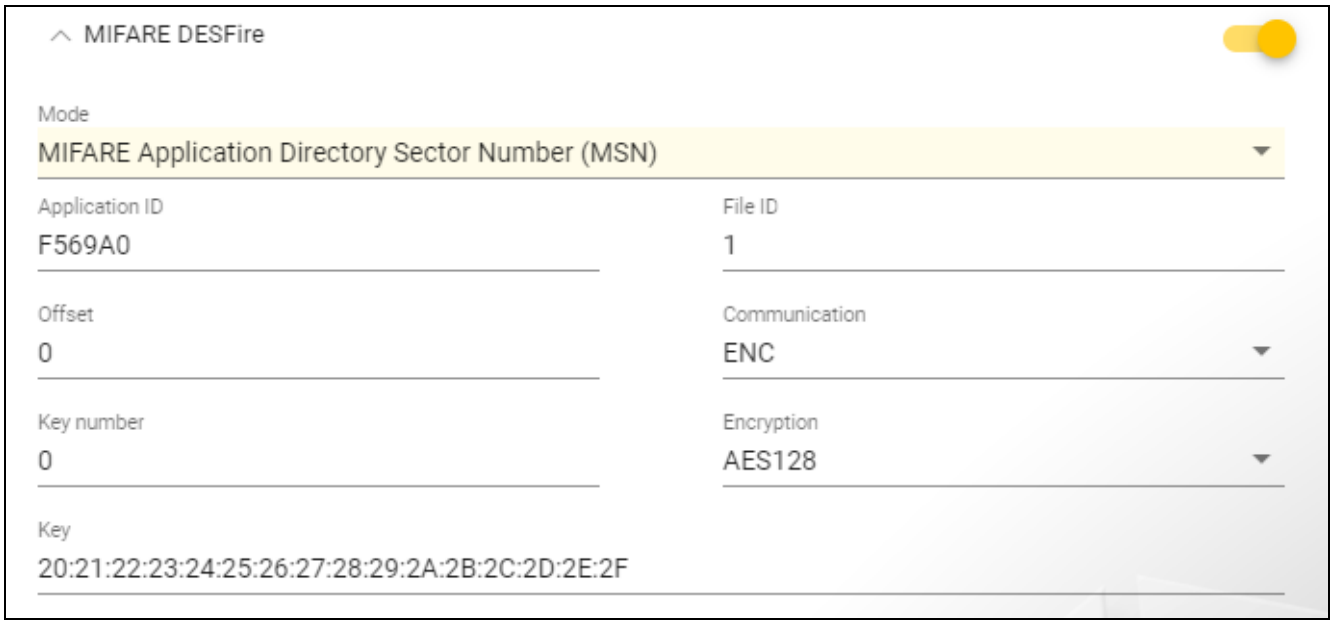
The key should be unique for each project.

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 signed.

ENC – communication is encrypted.

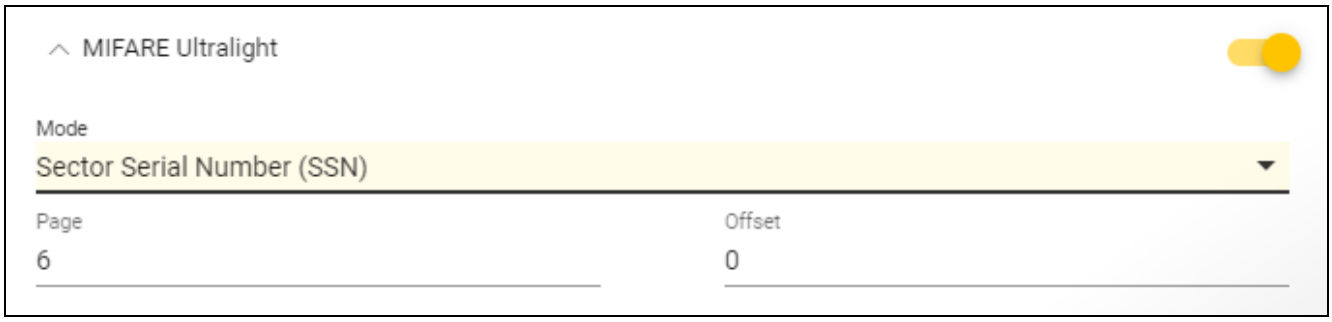
Key number – number of the key used to encrypt the card number file. This parameter applies to digitally signed communication (MAC) and encrypted communication (ENC).

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.

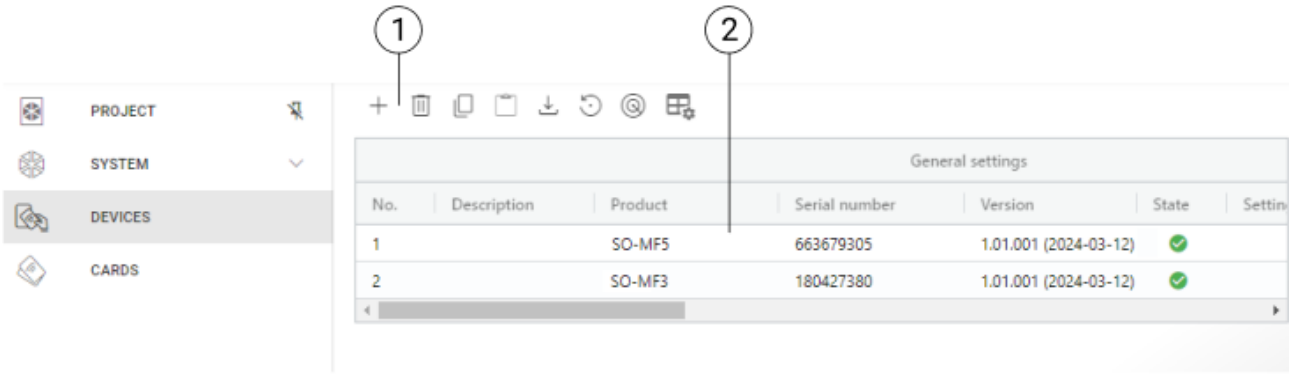
Offset – card number's first byte position on the page. You can enter a number from 0 to 3.

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.

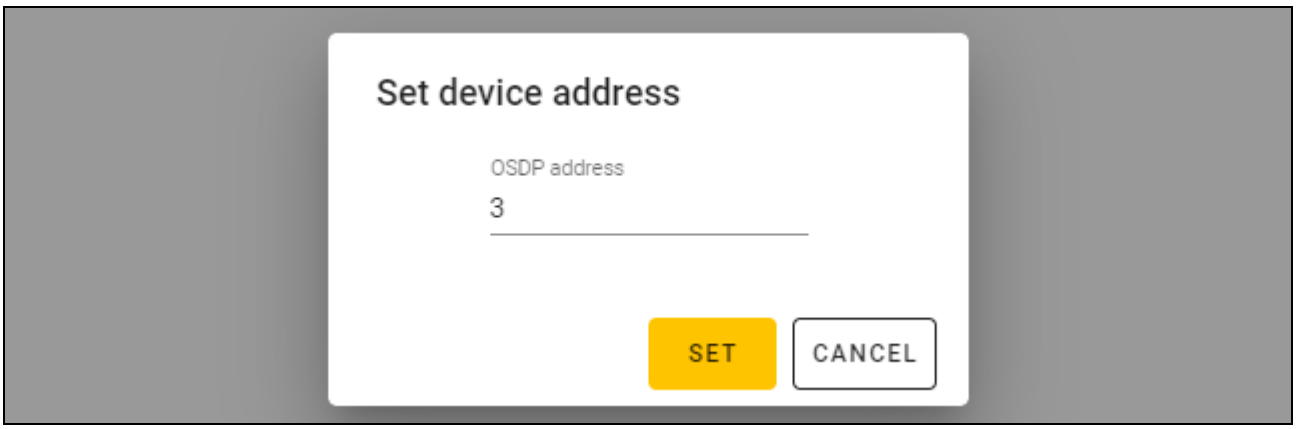
Adding a device to the project

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. 16).

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.

Keypad 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. 16). You can set a different address in the range from 1 to 126 (see: “Changing the device’s OSDP address” p. 25).

Additional interface

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

Type – type of additional interface used by the keypad:

Not used – additional interface is not used.

Wiegand – interface used in systems of other manufacturers.

INT-SCR – interface used in the INTEGRA system.

ACCO-SCR – interface used in the ACCO system.

Address (SATEL bus) – keypad address for the purpose of the SATEL bus:

INTEGRA system – set a unique address in the range from 0 to 31.

ACCO system – set the address 0 (terminal A – entry) or 1 (terminal B – exit).

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 turned on 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).

i *For the* Shorten the door unlock time *function to work, the door status 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

Keypad backlight – keys backlight operating mode (this parameter is not available for an *On-line system: INTEGRA/ACCO* type project:

Always off – keys backlight is turned off.

Auto – keys backlight is turned on for 40 seconds after any key is touched or a card is presented.

Always on – keys backlight is turned on.

Keys sounds – if this option is enabled, touching the keys is confirmed by a sound.

Beep volume – volume of sounds emitted by the keypad.

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", 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.

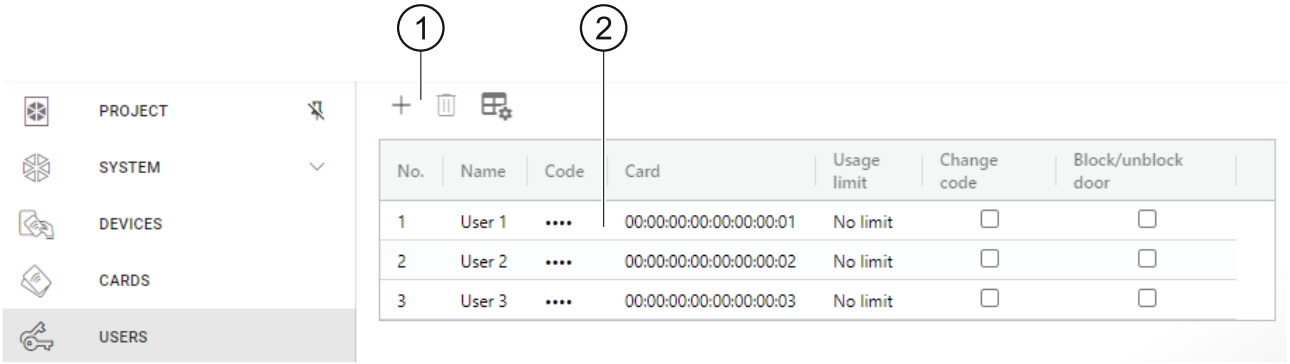
Deleting a device from the project

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 code (see: “Add a code to the user”) or a card (see: “Adding a card to the user”) 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 – if the user has no code, the button is displayed in the field – click to add a code to the user (see: “Add a code to the user”). If the user has a code, dots are displayed in the

field – click to change the user's code (see: "Changing the user's code") or delete the code ("Deleting the user's code").

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").

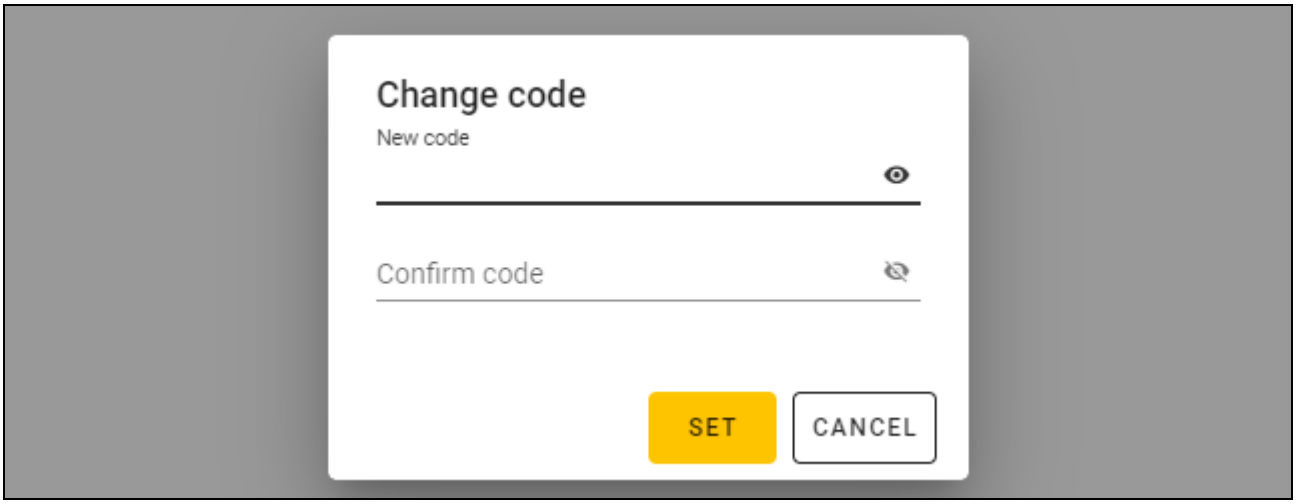
Usage limit – number of times the code or the card can be used until the user loses access to the device.

Change code – if this option is enabled, the user can change the code.

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

Add a code to the user

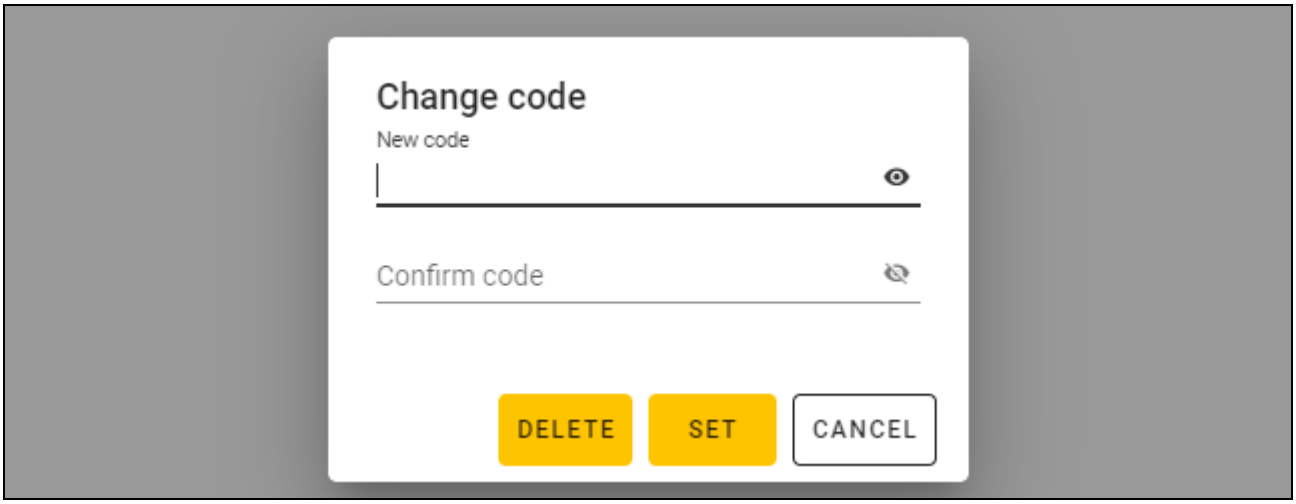
1. Click ⊞ in the "Code" column. The "Change code" window will be displayed.



2. In the "New code" field, enter a code (from 4 to 12 digits).
3. In the "Confirm code" field, enter the same code.
4. Click "SET". The "Change code" window will be closed. Dots will be displayed in the "Code" column.

Changing the user's code

1. Click the user's code (shown as dots). The "Change code" window will be displayed.



2. In the “New code” field, enter a new code (from 4 to 12 digits).
3. In the “Confirm code” field, enter the same code.
4. Click “SET”. The “Change code” window will be closed.

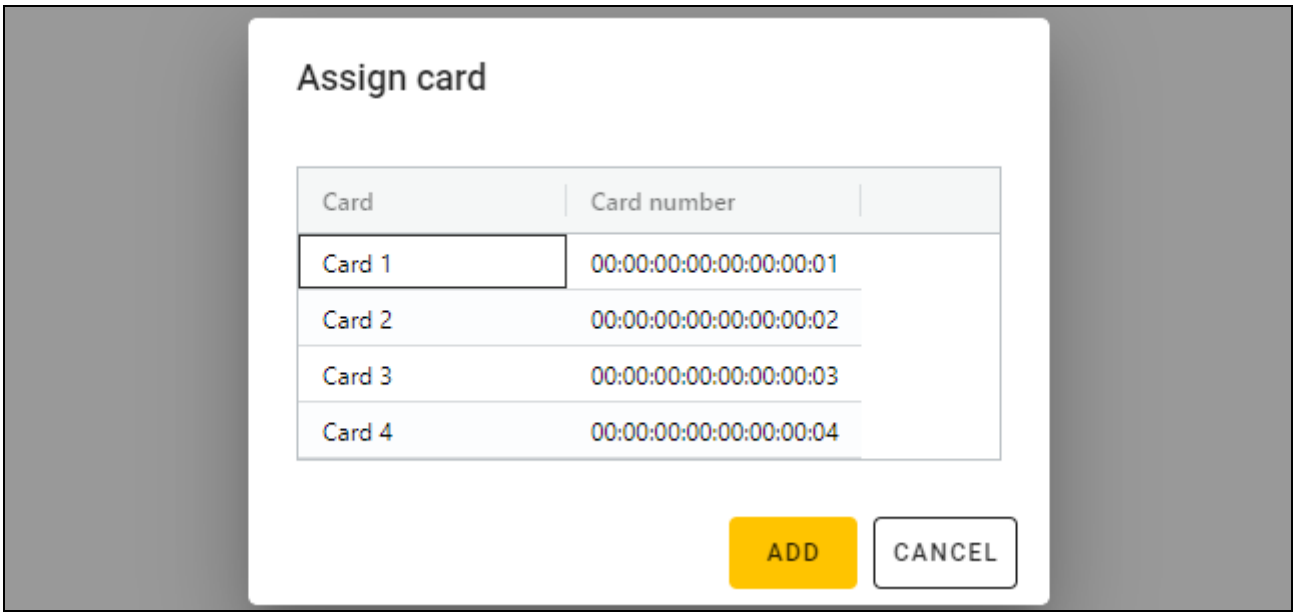
Deleting the user’s code

1. Click the user’s code (shown as dots). The “Change code” window will be displayed.
2. Click „DELETE”. The “Change code” window will be closed. In the “Code” column, the ⊞ button will be displayed.

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.

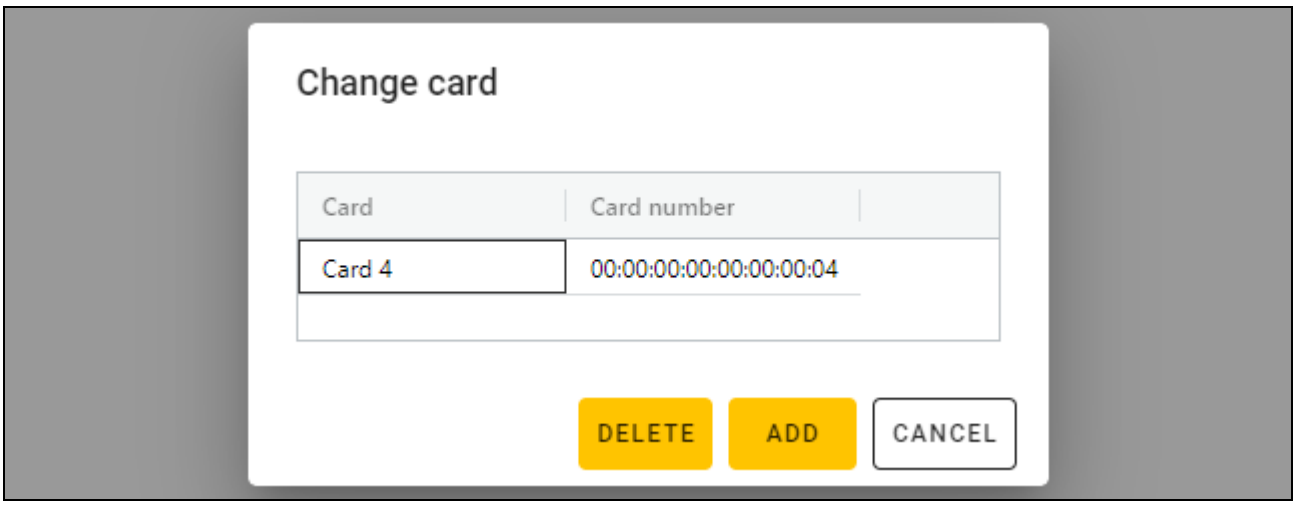


2. Click the card that you want to add to the user.
3. Click “ADD”. The “Assign card” window will be closed. In the “Card” column, the card number will be displayed.

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.

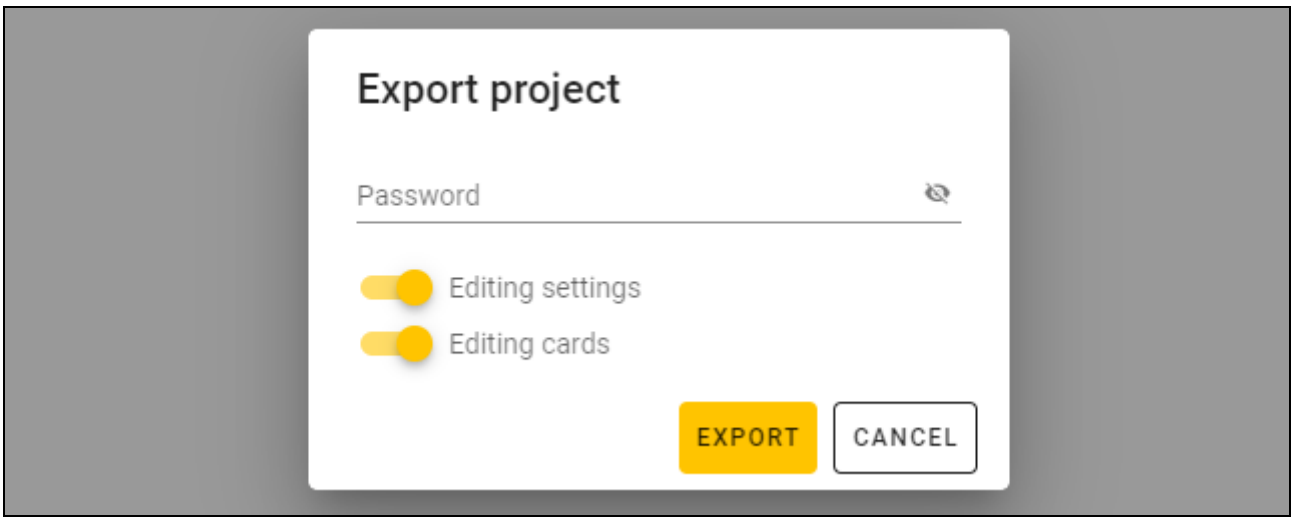
You can use the Ctrl + S shortcut to skip the first two steps and open the saving window right away.

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. The INT-SCR keypad in the INTEGRA system

5.1 Features

- Functions started using the code / proximity card:
  - arming / disarming the partition and clearing alarm in the partition,
  - unlocking the door,
  - controlling the *24. MONO switch* and *25. BI switch* type outputs,
  - confirming the guard round,
  - temporary partition blocking,
  - unblocking cash machine access,
  - changing the code by the user.
- Functions started without using the code / proximity card:
  - quick arming the partition,
  - generating the alarm from the keypad,
  - silencing the alarm at the keypad.
- Single door control.
- Additional function started using the F1 function key.

5.2 Installation in the INTEGRA system

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

The keypad must be connected to the INTEGRA series control panel expander bus.

Disconnect power before making any electrical connections.

5.2.1 Installation in short

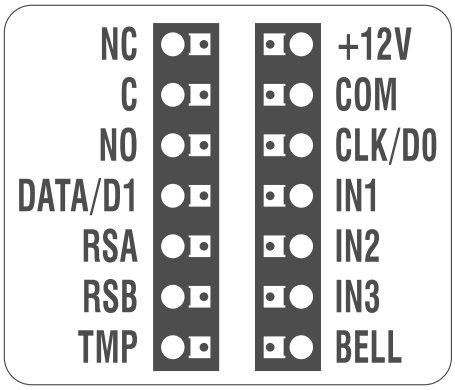
1. Open the keypad enclosure (see “Enclosure opening tool” p. 6).
2. Connect the keypad to the computer (p. 7).
3. Program the keypad in the CR SOFT program.
   3.1. Create a new *On-line system: INTEGRA/ACCO* type project (p. 14) or open an existing project.
   3.2. Establish connection between the program and the device (p. 16).
   3.3. Program the cards settings (p. 18).
   3.4. Program the keypad settings (p. 21):
   - select *INT-SCR* as the additional interface type.
   - set the keypad address for the purpose of the SATEL bus. It must be a unique address in the range from 0 to 31 (different from that of the other devices connected to the same control panel bus).
   - program the remaining settings.
4. Disconnect the keypad from the computer.
5. Run the cables to the place where you want to install the keypad. Use unshielded straight-through cables.

The total length of the expander bus must not exceed 1000 m.

6. Mount the keypad and start it (p. 32).
7. Program the keypad settings in the DLOADX program or in the LCD keypad (p. 33):

5.2.2 Description of terminals for keypad in the INTEGRA system

5



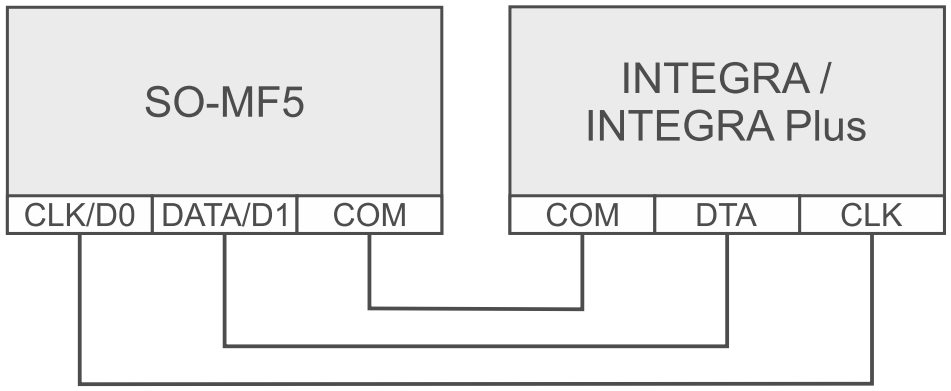
Terminal	Description
NC	relay output normally closed contact
C	relay output common contact
NO	relay output normally open contact
DATA/D1	data [INT-SCR interface]
RSA	RS-485 bus terminal [OSDP]
RSB	RS-485 bus terminal [OSDP]
TMP	*not used*

+12V	+12 VDC power input
COM	common ground
CLK/D0	clock [INT-SCR interface]
IN1	NC type door status input
IN2	NO type request-to-exit input
IN3	*not used*
BELL	OC type output

5.2.3 Mounting the keypad 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 COM, DATA/D1 and CLK/D0 terminals with the control panel expander bus terminals (Fig. 6).

6

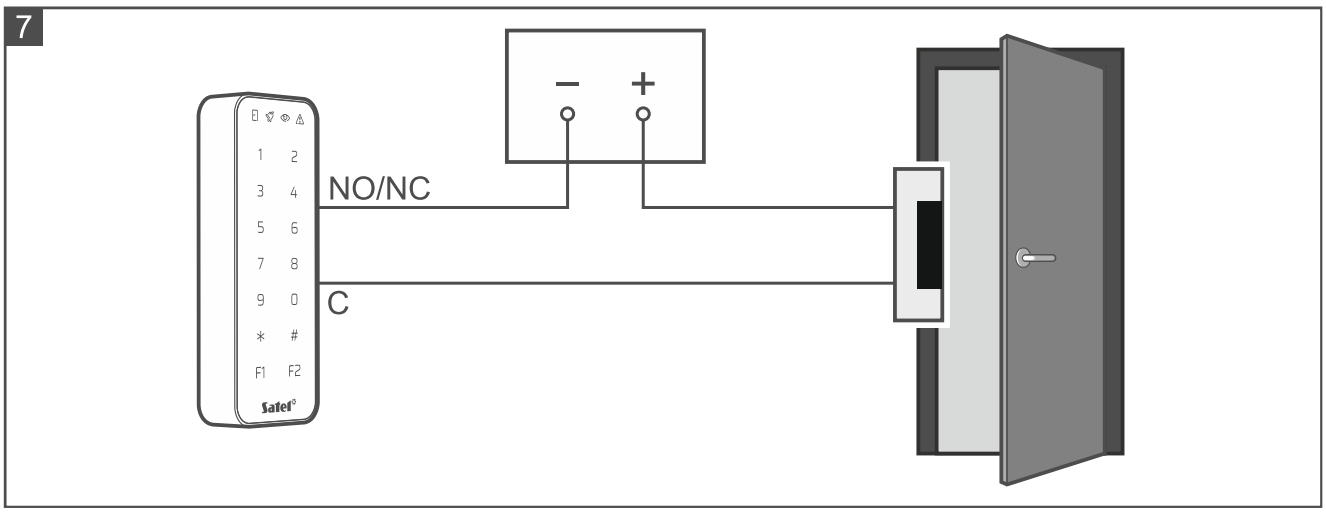


6. If the keypad is to control an electric strike, electromagnetic lock or another door actuator, connect this device to the relay output as shown in Fig. 7. Depending on the device type, use the following terminals:
   - NC: NC and C,
   - NO: NO and C.

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

7. If the keypad is to control the door status, connect the detector controlling the door status to the IN1 and COM terminals. If the keypad is not to control the door status, connect the IN1 and COM terminals together or set 0 for the *Max. door open time* parameter (DLOADX program or LCD keypad).
8. If the request-to-exit button is to be used, connect it to the IN2 and COM terminals. We recommend using a monostable button.
9. You can connect the BELL terminal (OC type output) e.g. to the alarm control zone.
10. Connect the power to the +12V and COM terminals. The keypad can be powered directly from the control panel, from an expander with power supply, or from a power supply.

7



11. Close the keypad enclosure.
12. Power on the keypad.
13. Start the identification function in the control panel (see the control panel installer manual). The keypad will be identified as INT-SCR.

5.2.4 Programming the keypad in the INTEGRA system

You can program the keypad settings in the DLOADX program or in the LCD keypad. Names of parameters and options from the DLOADX program are used in this manual. When a parameter or option is described, its name from the LCD keypad is shown in square brackets.

Programming in the DLOADX program

Required version of the DLOADX program: 1.21.002 (or newer).

1. Click  in the main menu. The “Structure” window will be displayed.
2. Click the “Hardware” tab.
3. Click the “Expansion modules” branch.
4. Click the name of the keypad whose settings you want to program.
5. Program the keypad settings.
6. Click  in the main menu to save changes to the control panel.

Programming in the LCD keypad

1. Enter the **service code** (by factory: 12345) and press * . The user menu will be displayed.
2. Press 9 WXYZ. The service menu will be displayed.
3. Start the “Settings” function (▶Structure ▶Hardware ▶Expanders ▶Settings).
4. Find the keypad whose settings you want to program (use the upwards or downwards arrow key) and press # .
5. Program the keypad settings.

Keypad settings

Name – individual name of the device (up to 16 characters).

Partition – partition operated by the keypad.

Lock [Lock feature] – if the option is enabled, the keypad can control access to a single door (the following parameters are available: *Lock features*, *Relay ON time*, *Max. door open time*, etc.).

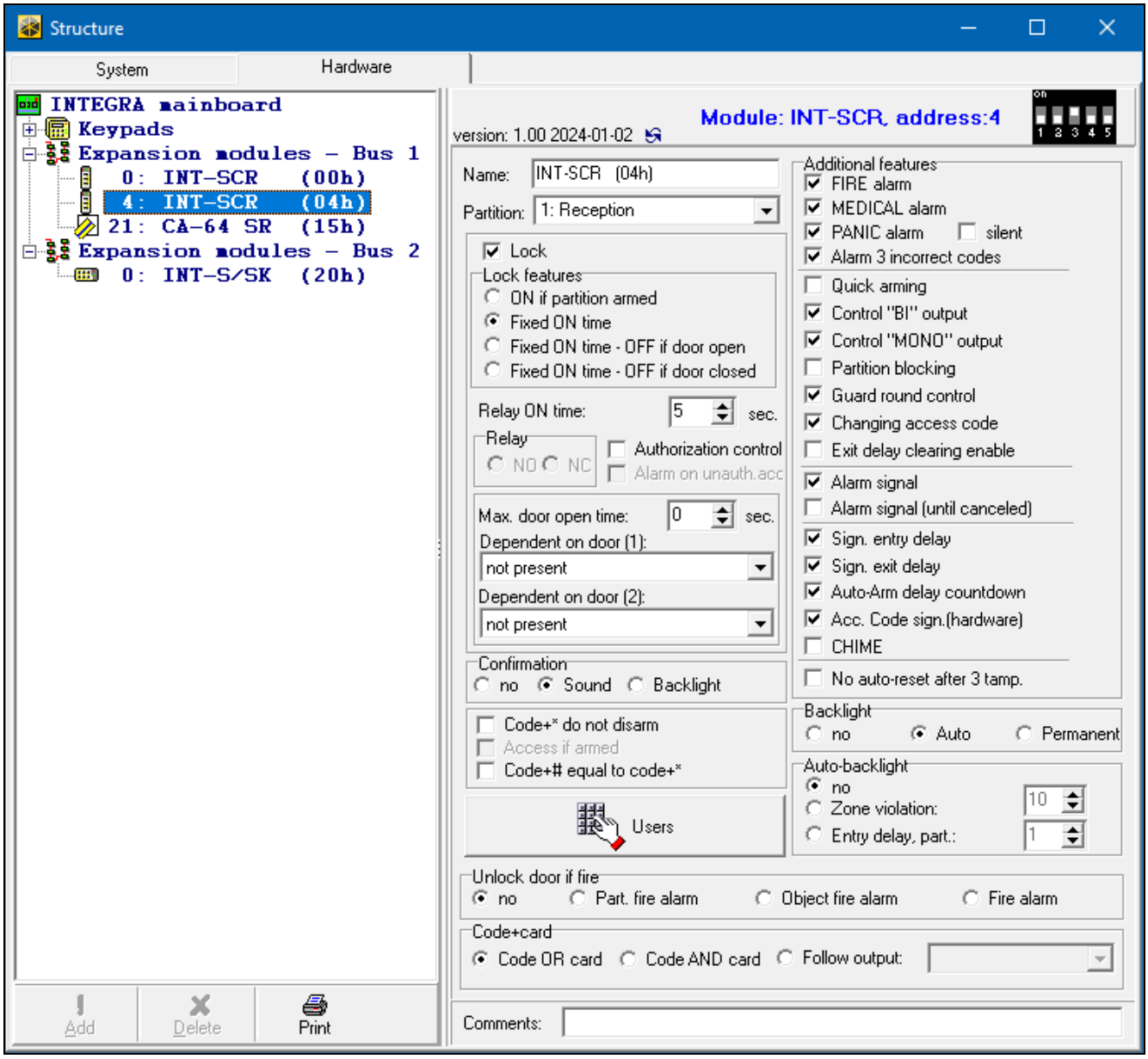
Lock features [Lock function] – operating mode of the relay output after the access is granted:

ON if partition armed [On if part.armed] – the relay output will be turned on until the partition is armed. When the partition is armed, users cannot get access (to get access, the user must disarm the partition).

Fixed ON time [ON time] – the relay output will be turned on for the *Relay ON time*.

Fixed ON time – OFF if door open [ON, open→off] – the relay output will be turned on until the door is opened (door status input is disconnected from common ground), however not longer than for the *Relay ON time*.

Fixed ON time – OFF if door closed [ON, close→off] – the relay output will be turned on until the door is closed (door status input is reconnected to common ground), however not longer than for the *Relay ON time*.



Relay ON time – the time during which the relay output can be turned on after the access is granted. You can program from 1 to 255 seconds. The parameter does not apply to the *ON if partition armed* mode.

Authorization control [Unauth. event] – if this option is enabled, unauthorized opening of the door will save the event to the control panel memory.

Alarm on unauth. access [Unauth. alarm] – if this option is enabled, unauthorized opening of the door when the partition is armed will trigger an alarm. This option is available if the *Authorization control* option is enabled.

Max. door open time [Max. door open] – the maximum period of time during which the door can be open (the door status input can be disconnected from common ground). If the door is open longer, audible alarm will be triggered in the keypad, and the event will be saved to the control panel memory. You can program from 0 to 255 seconds. If you enter 0, the door can be open for any long period of time.

Dependent on door (1) / **Dependent on door (2)** – you can select the door that must be closed so that the user can get access (turn the relay output on). It allows you to create a mantrap. You may select a door controlled by another expander or alarm system zone programmed as type *57 Technical – door open*.

Confirmation – method of providing feedback to the user after using the keypad:

No – no feedback.

Sound – the keypad will use sounds to give feedback to the user.

Backlight – the keypad will use keys backlight to give feedback to the user.

Code+* do not disarm [Code* not dis.] – if this option is enabled, entering the code and touching * / presenting the card will not disarm the partition (to disarm the partition, the user must enter the code and touch # / hold the card).

Access if armed [Code* in arm] – if the option is enabled, the users can gain access (turn the relay output on) when the partition is armed. If the option is disabled, the users cannot gain access when the partition is armed. This option is available if the *Code+* do not disarm* option is enabled. The option does not apply to the *ON if partition armed* mode.

Code+# equal to code+* [Code#->Code*] – if the option is enabled, reaction to entering the code and touching # / holding the card is the same as to entering the code and touching * / presenting the card. This means that the functions normally available on entering the code and touching # / holding the card (e.g. arming the partition) are not available. This option is available when the *Lock* option is enabled.

Users [Master users / Users] – the administrators and users who are permitted to use the keypad.

Additional features

FIRE alarm – if this option is enabled, touching and holding # for 3 seconds will generate the fire alarm.

AUX. alarm [Medical alarm] – if this option is enabled, touching and holding 0 for 3 seconds will generate the medical alarm.

PANIC alarm – if this option is enabled, touching and holding * for 3 seconds will generate the panic alarm.

silent [Silent panic] – if this option is enabled, the panic alarm generated from the keypad will be a silent one, i.e. the keypad will not indicate it, there will be no audible signal, but the alarm will be reported to the monitoring station. The silent panic alarm is useful when the control panel is sending events to the monitoring station, but unauthorized persons should not be aware of the alarm being generated. The option is available if the *PANIC alarm* option is enabled.

Alarm 3 incorrect codes [3 wrong codes] – if this option is enabled, using an incorrect code / card three times will generate an alarm.

Quick arming [Quick arm] – if this option is enabled, the user needs no code / card to arm the partition using the keypad.

Control "BI" output [BI outs ctrl.] – if this option is enabled, the *"Bi" output operating* type of users can use the keypad to control outputs.

Control "MONO" output [MONO outs ctrl.] – if this option is enabled, the *"Mono" output operating* type of users can use the keypad to control outputs.

Partition blocking [Part.blocking] – if the option is enabled, using the code / card by a user of the *Blocking partition* or *Guard* type will block the armed partition (violating a zone belonging to the partition will trigger no alarm). The duration of blocking is to be defined for the partition or the user (the user of *Blocking partition* type).

Guard round control [Guard control] – if this option is enabled, using the code / card by a user of the *Guard* type will be registered as the guard round.

Changing access code [Changing code] – if this option is enabled, the user can change own code from the keypad.

Exit delay clearing enable [Fin.exit time] – if this option is enabled, the user can terminate the partition exit delay countdown by touching successively 9 and # (if the *Exit delay clearing* option is enabled for the partition).

Alarm signal [Alarm (time)] – if this option is enabled, the keypad will audibly signal alarms throughout the *Global alarm time* (parameter programmed in the control panel).

Alarm signal (until canceled) [Alarm (latch)] – if this option is enabled, the keypad will audibly signal alarms until they are cleared.

Sign. entry delay [Entry time] – if this option is enabled, the keypad will audibly signal the entry delay countdown.

Sign. exit delay [Exit time] – if this option is enabled, the keypad will audibly signal the exit delay countdown.

Auto-Arm delay countdown [Auto-arm delay] – if this option is enabled, the keypad will audibly signal the auto-arm delay countdown.

Acc. code sign. (hardware) [Code entered] – if this option is enabled, the keypad will confirm with a single beep that the code is entered / card is read (signaling independent of the control panel). The signaling is useful when there is a delay between entering the code / reading the card and the sounds emitted after verification of the code / card by the control panel.

CHIME [Chime zones] – if this option is enabled, the keypad will audibly signal violation of zones with *Chime in module* option enabled, belonging to the partition operated by means of the keypad.

No auto-reset after 3 tamp. [No autorst.3t.] – if this option is enabled, each tamper will trigger alarm. If this option is disabled, the tampers following after three uncleared alarms will not trigger alarm (this prevents multiple logging of the same events).

Backlight

No – keys backlight is turned off.

Auto – keys backlight is turned on for 40 seconds after any key is touched / card is read. Additionally, it can be turned on if a specific event occurs (see: *Auto-backlight*).

Permanent – keys backlight is turned on.

Auto-backlight

No – if you select this option, the backlight will only go on after a key is touched / card is presented.

Zone violation – if you select this option, the backlight will additionally go on if a selected zone is violated.

Entry delay, part. – if you select this option, the backlight will additionally go on if entry delay countdown starts in the selected partition.

Unlock door if fire

no [no open] – the door will not be unlocked in the event of fire alarm.

Part. fire alarm [on partit. fire] – the door will be unlocked in the event of fire alarm in the partition to which the keypad is assigned.

Object fire alarm [on object fire] – the door will be unlocked in the event of fire alarm in the object to which the keypad is assigned.

Fire alarm [on any fire] – the door will be unlocked in the event of fire alarm in the alarm system.

Code+card

The ways in which the users can start a function (e.g. arming / disarming, alarm clearing, gaining access, etc.).

Code OR card – using the code or the card.

Code AND card – using the code and the card.

Follow output – depending on the selected output state (output OFF – using the code or the card; output ON – using the code and the card).

5.3 Using the INT-SCR keypad

Most features are available on using the code or proximity card by the user.

By default, the following codes are preprogrammed in the control panel:

service code: 12345

object 1 master user (administrator) code: 1111

The factory codes should be changed before you start using the alarm system.

Do not make your code available to other people.

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

5.3.1 LED indicators

LED	Color	Description
	blue	not used
	red	**ON** or **flashing** – alarm or alarm memory
	green	**ON** – partition is armed **flashing** – exit delay countdown is running in the partition
	yellow	**flashing** – trouble or trouble memory (the LED goes out when the partition is armed)

Information about the armed state can be extinguished after a preset time.

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

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

5.3.2 Sound signaling

Beeps generated when operating

The installer can disable the sound signaling or replace it with flashing of the keypad backlight.

1 short beep – any number key is touched or the code / card is used.

2 short beeps – the first code / card is accepted during two-code arming / disarming.

3 short beeps – confirmation of:

- starting the arming procedure (there is exit delay in the partition) or arming (there is no exit delay in the partition),
- alarm clearing and/or disarming.

4 short and 1 long beeps – function is executed.

3 pairs of short beeps – code change is required.

1 long beep – refusal to arm (there are violated zones in the partition or there is a trouble).

2 long beeps – incorrect code / card.

3 long beeps – unavailable function.

Event signaling

The installer defines whether events are to be signaled audibly.

5 short beeps – zone violation (CHIME).

Long beep every 3 seconds, followed by a series of short beeps for 10 seconds and 1 long beep – countdown of exit delay (if the time is shorter than 10 seconds, only the final sequence of short beeps will be generated).

A sequence of 7 beeps of diminishing duration, repeated every few seconds – countdown of auto-arming delay.

2 short beeps every second – countdown of entry delay.

Continuous beep – alarm.

Long beep every 2 seconds – alarm memory.

Long beep every second – fire alarm.

Long beep every 2 seconds – fire alarm memory.

Very short beeps – door open too long.

5.3.3 Available functions

Availability of the functions depends on:

- type and rights of the user,
- keypad settings,
- partition state.

[Code] ✳ / presenting the card

Enter the code and touch ✳ / present the card to:

- disarm the partition,
- clear alarm,
- gain access (turn on the keypad relay),

- toggle the state of *25. BI switch* type outputs,
- turn on the *24. MONO switch* type outputs,
- confirm the guard round,
- temporarily block the partition.

You can start two or more functions at the same time (e.g. disarming, alarm clearing and gaining access).

If you use the code or card and the and LEDs start flashing alternately, this means that the code and the card must be used to start the functions.

If you use the code/card to disarm the partition and the and LEDs start flashing alternately, this means that the keypad is waiting for the code/card of the other user (disarming using 2 codes).

[Code] # / holding the card

Enter the code and touch # / hold the card to:

- start the procedure of partition arming / arm the partition,
- disarm the partition,
- clear alarm,
- gain access (turn on the keypad relay),
- toggle the state of *25. BI switch* type outputs,
- turn on the *24. MONO switch* type outputs,
- confirm the guard round,
- temporarily block the partition,
- unblock access to cash machine.

You can start two or more functions at the same time (e.g. disarming, alarm clearing and gaining access).

If you use the code or card and the and LEDs start flashing alternately, this means that the code and the card must be used to start the functions.

If you use the code/card to arm / disarm the partition and the and LEDs start flashing alternately, this means that the keypad is waiting for the code/card of the other user (arming / disarming using 2 codes).

Quick arming

The installer may permit arming without using the code / card.

1. To select the arming mode, touch one of the keys:
   0 – full arming,
   1 – full arming + bypasses,
   2 – arming without interior,
   3 – arming without interior and without entry delay.
2. Touch #. This will start the partition arming procedure (if the exit delay is 0, the partition will be armed instantly).

Generating the alarm from the keypad

The installer can permit generating alarms from the keypad. To generate an alarm:

fire alarm – touch and hold * for 3 seconds,

medical (auxiliary) alarm – touch and hold 0 for 3 seconds,

panic alarm – touch and hold # for 3 seconds. The installer defines whether the audible or silent panic alarm will be generated.

Silencing the alarm sound at the keypad

Touch any number key to silence the keypad sounder during an alarm condition for 40 seconds.

Code changing

You can change your code if it is permitted by the installer.

1. Touch and hold 1 for 3 seconds.
2. When the and LEDs start flashing alternately, enter the old code and touch #.
3. When the and LEDs start flashing alternately, enter the new code and touch #.

Impact of the EN 50131 standard on keypad use

If the control panel is configured in accordance with the requirements of Standard EN 50131 for Grade 2 (INTEGRA) or Grade 3 (INTEGRA Plus):

- the keypad does not signal alarms,
- the LED indicates alarms only after entering the code / reading the card,
- flashing of the LED indicates a trouble in the system, bypassed zones or an alarm,
- the LED goes out after 60 seconds (Grade 3),
- quick arming features are not available,
- arming procedure cannot be initiated, if there are violated zones in the partition or there is a trouble in the system,
- the partition will not be armed if, at the moment of completion of exit delay countdown:
  – there is a violated zone in partition which was not violated when the arming procedure was started,
  – there is a trouble which did not exist when the arming procedure was started.

6. The ACCO-SCR keypad in the ACCO system

6.1 Features

- Functions started using the code / proximity card:
  – unlocking the door.
  – blocking / unblocking the door.
- Additional function started using the F1 function key.
- Additional function started using the F2 function key (the keypad connected to the controller using the RS-485 bus (OSDP)).

6.2 Installation in the ACCO system

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

The keypad 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.

6.2.1 Installation in short

Connecting using the ACCO-SCR interface

The ACCO-SCR interface enables the keypad to be connected to any access control module.

1. Open the keypad enclosure (see “Enclosure opening tool” p. 6).
2. Connect the keypad to the computer (p. 7).
3. Program the keypad in the CR SOFT program.
   3.1. Create a new *On-line system: INTEGRA/ACCO* type project (p. 14) or open an existing project.
   3.2. Establish connection between the program and the device (p. 16).
   3.3. Program the cards settings (p. 18).
   3.4. Program the keypad settings (p. 21):
   - select *ACCO-SCR* as the additional interface type.
   - set the keypad address for the purpose of the SATEL bus. The keypad with address 0 will operate as terminal A (entry terminal). The keypad with address 1 will operate as terminal B (exit terminal).
   - program the remaining settings.
4. Disconnect the keypad from the computer.
5. Run the cables to the place where you want to install the keypad. Use unshielded straight-through cables.

The length of cable connecting the keypad with the module should not exceed 300 m.

6. Mount the keypad and start it (p. 42).
7. Program the keypad settings in the ACCO Soft program (ACCO NET system) or in the ACCO-SOFT-LT program (p. 43):

Connecting using the RS-485 bus (OSDP)

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

1. Open the keypad enclosure (see “Enclosure opening tool” p. 6).
2. Connect the keypad to the computer (p. 7).
3. Program the keypad in the CR SOFT program.
   3.1. Create a new *On-line system: INTEGRA/ACCO* type project (p. 14) or open an existing project.
   3.2. Establish connection between the program and the device (p. 16).
   3.3. Program the OSDP protocol settings (p. 17).
   3.4. Program the cards settings (p. 18).
   3.5. Program the keypad settings (p. 21):
   - select *Not used* as the additional interface type.
   - program the remaining settings.
4. Disconnect the keypad from the computer.

5. Run the cables to the place where you want to install the keypad. For the RS-485 bus, we recommend using a UTP cable (unshielded twisted pair). To make other connections, use unshielded straight-through cables.

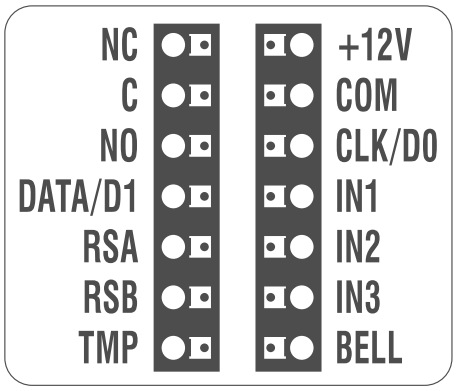
The RS-485 bus may be up to 1200 m long.

6. Mount the keypad and start it (p. 42).
7. Program the keypad settings in the ACCO Soft program (ACCO NET system) or in the ACCO-SOFT-LT program (p. 43):

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.

6.2.2 Description of terminals for keypad in the ACCO system

8



Terminal	Description
NC	*not used*
C	*not used*
NO	*not used*
DATA/D1	data [ACCO-SCR interface]
RSA	RS-485 bus terminal [OSDP]
RSB	RS-485 bus terminal [OSDP]
TMP	*not used*
+12V	+12 VDC power input
COM	common ground
CLK/D0	clock [ACCO-SCR interface]
IN1	*not used*
IN2	*not used*
IN3	*not used*
BELL	OC type output

6.2.3 Mounting the keypad in the ACCO system

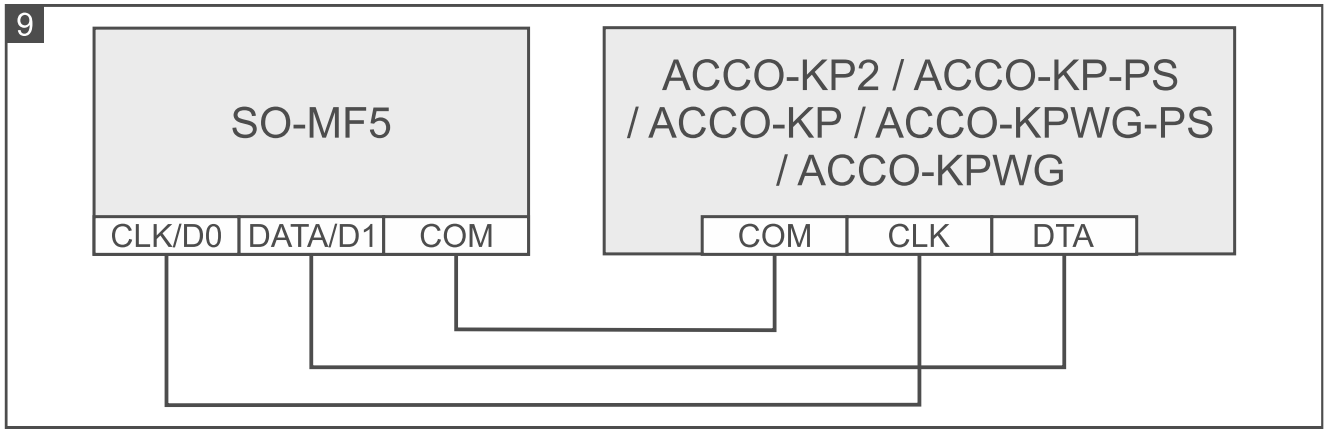
1. Place the enclosure base against the wall and mark the location of mounting holes.
2. Drill the holes in the wall for wall plugs (anchors).

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 keypad to the controller (see: “Connecting using the ACCO-SCR interface” or “Connecting using the RS-485 bus (OSDP)”).
6. You can connect the BELL terminal (OC type output) e.g. to the controller input.
7. Connect the power to the +12V and COM terminals. The keypad can be powered directly from the controller or from a power supply.
8. Close the keypad enclosure.
9. Power on the keypad.

Connecting using the ACCO-SCR interface

Connect the keypad’s COM, DATA/D1 and CLK/D0 terminals with the controller’s COM, DAT and CLK terminals (Fig. 9).

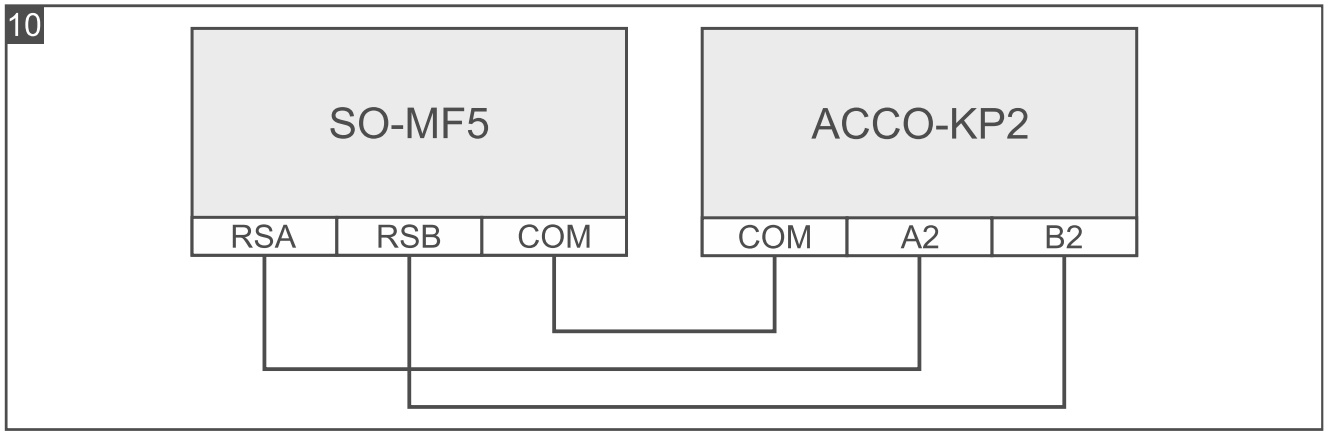
9



Connecting using the RS-485 bus (OSDP)

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

10



6.2.4 Programming the keypad in the ACCO system

If the keypad is to operate in the ACCO NET system, program the keypad settings in the ACCO Soft program (see the program manual). Otherwise, program the keypad settings in the ACCO-SOFT-LT program (see the ACCO-KP2 controller manual or the ACCO-KP-PS / ACCO-KP / ACCO-KPWG-PS / ACCO-KPWG controller manual).

6.3 Using the ACCO-SCR keypad

For information on how to use the keypad, please refer to the controller or the ACCO NET system manuals. Note that the LED indicators are different in the SO-MF5 keypad.

6.3.1 LED indicators

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. The keypad 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 keypad 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 keypad enclosure (see "Enclosure opening tool" p. 6).
2. Connect the keypad to the computer (p. 7).
3. Program the keypad in the CR SOFT program.
   3.1. Create a new *On-line system: Other* type project (p. 14) or open an existing project.
   3.2. Establish connection between the program and the device (p. 16).
   3.3. Program the OSDP or Wiegand protocol settings (p. 17).
   3.4. Program the cards settings (p. 18).
   3.5. Program the keypad settings (p. 21):
   - select *Not used* as the additional interface type if the RS-485 bus is to be used for connecting the keypad, or *Wiegand* if the Wiegand interface is to be used for connecting.
   - program the remaining settings.
4. Disconnect the keypad from the computer.

5. Run the cables to the place where you want to install the keypad. For the RS-485 bus, we recommend using a UTP cable (unshielded twisted pair). To make other connections, use unshielded straight-through cables.

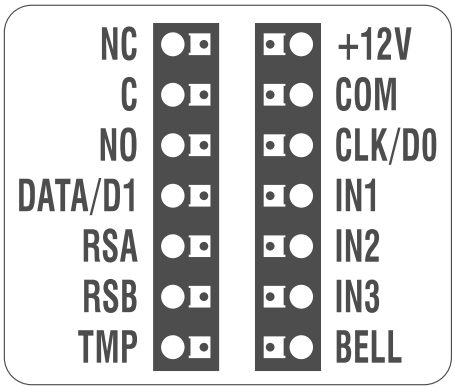
The RS-485 bus may be up to 1200 m long.

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

6. Mount the keypad and start it (p. 42).

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

11



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	OC type output

7.1.3 Mounting the keypad 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 keypad as required by the system in which the keypad is to operate.
6. Connect the power to the +12V and COM terminals.
7. Close the keypad enclosure.
8. Power on the keypad.

8. Standalone door control module

8.1 Features

- Support for up to 128 codes.
- Support for up to 128 proximity cards.
- Functions started using the code / proximity card:
  – unlocking the door,
  – blocking / unblocking the door,
  – changing the code by the user.
- Ability to specify the number of the code/card use.
- Ability to use the F1 function key to control e.g. a bell.

8.2 Installation of the standalone door control module

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

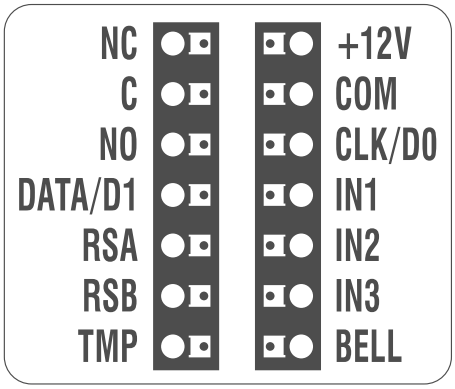
Disconnect power before making any electrical connections.

8.2.1 Installation in short

1. Open the keypad enclosure (see “Enclosure opening tool” p. 6).
2. Connect the keypad to the computer (p. 7).
3. Program the keypad in the CR SOFT program.
   3.1. Create a new *Standalone system* type project (p. 14) or open an existing project.
   3.2. Establish connection between the program and the device (p. 16).
   3.3. Program the cards settings (p. 18).
   3.4. Program the keypad settings (p. 21).
   3.5. Add users (p. 26).
4. Disconnect the keypad from the computer.
5. Run the cables to the place where you want to install the keypad. Use unshielded straight-through cables.
6. Mount the keypad and start it (p. 42).

8.2.2 Description of terminals for the standalone door control module

12

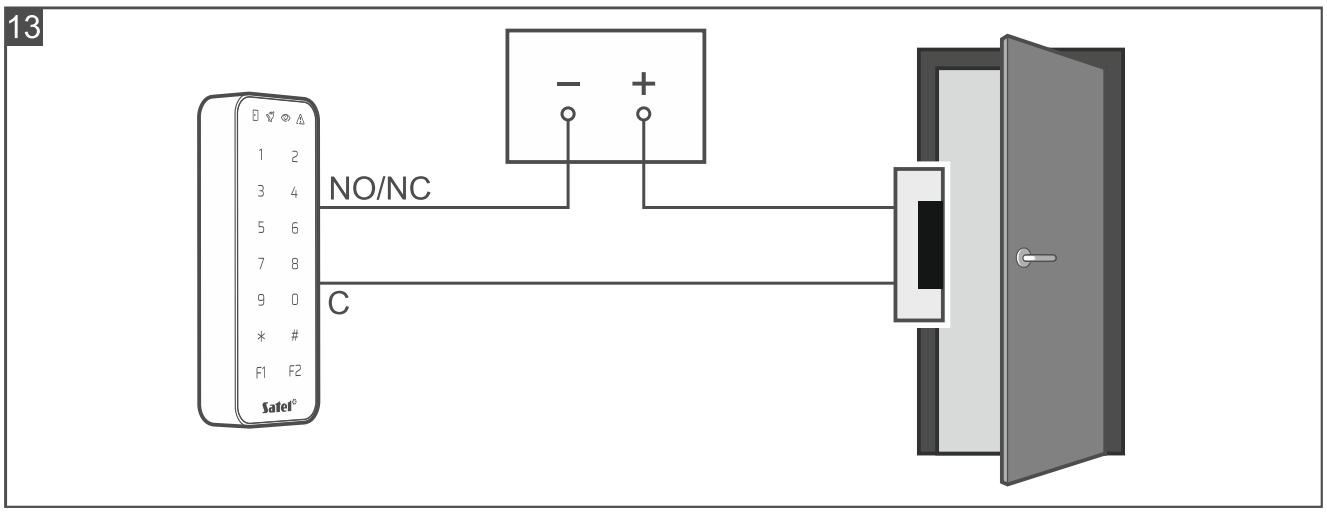


Terminal	Description
NC	relay output normally closed contact
C	relay output common contact
NO	relay output normally open contact
DATA/D1	*not used*
RSA	RS-485 bus terminal [OSDP]
RSB	RS-485 bus terminal [OSDP]
TMP	tamper output
+12V	+12 VDC power input
COM	common ground
CLK/D0	*not used*
IN1	door status input
IN2	request-to-exit input
IN3	*not used*
BELL	OC type output

8.2.3 Mounting the standalone door control module

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 electric strike, electromagnetic lock or other door actuator to the relay output as shown in Fig. 13. 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 keypad.



6. If the keypad is to control the door status, connect the detector controlling the door status to the IN1 and COM terminals. If the keypad is not to control the door status, program the IN1 input as *Not used* (CR SOFT program).
7. 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).
8. If the BELL output is to control e.g. a bell, connect to the output a relay that is to be used for control.
9. Connect the power to the +12V and COM terminals.
10. Close the keypad enclosure.
11. Power on the keypad.

8.3 Using the standalone door control module

Most features are available on using the code or proximity card by the user. Managing users and adding codes and proximity cards to the users can be done in the CR SOFT program (see: “Managing users” p. 26).

The keypad 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 keypad indicates alarm in the following cases:

- forced entry (if the door status is controlled – see: “Keypad settings” p. 23),
- 3 attempts to get access using an unknown code / card,
- module tamper (if the *Tamper* option is enabled – see: “Keypad settings” p. 23).

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 code / 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 or code 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. Enter the code and touch # or present the card to the keypad.
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 keypad 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. Enter the code and touch * or present the card to the keypad and hold. 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. Enter the code and touch # or present the card to the keypad.
2. When the LED starts flashing, open the door.
3. Enter the code and touch * or present the card to the keypad and hold. 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, enter the code and touch * or present the card to the keypad and hold. The door will be restored to normal operation mode. The LED will be turned off.

Changing the code

1. Touch 1 *. The and LEDs start flashing simultaneously.
2. Enter the code and touch #.
3. Enter the new code and touch #.

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 ..... 65 mA
Maximum current consumption ..... 120 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
BELL output, OC type ..... 30 mA / 12 VDC
Operating temperature range ..... -25°C...+55°C
Maximum humidity ..... 93±3%
Dimensions ..... 45 x 128 x 21 mm
Weight ..... 93 g