Configuration program for
ACCO NET access control module

ACCO SOFT

EN

ACCO NET 1.9
Program version 1.20

CE

acco soft_en 10/24

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

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

Signs in this manual

 Caution – information on the safety of users, devices, etc.

 Note – suggestion or additional information.

Changes made to firmware version 1.20

ACCO-NT control panel	Data encryption during communication between the ACCO-NT / ACCO-NT2 (version 1.16 or newer) and the ACCO-KP2 access control modules (version 1.01 or newer).
Controllers	Support for devices using the OSDP protocol by the ACCO-KP2 access control modules (version 1.01 or newer): – SATEL devices – third-party devices Capability to remotely update firmware of SATEL OSDP devices. New options for terminals connected to the ACCO-KP2 modules: – Terminal volume – Alternative door opening signal New options for terminals using the OSDP protocol: – Terminal tamper – Terminal keys sounds Capability to enable / disable LED indicators of terminals using the OSDP protocol. New functions for the “Indicator” type output for OSDP devices: – F1 – OSDP device A / B – F2 – OSDP device A / B Changed cut-off time of the “Failure” output for the “Long open door” function. New door settings (only ACCO-KP2): – Access time – Door open time Additional signaling of door open too long.

CONTENTS

1. General

The ACCO Soft program is used for programming and configuring the ACCO NET access control system. Communication between the program and the system takes place remotely via the Ethernet network.

The data are written to all control panels, access control modules and expanders included in the system.

2. Installation

2.1 System software requirements

The ACCO Soft program requires for its work the Java Runtime Environment version 8. Download this version of the program and install it on your computer.

2.2 Installation of the ACCO Soft program

1. Start your web browser.
2. Enter the address: https://[address of the computer on which the ACCO Server is installed] and log into the ACCO Web application as the Administrator (by default: login “admin” and password “admin”). If communication is to take place through a port other than the default one, enter the system address in the following way: https://[server address:port number].
3. Click the “Programs” command in the menu on the left side of the screen. Links to the installation files of ACCO-NT Conf, ACCO Soft and Map Editor programs will be displayed.
4. Click the ACCO Soft link (for Windows or Linux systems) and save the installation file to disk.
5. Run the installation file and follow the commands displayed.

After each update of the ACCO NET system, download and install the latest version of the ACCO Soft program.

3. Running the ACCO Soft program for the first time

3.1 Logging into the program

Access to the program is protected with password. When running the program for the first time, you can get access based on the factory default settings: login “admin” and password “admin” (you do not need to enter the data, just click the “Connect” button).

In the “System address” field, enter the network address of the computer on which the ACCO Server is installed. The address can be entered in the form of IP address (4 decimal numbers separated by dots) or as a name.

If the (RMI) port on which communication between the ACCO Server and the ACCO Soft program will take place is different than the default 2500 port, enter the port on which communication will take place after the IP address and colon.

Change the Administrator’s factory default program access password before you start using the system in the ACCO Web application.

The ACCO NET system Administrator has access to all functions of the program. Permissions of the other users must be defined by means of the ACCO Web application (see: ACCO Web user manual).

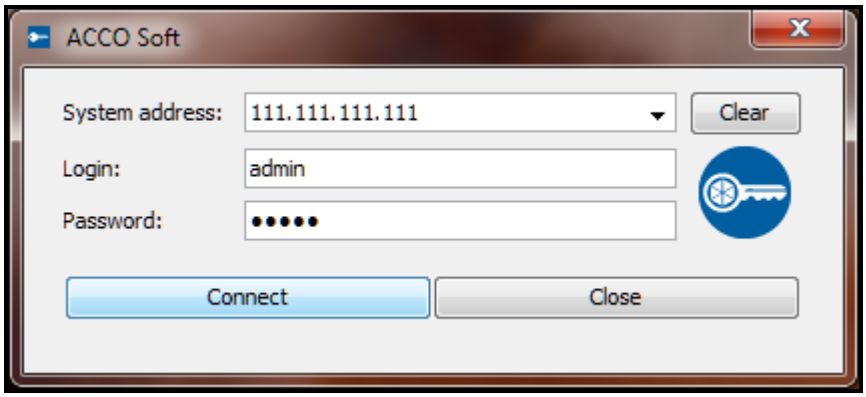


Fig. 1. Login window after starting the ACCO Soft program.

4. Description of the ACCO Soft program

If the button is displayed in the program main menu, this means that somebody else is configuring the ACCO NET system settings at the moment.

4.1 Main menu of the program

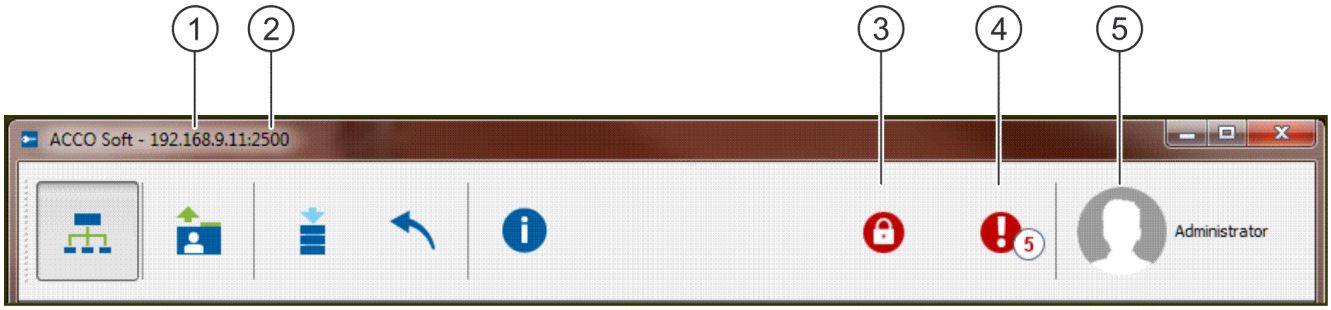


Fig. 2. Main menu of ACCO Soft program.

Explanations for Fig. 2:

1. network address of the computer on which the ACCO Server is installed.
2. number of the port on which communication between ACCO Server and ACCO Soft program takes place.
3. button indicating that the database is locked. Hover the mouse cursor over it to display information on the user that has started editing, but has failed to save the changes made. The lock will be released when changes are saved or after 15 minutes (by default) since the last change was made. After that time, you can click the button to unlock the database. To change the time after which the lock will be released, go to the ACCO Web application.

   The database locking information will also be displayed in the message which will appear:

   – if another user starts editing when you are logged into the program,

– if another user is editing the data when you start the program.

④ button indicating the current troubles / alarms in the system. Their number is displayed next to the button. Click the button to display the list of troubles / alarms (see: section “List of troubles / alarms”). If there is no connection between the ACCO Soft program and the ACCO Server, the button is displayed here to indicate that there is no communication.

⑤ name and picture of the logged in user.

Buttons:

- click to open the system configuration window.

- click to import the user data from files with kkd extension (from the ACCO-SOFT-LT program) or from files in CSV format.

- click to save the changes made.

- click to cancel all the changes that have been made since the last save.

- click to open the window with information on the version of ACCO NET system, ACCO Soft program, as well as versions and network addresses of server and database. The window also allows access to the licenses of ACCO Soft and ACCO Server programs as well as system integration (see section “Licences”).

4.1.1 List of troubles / alarms

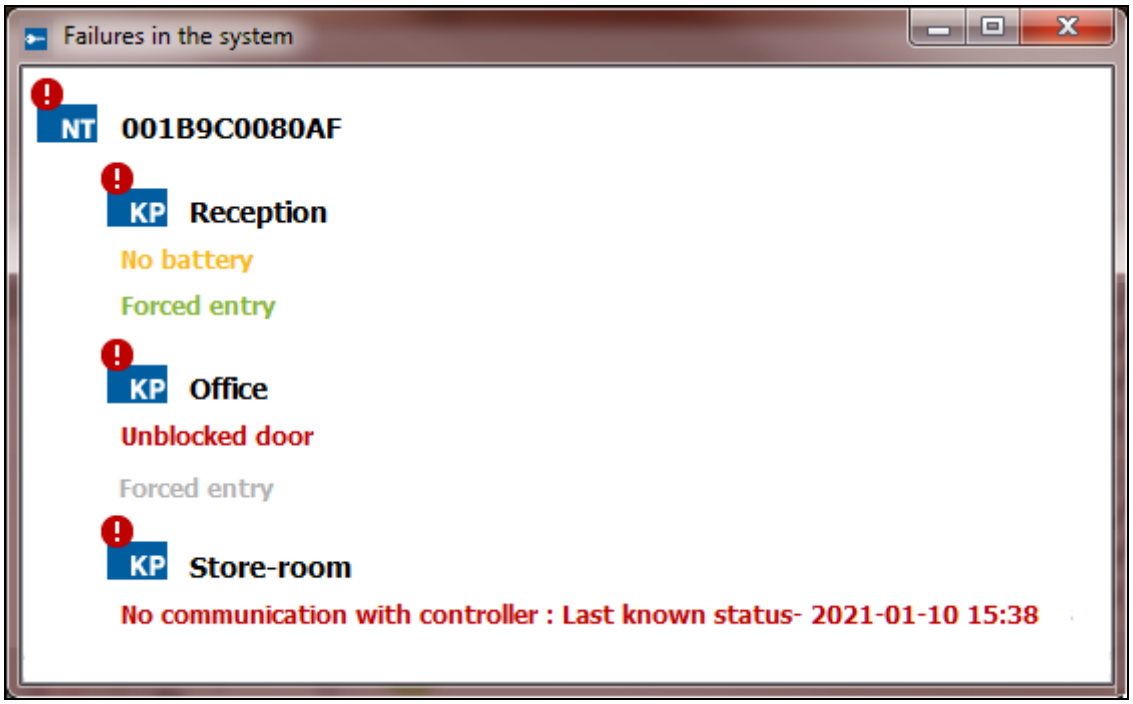


Fig. 3. An example of the list of current troubles in the system.

The window shows in a tree-form the devices included in the access control system. A suitable message will appear under the name of the device where a trouble / alarm occurred. The message color has the following meaning:

red – alarm;

orange – trouble;

green – confirmed alarm / trouble;

gray – alarm / trouble memory.

4.1.2 Licences

In the window that will open after you click the  button in the program main menu, you can find “Information about licenses” and the following buttons:

Show [next to ACCO Soft license] – click to open the window with license agreement for the ACCO Soft program.

Show [next to ACCO NET license] – click to open the window with license agreement for the ACCO Server program.

Manage [next to Integration license] – click to open the “Licences for systems integration” window.

Fig. 4. Window with information on versions of ACCO NET system, programs and database, and with license access buttons.

4.1.2.1 “Licences for systems integration” window

See also section “Integration”.

The INTEGRA or INTEGRA Plus alarm control panels can be assigned to one ACCO-NT access control panel. Integration of the ACCO-NT control panel with one alarm system is free of charge. If the ACCO-NT control panel is to be integrated with more than one alarm control panel, you will need the license key. The key is generated for the specific ACCO-NT control panel. It defines the maximum number of alarm control panels the access control panel can support.

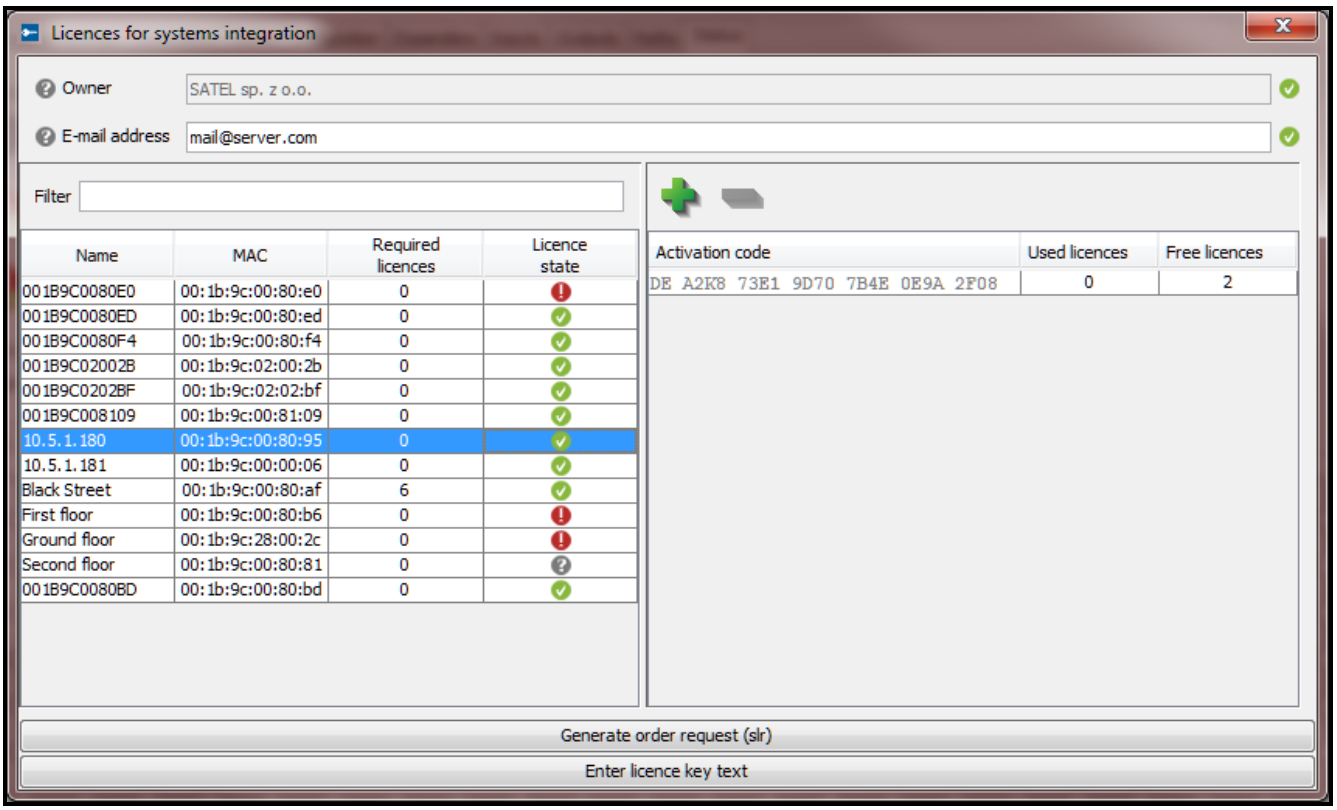


Fig. 5. “Licences for systems integration” window.

Owner – name of the company / first and last name of the person for which the license key is to be generated.

E-mail address – e-mail address to which the license key is to be sent.

Table with the list of ACCO-NT control panels in ACCO NET system

Filter – click the field and enter the name or MAC address of the control panel in full or in part. The data are being filtered as you enter each character.

Name – individual name of the control panel.

MAC – identification number of the control panel Ethernet card (MAC).

Required licences – the number of licenses required for integration purposes. It corresponds to the number of alarm systems to be added (see section “Integration”) minus one (one alarm system requires no license).

Licence state – the following information can be displayed in this field:

– license is waiting for decrypting (the icon will appear, if the text of license key entered for the given ACCO-NT control panel has not been decrypted because there is no communication between the ACCO Server and the ACCO-NT control panel, or after restart of the ACCO Server program, when the program has not established connection with the given ACCO-NT control panel yet),

– the number of licenses is insufficient,

– the number of licenses is sufficient.

Table with the list of activation codes

Clicking the ACCO-NT control panel will display a table with the list of activation codes:

– click to add an activation code.

– click to delete a selected activation code.

Activation code – activation code number you can purchase with an authorized SATEL distributor. The code consists of 26 characters (digits and letters). It defines the number of licenses you can obtain for the integrated alarm systems.

Used licences – the number of used licenses for alarm systems.

Free licences – the number of unused licenses for alarm systems.

Buttons

Generate order request (slr) – click to open the “Licences – summary” window that allows you to generate a license key request file (see section ““Licences – summary” window”).

Enter license key text – click to open the “Enter licence key text” window where you can paste the license key text (see section ““Enter licence key text” window”).

“Licences – summary” window

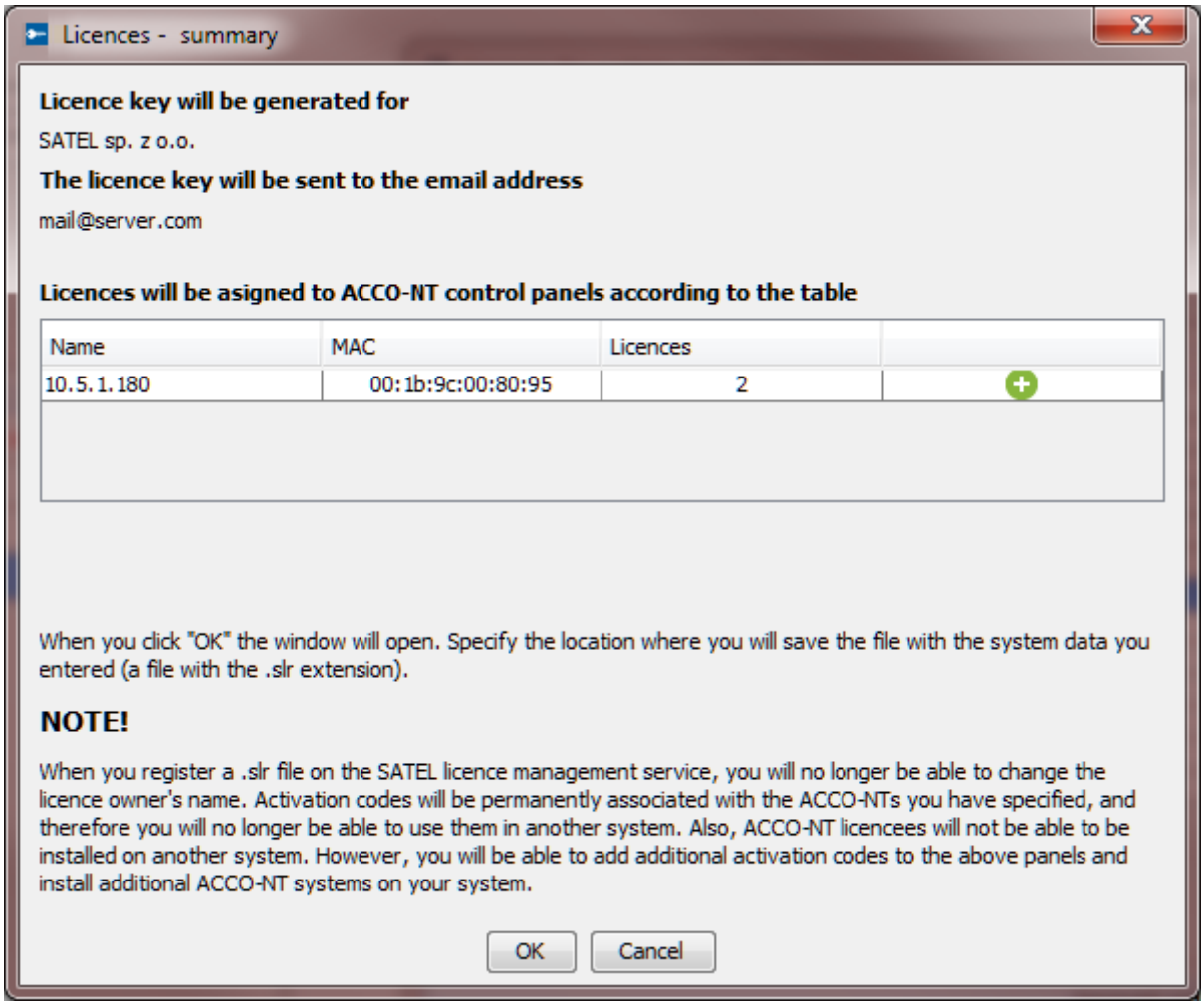


Fig. 6. “Licences – summary” window.

The window displays summary information based on the data from the “Licences for systems integration” window. This information will be saved in a file with .slr extension, based on which the license key text will be generated.

In the last column of the table showing the list of ACCO-NT control panels to which licenses will be assigned, the following information is displayed:

– new licence,

– unchanged licence,

– modified licence.

OK – click the button to generate the license key request file. A window will open where you can indicate location where the file with .slr extension, containing the data displayed, is to be saved (see section “Obtaining the license”).

“Enter licence key text” window

Enter in the window the text of license key received in the e-mail message.

OK – click the button to load into the system the license key containing licenses for the alarm systems. The button becomes active after you copy and paste the text. If the text is invalid, an appropriate message will be displayed to inform you about it.

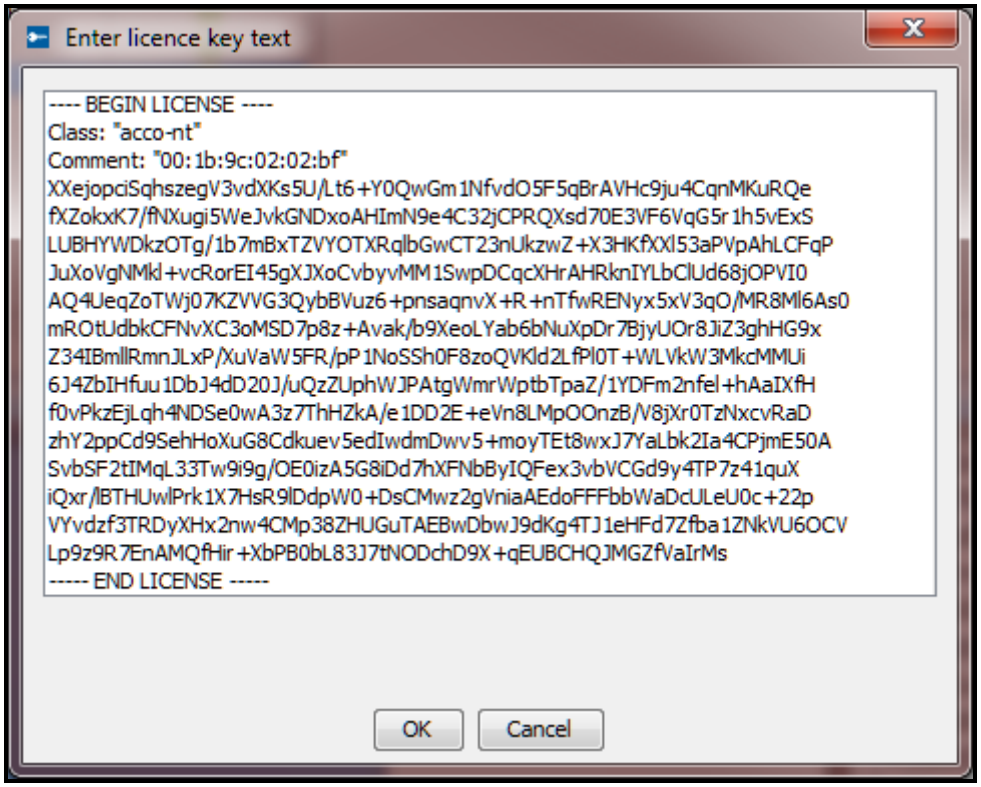


Fig. 7. Window with a license key text (example).

4.1.2.2 Obtaining the license

1. According to the procedure described in section “Adding an alarm system”, add an alarm system or systems.
2. In the main menu of the program, click the  button.
3. In the window that will open, click the “Manage” button.
4. In the “Owner” field, enter the name of the company or the first and last name of the person for which the license key is to be generated.
5. In the “E-mail address” field, enter the address to which the license key is to be sent.
6. In the table with the list of ACCO-NT control panels, select the control panel which is to handle the configured alarm systems.
7. When the table with the list of activation codes appears, click the  button.
8. In the “Activation code” window, enter the code number shown on your activation voucher. If the given ACCO-NT control panel is to support more alarm systems than the added code allows, enter further codes.

Do not enter any activation code for a larger number of alarm systems than the number of alarm systems added in the "Integration" tab (see section "Integration").

9. If the next ACCO-NT control panel is to support alarm systems, select it and repeat the steps 7 and 8.
10. Click the "Generate order request (slr)" button.
11. In the "Licences – summary" window, check that all data are correct and familiarize yourself with the information displayed at the bottom of the window.
12. Click the "OK" button.
13. In the window that will open, indicate where the file containing your data and system data is to be saved (the .slr file). You can rename the file to be saved. Click on the "Save" button.
14. Register the generated file in the SATEL license management service. To do this, start the web browser and enter the https://license.satel.pl address in it.

After the file with .slr extension is registered in the SATEL license management service:

- *the name of license owner cannot be changed,*
- *activation codes will be permanently associated with the ACCO-NT control panels you indicated and using them in another system will be impossible,*
- *the ACCO-NT control panels to which the licenses are assigned cannot be installed in another system.*

15. On the page that will open, click "ACCO NET".
16. You will be taken to the ACCO NET product registration page.
17. Click "Select file…" and, in the window that will open, indicate location of the previously generated file.
18. Click the "Register" button. Confirmation of the file registration will be displayed. You will also receive additional confirmation in a message sent to the e-mail address you gave when entering data.
19. In the next e-mail, you will receive the text of license key, that will contain the licenses requested by you.

4.1.2.3 Loading the license

1. Having received the license key, make sure that communication between ACCO Server and ACCO-NT control panel(s) for which the license key is to be loaded, proceeds normally.
2. In the main menu of the program, click the  button.
3. In the window that will open, click the "Manage" button.
4. In the "Licences for systems integration" window, click the "Enter licence key text" button.
5. When the "Enter licence key text" window opens, paste in it the copied text of license key you received.

The license key text to be pasted must begin with the "---- BEGIN LICENSE ----" phrase, and end with the "---- END LICENSE ----" phrase.

6. Click "OK".
7. After loading the license key, appropriate information will be displayed in the "Licence state" column, at the control panel(s) for which the license key has been loaded.

4.2 System structure

Description of the buttons

 - click to add an object.

 - click to delete the selected object.

 - click to add a control panel.

 - click to delete the highlighted control panel.

4.2.1 List of objects and control panels

The list presents objects and control panels assigned to them. A branch with list of unassigned control panels is also displayed. Shown at each control panel is an icon, which has the following meaning:

 – no connection with ACCO Server for more than 60 minutes (white exclamation mark on red background),

 – no connection with ACCO Server for less than 60 minutes (white exclamation mark on orange background),

 – communication with ACCO Server OK (white symbol on green background).

Shown in parentheses after the control panel name is information on its status:

- Unknown control panel status,
- No communication with the control panel,
- Control panel OK.,
- Restoring defaults – full,
- Restoring defaults – only control panel settings,
- Downloading configuration (transfer by ACCO Server to control panel of changes made to the system configuration),
- Controllers registration,
- Identification (when searching for controllers),
- Users broadcast (distribution of user data to controllers),
- Updating controller's firmware,
- Incorrect encoding key (refers to the key for encrypting the data sent between the ACCO Server and the control panel),
- Applying changes in control panel memory,
- Applying changes in controllers memory,
- Digits / numbers (information on currently processed data).

Buttons situated under the list of objects and control panels:

 – click to sort all objects from the list by names – from A to Z.

 – click to sort all objects from the list by names – from Z to A.

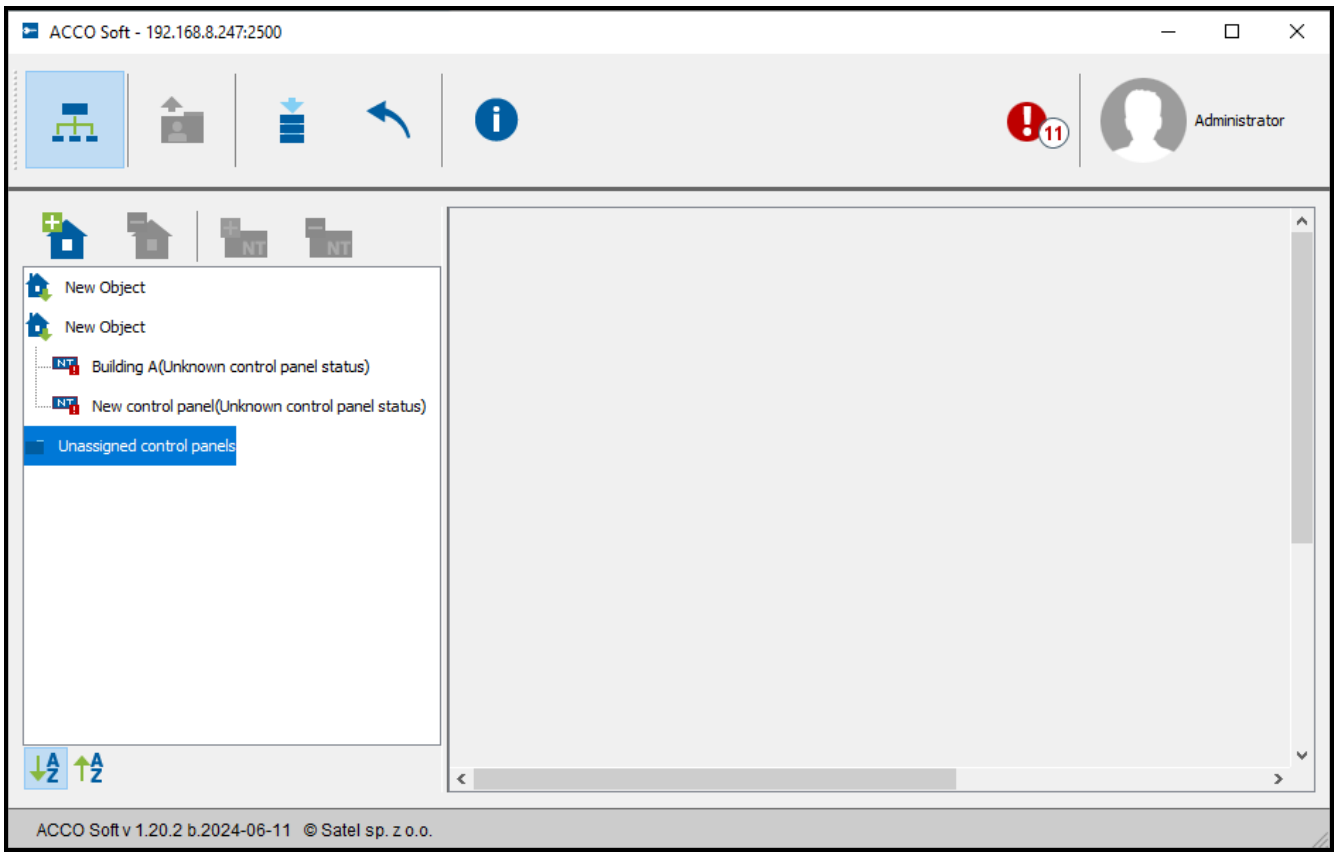


Fig. 8. List of objects and control panels.

4.2.1.1 Restarting the control panel

1. If you want to restart the control panel, highlight the selected device on the list.
2. Right-click your mouse.
3. Click the “Restart device” command.

The “Restart device” command is only available when communication between the control panel and ACCO Server proceeds normally.

If any problems occur with communication and thus with the control panel restart, a message will be displayed to inform you about it.

4. Icons displayed next to the control panel name will inform you in real time how the process of the control panel restart proceeds.
5. Reappearance of the NT icon means that the control panel has been restarted.

4.2.2 Objects

4.2.2.1 Adding an object

Click the button. The new object will appear on the list (see: section “List of objects and control panels”).

4.2.2.2 Programming the objects

Click the selected object on the list to program it. The object parameters will be displayed in the “Object settings” and “Control panels management” tabs.

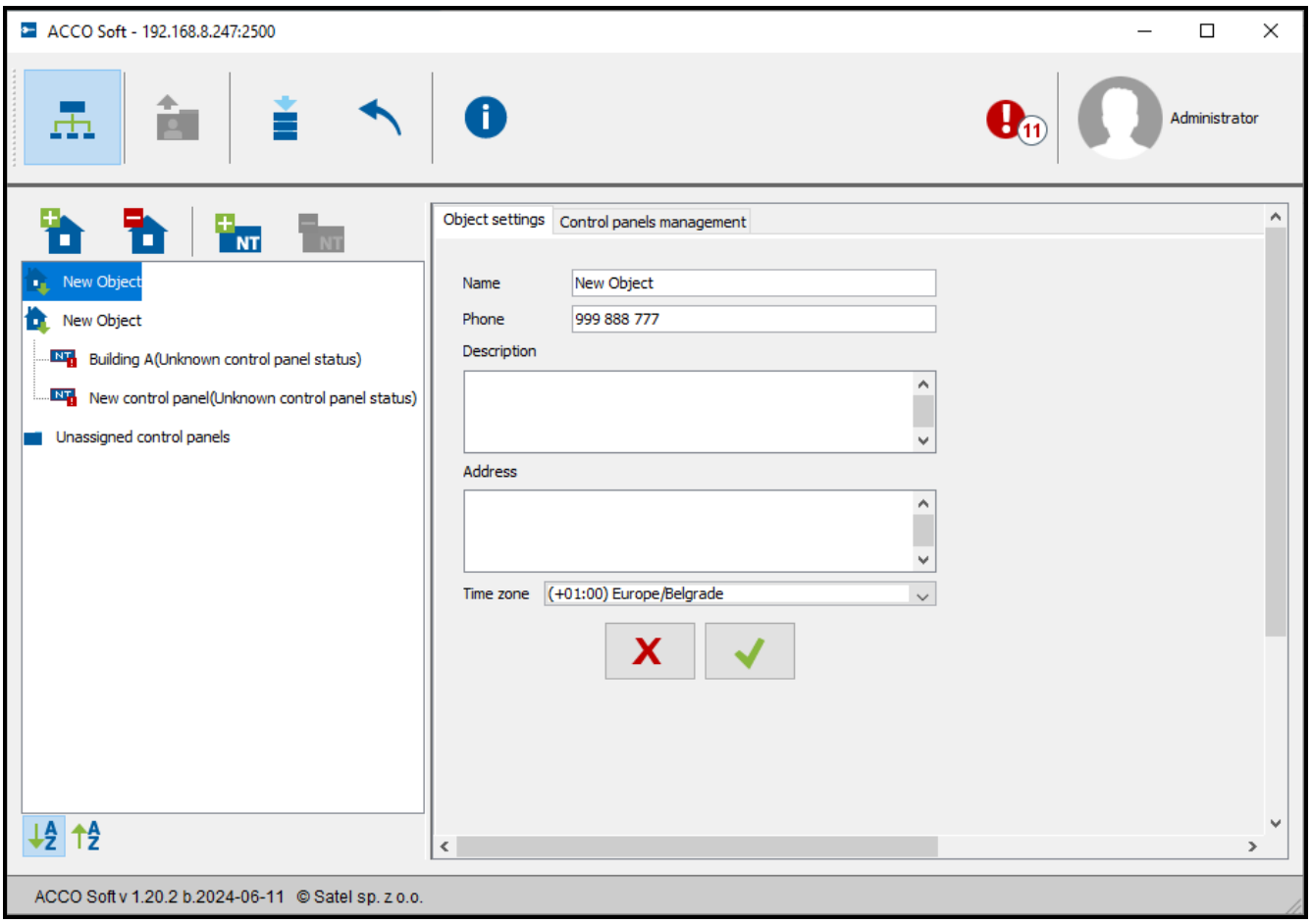


Fig. 9. “Object settings” tab.

Object parameters

“Object settings” tab

Name – individual name of the object (up to 32 characters).

Phone – number of object telephone.

Description – this field can be used for additional description of the object.

Address – object address.

Time zone – indicate the time zone, i.e. the difference between the universal time (GMT) and the time of the zone in which the given object is located. This makes it possible to properly save the event time to the data base, appropriately present events in the ACCO Web application, and display the correct time on the keypads connected to the controllers.

Making any change will display the following buttons:

– click to cancel the changes made.

– click to confirm the changes made.

“Control panels management” tab

Control panels in object – list of control panels assigned to the object.

Unassigned control panels – list of control panels which have not been assigned yet to any object.

Use the arrow buttons to move control panels between the lists – from the list of object control panels to the list of unassigned control panels and the other way round.

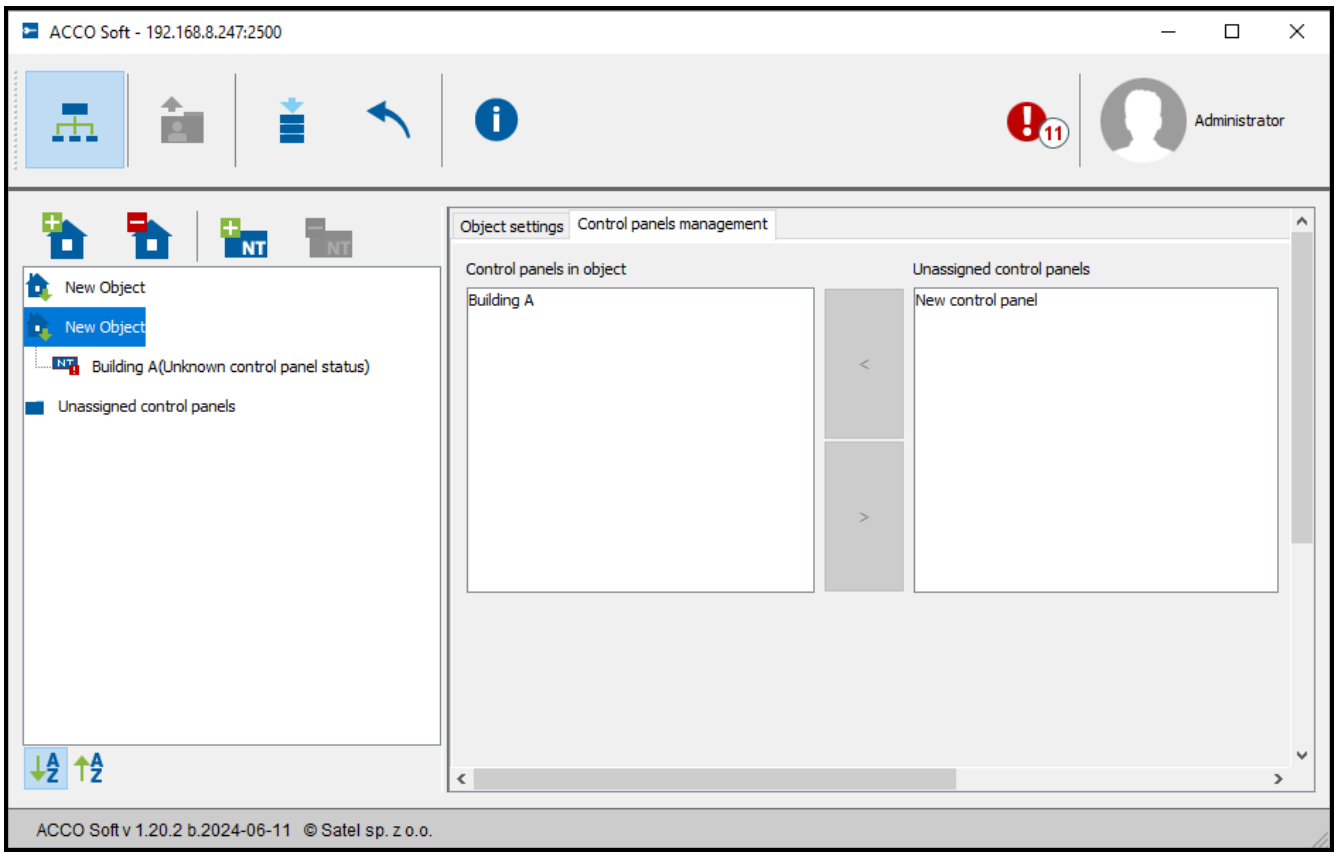


Fig. 10. “Control panels management” tab.

4.2.2.3 Deleting an object

1. If you want to delete a single object, use the cursor to highlight the selected object on the list of objects.
2. If you want to delete two or more objects at the same time, use the cursor to highlight one of the objects and, holding down the Ctrl key, select the next ones, highlighting them with the left mouse button.
3. If you want to delete all the objects at once, use the cursor to highlight one of the objects and press the Ctrl+A keys simultaneously.
4. Click the  button.
5. When a prompt appears asking you whether to delete the object, click “Yes”. The control panels assigned to the deleted object will be moved to the category of unassigned control panels.
6. Save the changes made.

4.2.3 Control panels

4.2.3.1 Adding the ACCO-NT control panel connected to Ethernet

1. Highlight on the list the object to which you want to assign the control panel being added.
2. Go to the “Control panels management” tab.
3. Highlight the control panel on the “Unassigned control panels” list. The list shows the control panels which established connection to the ACCO Server (the control panel MAC address is displayed as its name).
4. Click the arrow to move the control panel to the “Control panels in object” list.
5. When a prompt appears asking you whether to save the configuration, click “Yes”.

6. The control panel will be displayed on the list of objects and control panels as assigned to the object.

4.2.3.2 Adding the ACCO-NT control panel before connecting it to Ethernet

1. Highlight on the list the object to which you want to assign the control panel being added.
2. Use the 

button to add the control panel. It will be displayed on the list of objects and control panels as assigned to the object.
3. Highlight the control panel.
4. Click the “Control panel settings” tab. Configure the control panel settings, except of the MAC address (see: Fig. 11) and save them.
5. After connecting the control panel to the Ethernet network and establishing communication with the ACCO Server by it, click the drop-down menu symbol in the “MAC address” field. A list of MAC addresses of control panels not assigned to objects will be displayed.
6. Select the MAC address of appropriate control panel from the list.
7. When a prompt appears asking you whether to merge the devices together, click “Yes”.

4.2.3.3 Programming the control panel

Click the selected control panel on the list of objects and control panels to program it. Parameters will be displayed in the “Control panel settings” tab.

Control panel settings

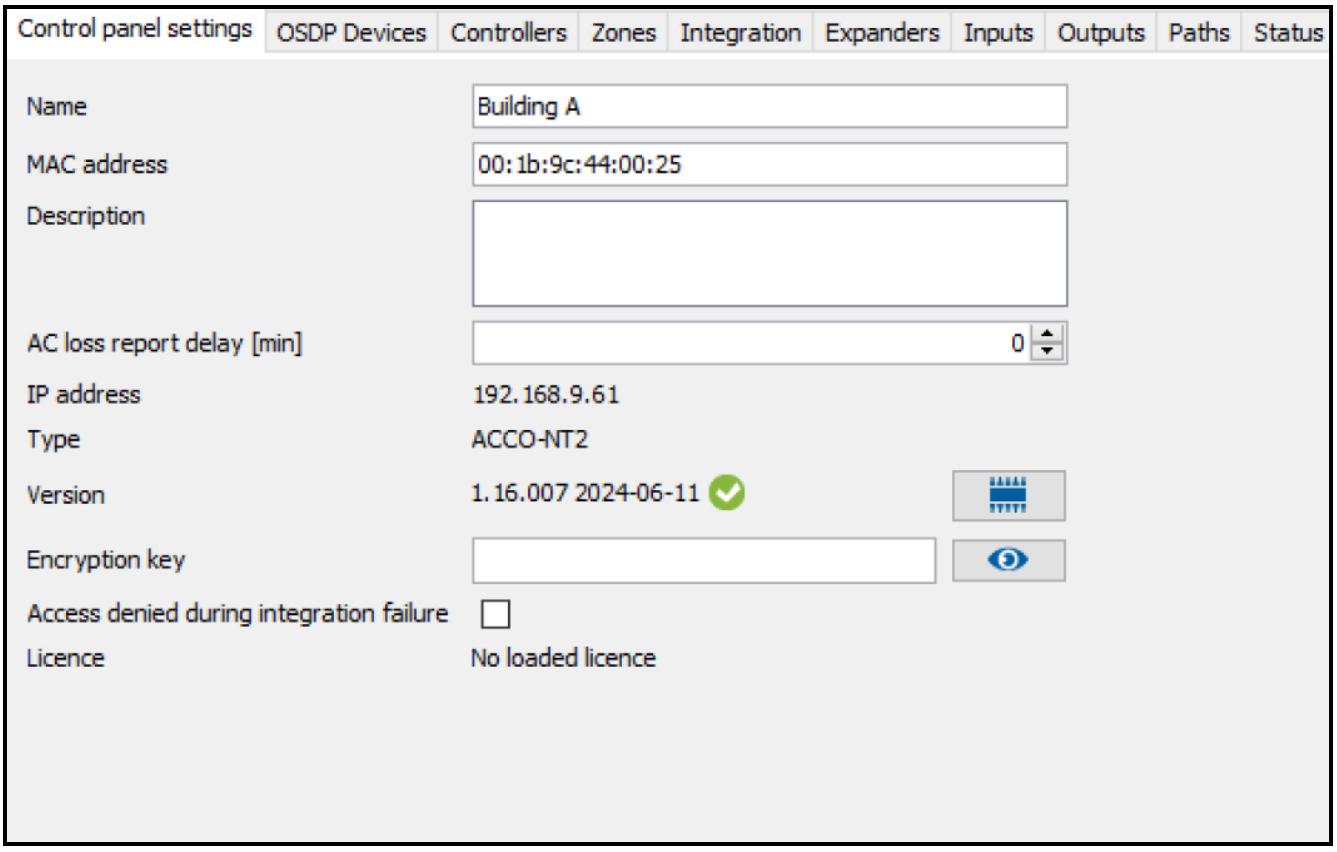


Fig. 11. “Control panel settings” tab.

Name – individual name of the control panel (up to 45 characters). By default, the control panel MAC address is used as the name.

MAC address – unique identification number of the Ethernet network card (MAC) of the control panel. If the "Merge with the device…" command is displayed in the field, you can click the field and select the MAC address from the list.

Description – this field can be used for additional description of the control panel.

AC loss report delay [min] – the time during which the control panel must be without AC power supply for the trouble to be reported. The trouble reporting delay prevents from being reported the momentary power losses which do not affect normal operation of the control panel. You can program up to 60 minutes.

IP address – IP address of the control panel.

Type – model of the control panel.

Version – control panel firmware version (version number and build date). Next to it, icons indicating the version may appear:

– current (white symbol against green background),

– to be updated (white exclamation point against orange background).

– click the button if you want to update the version of control panel firmware. (see: section "Remote update of the control panel firmware").

Encryption key – a string of up to 12 alphanumeric characters (digits, letters and special characters) defining the key to be used for encryption of the data sent between the ACCO Server and the control panels. **It must be consistent with the key defined in the control panel by means of the ACCO-NT Conf program.** The server will only establish connection with the device which will be using the appropriate key.

– click the button to check the value entered.

Access denied during integration failure – if this option is enabled and there is no communication with the alarm control panel, the users can't get access to the integrated zone of the access control system until normal communication is restored. If this option is disabled and there is no communication with the alarm control panel, the users can get access to the integrated zone of the access control system according to the same rules as without integration of the systems. The option applies to all alarm control panels assigned to the given ACCO-NT control panel (see section "Integration").

If the "Access denied during integration failure" option is disabled and communication between ACCO NET and alarm system is lost, the "Armed" status of the ACCO NET zone will change to "Zone blocked". Thus you can get access to individual doors of the ACCO NET system. At the moment the user gets access to that zone, the zone status will change to "Zone controlled". When communication between the systems is restored, the zone status will change again to "Armed".

Licence – number of the license assigned to the control panel or a message with information on the license status.

Making any change will display the following buttons:

– click to cancel the changes made.

– click to confirm the changes made.

4.2.3.4 Remote update of the control panel firmware

After updating the ACCO-NT control panel firmware, it is advisable to update the firmware of all access control modules connected to that control panel (see section "Remote update of the controller firmware").

1. If in the “Version” field, next to the current version of the control panel firmware, the ⚠ icon is displayed, click the button.
2. A window will open with the data of the current version of device firmware, as well as information on the new available version (see Fig. 12).

Click to check if there is a new version of control panel firmware available on the SATEL server.

3. Click the “Update” button.
4. The process of control panel firmware update will start.
5. When the update is completed, an appropriate message will be displayed.
6. Click the “OK” button and close the “Firmware version” window.

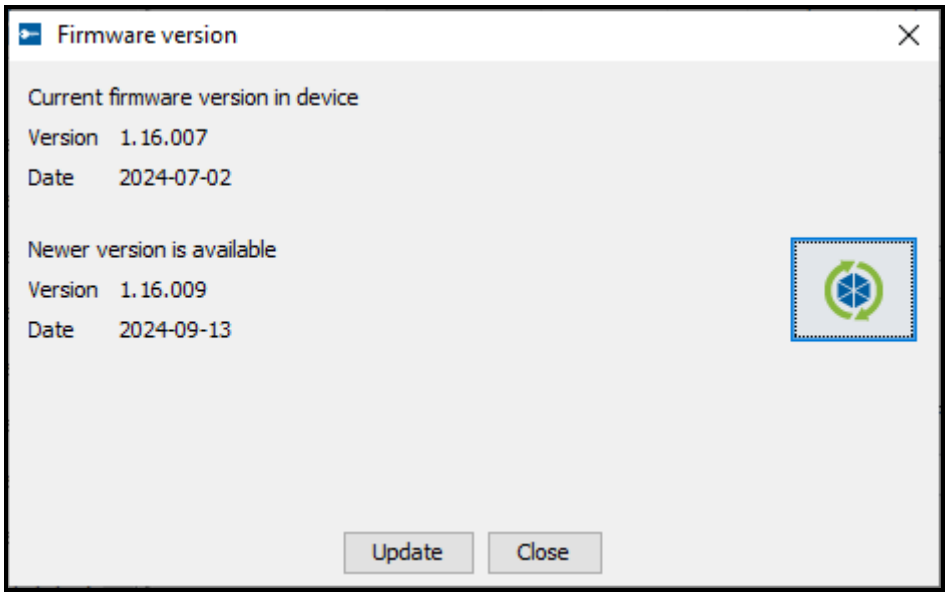


Fig. 12. Control panel firmware update window.

4.2.3.5 Deleting a control panel

1. On the list of objects and control panels, highlight the control panel to be deleted.
2. Click the NT button.
3. When a prompt appears asking you whether to delete the control panel, click “Yes”. If the control panel to be deleted was assigned to an object, it will be moved to the category of unassigned control panels. If the control panel to be deleted was not assigned to any object (it was on the list of unassigned control panels), it will be deleted from the system.
4. Save the changes made.

4.2.4 OSDP devices

OSDP devices are devices connected to the RS-485 bus that use the OSDP protocol (Open Supervised Device Protocol) for communication. The communication is a two-way, encrypted communication. Devices that use the OSDP protocol are supported by the ACCO-KP2 access control modules (version 1.01 or newer):

4.2.4.1 OSDP

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

The ACCO NET system supports the following OSDP baud rates: 9600, 19200, 38400, 57600 and 115200.

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 system is created. It can be changed. You can enter 32 hexadecimal characters (16 bytes).

In each system the key should be unique (different for each system).

Use SATEL token key – if this option is enabled, the SATEL token key is used. The fields "SATEL token key" and "No encryption (use Card Serial Number only)" are available. The fields in the "MIFARE Classic", "MIFARE DESFire" and "MIFARE Ultralight" fields used for programming the settings of each card type are unavailable.

No encryption (use Card Serial Number only) – 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.
- "SATEL token key" field is unavailable.

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

If the ACCO NET system is integrated with the INTEGRA alarm system, program the same settings in both systems.

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

In each system the key should be unique (different for each system).

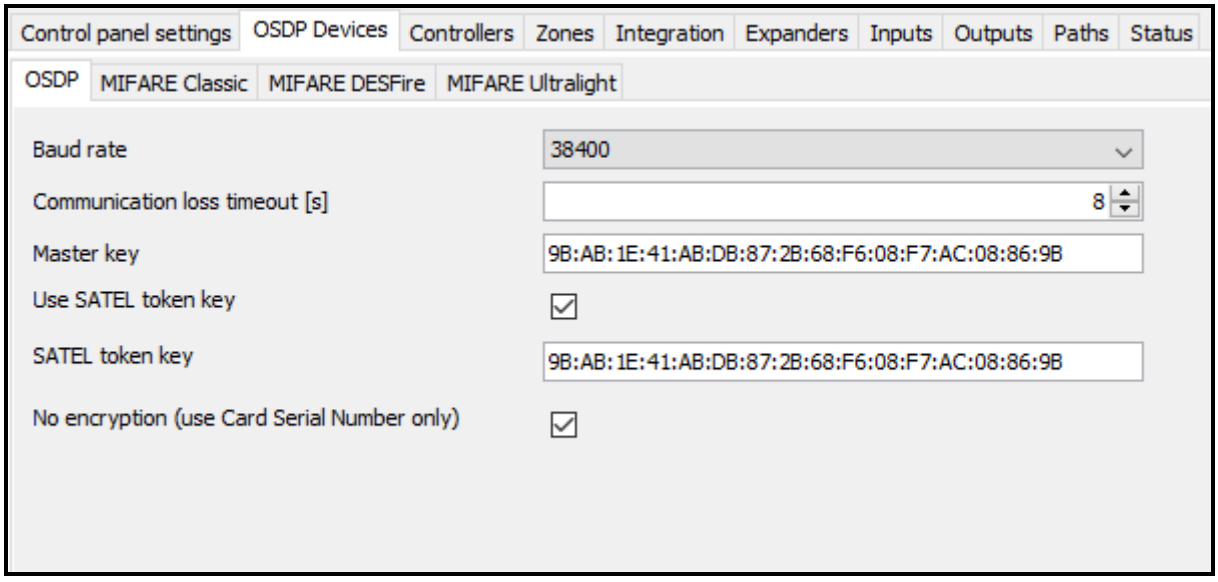


Fig. 13. "OSDP" tab.

4.2.4.2 MIFARE Classic

Supported – if this option is enabled, MIFARE Classic cards are supported and their settings are available.

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 Sector Number (MSN) – card number can be programmed and written in the card memory sector identified by the “Application ID”.

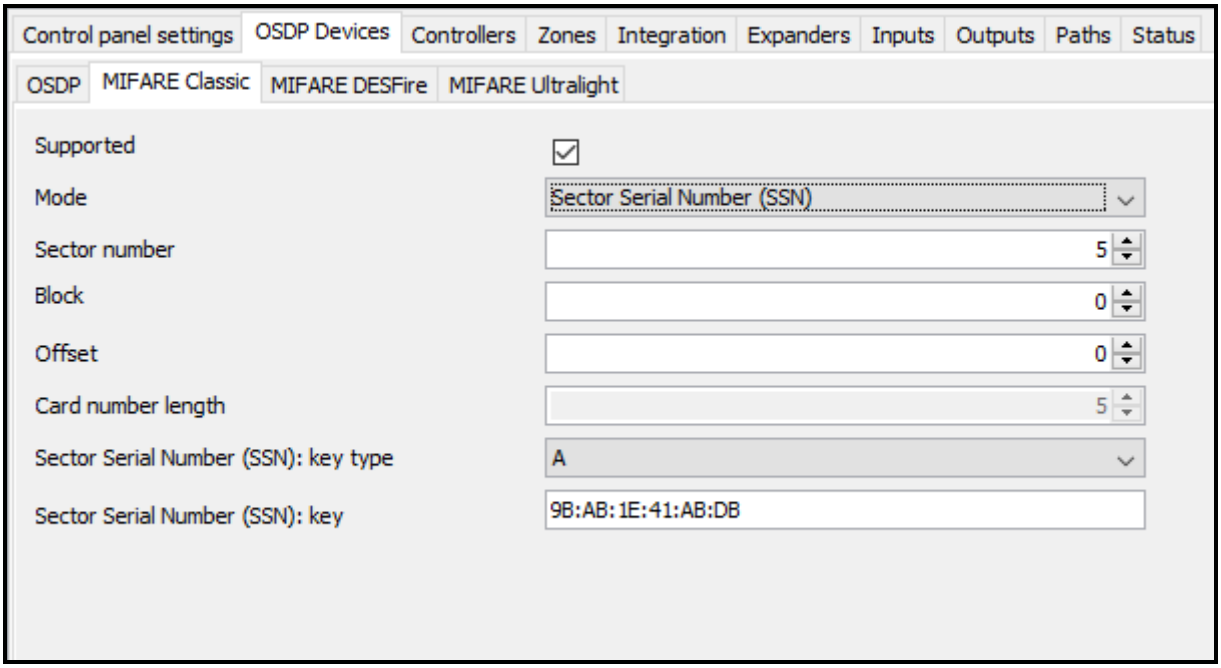


Fig. 14. “MIFARE Classic” tab.

Sector number – number of the data sector in which the card number is to be written. You can enter a number from 0 to 15. 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.

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.

Offset – card number’s first byte position in the block. You can enter a number from 0 to 15.

Card number length – number of bytes used for the card number. For the ACCO NET system it is 5 bytes.

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.

By default, the first 6 bytes of the master key are used.

In each system the key should be unique (different for each system).

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

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

By default, the first 6 bytes of the master key are used.

> *In each system the key should be unique (different for each system).*

4.2.4.3 MIFARE DESFire

Supported – if this option is enabled, MIFARE DESFire cards are supported and their settings are available.

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 Sector 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 the card number.

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

Card number length – number of bytes used for the card number. For the ACCO NET system it is 5 bytes.

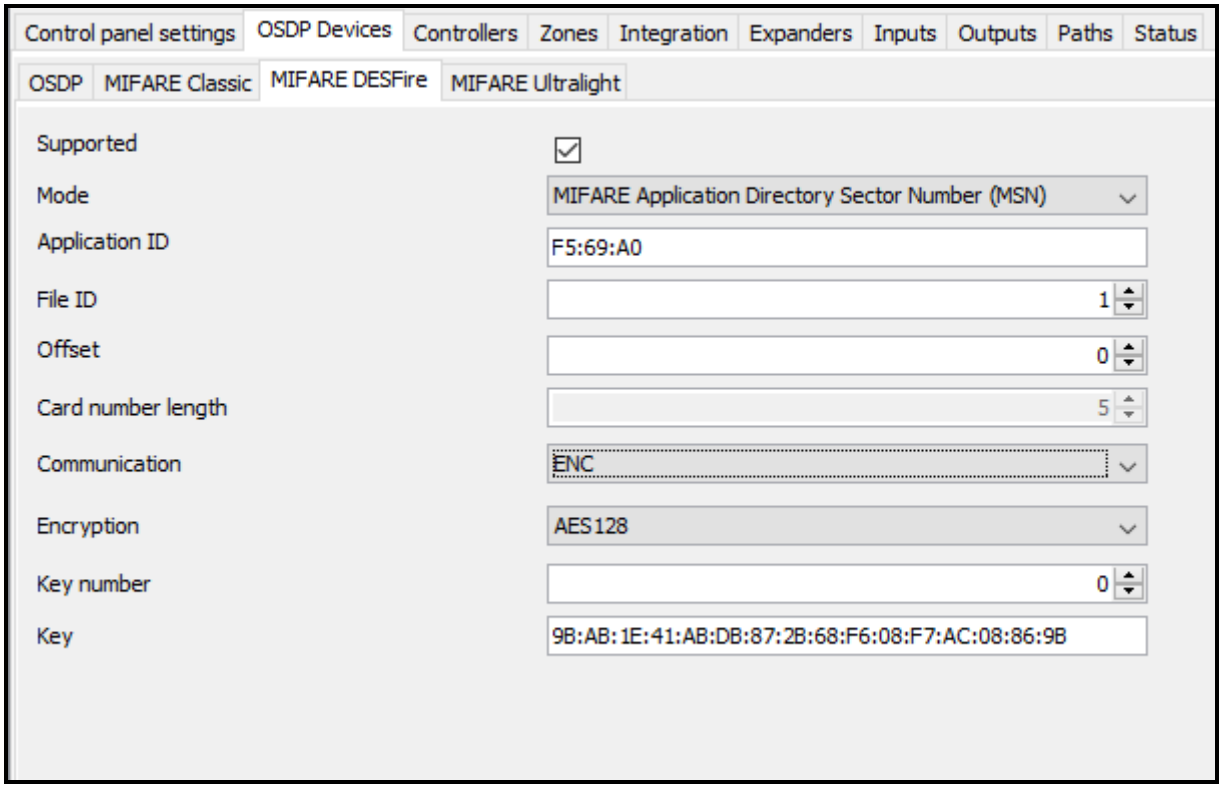


Fig. 15. "MIFARE DESFire" tab.

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. Default setting.

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 number – number of the key used to encrypt the card number file. 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).

By default, the master key is used.

In each system the key should be unique (different for each system).

4.2.4.4 MIFARE Ultralight

Supported – if this option is enabled, MIFARE Ultralight cards are supported and their settings are available.

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.

Card number length – number of bytes used for the card number. For the ACCO NET system it is 5 bytes.

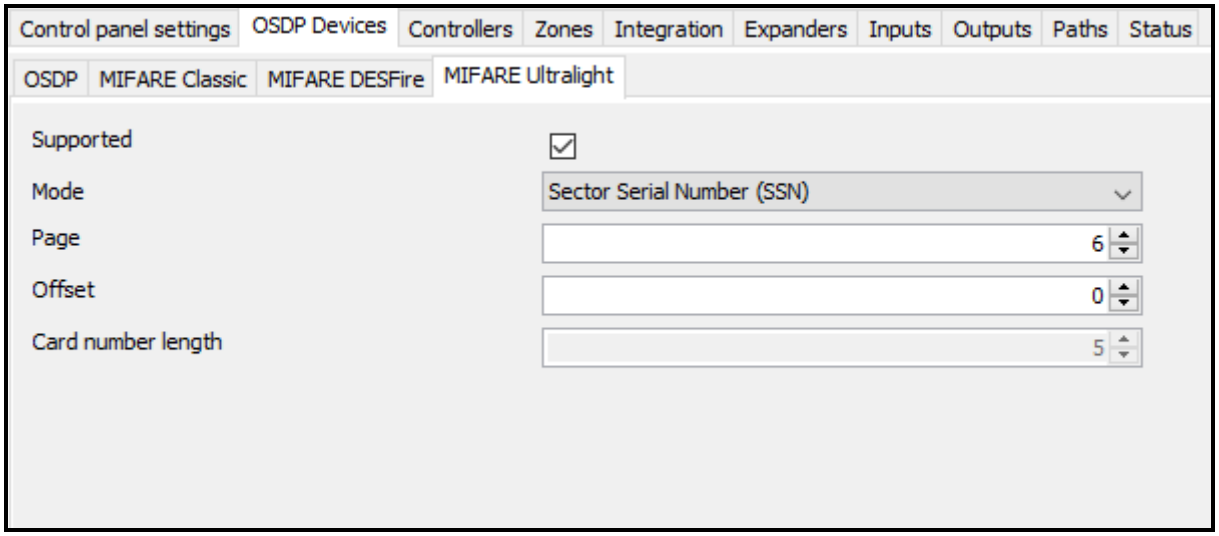


Fig. 16. "MIFARE Ultralight" tab.

4.2.5 Controllers

Description of the buttons

- click to add a module.

- click to delete the highlighted module from the list of modules (see: section "Deleting a controller").

- click and select:
  - "Find controllers" if you want to run the identification procedure for modules connected to the control panel. After completion of the procedure, the "Summary – controllers" window will be displayed, showing information on the identified controllers (see: section "Identification of controllers connected to the system").
  - "Find OSDP devices" if you want to run the identification procedure for the OSDP devices connected to the selected controller(s). After completion of

the procedure, the “Summary – OSDP devices” window will be displayed, showing information on the identified OSDP devices (see: section “Identification of OSDP devices connected to controllers”).

The button is only available when the status of the control panel to which controllers are connected is “Control panel OK.” (the status is displayed in parentheses next to the name of control panel on the list of objects and control panels), and the changes made have been saved.

- click and select:
  – „Update controllers” if you want to run the firmware update procedure for the selected module(s) (see: section “Remote update of the controller firmware”).
  – “Update OSDP devices” if you want to run the firmware update procedure for the OSDP devices connected to the selected module(s) (see: section “Remote update of the OSDP device”).

This button is available when there are no changes to be saved.

The number of controllers is displayed under the buttons. Hovering the cursor over the number will display information on the number of controllers connected to the first and second RS-485 bus of the selected ACCO-NT control panel.

4.2.5.1 Identification of controllers connected to the system

Each module must be identified so that the ACCO-NT control panel can establish communication with it. This will allow reading and writing of its data.

1. On the list of objects and control panels, select the control panel to which modules are connected.
2. Go to the “Controllers” tab and click  . Select the “Find controllers” command.
3. In the window that will open, identification progress information will be displayed.
4. After identification is completed, the “Summary – controllers” window will be displayed (see: section ““Summary – controllers” window”). The new controllers will have the “New controller” status.
5. Click the “Confirm” button.
6. A window prompt will be displayed asking you whether to save the configuration. Click “Yes”.

Run the identification function each time when a new device is connected to any bus or the address is changed in a device connected to any bus.

Disconnecting an identified device from the communication bus will:

– *generate an event indicating a control panel trouble, with the following content “Trouble start. No controller. Device index…”,*
– *change into red the controller name color on the list of controllers (see: section “Table with the list of controllers”).*

The users can get access to the partition immediately after registering the controller which supervises a door belonging to the partition.

“Summary – controllers” window

Identified controllers number – number of identified controllers.

Address – address set in the controller.

Module name – controller name.

Status – in the column, the following information can be displayed:

Unchanged – module whose data are consistent with the program data.

New controller – module which has been added to the system.

Changed – module whose data are not consistent with the program data.

No communication – module which was previously available in the system, and with which the control panel failed to establish communication during the current identification procedure.

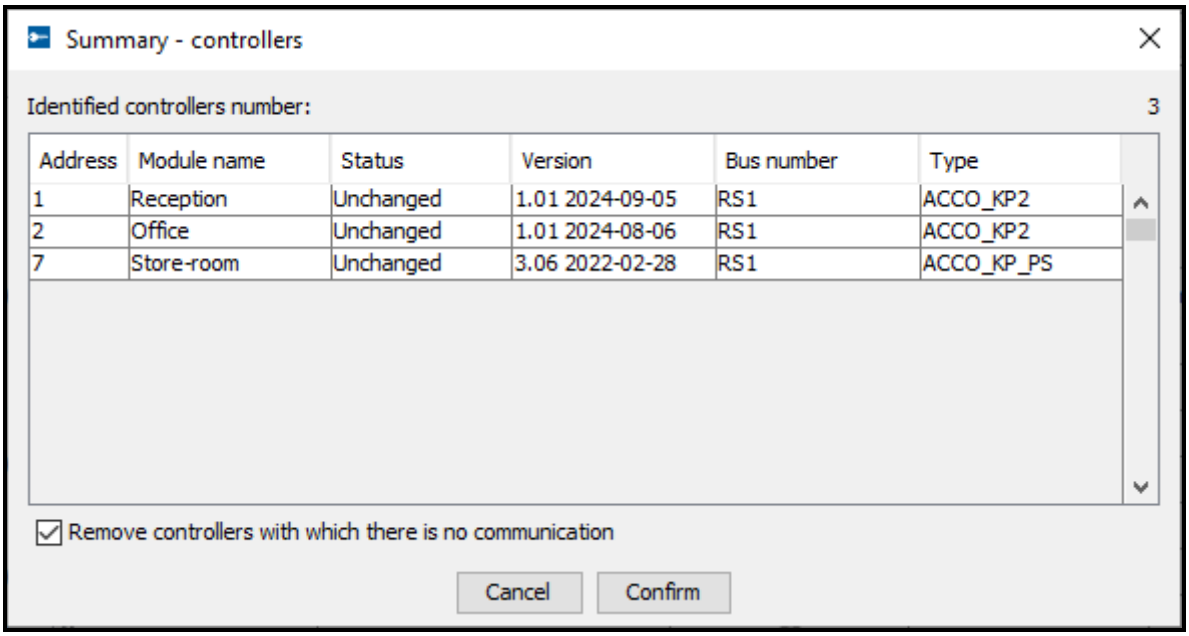


Fig. 17. “Summary – controllers” window displayed after completion of the controllers identification procedure.

Version – controller firmware version.

Bus number – number of RS-485 bus to which the identified controller is connected.

Type – model of controller.

Remove controllers with which there is no communication – if this option is enabled, the controllers communication with which could not be successfully established will be deleted after you click the “Confirm” button. If the option is disabled, clicking the “Confirm” button will not remove any controller.

Cancel – click to cancel the identification procedure.

Confirm – click to confirm the data read during identification.

4.2.5.2 Adding a controller before connecting it to the system

1. On the list of objects and control panels, highlight the control panel to which you want to add a controller.
2. Click the 

button.
3. In the window that will be displayed, select the module address and type, then click “Add”.
4. Configure and save the module settings.
5. After connecting a controller to the control panel (connected to the Ethernet network), click the  button. Select the “Find controllers” command.
6. In the window that will open, identification progress information will be displayed (you can click the “Get results” button to cancel the procedure).

7. The “Summary – controllers” window will be displayed (see: section ““Summary – controllers” window”). The controller will have the “Changed” status.
8. Click the “Confirm” button.
9. A window prompt will be displayed asking you whether to save the configuration. Click “Yes”.

4.2.5.3 Identification of OSDP devices connected to controllers

Each OSDP device must be identified so that the controllers can establish communication with it.

1. On the list of controllers, select the controllers to which OSDP devices are connected.
2. Click  . Select the “Find OSDP devices” command.
3. In the window that will open, identification progress information will be displayed.
4. After identification is completed, the “Summary – OSDP devices” window will be displayed (see: section ““Summary – OSDP devices” window”). The new devices will have the “New” status.
5. Click the “Confirm” button.
6. A window prompt will be displayed asking you whether to save the configuration. Click “Yes”.

Run the identification function each time a new OSDP device is connected to any of the controllers.

You cannot connect two devices with the same address. Before you connect a third-party OSDP device, remember to check its address and change it manually if necessary.

“Summary – OSDP devices” window

Identified OSDP devices – number of identified OSDP devices.

Controller Address – address of the controller to which the OSDP device is connected.

Serial number – serial number of the OSDP device.

Status – in the column, the following information can be displayed:

Unchanged – the OSDP device connected to the module is already in the system.

New – the OSDP device connected to the module is new.

Changed – data of the OSDP device connected to the module are not consistent with the program data.

No communication – failure to establish communication with the OSDP device that has previously been connected to the module.

Version – firmware version of the OSDP device.

Type – model of the OSDP device.

Remove OSDP devices with which there is no communication – if this option is enabled, the OSDP devices with which communication could not be established will be deleted after you click the “Confirm” button. If the option is disabled, the devices will remain in the system after you click the “Confirm” button.

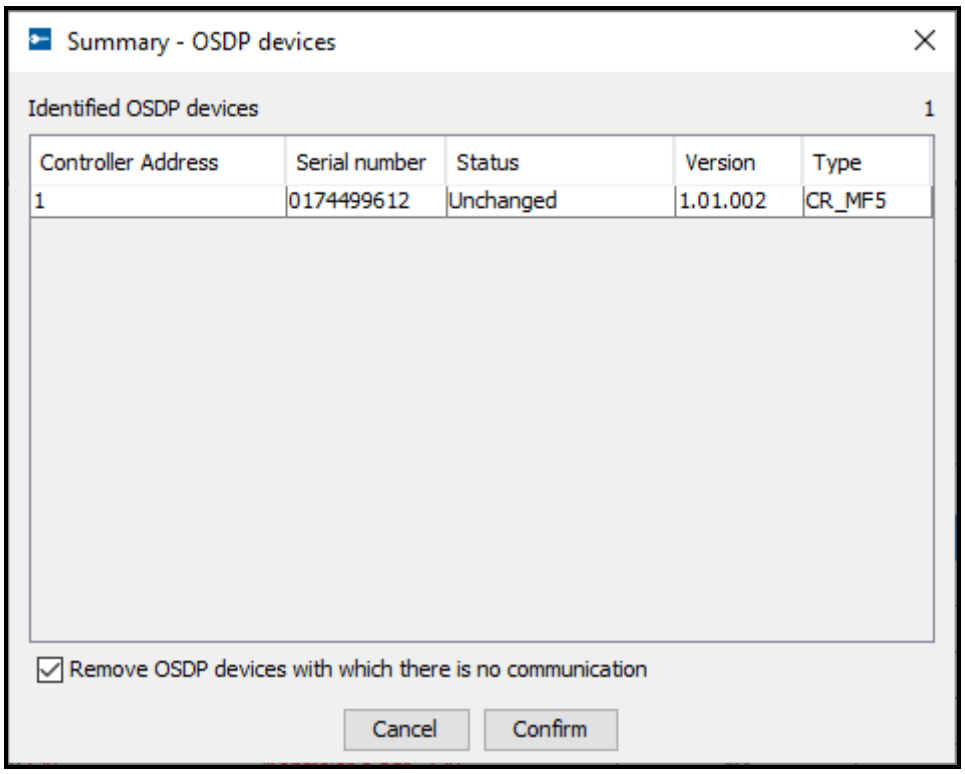


Fig 18. “Summary – OSDP devices” window displayed after completion of the OSDP devices identification procedure.

Cancel – click to cancel the identification procedure.

Confirm – click to confirm the data read during identification.

4.2.5.4 Table with the list of controllers

Address – controller address.

Name – individual controller name (up to 32 characters). The controller names can be presented in the following colors:

gray – controller added, but not saved yet;

red – controller saved; no communication with the controller;

black – controller saved; communication OK.

Status – icons to indicate the controller status.

– alarm / trouble (white exclamation mark on red background),

– alarm memory / trouble memory (white exclamation mark on gray background),

– everything OK (white symbol on green background),

– no communication with the control panel (white question mark on gray background).

Click the icon to display the “Status” tab.

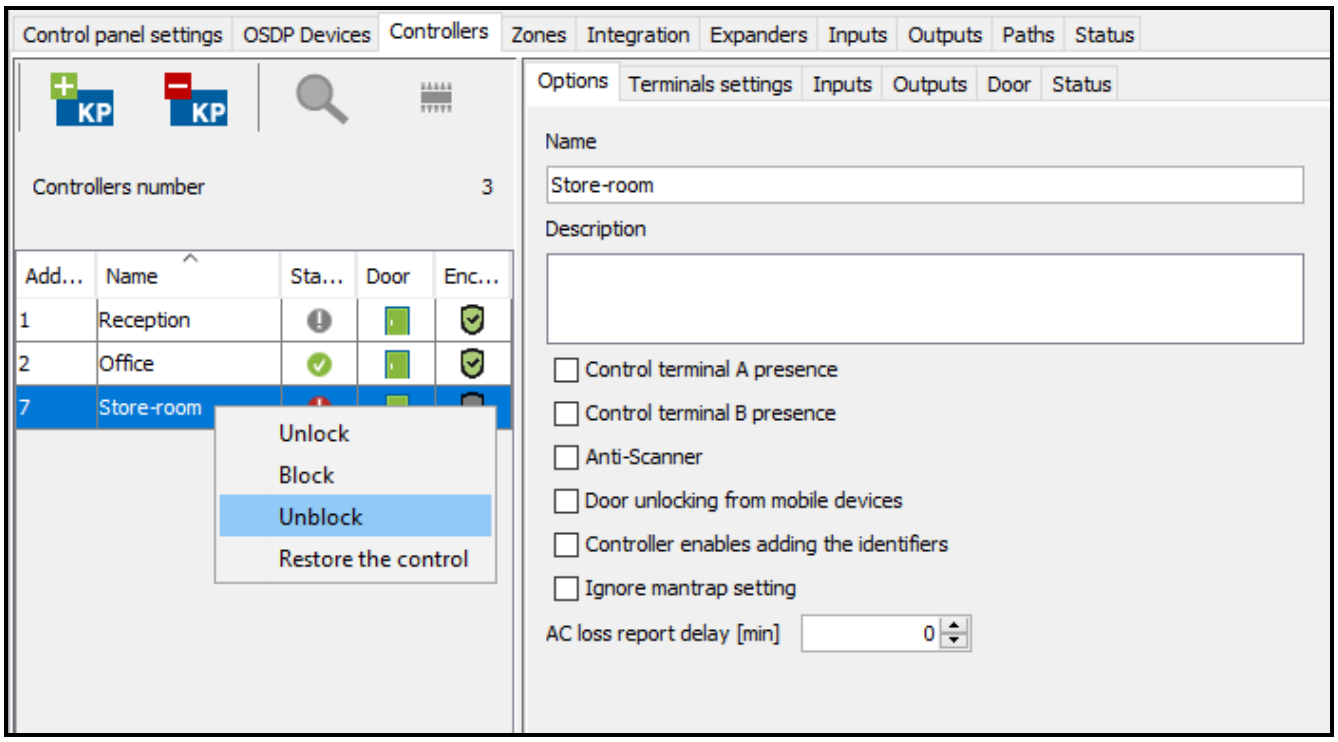


Fig. 19. List of controllers in the “Controllers” tab.

Door – icons to indicate the status of door supervised by the controller:

- – door blocked and closed (red door closed),
- – door blocked and open (red door half-open),
- – door blocked (alarm) and closed (red bell and red door closed),
- – door blocked (alarm) and open (red bell and red door half-open),
- – door controlled and closed (green door closed),
- – door controlled and open (green door half-open),
- – door unblocked and closed (blue door closed),
- – door unblocked and open (blue door half-open),
- – door unblocked (fire) and closed (red flame and blue door closed),
- – door unblocked (fire) and open (red flame and blue door half-open).

Encryption – icons to indicate the status of data encryption.

- – connection of the controller to OSDP terminals is not encrypted (black cross mark on red background),

  If the connection to both OSDP terminals A and B is not encrypted, the hint displayed when you hover the cursor over the icon will only mention that there is no encryption of connection to terminal A.

- – connection of the controller to the control panel is not encrypted (black minus sign on gray background),

  Encryption is not available for ACCO-KP controllers.

- – communication is encrypted (black check mark on green background).

Highlight the selected controller on the list and right click it to display the drop-down menu:

Unlock – click to unlock the door for the time preprogrammed in the "Access time" field, "Door" tab.

Block – click to permanently lock the door. The door will remain locked until its status is changed by a user having the "Switching" right (unless an event occurs that will otherwise change the door status).

Unblock – click to permanently unlock the door. The door will remain unlocked until its status is changed by a user having the "Switching" right (unless an event occurs that will otherwise change the door status).

Restore the control – click to restore the door control.

4.2.5.5 Programming the controller

Click the selected module on the list of controllers to program it. The module parameters will be displayed in the tabs in the window next to the list.

"Options" tab

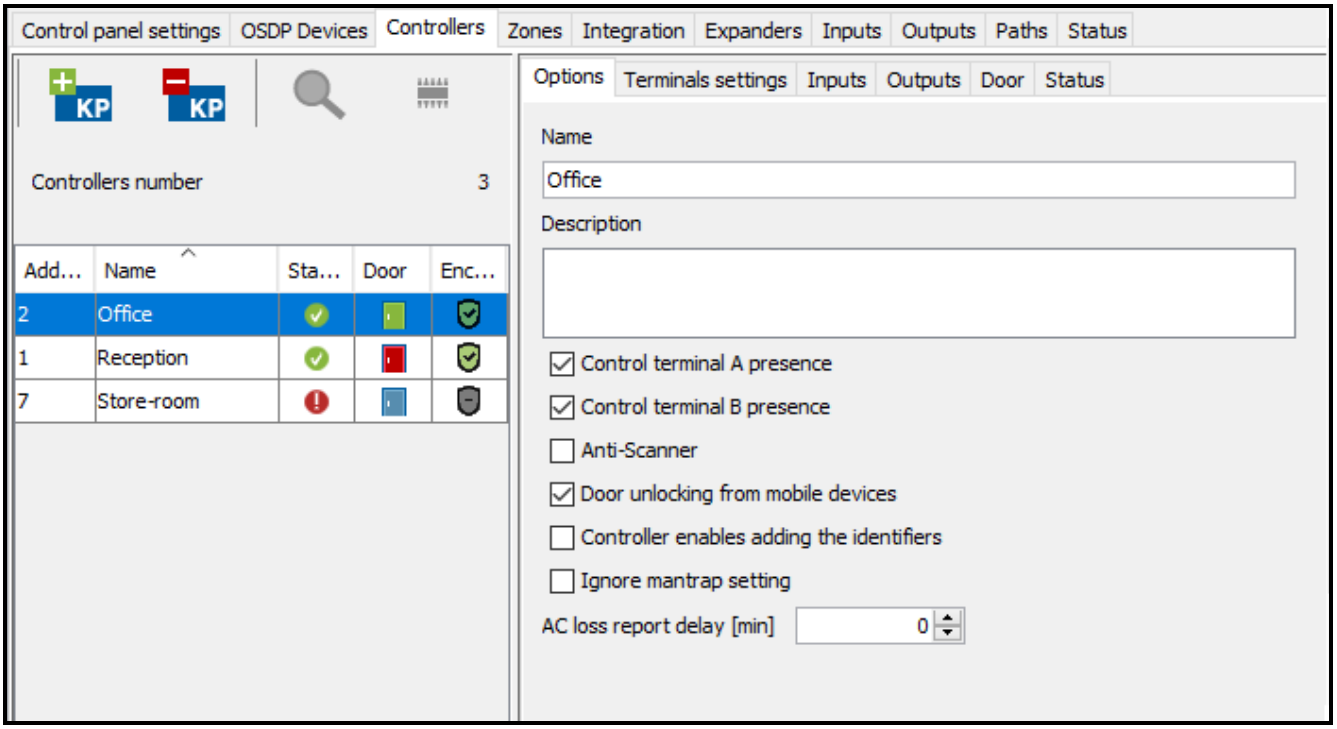


Fig. 20. "Options" tab.

Name – individual name of the controller (up to 32 characters).

Description – this field can be used for additional description of the controller.

Control terminal A / B presence – with the option enabled, the module checks presence of keypads and proximity card readers working as terminal A or B. The presence of keypads will be checked first, and only then the presence of proximity card readers. If this option is disabled, the module will in no way report a missing terminal (the alarm will not be generated, the event will not be saved and the "No terminal" output will not be activated).

The module is unable to verify the presence of DALLAS iButton readers. If you connect this type of reader, it is recommended that the "Control terminal A / B presence" option be not enabled.

Anti-Scanner – when this option is enabled, 5 attempts to get access on the basis of an unknown card, unknown iButton or code within 3 minutes will block the terminals for about 5 minutes.

Door unlocking from mobile devices – when this option is enabled, the door can be unlocked by the user from mobile devices.

Controller enables adding the identifiers – if this option is enabled, the controller will be displayed when adding a card to the user / checking a user's card in the ACCO Web application. If the option is disabled, the controller will not be shown (it does not apply to the modules to which readers supporting the DALLAS, EM Marin and Wiegand 40/42/56 formats are connected – these are shown at all times).

A card added on a reader supporting particular type of Wiegand format will be read only by the terminals supporting this format type, as well as by the terminals that can read shorter numbers of bits in the proximity card numbers. For example, if the card is added by means of a reader that supports the Wiegand 34 format, the card will be read by terminals supporting the Wiegand 34/32/26 formats. Therefore, it is advisable to add cards on terminals that can read the longest numbers of bits in the card numbers. If added in this way, the card can be handled by all readers in the system, including those that can read shorter numbers of bits in the proximity card numbers.

Ignore mantrap setting – if this option is enabled, the door in the zone acting as mantrap will operate regardless of the mantrap settings (see: description of “Mantrap” option).

AC loss report delay [min] – this function applies to the ACCO-KP-PS, ACCO-KPWG-PS and ACCO-KP2 modules. It makes it possible to define the time during which the module can do without the AC supply. After expiry of this time, a failure will be reported. The time is programmed in minutes and its maximum value is 255 minutes. Entering the value 0 means that the AC supply failure will not be reported.

Making any change will display the following buttons:

 – click to cancel the changes made.

 – click to confirm the changes made.

“Terminal settings” tab

“Terminal A / B” tab

Transmission format of terminal A / B – the format of data transmission used by terminals connected to the controller.

In the WIEGAND format, double-tapping the same card (identifier) on the reader is interpreted as holding the card. Not all readers will support this feature. Please check your readers for this functionality.

It is recommended that the SATEL’s CZ-EMM3 and CZ-EMM4 proximity card readers work in the EM Marin format.

In case of third-party OSDP devices, double-tapping the same card (identifier) on the reader is interpreted as holding the card.

Backlight of terminal A / B – the function that defines the rules of backlighting the keys and display in the keypads connected to the module. The following options are available:

- backlight off,
- automatic backlight (switched on by pressing any key or presenting the card),
- permanent backlight.

Terminal A / B tamper – if this option is enabled, the device controls the status of tamper protection (enclosure opening and removal from the wall). Option only for OSDP devices.

Volume of terminal A / B – level of sounds emitted by the device. Applies only to devices connected to the ACCO-KP2 modules.

Keys sounds of terminal A / B – if this option is enabled, pressing the keys is confirmed by a sound. Option only for OSDP devices.

Alternative door opening signal – if this option is enabled, granting access and opening the door is indicated by 4 short beeps and 1 long beep. Applies only to devices connected to the ACCO-KP2 modules.

OSDP device – serial number of the OSDP device that is to be used as terminal A / B. It is read after the device has been identified (see: section "Identification of OSDP devices connected to controllers"). Click the field and select the number of the device that is to serve as terminal A / B.

In case of SATEL devices, you will find the serial number on the label inside the device enclosure (marked as Satel MNI).

- if you click this button, all LEDs of the OSDP device with the selected serial number will start flashing. The flashing will stop after 5 minutes or if you click .

- if you click this button, all LEDs of the OSDP device with the selected serial number will stop flashing.

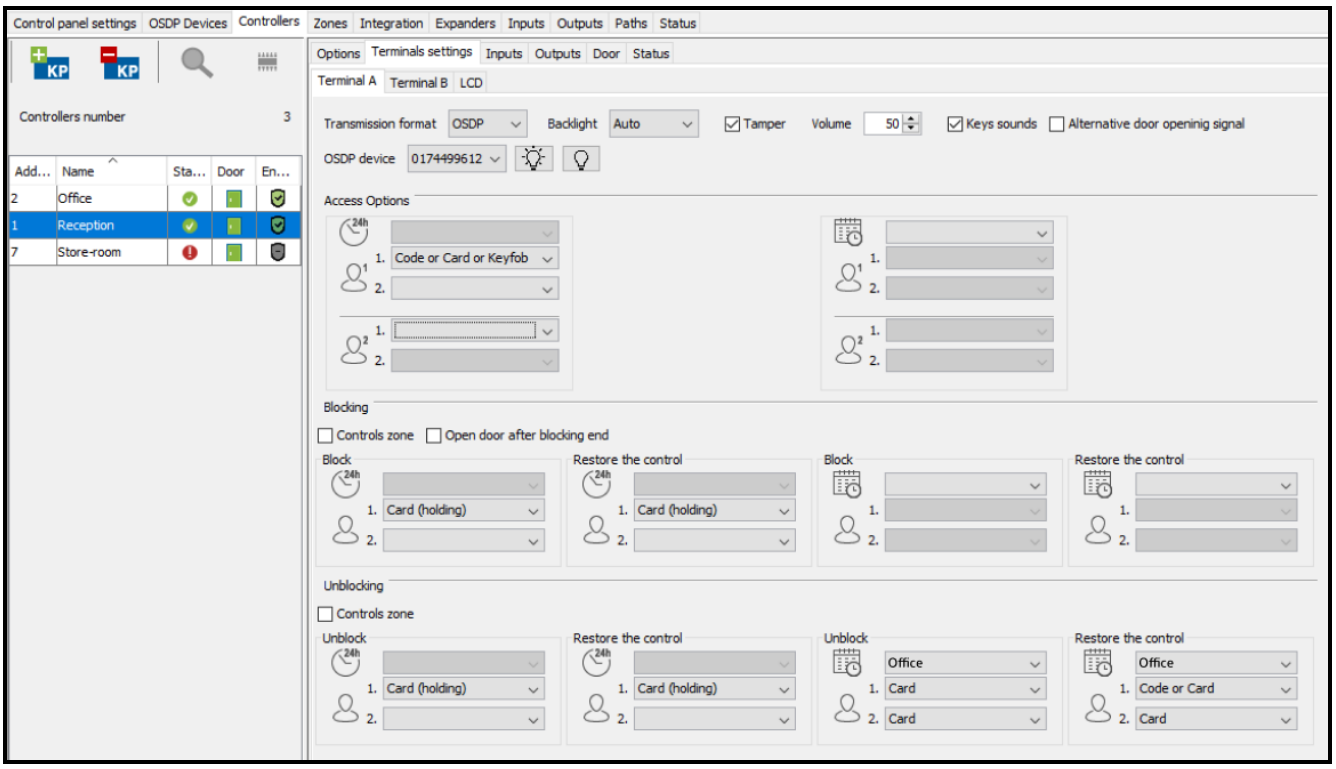


Fig. 21. "Terminal A" tab.

Access options

If the user is to have access to the given zone, the "Authorized to access" option must be enabled and suitable access calendar must be assigned in the ACCO Web application for the user (→"Users" →"List" →[user name] →"Zones" tab).

If access is to be granted based on two identifiers:

– *after using the first identifier, devices working as terminals will inform you that a second identifier is required (LCD keypad: by displaying a message; keypads and proximity card readers: by additional audible signaling – 3 short beeps),*

– the user is required to enter the second identifier within 30 seconds.

Configuration of the access options, as described in this section, is only possible for the ACCO-NT control panel firmware version 1.14.xxx or newer. For the control panels with an older firmware version, the existing identifier type which defines the method of access will be assigned to the first user for the terminal A according to the following rules:

– card = 1st identifier: card, 2nd identifier: unidentified,

– code = 1st identifier: code, 2nd identifier: unidentified,

– card and code = 1st identifier: code or card, 2nd identifier: code or card,

– card or code = 1st identifier: code or card, 2nd identifier: unidentified.

Configuration settings for the terminal B will not be available.

For the ACCO-NT control panel firmware version 1.14.xxx or newer, after the ACCO NET system is updated to version 1.7, the existing settings of access options will be assigned to the first user as valid around the clock for both terminals of the given controller and mapped as described above.

You can get or confirm access by using:

- code,
- card,
- keyfob,
- code or card,
- card or keyfob,
- code or keyfob,
- code or card or keyfob.

– access rules valid around the clock

If you define no access rules valid around the clock, access will be granted to the users based on the rules valid during the time period determined by the selected access calendar.

– user access rules:

1. – first identifier,

2. – second identifier (if not selected, the user will get access by using the first identifier).

– rules of access confirmation by the second user (define, if getting access is to be made dependent on the second user):

1. – first identifier,

2. – second identifier (if not selected, using the first identifier will be sufficient to confirm access).

The "Confirmation" option (→"Users" →"List" →[user name] →"Zones" tab) must be enabled in the ACCO Web application for the user which is confirming access.

– access rules valid during the time determined by access calendar

If you define no access rules valid during the time period determined by the access calendar, access will be granted based on the rules valid around the clock.

– click the field if, during the time determined by the access calendar, access is to be granted to the users based on rules other than around the clock. A list of access calendars created in the ACCO Web application will be displayed. Click one of them.

– user access rules:

1. – first identifier,

2. – second identifier (if not selected, the user will get access by using the first identifier).

– rules of access confirmation by the second user (define, if getting access is to be made dependent on the second user):

1. – first identifier,

2. – second identifier (if not selected, using the first identifier will be sufficient to confirm access).

The "Confirmation" option (→"Users" →"List" →[user name] →"Zones" tab) must be enabled in the ACCO Web application for the user which is confirming access.

Control options – Blocking

The control functions are implemented correctly only if one of the module inputs supervises the door status (is programmed as "Door status control").

If the user is to control a zone, he must have access to that zone as well as permission to switch its status (the "Authorized to access" and "Switching" options in the ACCO Web application (→"Users" →"List" →[user name] →"Zones" tab) must be enabled) and an access calendar assigned.

If the zone control is to take place based on two identifiers:

- *after using the first identifier, devices working as terminals will inform you that a second identifier is required (LCD keypad: by displaying a message; keypads and proximity card readers: by additional audible signaling – 3 short beeps),*
- *the user is required to enter the second identifier within 30 seconds.*

You must define identifiers to be used both for blocking the zone and restoring its control.

If:

- *the first identifiers for zone blocking are the same as the first identifiers for zone unblocking and/or*
- *the first identifiers for restoring control in the blocked zone are the same as the first identifiers for restoring control in the unblocked zone,*

how the zone status changes depends on the door status. If the door is closed, using the identifier will block the zone or restore control in the blocked zone. If the door is open, using the identifier will unblock the zone or restore control in the unblocked zone.

Configuration of the blocking options, as described in this section, is possible for the ACCO-NT control panel firmware version 1.14.xxx or newer. For control panels with an older firmware version, blocking the doors and zones as well as restoring their control will be possible based on the same rules that were valid for the 1.5 version of the system.

For the ACCO-NT control panel firmware version 1.14.xxx or newer, after the ACCO NET system is updated to version 1.7 and higher, the present settings of the cone control options will be mapped in the new system. If the "Block the zone after holding the card" option was enabled so far, after the system update, the "Controls zone" option will be enabled for all entry terminals in that zone.

You can block a zone or restore control in it by using:

- code,
- card,
- card (holding),
- code or card,
- card (presenting or holding),
- code or card (holding),
- code or card (presenting or holding).

Controls zone – after enabling this option, you can block the zone and restore control in it by means of the entry terminal in that zone. In the case of integration, blocking a zone of the access control system by using the entry terminal will arm the integrated partition of the alarm system.

Open door after blocking end – if this option is enabled and the user will restore control of the door or zone (with the "Controls zone" option enabled), he will get access to the door.

– rules of zone blocking valid around the clock

If you define no zone blocking rules valid around the clock, zone blocking will be possible based on the rules valid during the time period determined by the selected access calendar.

– rules of zone blocking by the user:

1. – first identifier,

2. – second identifier (if not selected, the user will block the zone by using the first identifier).

– rules of restoring control in a blocked zone valid around the clock

If you define no rules for restoring control in a blocked zone, which are valid around the clock, it will be possible to restore control in the zone based on the rules valid during the time period determined by the selected access calendar.

– rules of restoring control in a blocked zone by the user:

1. – first identifier,

2. – second identifier (if not selected, the user will restore control in the blocked zone by using the first identifier).

– rules of zone blocking during the time determined by access calendar

If you define no zone blocking rules valid during the time period determined by the access calendar, zone blocking will be possible based on the rules valid around the clock.

– click the field if, during the time determined by the access calendar, the zone is to be blocked based on other rules than around the clock. A list of access calendars created in the ACCO Web application will be displayed. Click one of them.

– rules of zone blocking by the user:

1. – first identifier,

2. – second identifier (if not selected, the user will block the zone by using the first identifier).

– rules of restoring control in the blocked zone during the time determined by access calendar

If you define no rules of restoring control in the blocked zone valid during the time determined by the selected access calendar, it will be possible to restore control in the zone based on the rules valid around the clock.

– click the field if, during the time determined by access calendar, control in the blocked zone is to be restored based on rules other than around the clock. A list of access calendars created in the ACCO Web application will be displayed. Click one of them.

– rules of restoring control in a blocked zone by the user:

1. – first identifier,

2. – second identifier (if not selected, the user will restore control in the blocked zone by using the first identifier).

Control options – Unblocking

The control functions are implemented correctly only if one of the module inputs supervises the door status (is programmed as "Door status control").

If the user is to control a zone, he must have access to that zone as well as permission to switch its status (the "Authorized to access" and "Switching" options in the ACCO Web application (→"Users" →"List" →[user name] →"Zones" tab) must be enabled) and an access calendar assigned.

If the zone control is to take place based on two identifiers:

– *after using the first identifier, devices working as terminals will inform you that a second identifier is required (LCD keypad: by displaying a message; keypads and proximity card readers: by additional audible signaling – 3 short beeps),*

– *the user is required to enter the second identifier within 30 seconds.*

You must define identifiers to be used both for unblocking the zone and restoring its control.

If:

– *the first identifiers for zone unblocking are the same as the first identifiers for zone blocking and/or*

– *the first identifiers for restoring control in the unblocked zone are the same as the first identifiers for restoring control in the blocked zone,*

how the zone status changes depends on the door status. If the door is open, using the identifier will unblock the zone or restore control in the unblocked zone. If the door is closed, using the identifier will block the zone or restore control in the blocked zone.

Configuration of the unblocking options, as described in this section, is possible for the ACCO-NT control panel firmware version 1.14.xxx or newer. For control panels with an older firmware version, unblocking the doors and zones as well as restoring their

control will be possible based on the same rules that were valid for the 1.5 version of the system.

For the ACCO-NT control panel firmware version 1.14.xxx or newer, after the ACCO NET system is updated to version 1.7 and higher, the present settings of the zone control options will be mapped in the new system. If the "Block the zone after holding the card" option was enabled so far, after the system update, the "Controls zone" option will be enabled for all entry terminals in that zone.

You can unblock a zone or restore control in it by using:

- code,
- card,
- card (holding),
- code or card,
- card (presenting or holding),
- code or card (holding),
- code or card (presenting or holding).

Controls zone – after enabling this option, you can unblock the zone and restore control in it by means of the entry terminal in that zone.

 – rules of zone unblocking valid around the clock

If you define no zone unblocking rules valid around the clock, zone unblocking will be possible based on the rules valid during the time period determined by the selected access calendar.

 – rules of zone unblocking by the user:

1. – first identifier,

2. – second identifier (if not selected, the user will unblock the zone by using the first identifier).

 – rules of restoring control in unblocked zone valid around the clock

If you define no rules of restoring control in unblocked zone valid around the clock, it will be possible to restore control in the zone based on rules valid during the time period determined by the selected access calendar.

 – rules of restoring control in the unblocked zone by the user:

1. – first identifier,

2. – second identifier (if not selected, the user will restore control in the unblocked zone by using the first identifier).

 – rules of zone unblocking during the time determined by access calendar

If you define no rules of zone unblocking valid during the time determined by access calendar, it will be possible to unblock the zone based on the rules valid around the clock.

 – click the field if during the time determined by access calendar the zone is to be unblocked based on rules other than around the clock. A list of access calendars created in the ACCO Web application will be displayed. Click one of them.

– rules of zone unblocking by the user:

1. – first identifier,

2. – second identifier (if not selected, the user will unblock the zone by using the first identifier).

– rules of restoring control in the unblocked zone during the time determined by access calendar

If you define no rules of restoring control in the unblocked zone valid during the time determined by the selected access calendar, it will be possible to restore control in the zone based on the rules valid around the clock.

– click the field if during the time determined by access calendar restoring control in the unblocked zone is to take place based on rules other than around the clock. A list of access calendars created in the ACCO Web application will be displayed. Click one of them.

– rules of restoring control in the unblocked zone by the user:

1. – first identifier,

2. – second identifier (if not selected, the user will restore control in the unblocked zone by using the first identifier).

Examples

An example of defining access options

The selected access calendar entitles users to access from 8:00 to 16:00. During this time, the user will get access by using two identifiers: 1st – code and 2nd – card. The second user will confirm access also by using two identifiers: 1st – keyfob and 2nd – code or card. In the remaining hours (until 8:00 and from 16:00, when the selected calendar does not apply), the user will get access by using two identifiers: 1st – card and 2nd – card, and the second user will confirm access also by using two identifiers: 1st – code and 2nd – card or keyfob.

In the hours between 8:00 and 16:00, the user will get access if:

- he enters and confirms the code using the # or OK button, then taps the card on the reader,
- the user authorized to confirm will use the keyfob, then enter the code and confirm it with the # or OK button or tap the card on the reader.

Between 16:00 and 8:00, the user will gain access if:

- he taps two cards on the reader,
- the user authorized to confirm will enter the code and confirm it with the # or OK button, then he will tap the card on the reader or use the keyfob.

An example of defining the options of zone blocking and restoring control in the blocked zone

The selected access calendar entitles users to control the zone from 6:00 to 18:00. During this time, the user will block the zone by using two identifiers: 1st – code and 2nd – card, and will restore control in the blocked zone by using: 1st – card and 2nd – code or card. In the remaining hours (until 8:00 and from 16:00, when the selected calendar does not apply), the user will block the zone by using two identifiers: 1st – card (holding) and 2nd – code, and will restore control in the blocked zone by using one identifier: 1st – card.

Between 6:00 and 18:00, the user will block the zone if he enters the code and confirms it with the # or OK button, and then taps the card on the reader. Control in the blocked zone will be restored if the user taps the card on the reader, then enters the code and confirms it with the # or OK button, or taps the card on the reader.

Between 18:00 and 6:00, the user will block the zone if he holds the card near the reader for about 3 seconds, then enters the code and confirms it using the # or OK button. Control in the blocked zone will be restored if the user taps the card on the reader.

An example of defining the options of zone unblocking and restoring control in the unblocked zone

The selected access calendar entitles users to control the zone from 10:00 to 14:00. During this time, the user will unblock the zone by using one identifier: 1st – card, and will restore control in the unblocked zone by using: 1st – code. In the remaining hours (until 10:00 and from 14:00, when the selected calendar does not apply), the user will unblock the zone using one identifier: 1st – code, and will restore control in the unblocked zone by using: 1st – card (holding).

Between 10:00 and 14:00, the user will unblock the zone if he taps the card on the reader. Control in the unblocked zone will be restored if the user enters the code and confirms it with the # or OK button.

Between 14:00 and 10:00, the user will unblock the zone if he enters the code and confirms it using the # or OK button. Control in the unblocked zone will be restored if the user holds the card near the reader for about 3 seconds.

An example of controlling a zone with two doors

Fig. 22. An example of access control system zone.

Legend to Fig. 22:

1 (number on gray background) – access control system zone.

D1 – controller assigned to zone 1. Terminal A is entry into zone 1, and terminal B is exit from zone 1.

D2 – controller assigned to zone 1. Terminal A is entry into zone 1, and terminal B is exit from zone 1.

ZONE BLOCKING

If you want to block zone 1:

- if there is an entry terminal in the zone for which the “Controls zone” option is enabled, use this terminal.

If you block in this way an access control zone integrated with an alarm system partition, you will arm the alarm system partition.

- if there is no entry terminal in the zone for which the “Controls zone” option is enabled, block all doors.

ZONE UNBLOCKING

If you want to unblock zone 1:

- if there is an entry terminal in the zone for which the “Controls zone” option is enabled, use this terminal;
- if there is no entry terminal in the zone for which the “Controls zone” option is enabled, unblock all doors.

If the zone is integrated with with an alarm system partition which is armed, you cannot unblock either the zone or the doors by using the terminals.

RESTORING CONTROL IN THE ZONE

If you want to restore control in the blocked / unblocked zone 1:

- if there is an entry terminal in the zone for which the “Controls zone” option is enabled, use this terminal.
- if there is no entry terminal in the zone for which the “Controls zone” option is enabled, restore control in all doors.

“LCD” tab

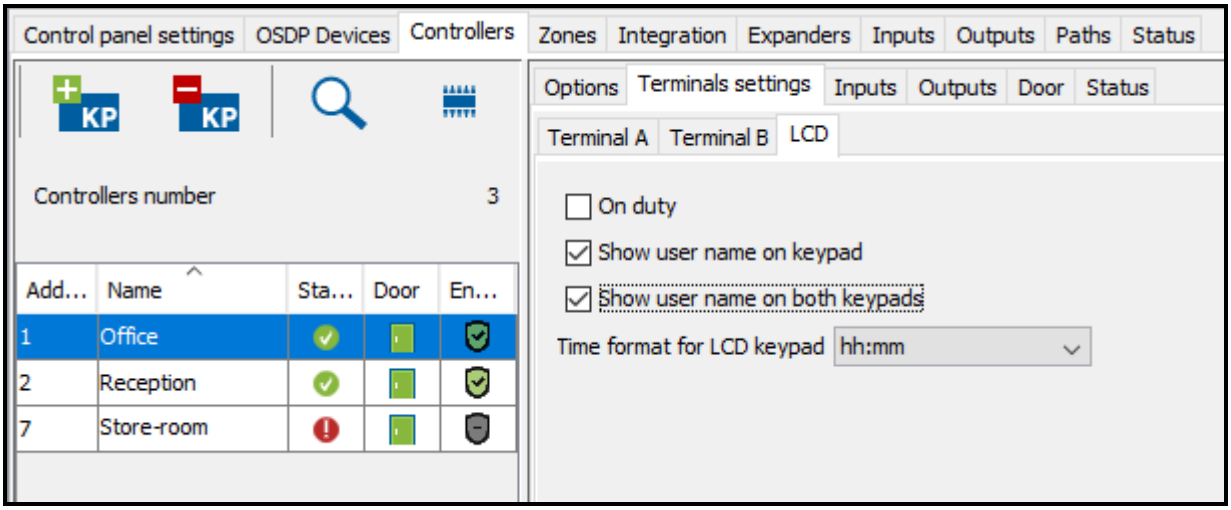


Fig. 23. “LCD” tab.

On duty – if this option is enabled, the “On duty” message will be displayed after access is granted. If the entry / exit is connected with business duties, the user should press the ▲ key. The message will be displayed on the keypad until the user presses the key or unlocks the door. Suitable information will then be added to the event details. This information is useful, if the user passes registered by the door module are to help in determining the work time of the users.

The function will not be executed, if the door status is not controlled or the door is open.

Show user name on keypad – if this option is enabled, the name of the user who unlocked the door will be displayed on the LCD keypad by means of which the door was unlocked.

Show user name on both keypads – if this option is enabled, the name of the user who unlocked the door will be displayed on both LCD keypads connected to the controller. Enabling the option enables the “Show user name on keypad” option at the same time.

Time format for LCD keypad – the function makes it possible to choose how the time and date will be displayed on the keypad screen.

Making any change will display the following buttons:

– click to cancel the changes made.

– click to confirm the changes made.

“Inputs” tab

Table with the list of controller inputs

Number – controller input number.

Input type (see: section “Controller input types”)

Wiring type – you can select:

NO – the input handles device having NO (normally open) type output,

NC – the input handles device having NC (normally closed) type output.

Parameter only available for programmable inputs.

Sensitivity [ms] – time during which the input status must be changed to be registered. This time can be programmed within the range from 10 ms to 2.55 s. Parameter only available for programmable inputs.

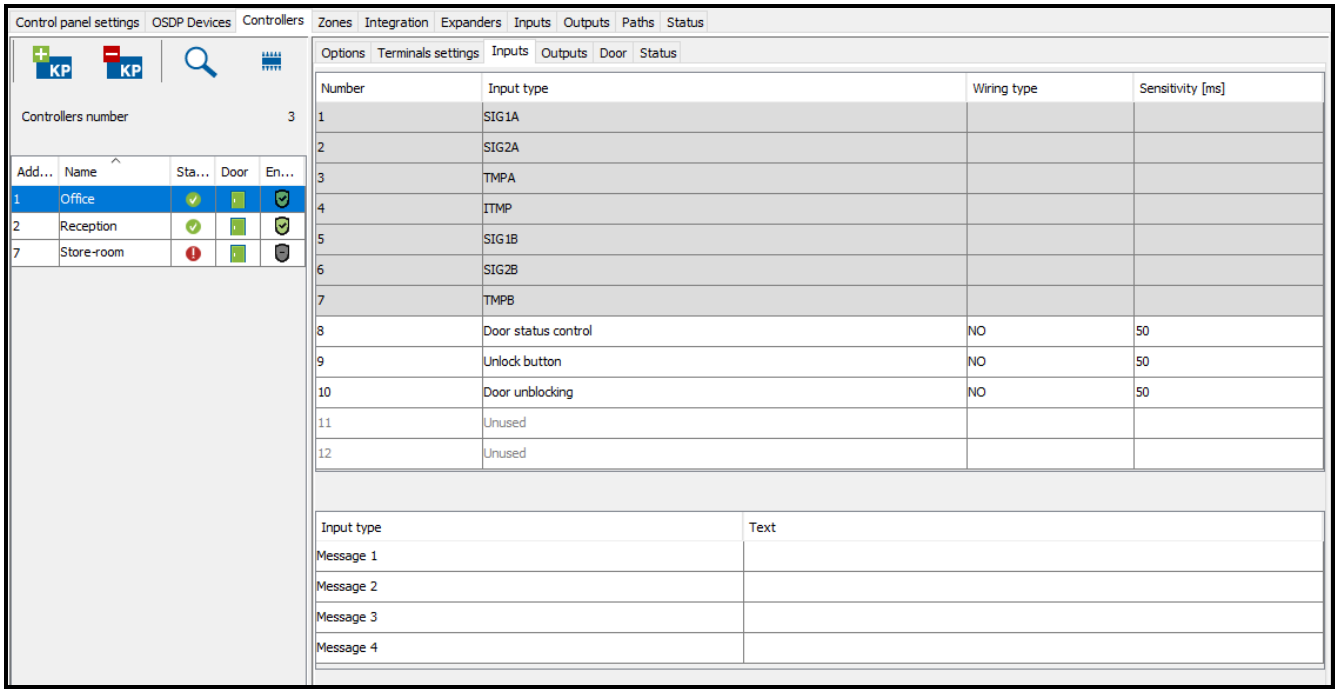


Fig. 24. “Inputs” tab.

Controller input types

To select the type for programmable inputs, right-click the field assigned to the input:

Unused

Door status control – control of the door status.

The door status control, i.e. connecting a sensor to the input programmed as “Door status control” is necessary for correct execution of all the functions of access control.

Unlock button – unlocks the door.

Door unblocking – permanently unlocks the door. The door will stay unlocked as long as the input is active (unless another event occurs which will otherwise change the door status).

Door blocking – permanently locks the door. The door will stay locked as long as the input is active (unless another event occurs which will otherwise change the door status).

Interlocking door control – status control of the other doors, forming a mantrap or airlock. In the mantrap / airlock configuration, only 1 door can be open.

Fire – unblock door – permanently unlocks the door in case of fire. The door will remain unlocked until normal status of the input is restored. The door can only be switched over by a user having the "Switching" permission.

Alarm – block door – permanently locks the door in case of alarm. The door will remain locked until its status is changed by using a code or holding the card for a moment near the reader by a user having the "Switching" permission. The time during which the input will be active has no effect on the door blocking time.

Bell signal – activates the "Bell signal" type of outputs.

Message 1÷4 – generating a preprogrammed event. You can define its content in the bottom table.

Events programmed for the "Message 1÷4" input type are not global. They need to be defined individually for each controller.

In the ACCO-KP2 module, some input types are fixed and cannot be changed:
SIG1A – connecting terminal A: data (0),
SIG2A –connecting terminal A: data (1),
TMPA – terminal A presence control,
ITMP – connecting tamper circuit,
SIG1B – connecting terminal B: data (0),
SIG2B – connecting terminal B: data (1),
TMPB – terminal B presence control.

"Outputs" tab

Table with the list of controller outputs

Number – controller output number.

Output type (see: section "Controller output types").

Cut-off time – if the output is to be turned on for a period of time, the time must be defined. After the time has expired, the output will be turned off. You can program from 1 to 120 seconds or minutes (0 is available for the ACCO-KP2 module for some output functions). Parameter only available for programmable outputs.

in min / sec – select, whether the cut-off time is to be counted in seconds or minutes. Parameter only available for programmable outputs.

Polarity – the option defines how the output will operate. In the event of reversed polarity, in active state:

- the output is disconnected from the common ground,
- the NO terminal of relay output is opened, and the NC terminal closed.

Parameter only available for programmable outputs.

Controller output types

To select the output type, right-click the field:

Unused

Door status – provides information on the current status of the door (if the door status is supervised by the "Door status control" module input) It is activated with opening of the door and remains active until the door is closed. The output configured as "Door status" cannot perform other functions.

Indicator – after you select this type, the following functions available for the output will be displayed next to the table:

Door opening – is activated for the programmed time period after opening the door (if the door status is supervised by the "Door status control" module input).

Bell signal – becomes active for the programmed time period after signal is supplied to the input programmed as "Bell signal".

F1 – OSDP device A / B – is active when the F1 (SO-MF5) or (CR-MF5) function key of the A / B terminal is pressed.

The "F1 – OSDP device A / B" function applies only to the SO-MF5 / CR-MF5 keypad connected to the controller using the RS-485 bus.

F2 – OSDP device A / B – is active when the F2 (SO-MF5) function key of the A / B terminal is pressed.

The "F2 – OSDP device A / B" function applies only to the SO-MF5 keypad connected to the controller using the RS-485 bus.

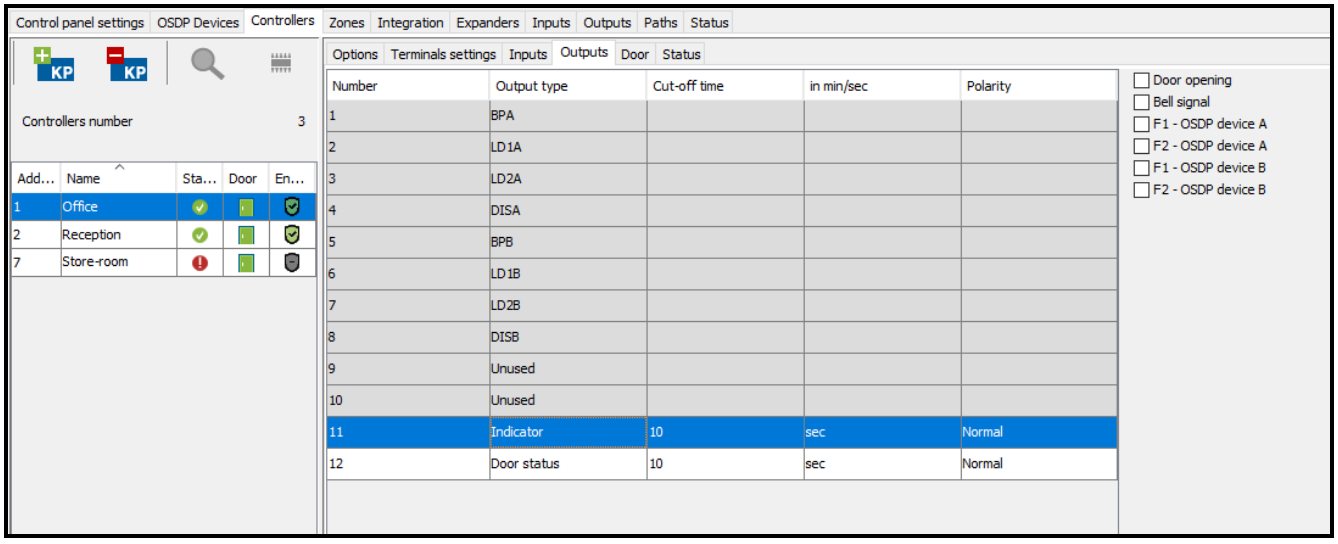


Fig. 25. "Outputs" tab.

Failure – after you select this type, the following functions available for the output will be displayed next to the table:

Forced entry – becomes active for a programmed time period after unauthorized opening of the door, when the door is locked (if the door status is supervised by the "Door status control" module input).

Long open door – becomes active for a programmed time period, if the door remains open after expiry of the "Door open time" (if the door status is supervised by the "Door status control" module input). In case of the ACCO-KP2 modules, if you set 0 as the cut-off time, the output will be active until the door is closed.

No terminal – becomes active for a programmed time period, if no terminal (LCD keypad, keypad or proximity card reader) has been found during the test. The module controls presence of terminals only when corresponding options are enabled ("Control terminal A / B presence").

Failed access attempts – becomes active for a programmed time period, after 5 attempts to read an unregistered proximity card, unregistered DALLAS iButton or enter an

unknown code have taken place. The input is activated irrespective of whether the "Anti-Scanner" option is enabled or not.

AC supply failure – becomes active, if the time programmed as "AC loss report delay" has elapsed since the AC supply was lost by the ACCO-KP-PS / ACCO-KPWG-PS / ACCO-KP2 module, and the supply has not been restored. The output remains active until the AC supply is restored.

Low battery – becomes active, if the voltage of battery connected to the ACCO-KP-PS / ACCO-KPWG-PS / ACCO-KP2 module drops below 11 V for a period of time longer than 12 minutes (3 battery tests). The output remains active until the battery voltage rises above 11 V for a period of time longer than 12 minutes (3 battery tests).

Tamper – activates, if the ITMP input is activated.

Access from terminal – after you select this type, the functions which the output is able to execute will be displayed next to the table:

Access from terminal A / B – activates, if the authorized user gets access to the door using the A / B reader.

In the ACCO-KP2 module, some output functions are fixed and cannot be changed:
BPA – reader A sound control,
LD1A – reader A green LED control,
LD2A – reader A red LED control,
DISA – disabling reader A operation,
BPB – reader B sound control,
LD1B – reader B green LED control,
LD2B – reader B red LED control,
DISB – disabling reader B operation.

"Door" tab

Terminals – information on which exit / entry zone has been assigned to the module terminal A / B is displayed in tabular form.

Relay off when door open – if this option is enabled, the relay controlling the door activation device will be switched off as soon as the door is opened.

Relay off when door closed – if this option is enabled, the relay controlling the door activation device will be switched off as soon as the open door is closed.

If none of the options determining the moment of switching the relay off is enabled, the relay will only be switched off after expiry of the "Access time".

In the following cases the relay will be switched off after expiry of the "Access time", despite enabling one of the options which determine the moment of switching the relay off:

- *none of the inputs informs about the door status (the door status monitoring sensor has not been installed),*
- *the "Door status control disabled" option is enabled,*
- *the user has got access, but has not opened the door.*

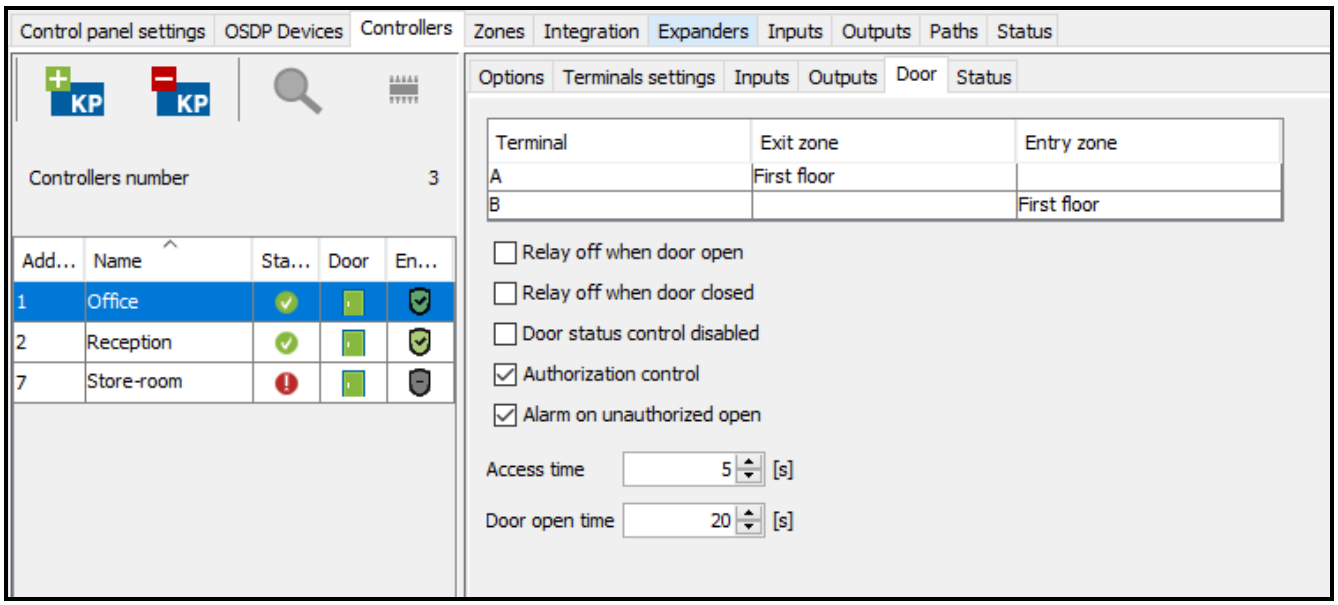


Fig. 26. “Door” tab for the selected controller.

Door status control disabled – enabling this option is recommended if no information on the door status can reach the module (the status sensor has got damaged or, for some reason, has not been connected). This will prevent generating wrong events. When the option is enabled:

- getting access is recognized as equivalent to opening the door (an event will be generated to inform you about the door having no door status control),
- some events are not generated (e.g. events informing about forced opening of the door, long open door, etc.),
- the “On duty” option is disabled,
- the door in the zone acting as mantrap will operate regardless of the mantrap settings (see: description of “Mantrap” option).

The “Door status control disabled” option is to be only enabled in emergency situations, since it seriously affects functionality of the access control.

Authorization control – if the option is enabled, opening the door without authorization will generate a “Forced entry” event.

Alarm on unauthorized open – if the option is enabled, opening the door without authorization will generate alarm and a “Forced entry” event.

Access time – the time period for which the relay is turned on after getting access to make opening the door possible. In case of the ACCO-KP modules, it can be programmed within the range of 1 to 60 seconds. In case of the ACCO-KP2 modules, you can set values within the range of 1 to 300 seconds.

Door open time – the time during which the door can remain open after the relay is switched off. If the door stays open longer than for the specified time, the corresponding event will be generated. Additionally, the output programmed as “Long open door” will be activated. In case of the ACCO-KP modules, the time can be programmed within the range of 1 to 60 seconds. In case of the ACCO-KP2 modules, you can select a value within the range of 0 to 3600 seconds. If you set 0, the time will not be counted.

Making any change will display the following buttons:

X – click to cancel the changes made.

– click to confirm the changes made.

“Status” tab

If there is no communication between the control panel and the controller, information on absence of communication between the devices will be displayed, as well as the date and time of the last transmission from the controller received by the control panel.

Door status – current status of the door:

- Door controlled,
- Door blocked,
- Door unblocked,
- Unknown (no communication with the controller).

Power supply – current value of controller supply voltage.

Firmware version – controller firmware version (version number and build date).

Communication quality – current percent ratio between the amount of data sent (from control panel to module) to the amount of data received (from module to control panel).

Module type – model of controller.

Alarms – the following statuses are presented by means of icons: “Module tamper”, “Terminal A tamper”, “Terminal B tamper”, “Failed access attempts”, “Forced entry” and “Long open door”.

Failures – the following statuses are presented by means of icons: “Clock failure”, “No terminal A” and “No terminal B”.

Power failures – the following statuses are presented by means of icons: “No battery”, “Low battery” and “No AC power”.

Emergency Alarms – the following statuses are presented by means of icons: “Fire” and “Alarm”.

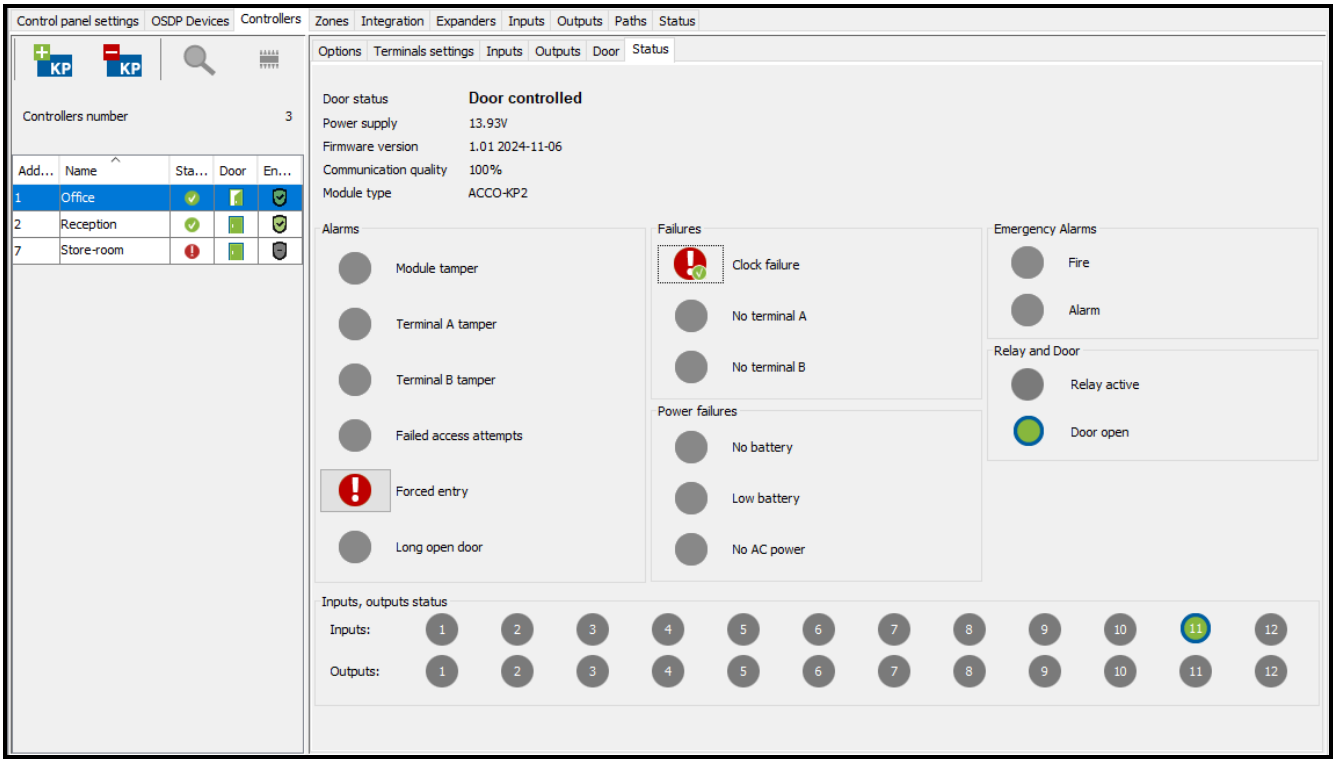


Fig. 27. “Status” tab.

The icons indicate the following status:

– no alarm / trouble (gray background).

– alarm / trouble (white exclamation mark on red background).

– confirmed alarm / confirmed trouble (white exclamation mark on red background and white symbol on green background).

– alarm memory / trouble memory (white exclamation mark on gray background).

– confirmed alarm / trouble memory (white exclamation mark on gray background and white symbol on green background).

– no status information (white question mark on gray background).

You can confirm troubles, alarms and emergency situations. If you want to confirm a trouble / alarm, click the button next to it.

Relay and Door – the following statuses are presented by means of icons: “Relay active” and “Door open”.

Inputs, outputs – status of inputs and outputs is presented by means of icons.

The icons indicate the following status:

– active relay / door open / active input / active output (green background with blue border).

– inactive relay / door closed / inactive input / inactive output (gray).

– unknown status (white question mark on gray background).

4.2.5.6 Remote update of the controller firmware

1. If you want to update the firmware of access control module(s), highlight the selected module(s) in the table with the list of controllers.
2. Click  and select the “Update controllers” command.
3. A window will be displayed with the available firmware version and a table with controller data (see Fig. 28).

Data on the controller firmware version will be indicated by the following colors:

***gray** – unknown version of controller firmware;*

***black** – outdated version of controller firmware;*

***green** – current version of controller firmware;*

***red** – invalid language version of controller firmware.*

Click  *to check if there are new controller firmware versions available on the SATEL server.*

4. Click the “Update” button.
5. A window will open with names of the controllers whose firmware will be updated. Click the “OK” button.

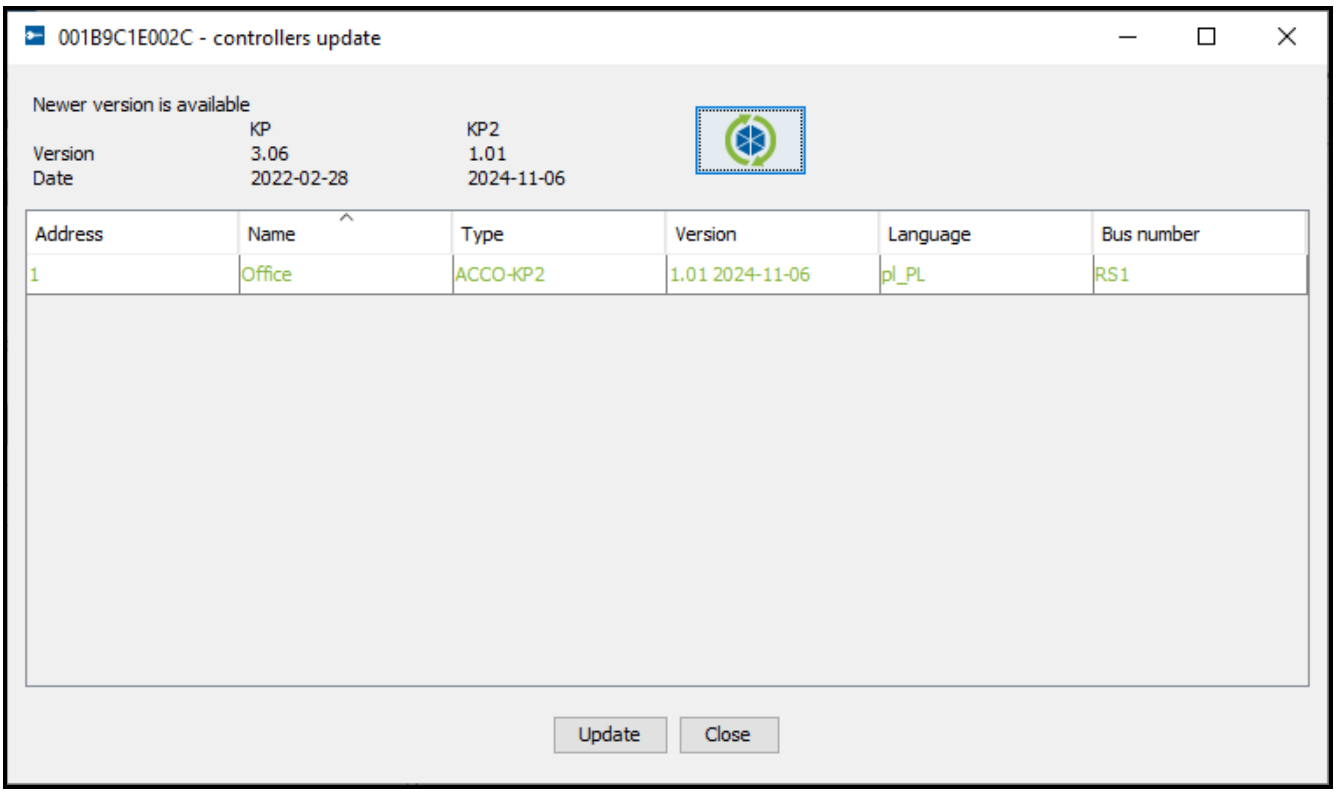


Fig. 28. Controller firmware update window.

6. This will start the firmware update process.

During remote update of the ACCO-KP access control module firmware, the other modules connected to the control panel are working in the offline mode (for description, please refer to the manual of ACCO-NT access control panel).

If any problems arise, an appropriate message will be displayed to inform you about this fact. You will have to rerun the update procedure.

7. When the update is successfully completed, an appropriate message will be displayed. Click “OK” and then “Close”.

4.2.5.7 Remote update of the OSDP device

1. If you want to update the firmware of OSDP device(s), in the table with the list of controllers select the module(s) to which the devices are connected.
2. Click  and select the “Update OSDP devices” command.
3. A window will be displayed with the available firmware version and a table with OSDP device data (see: Fig. 29).

Data on the OSDP devices will be indicated by the following colors:

***gray** – unknown version of OSDP device firmware;*

***black** – outdated version of OSDP device firmware;*

***green** – current version of OSDP device firmware.*

Click  *to check if there are new firmware versions of OSDP devices available on the SATEL server.*

4. Click the “Update” button.

5. A window will open with names of the OSDP devices whose firmware will be updated. Click the “OK” button.

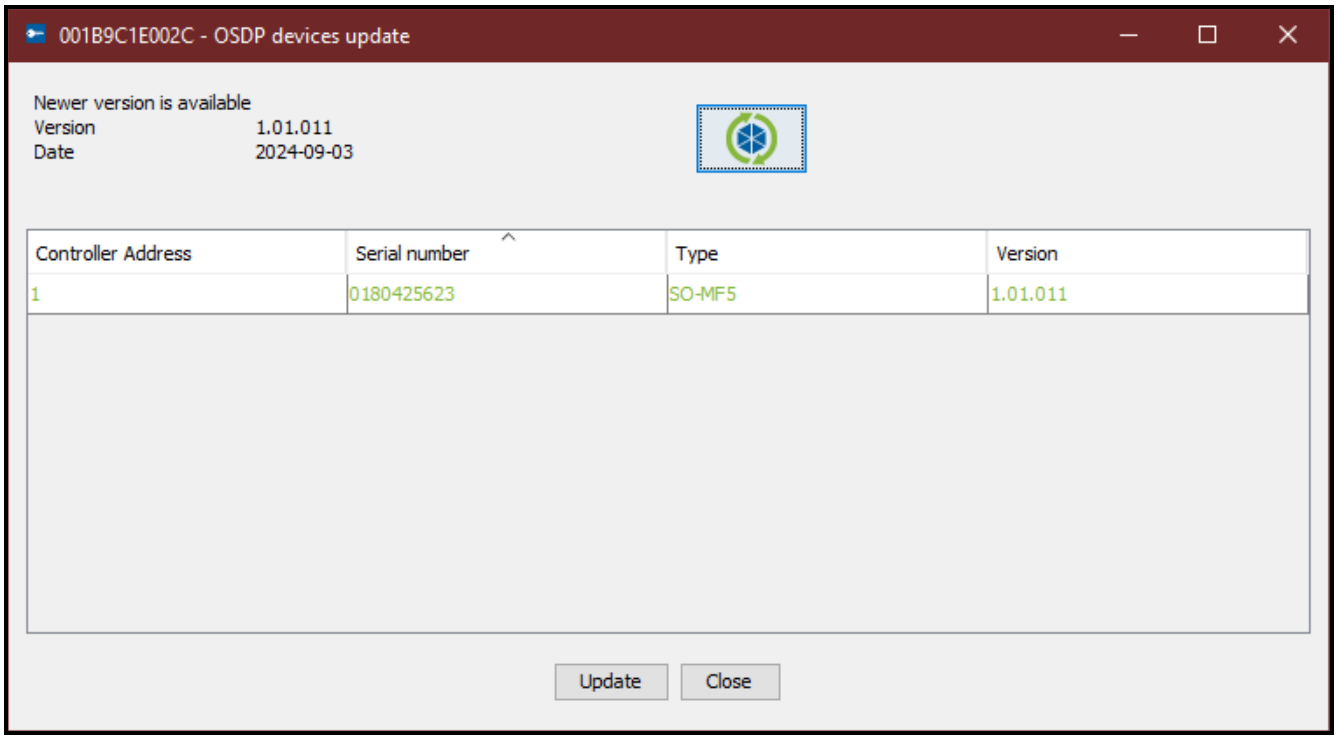


Fig. 29. OSDP device firmware update window.

6. This will start the firmware update process.

If any problems arise, an appropriate message will be displayed to inform you about this fact. You will have to rerun the update procedure.

7. When the update is successfully completed, an appropriate message will be displayed. Click “OK” and then “Close”.

4.2.5.8 Deleting a controller

1. If you want to delete a single controller, use the cursor to highlight the selected controller in the table with the list of controllers.
2. If you want to delete two or more controllers at once, use the cursor to highlight one of the controllers and, holding down the Ctrl key, select the next ones, highlighting them with the left mouse button.
3. If you want to delete all controllers at the same time, use the cursor to highlight one of the controllers and press the Ctrl+A keys simultaneously.
4. Click the 

button.
5. When a prompt appears asking you whether to delete the controller / controllers, click “Yes”.
6. Save the changes made.

4.2.6 Zones

The zone is a separated area in the protected premises. Division into zones makes it easier for the Administrator to manage the access control system.

Description of the buttons

 - click to add a zone.

 - click to delete the highlighted zone (see: section “Deleting a zone”).

Under the buttons, the number of zones is displayed. Hovering your cursor over the number will display information on the number of zones created in the program for the selected ACCO-NT control panel.

4.2.6.1 Creating a zone

1. Highlight a control panel on the list of objects and control panels.
2. Click the  button. The new zone will appear in the table.

4.2.6.2 Table with a list of zones

No. – number of the zone.

Zone – individual name of the zone (up to 32 characters). The zone names can be presented in the following colors:

gray – zone to which no controllers are assigned;

black – zone with assigned controllers.

Status – information on the current state of the zone:

Reading status,

Zone controlled,

Zone unblocked,

Zone blocked,

Armed,

Entry delay (entry delay time in progress in the integrated alarm system partition),

Exit delay < 10 s (exit delay time in progress in the integrated alarm system partition and there is less than 10 seconds left until it expires),

Exit delay > 10 s (exit delay time in progress in the integrated alarm system partition and there is more than 10 seconds left until it expires),

Mixed (doors supervised by controllers assigned to the zone have different statuses),

Alarm in the zone,

Fire in the zone,

Unknown (before saving the created zone),

Unavailable (wrong version of ACCO-NT firmware).

Number of users – number of people currently staying in the zone.

After you highlight a zone or several zones on the list and right click it / them, the drop-down menu will be displayed:

Unlock – click to unlock doors supervised by all controllers assigned to the selected zone / zones.

Block – click to permanently lock all doors in the zone.

Unblock – click to permanently unlock all doors in the zone.

If a module is assigned to two or more zones, blocking or unblocking the zone will, respectively, block or unblock the module controlled door in the other zones.

Restore the control – click to restore the door control in the zone.

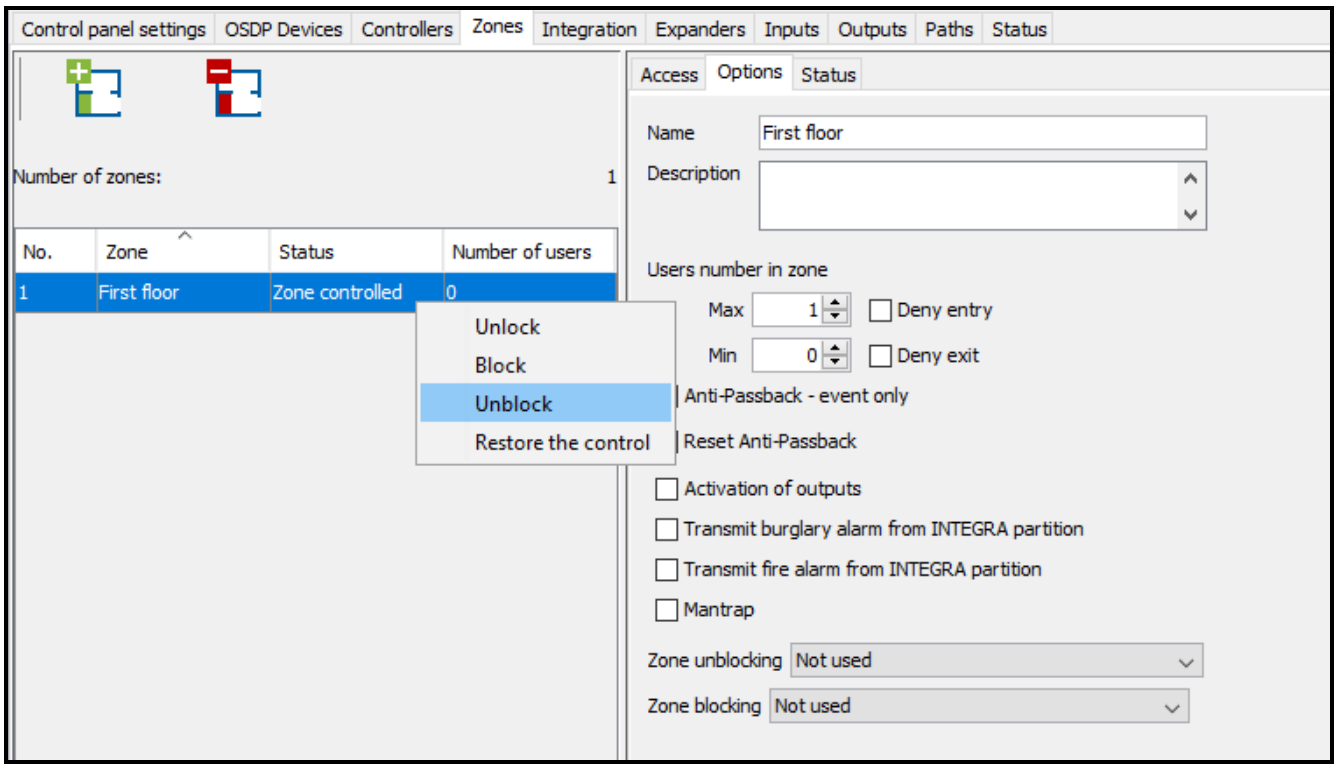


Fig. 30. List of zones in the “Zones” tab.

4.2.6.3 Programming the zones

Click the selected zone on the list of zones to program it. Parameters of the zone will be displayed in the “Access” and “Options” tabs.

Zone parameters

“Access” tab

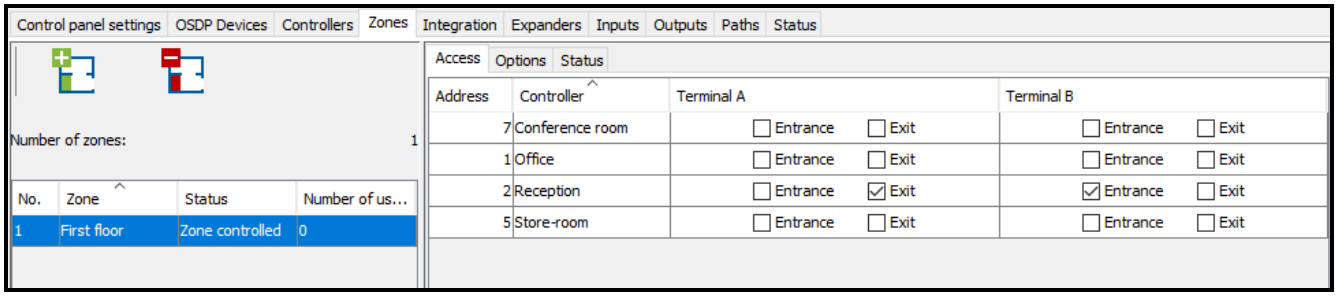


Fig. 31. “Access” tab.

Address – controller address.

Controller – controller name.

Terminal A / B – the terminal can control the zone entrance or the zone exit.

“Options” tab

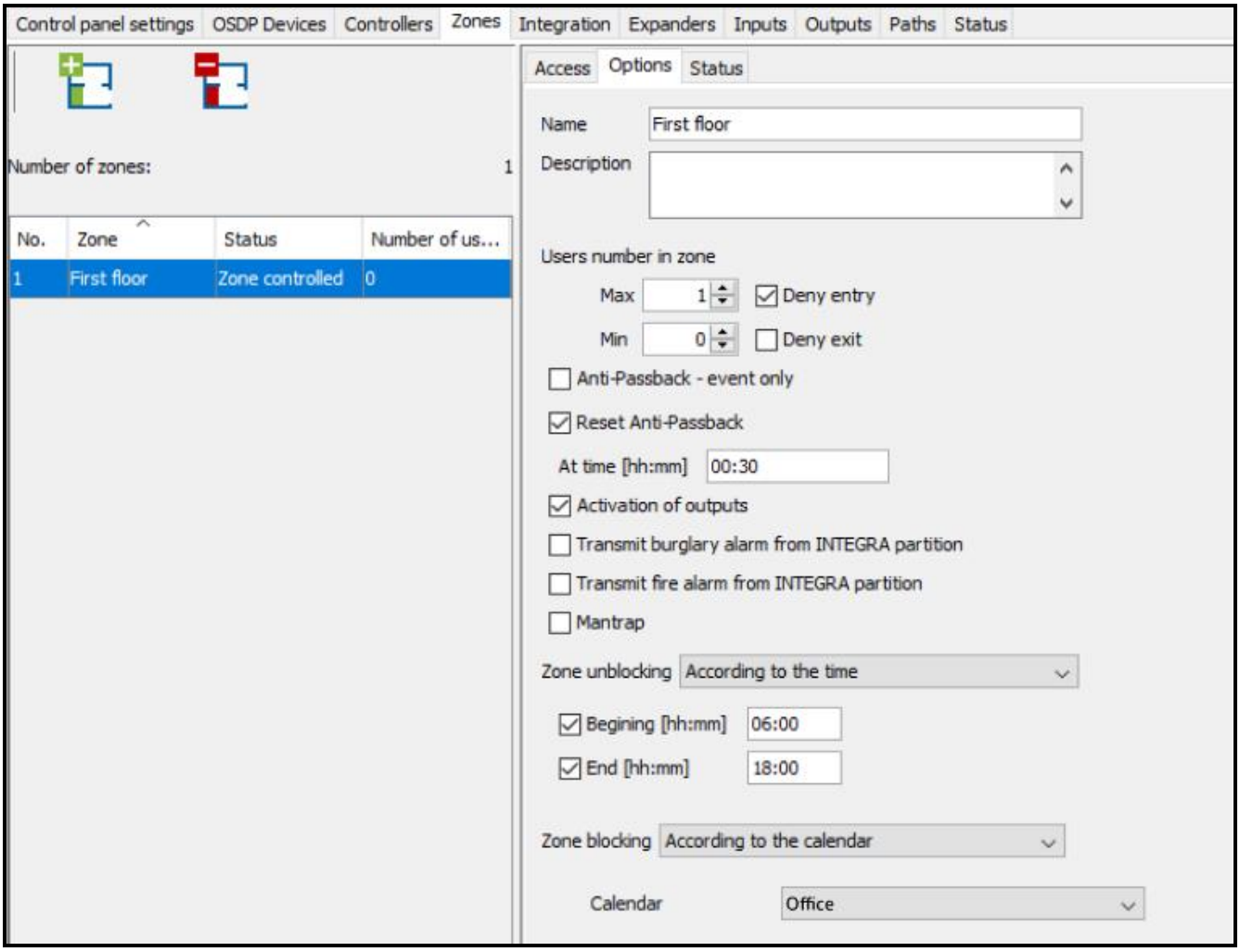


Fig. 32. “Options” tab.

Name – individual name of the zone (up to 32 characters).

Description – this field can be used for additional description of the zone.

Users number in zone

Max – this field defines the maximum number of users who can stay in the zone at the same time. You can program values from 1 to 8000. To edit the number, click the field (use the keypad to enter the value or select it with arrow keys). If the value of minimum number of users in the zone exceeds the maximum value, the value of maximum number of users in the zone will be automatically increased by 1 above the value of minimum number of users in the zone.

Deny entry – with this option enabled, the users cannot get access to the zone, if the maximum number of users stay in the zone.

Enabling the “Deny entry” option for the zone will have no impact on behavior of the “Indicator of max. users in zone” type of output associated with this zone.

Min – this field defines the minimum number of users who should stay in the zone at the same time. You can program values from 0 to 7999. To edit the number, click the field (use the keypad to enter the value or select it with arrow keys). If the value of the maximum number of users in the zone is lower than the minimum value, the value of minimum number of users in the zone will be automatically decreased by 1 below the value of maximum number of users in the zone.

Deny exit – with this option enabled, the users cannot leave the zone, if the minimum number of users stay in the zone.

Enabling the "Deny exit" for the zone will have no impact on behavior of the "Indicator of min. users in zone" type of output associated with this zone.

Anti-Passback – event only – if this option is enabled, effect of the Anti-Passback feature is limited to logging to memory the events of multiple user's pass in the same direction.

Reset Anti-Passback – checking the option will activate the "At time [hh:mm]" field where you can define the time of resetting the "Anti-Passback" function. The users whose exit from the zone was not registered will be able to get access to the zone after the specified hour.

Activation of outputs – if this option is enabled, the zone can control the outputs of the "Activation by access" type.

Transmit burglary alarm from INTEGRA partition – check the box, if the burglary alarm generated in an integrated partition of the alarm system is to permanently lock (block) the doors in the access control system zone. This option applies to the ACCO NET system integration with the alarm system (see section "Integration").

Transmit fire alarm from INTEGRA partition – check the box, if the fire alarm generated in an integrated partition of the alarm system is to permanently unlock (unblock) the doors in the access control system zone. This option applies to the ACCO NET system integration with the alarm system (see section "Integration").

Mantrap – if this option is enabled, the zone works as the mantrap, which means that only 1 door can be open in the zone. If any one of the doors in the zone is open, the users will not be able to open the other doors. This does not apply to the doors with the "Ignore mantrap setting" or "Door status control disabled" options enabled.

The zone can work as the mantrap if the door status is supervised (a sensor is connected to the module input programmed as "Door status control").

The administrator has access to the doors in the zone acting as mantrap regardless of the mantrap settings.

Zone unblocking – you can select whether the zone is to be unblocked according to the time (defined in the "Begining [hh:mm]" and "End [hh:mm]" fields), or according to the access calendar (you can select the calendar from the drop-down list in the "Calendar" field, provided that a calendar has been created in the ACCO Web application).

Zone blocking – you can select whether the zone is to be blocked according to the time (defined in the "Begining [hh:mm]" and "End [hh:mm]" fields), or according to the access calendar (you can select the calendar from the drop-down list in the "Calendar" field, provided that a calendar has been created in the ACCO Web application).

Making any change will display the following buttons:

 – click to cancel the changes made.

 – click to confirm the changes made.

“Status” tab

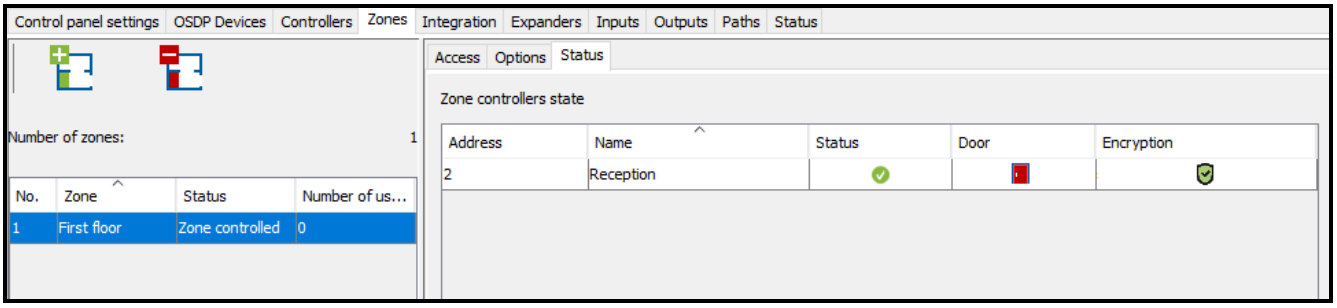


Fig. 33. “Status” tab.

The table displays the current states of controllers assigned to the zone.

Address – controller address.

Name – individual controller name.

Status – icons to indicate the controller status. For description of the icons denoting the device status, refer to section “Table with the list of controllers”.

Door – icons to indicate the status of door supervised by the controller. For description of the icons denoting the door status, refer to section “Table with the list of controllers”.

Encryption – icons to indicate the status of data encryption. The icons are described in the “Table with the list of controllers” section.

4.2.6.4 Deleting a zone

1. If you want to delete a single zone, use the cursor to highlight the required zone in the table containing the list of zones.
2. If you want to delete two or more zones at once, use the cursor to highlight one of the zones and, holding down the Ctrl key, select the next ones, highlighting them with the left mouse button.
3. If you want to delete all the zones at the same time, use the cursor to highlight one of the zones and press the Ctrl+A keys simultaneously.
4. Click the  button.
5. You will be asked if you want to delete the zone / zones. Click “Yes”.
6. Save the changes made.

You cannot delete a zone to which controllers are assigned.

4.2.7 Integration

The ACCO NET system can be integrated with the alarm systems based on INTEGRA or INTEGRA Plus alarm control panels (firmware version 1.17 or newer) via the Ethernet network. The ETHM-1 Plus module (firmware version 2.03 or newer) or ETHM-1 (firmware version 1.07 or newer) must be connected to the alarm control panel. Communication takes place through the GUARDX communication channel.

ACCO NET uses the same port for communication with the alarm control panel as e.g. GUARDX, INTEGRA Control or INTEGRUM. If ACCO NET is connected to the alarm control panel, establishing connection with the control panel from other programs via the same Ethernet module is impossible.

ACCO Server is responsible for connectivity and data exchange between the systems.

Integration makes it possible to simultaneously control the zones of access control system and the partitions of alarm system. You can create 255 zones in one ACCO-NT control panel. One alarm control panel can support up to 32 partitions. You can assign one ACCO NET

system zone to one partition of the alarm system. You can integrate all or just some of the zones, while the other zones of the ACCO NET system may work independently.

4.2.7.1 Configuring the alarm system

For information on how to configure the alarm control panel and the Ethernet module, please refer to the manuals of respective devices.

Settings of the alarm control panel

In the alarm control panel:

- program the “ACCO identifier” – identifier of communication between the systems (DLOADX program →“Communication” →“Connection settings”).

Communication identifiers in the alarm control panel and the DLOADX and ACCO Soft programs (“Integration” tab →selected alarm system →“Configuration” tab →“ACCO identifier” field) must be identical.

Described below are cases in which arming the system from the alarm control panel may be subject to some restrictions. If

- “Grade 2 / 3” option is enabled:
  - in the alarm system: the system can only be armed as required by the EN 50131 standard – for Grade 2 / 3, respectively; in the ACCO Web application, additional information will be seen in the events,
  - in the access control system: the zone can be blocked at all times,
- time for the “Blocked for guard round” parameter is defined and the “Guard” type user has used code / identifier:
  - in the alarm system: the armed partition is temporarily blocked for a preset period of time; in the ACCO Web application, additional information will be seen in the events,
  - in the access control system: the zone status is “Armed”,
- the user of “Blocking partition” type has used code / identifier:
  - in the alarm system: the armed partition is temporarily blocked for a period of time individually preset for that user; in the ACCO Web application, additional information will be seen in the events,
  - in the access control system: the zone status is “Armed”,
- “With temporary block” partition type is defined, “Default block time” option is enabled, time in the “Default part. block time” is defined:
  - in the alarm system: after arming, the partition is blocked for time defined by the installer,
  - in the access control system: the zone can be blocked; the alarm control panel partition is blocked automatically for the time defined by the installer, which can only be seen in the DLOADX program.
- “With temporary block” partition type is defined:
  - in the alarm system: after arming, the partition is blocked for the time defined by the user,
  - in the access control system: the zone can be blocked; the alarm control panel partition is not temporarily blocked,

When the alarm system partition is blocked, it can only be disarmed by a user with the "Access temporary blocked part" right. In the access control system, the user can only restore control in the zone by using an entry terminal for which the "Controls zone" option is enabled, if he/she:

- *has the "Switching" right,*
- *has access to the given zone, according to the access calendar assigned to the user.*

- global arming-related options are preset:
  - in the alarm system: partition can be armed, if there isn't any problem preventing the system from being armed – depending on the status of zones, outputs, existing troubles in the alarm system,
  - in the access control system: the zone can be blocked at all times.

Settings of the Ethernet module (ETHM-1, ETHM-1 Plus)

In the Ethernet module:

- enable the "GUARDX" and "GSM conn." options so that connection to the ACCO NET system via TCP/IP network can be established;
- preset the number of TCP port that will be used for communication with the ACCO NET system, if it is to be different from 7091 ("Port" field);
- program the key (a string of up to 12 alphanumeric characters – digits, letters and special characters) for encrypting the data during communication with the ACCO NET system ("GUARDX/Java key" field).

Description of buttons

 - click to add an alarm system.

 - click to remove the selected alarm system (see section "Deleting an alarm system").

Next to the buttons, a number in the x/y format is displayed, where x is the number of alarm systems integrated for the ACCO-NT control panel, and y is the maximum number of the alarm systems that can be supported by the ACCO-NT control panel (see section "Licences").

Colors have the following meaning:

– black – the maximum number of alarm systems for the given ACCO-NT control panel has not been exceeded yet,

– red – the maximum number of alarm systems for the given ACCO-NT control panel has been exceeded.

4.2.7.2 Adding an alarm system

1. Select the control panel on the list of objects and control panels.
2. Click the  button. The new alarm system will appear in the table.

4.2.7.3 Table with the list of alarm systems

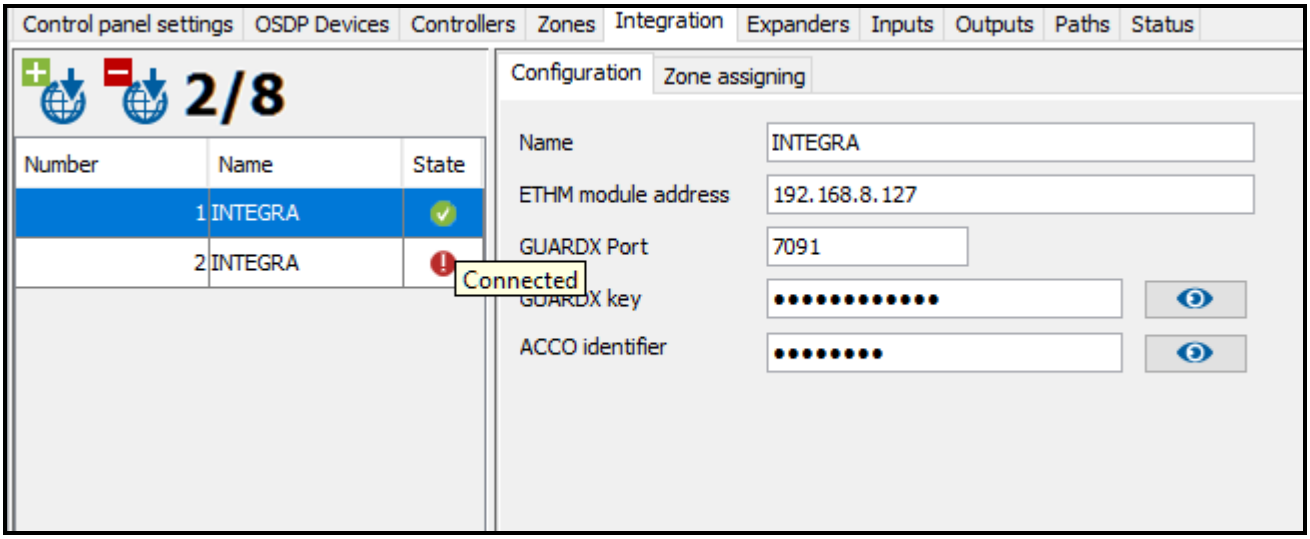


Fig. 34. Table with the list of systems in the “Integration” tab.

The table presents the list of alarm systems integrated with the ACCO NET system.

Number – number of the alarm system.

Name – name of the alarm system.

State – icons to indicate the status of communication between alarm systems and ACCO NET:

– communication not working properly; hovering the cursor over the icon will display the status description: “Busy”, “Disconnected”, “Incorrect GUARDX key”, “INTEGRA limit exceeded” or “Wrong connection configuration” (white exclamation mark on red background),

– communication between ACCO Server and Ethernet module working properly; hovering the cursor over the icon will display the “Connected” status (white symbol on green background),

– data not saved to database; hovering the cursor over the icon will display the “Unknown” status (white symbol on gray background).

4.2.7.4 Configuring the integration settings

Click the selected alarm system to configure the settings related to its integration with ACCO NET. The data will be displayed in the “Configuration” and “Zone assigning” tabs.

“Configuration” tab

Name – name of the alarm system in the ACCO NET system.

ETHM module address – IP address of the Ethernet module connected to the INTEGRA control panel.

GUARDX Port – number of TCP port used for communication between ACCO NET and alarm control panel.

GUARDX key – a string of up to 12 alphanumeric characters (digits, letters and special characters) for encryption of data during communication between the ACCO NET system and the control panel. Click to see the sequence of characters.

ACCO identifier – identifier for the purposes of ACCO NET system integration with alarm control panel. It consists of 8 digits. Click to see the sequence of characters.

Making any change will display the following buttons:

 – click to cancel the changes made.

 – click to confirm the changes made.

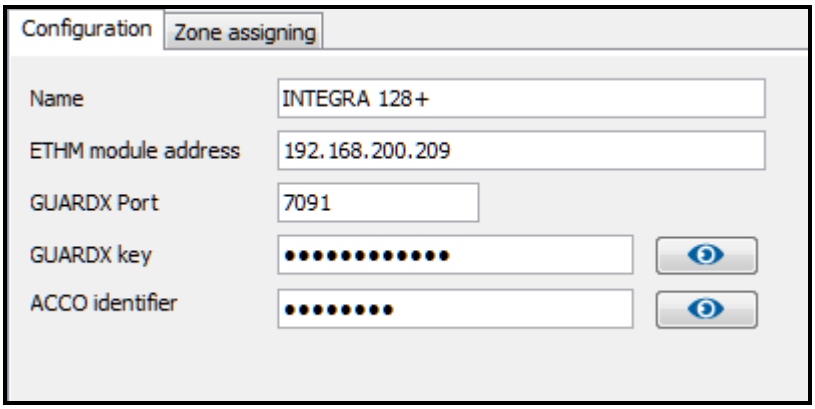


Fig. 35. “Configuration” tab.

“Zone assigning” tab

Show all – select this option, if all alarm system partitions are to be displayed in the table with zones. Their number depends on the control panel type. If the option is disabled, the table only shows alarm system partitions created in the given system, automatically read from the alarm control panel memory after establishing communication between the systems.

No. – number.

Partition – INTEGRA – name of the alarm system partition.

Zone – ACCO – name of the access control system zone which is integrated with the alarm system partition.

4.2.7.5 Assigning zones

1. In the “Zone – ACCO” column, right-click the field corresponding to the alarm system partition.
2. When the list of available zones of the ACCO NET system opens, click the zone you want to assign. Name of the selected zone will be displayed in the field.
3. Do the same to assign other ACCO NET system zones.
4. Save the changes made.

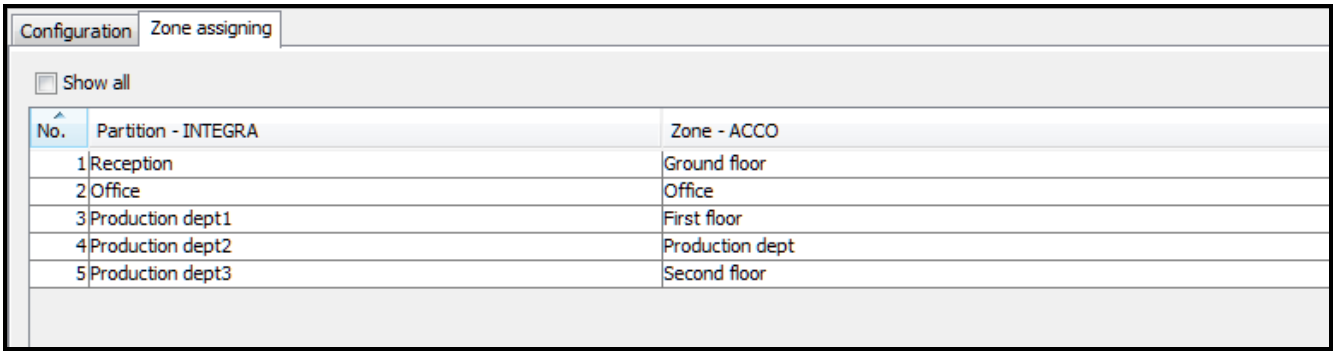


Fig. 36. “Zone assigning” tab.

4.2.7.6 Deleting an alarm system

1. Select the chosen system in the table with the list of systems.
2. Click the  button.
3. You will be asked if you want to delete the system. Click “Yes”.
4. Save the changes made.

4.2.8 Expanders

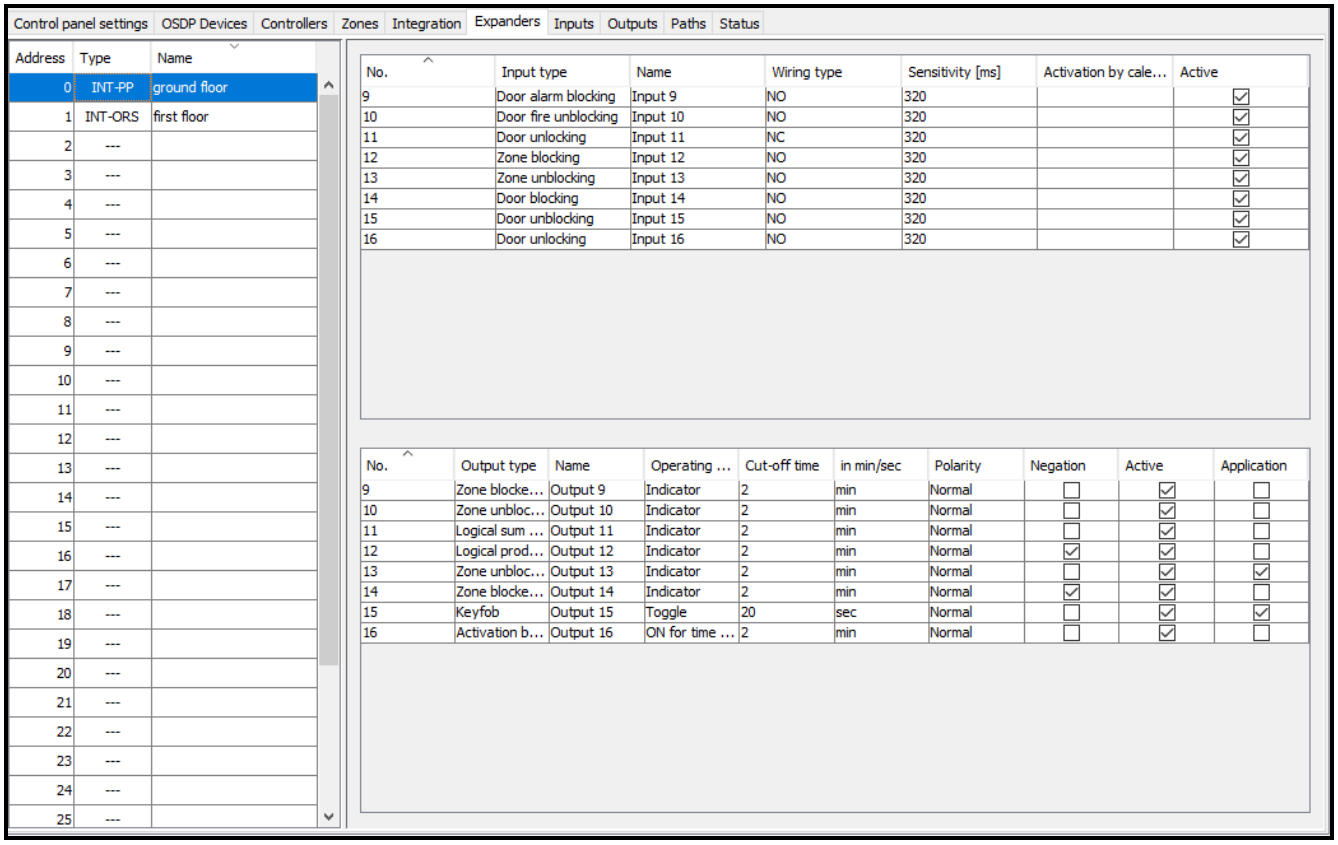


Fig. 37. “Expanders” tab.

4.2.8.1 Adding an expander

The expander will only be supported by the system if added in accordance with the procedure below.

1. Click the address which corresponds to that set in the expander.
2. Right click in the “Type” column. A list of expander types will be displayed.
3. Select the appropriate expander type.
4. In the “Name” column, enter the expander name.
5. Save the changes made.

4.2.8.2 Expander settings

Address – address of the expander.

Type – type of the expander. You can choose from: INT-O, INT-E, INT-PP, INT-RX-S, INT-ORS and INT-IORS.

Name – individual expander name.

In the case of expanders of inputs / outputs / inputs and outputs, highlighting the selected expander will display, next to the list of expanders, one or two tables with information on the

inputs / outputs in the highlighted expander (description of zones – see p. 59; description of outputs – see p. 61).

4.2.8.3 Deleting an expander

1. In the table with a list of expanders, select the module which is to be deleted.
2. In the “Type” column, right click and select a blank field.
3. Save the changes made.

4.2.9 Inputs

The access control system supports the following inputs:

- **wired** – on the control panel electronics board and in expanders.
- **virtual** – the inputs which do not exist physically, but can be programmed as “According to output”.

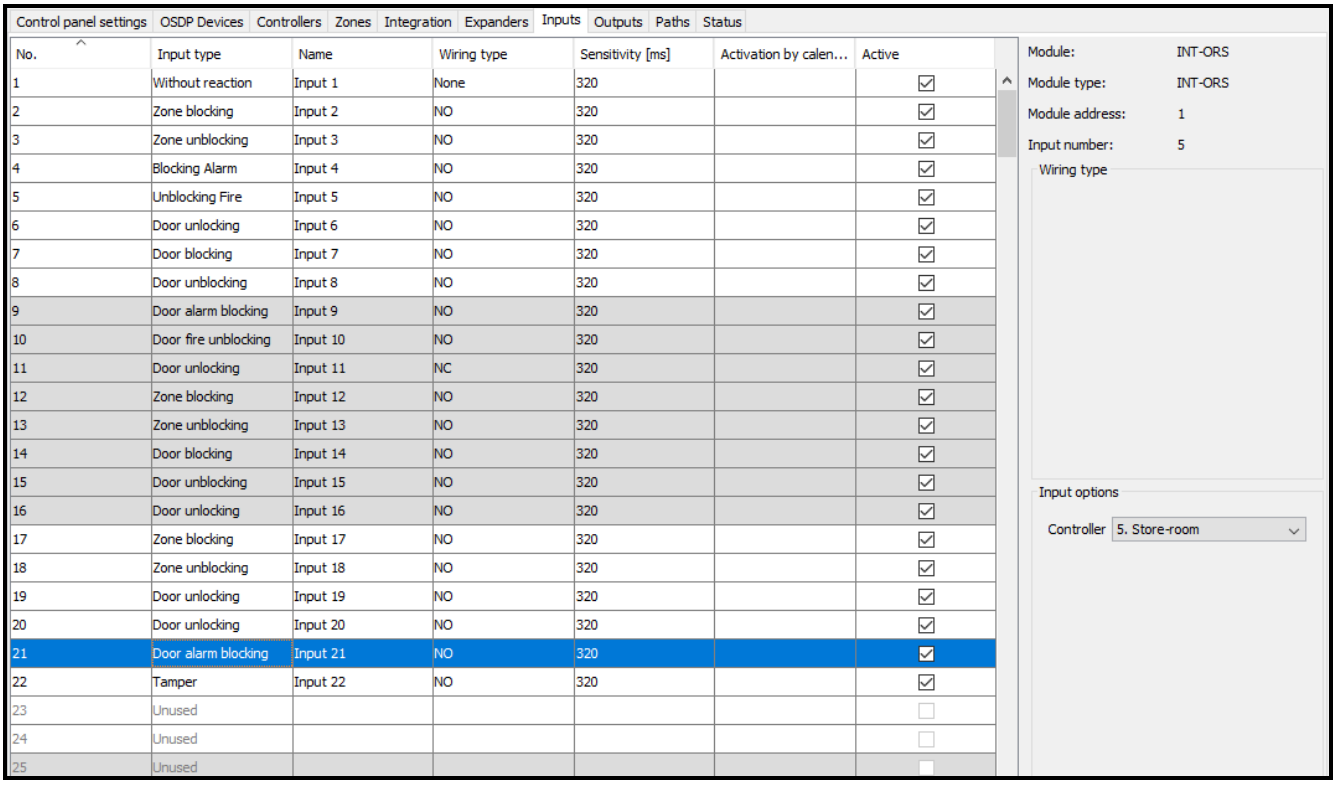
4.2.9.1 Numeration of inputs in the system

The inputs are given their numbers as follows:

- wired inputs on the control panel electronics board have numbers from 1 to 8.
- input numbers in the expanders are conditional upon the address of expander in the system (the numbers of inputs for individual expander addresses are reserved – e.g. for the expander with address 0, the inputs will have numbers from 9 to 16, for the expander with address 1, the inputs will have numbers from 17 to 24, etc.).

4.2.9.2 Programming the inputs

Click the “Inputs” tab. Select an input to program it.



No.	Input type	Name	Wiring type	Sensitivity [ms]	Activation by calen...	Active
1	Without reaction	Input 1	None	320		☑
2	Zone blocking	Input 2	NO	320		☑
3	Zone unblocking	Input 3	NO	320		☑
4	Blocking Alarm	Input 4	NO	320		☑
5	Unblocking Fire	Input 5	NO	320		☑
6	Door unlocking	Input 6	NO	320		☑
7	Door blocking	Input 7	NO	320		☑
8	Door unblocking	Input 8	NO	320		☑
9	Door alarm blocking	Input 9	NO	320		☑
10	Door fire unblocking	Input 10	NO	320		☑
11	Door unlocking	Input 11	NC	320		☑
12	Zone blocking	Input 12	NO	320		☑
13	Zone unblocking	Input 13	NO	320		☑
14	Door blocking	Input 14	NO	320		☑
15	Door unblocking	Input 15	NO	320		☑
16	Door unlocking	Input 16	NO	320		☑
17	Zone blocking	Input 17	NO	320		☑
18	Zone unblocking	Input 18	NO	320		☑
19	Door unlocking	Input 19	NO	320		☑
20	Door unlocking	Input 20	NO	320		☑
21	Door alarm blocking	Input 21	NO	320		☑
22	Tamper	Input 22	NO	320		☑
23	Unused					☐
24	Unused					☐
25	Unused					☐

Fig. 38. “Inputs” tab.

Assigning an input to the zone

1. Program one of the following input types: “Zone blocking”, “Zone unblocking”, “Blocking Alarm” or “Unblocking Fire”.

2. In the “Input options” on the right side of the window, assign the input to the selected zone or to all zones.

Assigning an input to the controller

1. Program one of the following input types: “Door unlocking”, “Door blocking”, “Door unblocking”, “Door alarm blocking” or “Door fire unblocking”.
2. In the window that will open, select the controller to which you want to assign an input and click “OK”.

Input parameters

Table with the list of inputs

No. – number of input in the system.

Input type (see: section “Input types”).

Name – individual name of the input (up to 32 characters).

Wiring type – you can program:

None – no device connected,

NO – supports device having an NO type output (normally open),

NC – supports device having an NC type output (normally closed),

According to output – the status depends on the status of selected output (supports no device connected).

Sensitivity [ms] – the period of time during which the input status must be changed to be registered. You can program the time within the range from 20 ms to 5.1 s.

Activation by calendar – if this option is enabled, the input will only be supported during the time defined by the access calendar. To select the calendar, you can right click on the field. You can create the access calendars in the ACCO Web application.

Active – when this option is enabled, the input is supported. The option is available, when the input type has been selected.

Input information

After an input is highlighted on the list, the following data will be displayed next to the table:

- name, type and address of the module and the number of input in the module,
- parameters defined for the given wiring type and input type:
  - output number (wiring type “According to output”),
  - controller (input type “Door unlocking”, “Door blocking”, “Door unblocking”, “Door alarm blocking” or “Door fire unblocking”),
  - zone – one or all (input type: “Zone blocking / unblocking”, “Blocking Alarm” or “Unblocking Fire”).

Input types

To select the input type, right click the field.

Unused

Without reaction – input used for complex logical operations on the outputs. Input activation will not trigger directly any reaction.

Zone blocking – input activation will block all doors supervised by controllers assigned to the selected zone. The doors will remain blocked as long as the input is active (unless an event occurs which will otherwise change the door status).

Zone unblocking – input activation will unblock all doors supervised by controllers assigned to the selected zone. The doors will remain unblocked as long as the input is active (unless an event occurs which will otherwise change the door status).

Blocking Alarm – permanent locking of all doors in the zone in case of alarm. The doors will remain blocked until their status is changed by using the code or holding the card for a moment in front of the reader by the user having the "Switching" permission.

Unblocking Fire – permanent unlocking of all doors in the zone in case of alarm. The doors will remain unlocked until all controller / ACCO-NT inputs are restored to their normal status. The doors can be switched over by a user having the "Switching" permission.

Door unlocking – input activation will unlock the door supervised by the selected controller for the time period preprogrammed in the field "Access time" (in the "Door" tab, after highlighting the appropriate controller on the list). You must indicate the controller in the window that will open after this input type is selected.

Door blocking – input activation will block the door supervised by the selected controller. You must indicate the controller in the window that will be displayed after selecting this input type for the input. The door will remain blocked until its status is changed by a user having the "Switching" permission or by using suitable functions in the ACCO Soft program or ACCO Web application.

Door unblocking – input activation will unblock the door supervised by the selected controller. You must indicate the controller in the window that will be displayed after selecting this input type for the input. The door will remain unblocked until its status is changed by a user having the "Switching" permission or by using suitable functions in the ACCO Soft program or ACCO Web application.

Door alarm blocking – permanent locking due to alarm of the door supervised by the selected controller. You must indicate the controller in the window that will be displayed after selecting this input type for the input. The door will remain blocked until its status is changed by a user having the "Switching" permission.

Door fire unblocking – permanent unlocking due to fire of the door supervised by the selected controller. You must indicate the controller in the window that will be displayed after selecting this input type for the input. The door will remain unlocked until the normal status of controller input is restored. The door can be switched over by a user having the "Switching" permission.

Tamper – activating the input will trigger:

- a trouble in the ACCO-NT control panel, indicated by the appropriate icon in the "Status" tab;
- a tamper alarm on the output configured as "Tamper alarm from control panel".

4.2.10 Outputs

The access control system supports the following outputs:

- **wired** – on the control panel electronics board and in the expanders.
- **virtual** – outputs which do not exist physically but which can be used e.g. for execution of logical functions.

4.2.10.1 Numeration of outputs in the system

The outputs receive their numbers in the following way:

- the wired outputs on control panel electronics board have numbers from 1 to 8.
- the numbers of outputs in expanders depend on the address of expander in the system (for individual expander addresses, the output numbers are reserved – e.g. for the expander with address 0, the outputs will have numbers from 9 to 16, for the expander with address 1, the outputs will have numbers from 17 to 24 etc.).

4.2.10.2 Programming the outputs

Click the “Outputs” tab. Highlight the output to program it.

Output parameters

Table with the list of outputs

No. – number of output in the system.

Output type (see: section “Output types”).

Name – individual name of the output (up to 32 characters).

Operating Mode – select the output operating mode:

ON for time (event prolongs) – the output will be turned on for the time defined in the “Cut-off time” field. When the output is active, its repeated triggering will restart the cut-off time countdown.

ON for time (event deactivates) – the output will be turned on for the time defined in the “Cut-off time” field. When the output is active, its repeated triggering will turn it off.

ON for time (ignore events) – the output will be turned on for the time defined in the “Cut-off time” field. When the output is active, its repeated triggering will have no effect on its status.

Toggle – triggering the output will toggle its status (if it was turned on, it will be turned off; if it was turned off, it will be turned on).

Indicator – the output will be active as long as the control signal is applied.

Cut-off time – time period during which the output is active. You can program from 0 to 127 seconds or minutes. If value 0 is preprogrammed, the output will be active as long as control signal is supplied.

If the cut-off time is preprogrammed in outputs of “Logical product of the outputs”, “Logical sum of the outputs”, “Logical product of the inputs” or “Logical sum of the inputs” type, the output will be active as long as control signal is supplied and, additionally, for the preprogrammed time.

in min/sec – select, whether the cut-off time is to be counted in seconds or minutes.

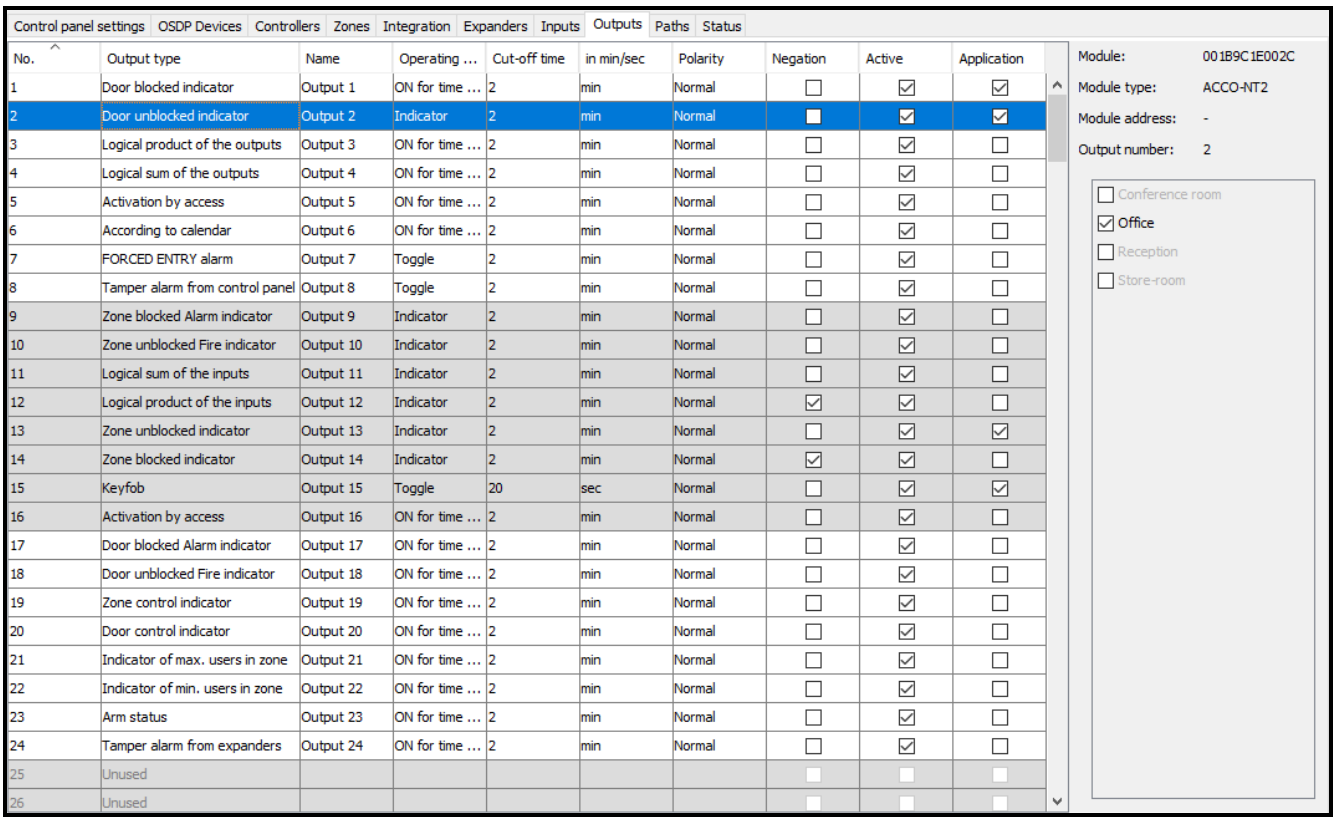
Polarity – the option defines how the output will operate. In the event of reversed polarity, in active state:

- the OC output type will be disconnected from common ground,
- the NO terminal of relay output is opened, and the NC terminal closed.

Negation – if the option is enabled, the physical state of the output is opposite to that presented in the system (the ON output is presented as inactive, the OFF output is presented as active).

Active – when this option is enabled, the output is supported. The option is available, when the output type has been selected.

Application – when this option is enabled, you can activate the output on the map in the ACCO Web application.



No.	Output type	Name	Operating ...	Cut-off time	in min/sec	Polarity	Negation	Active	Application
1	Door blocked indicator	Output 1	ON for time ...	2	min	Normal	☐	☑	☑
2	Door unblocked indicator	Output 2	Indicator	2	min	Normal	☐	☑	☑
3	Logical product of the outputs	Output 3	ON for time ...	2	min	Normal	☐	☑	☐
4	Logical sum of the outputs	Output 4	ON for time ...	2	min	Normal	☐	☑	☐
5	Activation by access	Output 5	ON for time ...	2	min	Normal	☐	☑	☐
6	According to calendar	Output 6	ON for time ...	2	min	Normal	☐	☑	☐
7	FORCED ENTRY alarm	Output 7	Toggle	2	min	Normal	☐	☑	☐
8	Tamper alarm from control panel	Output 8	Toggle	2	min	Normal	☐	☑	☐
9	Zone blocked Alarm indicator	Output 9	Indicator	2	min	Normal	☐	☑	☐
10	Zone unblocked Fire indicator	Output 10	Indicator	2	min	Normal	☐	☑	☐
11	Logical sum of the inputs	Output 11	Indicator	2	min	Normal	☐	☑	☐
12	Logical product of the inputs	Output 12	Indicator	2	min	Normal	☑	☑	☐
13	Zone unblocked indicator	Output 13	Indicator	2	min	Normal	☐	☑	☑
14	Zone blocked indicator	Output 14	Indicator	2	min	Normal	☑	☑	☐
15	Keyfob	Output 15	Toggle	20	sec	Normal	☐	☑	☑
16	Activation by access	Output 16	ON for time ...	2	min	Normal	☐	☑	☐
17	Door blocked Alarm indicator	Output 17	ON for time ...	2	min	Normal	☐	☑	☐
18	Door unblocked Fire indicator	Output 18	ON for time ...	2	min	Normal	☐	☑	☐
19	Zone control indicator	Output 19	ON for time ...	2	min	Normal	☐	☑	☐
20	Door control indicator	Output 20	ON for time ...	2	min	Normal	☐	☑	☐
21	Indicator of max. users in zone	Output 21	ON for time ...	2	min	Normal	☐	☑	☐
22	Indicator of min. users in zone	Output 22	ON for time ...	2	min	Normal	☐	☑	☐
23	Arm status	Output 23	ON for time ...	2	min	Normal	☐	☑	☐
24	Tamper alarm from expanders	Output 24	ON for time ...	2	min	Normal	☐	☑	☐
25	Unused						☐	☐	☐
26	Unused						☐	☐	☐

Fig. 39. “Outputs” tab.

Output information

After an output is highlighted on the list, the following information will be displayed next to the table:

- name, type and address of the module and the output number in the module,
- parameters to be defined for each output type:
  - output numbers (output type “Logical product of the outputs” or “Logical sum of the outputs”),
  - input numbers (output type “Logical product of the inputs” or “Logical sum of the inputs”),
  - zone – one or all (output type “Activation by access”),
  - zone – selected (output type: “Arm status”, “Zone blocked indicator”, “Zone unblocked indicator”, “Zone blocked Alarm indicator”, “Zone unblocked Fire indicator”, “Zone control indicator”, “Indicator of max. users in zone” or “Indicator of min. users in zone”),
  - door – selected (output type: “Door blocked indicator”, “Door unblocked indicator”, “Door blocked Alarm indicator”, “Door unblocked Fire indicator”, “Door control indicator”, “FORCED ENTRY alarm”, “Tamper alarm from controllers”, “Access granted” or “Access denied”),
  - access calendar (output type “According to calendar”),
  - expander (output type “Tamper alarm from expanders”).

Output types

To select the output type, you can right click the field.

Unused

Logical product of the outputs – triggered when all control outputs are active.

Logical sum of the outputs – triggered when any of the control outputs is active.

Logical product of the inputs – triggered when all control inputs are active.

Logical sum of the inputs – triggered when any of the control inputs is active.

Keyfob – triggered on pressing a keyfob button.

Activation by access – triggered after the user is granted access to the selected zone with the “Output activation” option enabled.

Zone blocked indicator – triggered when any of the selected zones is blocked.

Zone unblocked indicator – triggered when any of the selected zones is unblocked.

Zone blocked Alarm indicator – triggered when any doors in any of the selected zones are permanently locked because of alarm.

Zone unblocked Fire indicator – triggered when any doors in any of the selected zones are permanently unlocked because of fire.

Door blocked indicator – triggered when any of the selected doors is blocked.

Door unblocked indicator – triggered when any of the selected doors is unblocked.

Door blocked Alarm indicator – triggered when any of the selected doors is permanently locked because of alarm.

Door unblocked Fire indicator – triggered when any of the selected doors is permanently unlocked because of fire.

Zone control indicator – triggered when status of any of the selected zones is controlled.

Door control indicator – triggered when status of any of the selected doors is controlled.

According to calendar – triggered according to time frames assigned by the selected access calendar.

Indicator of max. users in zone – triggered when maximum number of users stay in any of the selected zones.

Indicator of min. users in zone – triggered when minimum number of users stay in any of the selected zones.

Arm status – triggered when any of the integrated partitions is armed.

FORCED ENTRY alarm – triggered when “Forced entry” alarm is triggered from any of the selected doors.

Tamper alarm from control panel – triggered during activation of the input programmed as “Tamper”. Tamper alarm of the ACCO-NT control panel will be triggered.

Tamper alarm from expanders – triggered when tamper alarm is triggered from any of the selected expanders.

Tamper alarm from controllers – triggered when tamper alarm is triggered from any of the selected controllers.

Access granted – triggered when access to any of the selected doors is granted.

Access denied – triggered when access to any of the selected doors is denied.

4.2.11 Paths

The path is the route the user will have to walk along when moving around the premises. Such a solution can be used e.g. for the cleaning personnel.

Description of the buttons

 - click to add a path.

 - click to delete the highlighted path (see: section “Deleting a path”).

4.2.11.1 Creating a path

1. Highlight a control panel on the list of objects and control panels.

2. Click the  button. A new path will appear on the list.
3. Right click a field in the “Zone” column and select one of the zones.
4. You can define the minimum duration of user's stay in the given zone.
5. If you want to assign further zones to the path, repeat the steps 3 and 4.
6. Save the changes made.

4.2.11.2 Programming the path

Click the “Paths” tab. Highlight the path to program it.

Name – individual name of the path (up to 45 characters).

If a new name is entered or the existing name is changed, the following buttons will appear:

 – click to cancel the changes made.

 – click to confirm the changes made.

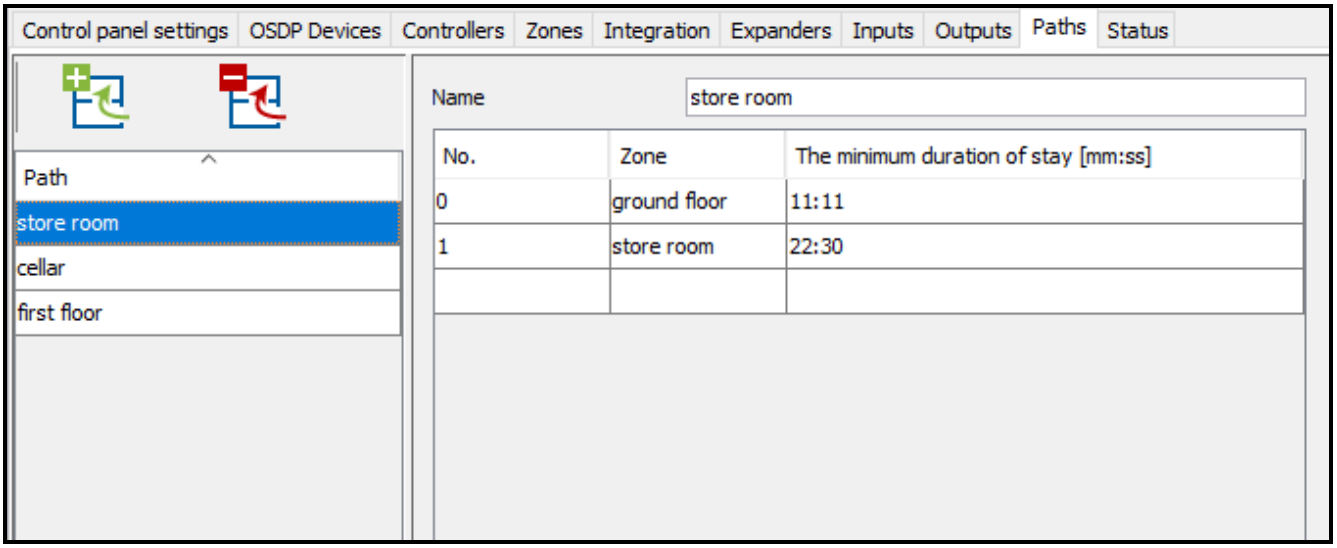


Fig. 40. “Paths” tab.

Table to define the path

No. – number defining the order of zones that create the route.

Zone – name of the zone included in the path.

The minimum duration of stay [mm:ss] – the minimum period of time during which the user will have to stay in the given zone, after expiry of which the user will be allowed to go to the next zone. You can program up to 59 minutes and 59 seconds.

If the zone name is displayed in the “Zone” column, right click a row in the table to open the drop-down menu:

Move up – click to move the highlighted zone up by one field.

Remove – click to delete the highlighted zone from the list.

Move down – click to move the highlighted zone down by one field.

4.2.11.3 Deleting a path

1. If you want to delete a single path, use the cursor to highlight the selected path on the list of paths.
2. If you want delete two or more paths at once, use the cursor to highlight one of the paths and, holding down the Ctrl key, select the next ones, highlighting them with the left mouse button.

3. If you want to delete all the paths at once, use the cursor to highlight one of the paths and press the Ctrl+A keys simultaneously.
4. Click the  button.
5. When a prompt appears asking you whether to delete the path, click “Yes”.
6. Save the changes made.

4.2.12 Status

In the “Status” tab, information on the current status of control panel, power supply, as well as inputs and outputs of the control panel and expanders is displayed.

If there is no communication between the ACCO Server and the control panel, information on the absence of communication, as well as the date and time of the last transmission received by the server from the control panel will be displayed.

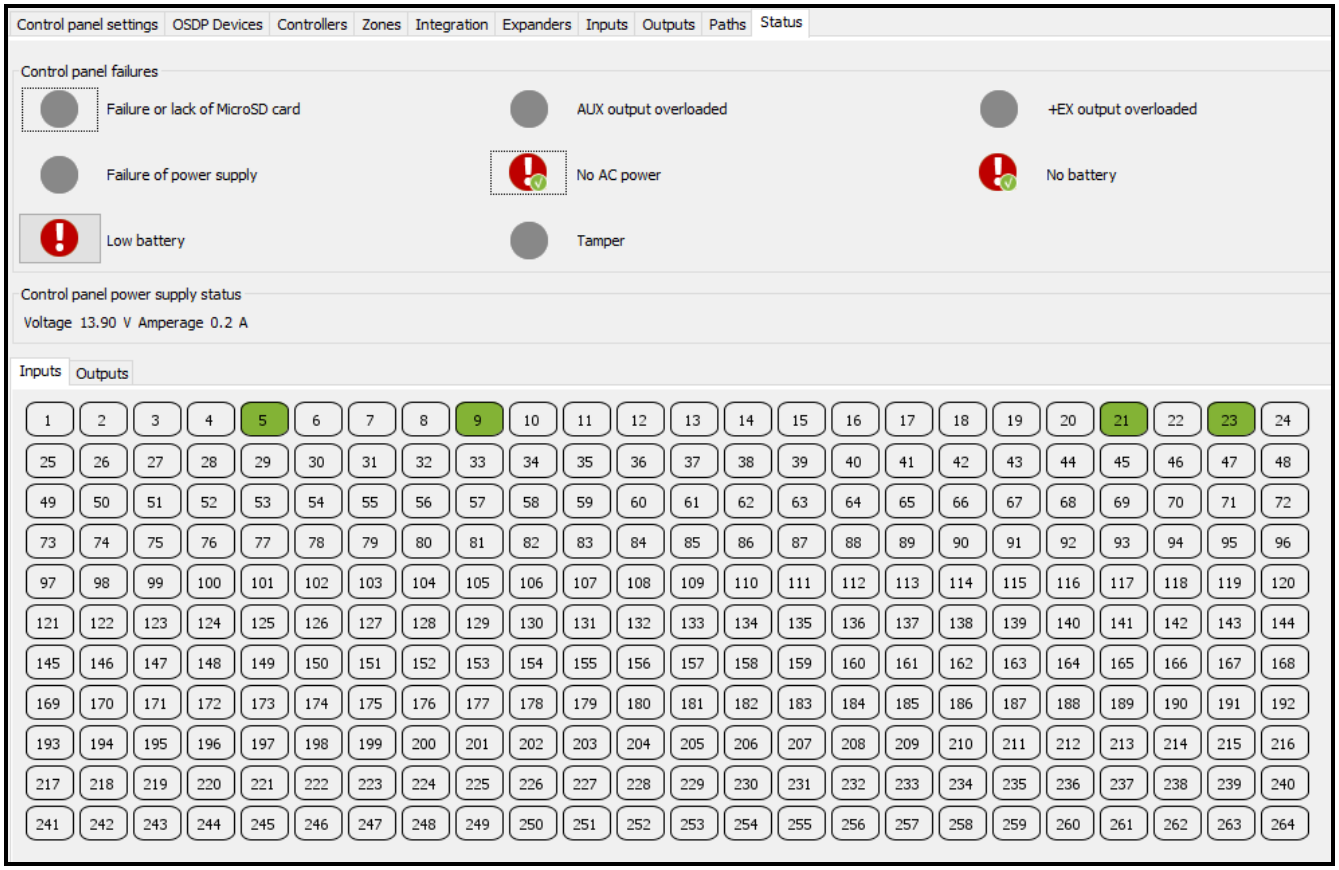


Fig. 41. “Status” tab.

4.2.12.1 Control panel failures

In this area, the icons are displayed indicating the:

- failure or lack of MicroSD card,
- AUX output overloaded,
- +EX output of the power supply unit connected to the expander bus overloaded,
- failure of power supply,
- no AC power,
- no battery,
- low battery,
- tamper.

The icons indicate the following status:

-  – everything OK (gray background),
-  – trouble (white exclamation mark on red background),
-  – confirmed trouble (white exclamation mark on red background and white symbol on green background),
-  – trouble memory (white exclamation mark on gray background),
-  – confirmed trouble memory (white exclamation mark on gray background and white symbol on green background).
-  – status unknown (white question mark on gray background).

If you want to confirm a trouble, click the button next to it.

4.2.12.2 Control panel power supply status

In this area, the power supply status information is displayed.

4.2.12.3 "Inputs" tab

In the tab, the input status information is displayed. The colors have the following meaning:
gray – inactive input,
green – active input.

4.2.12.4 "Outputs" tab

In the tab, the output status information is displayed. The colors have the following meaning:
gray – inactive output,
green – active output.

4.2.13 Import

Importing a packet of data related to several dozen users may last from ten to twenty minutes.

The "Import" button allows importing the user data and time schedules from ACCO-SOFT-LT program files (with kkd extension) and from CSV format files.

4.2.13.1 Importing data from CSV format files

1. In the main menu, click the  button.
2. In the menu that will be displayed, select the "Import from csv" command.
3. Indicate the data file you want to import.
4. In the window that will open, specify the character set and separator used in the file being imported.
5. Match the labels to the individual columns with imported data. **It is necessary to assign the "Name" label to the column containing the imported user names.**
6. Click the "Validation" button to check whether the selected file contains valid data.
7. If the data are valid, click the "Import" button to start the data import procedure. After completion of the procedure, a message will be displayed to inform you about it.
8. If the data are not valid, select another file and repeat the steps 4-7.

Charset – select the set of characters according to the language used in the file being imported.

Field separator – enter the character that is used in the file being imported to divide text into columns.

String separator – enter the character that is used in the file being imported to define the limits of textual data.

Assign… – right click the column name. A drop-down menu will be displayed with the list of data labels that have been imported from file. Match the selected label to the column content by clicking it.

Cancel – click to cancel the changes made.

Validation – click to check correctness of the imported file data. After the check, a message will be displayed to inform you about result of the validation. The button will become active after the “Name” label is assigned to the column containing the imported names of users.

Import – click to start the data import procedure. The button will be available after completion of the validation of data in the file being imported.

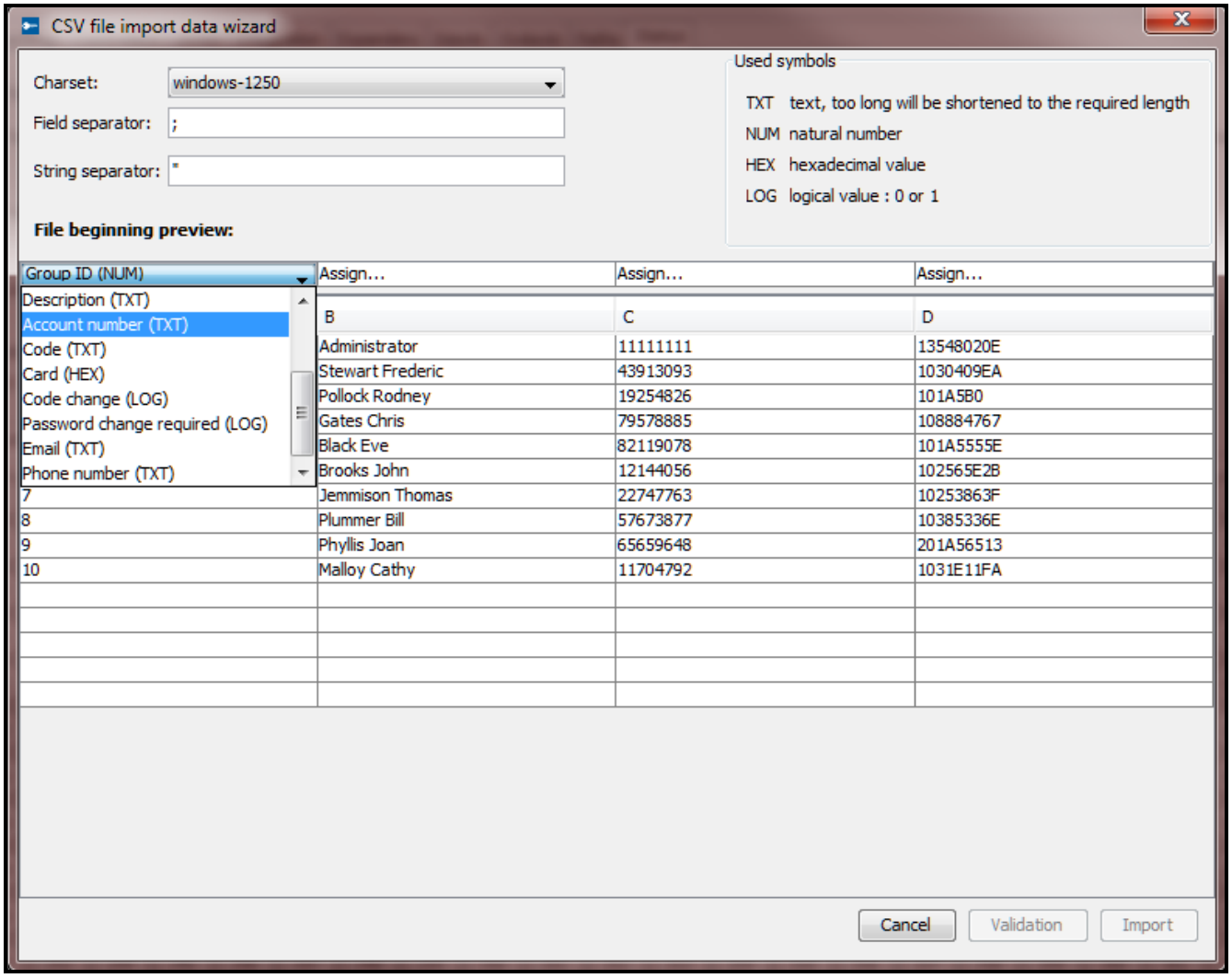


Fig. 42. Window for importing data from CSV format file.

4.2.13.2 Importing data from file with kkd extension

1. In the main menu, click the  button.
2. In the menu that will be displayed, select the “Import from ACCO-SOFT-LT” command.
3. Indicate the data file you want to import.
4. If you have defined your encryption key in ACCO-SOFT-LT program, select the “Non-standard encryption key” option and enter the key into the appropriate field. If you have defined no key, do not select this option.
5. Define the data encryption method.
6. Decide which data are to imported.
7. Click the “Continue” button.
8. Window with information on imported data will open (see: Fig. 44). Click the “Import” button to start the data import procedure. After completion of the procedure, a message will be displayed to inform you about it.

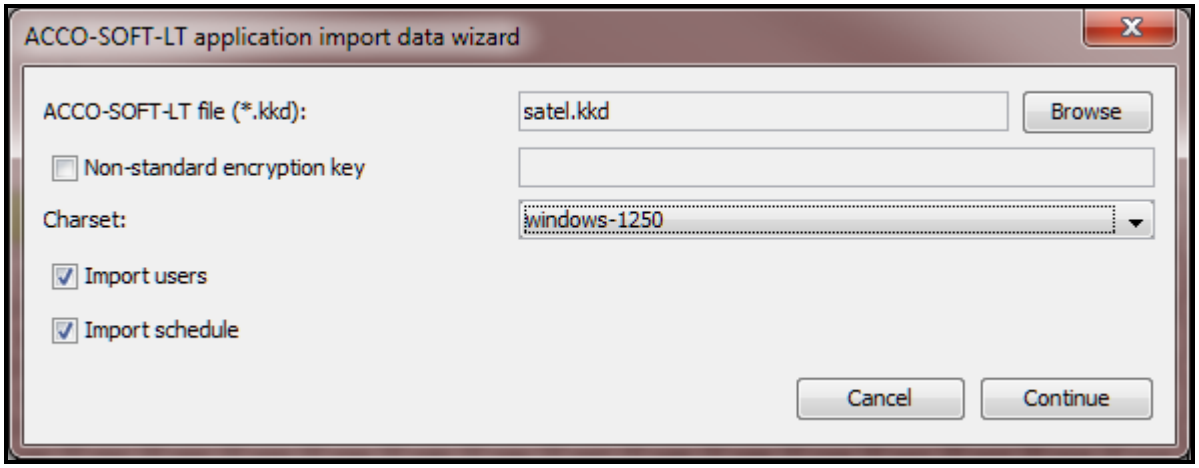


Fig. 43. Window for importing data from the ACCO-SOFT-LT program.

ACCO-SOFT-LT file (*.kkd) – name of the data file.

Browse – click to indicate the access path to the selected data file.

Non-standard encryption key – select the option and, in the field next to it, enter the individual encryption key (code) for data of the configuration file that has been used in the ACCO-SOFT-LT program.

Charset – select the character set suitable for the language used in the imported file.

Import users – select this option if you want to import the user data.

Import schedule – select this option if you want to import the time schedule data. The imported data will be displayed in the ACCO Web application as weekly and daily access schedules.

Cancel – click to cancel the changes made.

Continue – click to confirm the entered data. A window with information on the data imported from the ACCO-SOFT-LT program will open (see: Fig. 44).

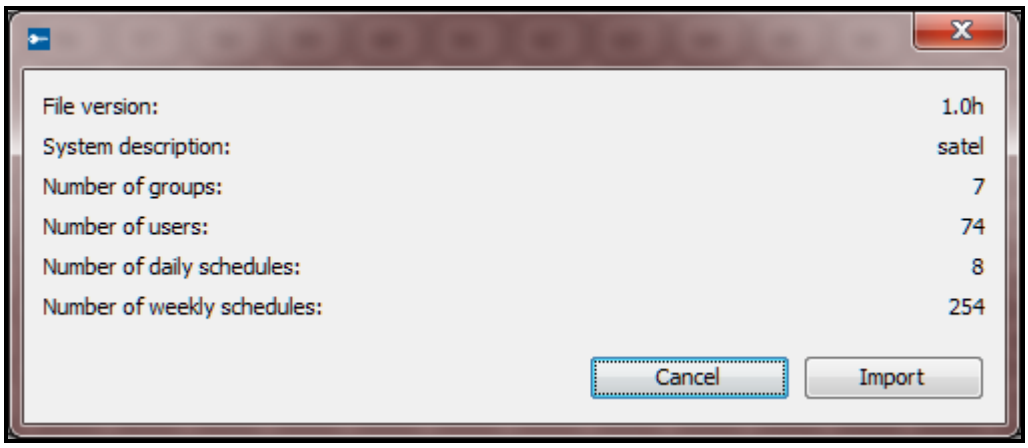


Fig. 44. Window with information on data imported from the ACCO-SOFT-LT program.

5. Appendix 1: How the system integration works

- Blocking the access control system zone will arm the alarm system partition.
- Restoring control in the access control system zone will disarm the alarm system partition.
- Arming the alarm system partition will block the access control system zone.
- Disarming the alarm system partition will restore control in the access control system zone.

If the controller settings are changed when the partition is armed, saving the new settings will automatically disarm the partition.

You can arm the alarm system partition by:

- blocking the access control system zone by using the ACCO Soft program or ACCO Web application,
- blocking the door by using the entry terminal for that zone; the “Controls zone” must be enabled for that terminal,
- blocking the doors supervised by the controllers belonging to the access control system zone (only if configuration of terminals connected to the controllers is suitable).

The zone can only be blocked by using the entry terminal for which the “Controls zone” option is enabled. By using the exit terminal, you can only block a door (blocking all doors in the zone will result in blocking the zone).

If the zone is blocked and several controllers are assigned to it, an attempt to get access to the door by a user having the “Switching” right will change the zone status to “Mixed” and unlock this door.

Unblocking the zone from the ACCO Soft program or ACCO Web application will disarm the partition.

If a door in the armed partition is unblocked from the ACCO Soft program or ACCO Web application, the partition will remain armed.

In the case of integration, changing the state of alarm system partition will affect the status of access control zone. For example: the object (premises) is divided into two zones. Two doors are assigned to each of them, one of them being shared. Both zones of the access control system are integrated with the alarm system partitions (as shown in Fig. 45). If:

- *the alarm system partition is armed, all doors assigned to the integrated zone of access control are blocked,*
- *the alarm system partition is disarmed:*
  - *current state of the adjacent partition is checked. If the adjacent partition is armed, the door shared by both zones will remain blocked.*
  - *current state of the door shared by both zones is checked. If it is unblocked, it will remain unblocked.*

In other cases, the door control will be restored.

You can disarm the alarm system partition by restoring control in the access control system zone.

Alarms that have been triggered in the alarm system can be transmitted to the access control system (see options “Transmit burglary alarm from INTEGRA partition” and “Transmit fire alarm from INTEGRA partition”). Alarm triggered in the alarm system can only be cleared in the alarm system.

Alarms that have been triggered in the access control system are not transmitted to the alarm system.

For detailed information, refer to the Appendix “Operating integrated zones”.

6. Appendix 2: Operating integrated zones

To arm the system, you can block the access control system zone:

- by using a reader serving as entry terminal, connected to one of the controllers in the zone; the “Controls zone” option must be enabled for that terminal,
- from the ACCO Soft program – in the “Zones” tab, hover the cursor over the selected zone on the list of zones, right-click and, in the drop-down menu that will open, select the “Block” function,
- from the ACCO Web application – in the menu on the left, click the “Management” command, then on “Structure”, go to the “Zones” tab, select the required zone on the list of zones and click the  button,
- from the ACCO Web application – in the menu on the left, click the “Maps” command, open the required map, hover the cursor over the area representing the selected zone on the map, left-click and select the “Block” function,
- according to the preset time or assigned access calendar – in the ACCO Soft program, “Zones” tab, select the required zone on the list of zones, go to the “Options” tab and using the “Zone blocking” function, define the time or assign the access calendar,
- by activating an input of the ACCO-NT control panel – in the ACCO Soft program, “Inputs” tab, program the selected input as “Zone blocking”,

The user can only block the zone, if he/she:

– *uses the entry terminal for which the “Controls zone” option is enabled,*

– *has the “Switching” right,*

– *has access to the given zone, according to the access calendar assigned to the user.*

The defined time and programmed calendar have no priority. This means that other events occurring in the module may change the zone status before the preset blocking time expires.

If the same type of identifier is used for the given terminal for getting access and blocking, access will be granted after the identifier is used. The status of door / zone will remain unchanged.

To disarm the system you can restore control in the access control system zone:

- by using a reader serving as entry terminal, connected to one of the controllers in the zone; the “Controls zone” option must be enabled for that terminal,
- from the ACCO Soft program – in the “Zones” tab, hover the cursor over the selected zone on the list of zones, right-click your mouse and, in the drop-down menu that will open, select the “Restore control” function,
- from the ACCO Web application – in the menu on the left, click the “Management” command, then on “Structure”, go to the “Zones” tab, select the required zone on the list of zones and click the ⇄ button,
- from the ACCO Web application – in the menu on the left, click the “Maps” command, open the required map, hover the cursor over the area representing the selected zone on the map, left-click and select the “Restore the control” function,
- after the activated input of the ACCO-NT control panel (programmed as “Zone blocking”) is restored to normal state,

The user can only restore control in the zone, if he/she:

– *uses the entry terminal for which the “Controls zone” option is enabled,*

– *has the “Switching” right,*

– *has access to the given zone, according to the access calendar assigned to the user.*

If the same type of identifier is used for the given terminal for getting access and restoring control, access will be granted after the identifier is used. The status of door / zone will remain unchanged.

6.1 Examples

6.1.1 Example 1

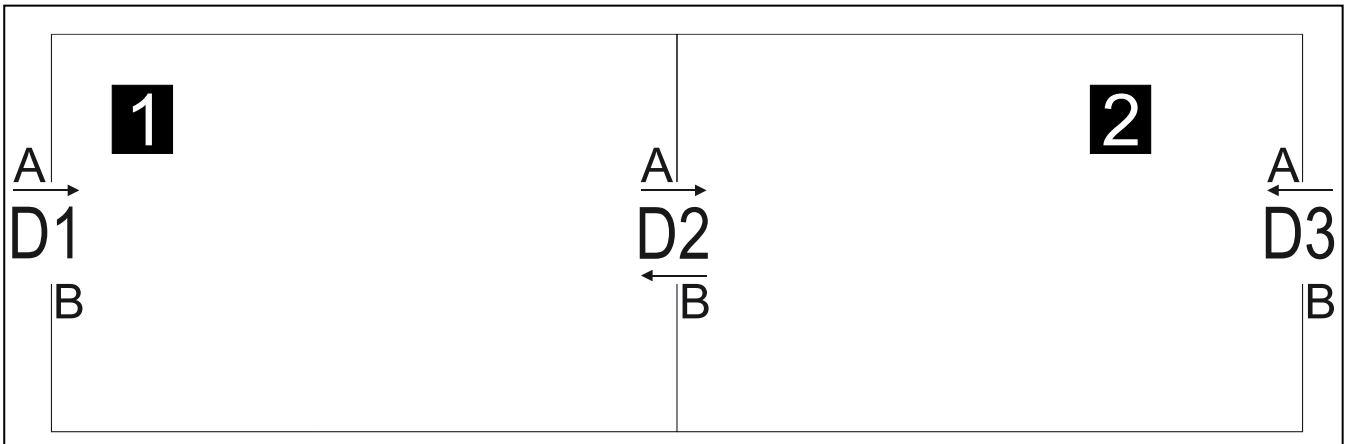


Fig. 45. An example of access control system zones integrated with alarm system partitions.

Legend to Fig. 45:

1 & **2** (numbers on black background) – zones integrated with alarm system partitions.

D1 – controller assigned to zone 1. Terminal A is entry into zone 1, and terminal B is exit from zone 1.

D2 – controller assigned to zones 1 & 2. Terminal A is entry into zone 2 and exit from zone 1. Terminal B is exit from zone 2 and entry into zone 1.

D3 – controller assigned to zone 2. Terminal A is entry into zone 2, and terminal B is exit from zone 2.

Arming

To arm the alarm system partition, you must block the zone of the access control system. You can only do so by using the terminal serving as the entry to that zone. The "Controls zone" option must be enabled for that terminal.

Operating the zone 1

If you want to arm the zone 1, use the terminal A of door D1 or the terminal B of door D2.

Operating the zone 2

If you want to arm the zone 2, use the terminal A of door D2 or the terminal A of door D3.

Disarming

To disarm the alarm system partition, you must restore control in the zone of the access control system. You can only do so by using the terminal serving as the entry to that zone. The "Controls zone" option must be enabled for that terminal.

Operating the zone 1

If you want to disarm the zone 1, use the terminal A of door D1 or the terminal B of door D2.

Operating the zone 2

If you want to disarm the zone 2, use the terminal A of door D2 or the terminal A of door D3.

6.2 Signaling of door / zone blocking by devices of the access control system

The chapter describes an additional signaling related to system integration.

6.2.1 Optical signaling

6.2.1.1 Status priorities in the ACCO NET system

If different events which can be indicated by LED indicators of the access control devices occur simultaneously in the ACCO NET system, they have the following priority (device indicates the event with the highest priority):

1. No communication between ACCO-NT control panel and ACCO-KP / ACCO-KP-PS / ACCO-KPWG / ACCO-KPWG-PS or ACCO-KP2 controller.
2. Door blocked because of burglary alarm.
3. Door blocked.
4. Door unblocked because of fire alarm.
5. Door unblocked.
6. Integration error (see description of the "State" column in table with the list of alarm systems in the "Integration" tab).

6.2.1.2 LCD keypads

When the door / zone is blocked, name of the user who has run this function may be displayed on the keypad.

The keypad LED indicators indicate the door / zone status in the following manner:

LED	Color	Description
	yellow	**ON** – door blocked (permanently locked) / zone blocked, integrated partition armed **flashing slowly** – door blocked (permanently locked) after the „Alarm – blocking door” type input is activated or because of burglary alarm in the alarm control panel
	green	**ON** – door unblocked (permanently unlocked) **flashing slowly** – door unblocked (permanently unlocked) after the “Fire – unblocking door” type input is activated or because of fire alarm in the alarm control panel
	red	**ON** – alarm or burglary / fire alarm in the alarm control panel **flashing** – alarm memory
	yellow and green	**flashing slowly alternately** – integration error **flashing rapidly alternately** – no communication between ACCO-NT control panel and ACCO-KP / ACCO-KP-PS / ACCO-KPWG / ACCO-KPWG-PS or ACCO-KP2 controller

After the alarm cause has ceased, the alarm memory signal on the keypad can be cleared by acknowledging the alarm memory in ACCO Soft program or in ACCO Web application.

6.2.1.3 Keypads with proximity card reader

ACCO-SCR

Information provided by the ACCO-SCR keypad by means of the  ,  and  LED indicators is identical to that provided by the LCD keypad.

CR-MF5

Information provided by the CR-MF5 keypad by means of the LED indicators is identical to that provided by the LCD keypad.

SO-MF5

The SO-MF5 keypad LED indicators indicate the door / zone status in the following manner:

LED	Color	Description
	blue	**ON** – door unblocked (permanently unlocked) **flashing slowly** – door unblocked (permanently unlocked) after the "Fire – unblocking door" type input is activated or because of fire alarm in the alarm control panel
	red	**ON** – alarm or burglary / fire alarm in the alarm control panel **flashing** – alarm memory
	green	**ON** – door blocked (permanently locked) / zone blocked, integrated partition armed **flashing slowly** – door blocked (permanently locked) after the "Alarm – blocking door" type input is activated or because of burglary alarm in the alarm control panel

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

6.2.1.4 Proximity card readers

CZ-EMM / CZ-EMM2

The bi-color LED in CZ-EMM and CZ-EMM2 readers indicates the door / zone status in the following manner:

Color	Description
green	**flashing slowly:** • door unblocked (permanently unlocked), • door unblocked (permanently unlocked) because of fire alarm in the alarm control panel
red	**flashing slowly:** • door blocked (permanently locked) / zone blocked, integrated partition armed, • door blocked because of burglary alarm in the alarm control panel
green and red	**flashing slowly alternately** – integration error **flashing rapidly alternately** – no communication between ACCO-NT control panel and ACCO-KP / ACCO-KP-PS / ACCO-KPWG / ACCO-KPWG-PS or ACCO-KP2 controller

CZ-EMM3 / CZ-EMM4

The LED indicators in CZ-EMM3 and CZ-EMM4 readers indicate the door / zone status in the following manner:

Color	Description
green	**flashing slowly:** • door unblocked (permanently unlocked), • door unblocked because of fire alarm in the alarm control panel
red	**flashing slowly:** • door blocked (permanently locked) / zone blocked, integrated partition armed • door blocked because of burglary alarm in the alarm control panel
red and green	**flashing slowly alternately** – integration error **flashing rapidly alternately** – no communication between ACCO-NT control panel and ACCO-KP / ACCO-KP-PS / ACCO-KPWG / ACCO-KPWG-PS or ACCO-KP2 controller

CR-MF3

Information provided by the CR-MF3 reader by means of the LED indicators depends on the operating mode of the device.

EM-Marin / Wiegand interface

The LED indicators in the CR-MF3 reader indicate the door / zone status in the same manner as the CZ-EMM3 and CZ-EMM4 readers.

While connecting the CR-MF3 reader, remember that if you program the IN1…IN3 inputs differently from what is described in the reader and ACCO-KP2 controller manuals, the LED indicators will operate differently.

RS-485 (OSDP) bus

The LED indicators in the CR-MF3 reader indicate the door / zone status in the following manner:

Color	Description
red	**ON** – alarm or burglary / fire alarm in the alarm control panel **flashing** – alarm memory
green	**ON** – door unblocked (permanently unlocked) because of fire alarm in the alarm control panel **flashing slowly** – door unblocked (permanently unlocked) after the "Fire – unblocking door" type input is activated
yellow	**ON** – door blocked (permanently locked) **flashing slowly** – door blocked (permanently locked) after the "Alarm – blocking door" type input is activated

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

SO-MF3

Information provided by the SO-MF3 reader by means of the LED indicators depends on the operating mode of the device.

EM-Marin / Wiegand interface

The LED indicators in the SO-MF3 reader indicate the door / zone status in the same manner as the CZ-EMM3 and CZ-EMM4 readers.

While connecting the SO-MF3 reader, remember that if you program the IN1…IN3 inputs differently from what is described in the reader and ACCO-KP2 controller manuals, the LED indicators will operate differently.

RS-485 (OSDP) bus

The LED indicators in the SO-MF3 reader indicate the door / zone status in the following manner:

LED	Color	Description
	blue	**ON** – door unblocked (permanently unlocked) **flashing slowly** – door unblocked (permanently unlocked) after the "Fire – unblocking door" type input is activated
	red	**ON** – alarm **flashing** – alarm memory
	green	**ON** – door blocked (permanently locked) **flashing slowly** – door blocked (permanently locked) after the "Alarm – blocking door" type input is activated
	yellow	unused

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

6.2.1.5 DALLAS iButton reader

The bi-color LED in the reader indicates the door / zone status in the following manner:

Color	Description
green	**flashing slowly:** • door unblocked (permanently unlocked), • door unblocked because of fire alarm in the alarm control panel
red	**flashing slowly:** • door blocked (permanently locked) / zone blocked, integrated partition armed, • door blocked because of burglary alarm in the alarm control panel
green and red	**flashing slowly alternately** – integration error **flashing rapidly alternately** – no communication between ACCO-NT control panel and ACCO-KP / ACCO-KP-PS / ACCO-KPWG / ACCO-KPWG-PS or ACCO-KP2 controller

6.2.2 Sound signaling

Devices supported by the ACCO-KP / ACCO-KP-PS / ACCO-KPWG / ACCO-KPWG-PS or ACCO-KP2 modules (LCD keypad, keypad with proximity card reader and proximity card readers) generate sounds that provide information:

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

Long beep lasting 10 seconds – alarm.

2 short beeps every second – entry delay in progress or door / zone restore to normal, i.e. partition disarming.

1 short beep followed by 2 short beeps – granting access and then blocking the door / zone, i.e. partition arming.

Very short beeps – door open too long. Beeps are generated until the door is locked or for 60 seconds.

While connecting the CR-MF3 / SO-MF3 reader, remember that if you program the IN1…IN3 inputs differently from what is described in the readers and ACCO-KP / ACCO-KP2 controller manuals, the sound signaling will operate differently.