



NODER EE12/EWE4

IP controller of Access Control and Intruder Alarm Systems

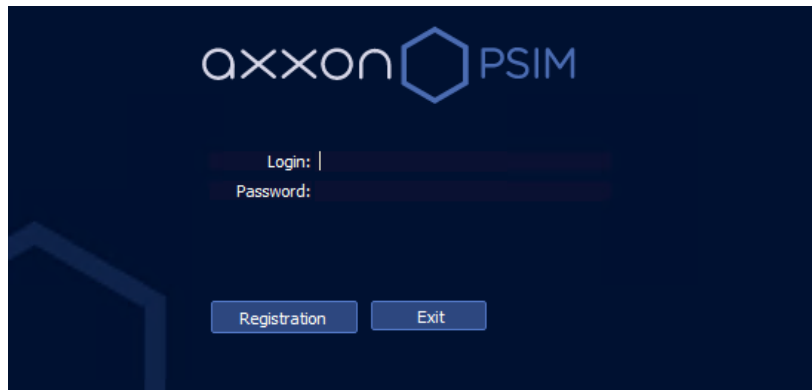
Operator's Manual


TABLE OF CONTENTS

TABLE OF CONTENTS	2
1. Login to system	3
1.1 Password changing.....	4
2. Working with AxxonSoft software	5
2.1 Main menu.....	5
2.2 Choosing an interface.....	6
3. Access Control Panel	7
3.1 Departments.....	8
3.1.1 Create and edit a user.....	10
3.2 Time zones.....	13
3.3 Access levels.....	16
3.4 Regions and areas.....	18
3.5 Reports.....	19
4. Noder Access Control visualisation	21
4.1 Noder Controller.....	21
4.2 Noder Reader.....	24
4.3 Noder Input.....	30
4.4 Noder Elevator module.....	33
4.4.1 Noder Floor.....	34
4.5 Noder Output.....	35
5. Noder Intruder alarm system visualisation	38
5.1 Noder Zone.....	38
5.2 Noder Input.....	39


1. Login to system

After starting client station, AxxonSoft software starts automatically, and then a login window appears in which you must enter the operator's login and password.

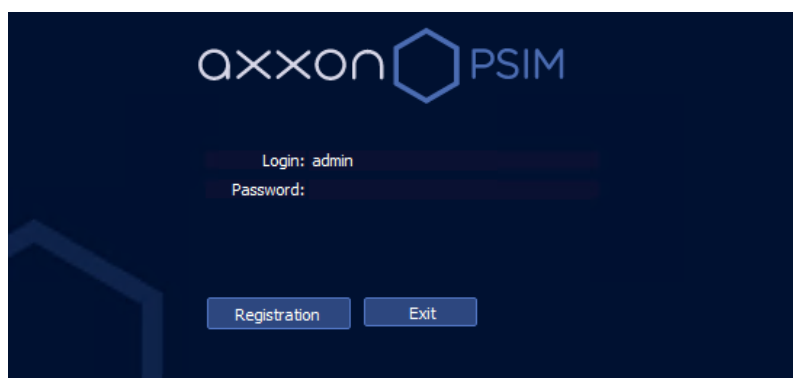


If program is not running, call it from the shortcut on desktop  **Client's workplace**. However, if it is already running, the same icon should be in system tray (next to the clock).

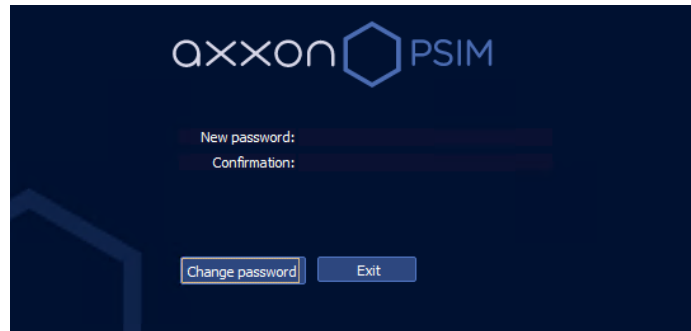
Many users can work in system, where administrator assigns the rights to perform specific tasks in system. The new operator who starts working with system should log into system using a personal login and temporary password received from the administrator. During the first login, he will be asked to change temporary password on his own.

To log into system, log out current user using **Log off** option, in the main program menu. To open main program menu, move mouse cursor to the upper right corner of the screen, and then after quick access bar appears, click left mouse  button on icon and select **Log off**.


In login window, enter the username (login) and password and click **Registration**.

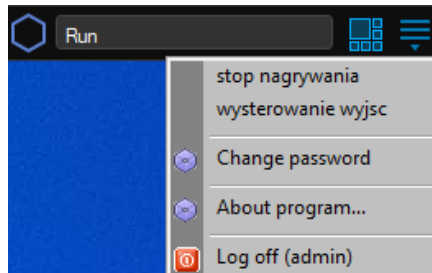


For the first login, the user will be asked to enter your own new password which must be different from the previous one. In field **Confirmation** enter new password again, and then click **Change password**.

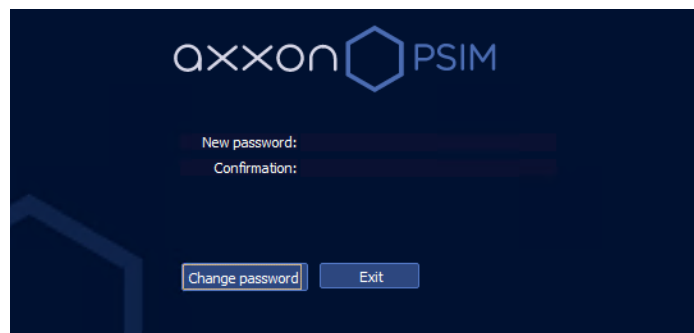


1.1 Password changing

To change password, click  button and choose option **Change password**.




The new password must be different from the previous one. In field **Confirmation** enter new password again, and then click **Change password**. Password will be changed and user will be logged after using new password.




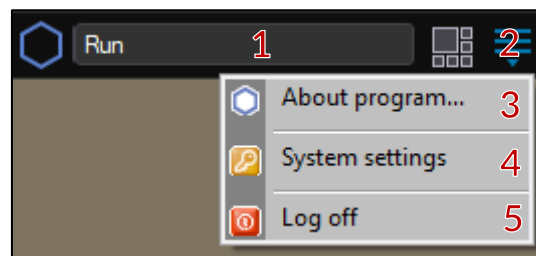
2. Working with AxxonSoft software

After starting the computer, AxxonSoft software program is started automatically. To start working with software, user must log in using login and password granted by the Administrator. If the default user is set, it will be logged in automatically and the interface configured as default will be displayed on the screen.

If the program is not running, call it from the shortcut on desktop  *Client's workplace*. However, if it is already running, the same icon should be in system tray (next to the clock).

2.1 Main menu

To open main program menu, move mouse cursor to the upper right corner of the screen, and then after quick access bar appears, click the left mouse button on  the icon .



1 - Quick access bar

2 - Icon opening the main program menu


3 - Informations about program

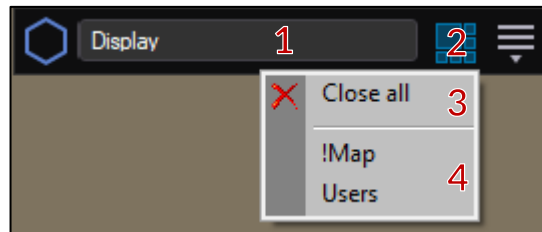
4 - System settings (available for administrator)

5 - Log out the user and close program

If macros available to the operator have been created in the system, they will be displayed above **3- Information about program**. Clicking on them will bring them up.

2.2 Choosing an interface

Interface is a graphical program window containing selected software functions depending on the purpose. To change currently displayed interface, move mouse cursor to the upper right corner of screen, and then after quick access bar appears,  select icon by clicking left mouse button. In the next step, select interface from displayed list.



1 - Quick access bar

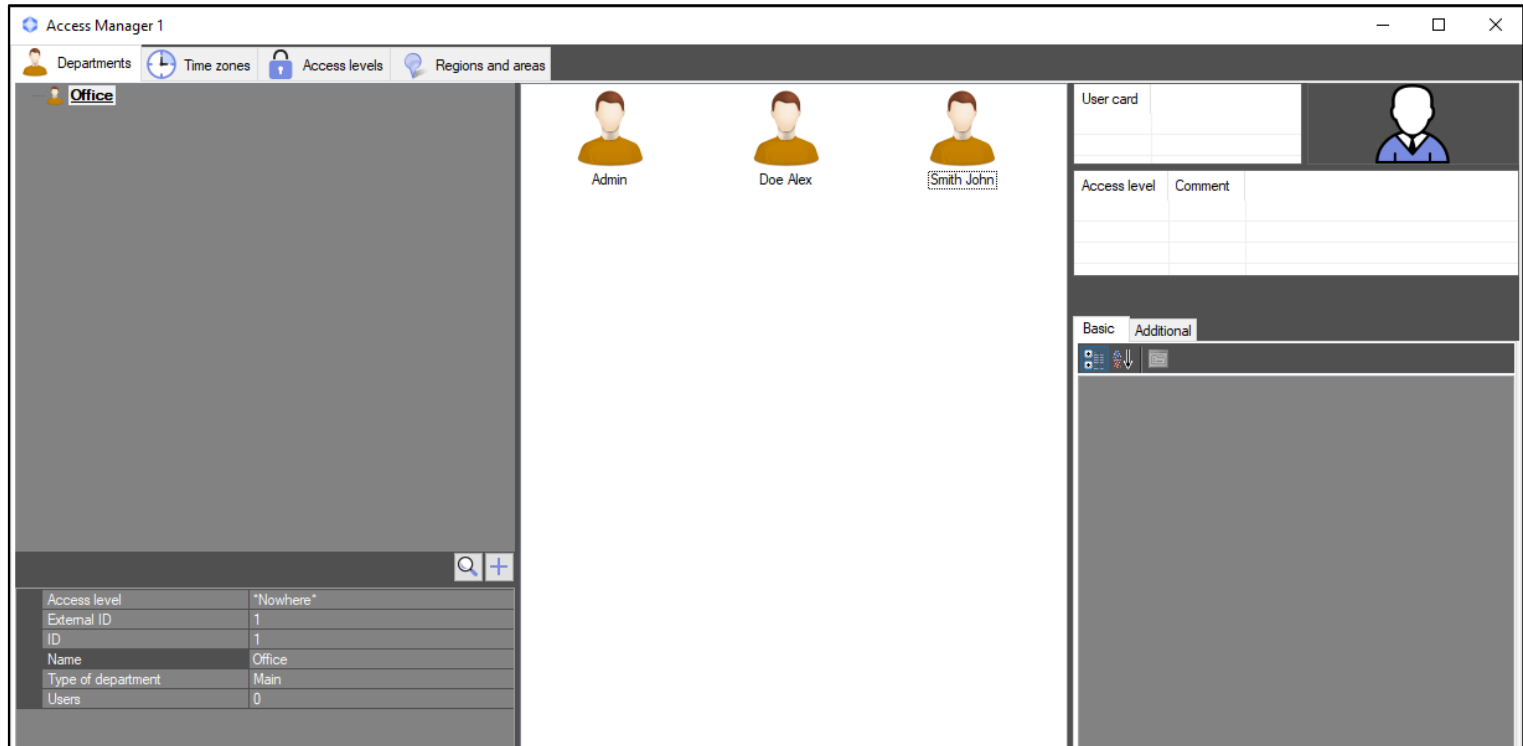
2 - Icon opening Interface list menu

3 - Close all interfaces

4 - Interfaces available to the operator

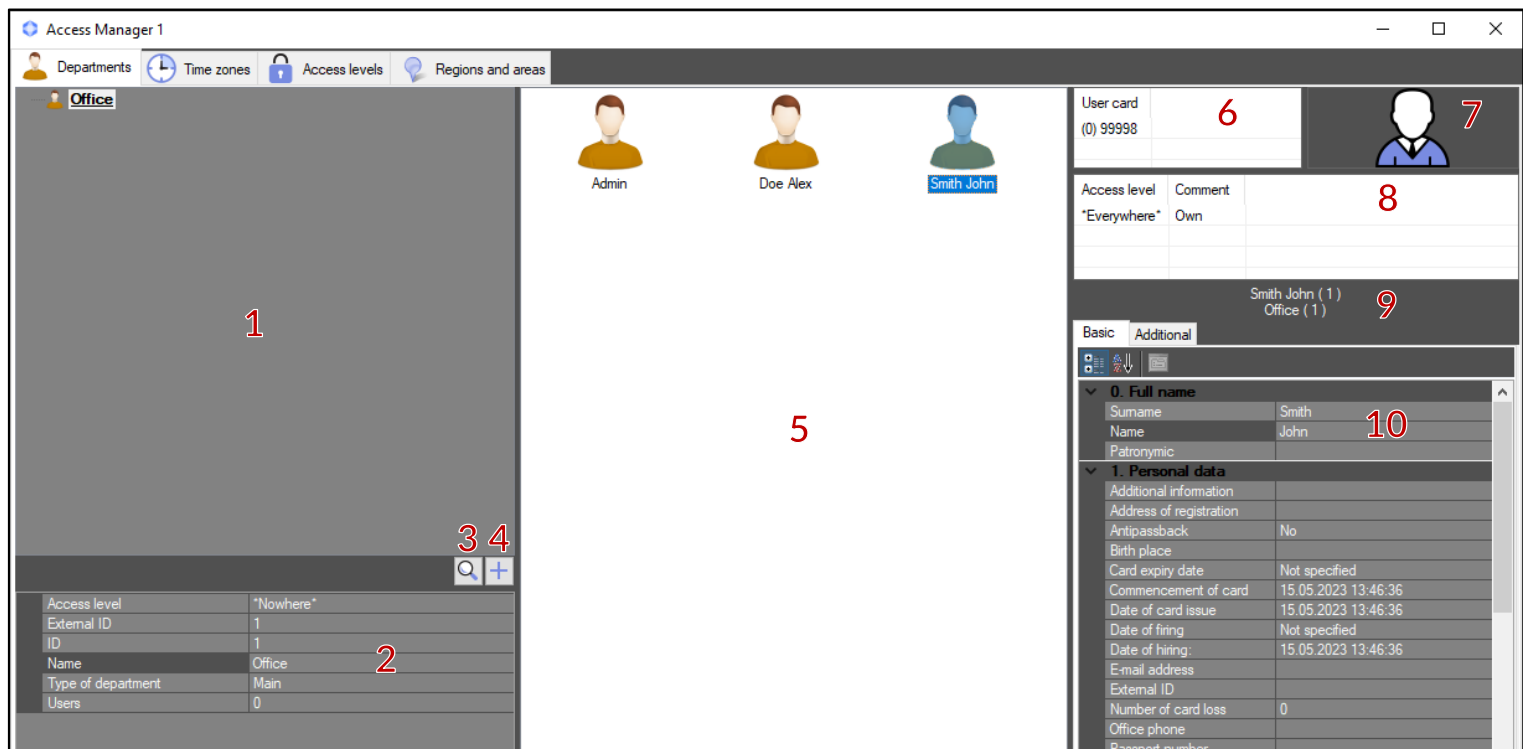
3. Access Control Panel

Access Control Panel is used to manage departments, users, access levels (PD) and schedules. AC panel is available in one of interfaces from quick access bar.



3.1 Departments

The tab enables creating and editing users (assigning cards, adding access levels, etc.) and assigning them to appropriate departments.



The screenshot shows the 'Access Manager 1' application interface. The 'Departments' tab is active, displaying a tree structure of departments (1), a list of users (Admin, Doe Alex, Smith John) (5), and a detailed user profile for 'Smith John' (10). The profile includes fields for 'Full name', 'Personal data', and 'Card information'. The 'Access level' is set to 'Everywhere' (8), and the 'User card' is (0) 99998 (6). The 'Department' is 'Office' (2), and the 'Number of users' is 0. The 'Access level' is 'Nowhere'.

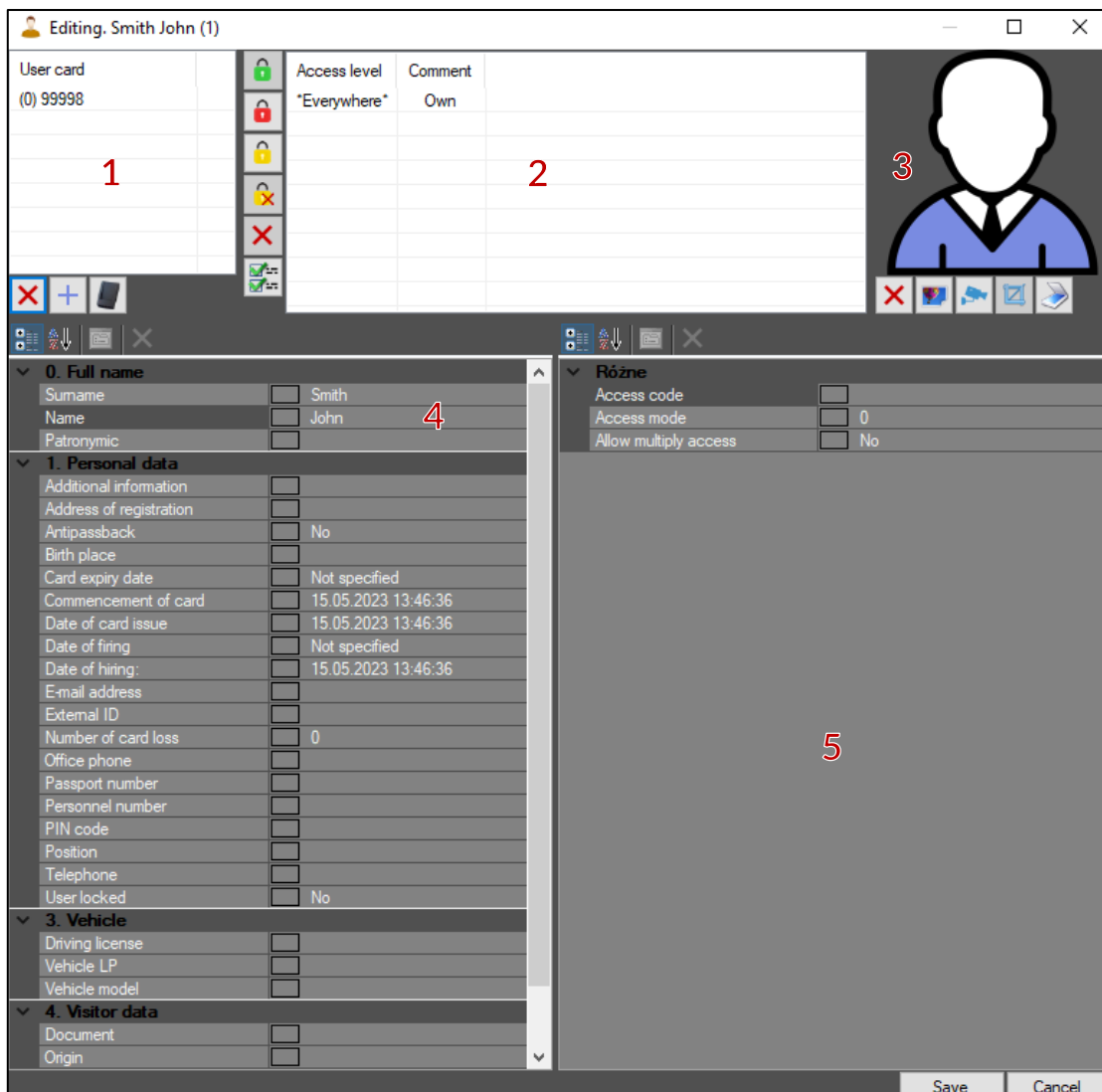
1 – Structured tree of departments - presentation of the entire structure of created departments and subdivisions in the form of an expandable tree. After clicking on the department, users will be displayed. context menu is available using the right mouse button; clicking on sections: **Delete department, Replace, Create subsidiary department, Department report**. The first three are used to work on the structure of departments, the last one to generate following reports

2 – Department basic parameters - when clicking on a department, basic information about the department is obtained, such as: default access level, department type, number of users.

- 5 – *List of users from department* - the list of users assigned to department. If you click on a user, information about that user will be displayed (items 6-10).
- 6 – *List of space cards assigned to the user* - user cards (several cards may be added to a user).
- 7 – *User photo* - if assigned, the user's photo will be displayed here.
- 8 – *List of user access levels* - access levels assigned to the user.
- 9 – *User information* – ID, actual region, department
- 10 – *User parameters* - displays all user parameters

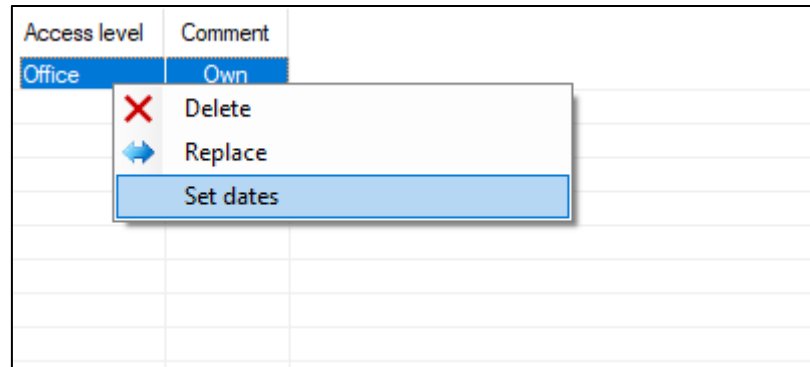
3.1.1 Create and edit a user

To add user to a specific department, select this section and then right-click on the white background in the middle part of the window. Select **New**, from context menu that appears, and then enter **Surname and Name** of the user you are creating and click **OK**. A user editing window appears in which all the parameters relating to the user must be specified. The items contained in this window depend on the rights of the operator.

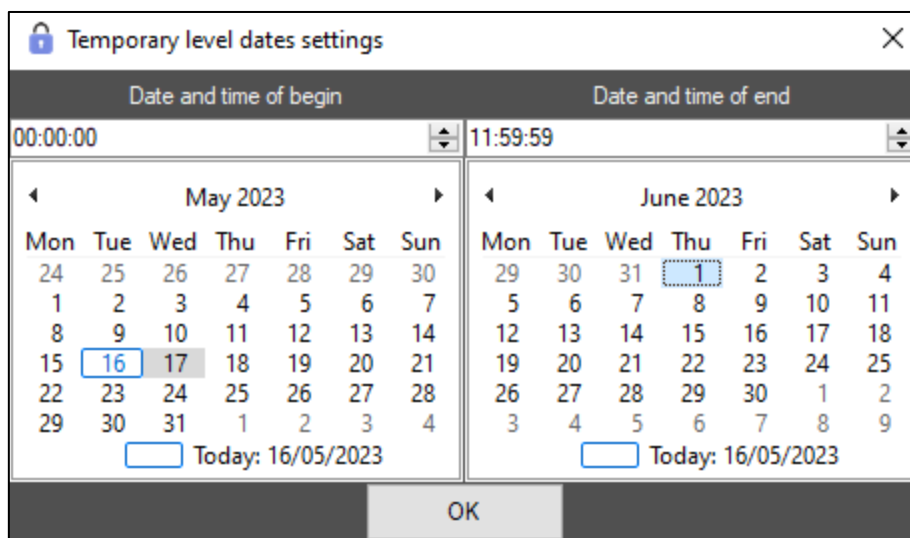


The screenshot shows a software window titled "Editing. Smith John (1)". The top part contains a table for "User card" with columns for "Access level" and "Comment". Below the table are several icons for managing access levels (lock, unlock, delete, add). To the right is a placeholder for a user photo. The bottom part of the window is a form with various fields categorized into sections: "0. Full name", "1. Personal data", "3. Vehicle", and "4. Visitor data". A "Różne" (Other) section is also present. Red numbers 1 through 5 are overlaid on the image to highlight specific elements: 1 points to the user card table, 2 to the access level table, 3 to the photo placeholder, 4 to the name fields, and 5 to the "Różne" section.

Operator can create temporary access levels for the user. To do this, right-click on the selected access level and select **Set dates**.





In the next step, select the beginning and end of the temporary access level.



The dates in the temporary access levels are crossed out before and after they start.

Access level	Comment	Start	End
Office	Own	17/05/2023 00:00:00	01/06/2023 11:59:59

3 - User photo - the operator has the option to assign a photo to a user:

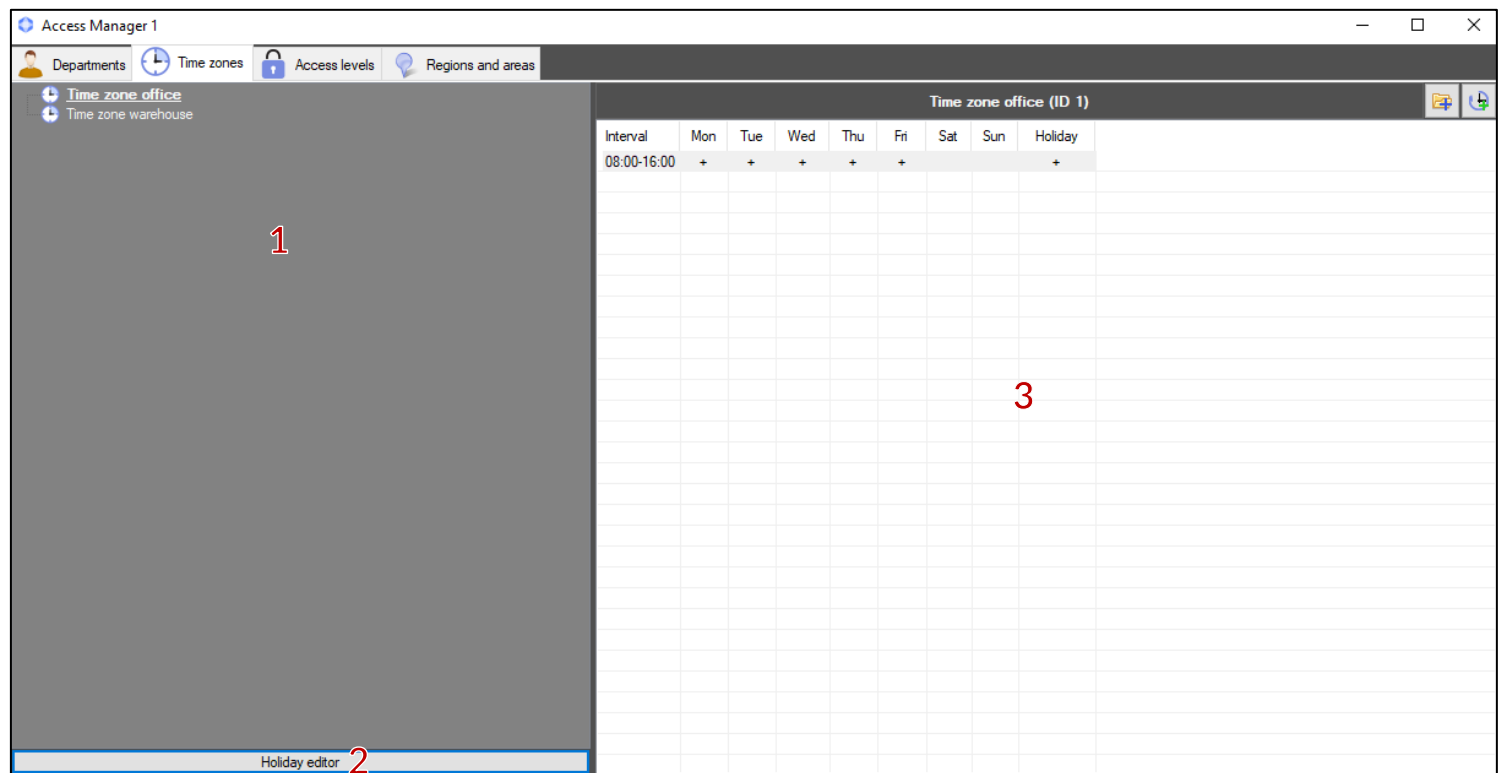
-  **Select file** - bmp, jpg or png formats are supported.
-  **From camera** - choose camera to capture photos for this interface.

4 - User information - standard fields where user information can be edited: first name, last name, car, PIN code, card expiry date, etc.

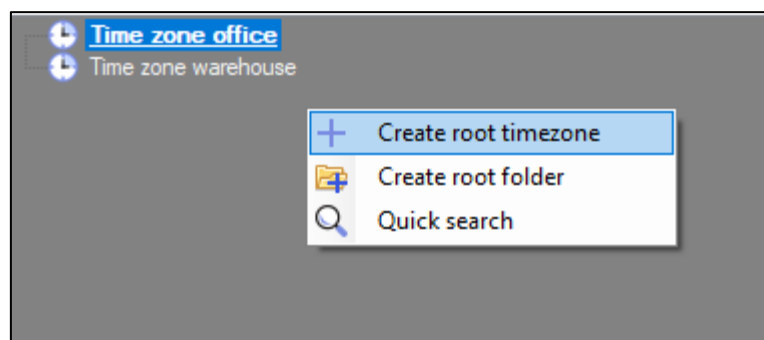
5 - User information - additional fields where user information can be edited: allowing multiple access, biometrics, etc.

3.2 Time zones

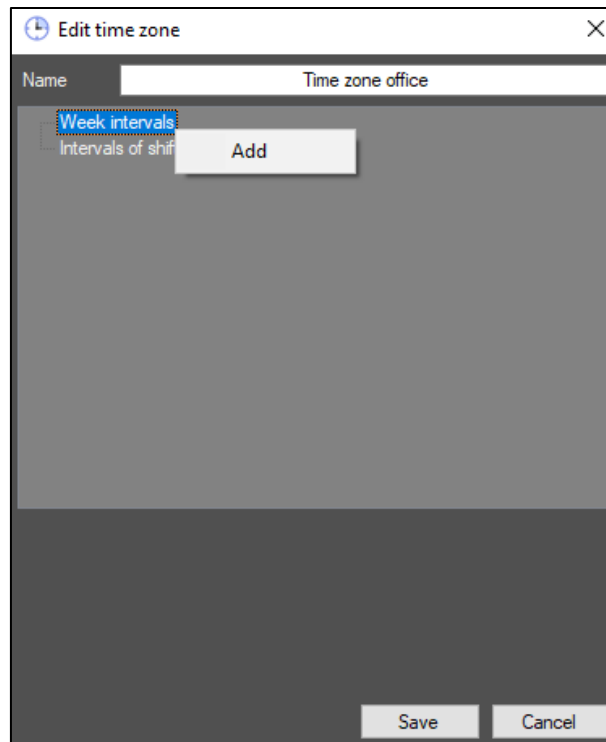
Time zone allow easy configuration of access control for users and devices in the case of repetitive operation, e.g. fixed office opening hours or guard rounds. The time zone created can apply not only to Noder access control devices.



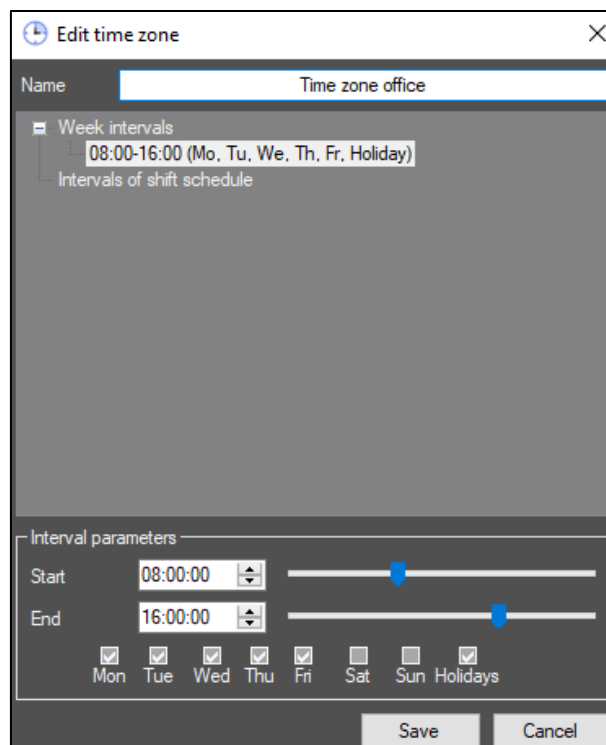
1 - List of time zones - double-click on the name to edit the time zones and their associated time intervals, weekdays and holidays. To add a new time zones, right-click on the background and select **Create root timezone**.



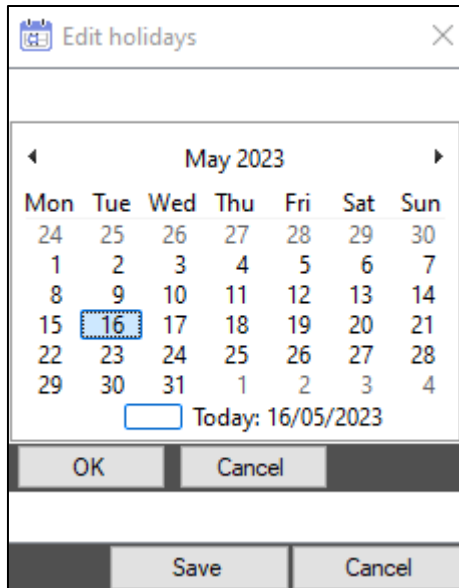
After selecting the option, the time zone editing window will open. Noder KD and SSWiN systems support **Weeks intervals**. After clicking on it with the right mouse button, add such a schedule.



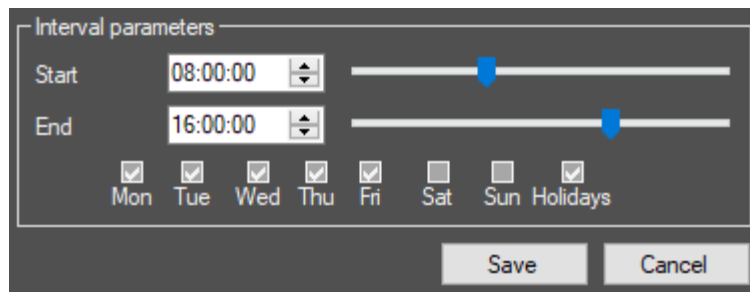
In the next step, select the days of the week and times belonging to the schedule.



2 - **Holiday editor** - a tool for adding holidays. After clicking on the button, the *Edit holidays* window will open. After that, right-click and from context menu choose **Add**. Choose holiday day and click **OK**.



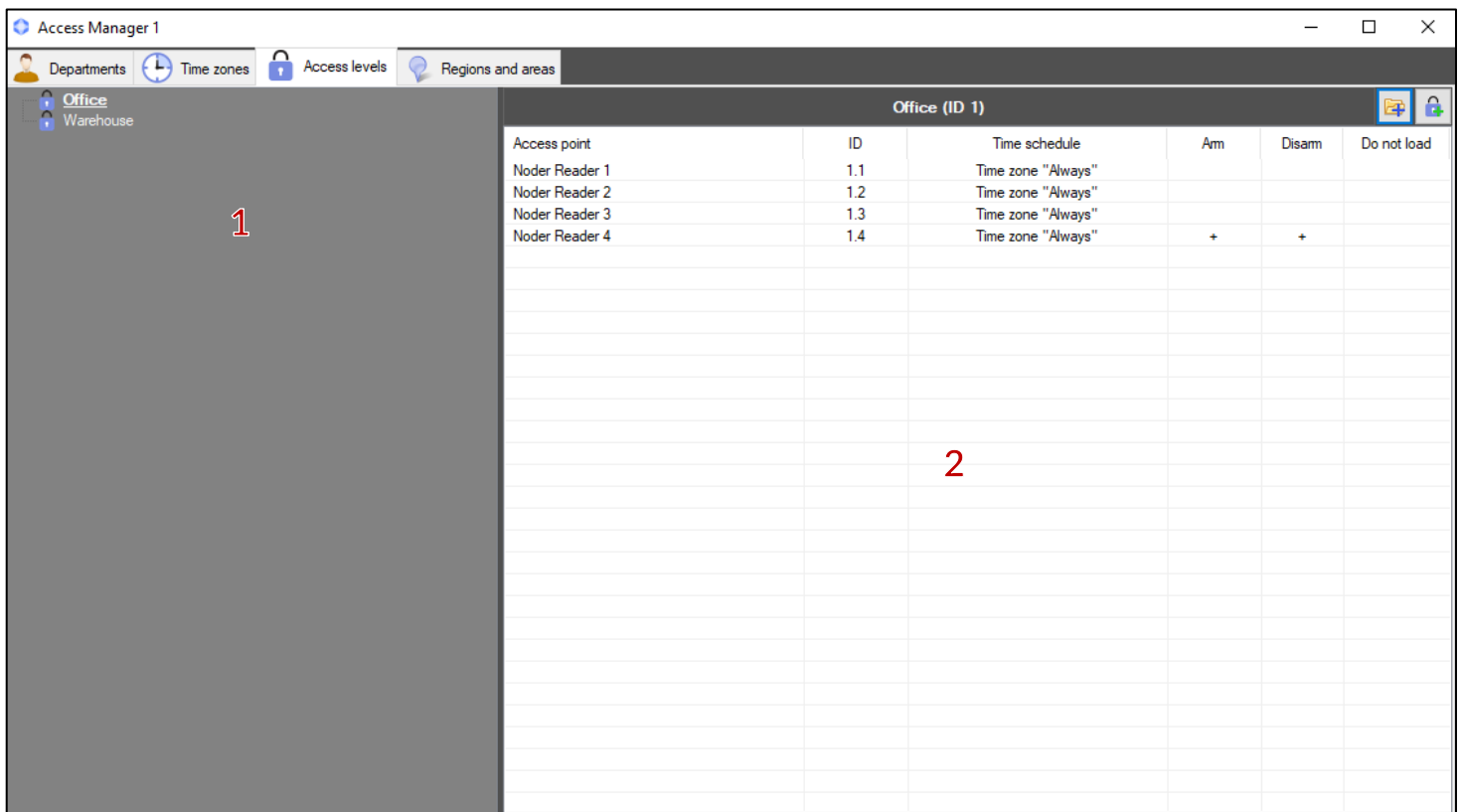
To add a public holiday to the schedule, select the No holidays option in the schedule.




3 - **Time zones intervals** - time intervals belonging to the schedule. The operator is able to quickly view which time intervals belong to the schedule.

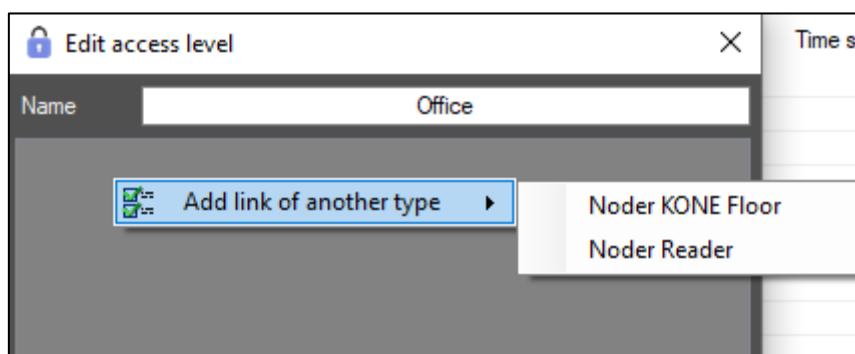
3.3 Access levels

Access levels define sets of devices (readers) to which the user has access in the time frame of the schedule. It is possible to catalog access levels.

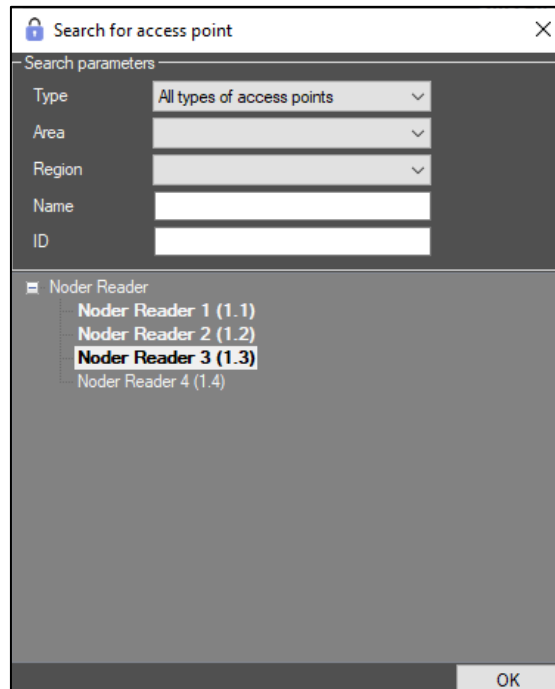


Access point	ID	Time schedule	Am	Disam	Do not load
Noder Reader 1	1.1	Time zone "Always"			
Noder Reader 2	1.2	Time zone "Always"			
Noder Reader 3	1.3	Time zone "Always"			
Noder Reader 4	1.4	Time zone "Always"	+	+	

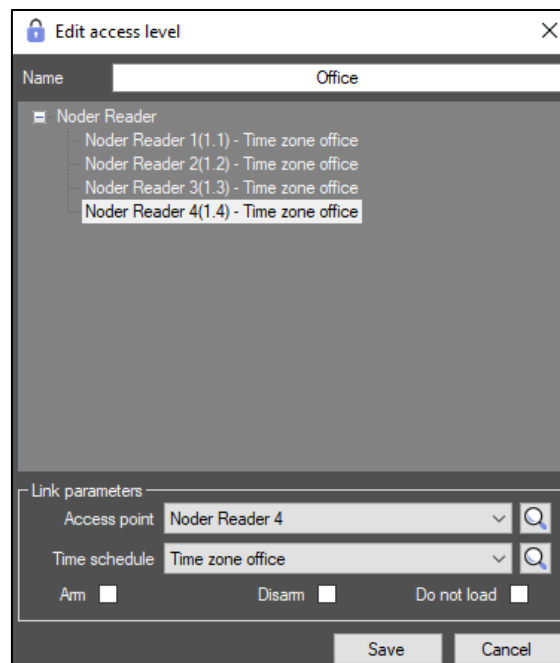
1 - Access levels list - list of created access levels. To create a new access level, right click and select **Create root level** . In the window that opens, right-click and select **Add link of another type**. In the case of adding a Noder Reader, this will be the **Noder Reader** object. The system allows you to add several types of devices to an Access Level.



In the next step, select the devices and click on them twice (the selected items will be bolded).



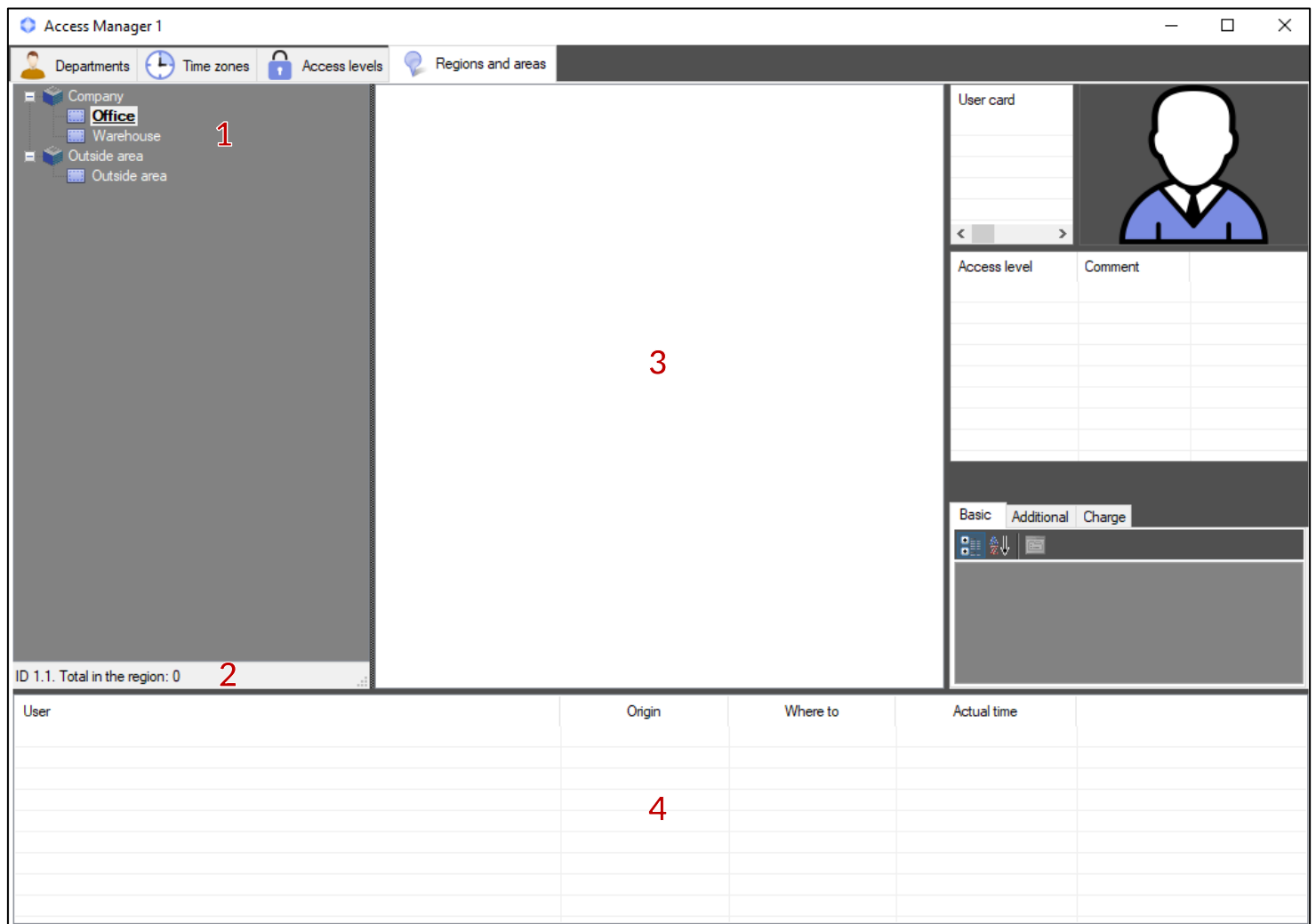
The next step is to select which schedule each device is to be part of. If the reader is to be used for arming and disarming a partition in SSWIN, select **Arm** and **Disarm**.



2 - Items in the access level - a list of items included in that Access Level. Clicking on a particular access level will display information about the devices and schedules associated with it.

3.4 Regions and areas

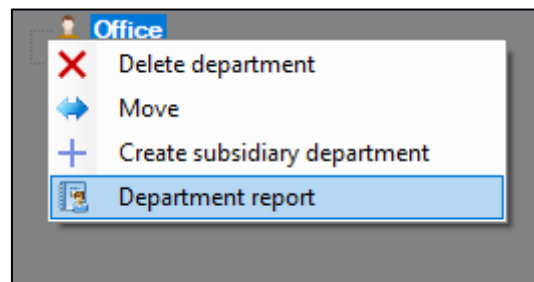
The card allows the current location of users to be checked. Assigning users to zones is essential for use in the AntiPassBack system.



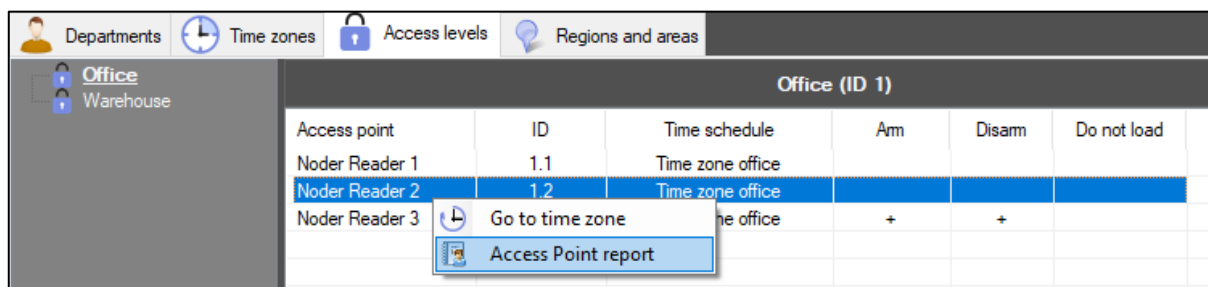
- 1 – *Tree of regions and areas* – tree containing areas and the regions assigned to them.
- 2 – *Region/area ID and number of people in the region/area* – when you click on a area or region, its ID and the number of people in it are displayed.
- 3 – *List of people in a region/area* – list of people located in a region/area. When you click on a user, information about that user is displayed in the right-hand part of the window (described in [3.1 Departments](#)).
- 4 – *Relocation information* – information on recent relocation of users.

3.5 Reports

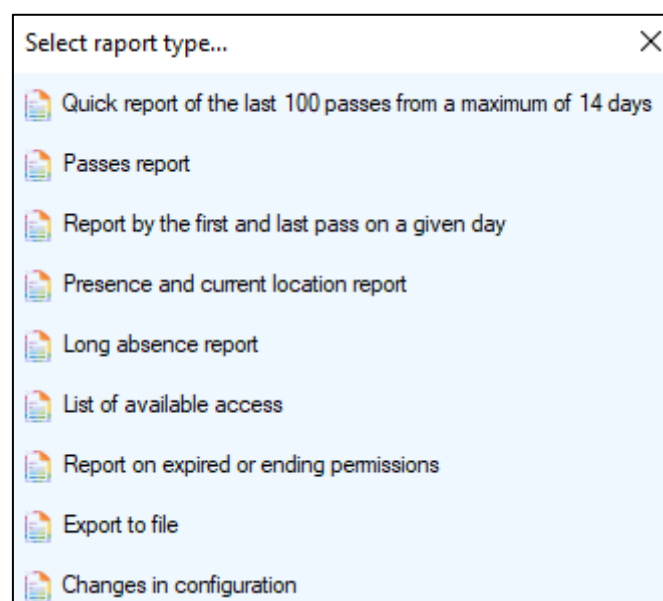
Operator can generate reports for a Department, individual users or a selected access point. After right-click on a department or specific user, select **Department reports**.



For an access point report, go to the **Access Levels** tab and select the access point. In the context menu, you need to select **Access Point report**.



Depending on the object, a window will appear with reports to choose from. Example report for a specific department:



Please note that the availability of fields in the reports depends on the access levels in Access Manager.

After filtering the results to be displayed, click Generate. A window will open with the events, which can be exported to Excel or CSV.


Report of the last 100 events from 14 days. Report of the day: 2023-05-19 09:01:52

Export to Excel Export to CSV file Search:

Access point name	Event	Additional information	Date and time	Card used
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 08:43:27	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 08:43:22	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 08:43:17	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 08:43:12	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 08:43:07	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 08:43:03	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 08:42:58	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 08:02:51	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 08:00:53	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 08:00:46	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 08:00:32	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 08:00:24	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 08:00:19	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 08:00:12	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 08:00:04	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 07:59:57	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 07:59:51	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 07:59:45	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 07:59:37	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 07:59:30	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 07:59:18	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 07:59:11	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 07:59:06	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-19 07:59:02	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-18 11:20:56	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-18 11:20:50	(0) 30896
Noder Reader 1	No passage after access was granted	Smith John	2023-05-18 11:20:00	(0) 30896

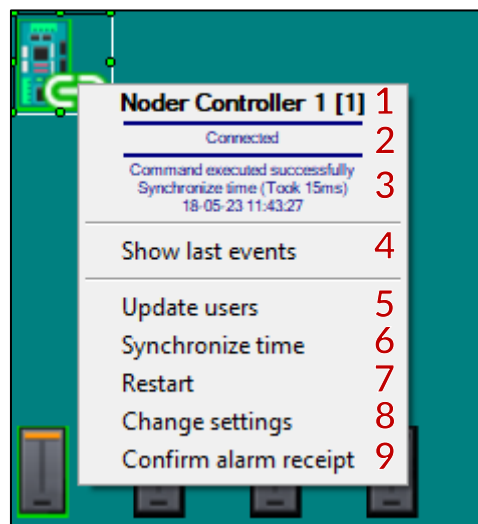
Rows: 27 Columns: 5 Cells: 135 v1.7.0.42 Generated in 499ms

4. Noder Access Control visualisation

To start the appropriate interface containing visualization of Noder Access Control System, move the mouse cursor to the upper right corner of the screen, and then after displaying the quick access bar, select icon  by clicking the left mouse button. In the next step, select interface from displayed list.







4.1 Noder Controller





To display the context menu for the controller, right-click on its icon. In the next step, select appropriate action from displayed list.



1 – *Controller name* –current name of controller.

2 – *Current state* –current status of controller:

Current state	Icon	Description
Connected		status indicating that controller is connected to the central system and works online
No connection		status indicating that controller is not connected to the central system and works offline or has no power supply
Unknown state		system does not read the current status of controller
Updating users		status informing about user update process on the controller
Connection secured		Status informing about a secure connection after configuring the firewall and SSH tunneling
No 230V AC power supply		status informing about no 230V power supply

Battery voltage low		status informing about discharging batteries
Housing tamper		status informing about the opening of controller or battery housing
Power supply failure		status informing about damage 12V DC power supply
DEC off		status, which follows <i>DEC output and reader power supply</i> command. the status informs that the readers connected to the controller ports and devices connected to the DEC output are disconnected from the power supply

3 - *Last action* - last action performed on controller.

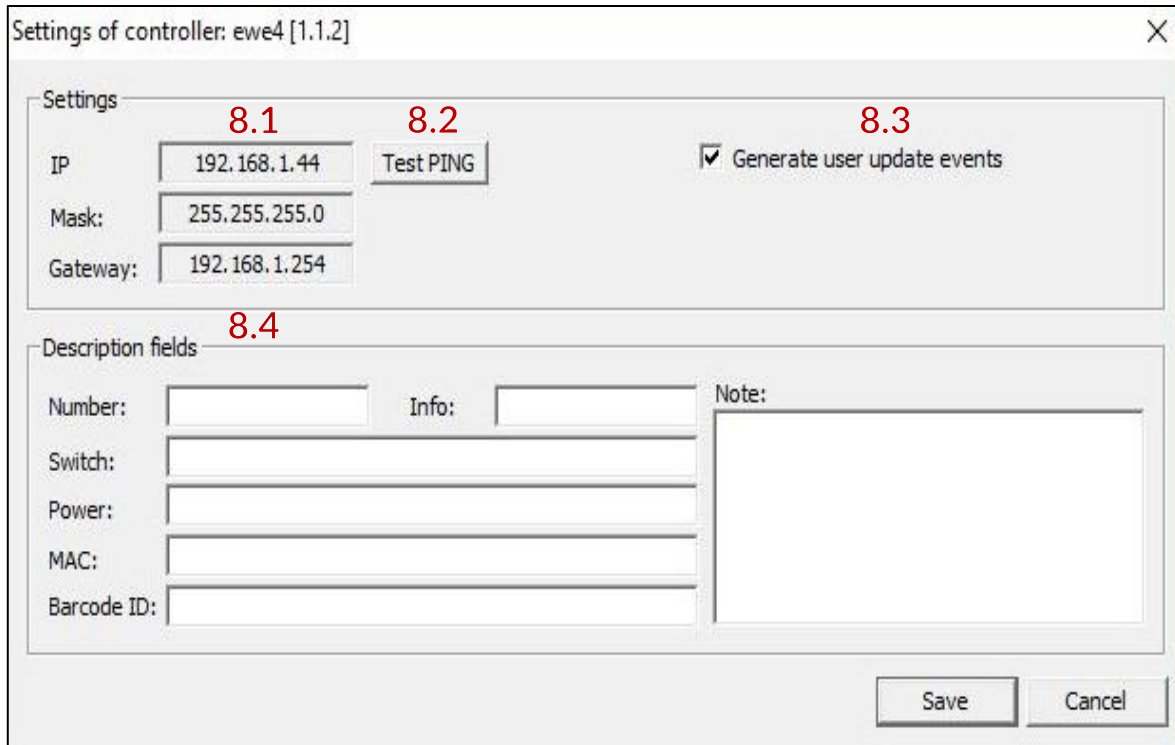
4 - *Show last events* - option allowing to open a window in which the last events called on controller will be displayed (since the last time the system operator logged in at a given client station, but no more than 50 events). If controller is in offline mode, the information will be displayed as described in the section *Last events*.

5 - *Update users* - command allowing to update the user database on controller, according to the user database on the server. During upgrade process, it is not possible to perform additional operations on controller. All invoked operations will be performed after the users have been updated. This process does not interfere with operation of transitions and receiving current events. Upgrade process can take anywhere from 10 to 30 minutes.

6 - *Synchronize time* - command enabling time synchronization on a controller with the main AC server.

7 - *Restart* - restart controller.

8 – Change settings – option allows to open a window containing the settings of controller. To make changes to controller, click the left mouse button and select **Change settings** from context menu.



8.1 – Controller network setting – non-editable fields informing about the network settings of a specific controller.

8.2 – Test PING – allows to call a window in which you can check controller's network connection.

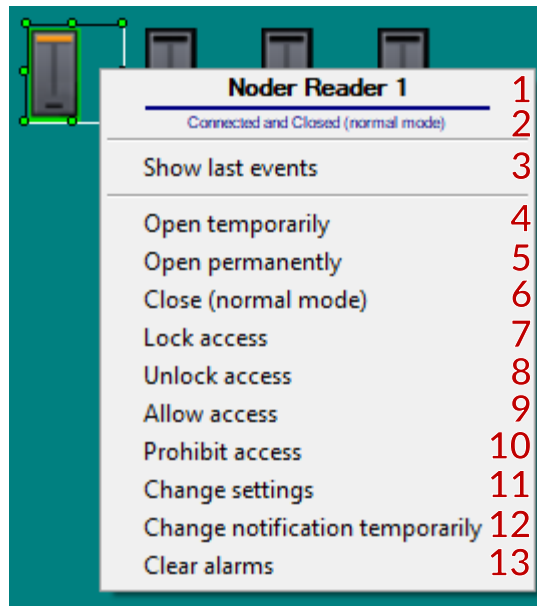
8.3 – Generate user update events – if this option is checked and controller works online, an event will be generated confirming that the user has been updated on controller. However, if there is no connection to controller **Update users Link lost** event will be generated, Unchecking this option will cause that an event confirming the user update will not be generated, however, an event will always be generated if this update fails.

8.4 – Description fields - editable fields that allow you to enter additional information about the controller in question. The settings do not affect the operation of the controller.

9 – Confirm alarm receipt - operator has the ability to accept the alarm








4.2 Noder Reader











To display the context menu for the selected reader, right-click on the reader icon. In the next step, select the appropriate action from displayed list.



1 - *Reader name* - current name of reader.

2 - *Current state* - current status of the reader:

Current state	Icon	Description
Connected		status informing that reader is connected to controller and both the reader and the transition are operating correctly
No connection		status informing that reader is not connected to controller or controller is not connected to the central system and works offline
Unknown state		status informing that system does not read current reader status
No connection		status informing that reader's mode of operation is set to inactive, unable to pass using the card/face/PIN
Reader updating		status informing that reader firmware updating
Unlocked		status informing that transition has been opened
<i>Exit button pushed</i>		status informing that exit button has been pressed, option to go without using a card on reader

Door open		status informing that transition has been physically opened
Locked (by system command)		status informing that reader's mode of operation is set as blocked, no possibility of using the card and exit button (<i>for two-sided passage also on the second reader</i>)
Locked by sluce logic		status informing that reader's mode of operation is set as blocked by input activation, no possibility of using the card on reader
Reader locked		status informing that reader has been blocked by System Administrator. Exit button or second reader on passage are no locked
Door violation		status informing that passage violation. Status ends after closing the door
Door hold		status informing that passage hold (door open too long after authorized access). Status ends after closing the door
Alarm		status informing that alarm on passage after forcing or too long-open transition. The time after which the status disappears depends on the reader alarming settings
Emergency exit button pressed		status informing that emergency exit button was pressed
Door unlocked too long		status informing that door was unlocked too long after <i>Open permanently</i> command
Reader tamper violation		status informing about reader tamper violation on reader

3 – **Show last event** – option to open a window in which events related to the selected transition will be displayed (since the last time the system operator logged in at a given client station, but no more than 50 events). In the absence of connection to the reader, information will be displayed as described in point: **Last events**.

4 – **Open temporarily** – functionality allows to open the door for a specified time (default 4s). This time can be changed in the parameter of selected reader: **Opening time (sec.)**

5 – **Open permanently** – functionality allows to open the transition permanently, until command **Close** will be called. In the time, you can use transition without using the card and the exit button, executive elements (jumper, electric strike, etc.) are released. The diode on reader lights up green.

6 – **Close (normal mode)** – an option enabling system to close the door, after it has been opened (**Open temporarily, Open permanently**) or locked (**Lock access**) earlier. The actuators will be blocked, the LED on reader turns red. To use selected transition, use ID or exit button.

- 7 - **Lock access** - functionality allows blocking selected transition. It is not possible to use transition using the ID or exit button. Actuators remain in the state before the function was called (if the door was closed - it remains closed, if it was permanently unlocked - it remains permanently unlocked). Using an identifier on such a transition will generate an event: **Using the card when the entrance is locked**, using the exit button will generate an event: **Using exit button at a door locked by server command**, in case of forcing the door, system will generate an event: **Door violation**.
- 8 - **Unlock access** -- an option enabling system to close the door (normal mode) after Locking access.
- 9 - **Allow access** - option allows to admit access by the Operator in the system. Controller must be in mode **Online - Operator** decides for the function to work.
- 10 - **Prohibit access** - option allows the Operator to reject the request for access in the system from running AntiPassBack and the selected function **Operator decides**.
- 11 - **Change settings** - option that allows to open a window containing the settings of selected door/reader. To make changes concerning selected passage/reader, click the left mouse button and select **Update settings** from context menu.

Settings of reader: Noder Reader 1 [1.1]

Settings

State: **11.1** Active

Name: Noder Reader 1

Door output settings **11.2**

Opening time [s]: 4.0

Block after: door opening time

Delay of the door lock [s]: 0.3

Do not log events **11.6**

Opening by exit button

Access denied

Access denied (antipassback)

End of violation of door sensor

End of door hold on

Signaling on door hold (0 = function disabled) **11.3**

Time to close the door [s]: 20.0

Delay of door hold event [s]: 10.0

Time to close the door after unlock [s]: 0 (0d 0h 0min)

Work schedule **11.7**

Unlocked:

Alarms **11.4**

Alarm activation time (0 = endless) [s]: 5.0

Sound signal on alarm

End alarm after the violation

Alarm on door violation (arm)

Access granted settings **11.8**

Sound signal for authorized card

Enable tracking of access transaction

Send access granted event

Send event if there was no passage

Settings of multiple access **11.5**

Second access prohibited in time [s]: 60.0 (Ask Administrator to enable this feature on the server)

Descriptions fields **11.1**

Number: Info: Barcode ID: Notes:

Save Cancel

11.1 – State – mode of operation of reader:

- **Active (default)** - normal operation of the reader in logic. Default state: **Connected/Closed (normal mode)**.
- **Inactive** - reader inactive, card will not be read in the system. The LED on the reader will be off and there will be a short blink of the red LED when the card is applied. Physical disconnection of the reader, forcing a passage or using the exit button will not be recorded in the system. System commands (**Open once, Close (normal mode), Lock access**) will not work.
- **Locked** - the reader is locked, the card is being read. The LED on the reader is off in the normal state. When a card (authorized or unauthorized) is inserted, the LED on the reader flashes red, followed by 2 orange LED flashes and a beep at a frequency of 2 Hz. The physical disconnection of the reader is not recorded on the map. The system commands (**Open once, Close (normal mode), Lock access**) do not work. The exit button assigned to a passage works correctly.

11.2 – Door output settings - options allow the operation of the actuator to be tailored to the needs of the system.

- **Opening time [s]** – time, after which the passage will be locked after the card is applied, the exit button is pressed, or the **Open temporarily** command is used once.
- **Block after** – this option allows the passage to be closed earlier after the **door opening** or the **door closing**. Selecting **door opening time** closes the door after the **Door Open Time [s]**.
- **Delay of the door lock [s]** – this option enables adding a time delay after which the passage is locked for the option **Lock after: door opening and door closing**.

11.3 – Signaling on door hold – options allow you to adapt the time the door is open to the needs of the system.

- **Time to close the door [s]** – time after which the user is warned to hold the door. If this time is exceeded, a signal is emitted at the reader (beep of the reader and an orange diode at a frequency of 1 Hz). Setting a value of 0 disables the option.
- **Delay of door hold event [s]** – after the Delay of door hold has elapsed, the user is warned to hold the door (reader beep and orange LED at 1Hz frequency). The warning time for the user, depends on this parameter. If the door is not closed within time, an alarm is generated in the system (**Door open to long** event) and on the reader (beep and orange LED at 2.5 Hz) for the **Alarm activation time [s]**. The light signal is switched off when the violation has ceased.
- **Time to close the door after unlock [s]** – time to close door after **Open permanently** or **schedule**. When the time expires, the Open permanently door is generated and orange diode sound and light signal is generated with the frequency 1Hz for the **Alarm activation time [s]** (alarm relay is not activated). Subsequent events and signaling are triggered cyclically every **Time to close the door after unlock [s]**.

11.4 – Alarms – allow the alarm method to be adapted to the needs of the system.

- **Alarm activation time [s]** – parameter determines the time during which reader signals an alarm situation (flashing of the diode and sound signaling) – forcing or too long-open transition. If the cause of the alarm does not stop, the acoustic signaling will be repeated every 24 hours. The visual indication is kept until the cause of the alarm is removed. The signaling is as follows:
 - **when door are violated** – continuous sound for **Alarm activation time**/end of violation, LED flashes orange at approximately 2/3 Hz to end of violation
 - **when door are held** – sound signal with a frequency of about 2.5 Hz for **Alarm activation time**/end of door hold and the LED blinking in orange at the same frequency
- **Sound signal on alarm** – when option is not selected, alarm on reader is signaled only by the orange blinking diode.

- **End alarm after the violation** – when option is selected, in the event of an alarm (forcing or a long-open transition) the acoustic and visual signaling is deleted immediately after the cause of alarm has been ended (closing the transition). Otherwise, audible alarm is signaled by **Alarm activation time**. If this option is not selected, the LED diode on reader will continue to flash orange after alarm time, until the authorized card is applied to reader/operator **Clear alarms** command.
- **Alarm on door violation (arm)** – this option allows you to disable the generation of an alarm in the event of an unauthorized opening door. The function of signaling an overly long open passage will still work.

11.5 – Settings of multiple access – allows you to set the time after which the authorized user will be able to use the reader again. The activation of the option is dependent on the system administrator.

11.6 – Do not log events – enables to disable logging of some events in the central system.

11.7 – Work schedule – the option enables the door to be unblocked according to a previously set schedule.

11.8 – Access granted settings – allow the behavior of the reader and the events sent by the controller to be adapted to the needs of the system.

- **Sound signal for authorized card** – unchecking the option turns off the sound signaling for the authorized card (only the green LED lights up on the reader).
- **Enable tracking of access transaction** – if option is deselected, an event is generated immediately after the application of the approved card: **Access in**. If option is selected, an event **Access in** is generated only after opening the door. Also when this function is enabled, two other settings are possible:
 - **Send access granted event** – if this option is selected, an event **Access granted** is generated for the user when a authorized card is applied.
 - **Send event if there was no passage** – selecting this option will result in the application of a authorized card, if the door is not opened, then after **Door opening time**, event **No passage after access was granted** will be generated.

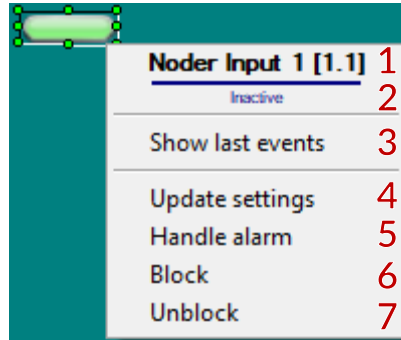
11.9 – Descriptions fields – editable fields that allows to enter any description for reader or transition.

12 – Change notification temporarily – temporarily changes the light and sound signals. The default setting is 5 beeps and a green flash

13 – Clear alarms – clears the alarm status at the specific reader. If the option End alarm after the violation is not selected, the alarm states will not be cleared immediately after the cause of the alarm ceases.










4.3 Noder Input

















To display the context menu for the selected input, right-click on the input icon. In the next step, select the appropriate action from displayed list.

















1 - **Input name** -current name of input.

2 - **Current state** -current status of input:

Current state	Icon	Icon name	Description
Inactive		Door	input icons for Off/Normal state (option <i>Reverse logic</i> unchecked)
		Door sensor	
		Emergency button	
		Exit button	
		Green-red bulb	
		Green-red flasher	
		Green-red LED	
		Module input	
		Module output	

		Padlock	
		Switch	
		White-green bulb, White-red bulb, White-green bulb	
		White-yellow flasher	
Active		Door	
		Door sensor	
		Emergency button	
		Exit button	
		Green-red bulb	
		Green-red flasher	input icons for Active state (option <i>Reverse logic</i> unchecked). For notification modes Normal/Alarm and Normal/Failure icons flash at 1 Hz.
		Green-red LED	
		Module input	
		Module output	
		Padlock	
		Switch	
		White-green bulb, White-red bulb, White-yellow bulb	

		White-yellow flasher	
		Door	
		Door sensor	
		Emergency button	
		Exit button	
		Green-red bulb	
		Green-red flasher	
Disabled by operator		Green-red LED	input disabled by operator.
		Module input	
		Module output	
		Padlock	
		Switch	
		White-green bulb, White-red bulb, White-yellow bulb	
		White-yellow flasher	

3 – **Show last event** – option to open a window in which events related to the selected input will be displayed (since the last time the system operator logged in at a given client station, but no more than 50 events).

4 – **Update settings** – option opens a window where operator can disable input

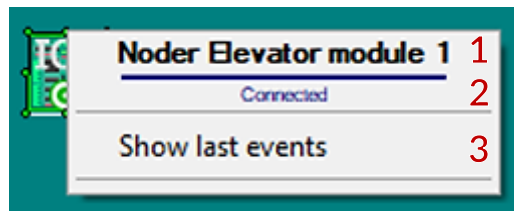
5 – **Handle alarm** – option not used in access control system

6 – **Block** – option not used in access control system. An **Failed to execute command** event will be received after the command.

7 - **Unblock** - option not used in access control system. . An **Failed to execute command** event will be received after the command




4.4 Noder Elevator module

To display the context menu for the selected elevator module, right-click on the input icon. In the next step, select the appropriate action from displayed list.



1 - **Elevator module name** -current name of elevator module.

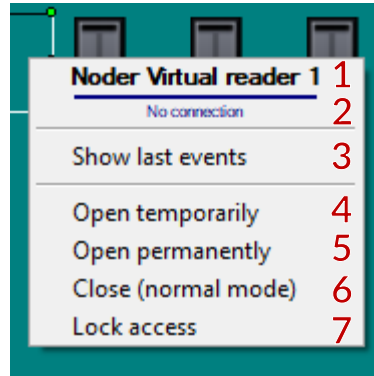
2 - **Current state** -current status of elevator module:

Current state	Icon	Description
Connected		status informing that elevator module is connected to controller
No connection		status informing that elevator module is not connected to controller or controller is not connected to the central system and works offline
Unknown state		status informing that system does not read current elevator module status

4 - **Show last event** - option to open a window in which events related to the selected module will be displayed (since the last time the system operator logged in at a given client station, but no more than 50 events).




4.4.1 Noder Floor

To display the context menu for the selected floor, right-click on the input icon. In the next step, select the appropriate action from displayed list.



1 – *Elevator module name* –current name of elevator module.

2 – *Current state* –current status of elevator module:

Current state	Icon	Description
Connected		status informing that reader is connected to controller and both the reader and the transition are operating correctly
No connection		status informing that reader is not connected to controller or controller is not connected to the central system and works offline
Unlocked		status informing that floor relay has been opened

3 – *Show last event* – option to open a window in which events related to the selected floor will be displayed (since the last time the system operator logged in at a given client station, but no more than 50 events).

4 – *Open temporarily* – functionality allows to open relay of floor for a specified time (default 4s). This time can be changed in the parameter of selected floor: *Output opening time (sec.)*

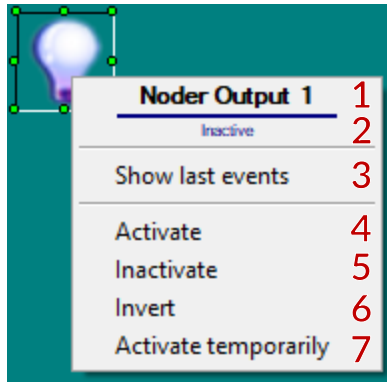
5 – *Open permanently* – functionality allows to open relay of floor permanently, until command *Close* will be called.

6 – *Close (normal mode)* – an option enabling system to close the relay of floor, after it has been opened (*Open temporarily, Open permanently*)

7 – *Lock access* – option enabling the system to block the module relay after an administrator command. Applying an authorized card will not open the relay.









4.5 Noder Output


To display the context menu for the selected output, right-click on the output icon. In the next step, select the appropriate action from displayed list.



1 – **Output name** –current name of output.

2 – **Current state** –current status of output:

Current state	Icon	Icon name	Description
Inactive		Door	output icons for inactive state (option <i>Reverse logic</i> unchecked)
		Door sensor	
		Emergency button	
		Exit button	
		Green-red bulb	
		Green-red flasher	
		Green-red LED	
		Module input	

		Module output	
		Padlock	
		Switch	
		White-green bulb, White-red bulb, White-green bulb	
		White-yellow flasher	
		Door	
		Door sensor	
		Emergency button	
		Exit button	
		Green-red bulb	
Active		Green-red flasher	output icons for Active state (option <i>Reverse logic</i> unchecked)..
		Green-red LED	
		Module input	
		Module output	
		Padlock	
		Switch	



White-green bulb,
White-red bulb,
White-yellow bulb




White-yellow
flasher

- 4 - **Show last event** - option to open a window in which events related to the selected output will be displayed (since the last time the system operator logged in at a given client station, but no more than 50 events).
- 5 - **Activate** - option activates relay output state.
- 6 - **Inactivate** - option deactivates relay output state.
- 7 - **Invert** - option change relay output state for invert.
- 7 - **Open temporarily** - the option generates a square wave at relay output (option *Default values* "Activate temporarily" command).

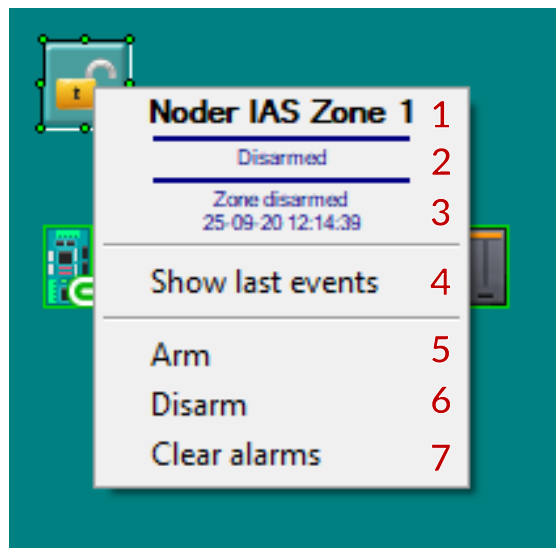


5. Noder Intruder alarm system visualisation

To start the appropriate interface containing visualization of Noder Intruder Alarm System, move the mouse cursor to the upper right corner of the screen, and then after displaying the quick access bar, select icon  by clicking the left mouse button. In the next step, select interface from displayed list.





5.1 Noder Zone



To display the context menu for the IAS Zone, right-click on its icon. In the next step, select appropriate action from displayed list.



1 – *Controller name* –current name of controller.

2 – *Current state* –current status of controller:

Current state	Icon	Description
Disarmed		status informing that zone is disarmed
Armed		status informing that zone is armed. The alarm will be triggered after the action according to the input setting (Noder M-EE12-EWE4-Start-up&Configuration – Inputs)
Fault		applies to EOL/2EOL inputs. Indicates a short circuit in the detector cables
Tamper		applies to EOL/2EOL inputs. Indicates a violation of the detector

Not ready to arm		status informing that zone cannot be armed
Alarm		status informing about alarm after input activation.

3 - *Last action* - last action on module

4 - *Show last event* - option to open a window in which events related to the selected IAS Zone will be displayed (since the last time the system operator logged in at a given client station, but no more than 50 events).

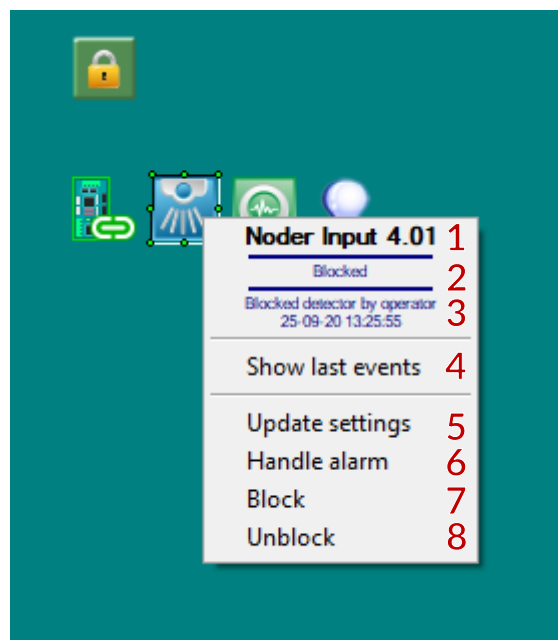
5 - *Arm* - arming the zone.

6 - *Disarm* - disarming the zone.

7 - *Clear alarms* - when an alarm or a tamper is triggered operator has the ability to disable the alarm.

5.2 Noder Input


















To display the context menu for the IAS Zone, right-click on its icon. In the next step, select appropriate action from displayed list





































1 - *Input name* - current name of input is.

2 - **Current state** - current status of the input:

Current state	Icon	Icon name	Description
Normal		Door sensor	status informing that output of detector is in normal state when zone is disarmed
		Acoustic	
		Magnetic detector	
		MCP	
		Panic button	
		PIR	
		PIR 360	
		Seismic detector	
		Smoke detector	
		White-yellow bulb	
Armed		Door sensor	status informing that output of detector is in normal state when zone is armed
		Acoustic	
		Magnetic detector	
		MCP	
		Panic button	

		PIR	
		PIR 360	
		Seismic detector	
		Smoke detector	
		White-yellow bulb	
Blocked		Door sensor	status informing that detector is disabled in the zone by operator
		Acoustic	
		Magnetic detector	
		MCP	
		Panic button	
		PIR	
		PIR 360	
		Seismic detector	
		Smoke detector	
		White-yellow bulb	
Actuated		Door sensor	status informing that output of detector is enabled when the zone is disarmed
		Acoustic	

		Magnetic detector	
		MCP	
		Panic button	
		PIR	
		PIR 360	
		Seismic detector	
		Smoke detector	
		White-yellow bulb	
		Door sensor	
		Acoustic	
		Magnetic detector	
		MCP	
Tamper		Panic button	applies to EOL/2EOL inputs. Indicates a violation of the detector.
		PIR	
		PIR 360	
		Seismic detector	
		Smoke detector	

		White-yellow bulb	
Fault		Door sensor	applies to EOL/2EOL inputs. Indicates a short circuit in the detector cables
		Acoustic	
		Magnetic detector	
		MCP	
		Panic button	
		PIR	
		PIR 360	
		Seismic detector	
		Smoke detector	
		White-yellow bulb	
Alarm		Door sensor	status informing about alarm after input activation
		Acoustic	
		Magnetic detector	
		MCP	
		Panic button	
		PIR	



PIR 360



Seismic detector



Smoke detector



White-yellow bulb

3 - Last action - last operator action on the input.

4 - Show last event - option to open a window in which events related to the selected input will be displayed (since the last time the system operator logged in at a given client station, but no more than 50 events).

5 - Update settings - window will be displayed in which you can enable/disable the input.

6 - Handle the alarm - deactivates alarm on outputs and readers.

7 - Block - detector connected to the input will not generate alarms.

8 - Unblock - return to normal detector state