Installation and operation manual

NOVUS MANAGEMENT SYSTEM AC

SOFTWARE FOR INTEGRATION, CONFIGURATION AND VISUALIZATION OF SECURITY SYSTEMS

Version 6.03.032 Update 04-08-2025

AAT SYSTEMY BEZPIECZEŃSTWA Sp. z o.o.
ul. Puławska 431, 02-801 Warszawa, tel. 22 546 05 46, faks 22 546 05 01
www.aat.pl

TABLE OF CONTENTS

What is it for and for whom this manual is intended.

This manual is intended for installers and individuals who want to familiarize themselves with the process of installing NOVUS MANAGEMENT SYSTEM AC, programming the system and verifying the correctness of its operation in terms of communication and utility. Therefore, it describes the next steps to follow to accomplish this. The manual is limited in its content to the most important steps needed to do this. The following steps are described in the recommended order of execution. This should make it much easier for people who need to perform only basic tasks related to the configuration of the devices included in the system, the addition of cards and users, together with privileges in terms of access to premises, checking the system status and generating basic reports.

Section 1. Introduction

1.1 Basic information

NOVUS MANAGEMENT SYSTEM AC is software that is a comprehensive solution for integrating systems physical access control , video surveillance, time and attendance, license plates recognition (LPR), intrusion & hold-up alarm systems, fire alarm and building automation. It works with the following devices in terms of individual systems.

Access control (AC): standard type controllers KDH-KS3012-IP, KDH-KS3024-IP, KDH-KS3000-IP-ELV, biometric KDH-KZ3000FP-IP-U,KDH-KZ3000FP-IP-M, integrated KDH-KZ3000-IP-U, KDH-KZ3000-IP-M, HID® Aero® controllers - X1100, HID® Aero® expansion modules- X100, X200, X300.

Time and attendance (T&A): terminal KDH-TA500C-IP-UMD i KDH-TA500CFP-IP-UMD

Video Surveillance System (VSS): NOVUS IP cameras 4000/6000/8000 series, IP NOVUS NVR's 4000/6000 series, multistandard NOVUS recorders 4000/6000 series, IP NOVUS MANAGEMENT SYSTEM VSS recorders, IP NMS recorders, and via the ONVIF/RTSP protocol with equipment from other manufacturers.

License plate recognition (LPR): IP cameras NVIP-2H-6732M/LPR, NVIP-4H-6732M/LPR from the 6000 series by NOVUS.

Intrusion & hold-up alarm systems (SSWiN): centrale alarmowe Integra firmy SATEL.

Fire alarm: Polon 6000

Building automation: Tinycontrol

Due to the client-server type structure, it is possible to operate it from multiple workstations (1 stations under a free license, additional after purchasing expansion licenses). The system is easy to install and has operator friendly graphical interface. Thanks to implementation several server advanced functions, it can also be used in systems with multiple locations.

The operator interface allows:

- defining system parameters (permissions for operators, licenses, backup)
- configuration of parameters of physical system components (controllers, doors, readers)
- configuration and visualization systems from many local servers in the same time
- defining logical elements (schedules, access levels, cards)
- define scenarios that automatically react to events in the system
- monitoring the status of the "on-line" system using the icons of system elements located on the site maps (with hierarchical structure), on the synoptic array and through the messages displayed on the event stack
- displaying user pictures after using the card
- displaying of cameras located in controlled passages automatically after an event or by clicking on the icon
- Floor access control through a reader located in the elevator cab with the option to unlock all or selected floors by the operator or scheduler; (* option available soon)
- generating filtered event reports (automatically or on demand) and save in CSV or HTML format (with print to PDF option)
- generating RCP reports based on time and attendance schedules and displaying the attendance list
- defining the company's structure
- sending notifications regarding the employee's time settlement to email
- preview, playback and export of video/audio recordings
- visualization and operation of SATEL alarm systems based on Integra control panels
- Operation of a parking lot with controlled entry

The NOVUS MANAGEMENT SYSTEM AC software also offers a number of features described in detail further that allow to meet the requirements often posed by the system administrator, such as: access after using 2, 3 or 4 cards, the first unlock of the controlled passage using the so-called "first card" with special privileges, multi-read, access after confirmation by operator, interlock and anti-passback (one controller), global zones visualization and T&A report generator. The program will be gradually expanded with new features.

The list of key functions and parameters of the system is presented in the attached table and the structure of the system is shown in the enclosed scheme. Controllers with IP ports communicate with the server service over Ethernet.

1.2 NOVUS MANAGEMENT SYSTEM AC system functions and parameters

General	
Parameter or function name	**Parameter or function value**
PC operating system	Windows 10/11 Pro 64 Bit
Database	Microsoft SQL 2019
Language	English, Polish, Azerbaijani, Magyar
"Online" monitoring	YES
Multi-server (distributed systems)	YES
Client-server structure	YES
Multiple monitors	YES, to 6 monitors
Panels with system elements icons	YES
Defined triggering scenarios	YES
Definiowanie grup elementów	YES
Importing user data from a file	YES
Communication	
Built-in IP ports	via Ethernet
Event reports	Filtered, save in csv, html, pdf format
Native systems	
Access Control (AC)	YES, KaDe, HID®Aero®
Time and attendance (T&A)	YES, KaDe, HID®Aero®, Kantech
License plate recognition (LPR)	YES, NOVUS
Integrated systems	
Access control (integration/visualization)	YES, Kantech
Video Surveillance System (VSS)	YES, NOVUS, ONVIF, RTSP
Intrusion & hold-up alarm systems (I&HAS)	YES, SATEL Integra
I/O Control Modules	YES, Tinycontrol
Fire alarm	YES, POLON 6000

Access Control (AC) by KaDe	
Parameter or function name	**Parameter or function value**
'On-line' monitoring	YES
User photos displaying	YES
Access related functions	
- user identification mode	Card, PIN, card or PIN, card + PIN, fingerprint and combinations with card or PIN
- local anti-passback	YES
- global anti-passback, global interlock	YES
- first opening card	YES
- supervisor mode	YES
- access after using multiple cards (od 2 do 4)	YES
- multiple access (2 - 4)	YES
- latch mode	YES
- schedule based with first opening card or automatic unlocking	YES
Alarm functions	
- threaten code	YES
Users import from file	YES
Controllers	KDH-KS3012-IP, KDH-KS3024-IP, KDH-KS3024-IP-II, KDH-KS3012-IP-II, KDH-KS3000-IP-ELV, KDH-KZ3000-IP-U/M, KDH-KZ3000FP-IP-U/M
KaDe controller's memory capacity	
- card memory	20 000
- event memory	50 000
Communication	
Built in IP port	Via Ethernet
Readers and cards	
- card format	Compatible with 26-40 bit Wiegand format
- card type	Any technology compatible with the reader
Event reports	Filtered, save in CSV, HTML (PDF) format
T&A reports (terminals or KD readers)	Based on a schedule

Access Control (AC) by HID®Aero®	
Parameter or function name	**Parameter or function value**
Monitoring „on-line”	YES
User photos displaying	YES
Functions realted with access	
- user identification mode	Card, PIN, card or PIN, card + PIN, Facility code
- local anti-passback	YES
- global anti-passback, global interlock	YES
- first opening card	YES
- access after confirm by the operator	YES
- access after using multiple cards	YES
- card multi-reading (2-times)	YES
- unlocking according to the schedule after reading a valid card or automatically	YES
- support for location function code (FC)	YES
Users import from file	YES
Controllers	HID®Aero® X1100 (master controller), X100, X200, X300
HID® Aero® controller’s memory capacity	
- card memory	250 000 (master controller)
- event memory	50 000
Communication	
Built in TCP/IP ports	Via Ethernet (to the master controller)
Built in RS-485 ports	For encrypted communication with expansion modules
Readers and cards	
- card format	Multi-format
- card type	any reader compatible technology
- readers	Compatible with WIEGAND or OSDP
Event reports	Filtered, save in CSV, HTML (PDF) format
T&A reports (AC readers)	Based on a schedule

Access Control (AC) by KANTECH	
Parameter or Function Name	**Parameter Value or Function Description**
Commands	Update Lock / Unlock Door Temporarily Unlock Door Return to Schedule Enable / Disable Reader Enable / Disable Relay Temporarily Enable Relay Enable / Disable Supervision Line Monitoring
Events	Alarm Controller Fault Door Locked / Unlocked Door Held Open Door in Normal State Door Forced Open Reader Active / Inactive Access Granted / Denied Supervision Line Monitoring Enabled / Disabled Relay On / Off Communication Lost Communication Restored Disconnected by Operator
User Management	View Users and Cards Configured via EntraPass Add and Remove Users and Cards via NOVUS MANAGEMENT SYSTEM AC

Time and Attendance (T&A)	
Parameter or function name	**Parameter or function value**
Supported devices	
T&A terminal	KDH-TA500CFP-IP-U/M/D, KDH-TA500C-IP-U/M/D
Controllers	KDH-KS3012-IP, KDH-KS3024-IP, KDH-KS3024 -IP-II, KDH-KS3012-IP-II, KDH-KS3000-IP-ELV KDH-KZ3000-IP-U/M, KDH-KZ3000FP-IP-U/M Intelligent HID®Aero® X1100 IP Controller (Master Controller) HID®Aero® X100 RS Expansion Door Controller (Slave) Kantech Integrated System Controllers
Company structure	YES
Video verification of events	YES
Event adjustments	YES
Attendance list	YES
Automatic reports	YES
Single-shift mode	YES
Multi-shift mode	YES (1 to 4 shifts per day)
Working time schedules	YES
Working time calendars	YES
Event reports	Filtered, save in CSV, HTML (PDF) format
T&A reports (terminals or KD readers)	Based on a schedule

Video Surveillance System (VSS)	
Parameter or function name	**Parameter or function value**
Video	TAK
Supported devices	Cameras: IP Novus 4000/6000/8000 series, ONVIF/RTSP, IP recorders: IP Novus 4000/6000 series Multistandard recorders: Novus 4000/6000 series NOVUS MANAGEMENT SYSTEM VSS / NMS IP recorders
Number of supported video/audio channels	No program restrictions
Supported protocols	Novus, ONVIF, RTSP
Supported codecs	H.264, H.264+, H.265, H.265+, MJPEG
Dual stream support	YES
Support for fisheye cameras	YES
Displaying	YES
Multi-monitor support	YES, to 6 monitors
Maximum resolution	6 x 4K UltraHD
Playback of recordings	YES
Forward playback	YES
Speeded up playback	YES, to x10
Slowed playback	YES, to x0.1
Playback backwards	YES
Downloading recordings	YES
Format of downloaded recordings	AVI, MP4
Attaching metadata to video	YES, channel name, device name, watermark, time stamp
Schedule for downloading recordings	YES
Alarms	YES
Alarm inputs/outputs in cameras/recorders	YES, support for alarm inputs/outputs available on cameras
Motion detection	YES, support for motion detection available in cameras/recorders
Image analysis	YES, support for image analysis features available in cameras/recorders
License plate number recognition (LPR).	YES, compatible with Novus cameras NVIP-2H-6732M/LPR and NVIP-4H-6732M/LPR
PTZ control	YES
PTZ function	pan, tilt, zoom, presets, routes, patrols, scans, focus, iris
Other	YES
Possibility to connect surveillance television	YES

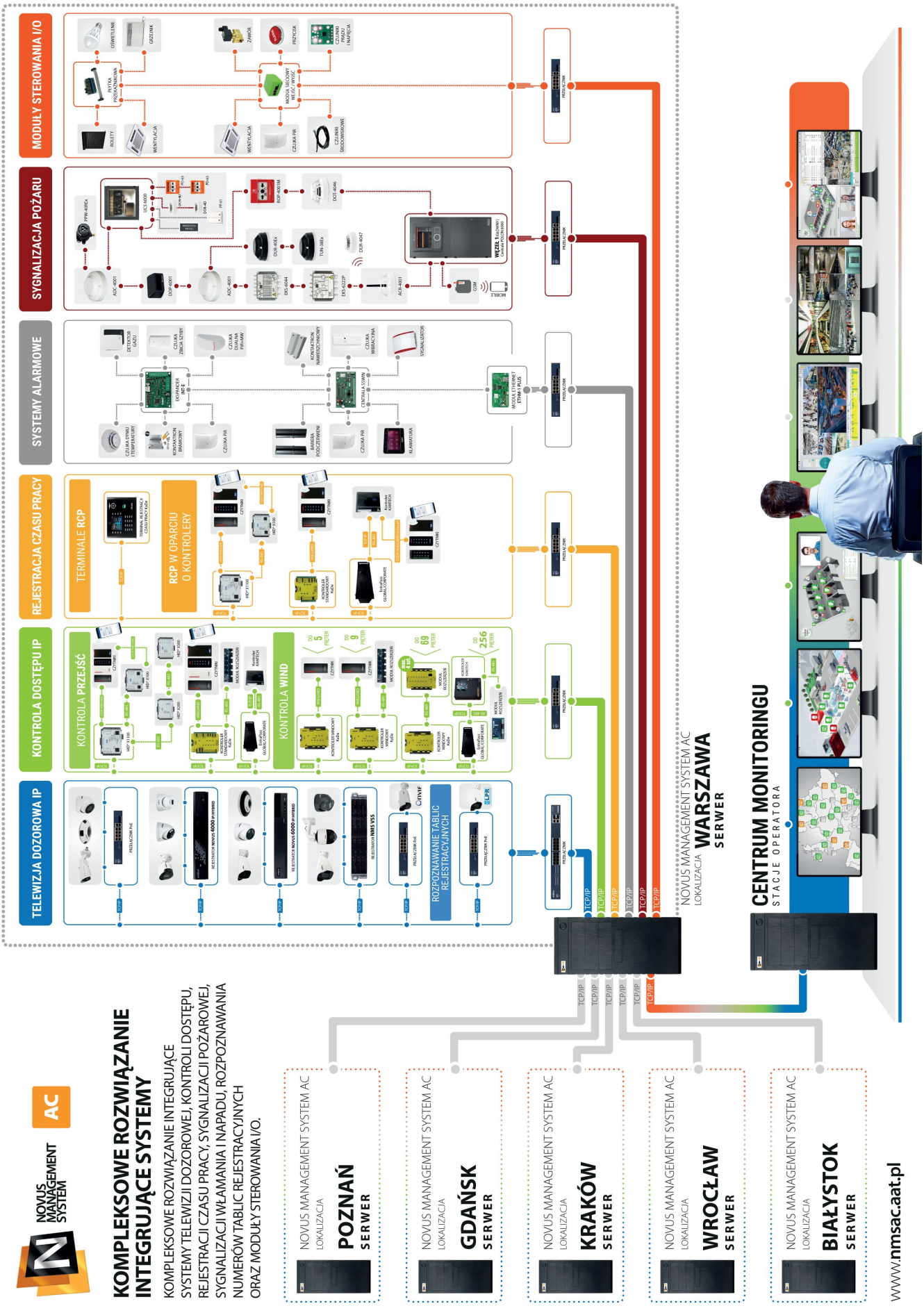
License plate recognition (LPR)	
Parameter or function name	**Parameter or function value**
Supported devices	IP cameras Novus NVIP-2H-6732M/LPR / NVIP -4H-6732M/LPR connected directly or via an NOVUS MANAGEMENT SYSTEM VSS IP recorder
Number of cameras supported	No program limitations
Support for QR code printers	YES
Parking zones	YES
Access levels	YES
Operation schedules	YES
Visualization of the number of vehicles in zones	YES
Database of license plate numbers	YES
Import/export of license plate numbers license plate numbers	YES
Search for events related to related to recognition	YES
Defining the reactions associated related to the recognition of	YES
Limit of vehicles in the parking zone	YES
Cooperation with barriers, gates, etc.	YES
Operation of entry buttons	YES
Alarms	YES
Alarm inputs/outputs in cameras/recorders	YES, support for alarm inputs/outputs available

Intrusion & hold-up alarm systems (I&HAS)	
Parameter or function name	**Parameter or function value**
Supported devices	Alarm control panels Satel: Integra 24, Integra 32, Integra 64, Integra 64 Plus, Integra 128, Integra 128 Plus, Integra 128-WRL, Integra 256 Plus
Executive functions	Arm disarm partition, arm disarm all partitions, arm/disarm zone, arm/disarm all zones, lock detector, unlock detector, clear partition alarm, clear zone alarm, clear all zones, clear alarm memory history, output on/off, view current panel users, enter first password to arm, enter first password to disarm, update structure from current configuration, cancel first password, set timer **User management** **(add, delete, modify):** - username - password - user type - zone access - permissions
Actions (incoming events)	**Alarms:** Burglary, Tamper, Perimeter Entry Alarm input/Outpur, Gas Alarm Guard presense, Duress Alarm ,Pressure Alarm, Security Loop Violation, Pump Alarm Temperature Alarm, Valve Sensor Alarm Water leak Alarm, Water level Alarm **Fire Alarm:** Button, Flames detector, Smoke detector Temperature sensor, Water Flow **Information about faults**, Battery fault Arm/Disarm, Tamper, Masking (Only Integra Plus panels), Sensor Bypass, Output ON/OFF, Partitions Bypass, Connections Faults, Connected/Disconnected, Enter first code, Enter first code failed, Cancel first code failed, 3 wrong access codes, First code expired

Fire alarm systems	
Parameter or function name	**Parameter or function value**
Supported devices	POLON 6000 system (firmware version 1.016 or higher)
Actions (incoming events)	Alarm confirmation, Loss of communication, Fire alarm confirmed, First stage fire alarm, Second stage fire alarm, Pre-alarm, Test fire alarm, End of fire alarm, End of test fire alarm, Fault, No faults, End of fault, The module is not responding The module does not respond on channel a, The module does not respond on channel b, Incorrect state in channel a, Incorrect state on channel b, Testing, End of testing, Blocking, End of blocking, Missing or damaged 230V power supply Low battery voltage No battery Earthing fault in the control panel Internal battery resistance exceeded Defective charging rail Faulty control rail 24V voltage fault No 27V power supply 27V Voltage too low 27V Voltage too high Load current exceeded CPU restart Signal line Is - break, short circuit Temperature probe missing or error PK2 output - no continuity Battery cabinet raised the temperature Control output turned on, Control output disabled, Control output - no continuity of the control line Control output - short circuit Control output - line break Control output - relay damage Control output - the module containing the output does not respond Addressable detection line - loop short circuit Addressable detection line - line short circuit Addressable detection line - line break Addressable detection line - the order of elements on the line is changed Addressable detection line - elements do not respond Addressable detection line - undeclared elements Addressable detection line - incorrect r/c parameters Addressable detection line - too many elements in the line Addressable detection line - the module containing the line does not respond The line element is not responding Line element - eeprom memory damage Line element - short circuit isolator included Line element - hardware fault

I/O Control Modules	
Supported devices	Network Input/Output Module LANKON-008 by Tinycontrol
Event Reception	YES
Environmental parameter measurement	YES
Current and voltage measurement	YES
Output Control	YES

1.3 System block diagram



Section 2. Software installation and running

In this chapter, issues related to the installation, first start-up and elements of the NOVUS MANAGEMENT SYSTEM AC program window will be discussed.

2.1 PC minimal requirements

Selection of appropriate computers for the server and client stations should be strictly dependent on the amount of equipment installed for integrated systems. This is especially true for VSS systems with a large number of cameras. In the case of VSS systems, the selection of computers should also take into account how many cameras will be displayed simultaneously with video streams. The number of connected cameras is of less importance in this case.

Monitor resolution should be set to Full HD (1920x 1200) or higher. Setting a lower resolution may result in some descriptions not being displayed.

The best solution is to buy a computer from our offer with installed software and licenses. The units are designed for continuous operation.

ATTENTION!

Controllers with NOVUS MANAGEMENT SYSTEM AC should work in separate physical network (switch, network card) or separate VLAN. This will help to avoid interference between access control system and other devices operate in network. If the program supports only access control system and television surveillance, we are recommend to use separate network cards to communicate with access control system and television surveillance devices.

The following are approximate parameters of computer units designed for NOVUS MANAGEMENT SYSTEM AC software.

Minimum configuration of a PC working as a server

1. CPU **Intel i3** 10-generation or newer (other CPUs are possible, but bear in mind that they have not been tested with the software).
2. RAM DDR4 or newer **16 GB** operating memory.
3. Operation system **Windows 10 IoT 64 bit.**
4. Network card **1 Gb/s** (Recommended additional network card 1Gbps, access control system should work in a separate network)
5. Sound card
6. System disk - **SSD 128 GB** or more.
7. Graphics card - **GeForce GTX 1050** or later (it is possible to use other graphics chips that support a resolution of min. 1920x1080, but keep in mind that they have not been tested with the software).

Recommended configuration of a PC working as a server

1. CPU **Intel i7** 11-generation or later / Intel Xeon Silver third generation or later (it is possible to use other CPUs, but keep in mind that they have not been tested with the software).
2. RAM DDR4 or newer **16GB ECC** operating memory.
3. Operation system **Windows 10 IoT 64 bit.**
4. Network card **1 Gb/s, 3 pieces** (the access control system should operate on a separate network).
5. Sound card.
6. System disk **SSD 256 GB** or more.
7. Graphics card - **GeForce GTX 1050** or later (it is possible to use other graphics chips that support a resolution of **min. 1920x1080**, but keep in mind that they have not been tested with the software).

Minimum configuration of a PC working as a client

1. CPU **Intel i3** 10-generation or newer (other CPUs are possible, but bear in mind that they have not been tested with the software).
2. RAM DDR4 or newer **8 GB** operating memory
3. Operation system **Windows 10 Pro 64 bit, Windows 11 Pro 64 bit, Windows 10 IoT 64 bit**.
4. Network card **1 Gb/s**.
5. Sound card.
6. System disk - **SSD 64 GB** or more.
7. Graphics card - **GeForce GTX 1050** or later (it is possible to use other graphics chips that support a resolution of **min. 1920x1080**, but keep in mind that they have not been tested with the software).

Recommended configuration of a PC working as a client

1. CPU **Intel i7** 11-generation or later / Intel Xeon Silver third generation or later (it is possible to use other CPUs, but keep in mind that they have not been tested with the software).
2. Pamięć operacyjna RAM DDR4 lub nowsza **16 GB**.
3. Operation system **Windows 10 Pro 64 bit, Windows 11 Pro 64 bit, Windows 10 IoT 64 bit**.
4. Network card **1 Gb/s**.
5. Sound card.
6. System disk - **SSD 128 GB** or more.
7. Graphics card - **GeForce GTX 1050** or later (it is possible to use other graphics chips that support a resolution of **min. 1920x1080**, but keep in mind that they have not been tested with the software).

Section 2. Software installation and running

2.2 Licenses

The use of NOVUS MANAGEMENT SYSTEM ADVANCED CONTROL requires registration and the purchase of appropriate licenses. The method of licensing in version 6 has been created so that it allows you to accurately match the number of licenses needed to the characteristics of each object. Also, additional licenses can be purchased to the system at any time to expand it or increase its functionality. The number of devices that can be connected to the **NOVUS MANAGEMENT SYSTEM AC** server is the responsibility of the **NOVUS MANAGEMENT SYSTEM AC PKT LIC v5** license for license points. They are sold per 1 point or in packs of 10 points. Each device added to the server consumes a specific number of license points. You must purchase a license for the number of license points to connect all the intended devices to the server.

As a standard, one operator station can connect to NOVUS MANAGEMENT SYSTEM AC server version 6.

To increase the number of workstations, purchase the appropriate number of licenses **NOVUS MANAGEMENT SYSTEM AC KL1 v5**

Incorporating time and attendance functionality is done using **NOVUS MANAGEMENT SYSTEM AC RCP v5** license, this license also supports 10 users. In order to increase the number of users of the Time & Attendance function, it is necessary to purchase the appropriate number of **NOVUS MANAGEMENT SYSTEM AC URCP v5** or **NOVUS MANAGEMENT SYSTEM AC URCP 100 v5** or **NOVUS MANAGEMENT SYSTEM AC URCP 500 v5** or **NOVUS MANAGEMENT SYSTEM AC URCP 2000 v5** licenses.

Enabling the license plate recognition functionality is done using **NOVUS MANAGEMENT SYSTEM AC LPR v5** license, this license also allows the support of 10 vehicles. To increase the number of vehicles supported by the license plate recognition function, purchase the appropriate number of **NOVUS MANAGEMENT SYSTEM AC ULPR v5 licenses or NOVUS MANAGEMENT SYSTEM AC ULPR 100 v5** or **NOVUS MANAGEMENT SYSTEM AC ULPR 500 v5** or **NOVUS MANAGEMENT SYSTEM AC ULPR 5000 v5** or extension **NOVUS MANAGEMENT SYSTEM AC ULPR OP v6** that disables the limitation of the number of vehicles.

For systems operating in distributed mode, purchase a **NOVUS MANAGEMENT SYSTEM AC SRV v5** license to enable muliservers. It allows you to operate multiple locations from a single interface of **NOVUS MANAGEMENT SYSTEM AC**. The license must be purchased for each server that is part of a multiserver (distributed) system.

There are also available extensions **NOVUS MANAGEMENT SYSTEM AC NMS VSS OP**, which causes the system do not charge license points for added NOVUS MANAGEMENT SYSTEM VSS devices and **NOVUS MANAGEMENT SYSTEM AC KaDe OP v6**, which causes the system do not charge license points for added KaDe access control devices.

License activation needs previous registration of **NOVUS MANAGEMENT SYSTEM AC** program.

Registration is done from the program itself. It is required that the computer from which we perform registration has access to the Internet (on-line registration). In case of lack of access to the Internet on the computer unit for which we want to perform registration, it is possible to perform off-line registration consisting in generating a special file, transferring it to a computer with access to the Internet, registering it on a dedicated website, and then using the resulting file on the computer unit for which we want to perform registration.

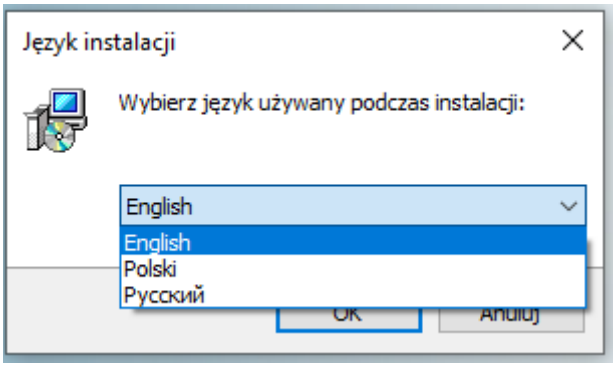
A trial license for the program (**TRIAL**) is also available, its duration is 60 days. It includes full functionality and a limit of 500,000 license points, 500,000 RCP users, 500,000 LPR vehicles and 100 operator stations. For detailed information, please contact the sales department of AAT SYSTEMY BEZPIECZEŃSTWA sp. z o.o.

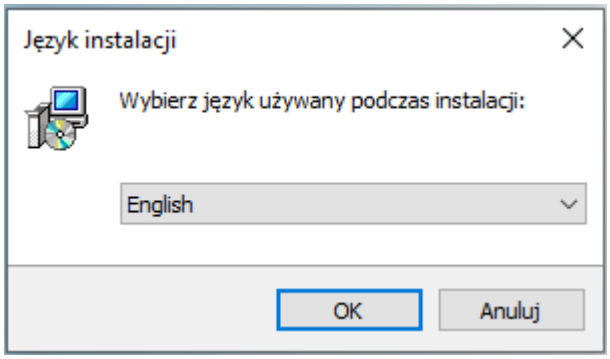
2.3 Software installation

To run the installation process, click on the **NOVUS MANAGEMENT SYSTEM AC_full_X.XX.XXX.exe** file or the Run command from the context menu. In order to obtain the installation version of Novus Management System AC software version 6, please contact the sales department of AAT SYSTEMY BEZPIECZEŃSTWA sp. z o.o. or purchase a dedicated USB media (price list item: NOVUS MANAGEMENT SYSTEM AC USB).

Additional licenses to increase the capacity of the system are available in the price list and can be purchased from the sales departments and added to the system according to the procedure described later in this manual (System tab).

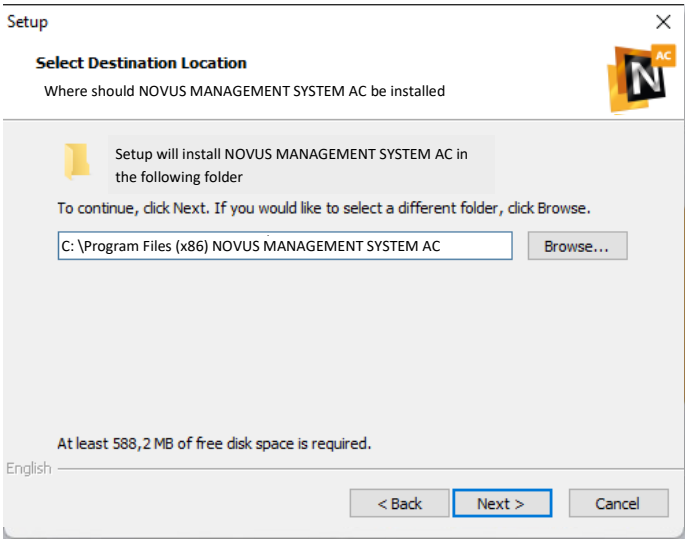
After running the **NOVUS MANAGEMENT SYSTEM AC installer**, the window shown below will appear on the screen. Select the language of the installer from the drop-down list and confirm with **OK**.

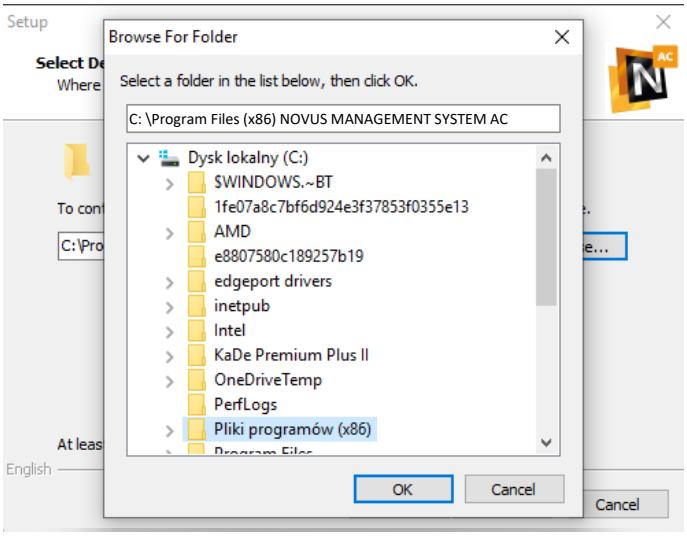




User License will be displayed, which need confirmation after reading to pass to the next installation step. After checking ***I accept the agreement*** checkbox click ***Next***.

In the following windows, select the installation path of the program. You can edit the default path in the text box or select from the directory tree when you click ***Browse…*** and confirm with ***OK***. After selecting NOVUS MANAGEMENT SYSTEM AC installation path, click the ***Next*** to proceed to the next installation step.

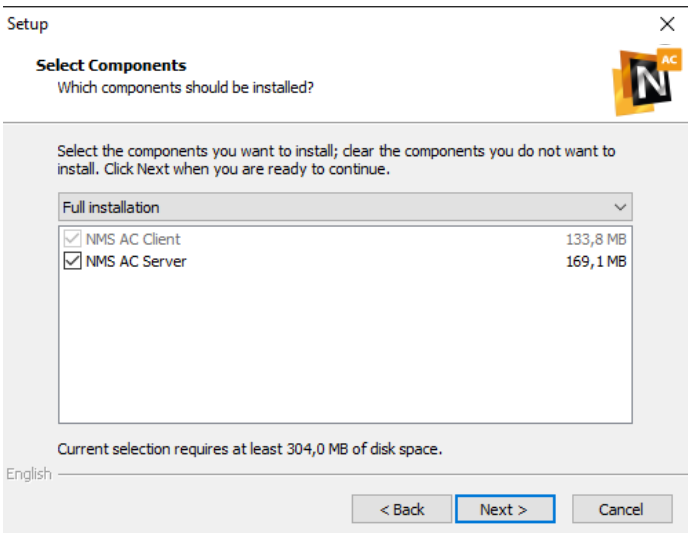


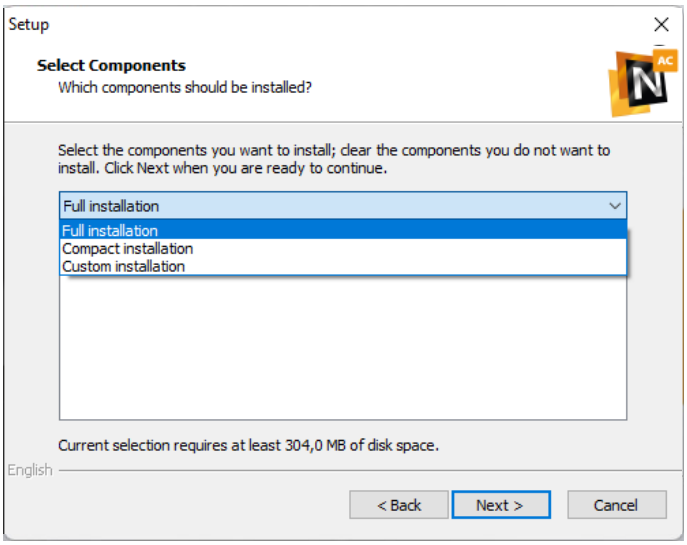


At this stage of the software installation, select its range. There are three options available in the drop-down list:

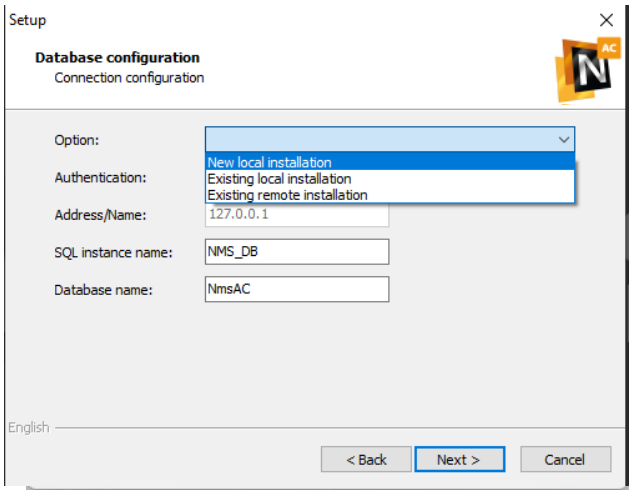
- ***Full installation*** - installs both NOVUS MANAGEMENT SYSTEM AC server and the client application
- ***Basic installation*** - installs only the client application which must be connected to the NOVUS MANAGEMENT SYSTEM AC server on another computer
- ***User installation*** - installs the components selected by the user by checking the appropriate check-boxes

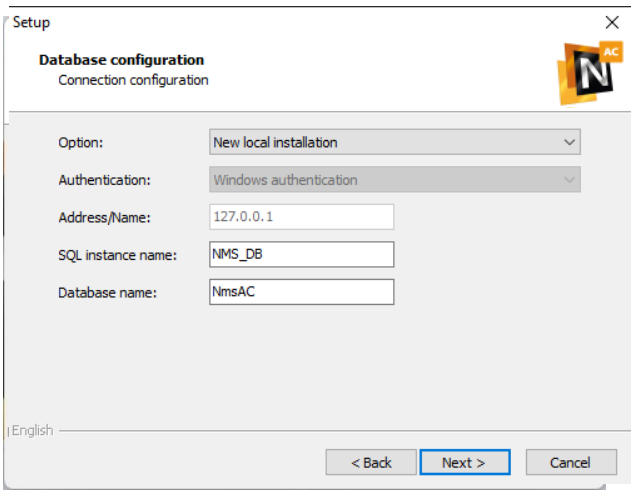
After selecting the installation range, click ***Next***.

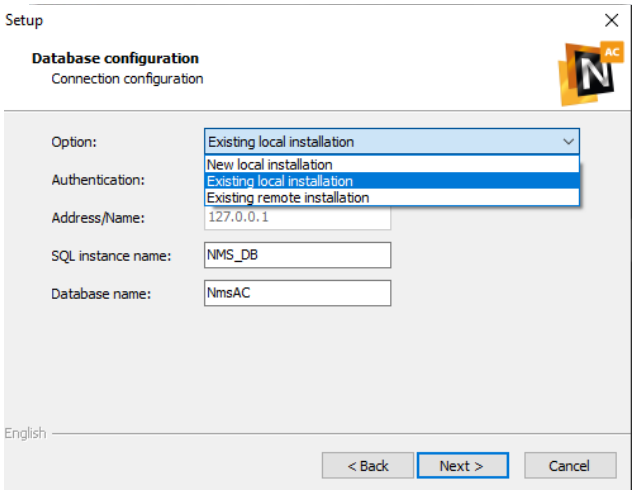


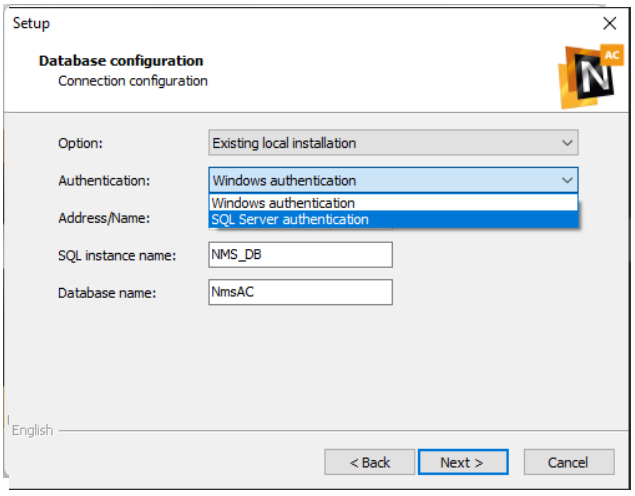


At the database configuration stage, select one of three options from the drop-down list below.





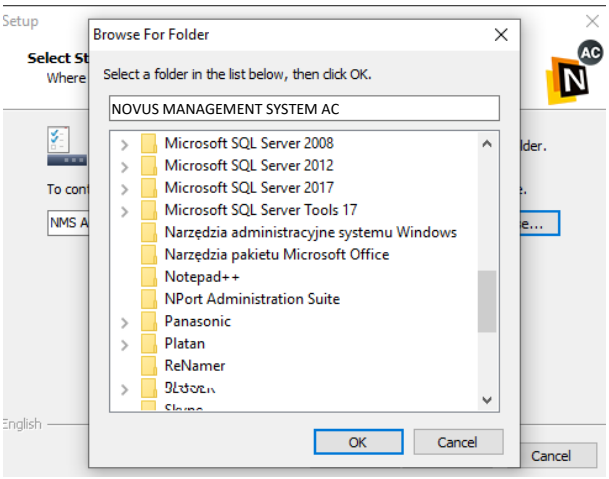




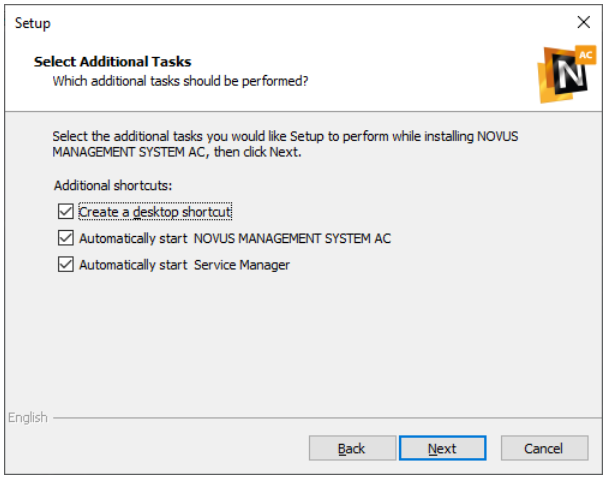
The new local installation - installs the SQL Server on the computer, creates a new SQL instance and database with the names specified in the text boxes.

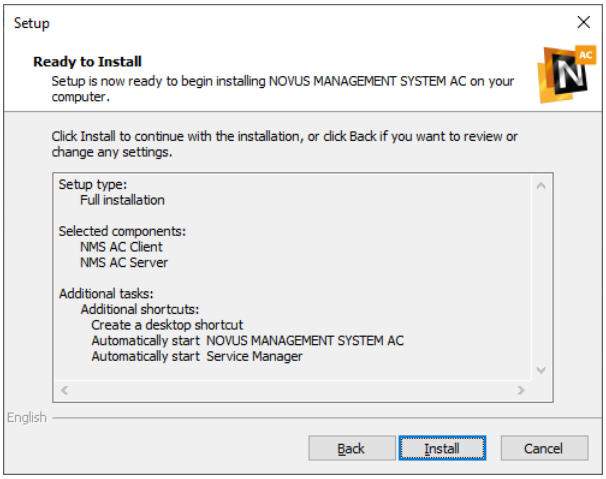
Existing local installation - this option can be selected if SQL Server is already installed on the computer; creates a new SQL instance and database with the names specified in the text boxes; if you choose to authenticate through SQL server, you must provide the login information used to confirm access to the SQL server.

Existing remote installation - allows you to connect NOVUS MANAGEMENT SYSTEM AC server to the SQL Server installed on another computer on the network; creates a new SQL instance and database with the name specified in the text boxes on the SQL Server with specified in *Address/name* field IP address; for the applicable SQL Server authentication you must provide the login information used to confirm access to the remote SQL Server



After you have configured the database, click ***OK*** to move to the next step where you should decide on the name of the shortcut folder on the Start menu, and when you click ***Next***, decide to create NOVUS MANAGEMENT SYSTEM AC application shortcut and automatic startup when the system is started by selecting or clearing the appropriate check boxes.

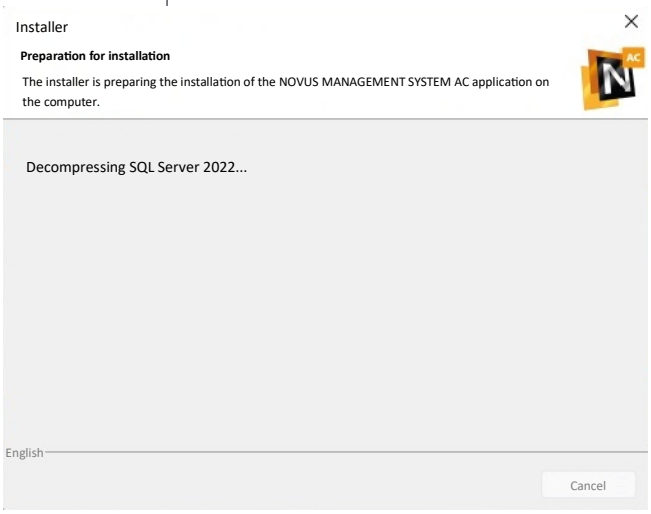


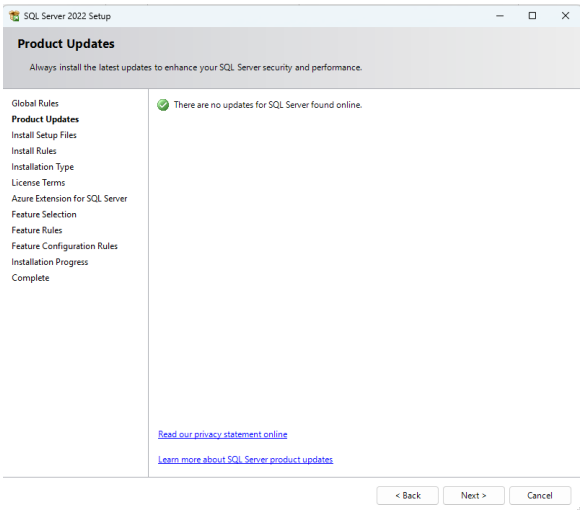


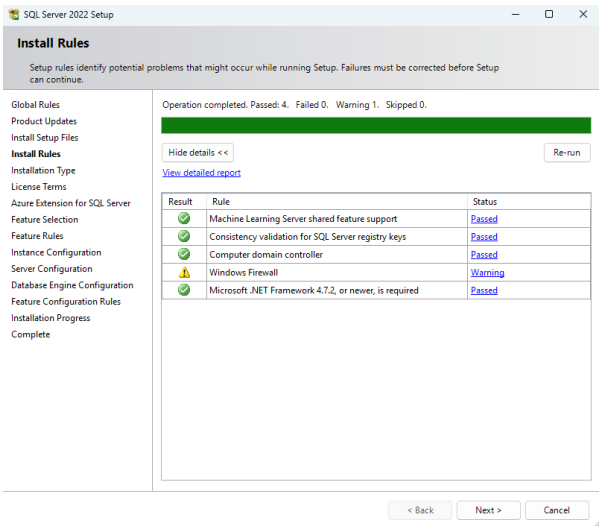
After pressing ***Next*** button, you will see the installation summary window with previously selected settings. Until this step you can go back to the previous steps of configuring the installation using ***Back*** button. If the summary settings are correct, click ***Install***.

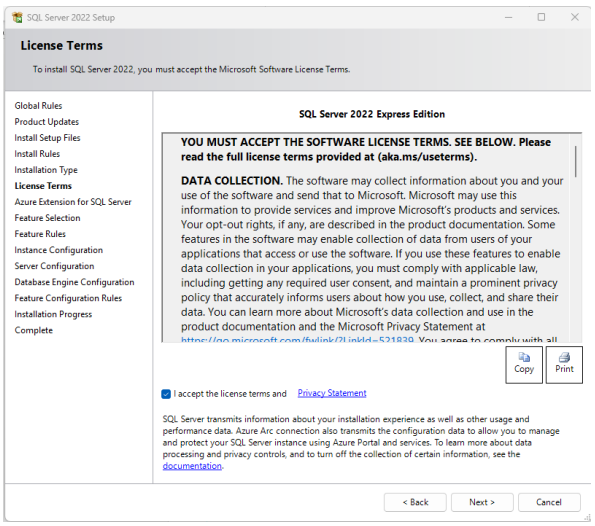
At this point, after selecting the location and names, the proper software installation process begins.

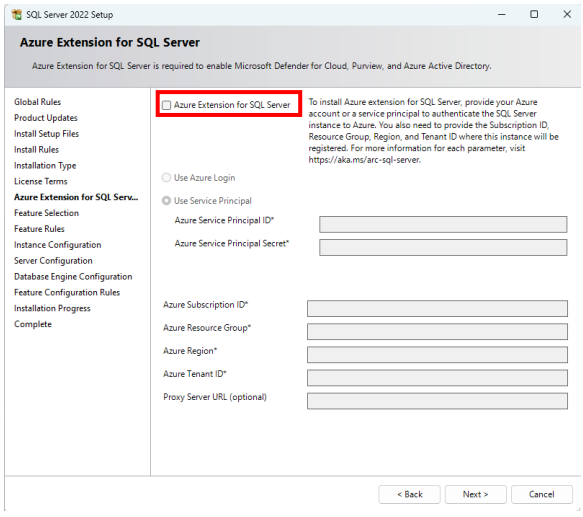
At the beginning, the SQL database will be installed according to the option you chose, and then the **NOVUS MANAGEMENT SYSTEM AC** application. If your computer is not connected to the Internet, you may be prompted to check for available updates during the installation of the SQL database, and then you must ignore it and click *Next.*

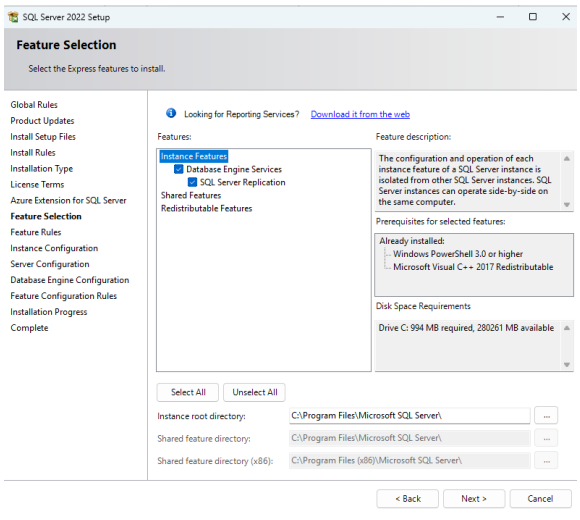




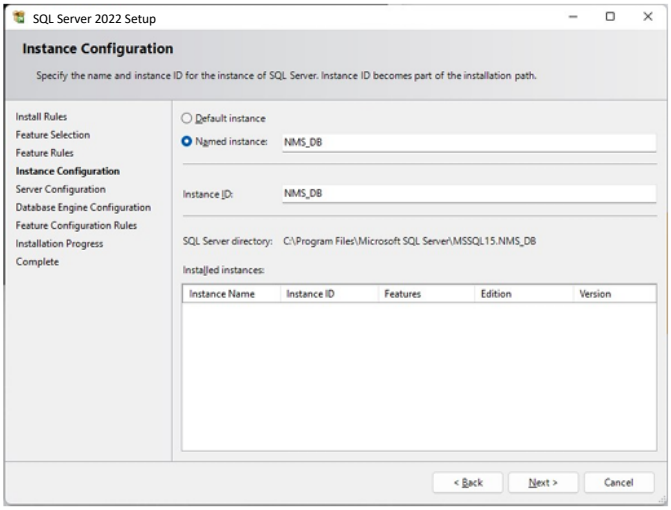


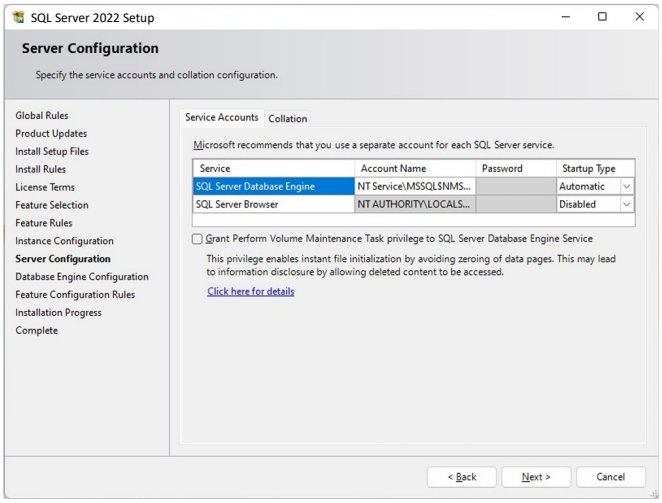


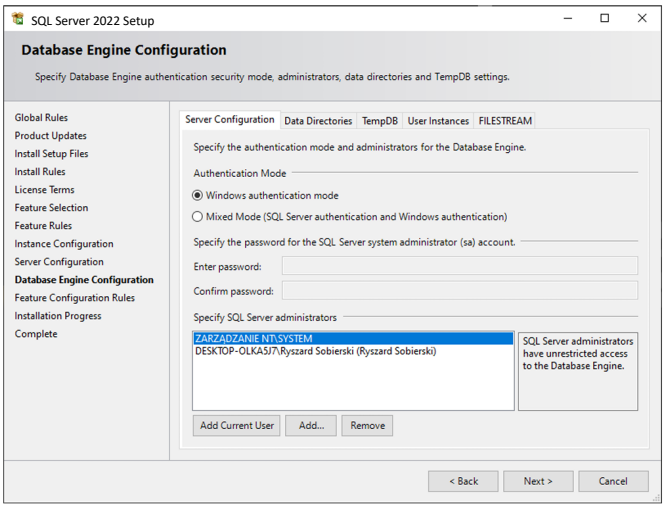


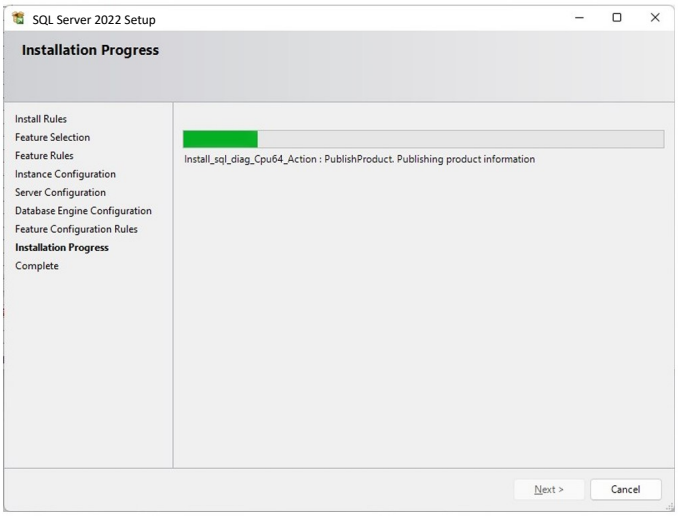


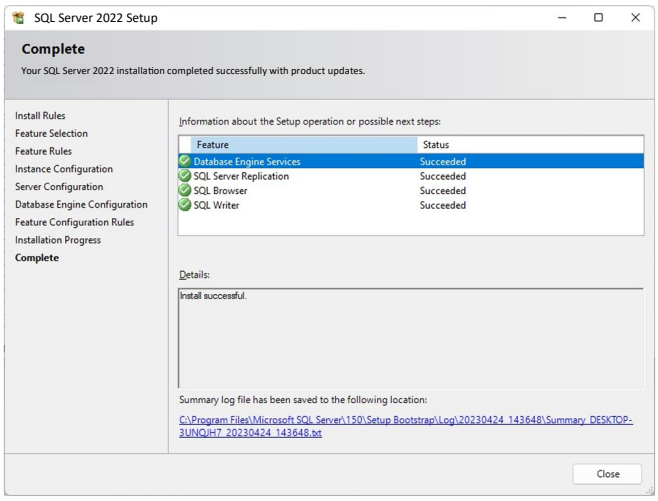
At this stage, in the next windows, click Next button and in the License Terms window, check the box for acceptance of the license (I accept the license terms and Privacy Statement).







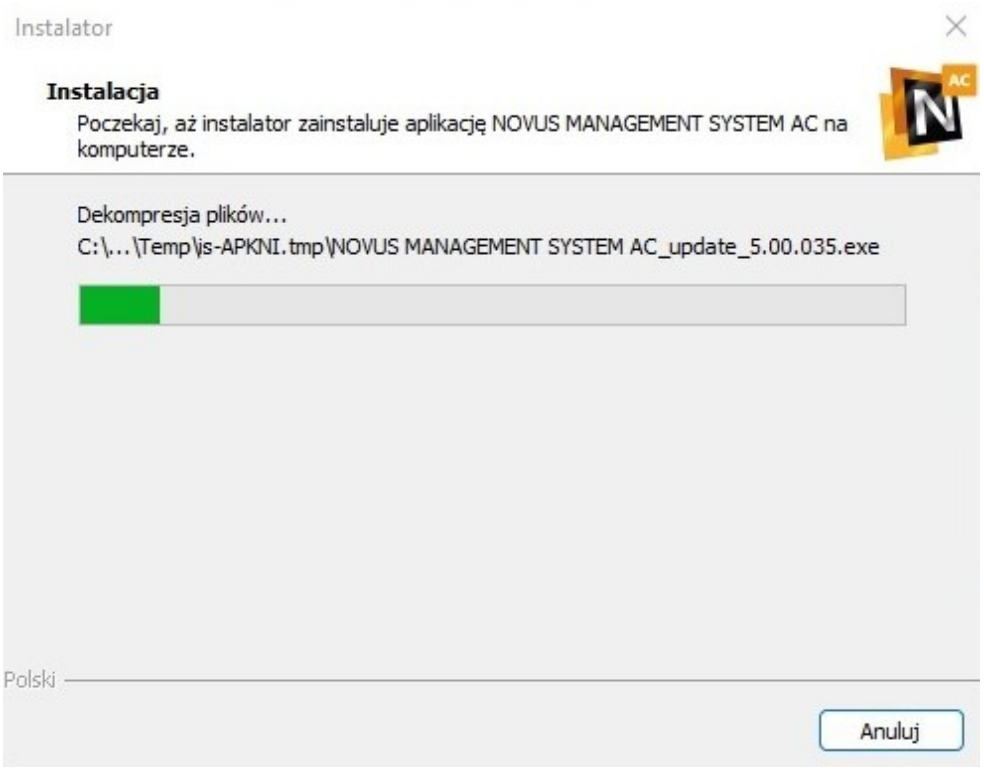




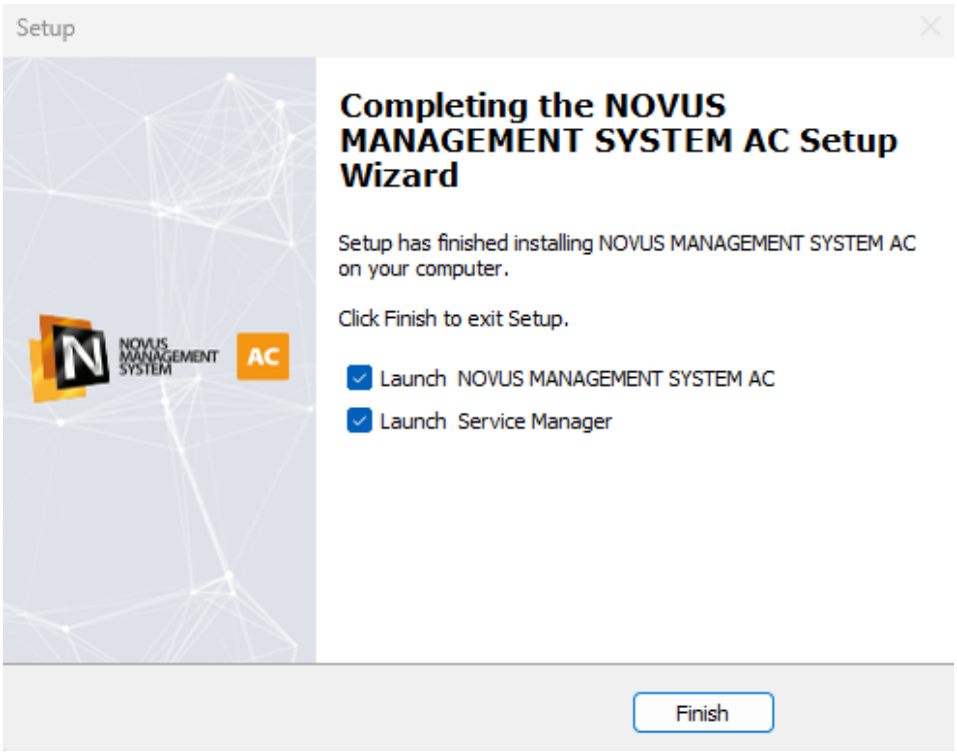
In the next steps of the installation, steps are performed according to the list on the right side of the window.

When the SQL database installation is successfully completed, the *Complete* window will show that this part of the installation has been successfully completed. Then click *Close.*

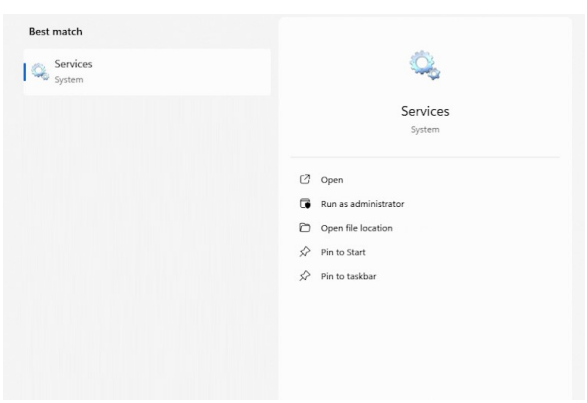
The installer will go through the process of installing the required components of NOVUS MANAGEMENT SYSTEM AC, which takes a few moments.

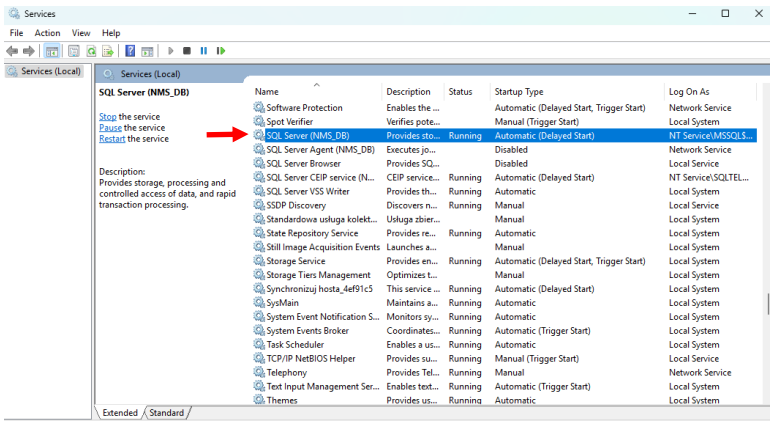


After installing the application, the information window shown below appears. You can start NOVUS MANAGEMENT SYSTEM AC immediately by clicking the ***Close*** button with the Run **NOVUS MANAGEMENT SYSTEM AC** application checkbox checked at the same time. Unchecking this box and clicking the button will result in exiting the installer without running the application. Checking the **Run Service Manager** box will result in an icon appearing in the "Tray" window in the lower right corner of the screen to stop or start the NOVUS MANAGEMENT SYSTEM AC Service.

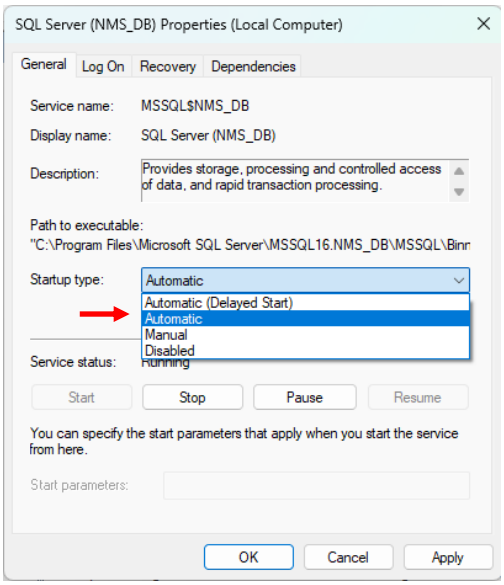


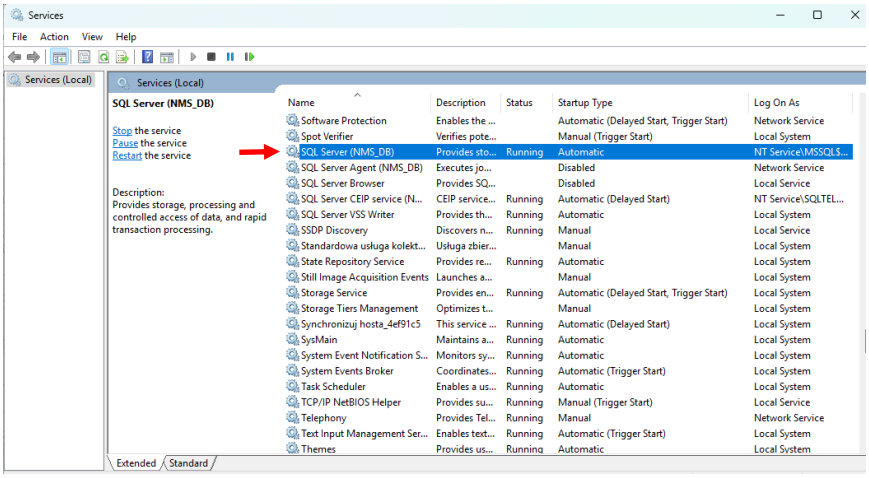
WARNING!
After installing the program server, you need to change the startup type of the SQL Server. To do this, search for “Services” in the search bar on the Windows 10/11 taskbar.





Find the service SQL Server (NMS_DB) and change the startup type from Automatic (Delayed Start) to Automatic, then confirm by clicking “OK.”





2.4 Program update

WARNING!

Direct upgrade of **MANAGEMENT SYSTEM AC** from version 4 to version 5/6 is not possible. Performing such an upgrade may damage the database.

To upgrade version 4 to version 5/6, perform an intermediate upgrade to version 4 to version 4.03.01 using the NMS AC_update_4.03.01.exe file. For more information on the subject, contact the sales department or technical support department of KD or VSS AAT SECURITY SYSTEMS Ltd.

Upgrading from version 6 to the newer version 6 can be done directly, without intermediate upgrades.

Upgrade files for higher versions of the program are named:

NOVUS MANAGEMENT SYSTEM AC_update_X.XX.XXX.exe.

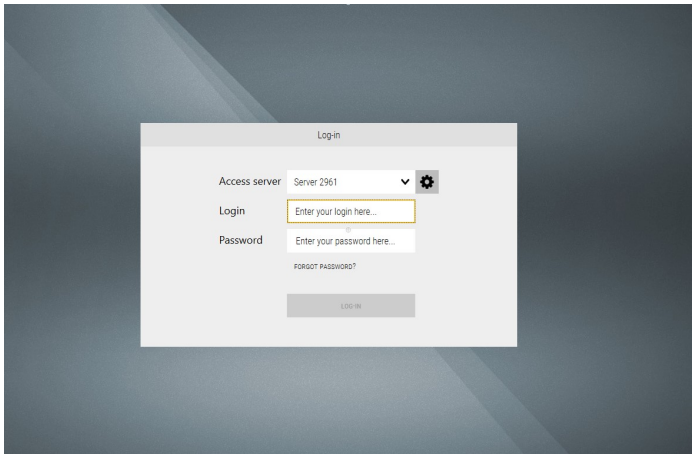
To perform the upgrade, follow the same steps as described in the section on program installation.

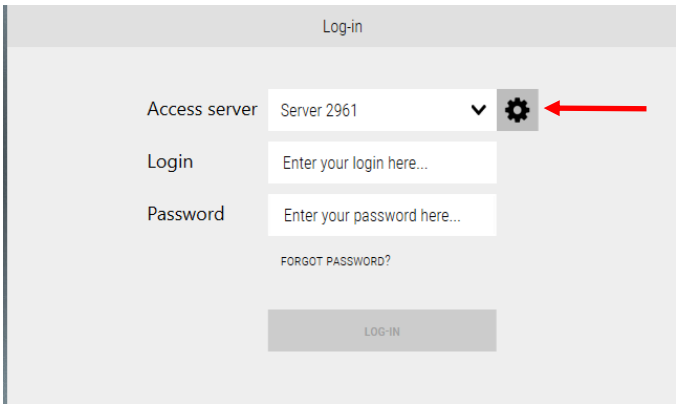
Before updating from version 6.00.004 to version 6.01.039 or later, an intermediate update to version 6.00.012 must be performed.

2.5 Running the program

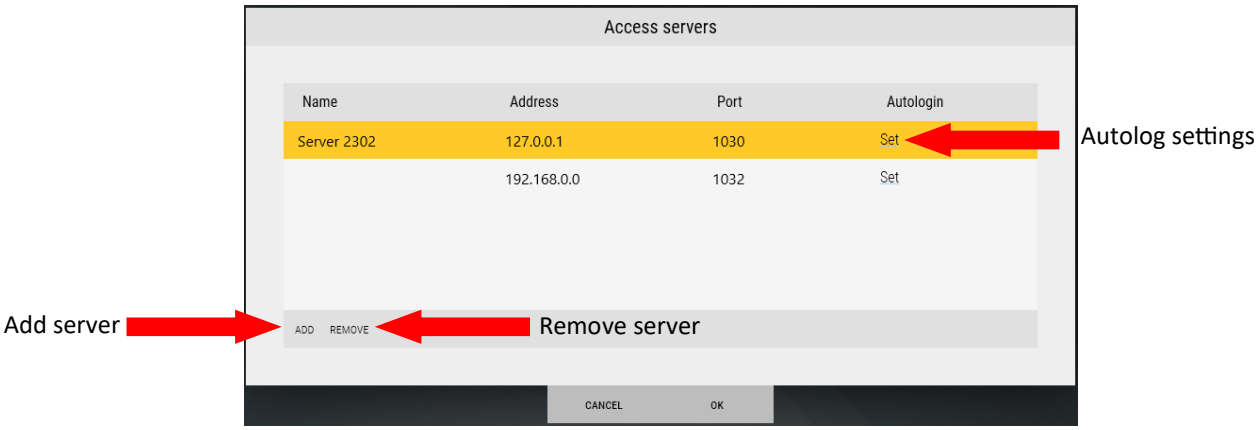
After installing **NOVUS MANAGEMENT SYSTEM AC** software, the icon shown below will appear on the desktop by default, and the **NOVUS MANAGEMENT SYSTEM AC** group will be created in the Windows start menu. You can use them to launch the program.

Launching the program results in the appearance of the login screen. In its central part is the login window. In the Server section, you can select the NOVUS MANAGEMENT SYSTEM AC server to connect to. The installed NOVUS MANAGEMENT SYSTEM AC Client application allows you to connect to one arbitrary server. The server application works as a service and is started by default with the start of Windows. Thanks to this, you can connect to it and log in from any client station within the network. The server service connects to the system's SQL database. The icon next to the checkbox highlighted in the figure below opens the **Server List.** Enter the operator's login information in the **Login and Password** fields. The login of the default operator is root, while the password is **pass.** In order to prevent unauthorized access to the system, it is recommended to change this password during setup. This action will be described later in the manual. The **Exit** button in the lower right corner closes the program.

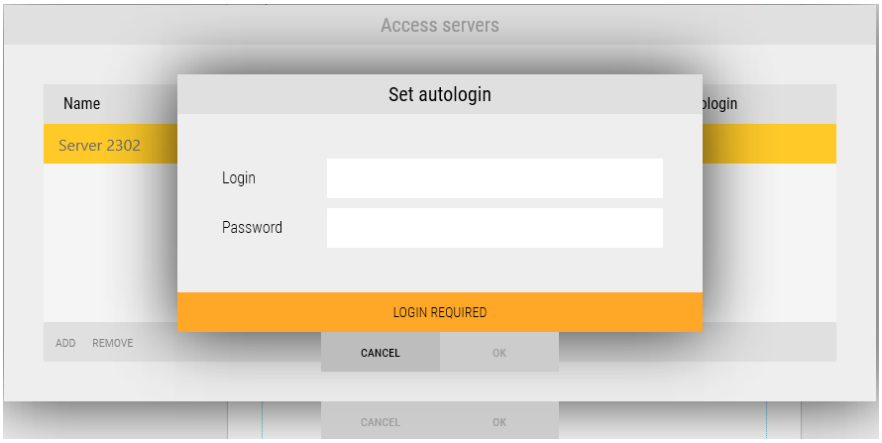




The access server list window allows you to add, delete and configure **NOVUS MANAGEMENT SYSTEM AC** servers to which the operator station can be connected. When adding a server, enter its IP address and port number (default is 1030). The server name will be downloaded automatically after the connection is established. For added servers, it is also possible to enable the autologing function.

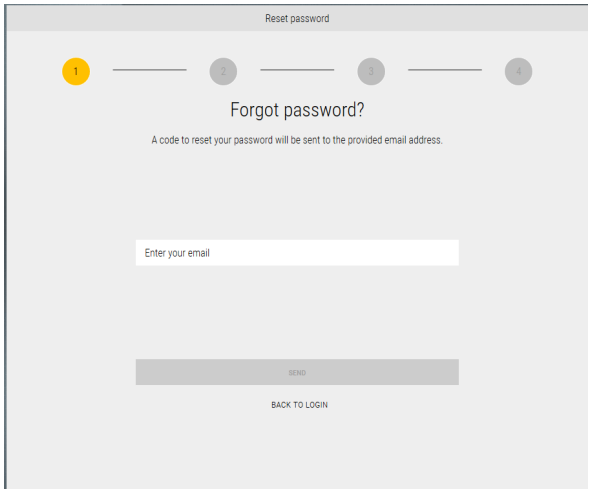


After clicking the **Set/Autologin button,** it is possible to set the name of the operator and the password for the automatic login of the operator added to the system immediately after starting the program.

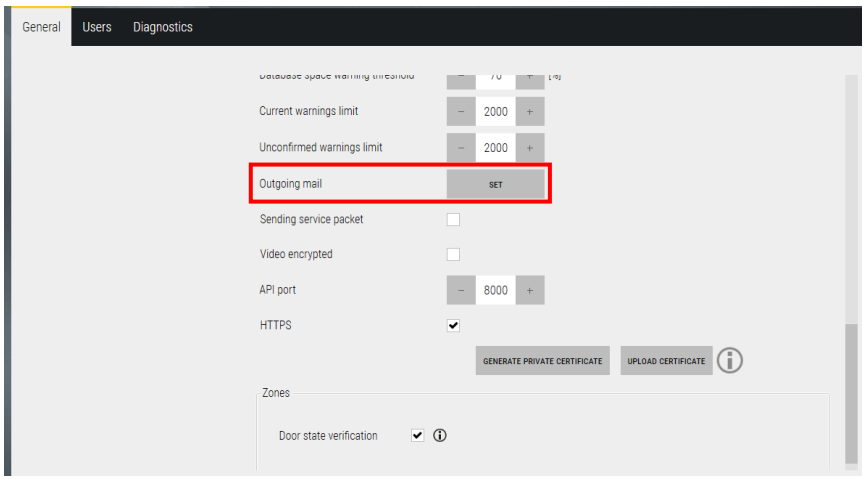


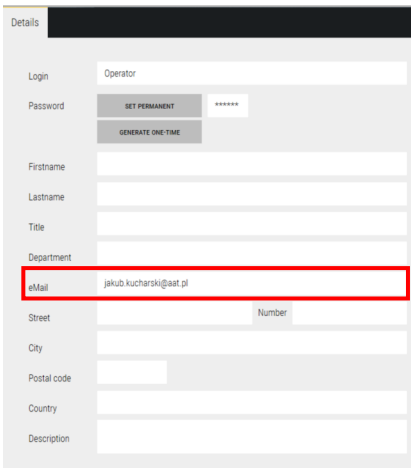
Please note that the autolog function is only available to operators assigned to groups with the "Autolog available" permission.

After clicking the FORGOT PASSWORD? button, it is possible to recover the Operator password for the system (works after prior configuration)."

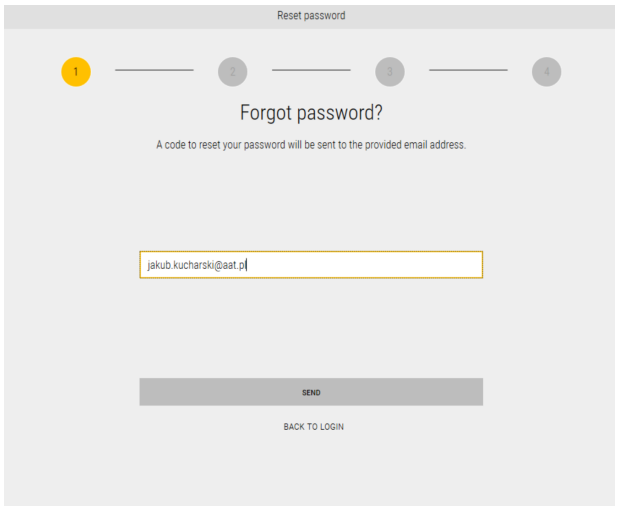


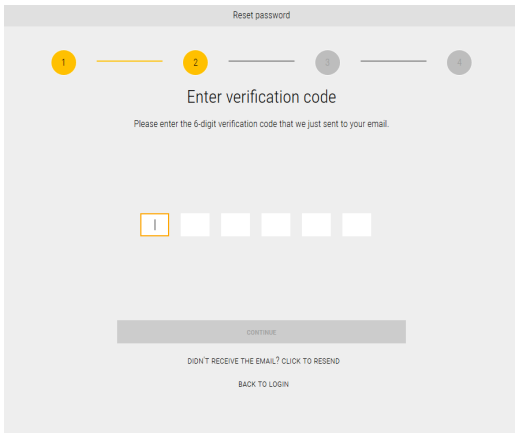
WARNING! This function works only after configuring the outgoing mail server in the **System > Server Settings** tab and setting the operator's email address in the **System > Groups and Operators** tab.

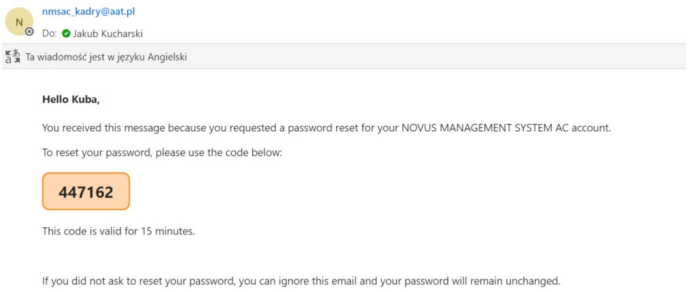


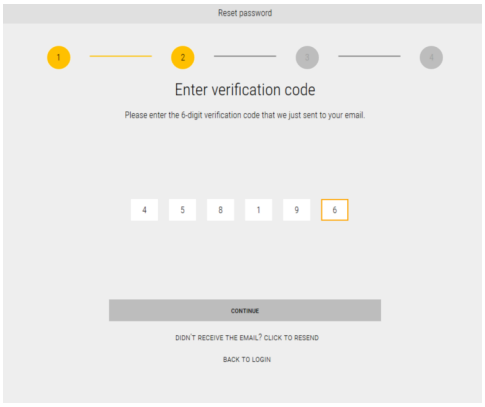


The operator recovers the password by entering their assigned email address, to which a six-digit code will be sent. The email is sent automatically after proceeding to the code entry window.

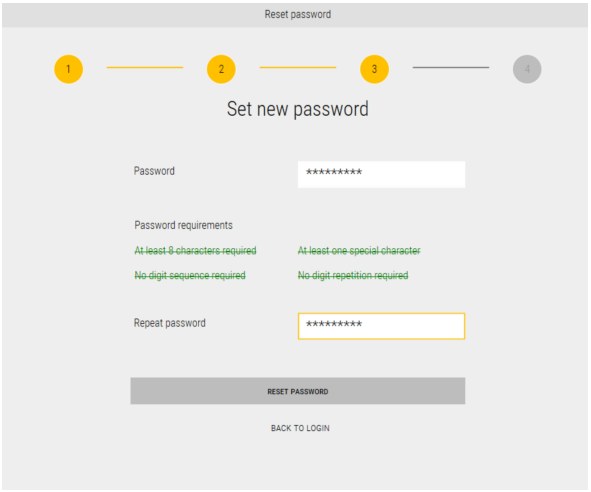


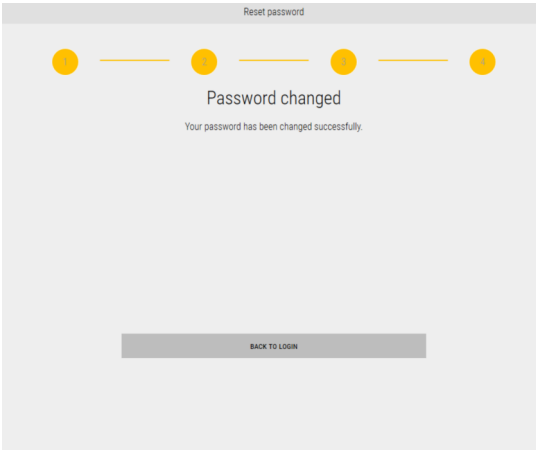






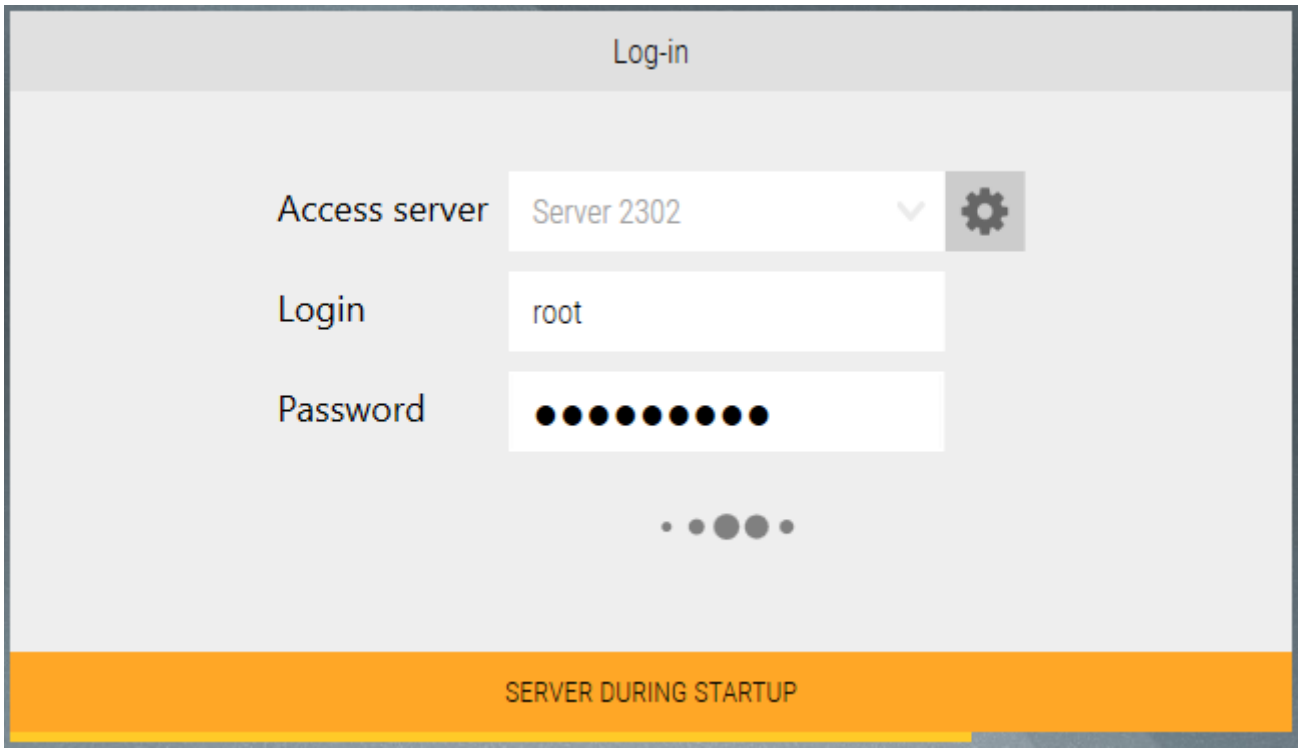
After correctly entering the six-digit code, the operator can change their password according to the specified requirements.
Once confirmed, the password is updated.



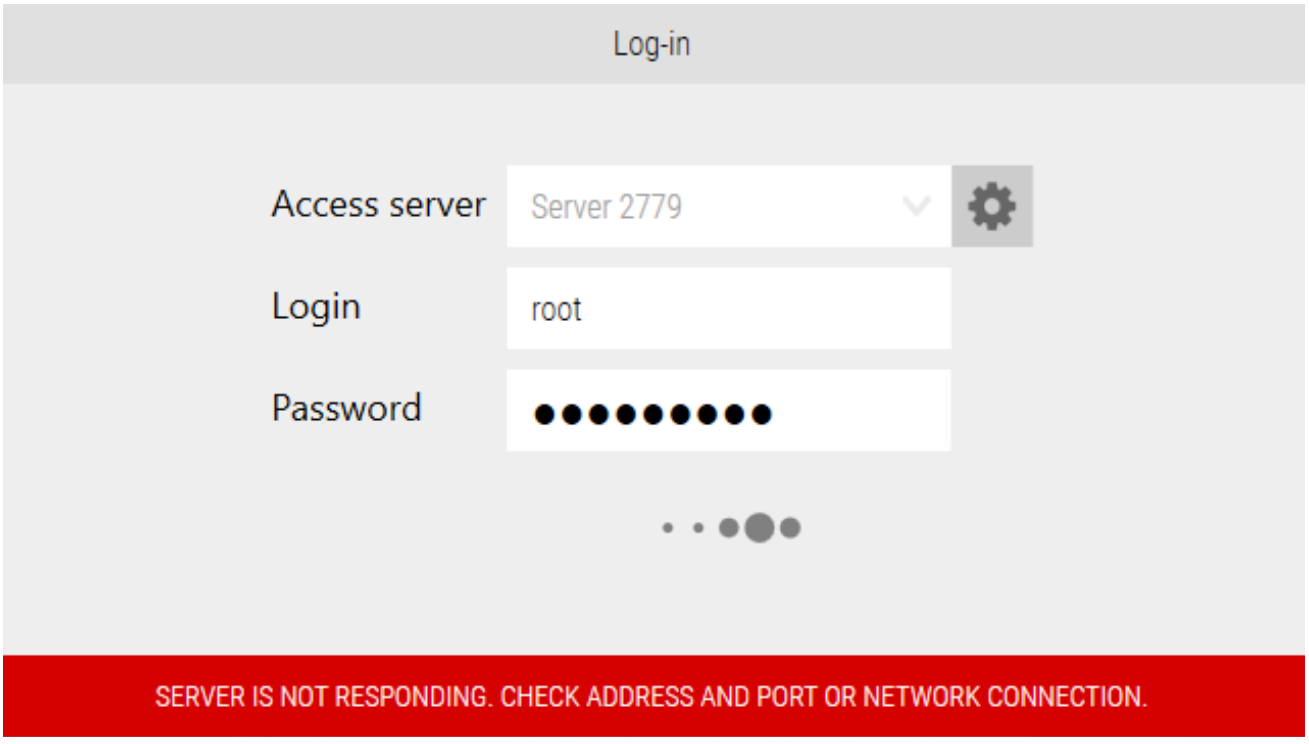


WARNING! If the email with the code is not delivered, click **"DIDN'T RECEIVE THE EMAIL? CLICK TO RESEND."**
If the email still does not arrive, check the **SPAM** folder in your mailbox.

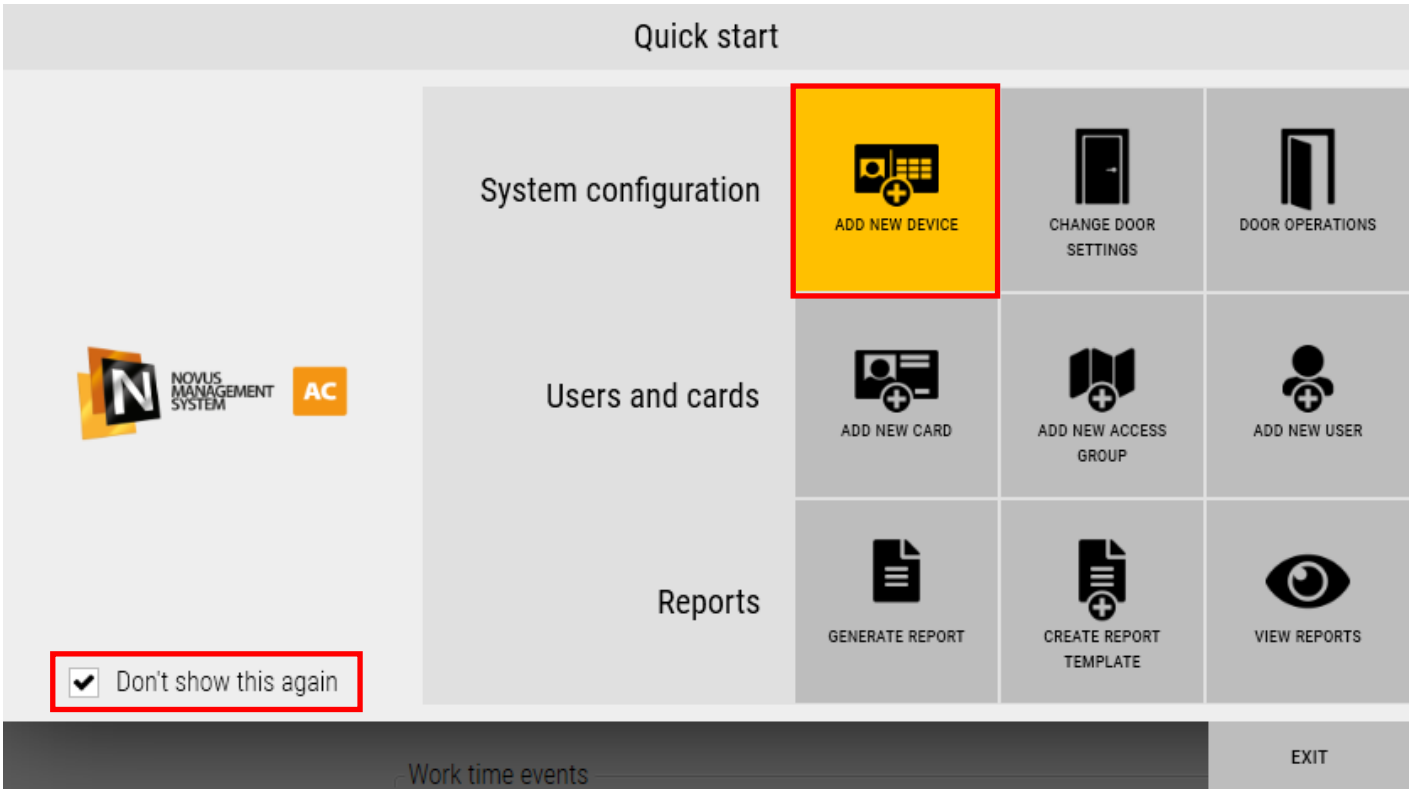
After you enter your name and password and click on the LOGIN button, you may see the message SERVER IN STARTING UP at the bottom of the window. This means that you should wait as the server service is starting up (e.g. after a reboot).



In an analogous situation, the message **SERVER IS NOT RESPONDING** may appear at the bottom of the window. This means that the server service has been stopped for some reason. You should then start the service manually using the Task Manager/Services window in Windows or by running the **start.cmd** script available in the applica-



Po wprowadzeniu poprawnych danych logowania na ekranie pojawi się okno ***Szybki start*** widoczne poniżej.



The ***Quick Start*** window contains nine shortcut icons for the most frequently used system options from three subject groups:

1. System configuration

- ***Add nee device*** - opens the window for adding devices to the system
- ***Change door settings*** - quickly opens the door settings details tab of the controllers added to the system
- ***Door operations*** - quickly opens the tab of operations possible on doors added to the system

2. Users and cards

- ***Add new card*** - opens the window for adding cards to the system
- ***Add new access group*** - quickly opens the Access Groups tab and adds a new access group
- ***Add new users***- quickly opens the Users tab and adds a new user

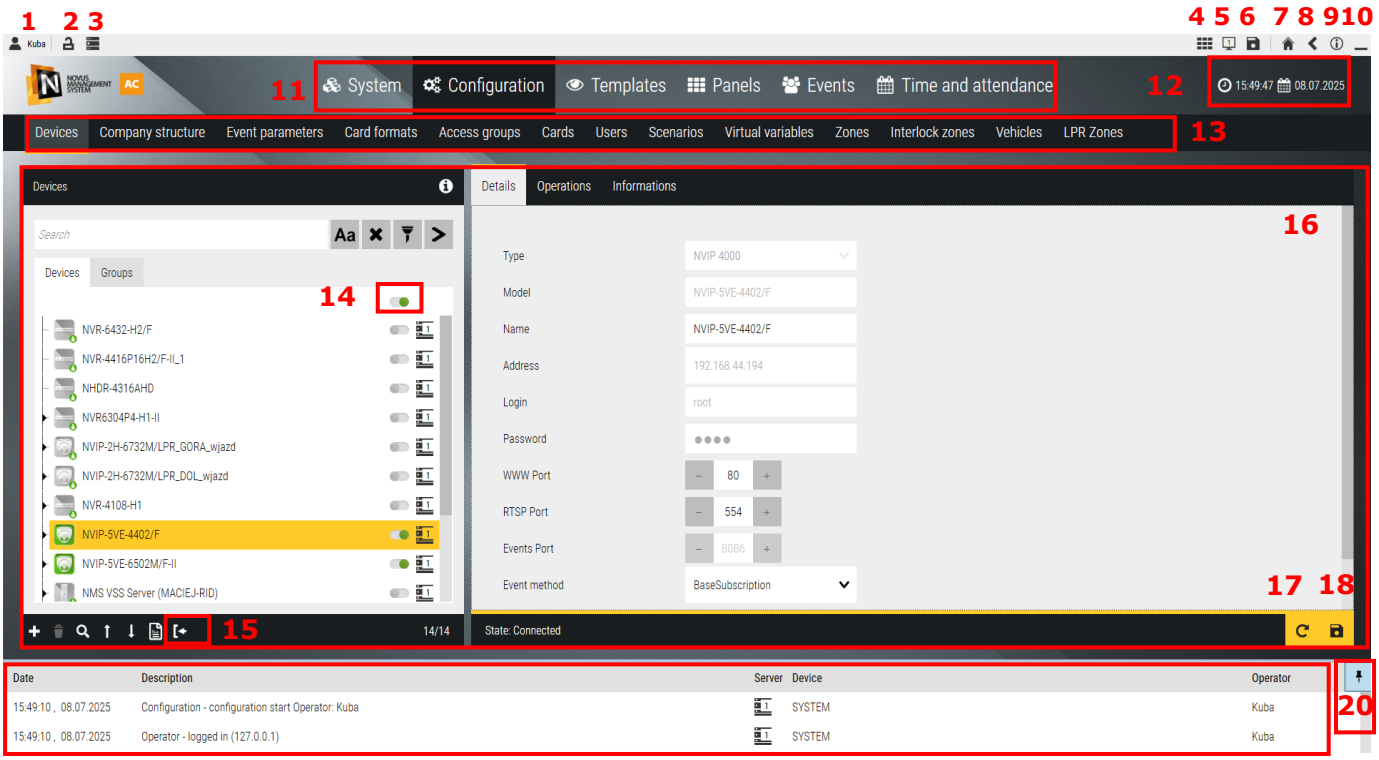
3. Reports

- ***Generate report*** - opens event list window where we can view and execute event report
- ***Create report template*** - opens the Events/Automatic Reports window
- ***View reports*** - opens the *Files* on Server tab in the Events section

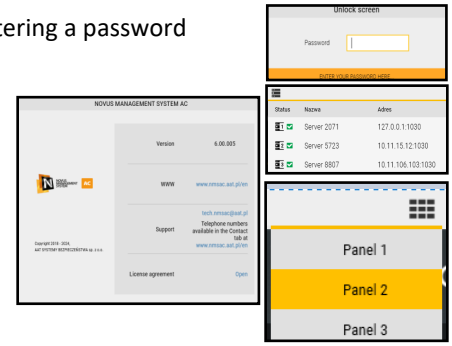
Selecting the **Don't show this again** checkbox detailed in the above figure causes the **Quick Start** window not to be automatically displayed when **NOVUS MANAGEMENT SYSTEM AC is** started. The Exit button closes the **Quick Start** window.

2.6 Operator screen and navigation in the program window

The operator's console is a graphical user interface that allows interaction with the NOVUS MANAGEMENT SYSTEM AC.



1. **Logout** button - logs out the current operator (next to the name) and opens the login screen.
2. **Screen Lock** button - blocks access to the program menu, unlocking requires entering a password
3. Shows the current server or the list of servers in the group (if created)
4. Shows a list of panels with the possibility to open the one selected from the list
5. Shows the number of the current monitor
6. Saves the current layout of the windows displayed on each monitor
7. **Quick Start** button - opens the Quick Start window.
8. **Back** button - displays the previous window
9. **About application** button - opens a window with the software version number and a link to the contents of the license



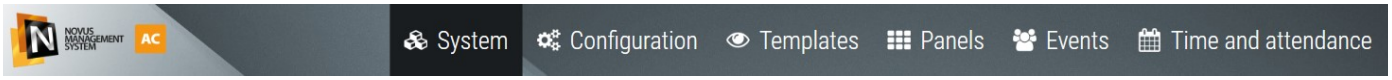
10. **Minimize** button - minimizes the program NOVUS MANAGEMENT SYSTEM AC window.
11. Section selection bar - click on the appropriate section to configure or preview options.
12. Current server time and date.
13. Tab bar - allows you to move between the various tabs of the selected section.
14. Button to connect/disconnect all devices on the list.
15. Button to import a list of devices from a file exported from the NOVUS MANAGEMENT SYSTEM VSS program.
16. Workspace - properties of the item selected in the left window
17. **Refresh** button - refreshes the displayed data
18. **Save** button - saves the changes made to the system configuration
19. **System log** window - displays logs about changes in system configuration and other system events.
20. Button to pin the log window (pin) - allows you to change the display of the log window - either as visible permanently in the screen area or have the form of a collapsible bar at the bottom of the screen thus increasing the working area (14). After clicking on this button, the beam can be collapsed. To expand it again, click on:

The bar automatically expands when new events appear in this window, and collapses when clicked in the workspace.

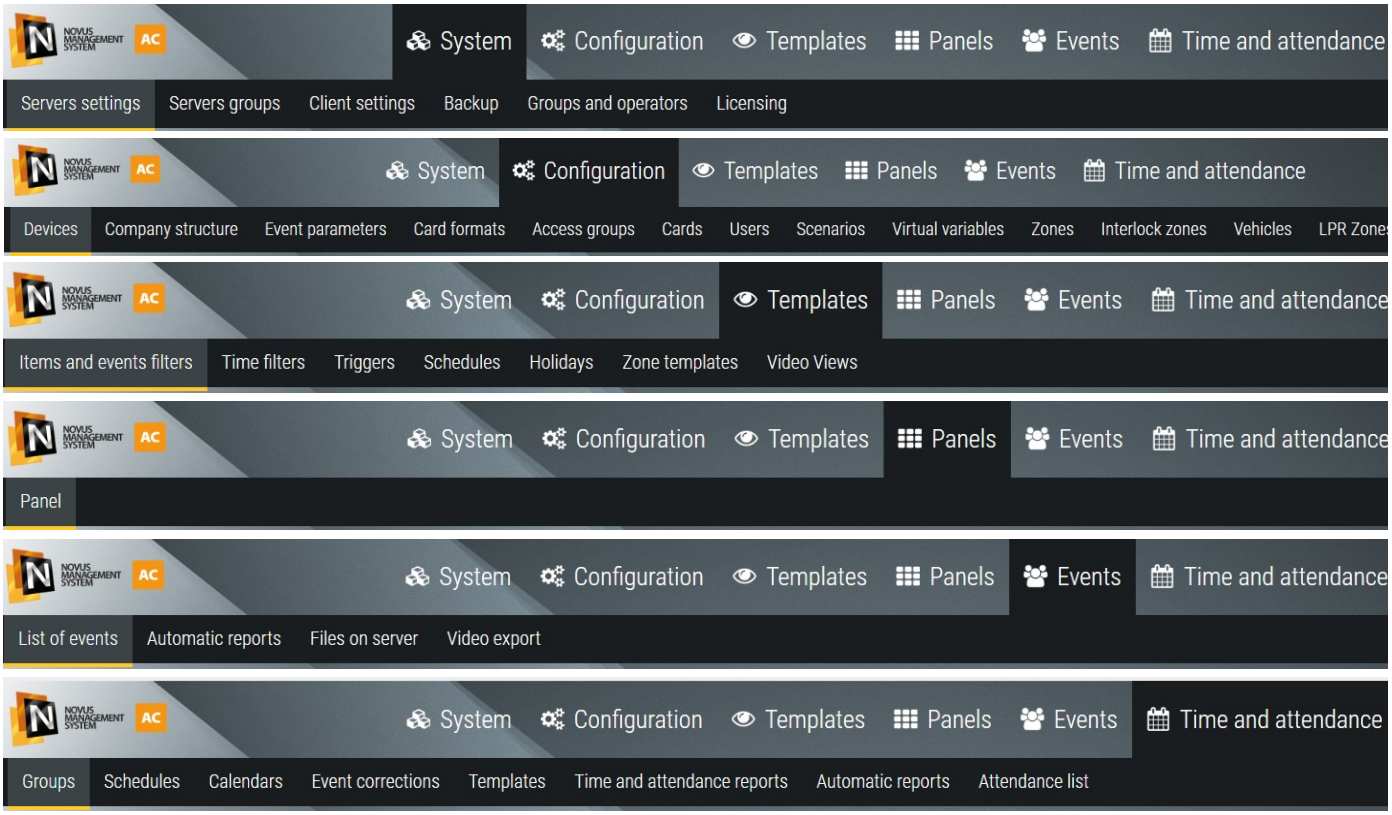
2.7 Program menu

The program menu contains two bars.

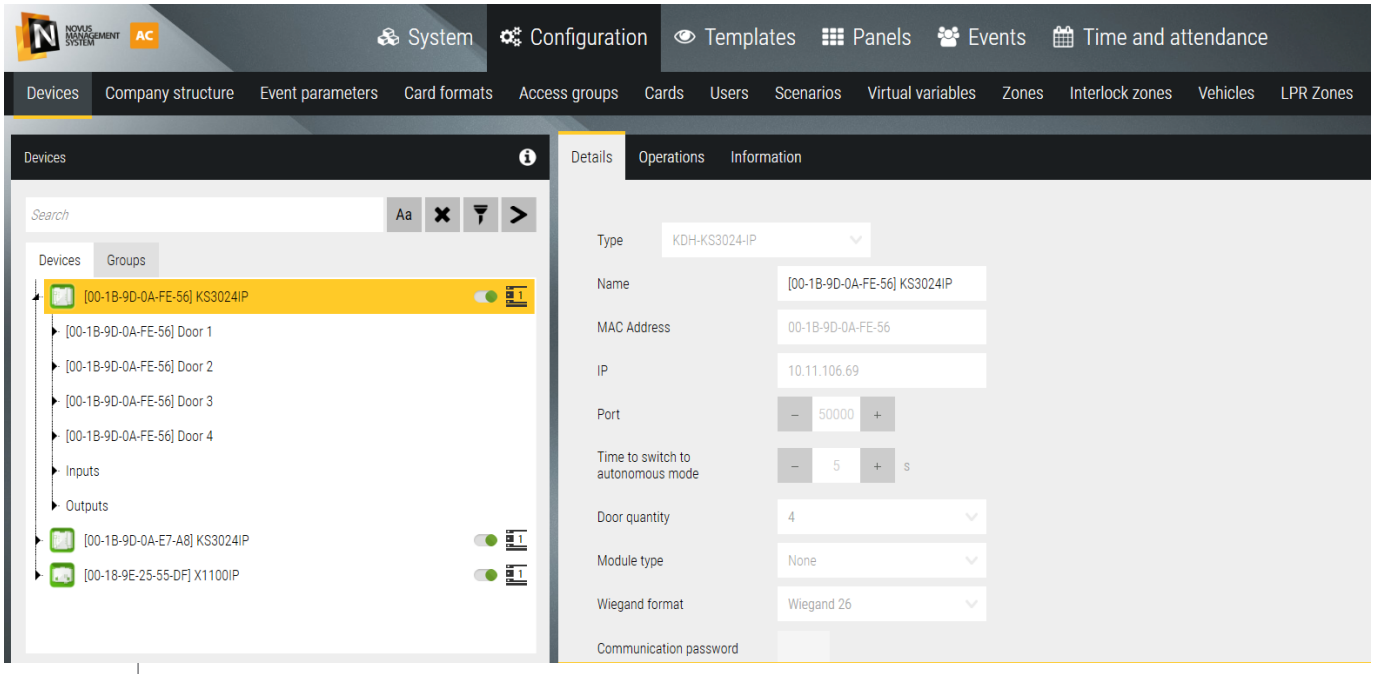
Main bar:



It has **6 tabs,** each of which contains the following items:



Each tab on the second bar contains further tabs and two windows: the left one with the list of items and the right one with the settings of the item selected in the left window. For example, in the Configuration / Devices window it looks as follows:



2.8 Icons ant their meaining

Icon symbol	Description	Location
	Back	Top bar
	Logout	Top bar
	About the application	Top bar
	Quick start	Top bar
	Monitor selection	Top bar
	Minimize	Top bar
	Edit panel	Top bar
	Return to configuration	Top bar
	Lock screen	Top bar
	List of servers	Top bar
	List of panels	Top bar
	Save windows on monitors	Top bar
	Search	Top bar
	Go to panel	Top bar
	Date	Top bar
	Time	Top bar
	Pin the console	-
	Server number	-
	Complete the setup	-

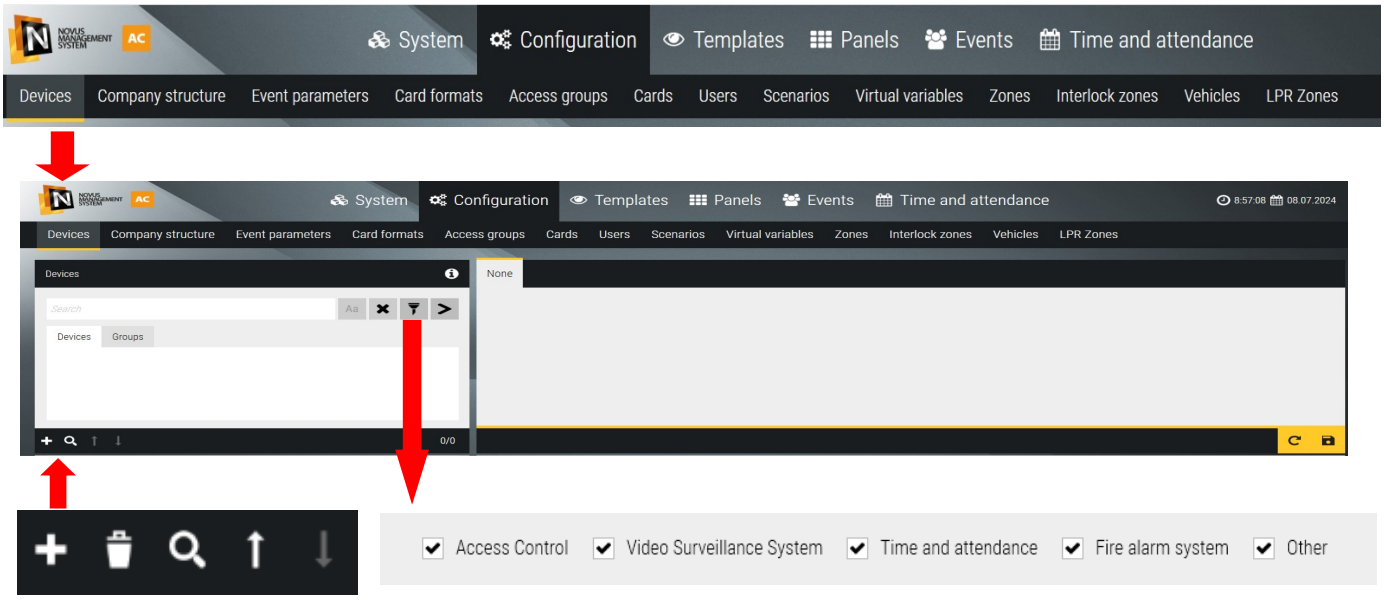
Icon symbol	Description	Location
	Report in CSV	Events
	Report in HTML	Events
	Auto report.	Events
	Alarm deletion	-
	Alarm	-
	Size of letters	-
	Error / info	-
	Refresh	Configuration
	Save	Configuration
	Add	Configuration
	Delete	Configuration
	Import list	Configuration
	Export list	Configuration
	Search	Configuration
	Clone	Configuration
	Reset to defaults	Configuration
	Set as default	Configuration
	Move up	Configuration
	Move down	Configuration

Section 3. System configuration

This chapter will discuss the configuration of the NOVUS MANAGEMENT SYSTEM AC system. These are activities performed by the system installer. The Configuration tab is used for this purpose. It contains a number of windows for adding devices to the system, access levels, cards and users, scenarios and virtual variables, vehicles, LPR zones and more.

3.1 Devices - Access control - Controllers

We start the configuration process from the *Devices* tab.



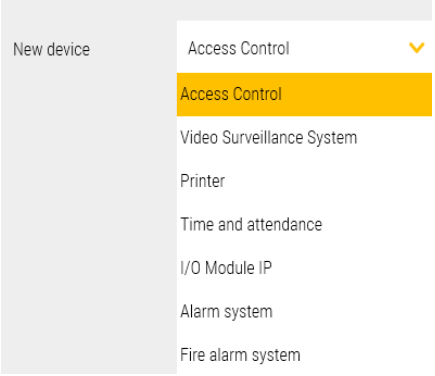
- add new device
- remove
- search
- change order of devices up/down

Type filter allows you to display a list of devices containing one or different types of devices

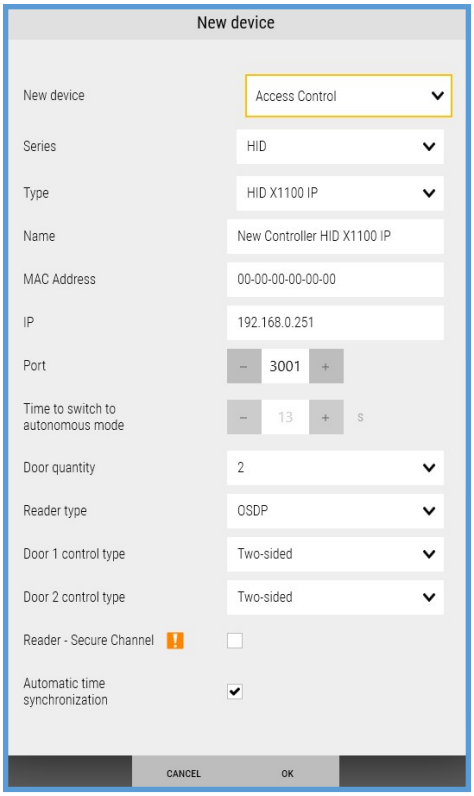
The system can be configured off-line before connecting to the system at the site, but it is much faster to configure the process on-line when we have the devices already installed, connected to the power supply and Ethernet network. We can then use a search engine, which, after searching the network, will display a list of available devices along with their address parameters. This procedure will be described in the next section.

Add a new device

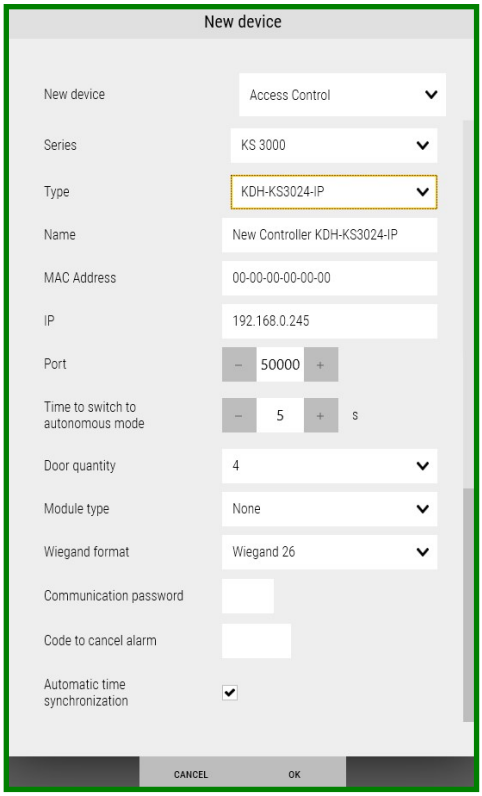
This option allows us to add a new device off-line when we cannot use the search engine. After clicking on this button, a window will appear as on the next page, where we can select the type of device we want to add:



Po wybraniu urządzenia do systemu kontroli dostępu wyświetli się okno jak poniżej:



HID® series



3000 Series

Series - you can select the series of controllers to be added from the drop-down list:

- HID®
- KS 3000

HID® series:

Type - you can select the controller model from the drop-down list:

- HID® Aero® X1100
- HID® Aero® X100
- HID® Aero® X200
- HID® Aero® X300

Name - editable field for entering controller name

MAC - editable field for entering the MAC address of the controller (it is on the sticker on the device).
If you do not know this address at this stage, leave the default one.
When communication is established with a device with an IP address as below, this field will be updated.

IP - editable field for entering the static IP address of the controller
(default for HID® 192.168.0.251 - should be changed to target)

Port - editable field for entering the port number (it is recommended to leave the default value)

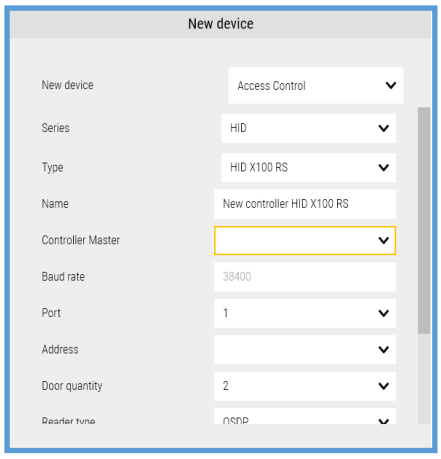
Configuration of the door, only for **HID® Aero® series** - X1100 i X100:

Door quantity - 1 or 2 doors can be selected from the drop-down list depending on the installation requirements.

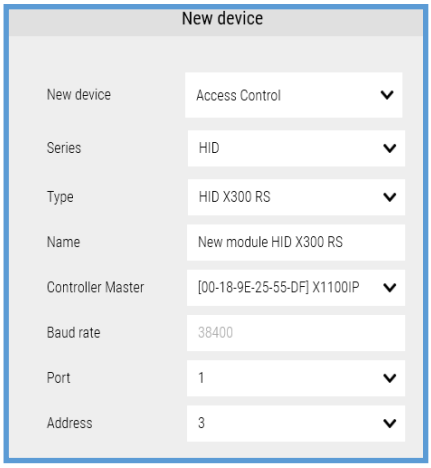
Reader type - OSDP or Wiegand, depending on the method of communication between the controller and the readers.

Door control type 1/2 - Two-sided or One-sided controlled, in the case of HID® controllers, we can make a mixed installation with one-sided and two-sided controlled transitions on a single unit.

Reader Secure Channel - Enable AES-128 encryption between controller and readers - **only for OSDP!**



HID® series



HID® series

Controller master - selection of the controller to which we will connect the modules (X100, X200 i X300)

Port - Selection of port 1 or 2 of the RS-485 bus to which the modules are connected (X100, X200 i X300)

Address - RS-485 bus address set on the DIP switches of the modules (X100, X200 and X300) specified in the range 0-31

3000 series:

Type - You can select a controller model from the drop-down list:

- KDH-KS3012-IP
- KDH-KS3024-IP
- KDH-KZ3000-IP-U lub M
- KDH-KZ3000FP-IP-U lub M
- KDH-KZ3000-IP-ELV

Name - editable field for entering controller name

MAC - editable field for entering the MAC address of the controller (it is on the sticker on the device).

If you do not know the address at this stage then leave the default one.

When communication is established with a device with an IP address as below, this field will be updated.

IP - editable field for entering the static IP address of the controller

(default for KS30xx 192.168.0.245 - change to target)

Port - editable field for entering the port number (it is recommended to leave the default value)

Door quantity - 1,2 or 4 doors can be selected from the drop-down list depending on the controller model

Module type - from the drop-down list can be selected depending on the controller model:

- KDH-MOD3000INOUT (for controllers KDH-KS3012/24),
- KDH-MOD-30004-ELV i KDH-MOD-30016-ELV (for the KDH-KS3000-IP-ELV controller)

Wiegand format - from the drop-down list select the appropriate format for the reader

Communication password - editable field for entering a 4-digit communication password (0000 - 9999)

Code to cancel alarm - editable field for entering 6-digit alarm reset code

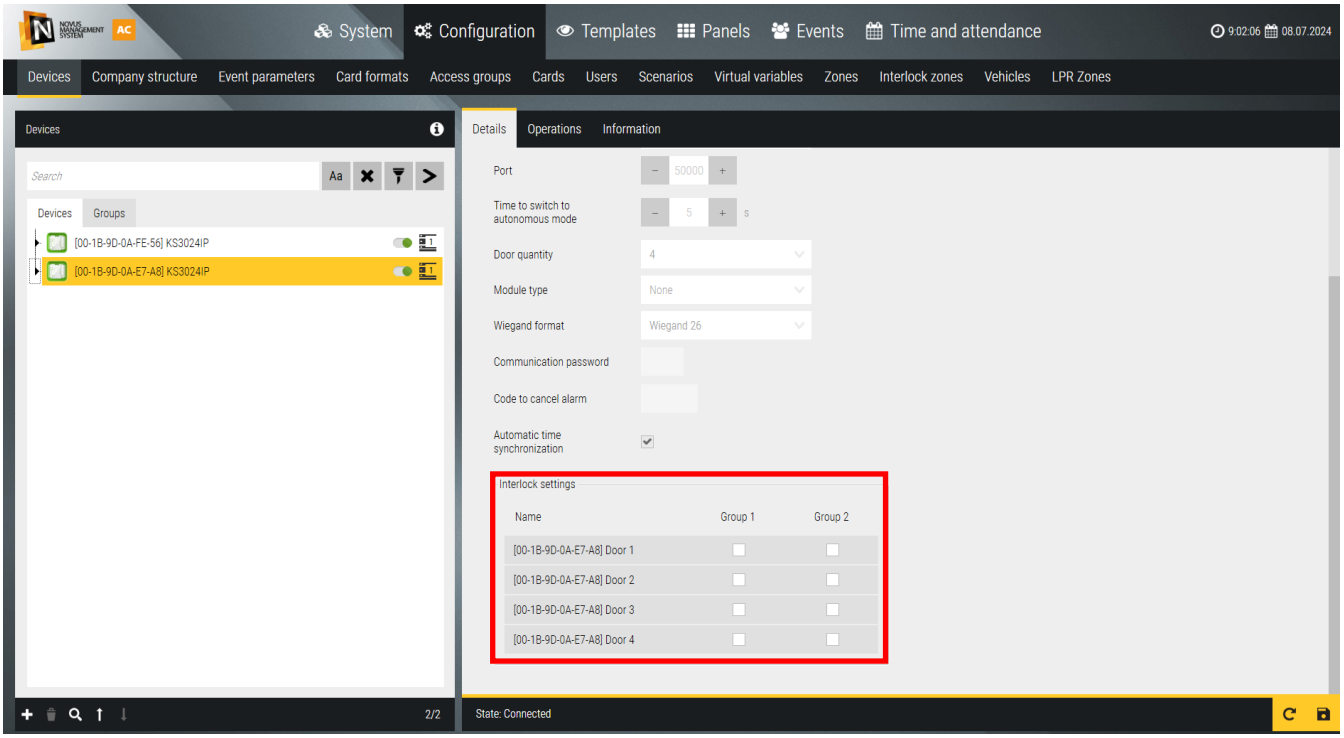
Automatic time synchronization - when this box is checked, the time in the controller will be synchronized from the server every 4 hours

Options for integrated controllers:

Administrator password - entering programming mode from the keypad (concerns KDH-KZ3000-IP-U and M)

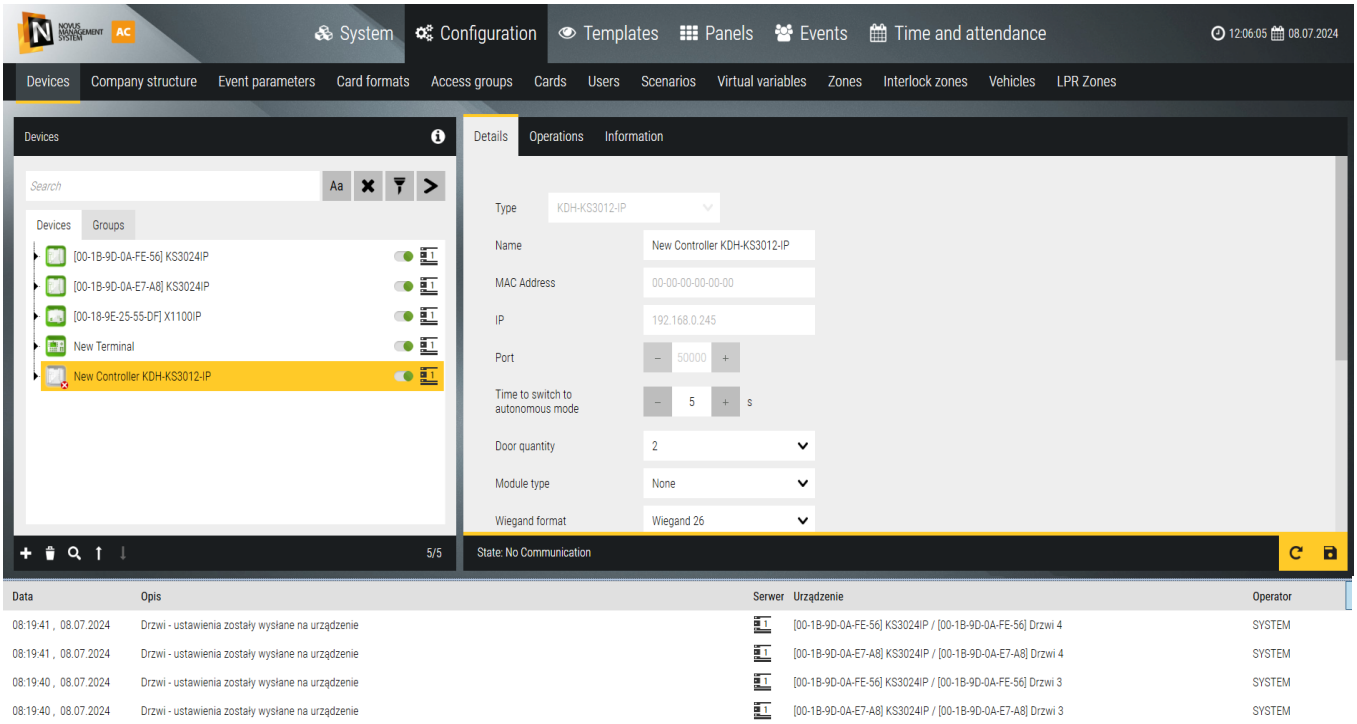
Enabled tamper alarm - activation/deactivation of the tamper alarm (concerns KDH-KZ3000-IP-U and M)

Enabled door magnet alarm - activation/deactivation of the door intrusion alarm (concerns KDH-KZ3000-IP-U and M. After making the above-mentioned settings, click OK - the program will return to the main configuration window, and the added device will appear in the list in the right window.



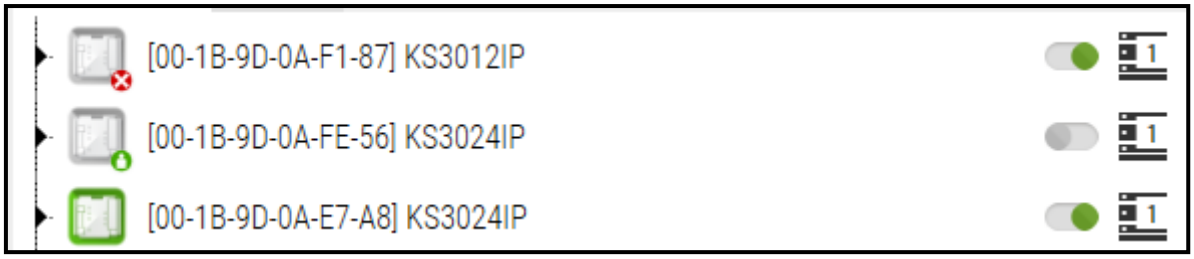
For KDH-KS3012/24-IP controllers, additional fields appear in the lower right window to add the controller's doors and readers to one or two groups. This applies to the lock function (i.e. mutual control of door leaf status) . These fields do not appear for the elevator controller.

After all settings have been made, save them by clicking on the floppy disk icon in the lower right corner. A series of messages about this operation will appear in the system log window and the controller icons will turn green. Saving can be done once after adding more than one device.

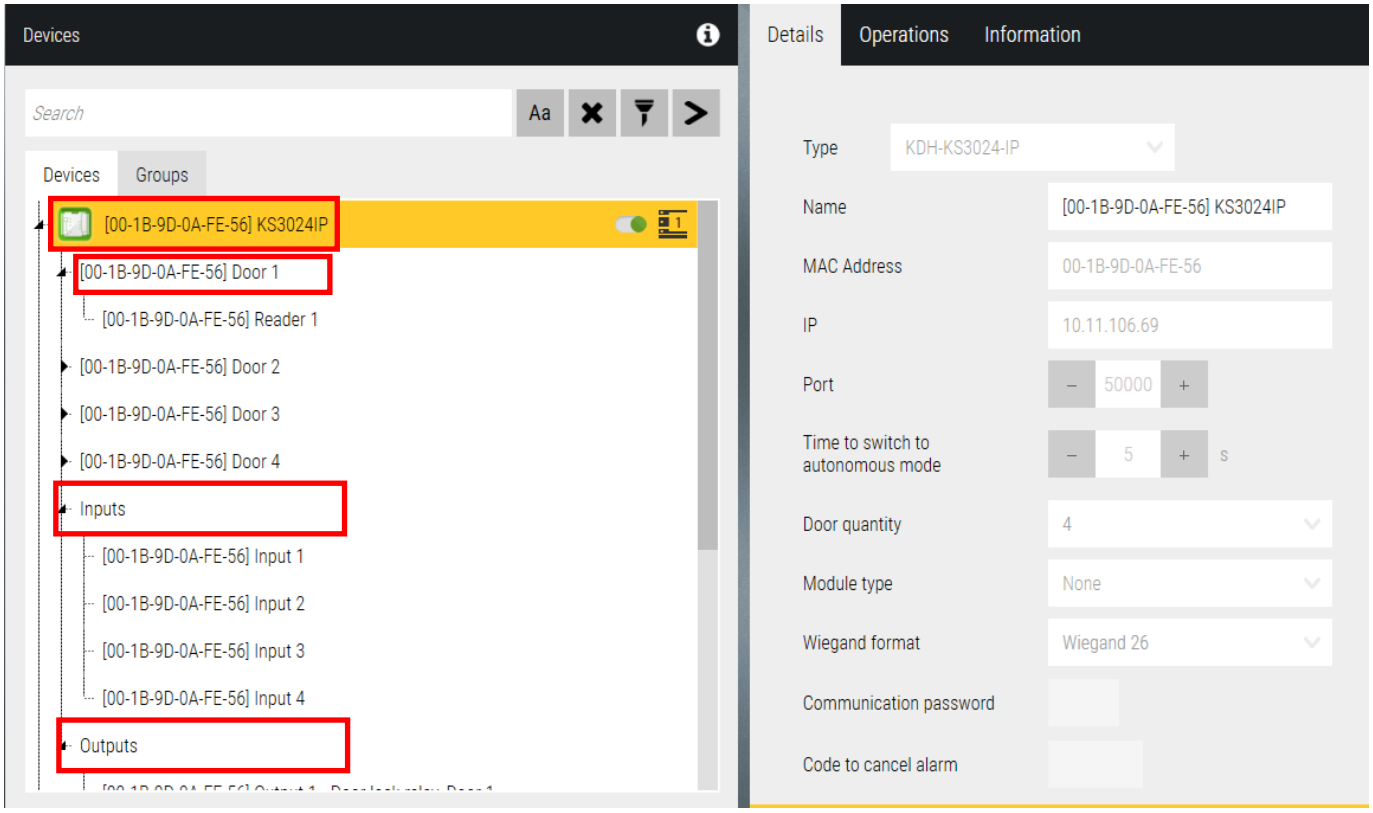


After saving the settings, the icon status can show one of three situations:

- No communication with the device - gray icon with red field (check address settings or network connection and power supply)
- Device disconnected by the operator - gray icon with a green field (disable monitoring by moving the slider on the right to the left, to edit settings or perform service actions)
- Communication correct - green icon



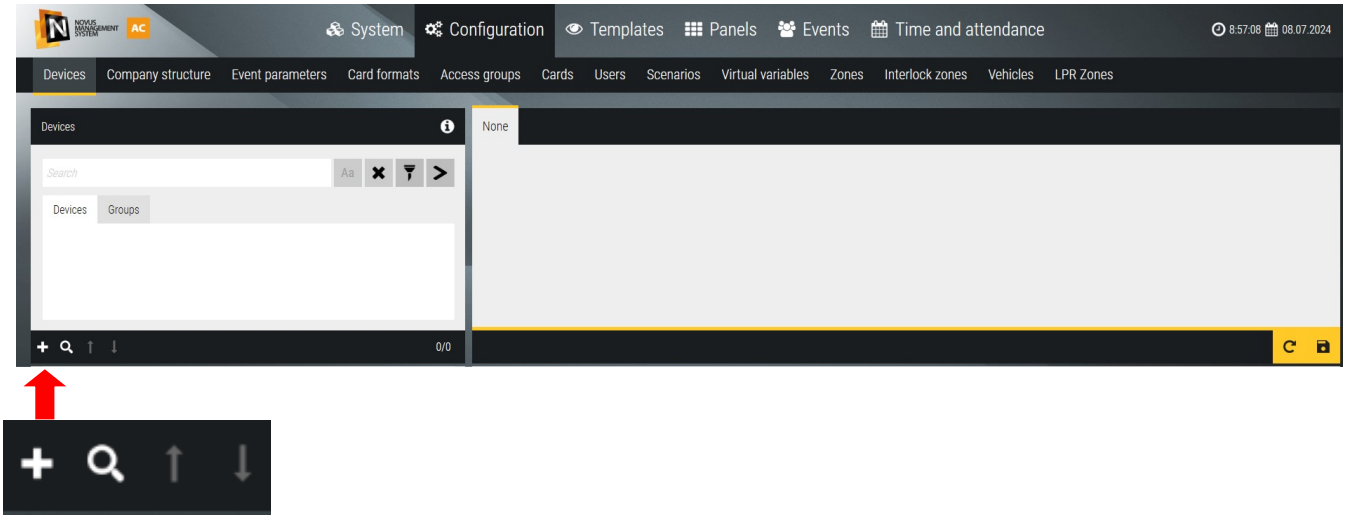
The controller icon can be expanded by clicking on the black triangle on the line of the main tree and display the cooperating elements. By selecting the desired element in the expanded list, we can edit its settings



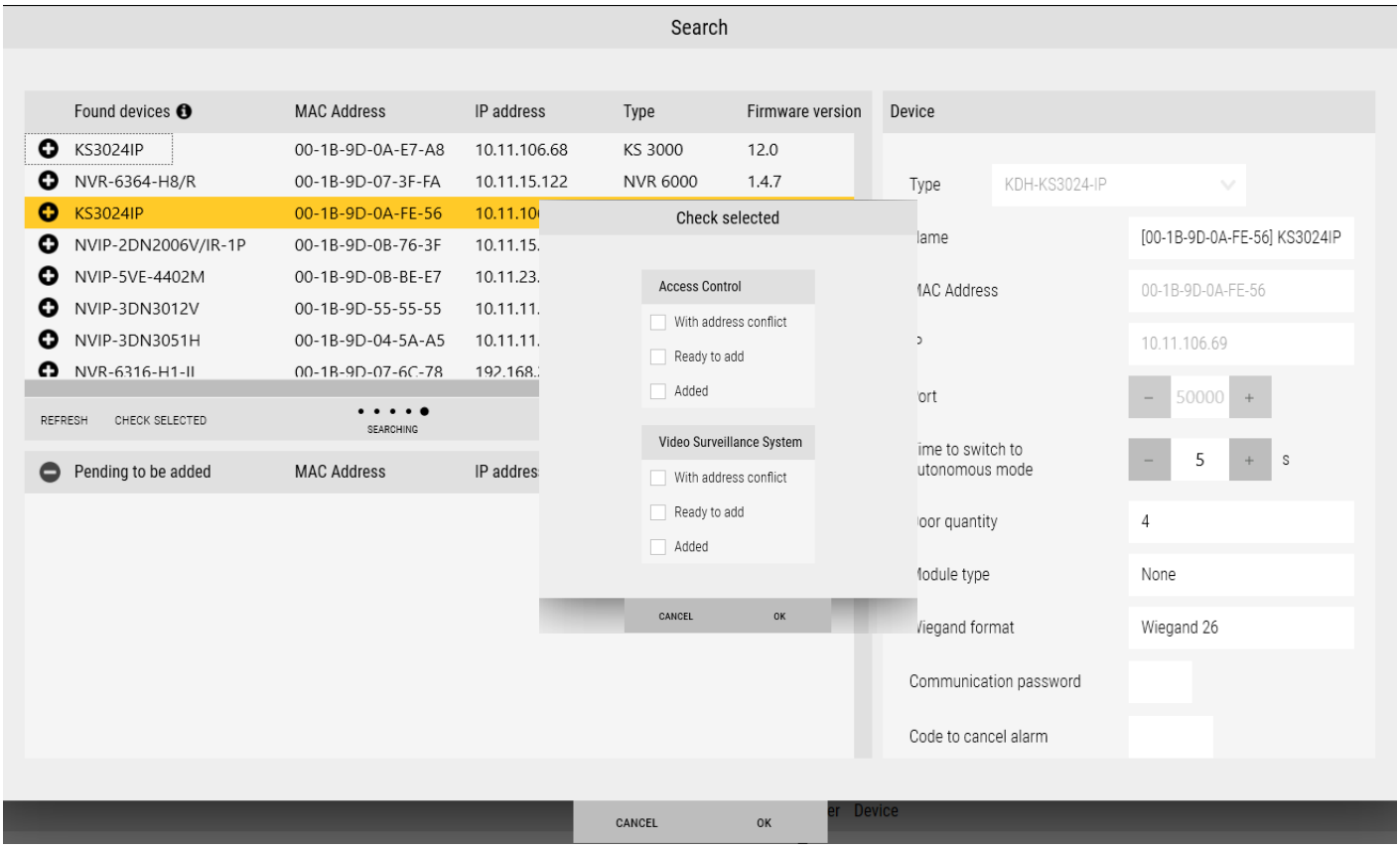
This includes such elements as doors, readers, input lines and control outputs. After selecting a selected element, its settings are displayed in the right window and can be edited. The selected element is highlighted in yellow. After changing the settings, save them by clicking on the floppy disk in the lower right corner of the configuration window. To edit the controller's settings, disconnect it by moving the green slider to the left. After editing, move the slider to the right again and click on the *Save* icon.

A configured controller can be edited or deleted by selecting it in the list and clicking on the *Delete* button in the lower left corner of the window. Along with the controller, all cooperating elements in the entire system are removed.

Search for access control devices



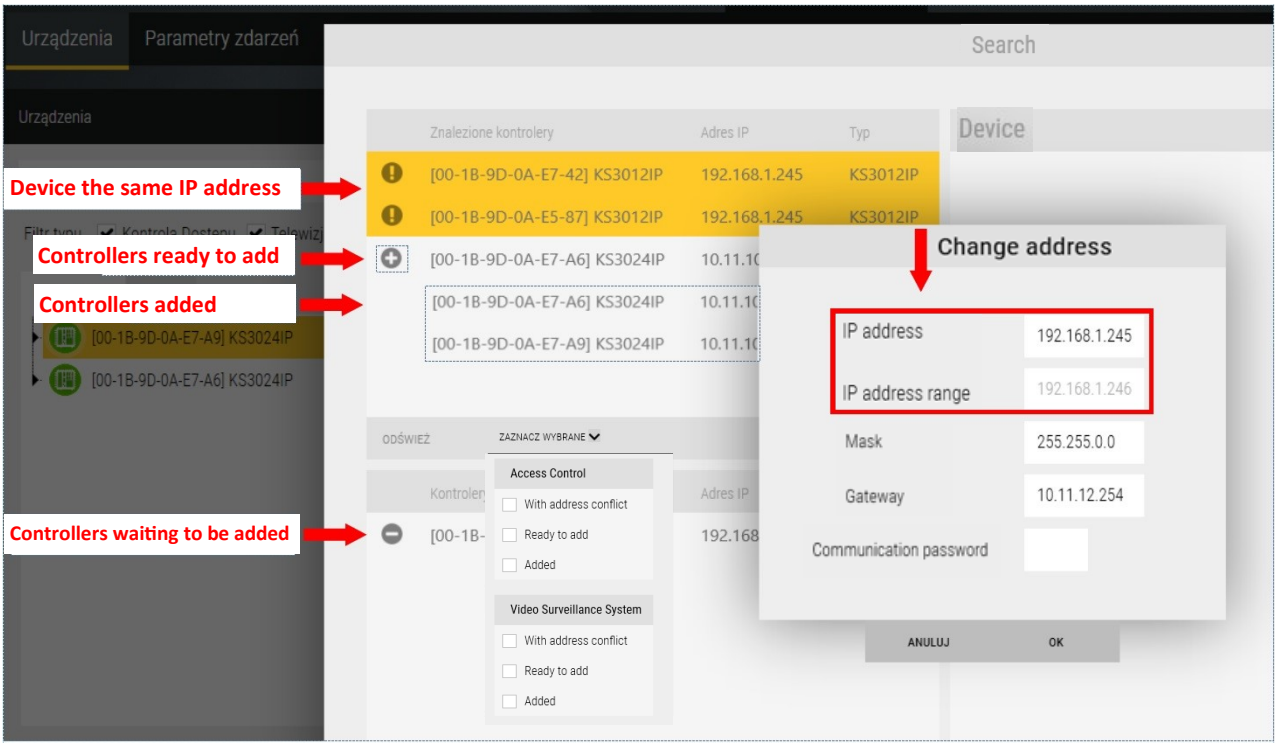
When the controllers have been installed on the site, connected to Ethernet and power, it is recommended to use the search engine available in the program to add them to the system database. This speeds up the process considerably. To start the search engine, click on the Search button at the bottom of the window as above. The program will display a window that lists the controllers searched for in the network.



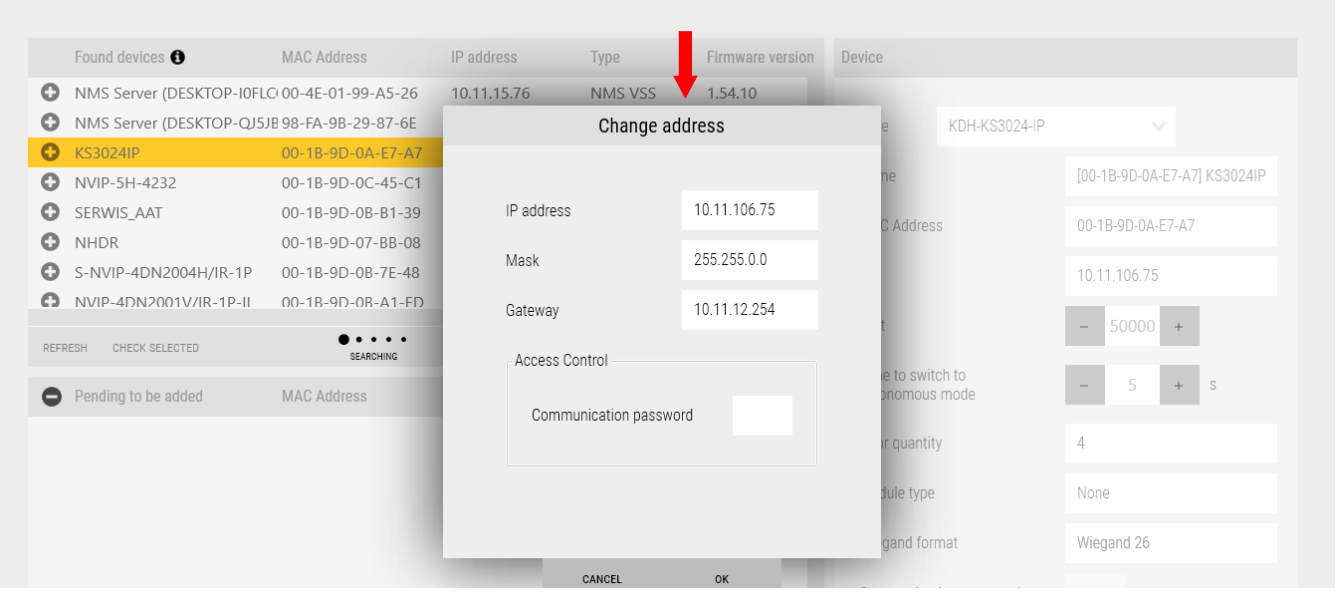
Statuses of searched controllers displayed in top left window:

- - controllers with the same IP addresses - are displayed at the very beginning of the list
- - controllers that can be added to the system
- - controllers moved from the list in the top window and waiting to be added
- - controllers already added to the system - no icon in front of the device

Each new 3000 series controller has the same default IP address - 192.168.0.245. This group of controllers is displayed at the beginning of the list with the icon - according to the address pool assigned by the administrator to the next destination by clicking on the *Change Address* button. *After entering the starting address, the end address of the range will be generated automatically depending on the number of selected controllers with the same IP address*. The icons will change to and can then be added to the bottom window by clicking on these icons. **HID® series** controller addresses must be configured from the browser according to the instructions included in the package, it is not possible to change the address from NOVUS MANAGEMENT SYSTEM AC software.



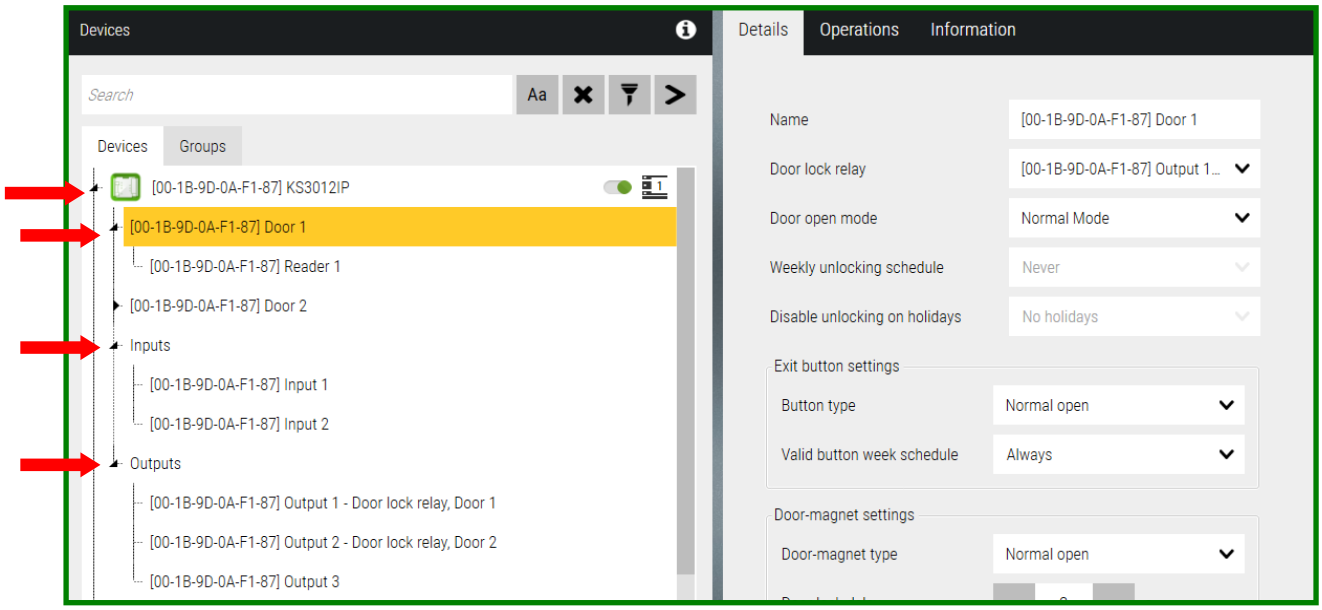
In the drop-down list, we can choose which group of controllers we want to select. In case we want to change the address of one retrieved controller, we select it in the list in the upper window and click on the *Change Address* button.



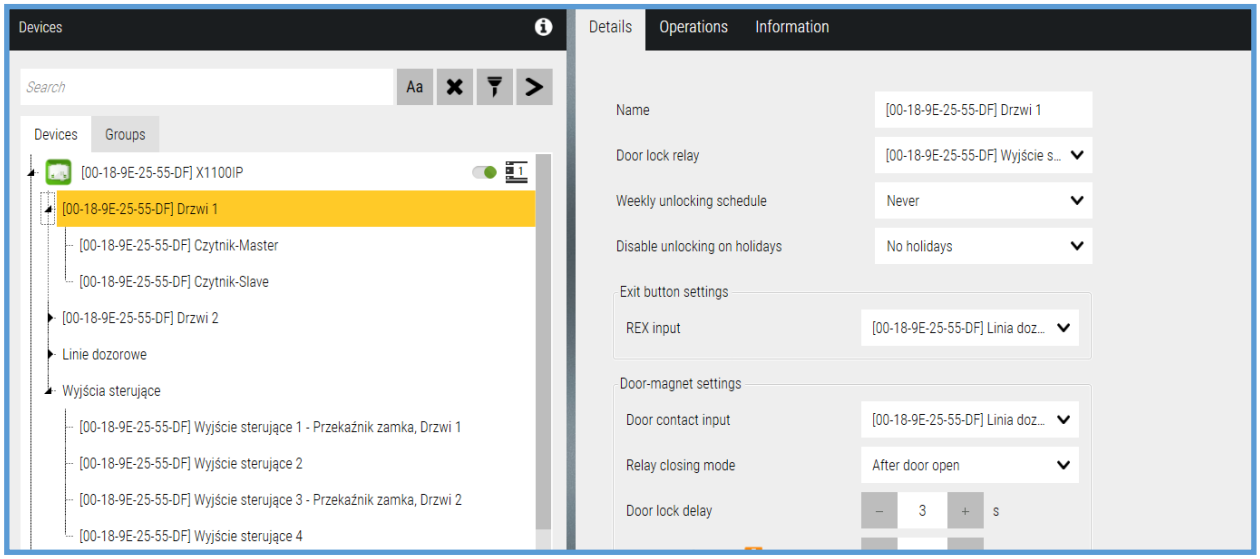
After setting the addresses and adding all controllers to the list in the bottom window, click on the OK button. The added controllers will appear in the *Devices* window.

3.2 Devices - Access control - Controller - Door

In the process of adding controllers, the program automatically adds mating components in quantities depending on the type of controller. This includes doors, supervisory lines, control outputs and expansion modules. These elements appear under each of the added controllers and can be displayed by clicking on the black triangles in the individual branches of the device tree.



3000 series



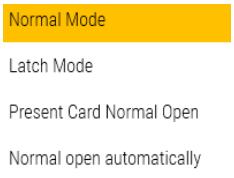
HID® series

Door settings

Name - An editable field for entering a door name in place of the default name.

Door lock relay - From the drop-down list, you can select the control output (relay) that will control the lock,
By default, relays 1-2 or 1-4 are assigned, and relay 3 or 5 is the relay to connecting an alarm siren.

Door open mode - to choose one of four modes - only on **3000 series** controllers:



Normal Mode - Unlocks the door for the time set in the field below.
Latch Mode - Unlocks and locks the door alternately after successive card readings.
Modes 3 and 4 require a schedule to be set, at the beginning of which the door is unlocked on a permanently after reading a valid card or automatically.

Weekly unlocking schedule - A preset schedule can be selected from a drop-down list, according to which the door will be permanently unlocked after reading a valid card (3000 series) or automatically depending on the option selected above.
Disable unlocking on holidays - applies to holidays, overrides the weekly unlock schedule and blocks its operation if there is a holiday during the week on which the door should not permanently unlock.

Exit button settings

3000 series:

Button type - NO or NC type can be selected from the drop-down list - NC is recommended.

Valid button week shedule - you can select a predefined schedule from the drop-down list, during the period of its activity the door will not be unlocked by pressing the button.

HID® series:

REX input - select from the drop-down list the monitoring line assigned to the exit button.

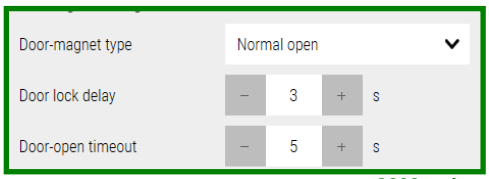
Door-magnet settings

3000 series:

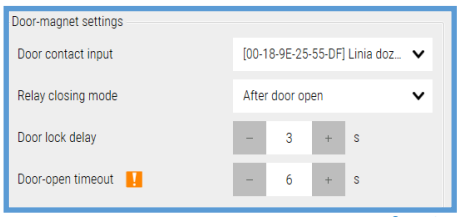
Door-magnet tpe - NO or NC type can be selected from the drop-down list

Door lock delay - editable field for entering the time (s) of unlocking the lock after reading a valid card or pressing the exit button. The time can also be set by clicking on the - or + buttons. Maximum value - 50 s.

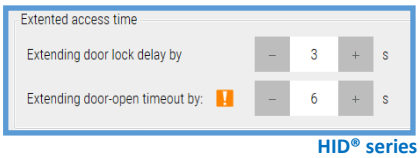
Door-open timeout - editable field for entering the time (s) for closing the door leaf. After the expiration of the time, which is the sum of the times for closing and unlocking, a Door Held alarm will be generated - default is 8 sec. (3+5). The time can also be set by clicking on the - or + buttons. The maximum value - 50 seconds.



3000 series



HID® series



HID® series

HID® series:

Door contact input - selecting from the list the monitoring line assigned to the door status sensor (door magnet)

Relay closing mode - After door open/ After door close

Door lock delay - editable field for entering the time (s) of unlocking the lock after reading a valid card or pressing the exit button. The time can also be set by clicking on the - or + buttons. Maximum value - 255 s.

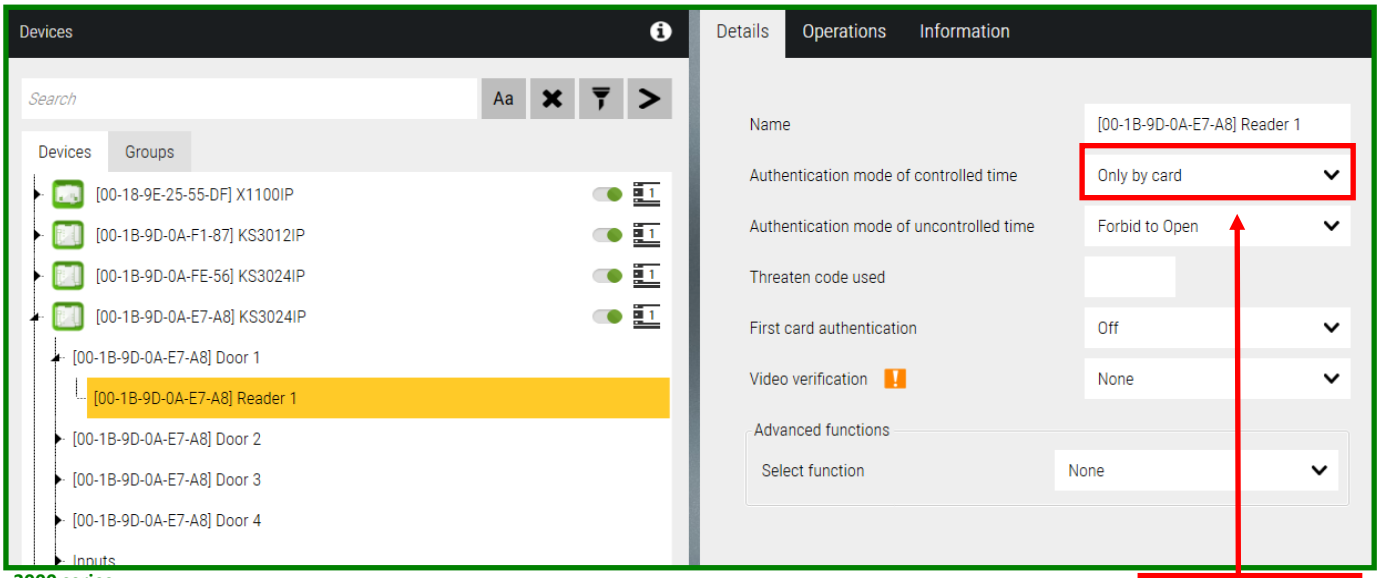
Door open timeout - editable field for entering the time (s) for closing the door leaf. After the expiration of the time, which is the sum of the times for closing and unlocking, an alarm Door Held , configurable only in the range of even numbers from 2 (s) to 512 (s), will be generated.

Extended acces time - allows you to increase the access time to a given passage for users with appropriate permissions

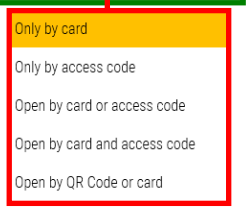
Extending door lock delay by - extends the unlocking time of the lock by the set time in seconds

Extending door-open timeout by - Extends the time to close the door by the set time in seconds (even numbers only)

3.3 Devices - Access control - Controller - Door - Readers



3000 series



3000 series:

Name - editable field for entering the name of the reader in place of the default name

Authentication mode of controlled time - You can select one of the options from the drop-down list:

Authentication mode of uncontrolled time - You can select one of the options from the drop-down list: (this mode applies to off-hours, weekends and holidays)

Threaten code used - field to enter the access code to be used on the reader keypad in case of forced entry. It causes a discrete alarm to be generated at the operator's station.

First card authentification - gaining access requires the use of a card with this option set to YES first within each 24-hour period (there is such a field in the card settings).

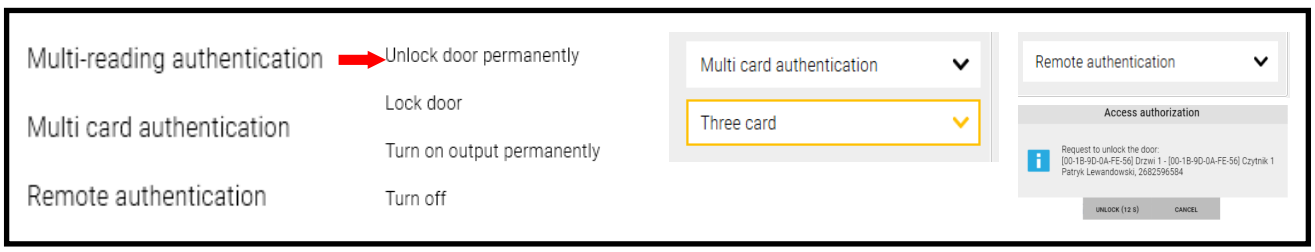
Video verification - allows you to assign a camera installed above (or built-in) the reader to record a freeze frame when the card is read. The freeze frame is attached to the event in the stack and in a report on the screen.

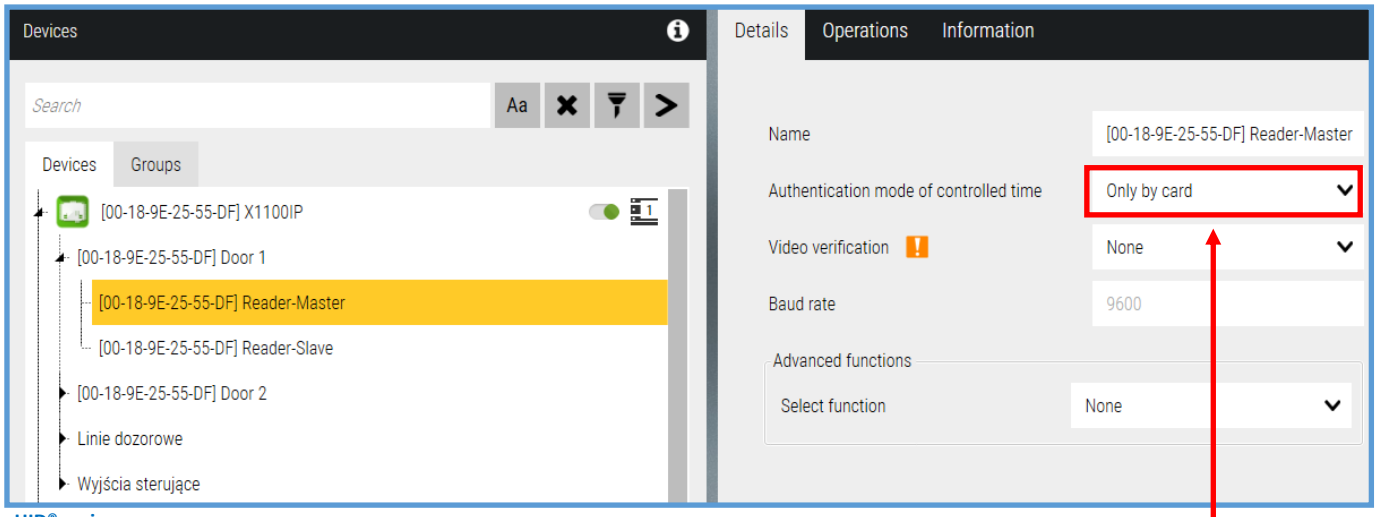
Advanced functions: - selection as in the window below:

Multi-reading authentification - Allows you to extend the function of the card. By reading the authorized card 2 or 3 times, it is possible to unlock/lock the door permanently or enable/disable the control output. Applies to selected door and authorized card.

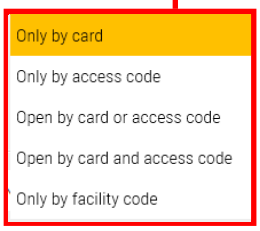
Multi card authentication - gaining access requires the use of one to four valid cards consecutively. Special option for rooms requiring greater security.

Remote authentication - when checked, gaining access from this reader will require reading a valid card and confirmation by the operator in a special pop-up window. Select this option only when the system is online and an operator or security officer is present at the station.





HID® series



HID® series:

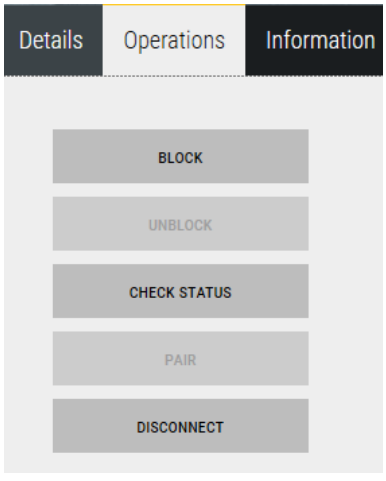
Reader-Master - Reader connected via OSDP protocol with address set to 0
Reader-Slave - Reader connected via OSDP protocol with address set to 1
Name - an editable field for entering the reader's name in place of the default name.
Authentication mode of controlled time - from the drop-down list, you can select one of the options shown on the right:

Video verification - allows you to assign a camera installed over the reader to register a freeze frame when the card is read. The freeze frame is attached to the event on the stack and in a report on the screen
Baud rate: Only for readers connected after OSDP - the speed of the data transmission (9600 as standard) requires setting the same configuration in the reader.

Advanced function - selection as in the window below:

Remote authentication - when checked, gaining access from this reader will require reading a valid card and confirmation by the operator in a special pop-up window. Select this option only when the system is online and an operator or security officer is present at the station.
Multi card authentication - gaining access requires the use of one to four valid cards consecutively.
Special option for rooms requiring greater security.
Multi-odczyt - allows you to extend the function of the card. By reading the authorized card 2 times, it is possible to unlock/lock the door permanently or enable/disable the control output. Applies to selected door and authorized card.

Operations:



HID® series

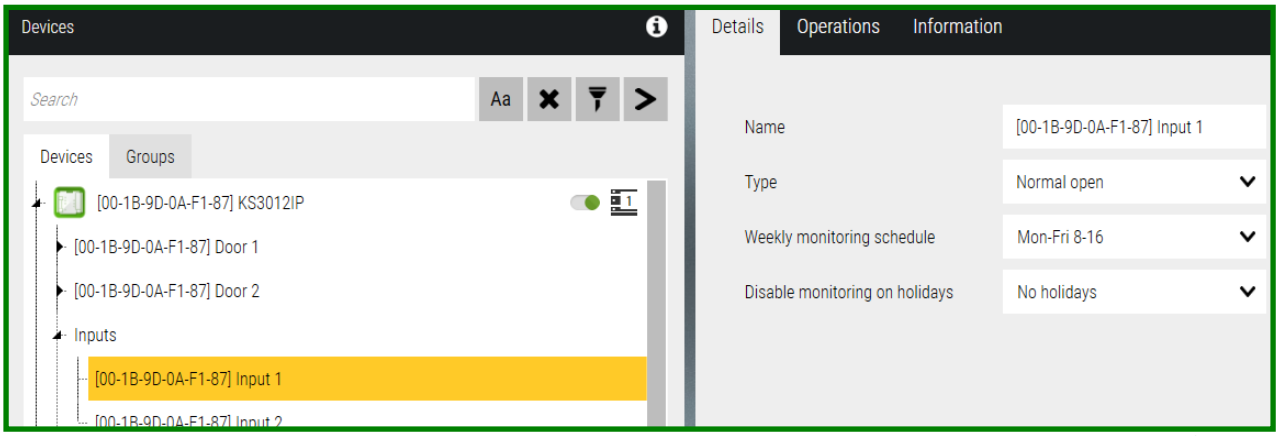
Block/ Unblock reader - allows locking/unlocking of the reader by the operator

Check status - displays the status of the reader (only for OSDP) indicating communication , connection encryption enabled or disabled.

Pair - is used to pair readers connected over OSDP with encryption (secure channel) enabled - in the HID® reader, its communication must be properly configured by enabling HID® Reader Manager in the mobile application*:* **SPEC COMPLIANCE - V2, Install Mode - włączony, Secure Mode - włączony**

Disconnect - is used to disconnect from readers connected after OSDP with encryption (secure channel) enabled. After disconnection, the reader must be reconfigured in the HID® Reader Manager application, the reader address and functions are reset **Instal Mode i Secure Mode**

3.4 Devices - Access control - Controller - Inputs



Seria 3000

Input lines located on the controller allow connection and monitoring of various types of detectors.

To enable the monitoring mode, the weekly and holiday schedule must be set to the input line. If monitoring is disabled then a change in the state of the line will only result in a change in the state of the icon on the panel Depending on the controller model, there are 2 or 4 supervision lines and 4 on the KDH-MOD2000INOUT expansion module for the 3000 series and 7 supervision lines for the HID® Aero® X1100 and X100 series, 19 supervision lines for the X200 module and 5 lines for the X300.

3000 series

Name - editable field for entering the name of the guard line in place of the default name.

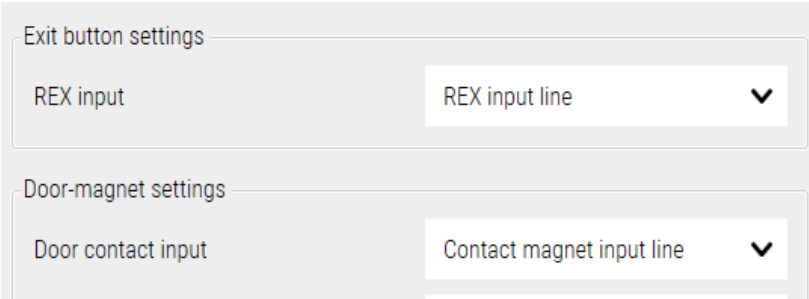
Type - NO or NC type can be selected from the drop-down list - NC is recommended.

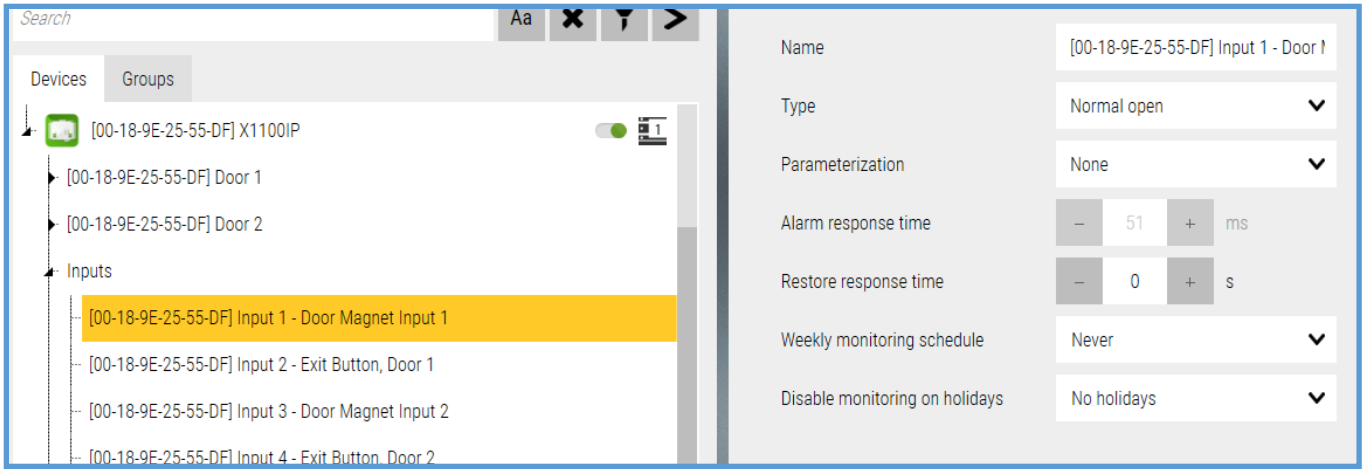
Weekly monitoring shedule - from the drop-down list, you can select a predefined schedule according to which the line will be monitored and then alarms will be generated.

Disable monitoring on holidays - applies to holidays, overrides the weekly weekly schedule, and changes its operation if there is a holiday during the week when the line should have a different monitoring schedule.

Analogous are the settings for the supervision lines on the expansion module if it has been installed

Settings for input lines intended for door status sensors and exit buttons are available in the *Door* configuration window.





HID® series

HID® series

Name - editable field for entering the name of the guard line in place of the default name.

Type - NO or NC type can be selected from the drop-down list - NC is recommended.

Parameterization - None/2xEOL - Parameterization of the input line with two resistors with a value of 1K, in the case of choosing the parameterization of the supervisory line, we can get 4 different states of the line:

normal state/alarm/tamper/fault

Alarm responce time - setting the input line response delay in the range of 0-255(ms)

Restore responce time - setting the input line repeat response delay in the range 0-15 (s)

Weekly monitoring shedule - from the drop-down list, you can select a predefined schedule according to which the line will be monitored and then alarms will be shown.

Disable monitoring on holidays - applies to holidays, overrides the weekly weekly schedule, and changes its operation if there is a holiday during the week when the line should have a different monitoring schedule.

Analogous are the settings for supervision lines on expansion modules if implemented.

Supervision line states:

Line monitored by schedule

- normal state

Operator monitored line

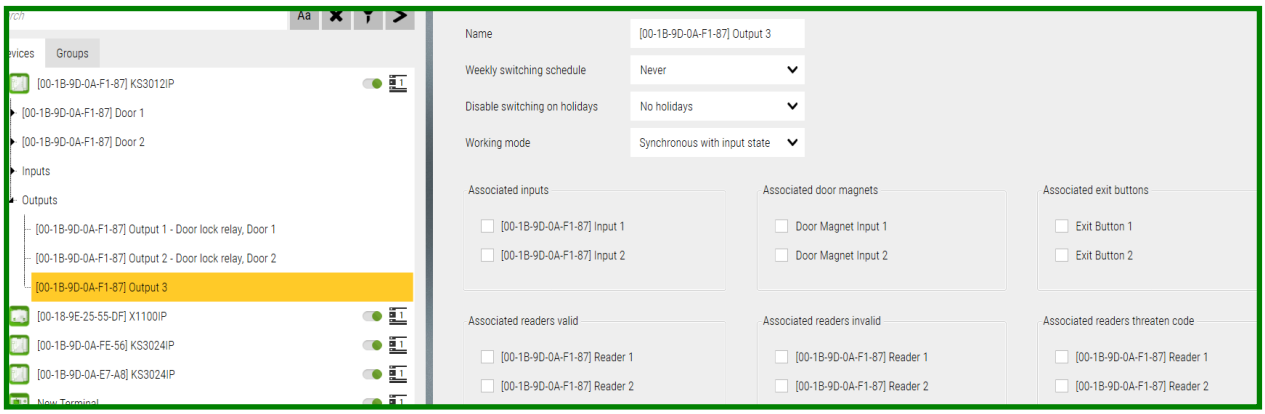
- normal state

Alarm

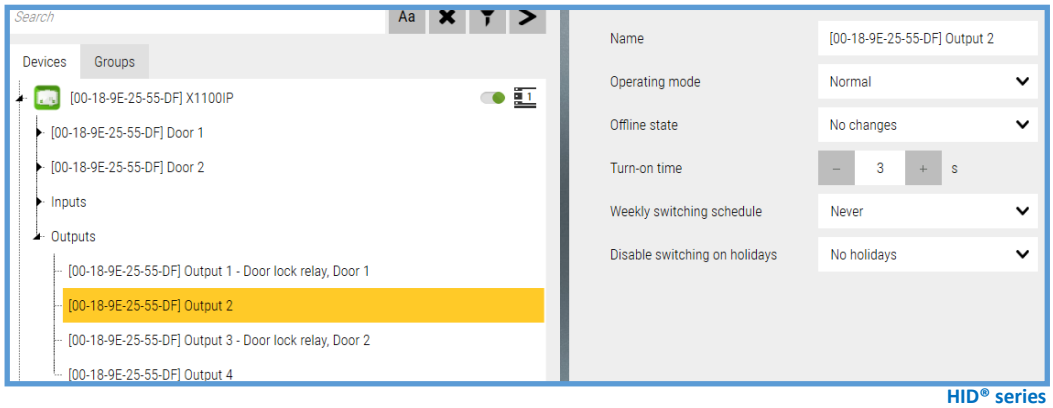
Fault/short circuit

Tamper

3.5 Devices - Access control - Controller - Outputs.



3000 series



HID® series

Control outputs located on the controller allow connection and control of various types of devices. In terms of functionality and settings, they are divided into two groups:

- Outputs assigned to the door and controlling the electric lock
- General control outputs

HID® series - In HID® Aero® X1100 controllers and X100 modules, additional control outputs (relays) are synchronized with electric lock control outputs and can be used, for example, to connect LED control on readers. Recommended when an LED control pulse is needed while driving the passage from the exit button, pressing the exit button does not trigger the GREEN LED outputs on the controllers!

The outputs that control the electric lock in the settings only have a name change and you can't put their icon on the panel because their status is shown by the padlock in the door icon.

Other outputs have settings as in the image above. You can assign to them the status of system elements located on the same controller or selected events. A change in the state of the assigned element or the occurrence of a selected event will then switch the relay.

Depending on the controller model, we have available for **3000 series** controllers - 3 or 5 control outputs and 4 on the KDH-MOD2000INOUT expansion module. For **HID® Aero® series** controllers - 4 control outputs for X1100 and X100, 2 control outputs for X200 module and 12 control outputs for X300 module.

Name - editable field for entering the name of the control output in place of the default name.

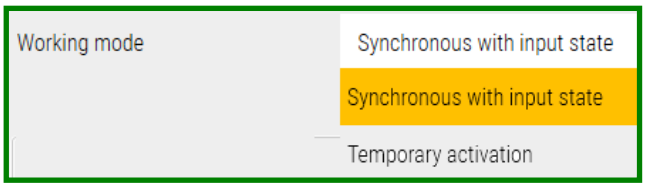
Weekly switching shedule - From the drop-down list, you can select a predefined schedule according to which the output will be automatically switched.

Disable switching on holidays - applies to holidays, overrides the weekly weekly schedule and changes its operation if there is a holiday during the week when the control output should have a different switch-on schedule.

Analogous are the settings for control outputs on the expansion module, if implemented.

Working mode - Tylko dla kontrolerów **serii 3000**, z rozwijanej listy można wybrać tryb działania:

Synchronous with input state - switches when the assigned input line enters or exits the alarm state



3000 series

To choose from:

- States of the three elements: inputs lines, door contact and REX button
- associated whith valid, invalid and readers threaten code

The synchronization assignment becomes active when the checkbox is checked.

Temportary activation - switches to the time set in the field below from 0 to 255 (s)

3000 series

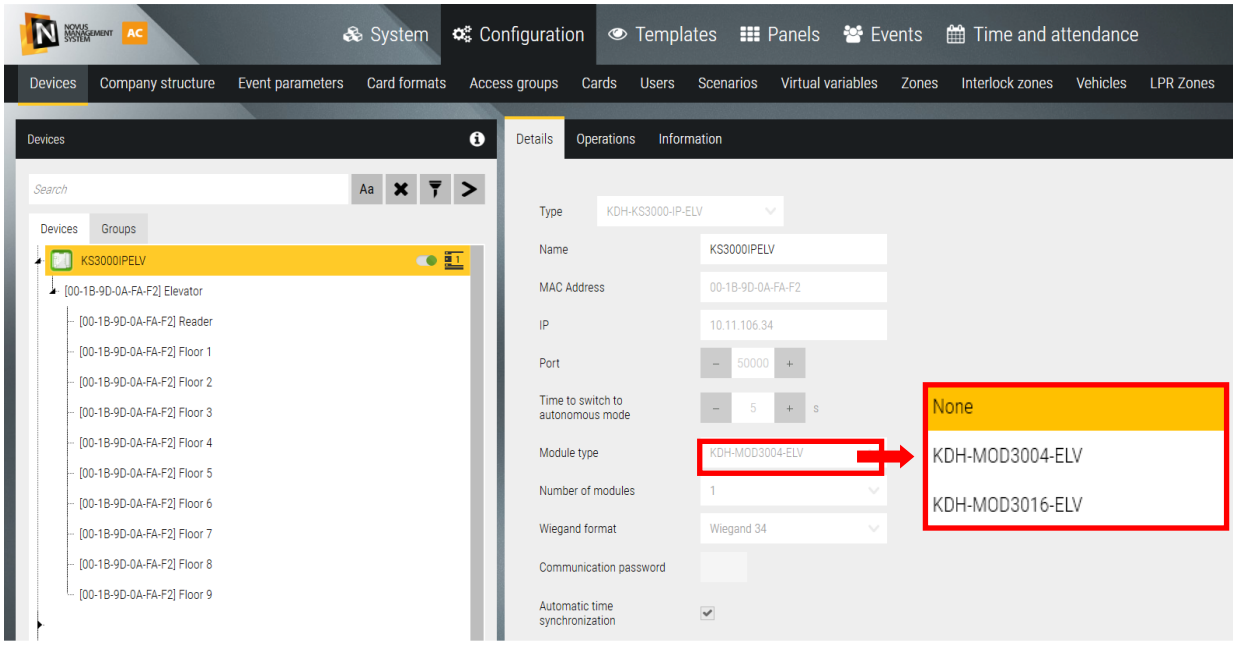
Offline state - For **HID® series** controllers only, status after the controller goes offline, selectable:

- No change
- Inactive
- Active

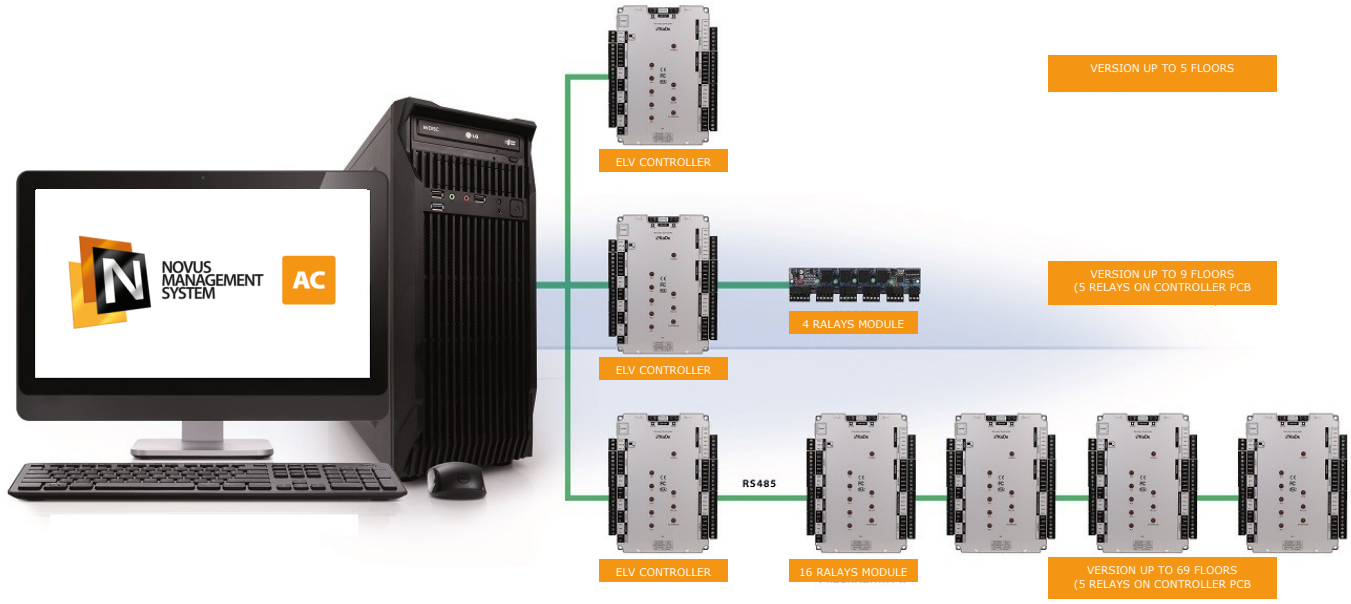
Turn-on time - switches to the time set in the field below

HID® series

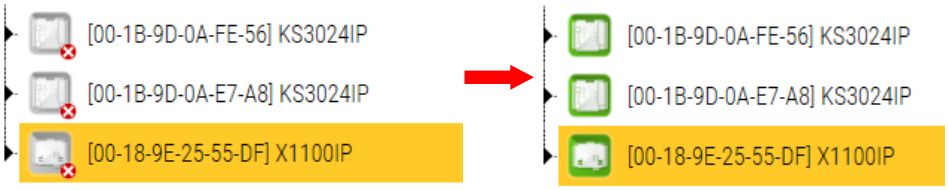
3.6 Devices - Access control - Elevator controller



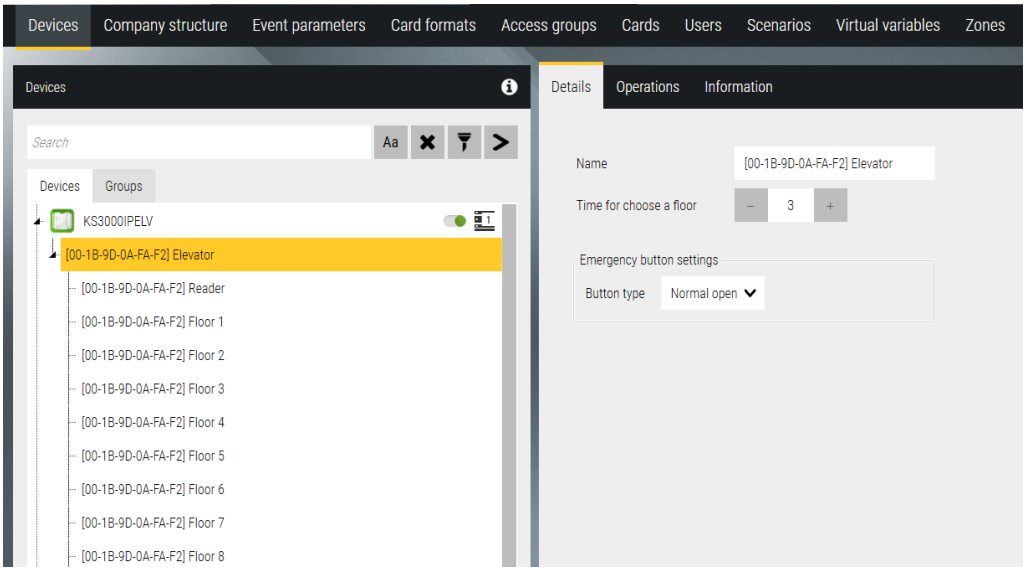
With the KDH-KS3000-IP-ELV controller, you can also add expansion modules. There are two types of modules to choose from. Depending on the number of floors to be served by the elevator, we have the following combinations.



After making all settings for each controller (similar to adding controllers off-line), click on the floppy disk icon in the lower right corner of the Configuration window to write to the database. During this process, a series of messages will appear in the system log window indicating that the enrollment has been successfully completed. The controllers' icons will change to green which shows proper communication:



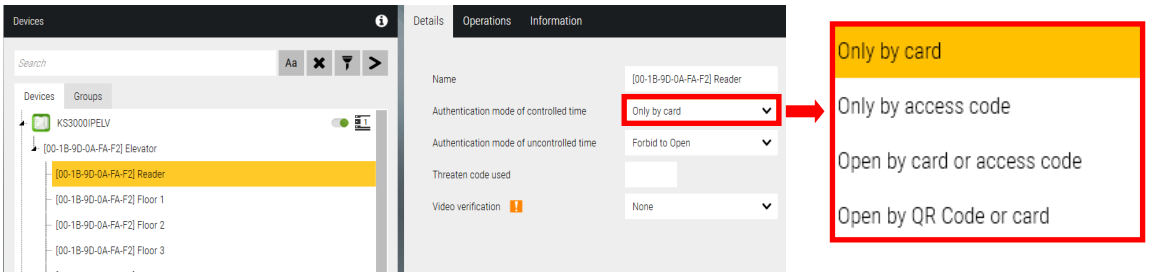
3.7 Devices - Access control - Elevator controller - Elevator



Nazwa - edytowalne pole na wpisanie nazwy windy w miejsce nazwy domyślnej.
Czas na wybór piętra - edytowalne pole na wpisanie lub ustawienie czasu na wybór piętra po odczycie ważnej karty
Ustawienia przycisku awaryjnego - służy do odblokowania wszystkich pięter na stałe, dlatego powinien być dwustanowy. Zalecany model KDH-EXIT1030-P - z wciskaną plastikową płytką (jak do awaryjnego odryglowania drzwi).

- Typ przycisku - do wyboru NO/NC

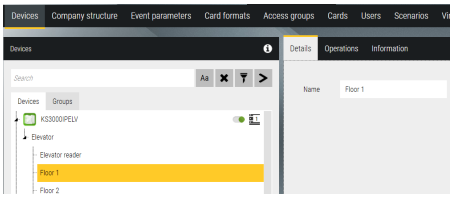
3.8 Devices - Access control - Elevator controller - Elevator—Reader



Name - editable field for entering the name of the reader in place of the default name
Authentication mode of controlled time - You can select one of the modes from the drop-down list
Authentication mode of uncontrolled time - You can select one of the modes from the drop-down list
(this mode applies to the period outside working hours, weekends and holidays)
Threaten code used - field for entering the access code to be used on the reader keypad in case of forced entry. It causes a discrete alarm to be generated at the operator's station.
Video verification - allows you to assign a camera installed over the reader to record a freeze frame when the card is read

3.9 Equipment - Access control - Elevator controller - Elevator - Floors

Name - editable field for entering the name of the reader in place of the default name

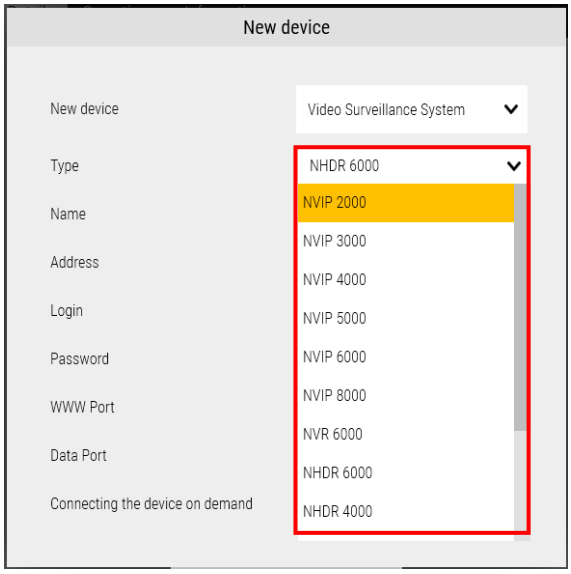


3.10 Devices - Video Surveillance System

NOVUS MANAGEMENT SYSTEM AC also integrates the video surveillance system. At this stage, this functionality is limited to:

- live image preview,
- playback and download of recordings
- defining advanced video views
- support for up to 6 monitors in 4k resolution
- dual-streaming support
- displaying live image from the selected camera after clicking on the icon located on the panel
- automatic display of such an image after a specific event occurs (e.g. forcing the door, card reading) as a result of the scenario execution
- assigning a camera to a reader - video verification
- PTZ camera control
- support for fisheye cameras
- receiving alarm events/image analysis
- control of alarm outputs
- On-demand connection of surveillance devices
- Support for single-stream surveillance devices

List of VSS devices that can be connected with NOVUS MANAGEMENT SYSTEM AC software:



The main items on the list are NOVUS devices (recorder and IP camera series), but integration with devices using RTSP and ONVIF protocols is also possible.

CCTV devices can be added manually using the *New device* - *Video surveillance system* option, the window as on the next page will be displayed. You can also use the automatic search engine that finds controllers and cameras, sorts them and allows you to assign the right addresses.

Type - first select the type of video device as on the list as above.

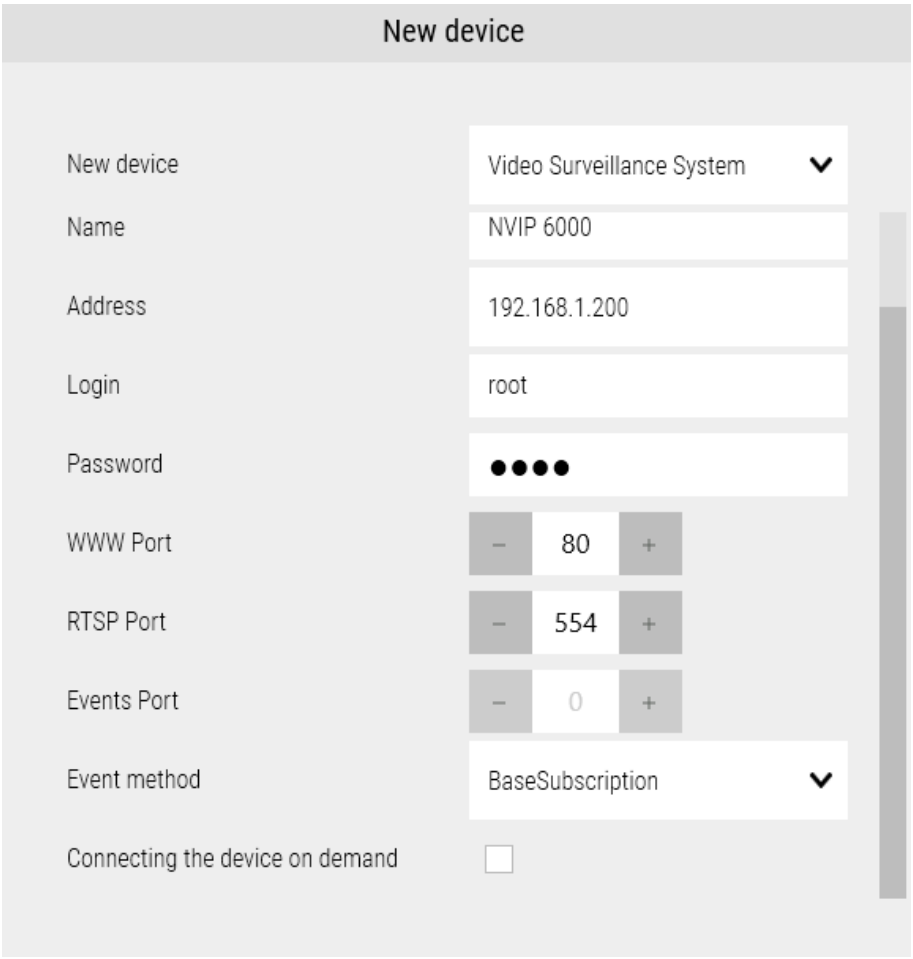
Name - editable field to type the name of the video device in place of the default name if you want. This field will be filled automatically when camera is connected.

IP Address - field for entering IP address that matches the settings of the camera

WWW Port - field for entering the port number that matches the settings of the camera

RTSP Port - field for entering the port number that matches the settings of the video device

Data Port - field to type the port number that matches the settings on the video device



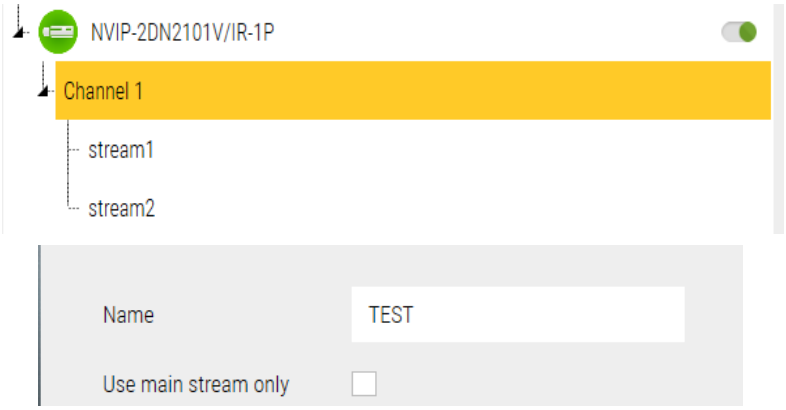
User - editable field to type a user name that matches the settings of the video device.

Password - editable field for typing a user password that matches the settings of the video device.

Connecting the device on demand – an option that allows the system to automatically establish a connection with a device when its video stream is displayed. If this option is disabled, the user must manually initiate the connection with the device.

After setting the required parameters click on the ***OK*** button, and when returning to the *Device* window save by clicking on the floppy disk icon in the lower right corner of the configuration window. A series of messages informing you that the settings have been saved to the database will appear in the System Log window. Then, when connected to the device, the icon turns green.

For panel operations, we use the Channel X position, which is displayed in the tree when expanded.



3.11 Devices - Time and Attendance terminal

ATTENTION!

Changes in software version 5.00.071 and newer. As of NOVUS MANAGEMENT SYSTEM AC software version 5.00.071, the method of communication with T&A terminals has been modified compared to version 5.00.035. The configuration method from version 5.00.071 is as follows:

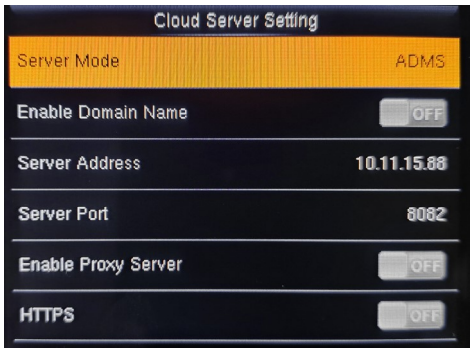
Time and Attendance terminal configuration

After entering the menu described on the next page, go to the tab *Communication - > Cloud server settings*.

Server Address - Set the IP address of the computer on which the NOVUS MANAGEMENT SYSTEM AC software server will run (this must be the address selected in the software configuration under Listening IP address).

Server Port - Set the port number according to the port number set for the terminal on the NOVUS MANAGEMENT SYSTEM AC server. Make sure that the port number is not used by another device, software, etc.

HTTPS - should be set to *OFF*.



Configure date/time settings.

Enter the *System - > Date Time - > Dailing Saving Mode* - mode menu and select *By date/time.* Then go to the menu *System - > Date Time - > Dailing Saving Setup* - configure and define the date and time of the start and end of the time change. By default, it is the last Sunday of October at 3:00 and the last Sunday of March at 2:00.

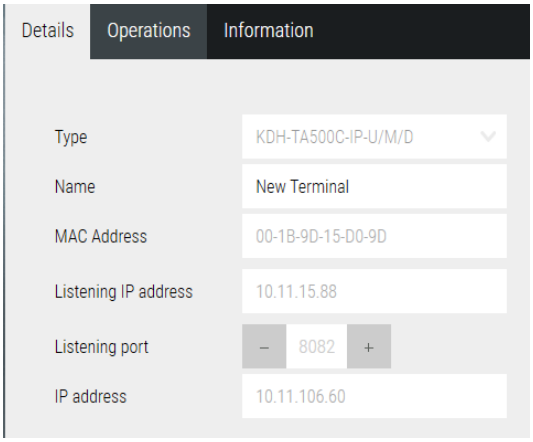
Terminal IP address settings

From version 5.00.071 and later, the use of DHCP mode is not recommended!

Configuration of NOVUS MANAGEMENT SYSTEM AC software.

Listening IP address - after selecting the ⚙ option, select from the list the IP address of the computer that will be used for communication with the time registration terminal (it must be the same address that was defined in the terminal under *Cloud Server Settings - >Server Address*).

Listening port - enter the port number that will be used for communication with the time registration terminal (this must be the same port number defined in the terminal under *Cloud Server Settings - >Server Address*).

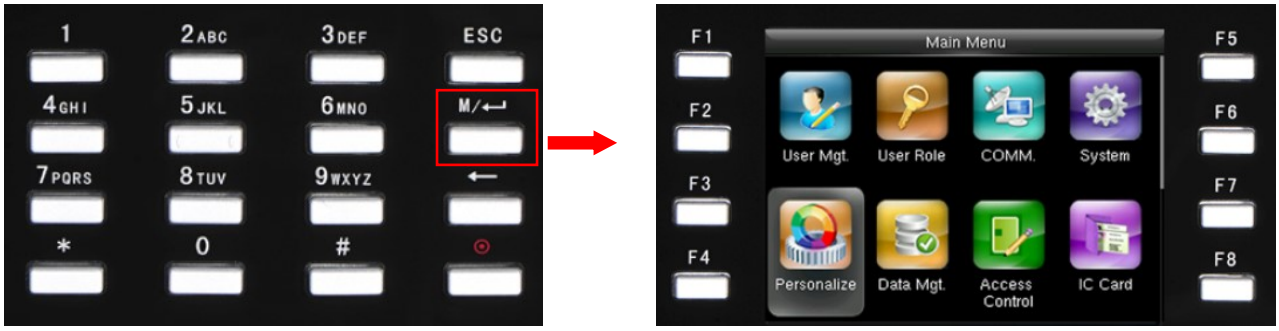


If you are upgrading from version **5.00.035** to version **5.00.071,** after completing the configuration process, perform an initialization operation on the terminal (in the Configuration - > Devices , select the terminal from the list and then the **Initialization** option from the Operations menu). Keep in mind that this will delete all events stored in the terminal's memory.

For other information on the configuration of time registration terminals, see the following section.

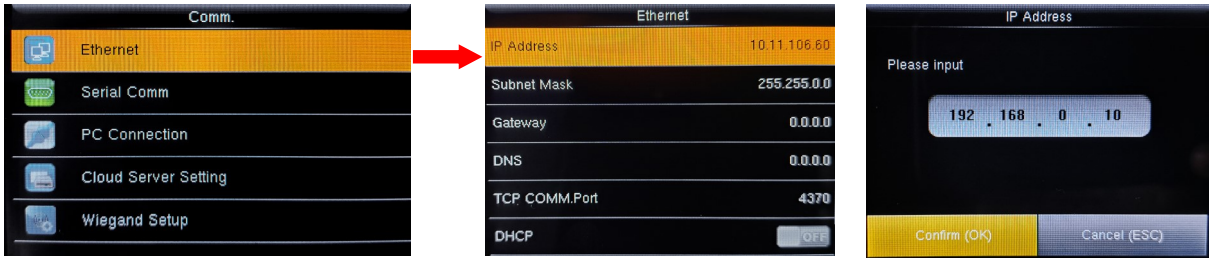
NOVUS MANAGEMENT SYSTEM AC program allows integration with time and attendance registration system. From version 4.02.XX and higher, these functions can be realized in cooperation with T&A terminals of KDH-TA500C-IP-UMD and KDH-TA500CFP-IP-UMD types, which offer registration of different types of I/O (normal, private , business and break (paid license, trial 60 days).

Before connecting the program to the terminal, the IP address, language and date format must be set in its menu. Enter the menu via the M key on the keyboard. No password is required at this stage.



Setting the IP address

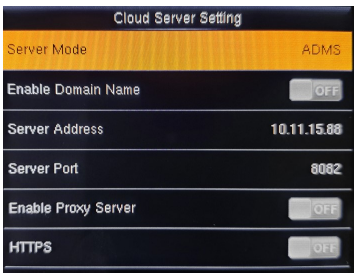
Selection of items with cursors. (upper right corner of the terminal)



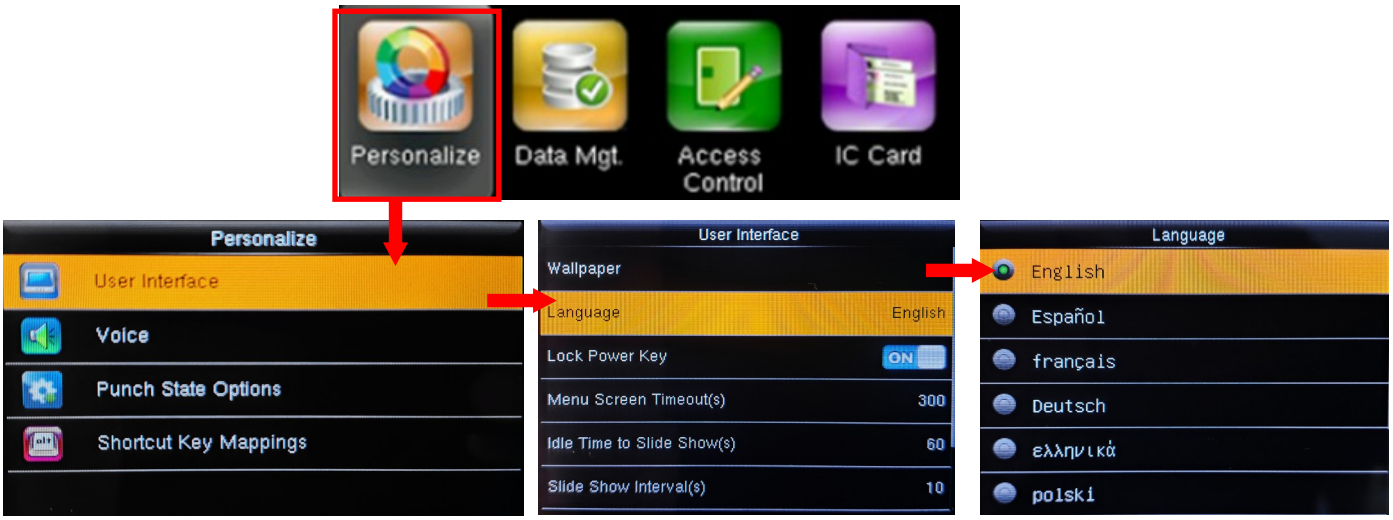
After clicking on the *Comm* icon, select *the Ethernet* item and click OK in the cursor field - upper right corner of the terminal. Fill in the first 4 fields - After selecting the field, click OK and enter the address-port values without changes. If you are using DHCP network, just select the last item at the bottom of the window and click OK **(Note! For version 5.00.071 and higher, using DHCP mode is not recommended)**. After restarting the terminal's power supply, re-enter this window and read the assigned address to enter it in the NOVUS MANAGEMENT SYSTEM AC configuration window.

Then go to the *Cloud Server Settings* item and, in the same way, set the address of the NOVUS MANAGEMENT SYSTEM AC server with which the terminal will connect. Only this item is needed for cooperation with NOVUS MANAGEMENT SYSTEM AC.

Use the ESC button on the keyboard to exit the menu

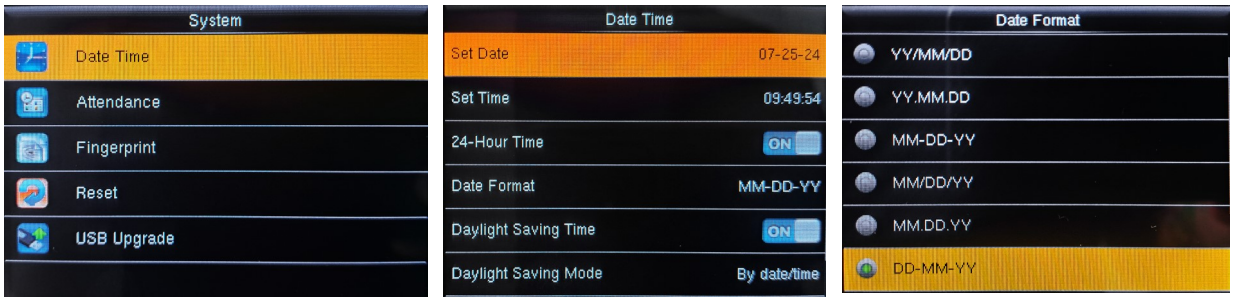


Choice of language



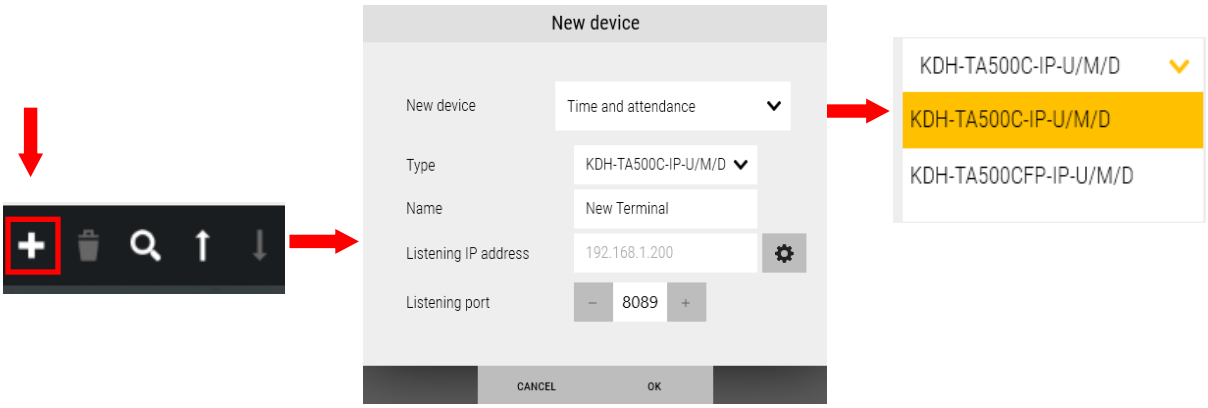
After clicking on the Personalization icon, select the User Interface item and in the next window Language.
Set the Polish language and exit the menu with the ESC button.

Data format



After clicking on the System icon, select Item Date Time and in the next window Date Format.
Set the format DD-MM-YYYYY and exit the menu with the ESC button.

Terminal configuration in the program



The terminal should be added manually using the New Device - Time and attendance option, a window as above will be displayed.

Type - First, select the type of device from the drop-down list as above. To choose:

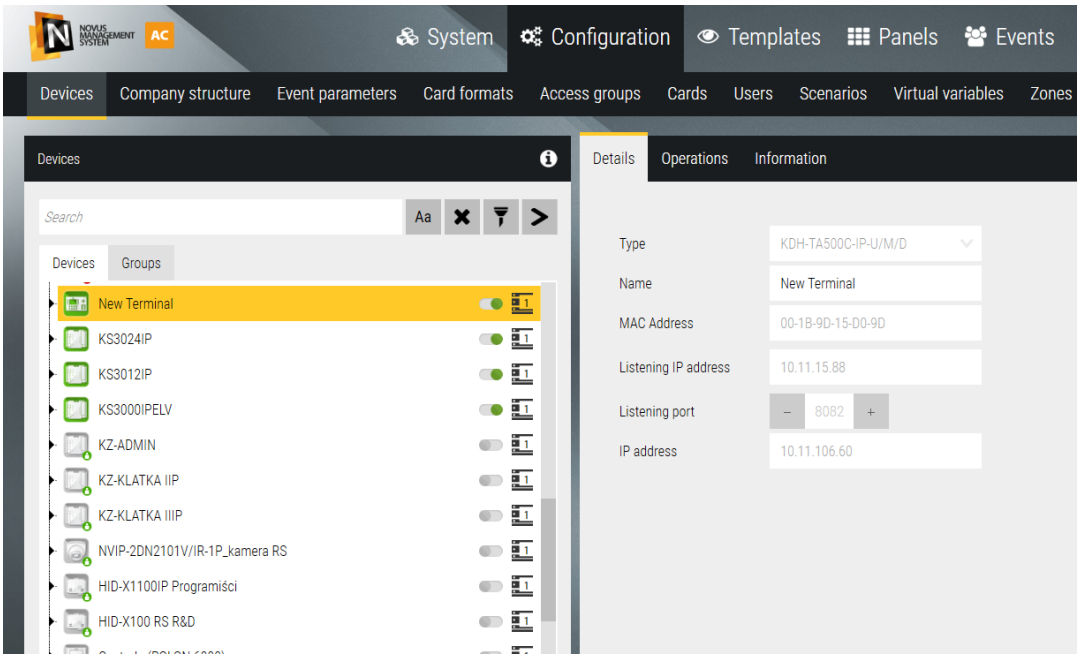
Model: **KDH-TA500C-IP-UMD** or **KDH-TA500CFP-IP-UMD** with biometrics scanner.

Name - editable field for entering the device name in place of the default name if you want to have your own name.

Listening IP address - server address set in the terminal in the *Comm/Cloud Server Setting*

Listening port - the server port number set in the terminal in the *Comm/Cloud Server Setting*

After clicking OK and Save (in the lower right corner of the Configuration window), the terminal will appear in the device list. Confirmation that communication has been established is the green colour of the terminal icon in the left window.

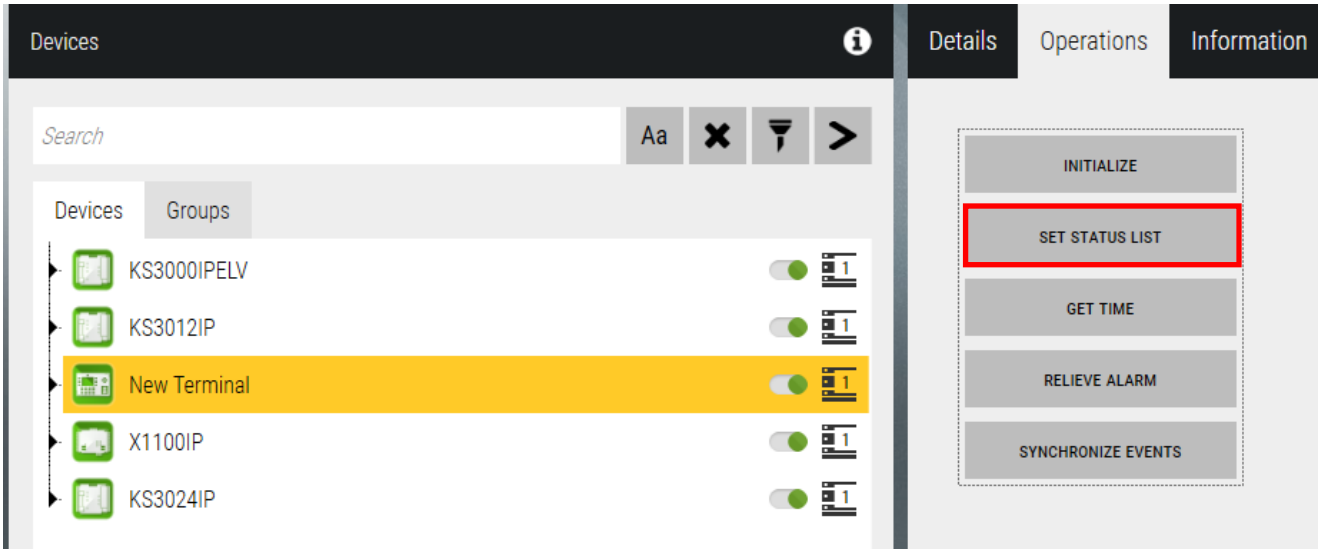


From this point on, entering the terminal menu requires the admin password. Default login: type admin ID - 1 and OK, Verify **password: 1 2 3 4 5 6 7 8** and Ok.

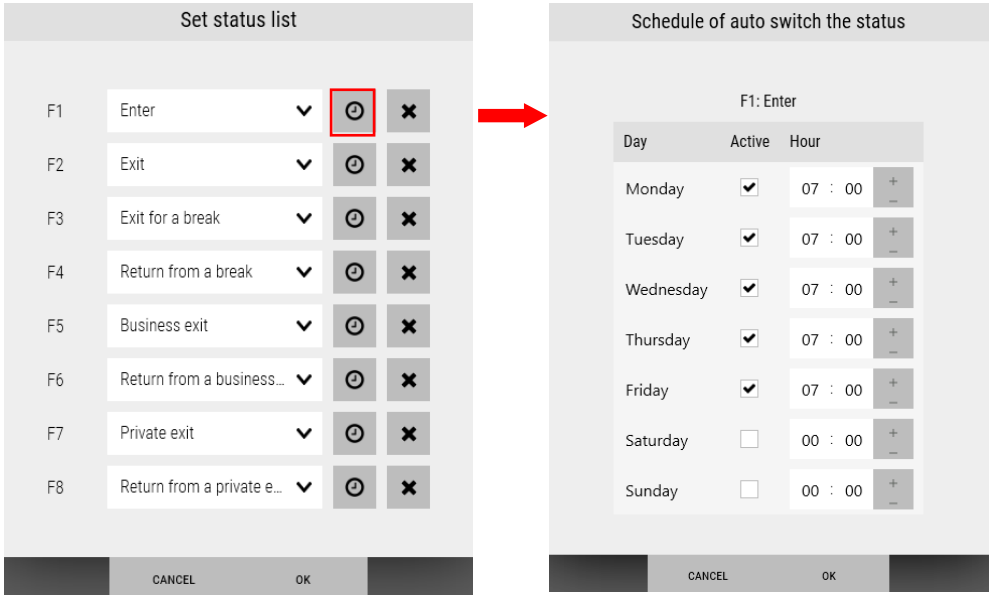
The default password must be changed after logging in the menu Manage user. By editing the Admin user.

Adding fingerprints to FP terminal via USB scanner is described in *Users* tab.

Set enter/exit registration statuses



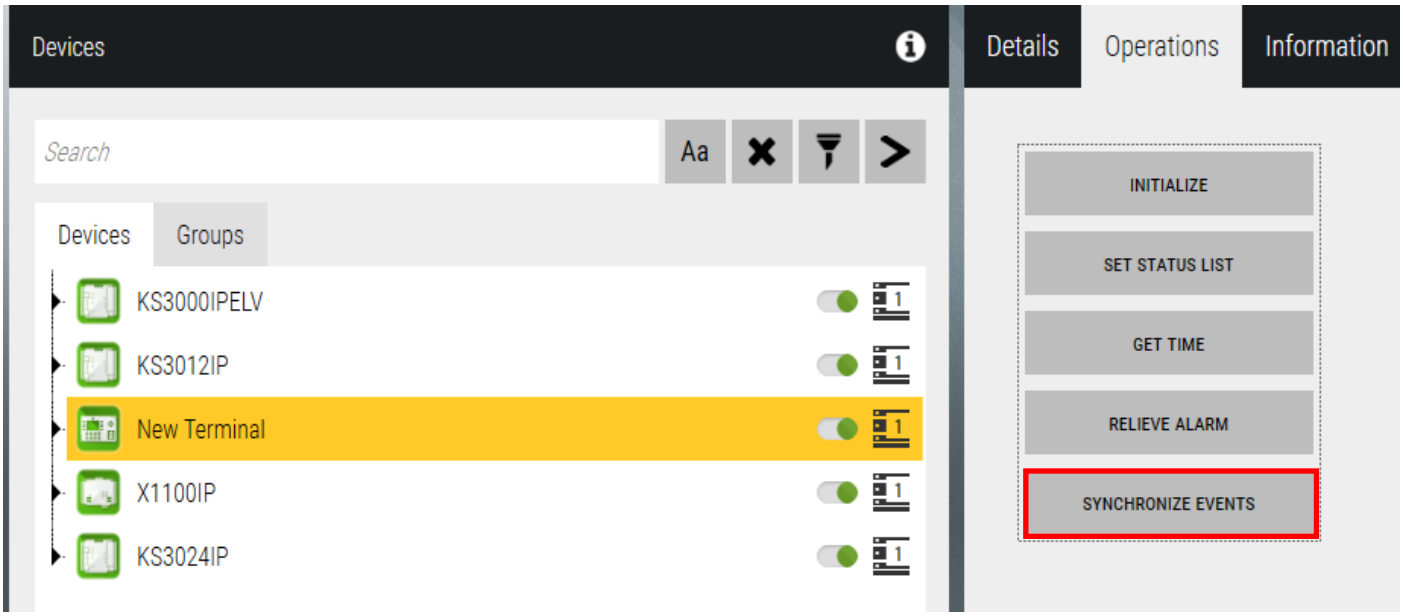
On the Operations tab, click on the Set Status List button. You can leave the default settings or set your own order by selecting a status from the drop-down list next to each button.
By clicking on the clock icon next to each button, you can set a schedule to automatically switch registration status for selected days of the week. When the user changes the status to another, the default status returns after 5 sec.

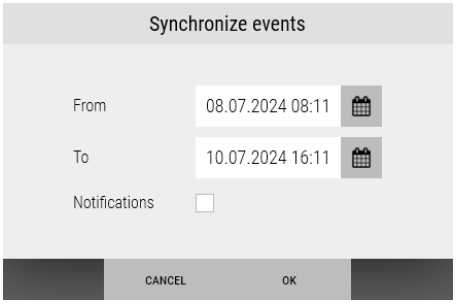


After completing the settings, confirm OK, and then click the Save button in the lower right corner of the configuration window. This will upload the correct registration status descriptions. This process can take up to several minutes. During this process, a description will appear on the terminal display in the button description fields: F1-Processing. Only after the whole process is completed will all the real status descriptions appear. The descriptions are displayed in the language of the logged-in operator.
The Operations tab also provides other options according to the descriptions on the buttons.
The Disable Alarm button is used to clear the alarm generated when the terminal's tamper sensor is violated. Alarm cancellation is also possible from the terminal icon on the panel.

Synchronization with the terminal

This option allows you to download logs from the T&A terminal in case, for various reasons, I/O registrations have been made by employees, but they are not in the program database, which manifests itself in the absence of these events in the T&A report.

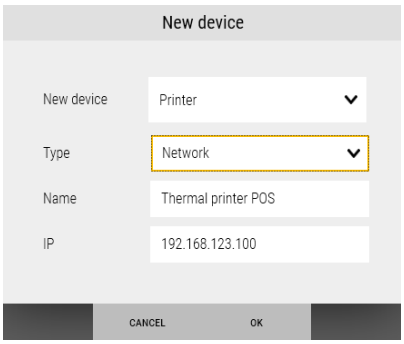




After clicking on the Synchronize Events button, the following window will be displayed:
Choose the date and time range from which you want to download events. Optionally, you can enable email notifications, but if there are a lot of undownloaded events, it is better not to use it in order not to fill up the employees' email inboxes. It is worth enabling it if the situation concerns the current day and there are no notifications in the morning. After clicking OK on the event stack panel, you will see information about the number of downloaded events and downloaded events. During this operation, only events that are missing from the database in the specified time period are downloaded from the terminal.

3.12 Devices - Ticket printer

NOVUS MANAGEMENT SYSTEM AC program allows you to add a printer dedicated to printing tickets with QR-codes for the LPR option. To add a printer, select its type (network or local) and then enter its IP address or select the appropriate COM port and click *Save.*

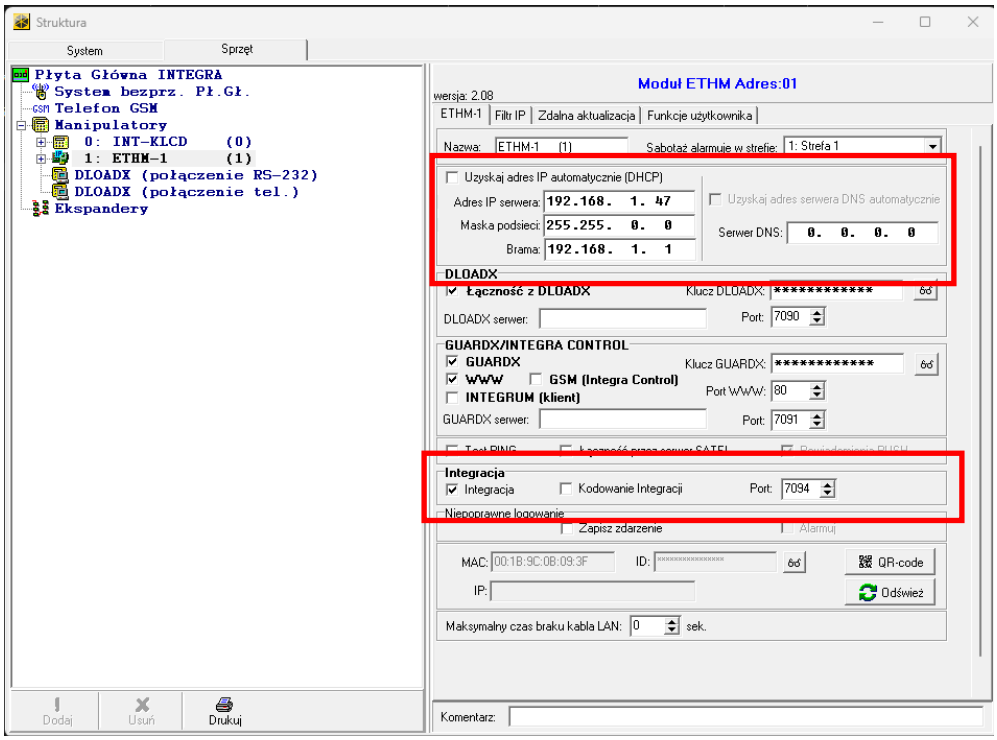


3.13 Devices — Intrusion and Hold-Up alarm system (I&HAS)

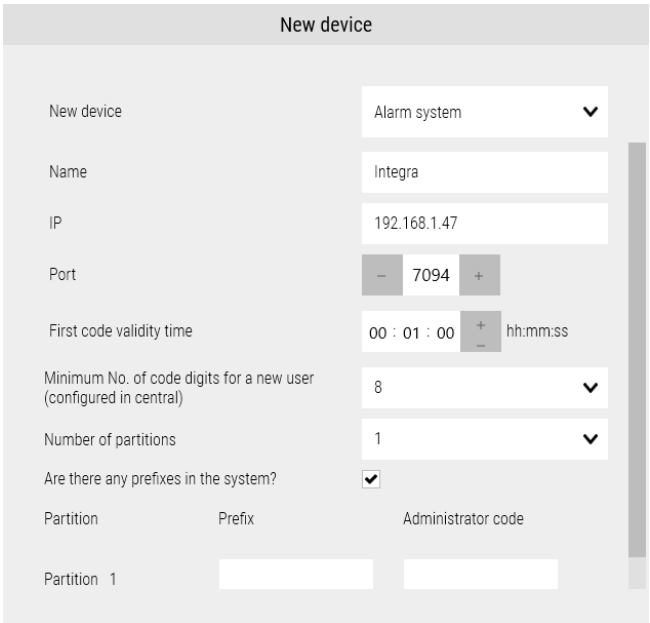
NOVUS MANAGEMENT SYSTEM AC program in version 5 or higher, enables in addition to access control, video surveillance and time attendance systems integration with intrusion and hold-up alarm system.

Satel's Integra series alarm control panels can be integrated with the NOVUS MANAGEMENT SYSTEM AC program via ETHM-1-PLUS communication module. In order for devices to establish proper communication, control panel must be in minimum version 1.19 and the ETHM-1-PLUS module must be in minimum version 2.07.

To establish communication with the NOVUS MANAGEMENT SYSTEM AC program, in the ETHM-1-PLUS module settings, address the module in the same network segment as the NOVUS MANAGEMENT SYSTEM AC server. Enable INTEGRATION option and set the integration port in accordance with manual of ETHM-1-PLUS.
Below is an example of DLOADX configuration program.



Intrusion and Hold-Up alarm system devices can be added manually using the New device—Alarm system option. The following window is displayed in the NOVUS MANAGEMENT SYSTEM AC program.



Name — text box for entering the name of the control panel in place of the default name.

IP — text box for setting the IP address of the control panel in accordance with the ETHM-1-PLUS configuration.

Port — text box for setting integration port number in accordance with the ETHM-1-PLUS configuration.

First code validity time — time where the first password will be valid after entering it by NMS ADVANCED CONTROL. Entering the second code on the keypad during this time will change the state of the properly configured partition.

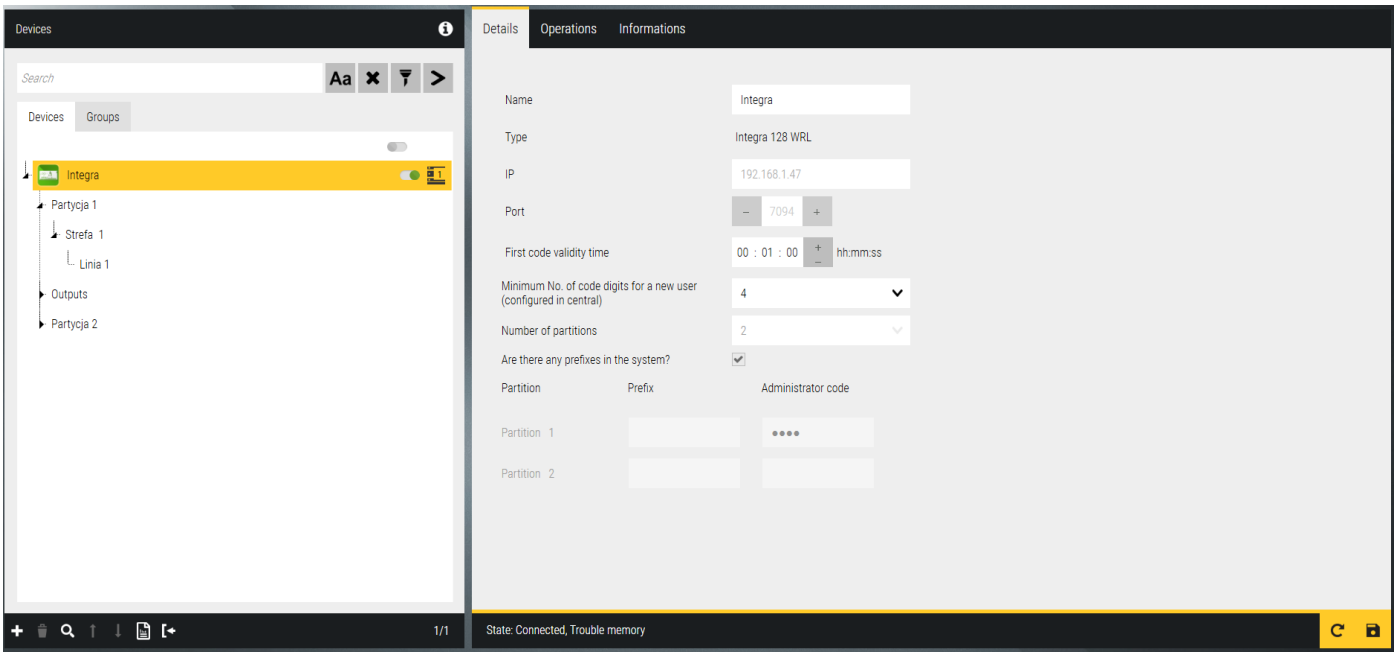
Minimum code length for a new user— minimum number of user code digits programmed in the panel.

Number of partitions—the number of partitions to be selected for addition to NOVUS MANAGEMENT SYSTEM AC. For each partition, specify the prefix (if any) and the partition administrator code.

Are there any prefixes in the system? — selecting the field allows you to enter a prefix for each partition if in the control panel, the installer specified the length of prefixes then they were defined by the partition administrator.

Below the listed options, enter the administrator code and prefix (if any) for each of the programmed partitions.

After setting the required parameters, click the OK button. Returning to the *Devices* window, save settings by clicking on the floppy disk in the lower right corner of the Configuration window. A couple logs will appear in the system log window informing about the saving new device to the database, panel icon will turn green and the NMS ADVANCED CONTROL. Program will start downloading the configuration of the control panel. During this operation, alarm system configuration will be downloaded including partitions ,zones and users access codes.

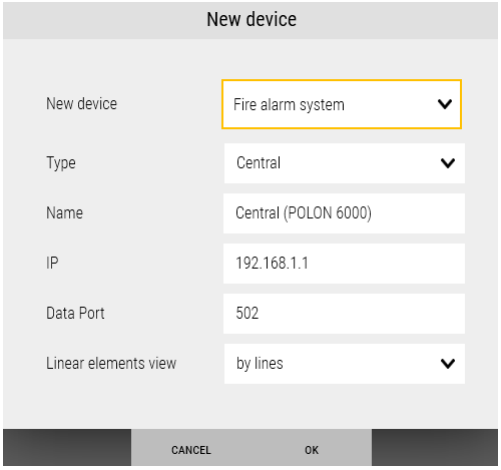


3.14 Devices - POLON 6000 Fire alarm system

The NOVUS MANAGEMENT SYSTEM AC software enables visualization of the Polon 6000 fire alarm system (software version **1.016 or newer** is required). A detailed description of the scope of functionality is described in chapter 1.2 of this user manual.

Devices of the Polon 6000 fire alarm system should be added manually using the *New Device - Fire alarm system*, the window as above will be displayed.

Adding the Polon 6000 system



Type - first, select the device type from the drop-down list

Name - an editable field to enter the name of the device instead of the default name, if we want to have our own name

IP - field for entering the IP address of the SSP main panel consistent with the settings in the SSP main panel

Data Port - field for entering the port number consistent with the settings in the SSP main panel

Linear elements view - from the drop-down list, select the method of displaying linear elements from those available *by lines* or *by zones.*

After configuring the above-mentioned elements, click OK.

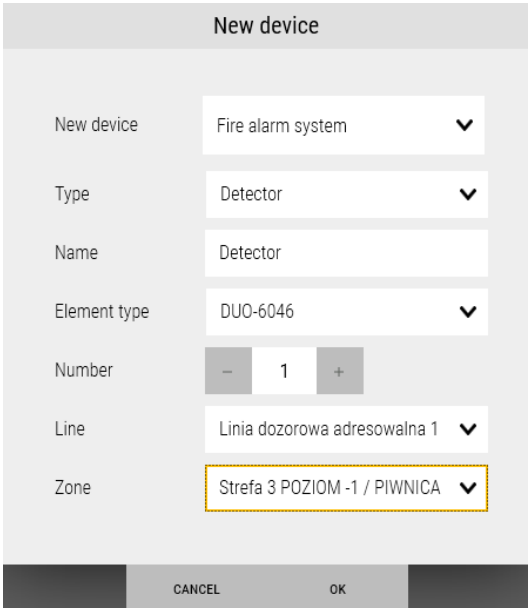
Note: To establish a connection with the Polon 6000 main panel, it must be properly configured. The description of the main panel configuration can be found in chapter 9.10 of this user manual.

Adding elements of the Polon 6000 system

There are two ways to add Polon 6000 system elements:

A) Manually adding system elements

Elements of the Polon 6000 system should be added in the same way as in the case of adding a control panel, except that in the Type item, select the appropriate *Type* of element that you want to add. The method of adding a *detector* type element is shown on the next page.



Type - select the appropriate device type, in this case a *detector*

Name - an editable field to enter the name of the device instead of the default name, if we want to have one

Element type - select the appropriate device type / model

Number - select the number of the element on the line

Line - select the detection line to which the given element should be assigned

Zone - select the zone to which the given element should be assigned

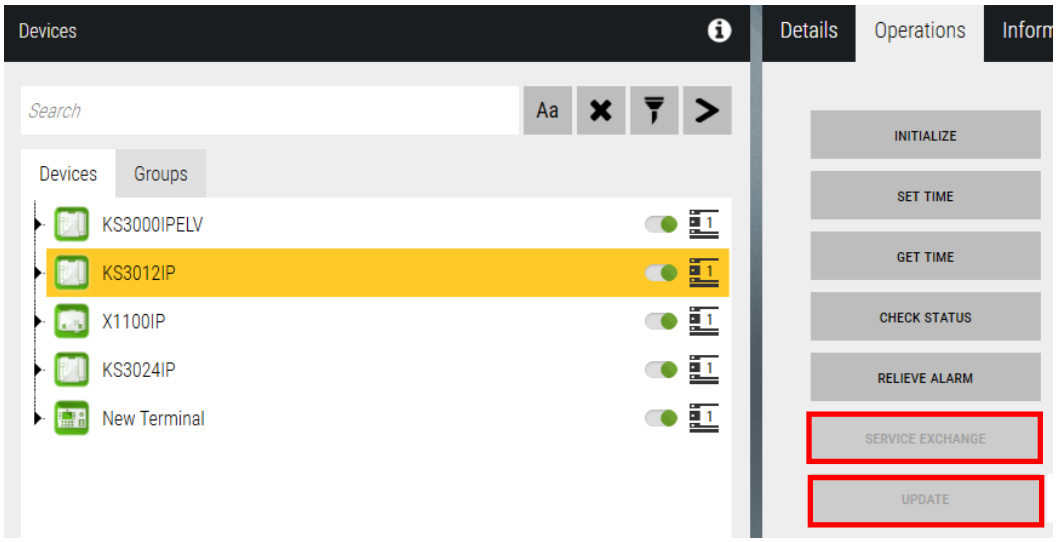
B) Loading the configuration exported from the main panel

The procedure is described in section 9.10 of this user manual.

3.15 Devices - Operations

The system components shown below under the *Operations* tab have commands for the operator to perform certain operations as listed below.

Kontroler

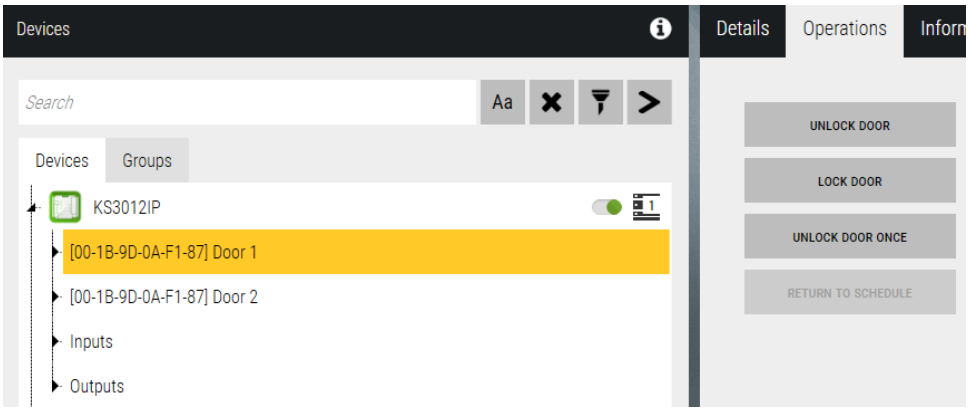


New buttons:

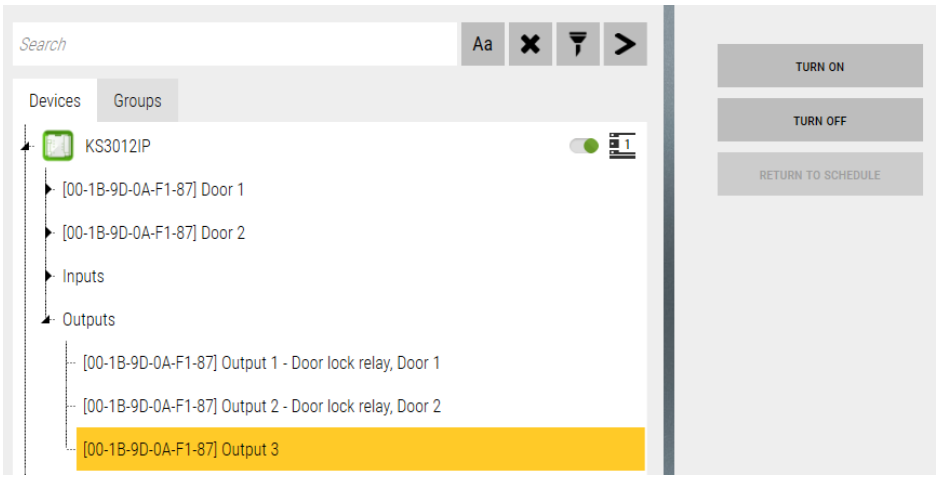
SERVICE EXCHANGE - allows you to replace the controller with a new one, which should be connected with the same IP address

UPDATE - allows you to upload new firmware from the program to the controller, is active when there is no version compatibility.

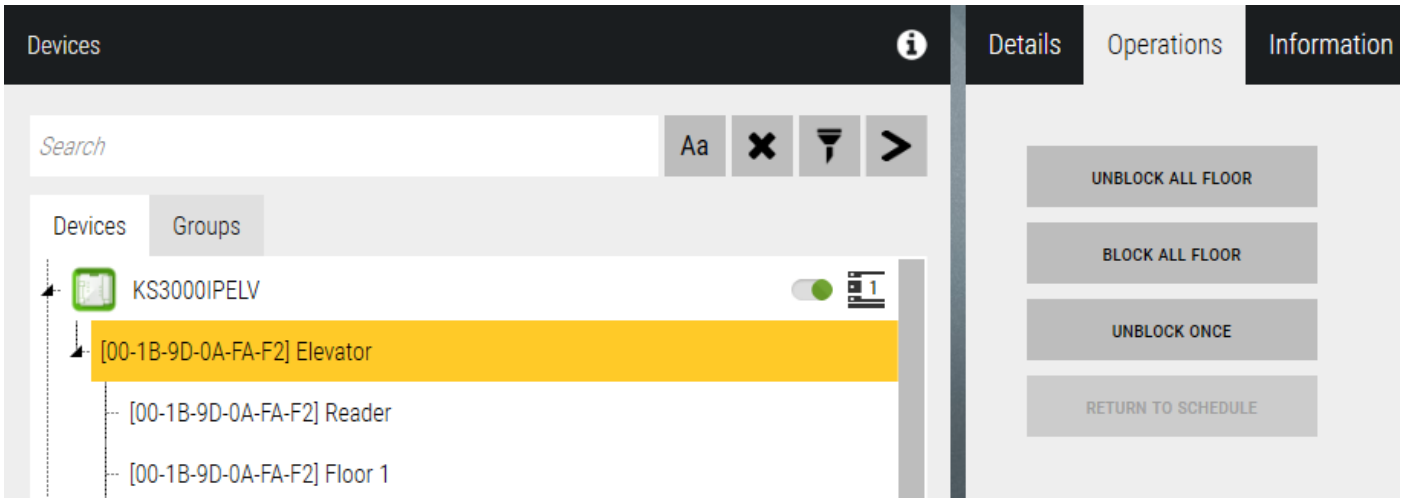
Door



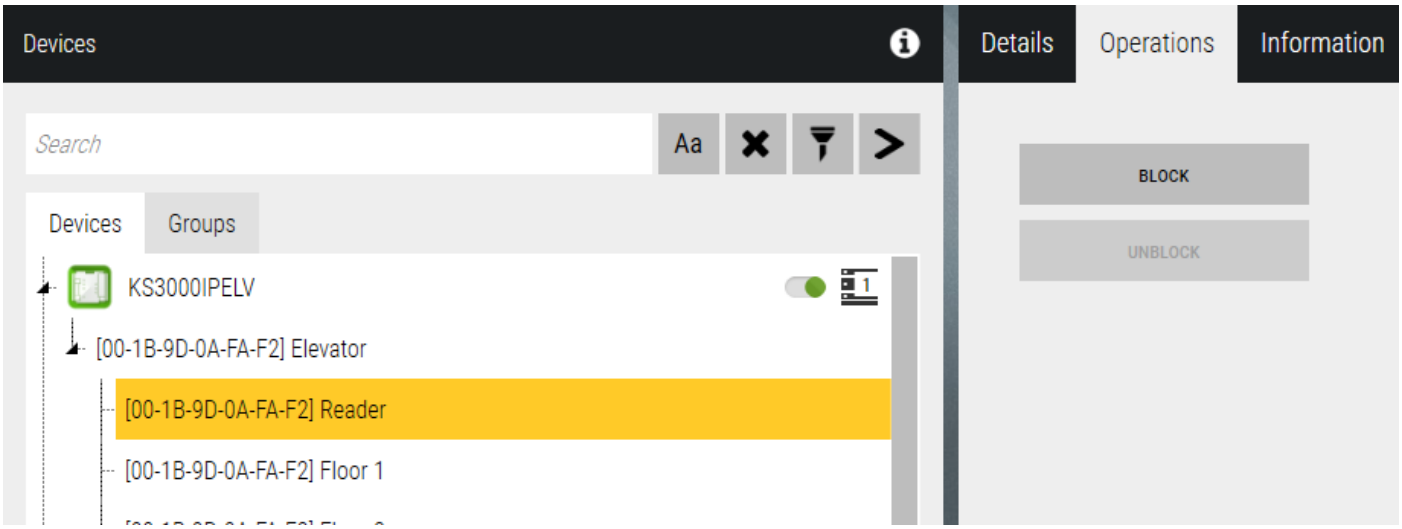
Outputs (only not assigned to the lock)



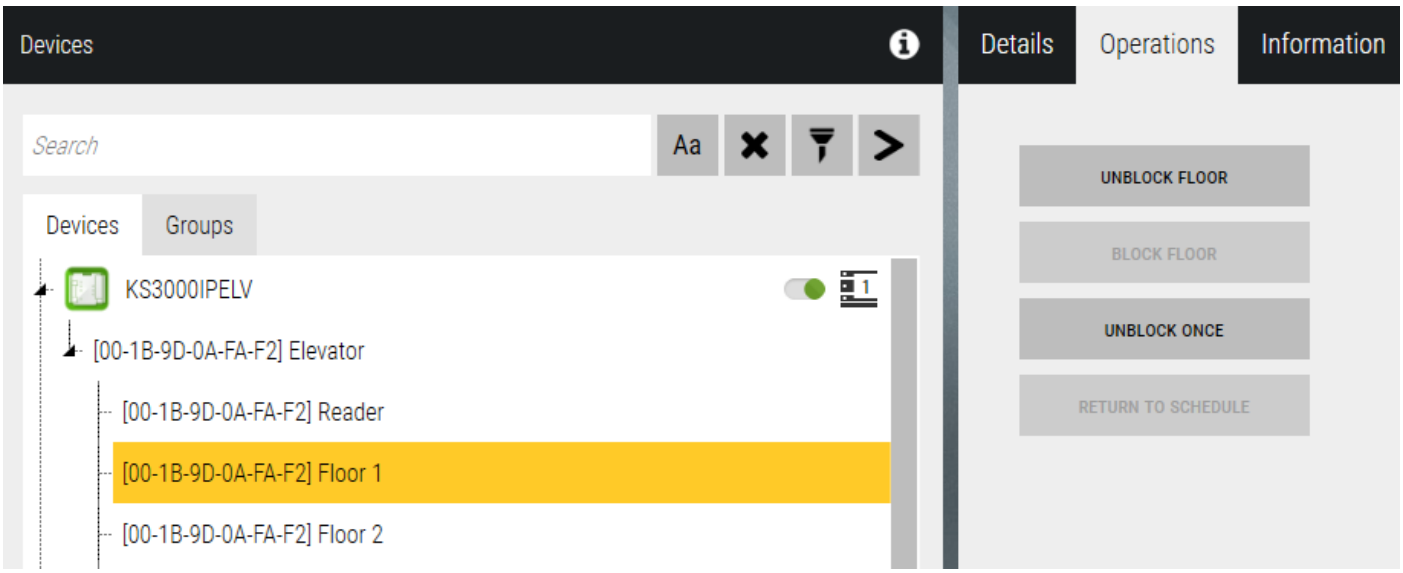
Elevator



Reader

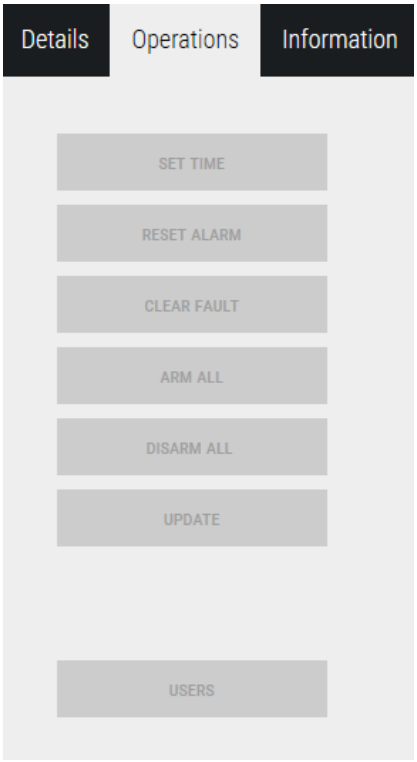


Floor



Devices - Intrusion and Hold-Up alarm system (I&HAS) - Operations

Panel Operations



Set time — setting the date and time in the panel according to the time of the computer which the NOVUS MANAGEMENT SYSTEM AC program is installed on.

Reset alarm — if an alarm occurred on the control panel and it is saved in the alarm memory, this button confirm alarm and remove alarm memory.

Clear fault — if any eliminated troubles are in the panel's trouble memory, this button confirm troubles and remove the trouble memory.

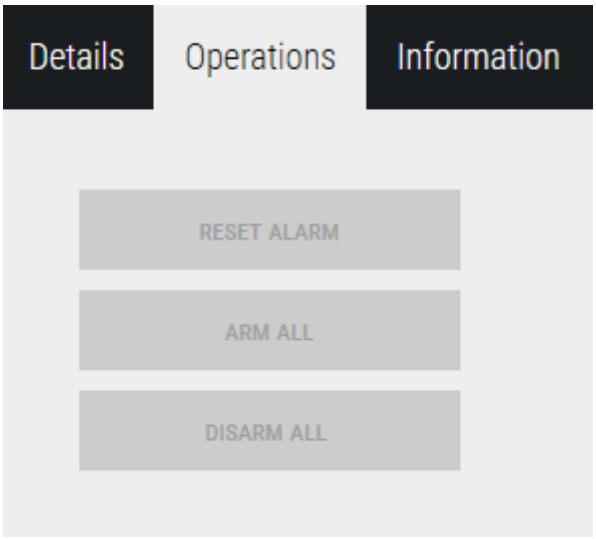
Arm all — button allows you to arm all disarmed objects and partitions in the system with status allow arming.

Disarm all — button allows you to disarms all armed objects and partitions in the system.

Update — downloads the entire panel configuration. During this operation, the program updates the system division into objects and partitions and user access codes.

Users — in this window, you can check all control panel users, both those configurated via NMS AC and keypad/ DLOADX.

Operations on objects

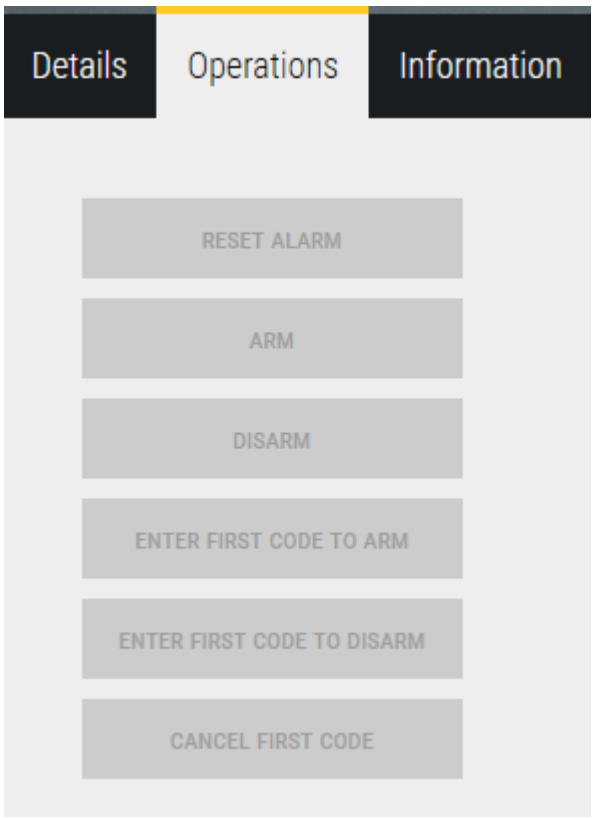


Reset alarm — if an alarm occurred on the object and it is saved in the alarm memory, this button clears the alarm memory.

Arm all — button allows you to arm all disarmed partitions in the object with status allows arming.

Disarm all — button allows you to disarm all armed partitions in the object.

Operations on partitions



Reset alarm — if an alarm occurred in the partition and it is saved in the alarm memory, this button confirm alarm and remove alarm memory.

Arm — button allows you to arm the selected partition if its status allows arming.

Disarm — button allows you to disarm the selected partition if its status allow disarming.

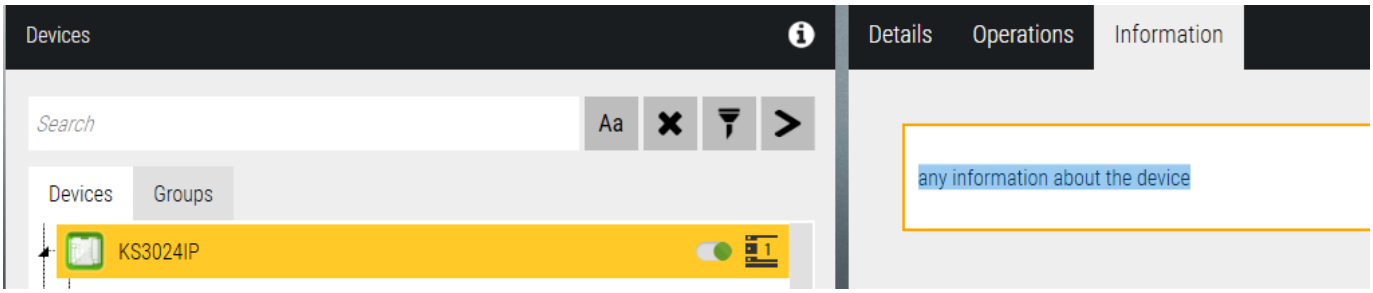
Enter first code to arm — button enters the first code to arm for a properly configured partition. The validity time of the first code is set when adding the control panel to NMS ADVANCED CONTROL.

Enter first code to disarm — button enters the first code to disarm for a properly configured partition. The validity time of the first code is set when adding the control panel to NMS ADVANCED CONTROL.

Cancel first code — button cancels entering the first access code.

3.16 Devices - Information

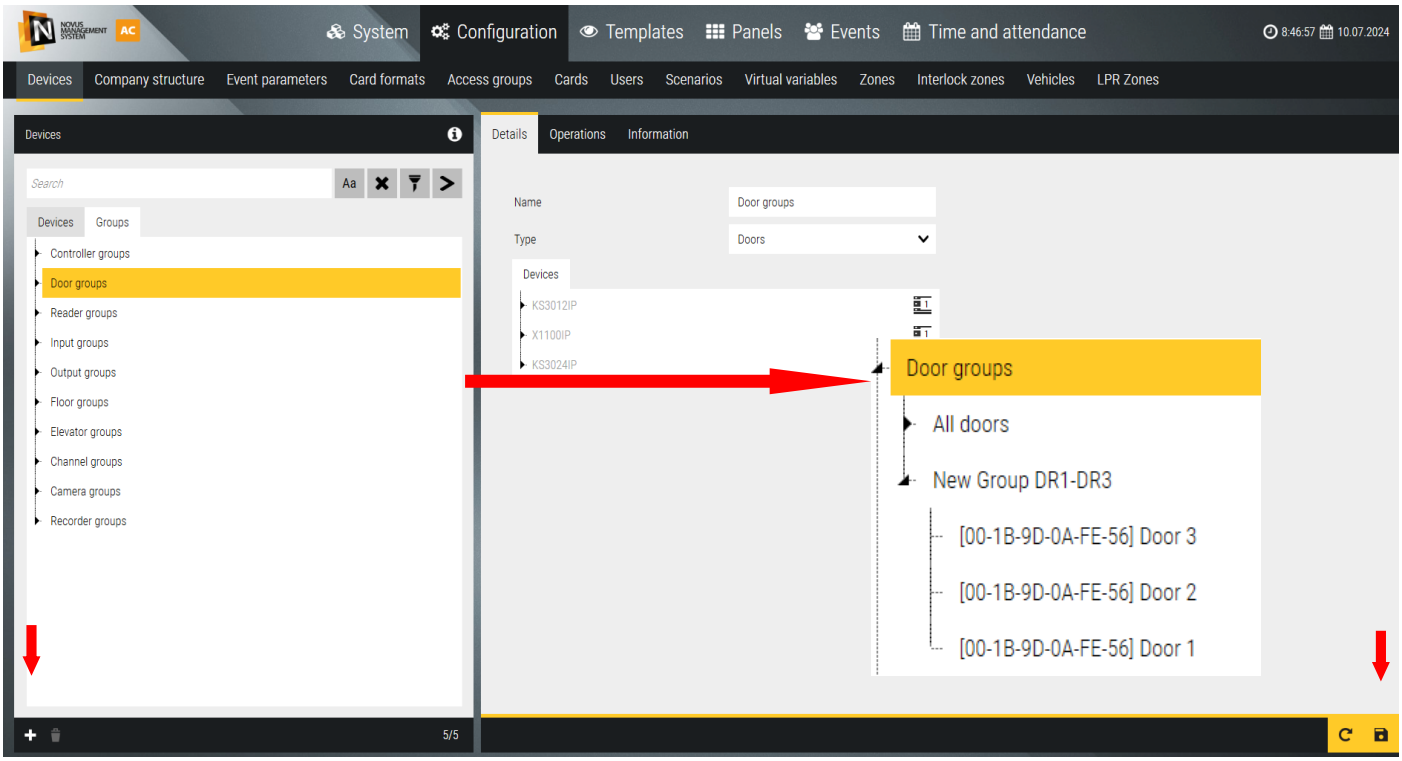
Each item has an Information tab, where you can put any description you want.



3.17 Devices - Groups

The *Groups* tab allows you to define groups of system elements. The list of main default groups is displayed in the left window. Each default group has a defined group that contains all elements of a given type (see Door Groups) and is automatically updated when a new element of a given type is added.

Groups are used to perform collective operations on system elements, e.g. unlocking a group of doors, which greatly speeds up the process when there are a large number of doors. Operations on groups can be performed from the context menu of the black group icon on the panel or by going to the Operations tab in this window.



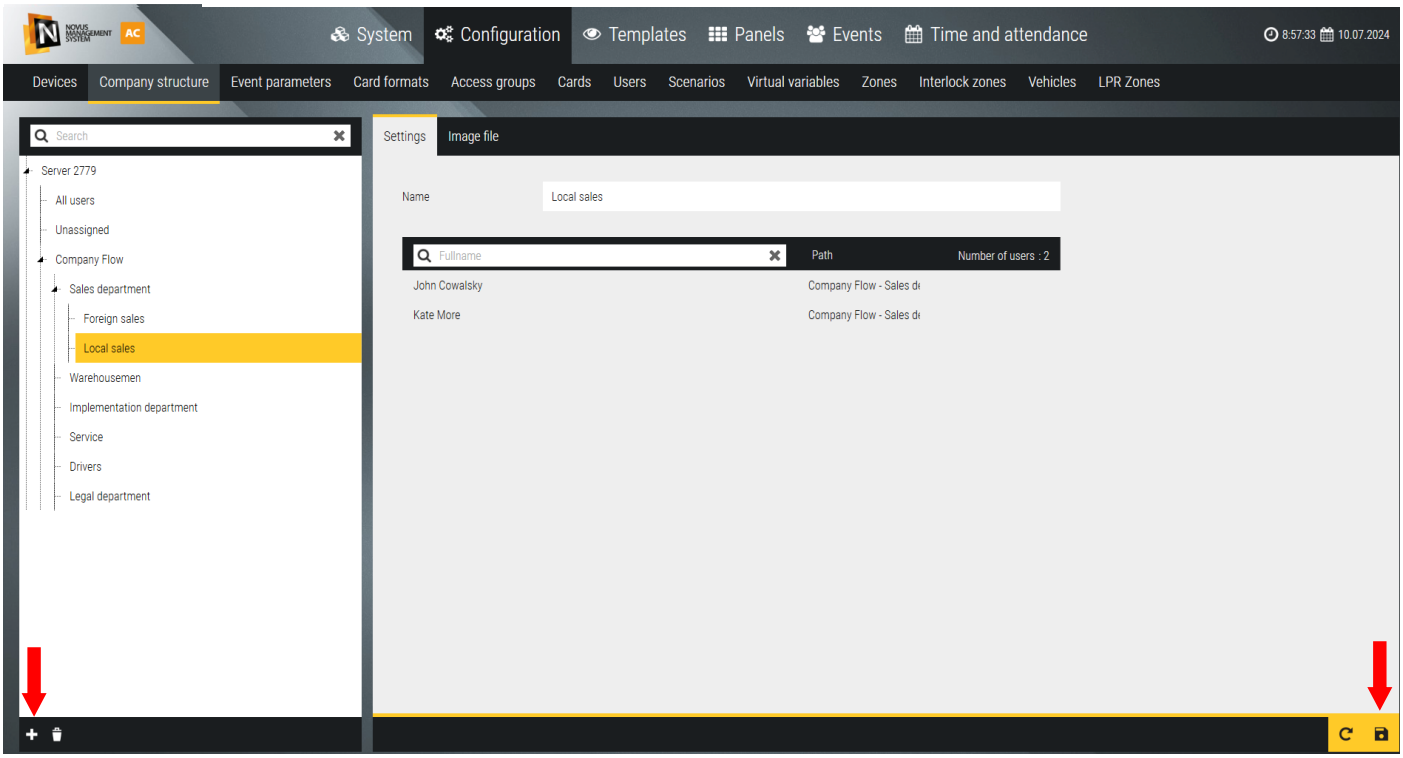
In addition to default groups containing all elements of a given type, we can define subgroups that contain only selected elements of a given type. To do this, select the default group of a given type and click the *Add* button at the bottom of the window. A new subgroup will appear in the group tree, and a list of all items of a given type will appear in the right window. Select the items you want to belong to the new group.

To add a new group in the main tree, no group must be selected. If there is such a selection (yellow bar) then click on it while holding down the CTRL button. A group added in the main tree can contain elements of different types. This can be used to create a system structure in multiple locations.

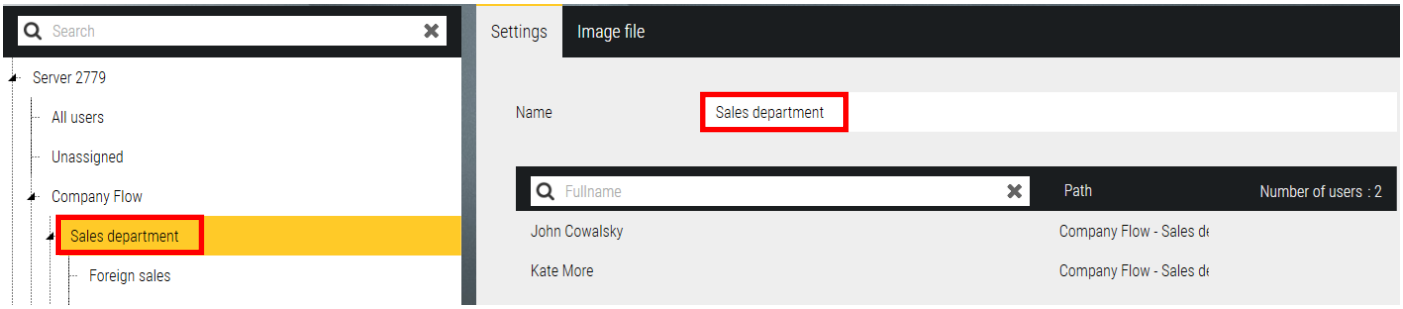
A defined group can be edited or deleted by selecting it in the list and clicking on the *Delete* button in the lower left corner of the window.

3.18 Configuration - Company structure

The tab allows you to define the company's organizational structure and then assign employees to it. This allows you to generate event reports and T&A reports for the selected department.
By default, there are two items in the left window:



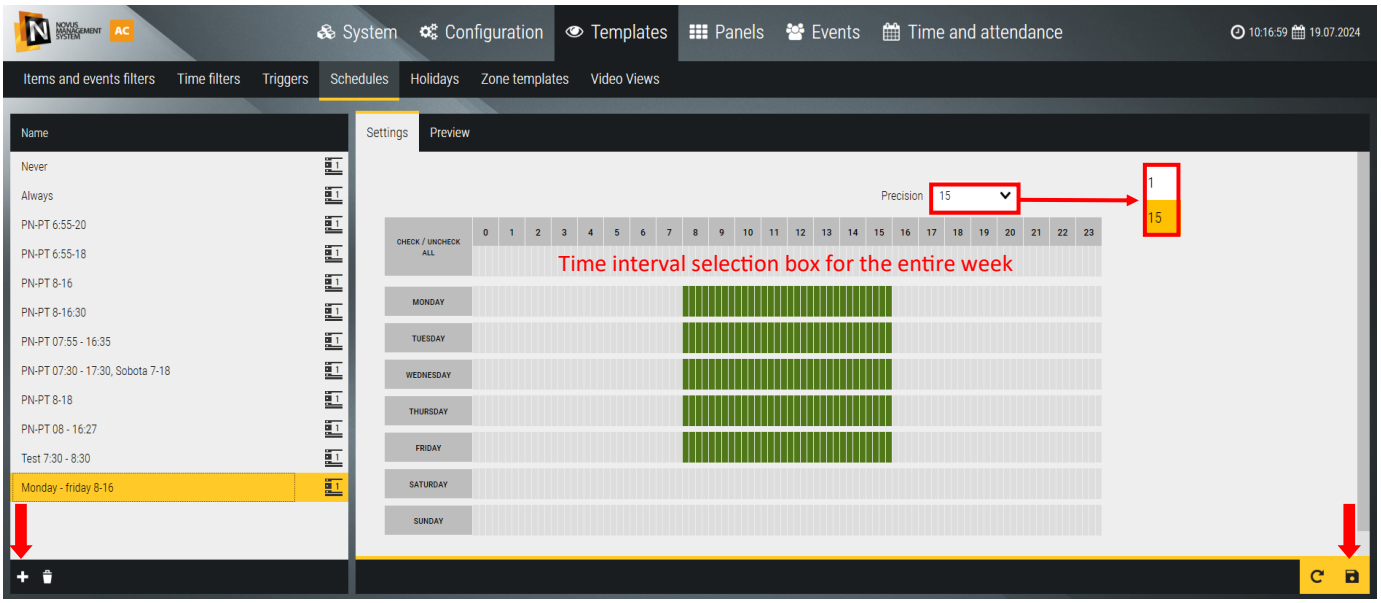
All users- displays in the right window a list of all users added to the database
Unassigned- displays in the right window a list of users not assigned to the structure
After adding users (manually or by import), both lists are the same.
To add a company structure, click on the Add button in the lower left corner.
A new position will appear in the tree. To add a new position in the main tree, no position must be selected (to de-select click on the selected one with the right mouse button). If there is a selected item in the main tree then you can add more items to it. In this way you can create a multi-level structure of the company - department, division department, etc.
In the right window you can edit the item name. After defining the structure, click the Save button in the lower right corner. Assigning an employee to the structure should be done in the user definition window.
In the right window, you can edit the name of the pos. After defining the structure, click on the *Save* button in the lower right corner. Assigning an employee to the structure should be done in the user definition window.



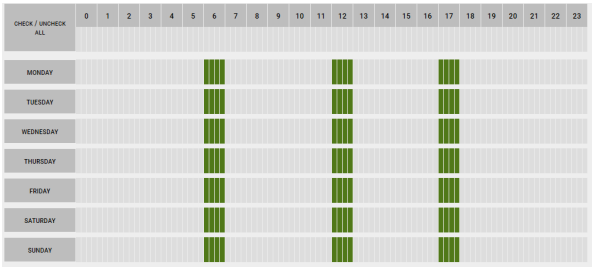
Section 4. Users, cards and access groups

4.1 Schedules

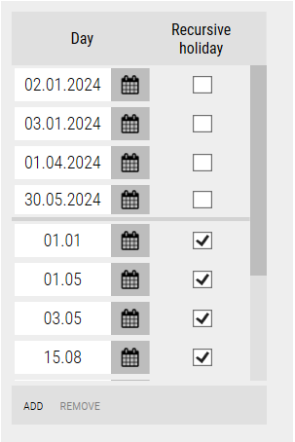
The Templates / Schedules tab allows you to define schedules intended in the KD system for access levels, automatic unlocking of doors, monitoring of guard lines at specific time intervals, and activation of control outputs and scenarios.

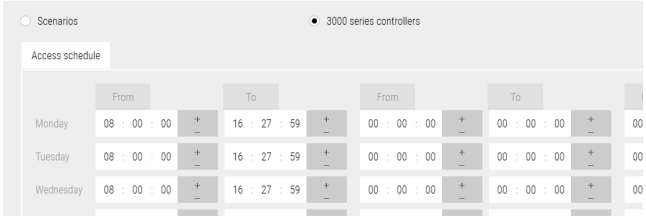


By default, two schedules are defined, *Never* and *Always*, which cannot be deleted or edited.
To add a new schedule, click on the Add button in the lower left corner of the screen. The default name in the yellow box can be changed to your own.
By clicking or dragging in the interval selection box with the right mouse button, we can highlight in green the active interval for the entire week. Then with the left mouse button, you can delete the active schedule for the selected day of the week by clicking on the name of the day on the left (e.g. Saturday, Sunday) or directly on the green box to delete the 15-minute intervals. In the schedule designed for KS3000 series controllers, you can define up to 3 time intervals per day - example opposite.

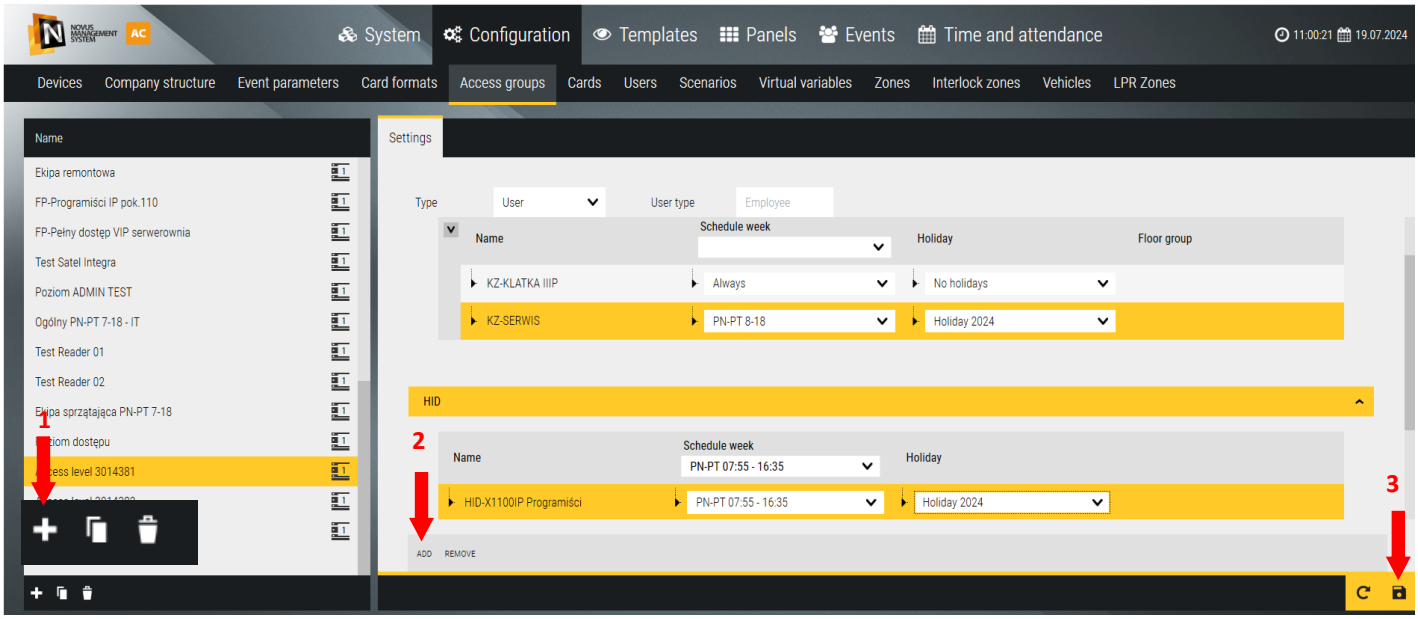


Holidays can be defined for the operation of scenarios by clicking on the button on the right side of the window. In the date fields, set the date of the holiday with the cursors in the order: year, month day. Then check the Special day checkbox. If the holiday is recurring, check the checkbox Repeat every year. If the holiday contains more than one day, we check the following checkboxes. On holidays, the schedule activity fields are slightly grayed out. The same or different special days can be assigned for each schedule.
For KD controllers, holidays are defined in the Configuration / Holidays tab.
In the Preview tab, you can view the appearance of the defined schedule in the form of a table
A defined schedule can be edited or deleted by selecting it in the list and clicking on the Delete button in the lower left corner of the window.

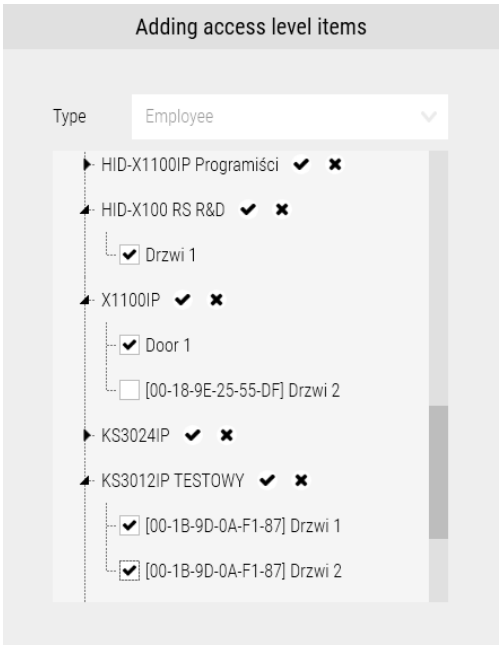




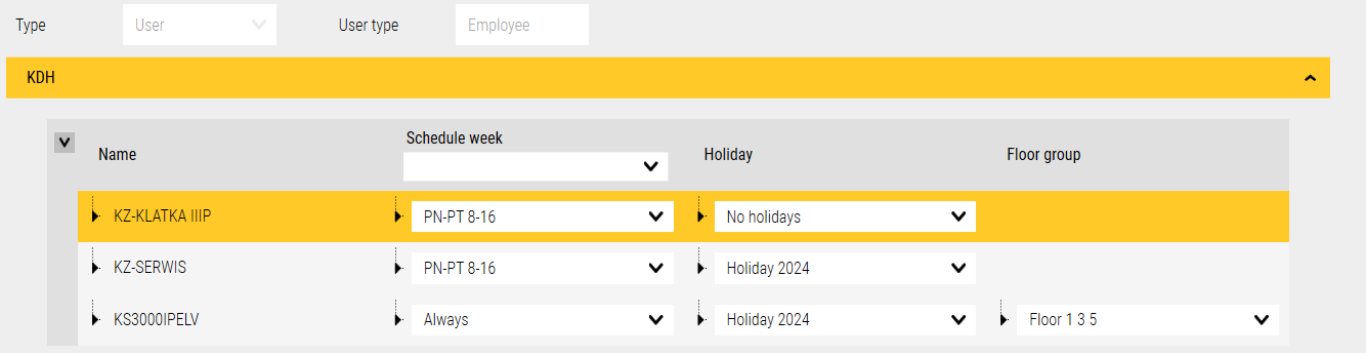
4.2 Acces groups



The Access Groups tab allows you to define access levels intended for card users and permissions deciding which partitions/zones of the control panel the user will have access to. The access level for the KD system is a set of permissions deciding to which passages and in what interval the user will have access. Detailed permissions for operations on the control panel are set in the user definition window - IDs/System tab. For elevators, the access level determines access to selected floors.
By default, two access levels are defined: No Access and Full Access, which cannot be deleted or edited.
To add a new access level, click on the Add button in the lower left corner of the screen. The default name in the yellow box
field can be changed to your own. Then click on the Add button in the right window. A window will appear, listing all the doors and elevators and exchanges that have been added previously. Select the doors and elevators (as readers in the booth) for which the user will have access privileges during the specified time interval and confirm with the OK button.
Checkboxes above the list allow you to quickly deselect and select all items.



The right window will display a table as below, containing the door and elevator selected in the previous window.



In the second column (Schedule week), select a schedule from the drop-down list according to the expected access permissions.

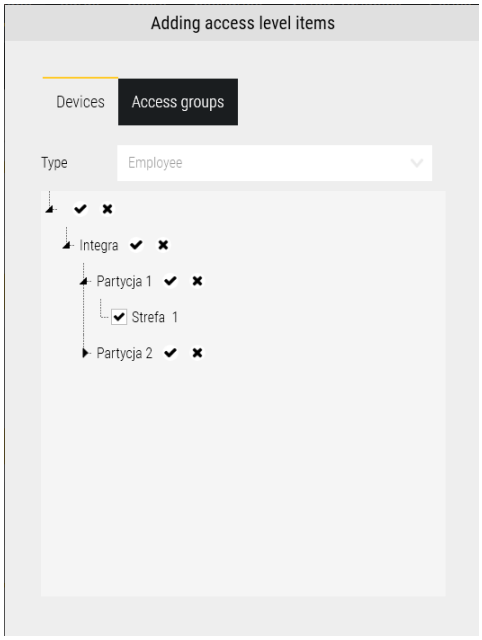
In the third column (Holiday), select a holiday from the drop-down list according to the expected access rights.

In the fourth column (Floor Group), select the floor group from the drop-down list according to the expected access rights.

Save the settings by clicking on the floppy disk icon in the lower right corner of the configuration window.

The access levels so defined will be able to be assigned to one or more users.
The icon  at the bottom of the left window is for deleting an entire access level, while the one on the right is for deleting a single line, i.e. a selected door. On the other hand, the icon  for copying already created levels for editing purposes

4.2.1 Access Groups — Intrusion and Hold-Up alarm system (I&HAS)



The Access groups tab allows you to define access levels for users. The access groups is a set of permissions that determine which objects/ partitions a user will have access to.

To add a new access groups, click on the  button in the lower left corner of the screen. You can customize the default name in the yellow field to your own.

Click on the Add button in the right window.

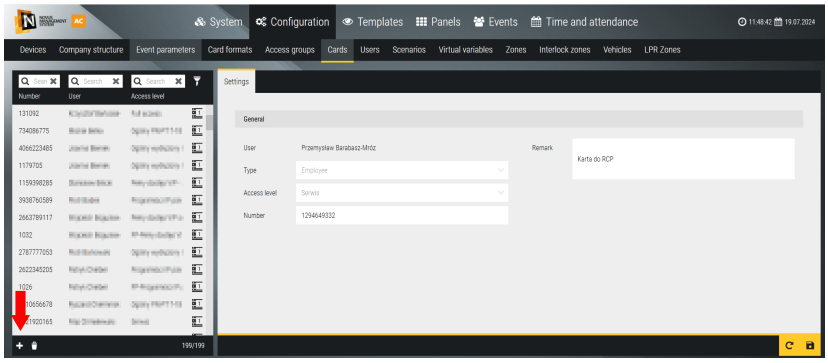
A window with a list of all previously added devices will be displayed.

Select the objects and partitions to which the given level will have access rights and confirm with the OK button.

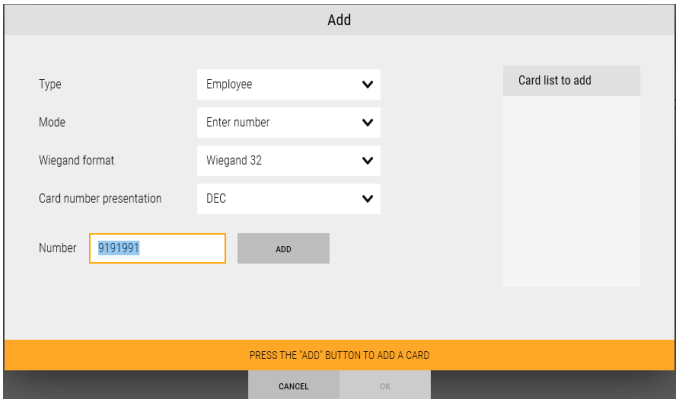
Checkboxes allow you to quickly check and uncheck and mark all items.

4.3 Cards

This tab allows you to create a list of numbered cards for later and faster assignment for any user.



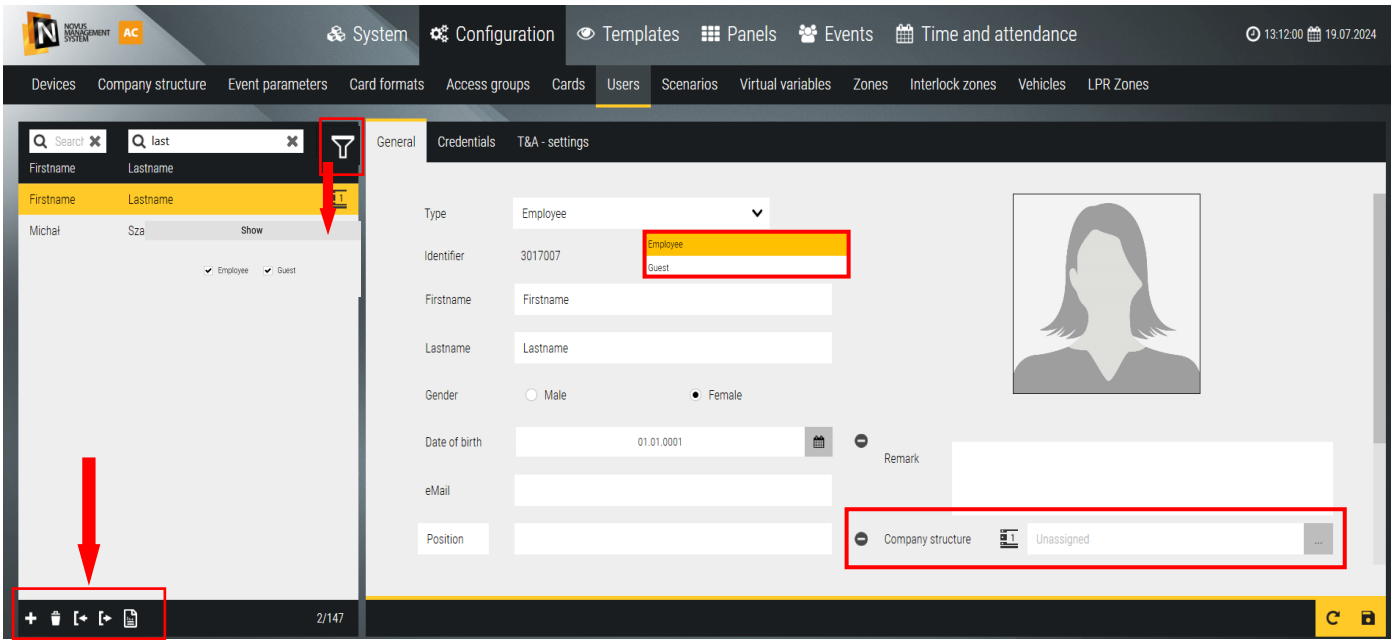
After clicking on the *Add* button, a window is displayed as below:



A detailed description of this procedure is described in section 4.4—*Users/Card.* In this window, adding cards assigns them right away for a particular user.

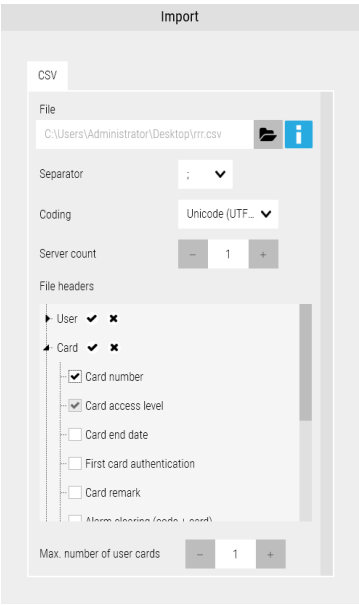
4.4 Users

This tab allows adding new users to the system's database and assigning them personal data, photos and IDs (card, PIN, fingerprint). It is possible to assign a user to an T&A group, which allows you to record and account for their working time based on defined schedules and calendars (paid license). It is also possible to enable filtering of the list by type. A new item is to assign a user to a defined company structure, which allows you to generate event and T&A reports for selected departments.



Users can be added manually or by importing data from a file. The file import procedure speeds up the process considerably in case of a large number of cards or license plate numbers.

To export a file containing user data, select the option
A window will appear as on the right.
By default, all available export options are selected in the Export window. You should choose only the options you want to export (e.g., User, Card), select the appropriate separator (default: ;), and encoding (default: Unicode UTF-8).

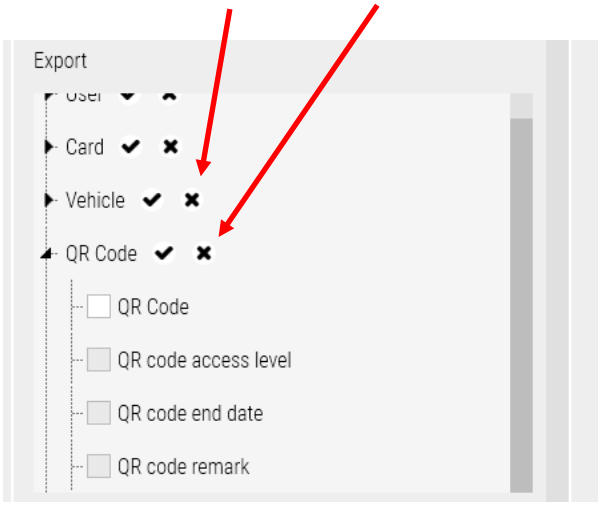


An example of an exported file with selected part of the options available for the User and Card items:

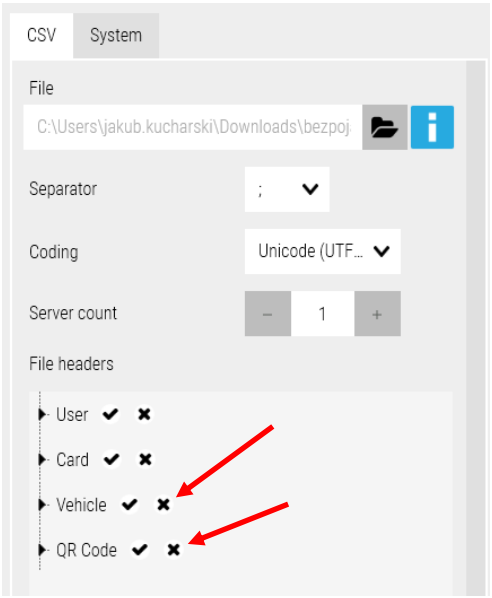
	A	B	C	D	E	F	G
1	Identifier	User type	Server name	Firstname	Lastname	Male	Card number
2	3006540	Employee	SRV AAT W-WA	Rafał	Nowak	Yes	755151267

Indicate the file from which the data is to be imported, select the appropriate separator, encoding and specify the maximum number of cards, vehicles and QR codes contained in the imported file. Under File headers, select only the data that the file contains. If not configured correctly, the import will fail. For new users, the ID column should be empty. For previously added ones, it will contain the ID assigned by the program and should not be changed. The server name must match the defined name of the server to which the data is to be imported.

Example. If a user is not associated with any vehicle or QR code, both options must be deselected during both export and import.



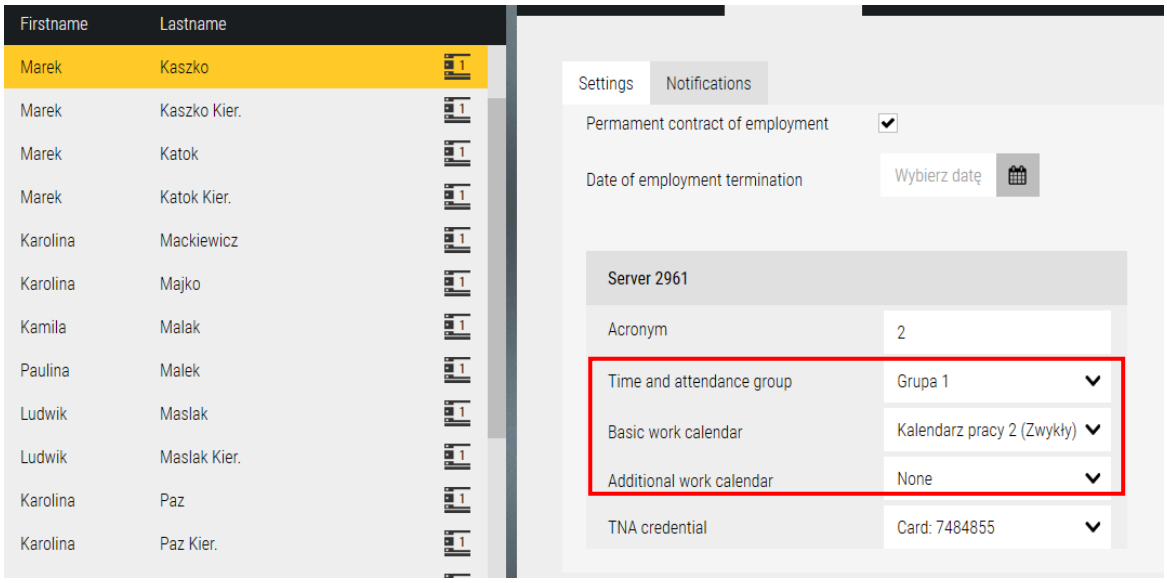
To import a file containing user data, select the icon
A window like the one shown below will appear.



A fragment of the imported file without the Vehicle and QR Code options:

AA	AB	AC	AD	AE	AF	AG	AH	AI
Firstname	Lastname	Male	eMail	Remark	Card number	Card access level	Card end date	First card authenticatior
Karolina	Paz	No						
Kamil	Poziomka Kier.	Yes						
Kamil	Poziomka	Yes						
Paulina	Tasak	No						
Marek	Citko	Yes						
Radosław	Utkasz	Yes						
Paulina	Tasak Kier.	No						
Agata	Tomczak	No						
Luiza	Ponatko	No						
Karolina	Majko	No						
Paulina	Malek	No						
Karolina	Paz Kier.	No						
Ludwik	Maslak	Yes						
Marek	Katok	Yes						
Karolina	Mackiewicz	No						
Tamara	Falko	No						
Marek	Kaszko Kier.	Yes						
Ludwik	Maslak Kier.	Yes						
Tadeusz	Retka	Yes						
Marek	Katok Kier.	Yes						
Marek	Kaszko	Yes			748	Pracownicy Terminal RCP		No

IMPORTANT! In the Users / T&A – Settings tab, it is not possible to export data related to time and attendance (T&A).

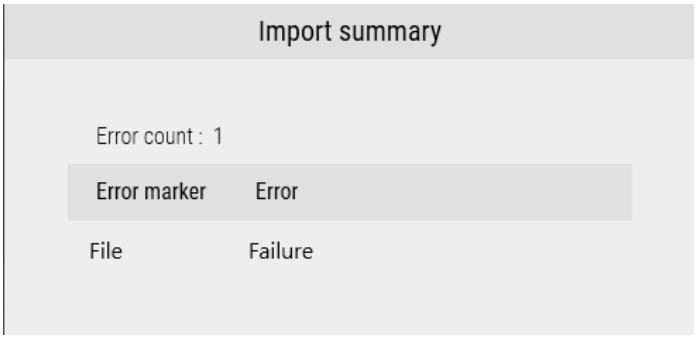


If the data in the columns are to be imported: Type, Work Calendar, Work Time Group, Access Level and Company Structure then these items must first be defined in the program and then their names copied and pasted into the appropriate columns. If, after the first import, you want to continue working on such a file (i.e. change the parameters of previously added users or add new ones), you should always export the current database first and work on such a file.

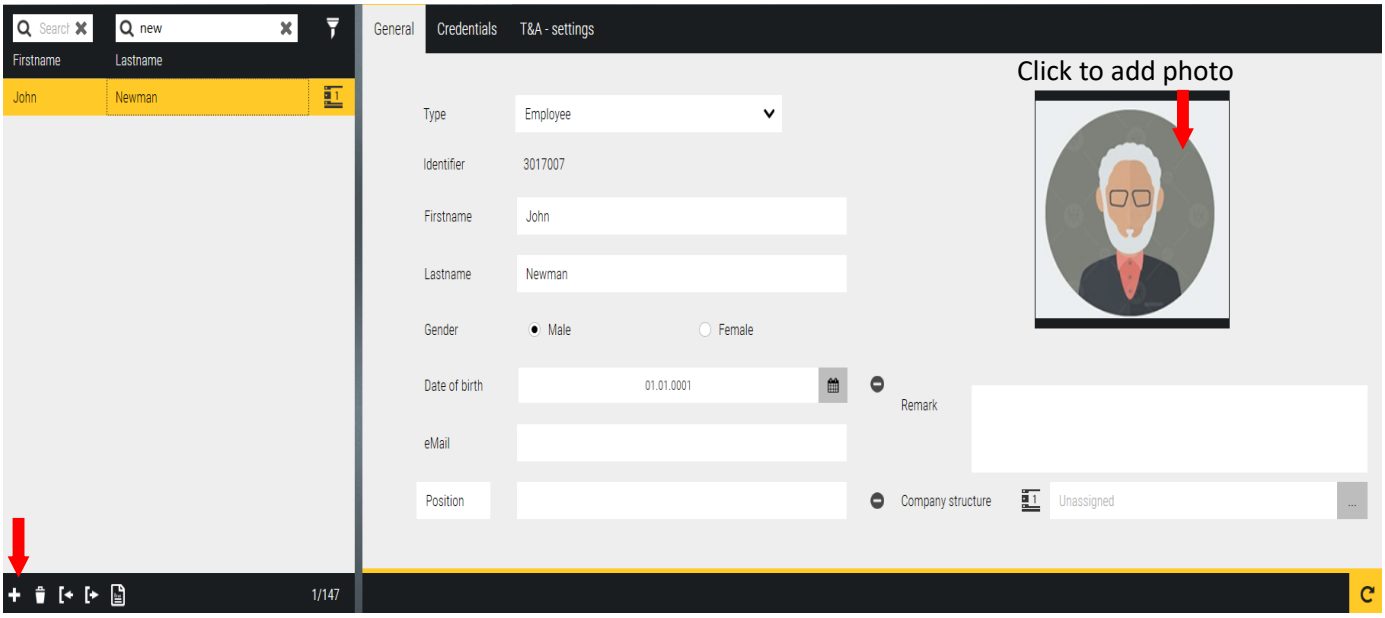
View of the exported CSV file:

A	B	C	D	E	F	G	H	I
Identifier	User type	Server name	Company structure	Acronym	Time and attendance group	Time and attendance calendar	Additional work calendar	Date of employment commencement
11146	Employee	Server 2961	Pracownicy RCP	3				18.06.2025 00:00
59022	Employee	Server 2961	Kierowcy	23				27.06.2025 00:00
11160	Employee	Server 2961	Pracownicy RCP	10				18.06.2025 00:00
11150	Employee	Server 2961	Pracownicy RCP	5				18.06.2025 00:00
65012	Guest	Server 2961	Kierowcy	28				27.06.2025 00:00
11166	Employee	Server 2961	Kierowcy	13				18.06.2025 00:00

IMPORTANT! During the data import process, the file being imported must not be open (e.g., in Excel or another editor). Otherwise, an error may occur:



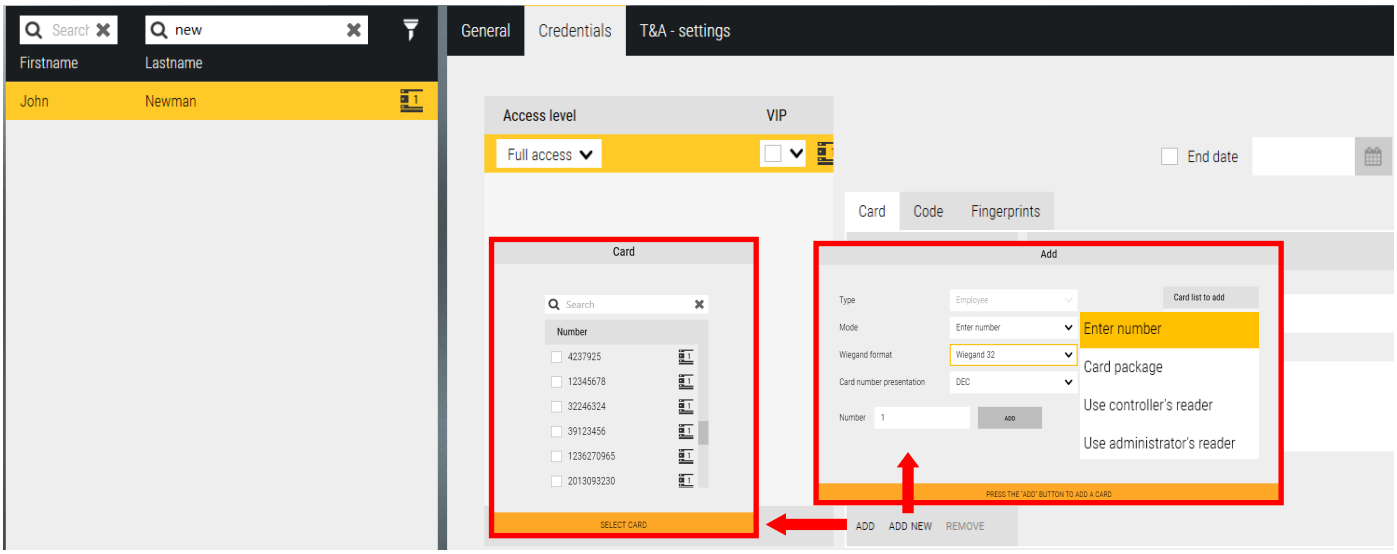
Adding a new user - click on the Add (+) button in the lower left corner of the window (to delete, select and click Delete). Then fill in the form fields in the right window. Except for the first and last name field, the other fields are not mandatory. You can also add a photo of the user from a file by clicking on the designated avatar field. The left window displays a list of added users.



If you click on the icon “+” you can add another information field with editable name

By clicking on the “-” icon you can delete it

Adding a card - You should go to the *Creditialc* tab. The program will display a window as below:

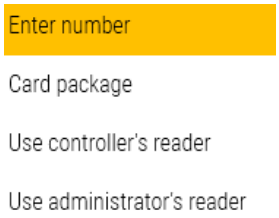


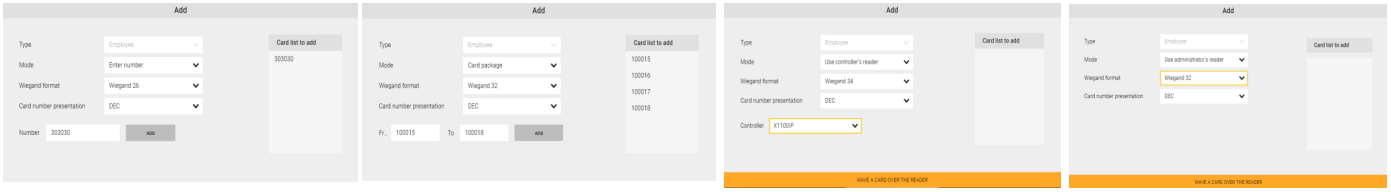
In the window on the previous page, we have two ways to assign a new card to a user. A user can have more than one card.

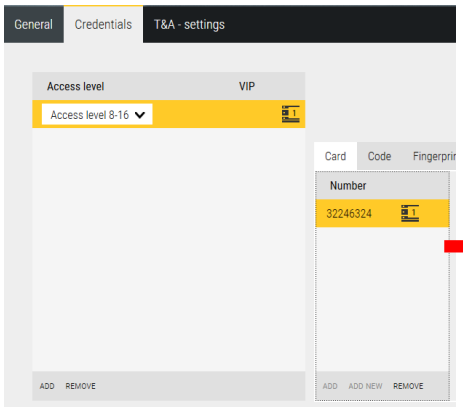
After clicking on the *Add* button, a window pops up as on the left with a list of cards added earlier through the Cards tab. Select the card numbers you want to assign to the user.

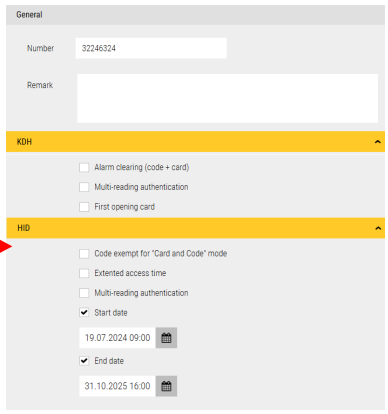
After clicking on the *Add New* button, a window pops up as on the right. In this window, we can choose one of four options for entering the card number in the list:

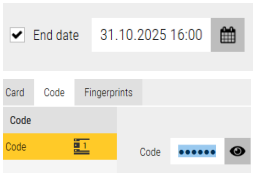
- Manual entry of the number in the editable field (when we know the card number) The entered number is subject to verification, if it already exists in the system database it is highlighted in red and cannot be added.
- Manual entry of the first number from the card pack (pack with consecutive numbers) and the final number
- Reading the card on the reader of one of the controllers
- Through the administrator's USB reader











After adding card numbers and fingerprints to the list, return to the *Users/Identifiers* tab:

Each card has a separate menu on the right side of the window, which is displayed when a card is selected in the list. Removing cards from the database only from the *Cards* tab.

Access level - select from the drop-down list

Number - unique identifier number displayed in the system

Remark - text field for entering additional description

KDH - ID function settings for 3000 series controllers:

Alarm clearing (code + card) - Enables deactivating an active alarm on the controller where the reader is attached, by entering the code for alarm clearing (other than PIN, defined in the controller settings) and reading the card

Multi-reading authentification - (2,3 times) authorizes to unlock/lock the door permanently or enable/disable the control output.

First opening card - option required if the user is to have permission to unlock card access for other users without this permission. Active on readers with this option enabled.

End date - after checking in the box below, set the required date, type or select from the calendar

HID® - ID function settings for HID®series controllers:

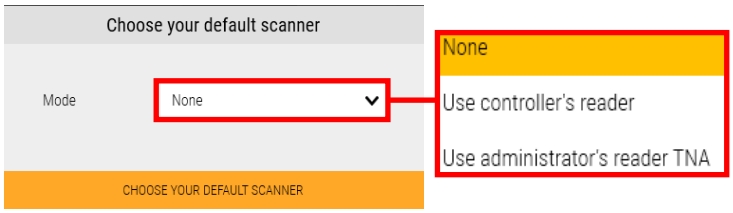
Code exempt for „Card and code" mode - transitions set in the "c&c" mode will not require entering a PIN.

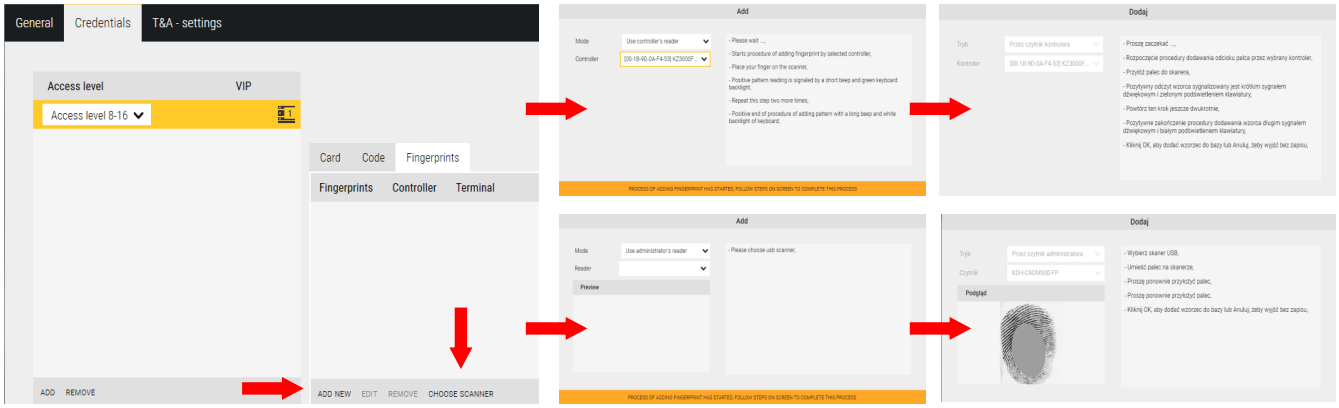
Extendet access time - Door unlatching and opening time will be as in the *Door/Extended Access Time* setting

Multi-reading authentification - (2 times) authorizes to unlock/lock the passage permanently or turn on/off the control output.

Start/End Date - allows you to enter the start and end date of the ID activity.

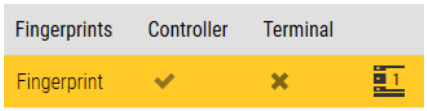
Adding fingerprints - applies **KDH-KS3000FP-IP-U_M i KDH-TA500CFP-IP-UMD**.
To start the procedure of adding fingerprints, click on the *Choose Scanner* button in the *Fingerprints* section.
For KDH-KS3000FP-IP-U_M models, add by selecting a controller from the list - Use controller's reader
For KDH-TA500CFP-IP-UMD adding via USB scanner - **KDH-CADM500-FP** - Use administrator's reader TNA
After selecting a scanner, click on *Add New* button





Adding fingerprints is done through a scanner in the selected biometric controller. Up to 3 fingerprints can be added. After opening the window as above and selecting the controller in the right window, the procedure instructions will be displayed.

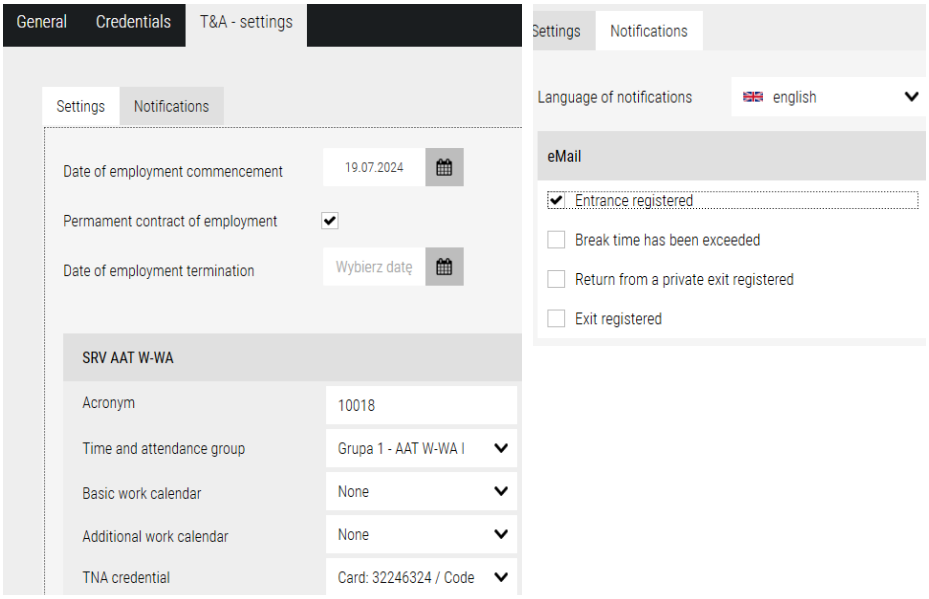
After completing the procedure (3 finger touchdowns), click OK, and after closing the window, you can add fingerprints from more fingers in the same way. Then click Save to save the user data to the database and send it to the controllers.



After adding prints, information about what they can be used for will appear next to each one:
Controller or Terminal

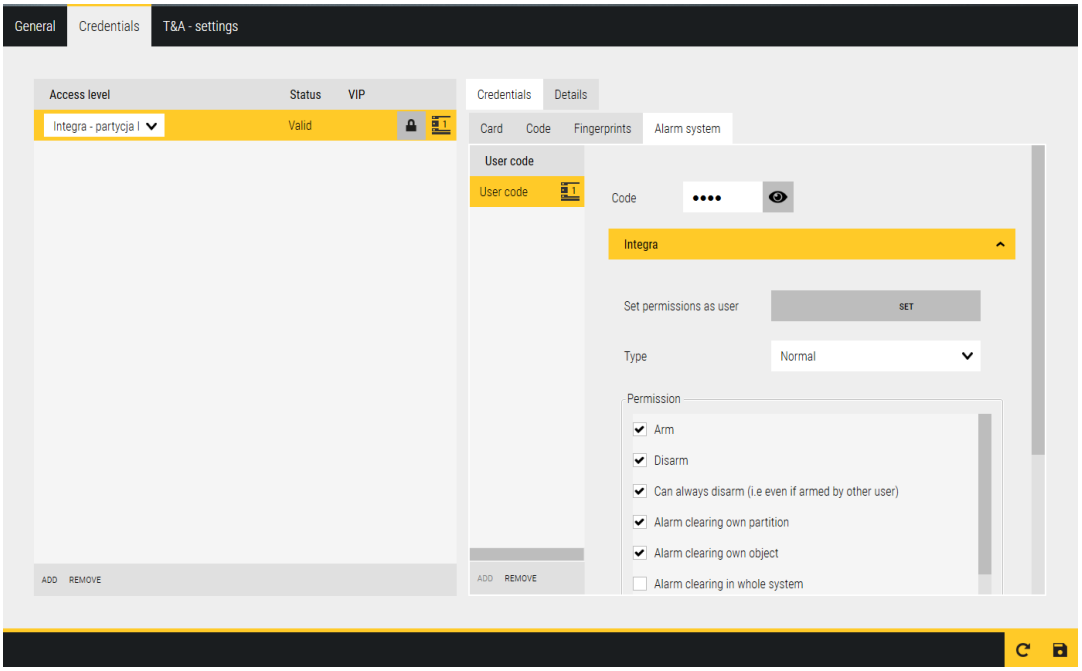
T&A settings - In this tab, you can define the user's start and end date of employment, assign group and working time calendars, and select an ID for time registration. You can also define an Acronym which is the user's identification number. This allows you to register *enter/exit* on the terminal or selected readers and generate time & attendance reports.

In the notifications tab, you can select T&A events after the occurrence of which an email will be sent to the employee with the current time for working the daily working time norm.
Time registration functionality is covered by a paid license!



4.4.1 Users - Inrusion and Hold-Up alarm system (I&HAS)

Adding users codes - after adding the access group containing the access level with the panel, go to the Alarm system tab.

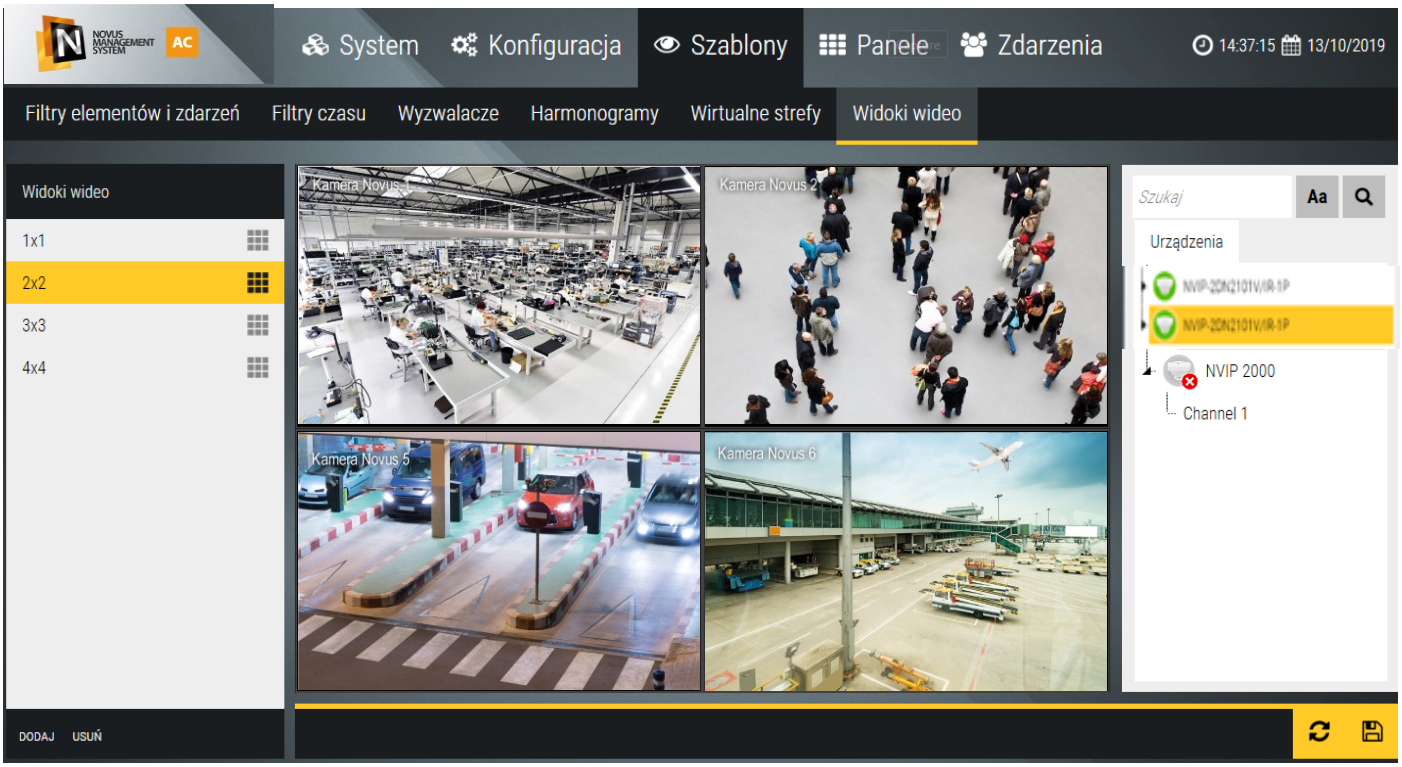


After clicking the Add button, define the user's password and its permissions (or copy from another user).
The password’s number of digits is defined when adding the new panel to NOVUS MANAGEMENT SYSTEM AC program.

Section 5. Templates

5.1 Video views

In the Video views tab, you can define sets of video views that are used to visualize and monitor the state of the system and display video streams from the cameras placed in the object. The list of defined video views is displayed in the left window. By default, four panels with different division are defined. After clicking the Add button you can add a new view, rename, assign a division to it by clicking on the icon in the view name field and the video stream by dragging it with the mouse from the list on the right in the selected view window. The video view can be viewed by clicking on its name in the left window.



Default views can be edited and changed to suit your needs.

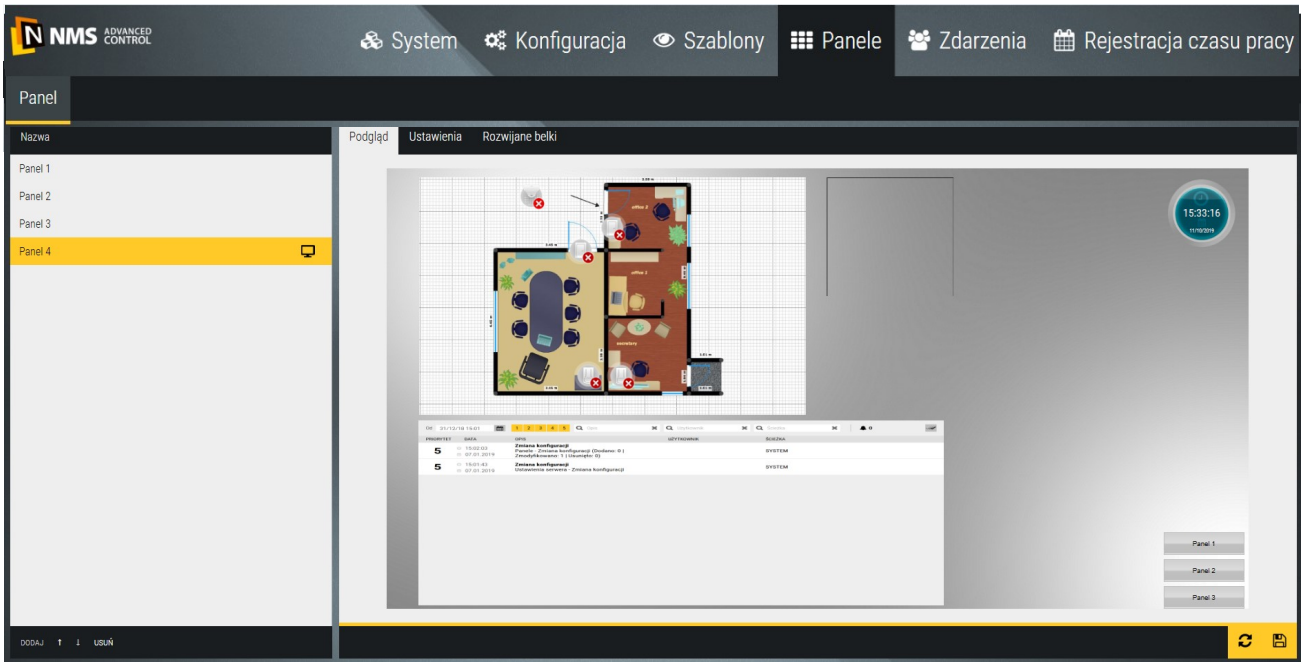
By right clicking on one of the split screens it can be set as a HOTSPOT window. This window will not have a permanently assigned camera. It will display the camera that the user click with the mouse wheel (middle button).

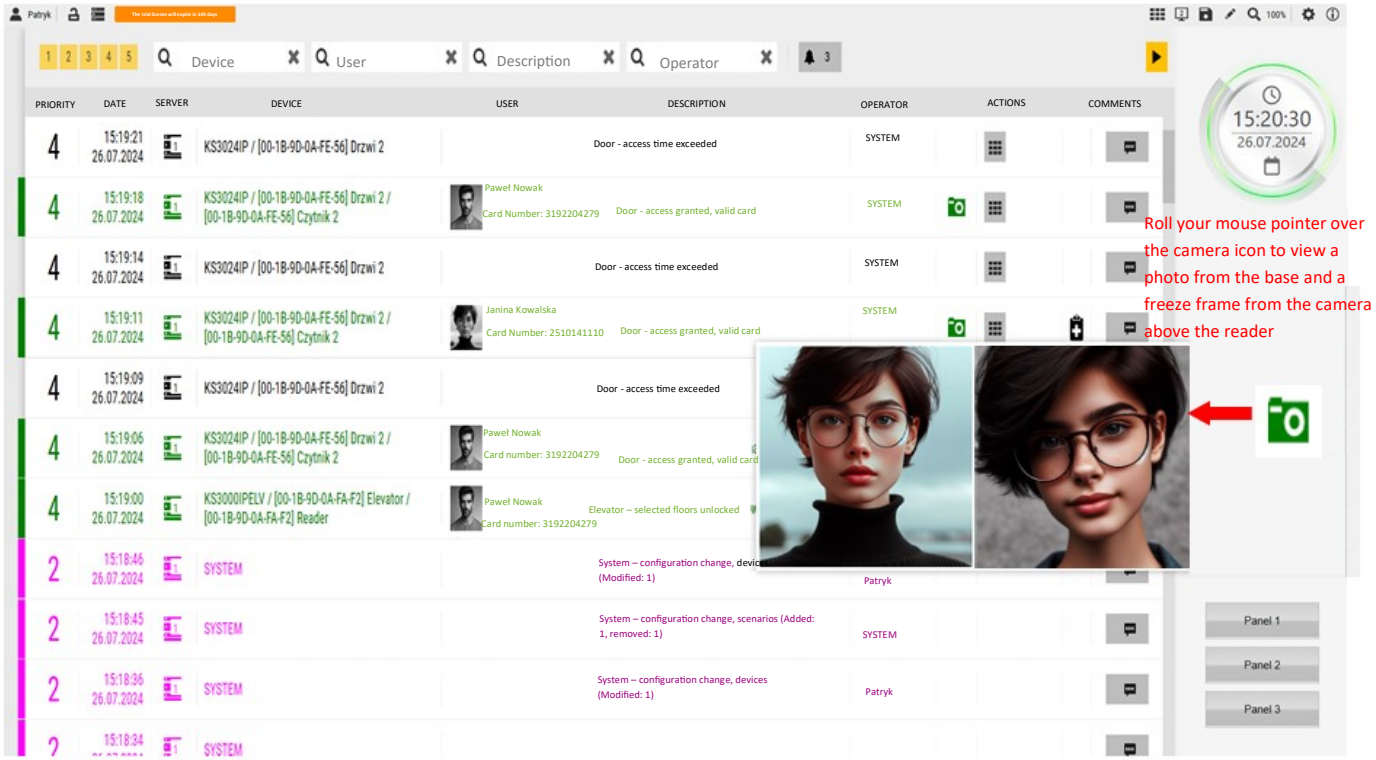
After you define the video views, click the Save button in the lower-right corner.
You can view defined video views on panels in video windows. Default Panel 3 includes this view window.

Section 6. Panels

In the *Panels* tab, we can define panels that are used to visualize and monitor the status of various system components and display events and other additional information. Panel can be displayed by clicking on its name in the left window.

The default Panel 1 contains: an event stack, a clock, and a button with a link to Panels 2 and 3.

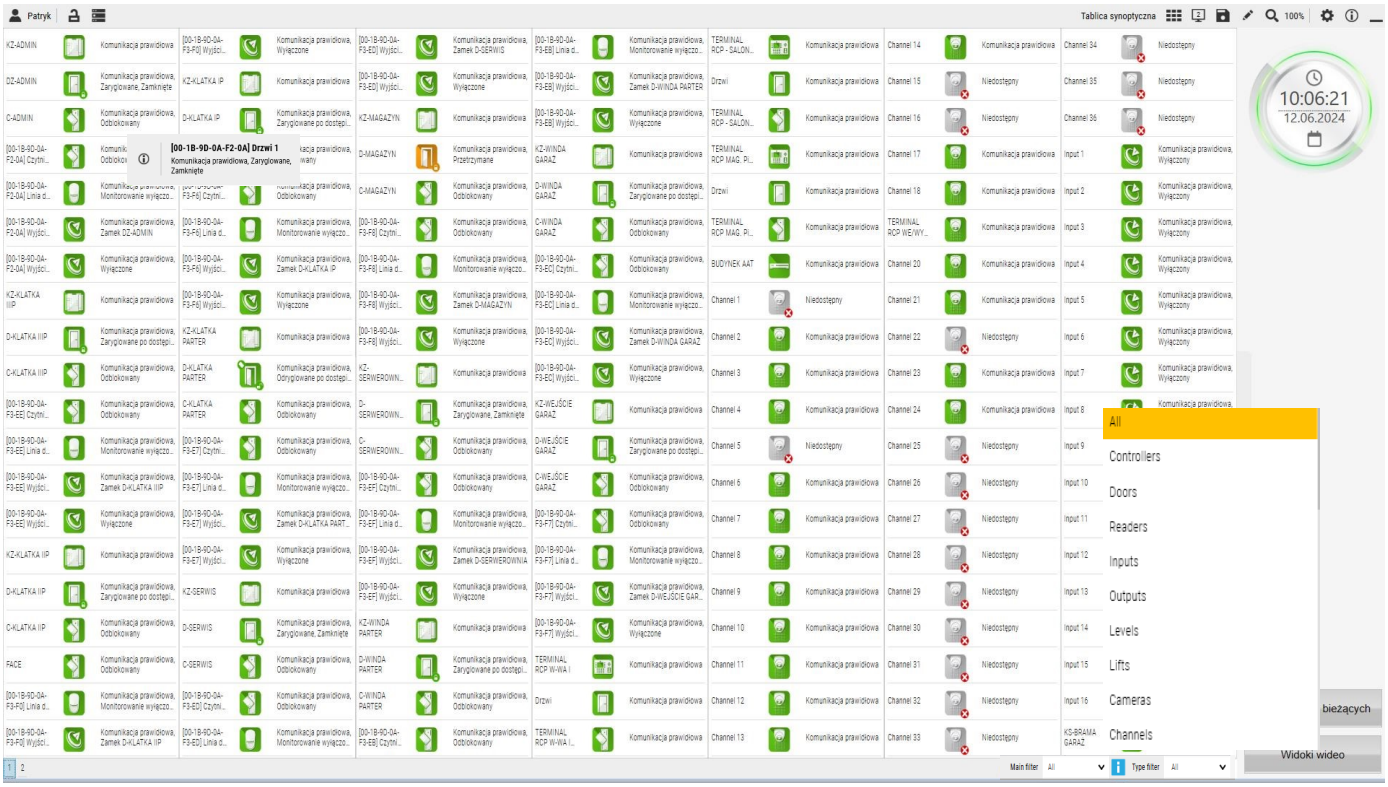




See the table on page 30 for a description of the icons on the top bar.

The *Event Stack* displays events according to the default settings in the *Event Parameters* tab.

Default Panel 2 contains: a synoptic board, a clock and buttons with links to the other panels.

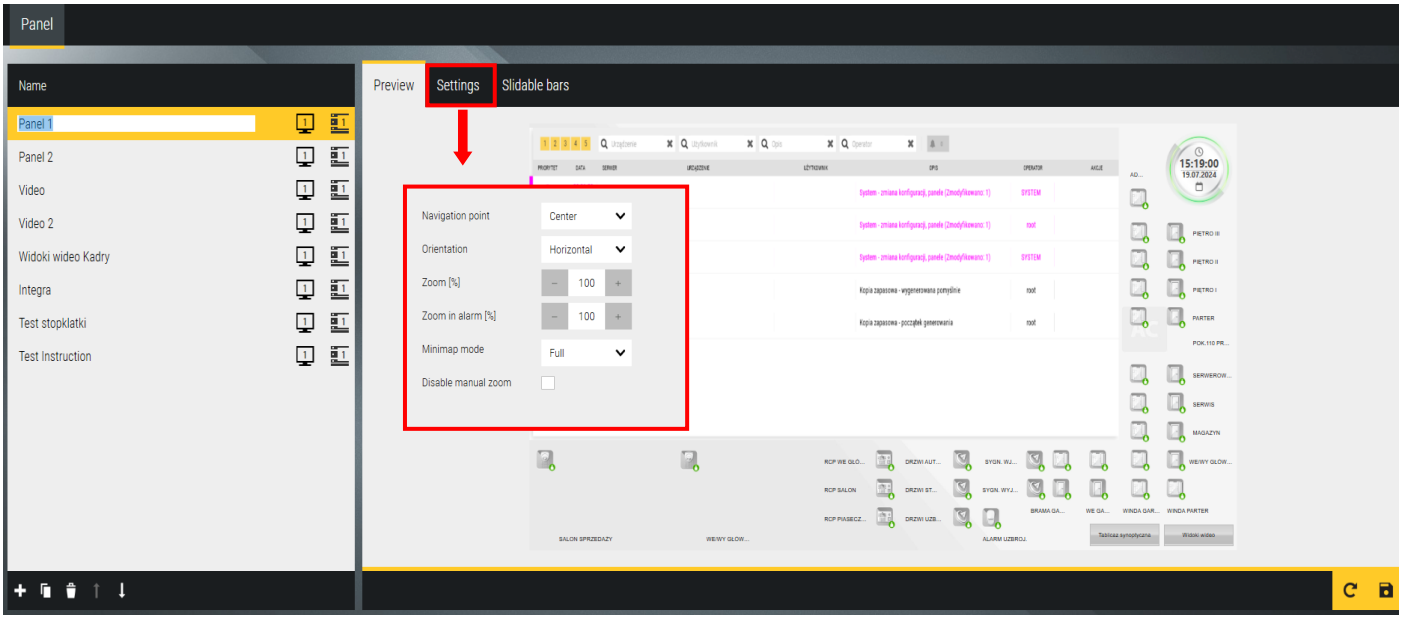


Panel 2 contains a synoptic table, to which successive added controllers are automatically added, along with associated elements (doors, supervisory lines, control outputs, elevators, floors) and CCTV devices in the form of icons showing their current status. The status of the icons is updated in real time (when there is proper communication with the devices). The icons have a context menu (left mouse button).
In the lower right corner of the synoptic table there are two filters that allow you to display in only selected items :

- Main filter - defined in the Templates/Filters tab for items and events and set in the panel editing mode
- Type filter - allows you to display items of only one type among those currently available on the board.
  Selection from the drop-down list.

The default *Panel 3* contains the video views window. Video views should be defined in the Templates/Video Views tab if you have added CCTV devices in the system.

To define a new panel, click on the *Add* button in the lower left corner of the *Panels* window.



The added panel appears in the list in the left window. The right one displays a preview of the panel's background.

Settings tab

Name - editable field for entering panel name

Navigation point - the point on the panel to which the process refers , by default Middle, other items will appear in this list after defining additional navigation points on the panel

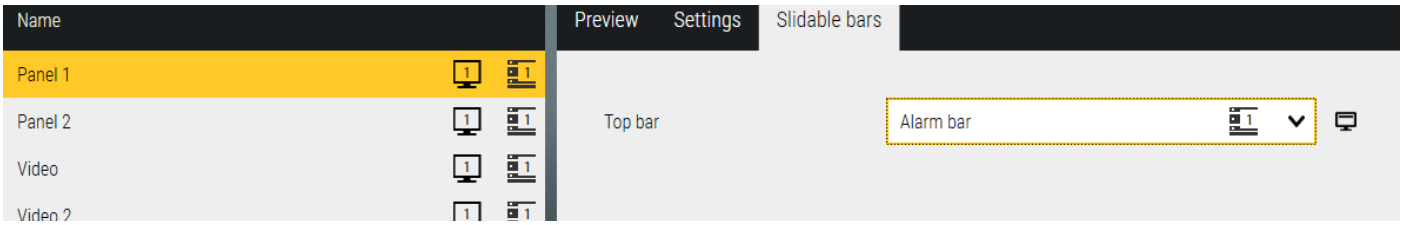
Zoom [%] - allows you to set the magnification value on the panel

Zoom in alarm [%] - pozwala ustawić wartość powiększenia dla zdarzeniu alarmowego na panelu

Disable manual zoom - allows you to set the magnification value for the alarm event on the panel

Minimap mode - to choose from a drop-down list the mode of displaying the thumbnail map: full, background only, transparent or no mini map.

Set background - allows you to select from the specified folder the background of the panel in bmp, jpg, png format or the default background



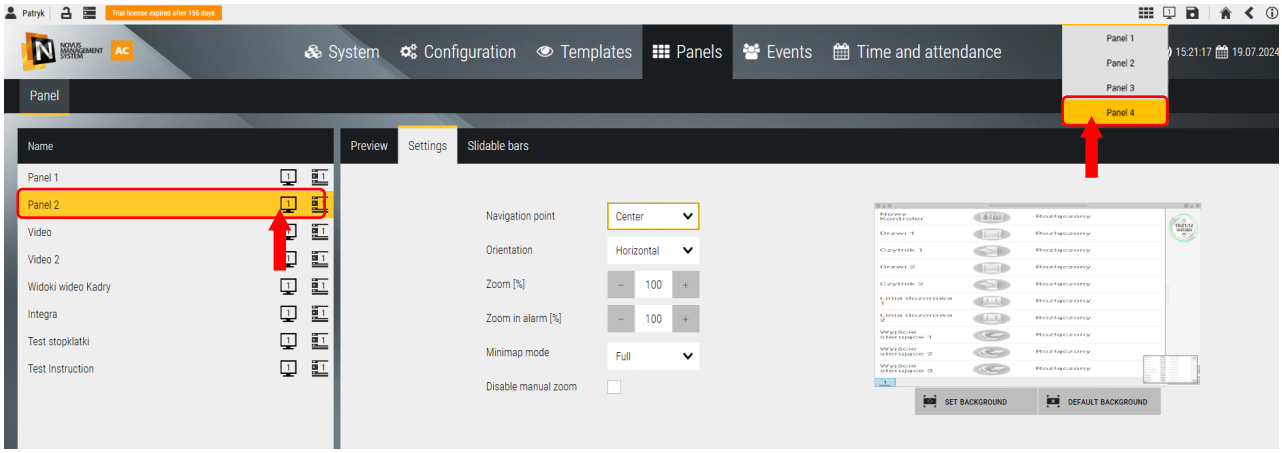
Tab *Slidacle bars*

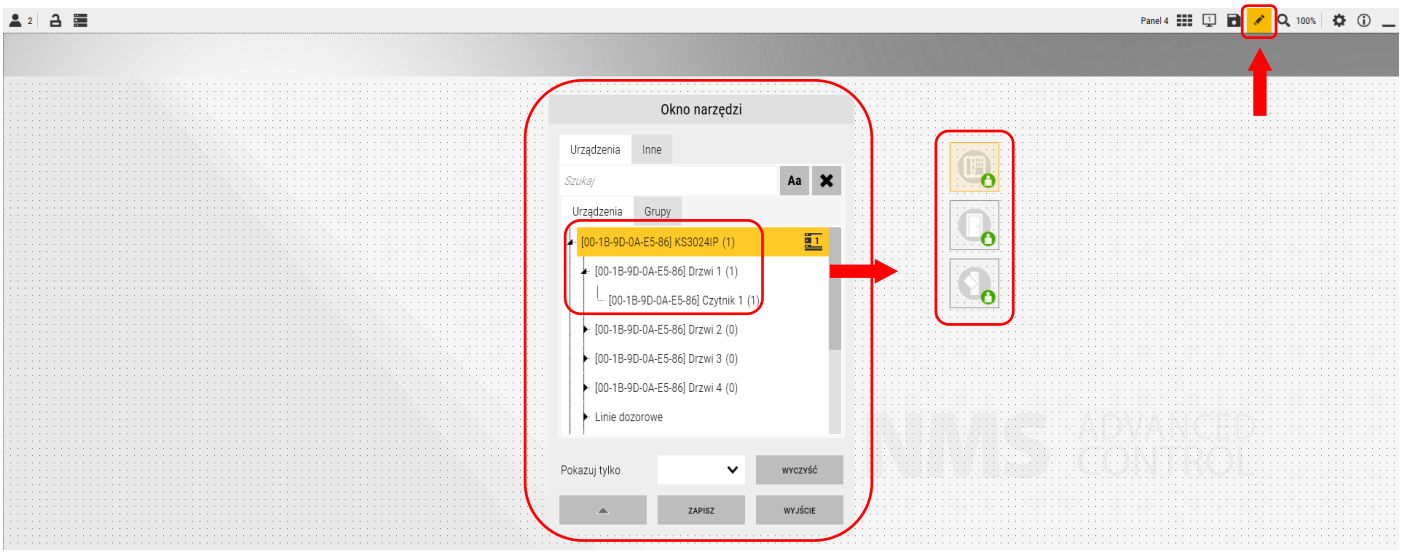
Top bar - to choose from the drop-down list: alarm bar or none

Once defined, save the settings for the new panel by clicking on the floppy disk icon in the lower right corner.

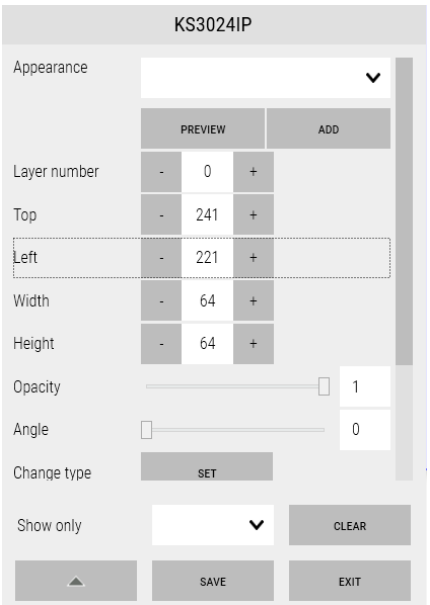
By clicking on the panel name in the left window, we can enter display mode and verify the settings.

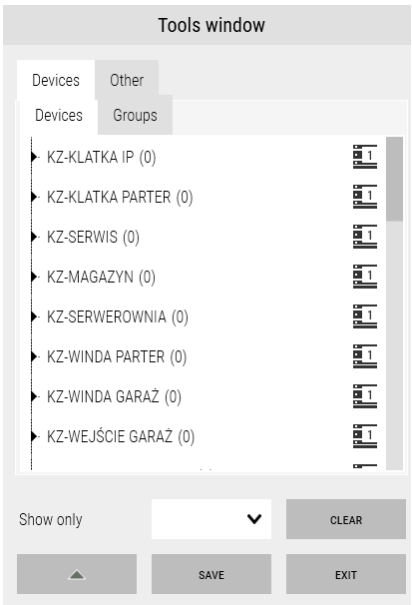
Configuration of the defined panel

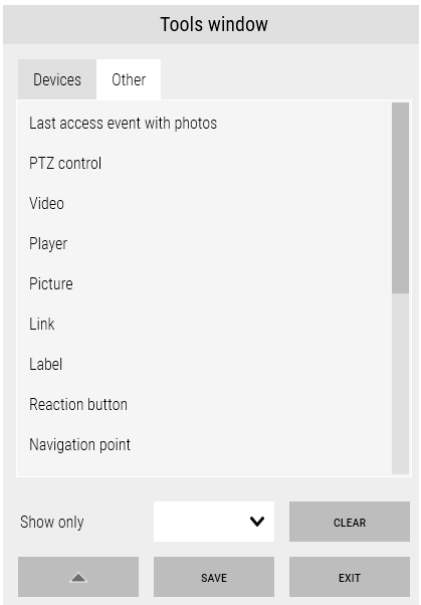




When you click on the list in the left window or in the upper right corner on the selected monitor, a window will appear as below. Clicking on the *Edit* icon in the upper right corner opens the Tools Window. The *Devices* tab displays a list of devices added to the system database, which can be dragged with the mouse to the panel window. When you click on an item set on the panel, its properties window is displayed - it is different for different items. In addition to devices, icons for element groups and



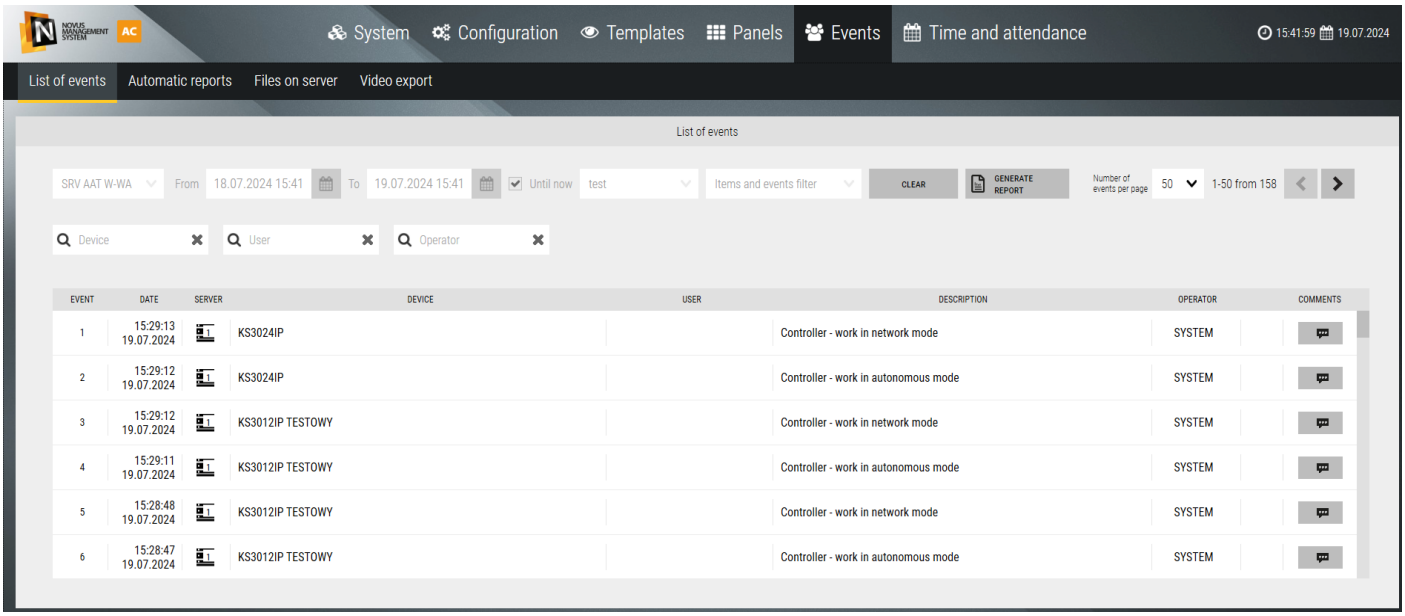




Section 7. Events and reports

7.1 List of events

In the Event List tab, we can generate a filtered report. The generated report is displayed on the screen and can be saved as a file on disk (buttons in the upper right corner of the window) in *.CSV or *.HTML format (with the possibility of exporting to pdf).



Each line of the report contains a date and time stamp, a description of the event, and links to the operator or card user and the physical system component affected by the event.

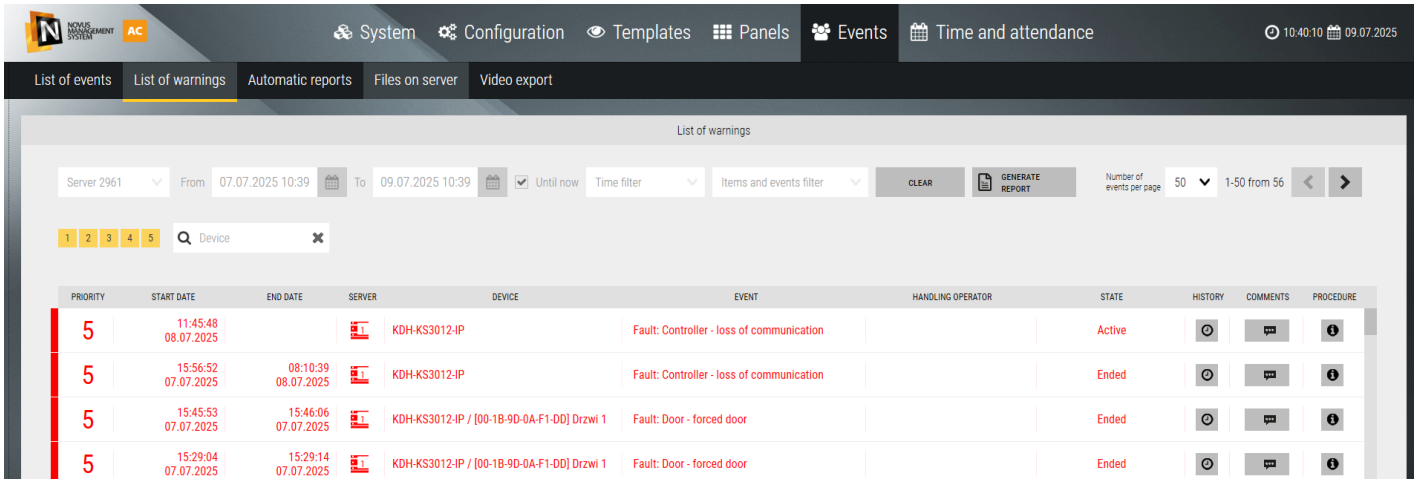
At the top of the window are filter windows for date, time interval (last 24 hours back by default), and items and events. This allows for easier analysis of events on the object

After setting the filters, click on the *Search* button. A report will be displayed in the window.

In the lower right corner of the window is displayed information about the number of events in the generated report. The maximum number of events in be 10,000. If, according to the filter settings, this value is exceeded this information is displayed. You should then change the filter settings.

7.2 Warning list

In the Warning List tab, you can generate a filtered report. The generated report is displayed on the screen and can be saved to disk (using the buttons in the top-right corner of the window) in .CSV or .HTML format (with the option to export to PDF).



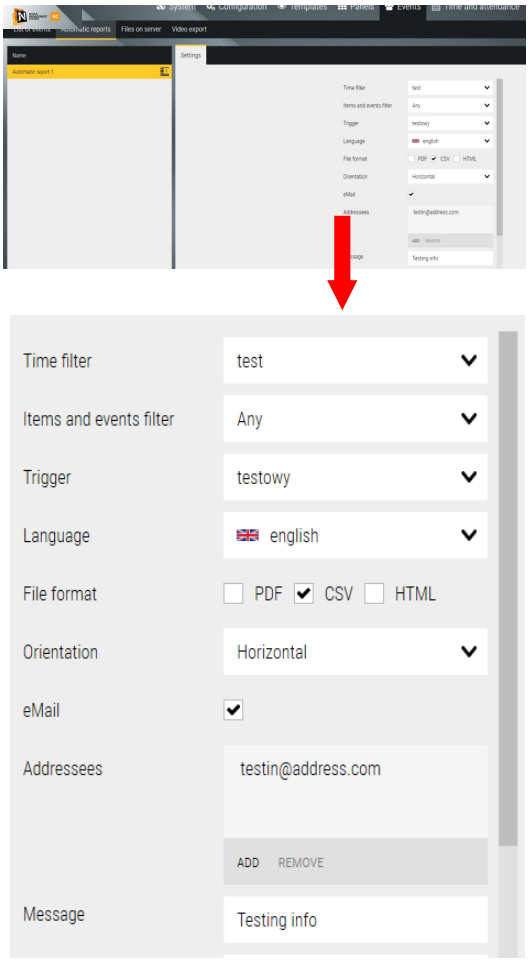
Each line in the report includes a timestamp indicating the date and time, a description of the event, associations with the operator or card user, and the physical system component related to the warning.

At the top of the window, there are filter fields that allow the user to specify the date, the time range (which defaults to the last 24 hours), and the system elements and events to be included in the report.

After setting the filters, click the Search button. The report will then be displayed in the window.
In the bottom-right corner of the window, the number of warnings in the generated report is shown. The maximum number of events is 10,000. If the number of events exceeds this limit based on the selected filters, a message will be displayed. In that case, you should adjust the filter settings.

7.3 Automatic reports

In the *Automatic Reports* tab, we can set the parameters of a new report template automatically generated according to the selected trigger. The generation of automatic reports is implemented through scenarios. For ease of use, an easy-to-use wizard for such scenarios has been implemented in this window. Analogous to manually generated reports, here we have a set of filters. We click Add and configure a new automatic report template.



Name - editable field for entering the name of the report template

Time filter - to be selected from the drop-down list previously defined in the window

Templates/Time Filters

Items and events filter - to be selected from the drop-down list defined in the window
Templates/Filters for elements and events

Trigger - to be selected from the drop-down list previously defined in the window
Templates/Triggers

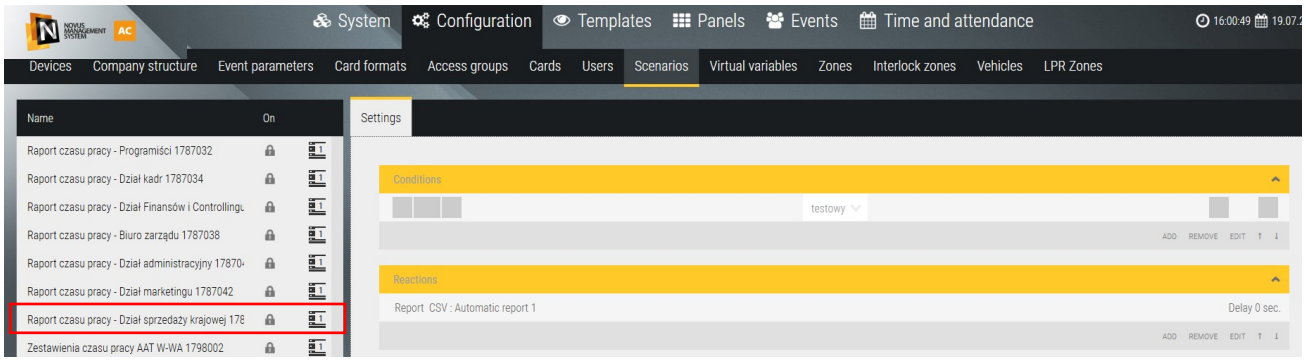
Note: Each of the above three options, when expanded, contains an "Add" item that opens a window to define a new filter or trigger

File format - choice of one of the file saving formats: csv or html

Orientation - Choice of horizontal or vertical page orientation for viewing or printing. Horizontal orientation is recommended due to the number of columns in the report and long descriptions.

Language - To choose from the drop-down list: Polish, English, Russian, Azeri. The following languages are in the process of translation.

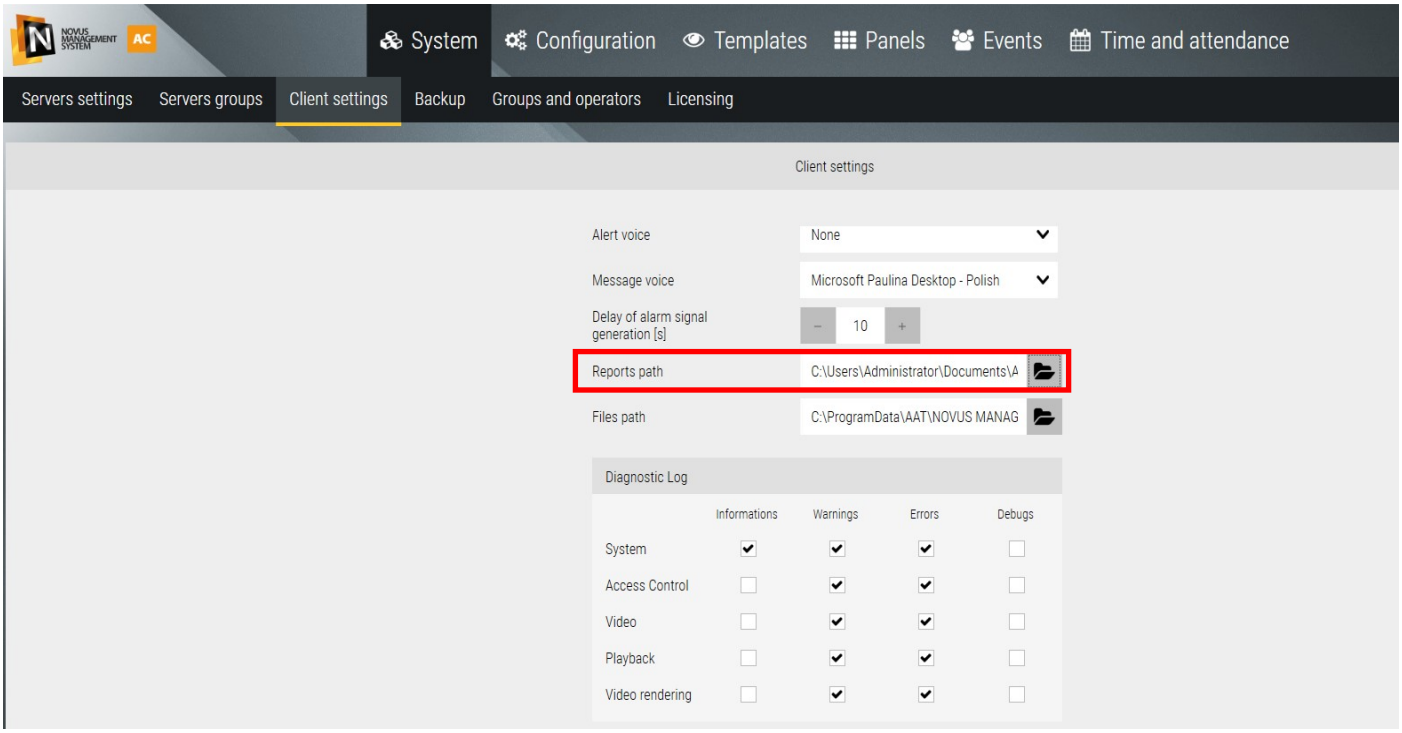
Email - A box to check if the report is to be sent as an email. Once checked, fields for entering email addressees and subject are displayed below. To add an addressee, click on the add button at the bottom of this field and enter the email address in the box that appears.



After making the settings and clicking OK, the corresponding scenario is created in the background, which we can display in the *Configuration /Scenarios* tab.

7.4 Files on server

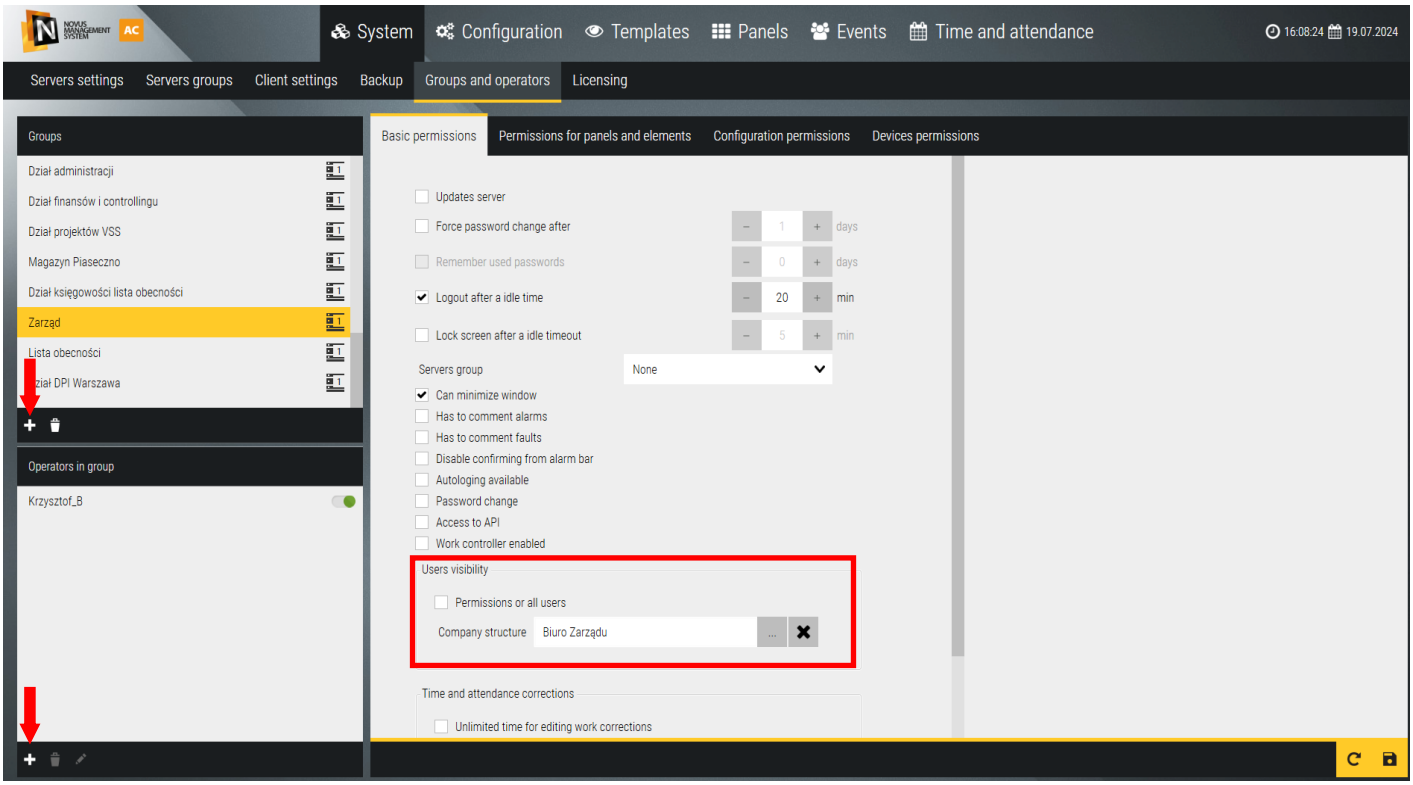
Reports generated automatically according to the trigger assigned in the template are saved in the report archive on the computer where the NOVUS MANAGEMENT SYSTEM AC server service is installed. You can change this path in the *System* tab.



On the client station, which is connected to the server, you can see in a window like the one below (Files tab on the server) a list of automatically generated reports. After selecting a report in the list, you can copy it to the client station to the indicated folder.

Section 8. System settings

In the System tab, we can, among other things, add new operators along with permissions regarding access to the program, set the language for the operator, make a copy of the system or restore it, and extend licenses.



8.1 Groups and operators

By default, one operator group named Administrator with full program and system privileges is defined. By clicking on the Add button in the upper left window, you can add other groups with limited privileges.

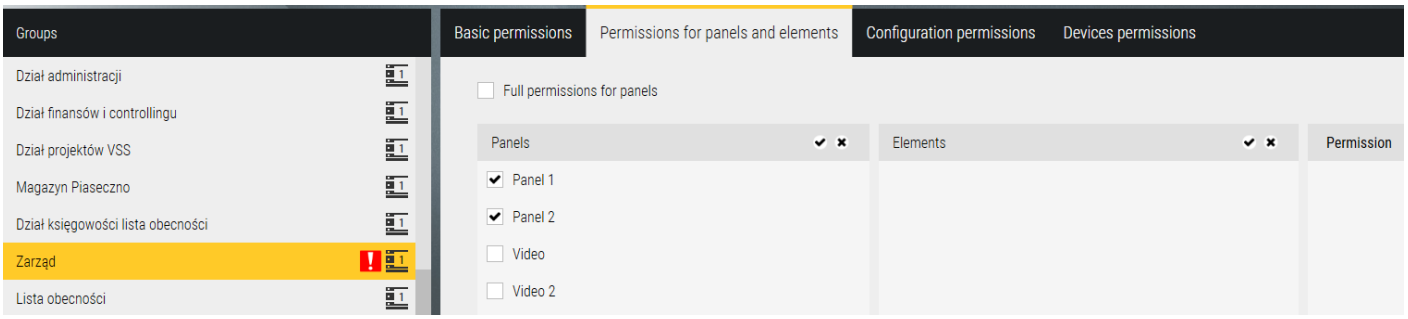
After selecting a group in the upper window, operators can be added to it. By default, one root operator with full privileges is defined in the Administrator group. Permissions are defined for the group (not for individual operators), for a new group of operators you should set them in the following tabs.

In the *Basic Permissions* tab, there are a number of *checkboxes* that must be checked to assign selected options.

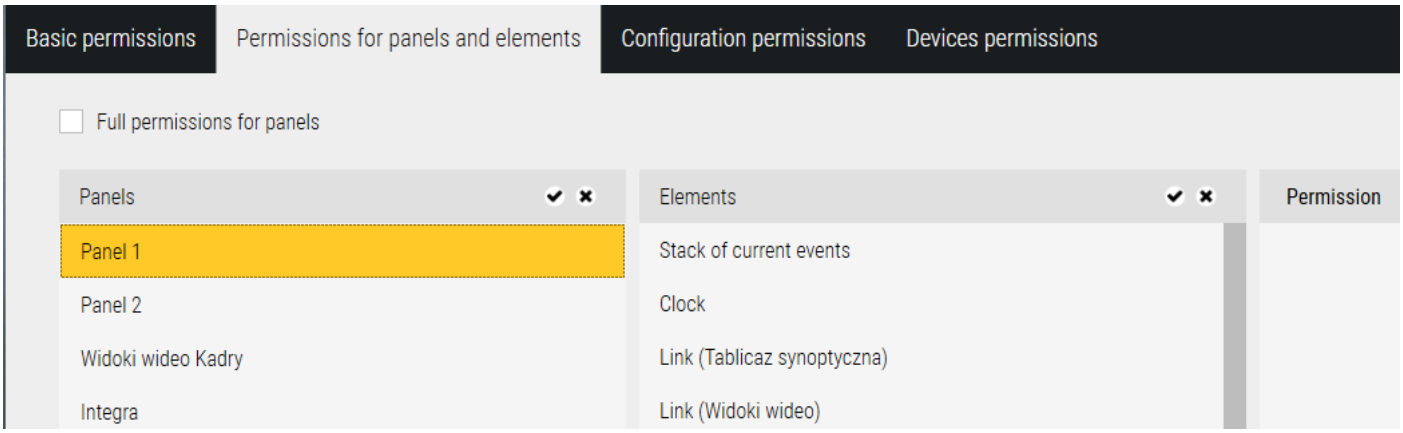
Info:

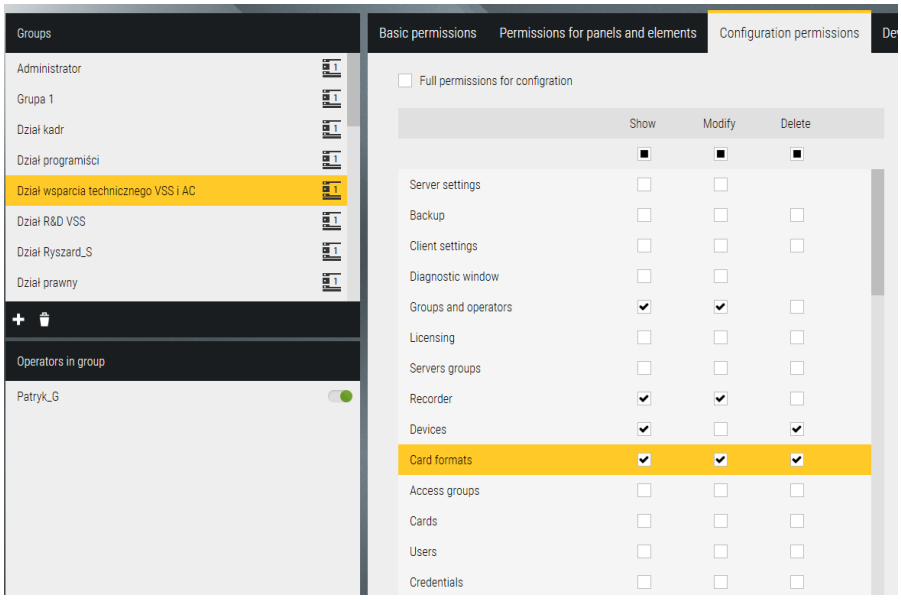
By default, no users are assigned for the newly created group. To change this, select All users or select users according to the company structure.

Permmision for panels and elements



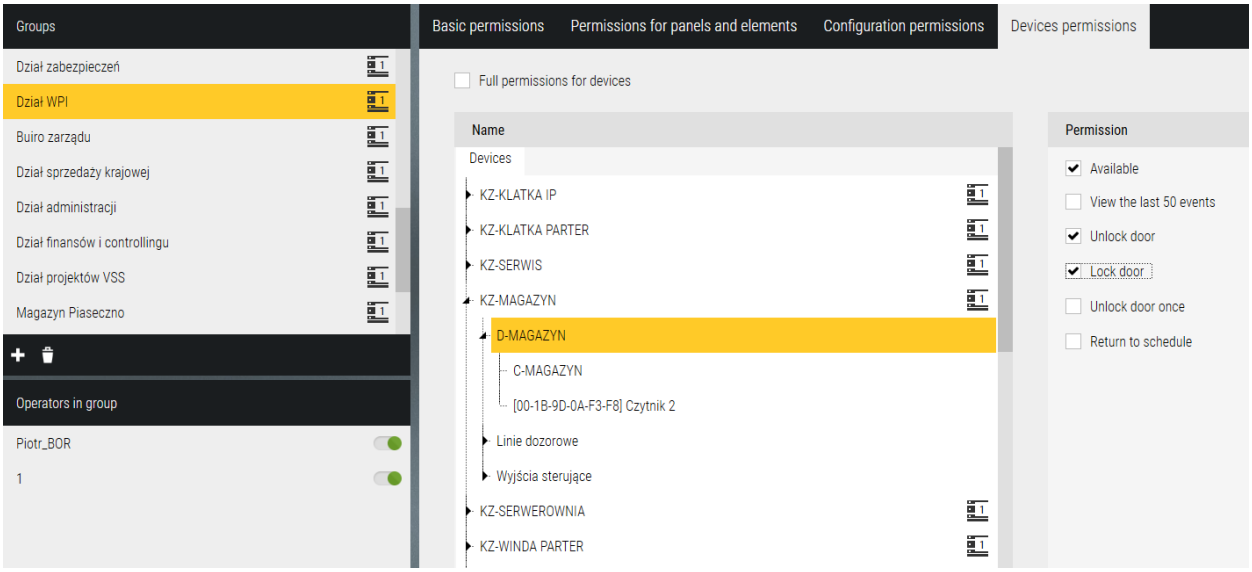
After clicking on the button at the bottom of the window, a list of available panels is displayed in the first column - select those to which operators from this group are to have access and OK.
The second column (Elements) displays a list of elements embedded on this panel. After selecting a selected element in this list, in the third column (Status) we can choose to HID®e this element on the panel.
Configuration permissions





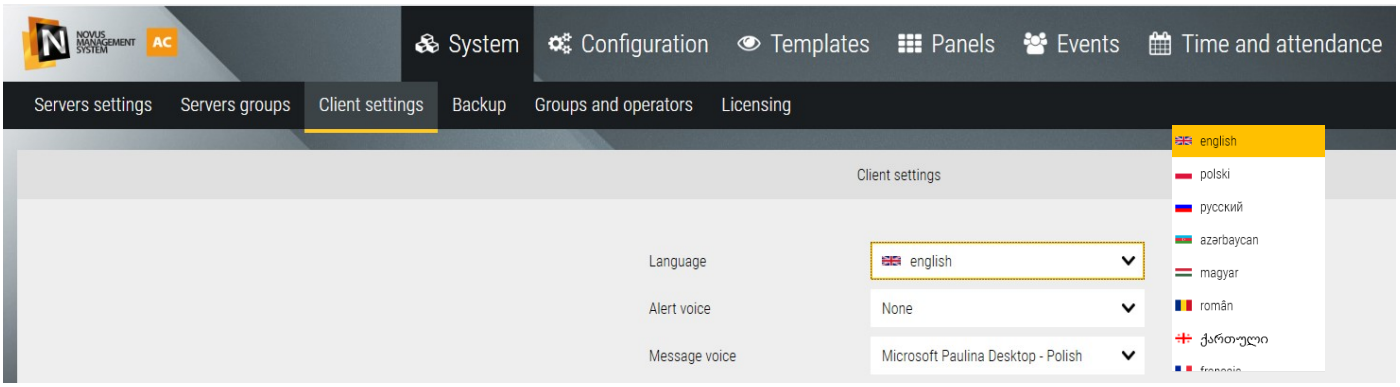
In this tab, set which items from the program's menu will be accessed by operators from this group. The administrator has full read, modify and delete access. For the *Security* group, most often only selected menu items with the *Show* attribute are left.

Devices permissions



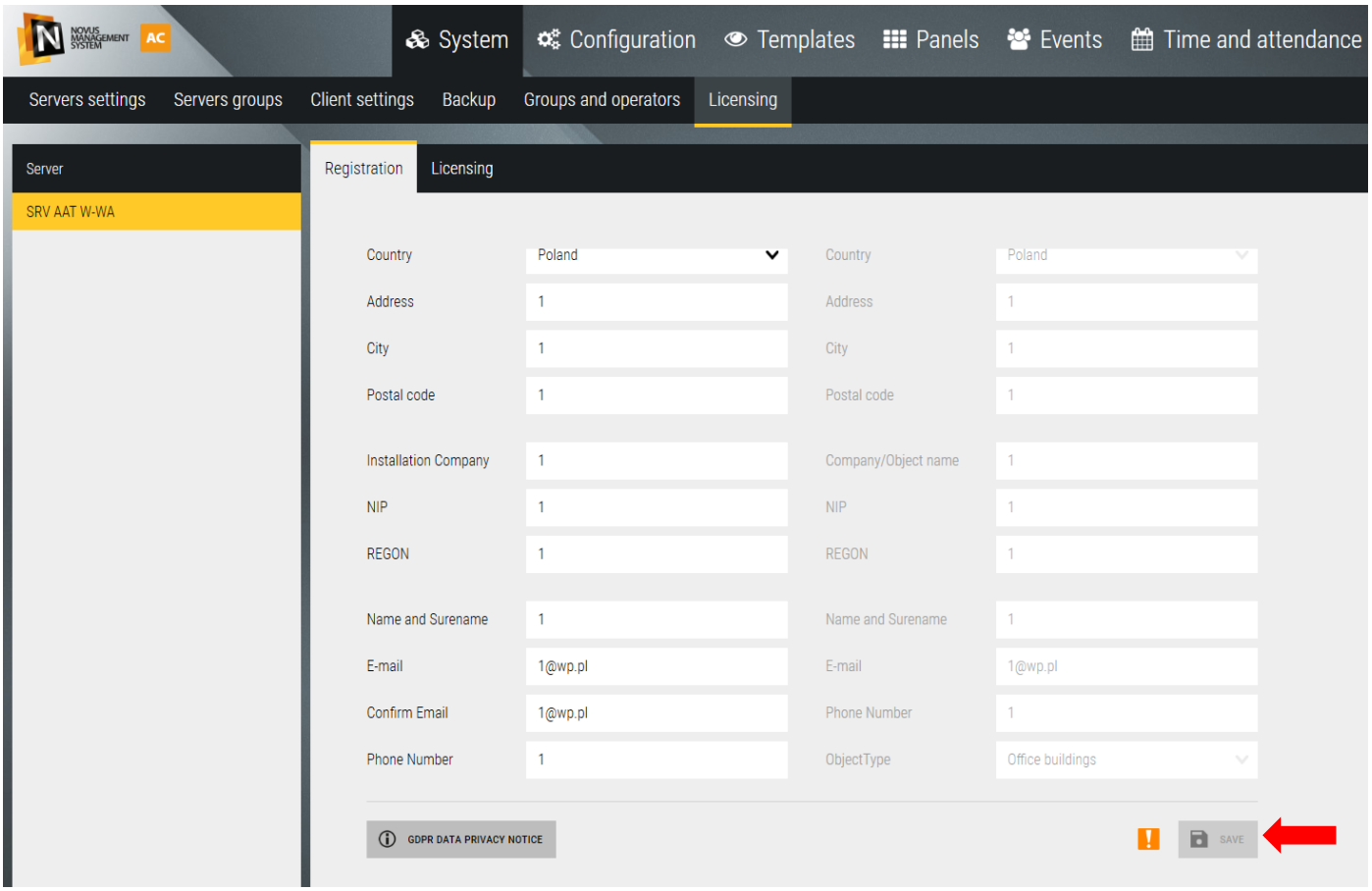
In this tab, set which system devices operators from this group will have access to perform certain operations on them. The administrator has full access to all operations. For the Security group, most often only selected items related to basic operations are left, e.g. Unlocking/locking doors.

8.2 Client setting (operator workstation)



In this tab you can set the language of the program menu for the operator. You can currently choose one of four languages: English, Polish, Russian or Azerbaijani. Other options are for settings related to alarm signaling.

8.3 Licensing

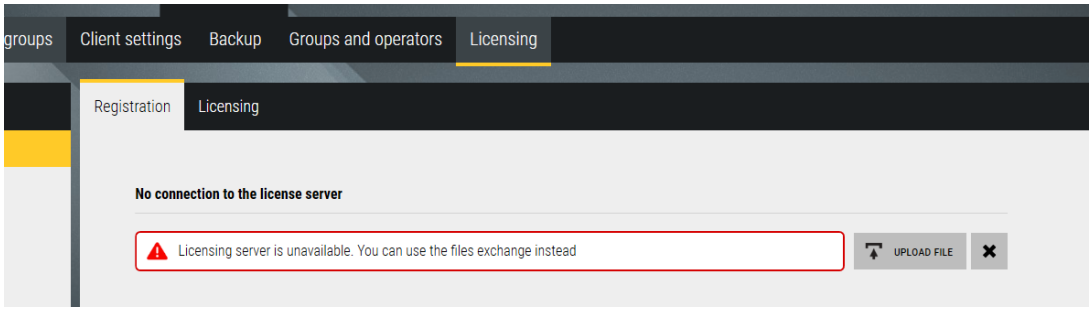


The use of NOVUS MANAGEMENT SYSTEM AC requires its registration and activation of the corresponding licenses. Activation of licenses is possible only after registering the program.
To register the program, fill in all the required fields shown in the image above.

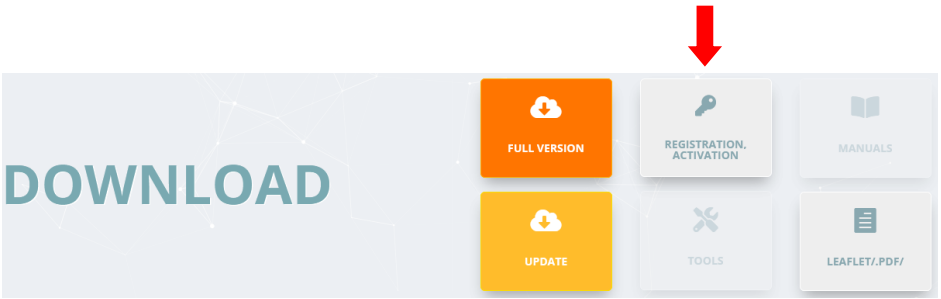
NOTE!
Once the registration process is completed, editing the data in the License User Data section will not be possible. In order to modify these data, please contact AAT SECURITY SYSTEMS Ltd. via e-mail address: kontakt@aat.pl.

When the computer on which you are registering has access to the Internet to complete the registration process, select the REGISTER button.

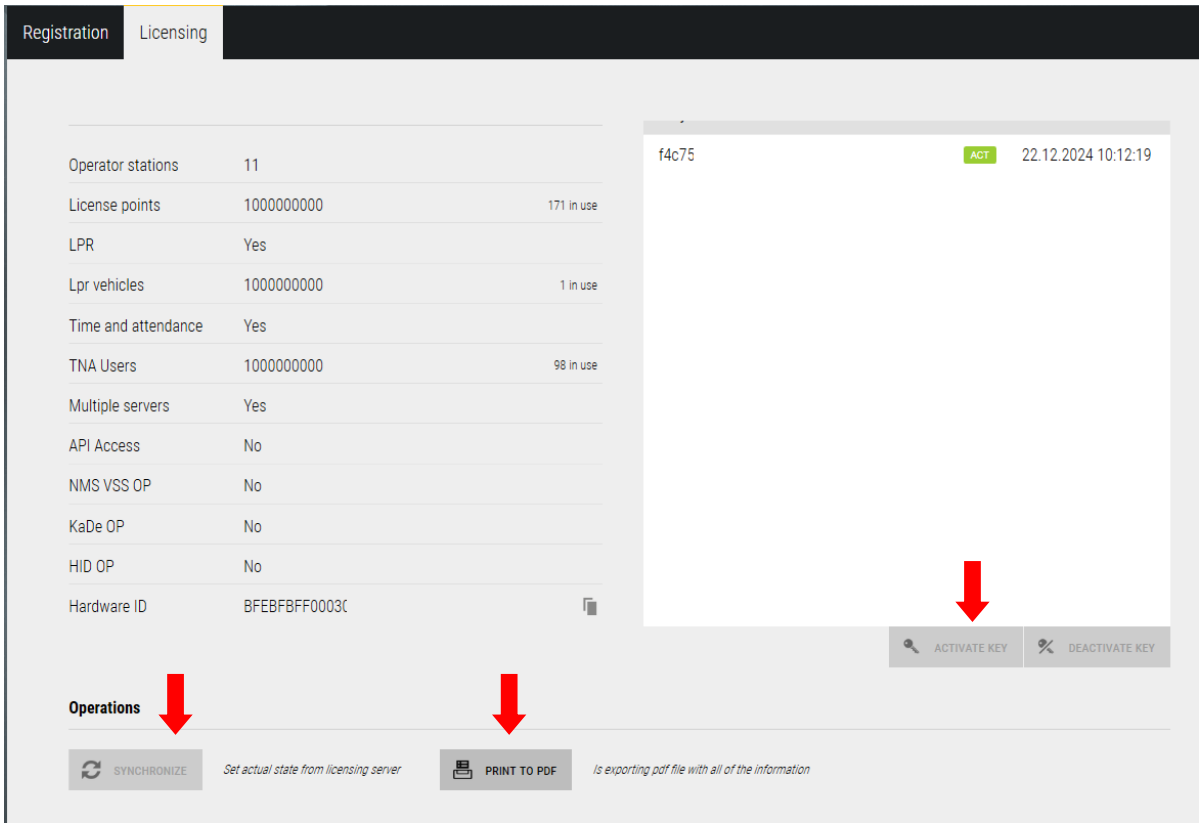
If you register from a computer without Internet access, the following option will appear in the *Upload File* window.



To register without access to the Internet (offline registration), fill in all the required fields and then select the SAVE button. A request.nlic file will be generated. The file should be transferred to a computer with Internet access and open the website https://nmsac.aat.pl/pl, then in the DOWNLOAD section select REGISTER, ACTIVATE and upload the request.nlic file according to the instructions given on the website.



When the process is successful, a response.nlic file will be generated in the response, which must be transferred to the computer to which you are registering and uploaded after selecting the option Upload FILE. Once this is done, the registration process is complete. In the System/Licenses menu, the Licenses tab will appear, containing information about the licenses of the computer unit in question.



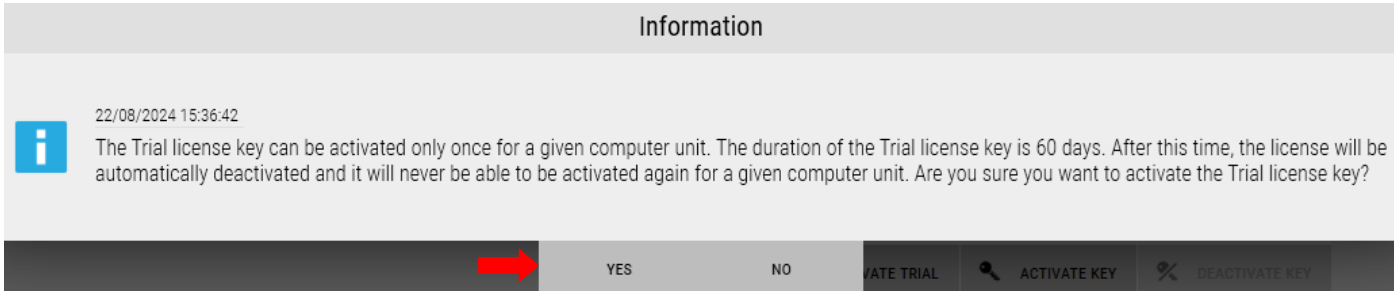
Selecting the SYNCHRONISE option downloads information about the computer unit from the license server (if the computer on which you are synchronizing has access to the Internet. Otherwise, a request.nlic file will be generated. To complete the synchronization process, follow the same steps as described for the registration process without Internet access (offline registration). If it has been registered in the past, a TRIAL license was activated for it, or there are active paid licenses, this information will be downloaded to the software. For example, if NOVUS MANAGEMENT SYSTEM AC software has been uninstalled and reinstalled, using the *SYNCHRONIZE* button will load all registration and license information.

The PRINT TO PDF option allows you to generate a PDF file containing license information for a given computer unit.

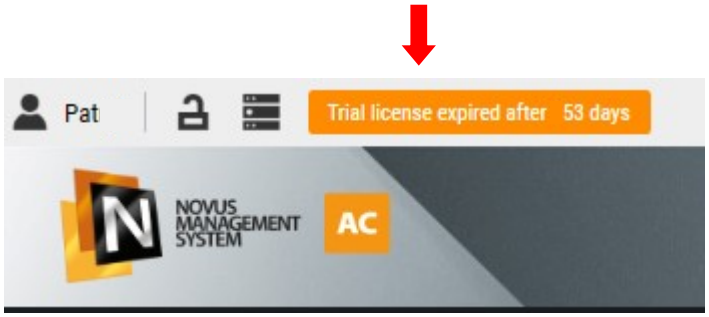
TRIAL license activation

A TRIAL test license is available to test the program's features. The duration is 60 days. To activate the TRIAL license, select the ACTIVATE TRIAL VERSION option indicated in the figure on the previous page. The following message will appear, select YES to continue.

If the computer currently has access to the Internet, the TRIAL license will be activated. Otherwise, a request.nlic file will be generated. To complete the license activation process, follow the same steps as described for the registration process without Internet access (offline registration) on the previous page.

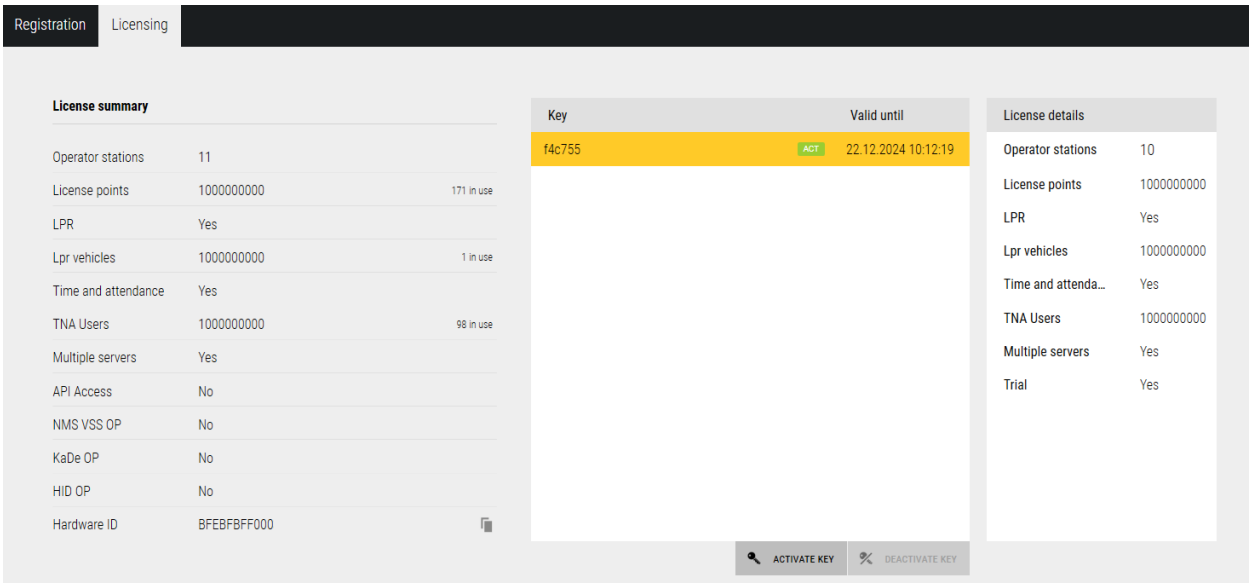


If paid licenses have not been activated, after the expiration of the TRIAL license period, all devices added to the system will be disconnected, but the system configuration will not change. Once the corresponding paid licenses have been purchased and activated, the ability to establish communication with the devices will be restored. Information about the time remaining until the expiration of the TRIAL license is displayed in the upper left corner of the program interface.



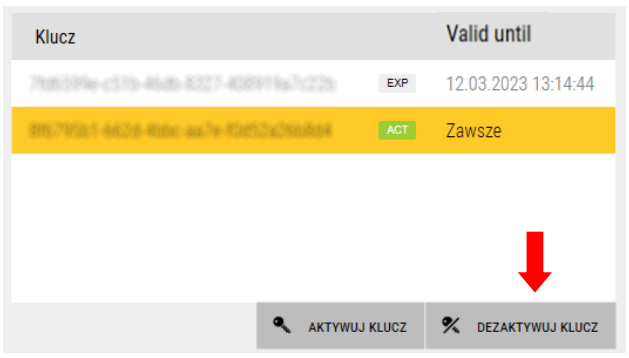
Activation of paid license key

The licenses are based on strings and do not require dongles.
After receiving a paid license key to activate it, select the ACTIVATE KEY option indicated in the figure below. A window will appear as below, where you need to type/paste the copied paid license key and select OK. If the computer on which you are activating has access to the Internet, the license key will be activated. Otherwise, a request.nlic file will be generated. To complete the license activation process, follow the same steps as described for the registration process without Internet access (offline registration) on the previous page.
A paid license can only be activated on one computer.
Information on the license keys assigned to a particular computer can be found in the window shown below. After selecting a license key from the list, the window on the right will display detailed information. On the left is a summary of the active licenses, their use on the system and the hardware ID.

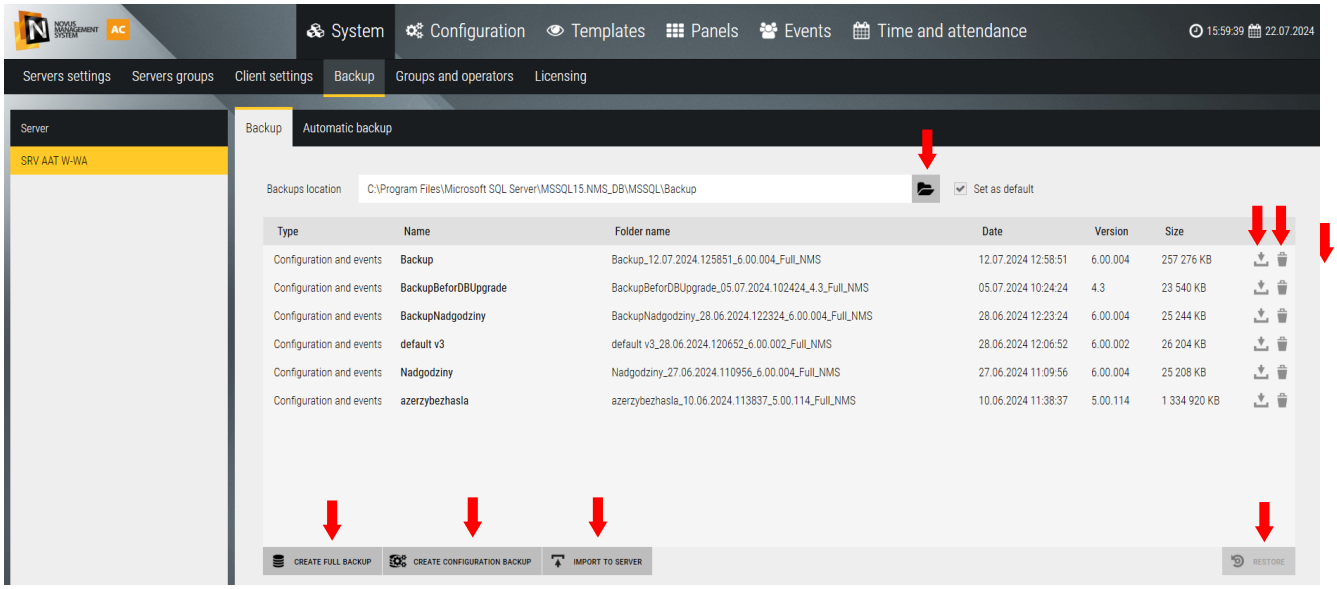


Deactivation of paid license key

NOVUS MANAGEMENT SYSTEM AC allows you to deactivate a paid license key from the computer on which it is currently activated and re-activate it on another computer. To deactivate a paid license key, select the key from the list in the System/Licenses/Licenses menu and then the DEACTIVATE KEY option. If the computer on which the activation is performed has access to the Internet, the license key will be deactivated. Otherwise, a request.nlic file will be generated. To complete the license key deactivation process, follow the same steps as described for the registration process without Internet access (offline registration). After completing the deactivation process, the license key can be activated on another computer.



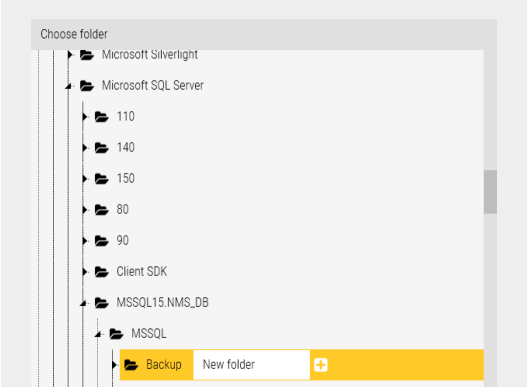
8.4 System backup



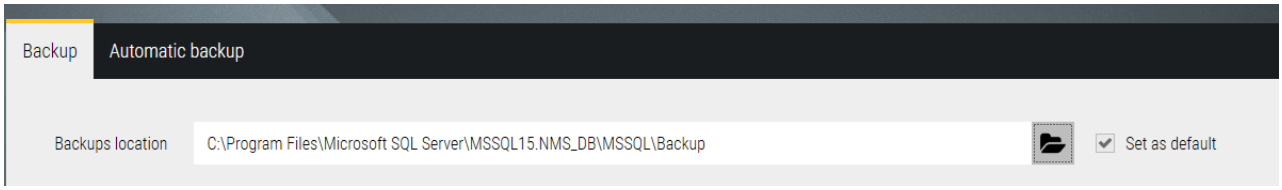
In this tab you can make or restore a backup of the system.

Create a backup

At the top of the window, the system backup location field is displayed. We can change the default path by clicking on the folder icon.



You can point to a folder of your choice on the current drive, flash drive or mapped drive of another computer and select it as the default location. You can make a copy of events and configuration or only configuration by clicking on one of the buttons at the bottom of the window. The beginning of the copy name can be changed. The default copy name includes a date and time stamp for its generation and the type of copy.



After the copy is made, it appears in the list. On the right side there is an icon for deleting it and an icon for retrieving the copy from the location where it is located.

The IMPORT TO SERVER option allows you to import the backup file for restoration.

Restoring a backup

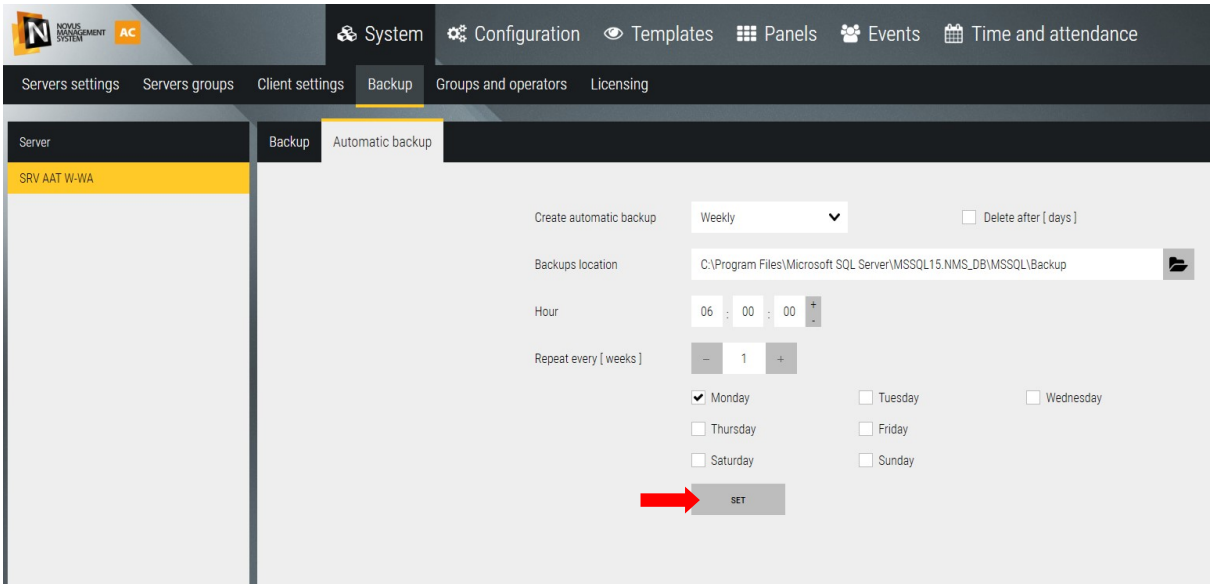
To restore a copy of the system, select it from the list (if the copy file is not on the list, use the IMPORT TO SERVER option), and then select the RESTORE button.

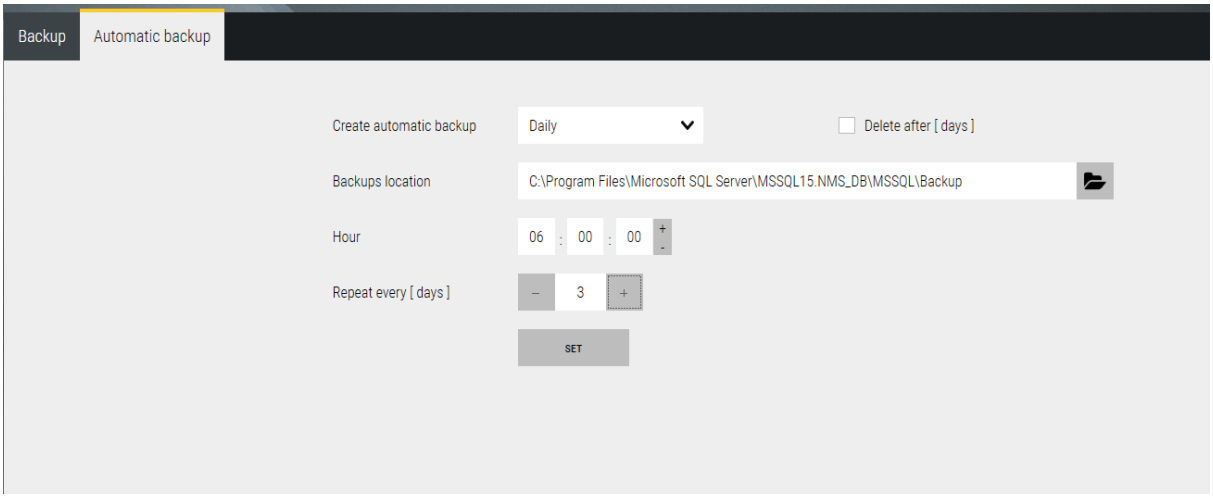
It is also possible to restore the initial state of the system (clearing the database) - for example, after testing the system. To do this, restore the backup under the name Default Settings, which is automatically generated after installing the system.

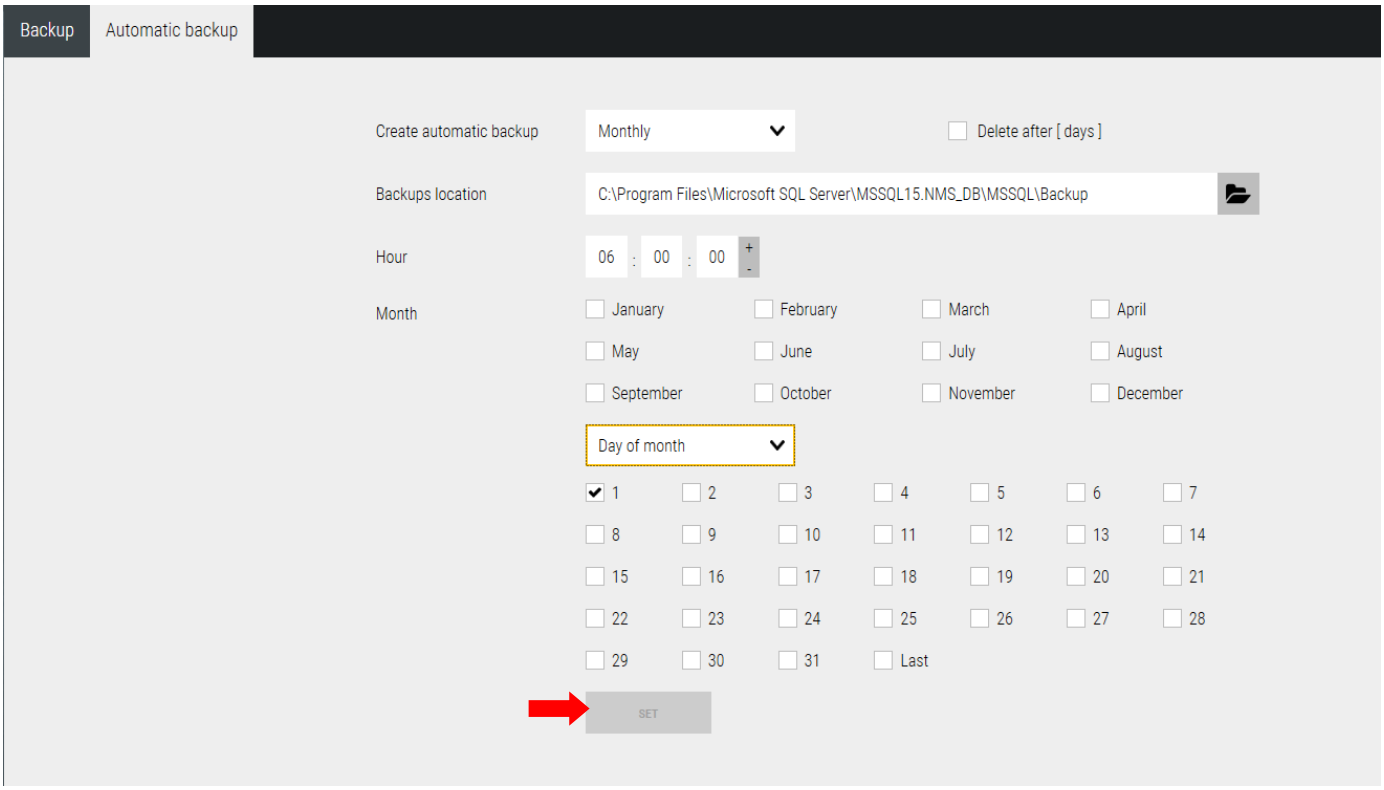
Automatic backup

A window where we can set parameters for automatic backup.

An automatic backup can be created and saved on a daily, weekly or monthly basis.







Section 9. Advanced Functions

9.1 Multi server

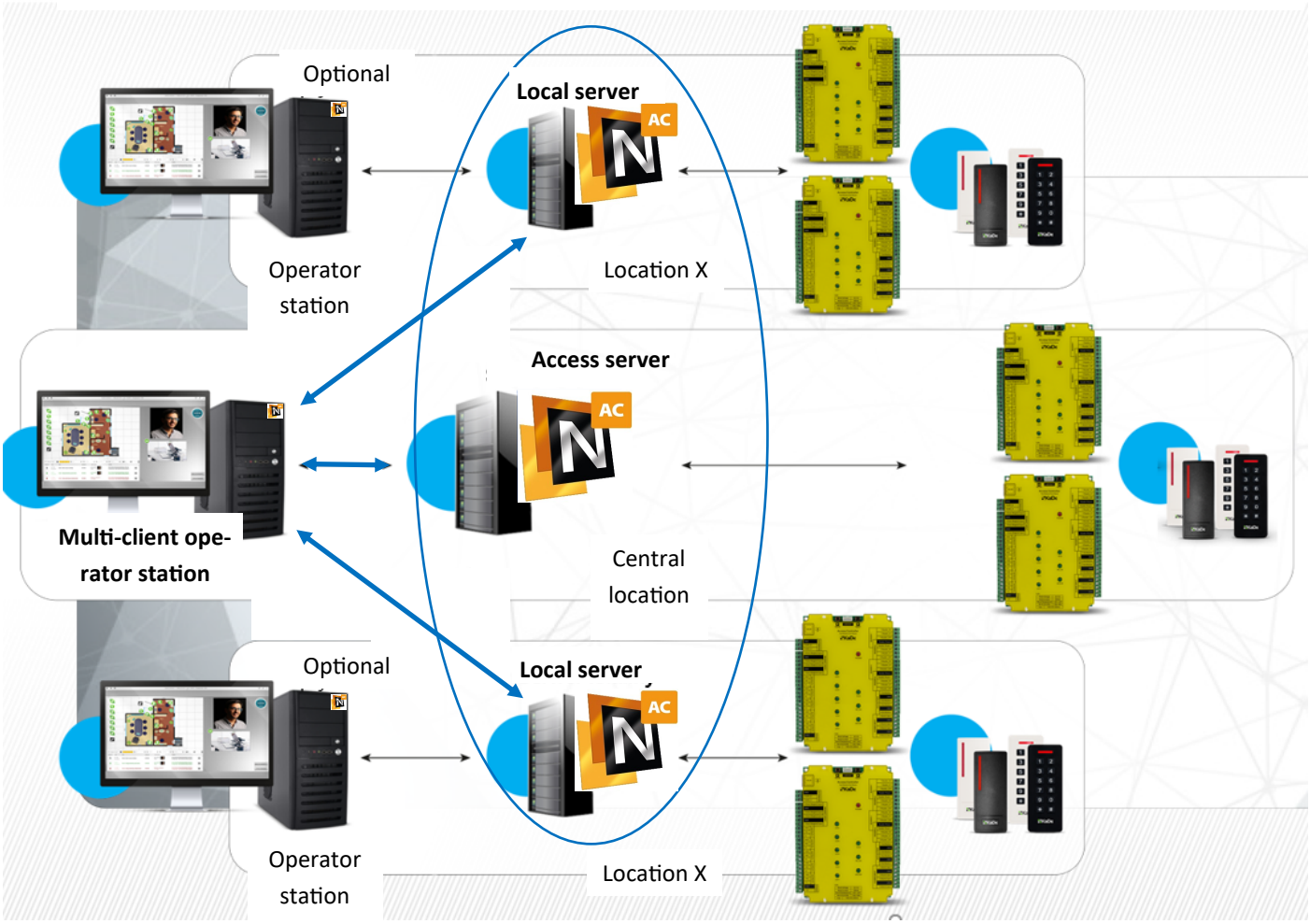
This options is available as a paid license in 4.0 version or higher. It is mainly designed to support systems in multiple locations, but can also be used to support large systems in one location especially if a large number of VSS devices are installed.

NMS AC servers installed in each location support local integrated systems and communicated with local operator stations as in the system without multi-server. This option allows you to add selected servers to group to configure and monitor these subsystems simultaneously from one or more client station (multi-client). This causes that loss of communications with a given location does not affect the work, configuration and monitoring of local systems. This is not possible with a system with one central server. Definitions used in the diagram and descriptions below:

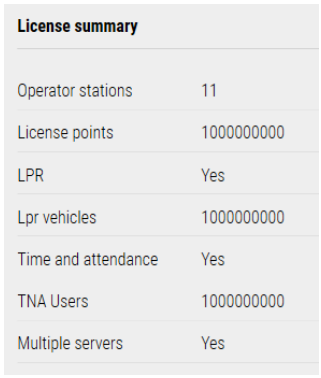
Access server - one server in system with a multi-servere license added, where is group made of local servers (each of them must have an added multi-server license). In the system and even within one group there can be more than one access server.

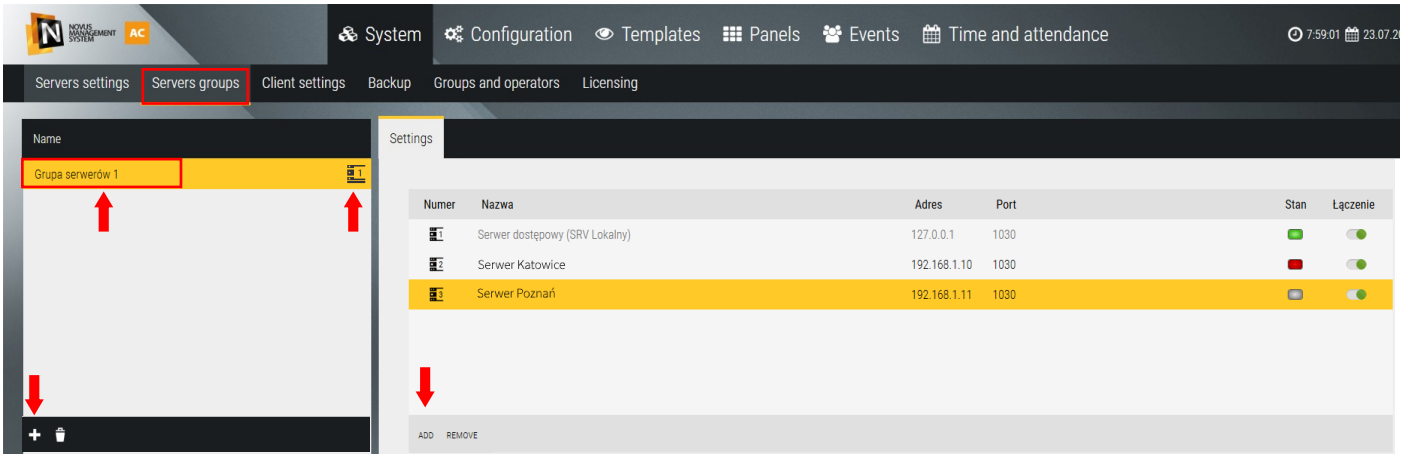
Multi-client - operator station (NOVUS MANAGEMENT SYSTEM AC Client) logged into the access server by an operator with a common login to all servers in the group.

NOVUS MANAGEMENT SYSTEM AC - system with multiple servers



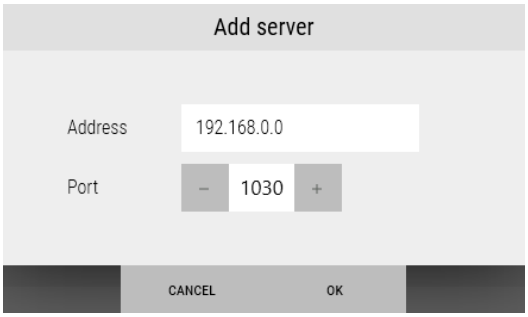
If you want to create a group of servers then the purchase of an additional NOVUS MANAGEMENT SYSTEM AC SRV v5 license is required for each of them . After adding the purchased license to the NOVUS MANAGEMENT SYSTEM AC server, a new tab - Server Groups - will appear in the SYSTEM tab and new icons in the configuration windows with the number of the server to which the item belongs

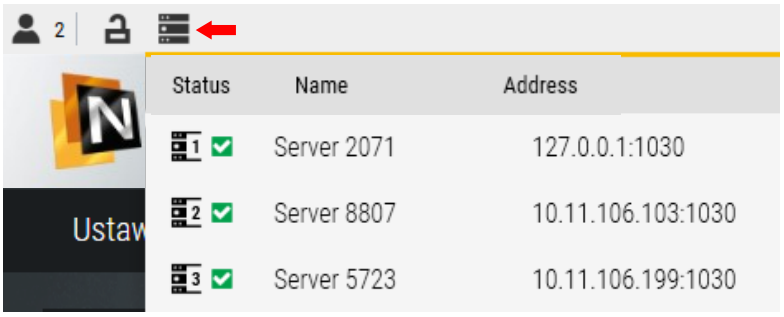




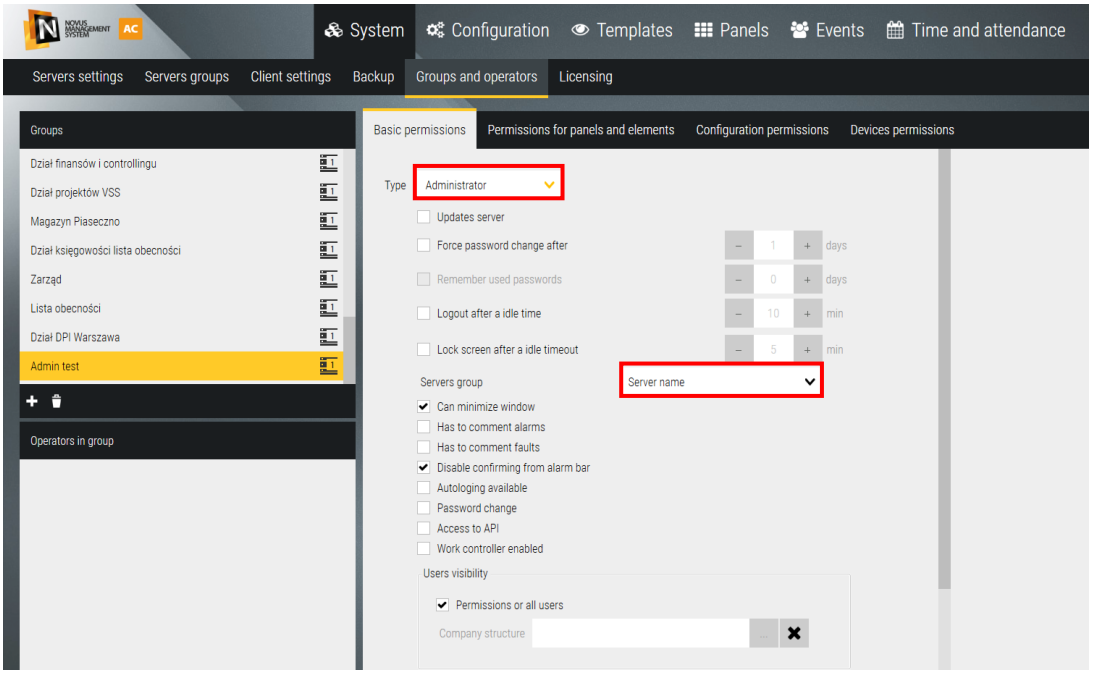
Add - To create a server group, click on the “+” (Add) button in the lower left corner of the window.
Then enter the name of the defined server group in the name field.

Once the group is defined, servers to which multiserver licenses have been added can be added to it.
To do this, click on the *Add* button in the right window:
After entering the address and clicking OK, the server will appear in the list. If it is running on a network available to this group, the icon to the left of the name will light up green. It will also appear in the list on the top left bar after pointing the mouse at the server list icon. You can define more than one server group.

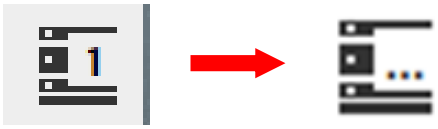


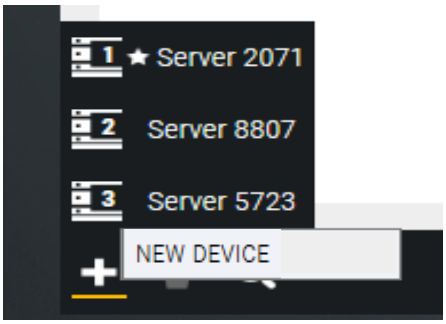


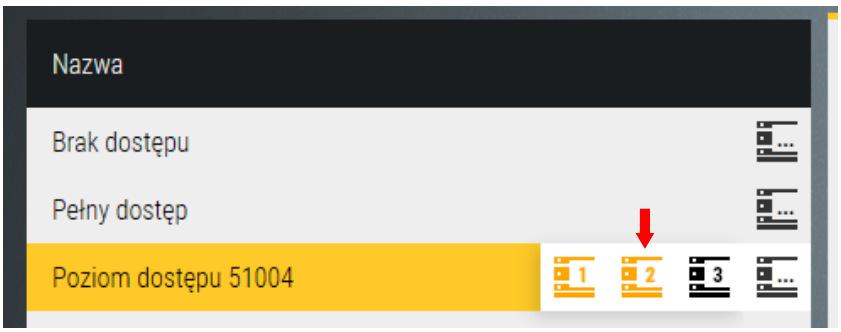
After creating a group of servers, define an operator assigned to that group on each server. This will allow you to access subsystems within the group after logging on to one of the client stations within the group. After adding a multi-server license, a new option - *Server Group* - appears in the defining operators tab.



From the drop-down list, select a group of servers to which the operator will have permissions. After logging in, the operator, depending on the assigned permissions, will be able to add, edit and delete items assigned to servers and specific operations on them (*e.g. Unlock door - in any location).* When adding new items, the operator can select the server to which he adds the new item. An asterisk indicates the access server on which we work locally. A new logical element added to one server (e.g., Access Level) can be assigned to the other servers in the group by hovering over and clicking with the mouse pointer on the icons with server numbers. The assigned servers are displayed in orange and the icon at the end of the list changes to:

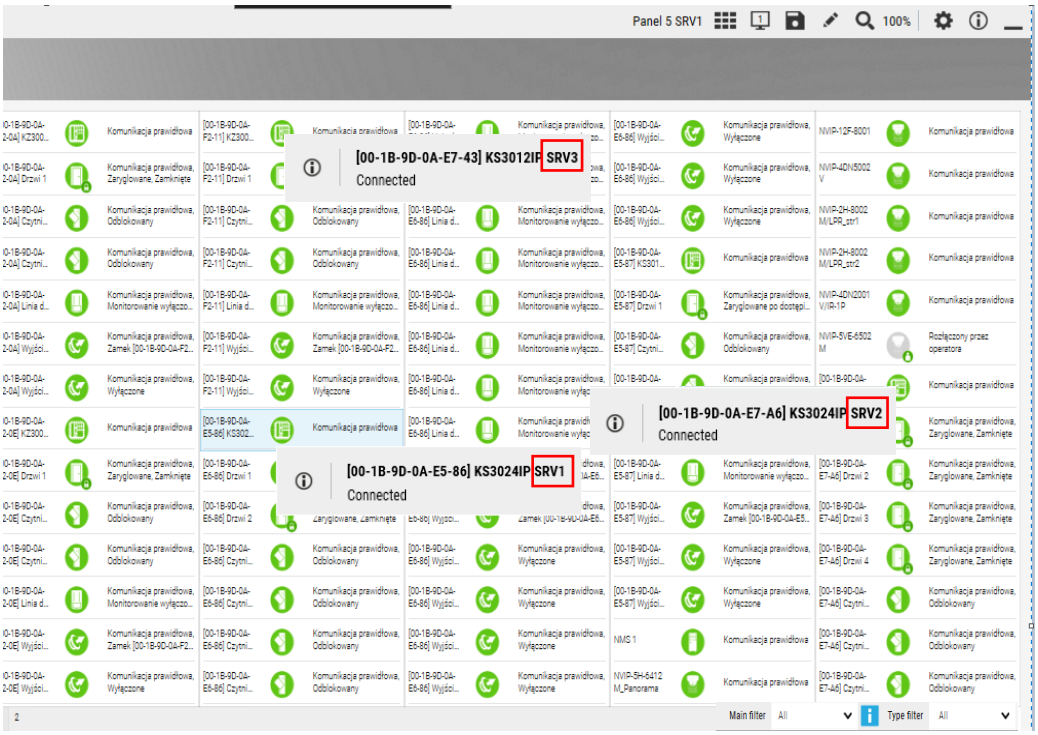






Selected default system items that are the same on servers are in the lists in the left window only once regardless of the number of servers in the group. This applies, for example, to schedules, access levels, holidays.

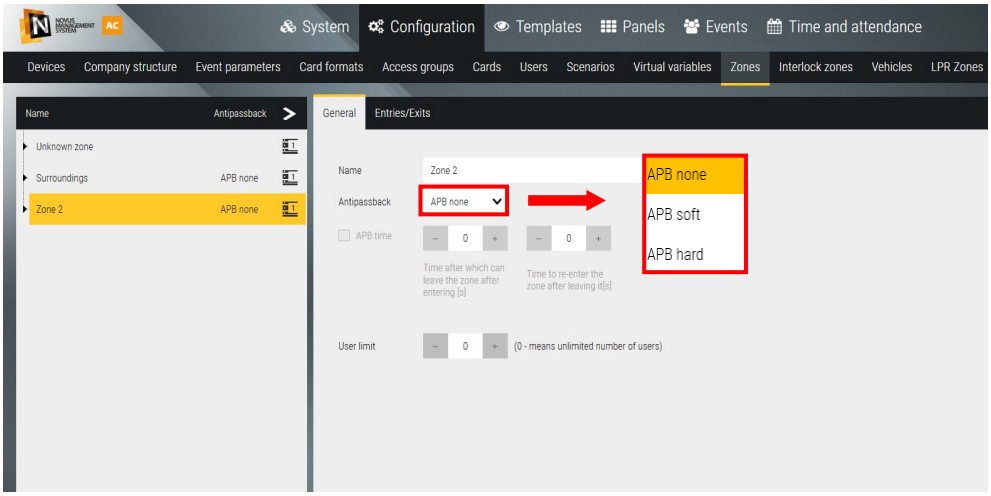
Similarly, this is the case with the synoptic table.



A similar rule applies to the current events stack, where events from all servers in the group can be displayed simultaneously.

9.2 Global zones

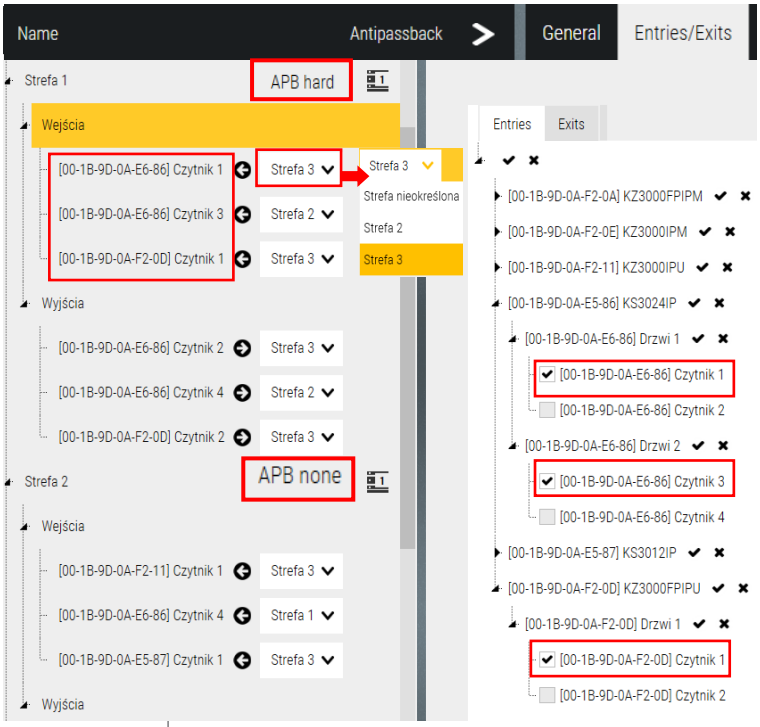
This option is designed to control the status of people and vehicles in areas covered by two-way access control. The global zone can include readers from many controllers, supports both hard, soft and timed antipassback. The function works only in online mode when the NOVUS MANAGEMENT SYSTEM AC server has communication with the controllers.



In a zone, you can set a limit of users, the exceeding of which is signalised by the color of the border on the panel and an appropriate response (such as blocking the entrance). You can also select the type of APB function - antipassback. The list displays the default Unspecified Zone, which contains a list of new users who have not yet moved around the facility. Before this functionality is activated, it contains all users added to the system database. Each time a card is read on a reader assigned to one of the zones and a door leaf is opened (violation of the door status sensor), the card (user) is rewritten to a new zone.

APB control can be assigned to selected zones that have been defined: *Soft, Hard* or *Timed*. *Hard APB* forces the card to be read at the entry and exit reader. *Soft APB* only generates a message about the wrong user location. *Time* APB restricts entry or exit from a zone for a specified period of time.

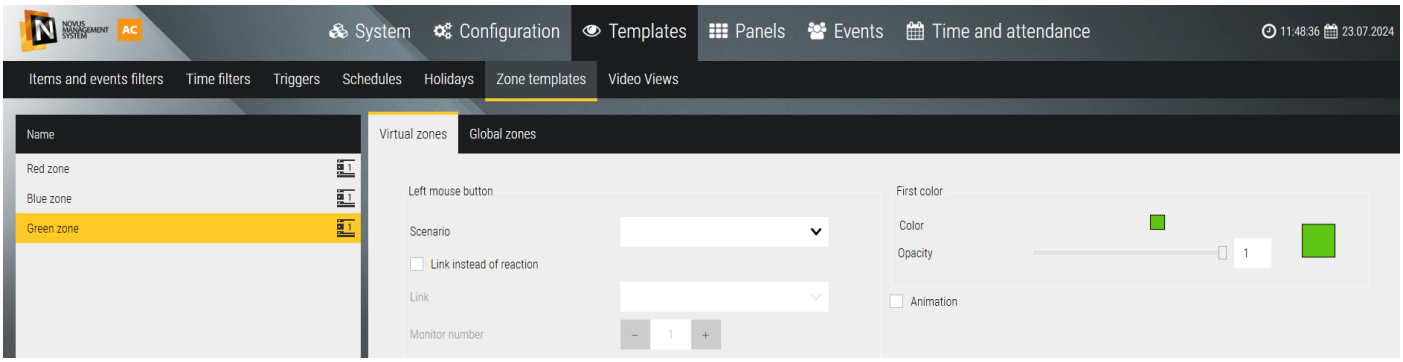
Before defining the zones, it is advisable to make a sketch on the plan of the facility or site, marking the periphery of the zones and the location of the entry/exit readers.



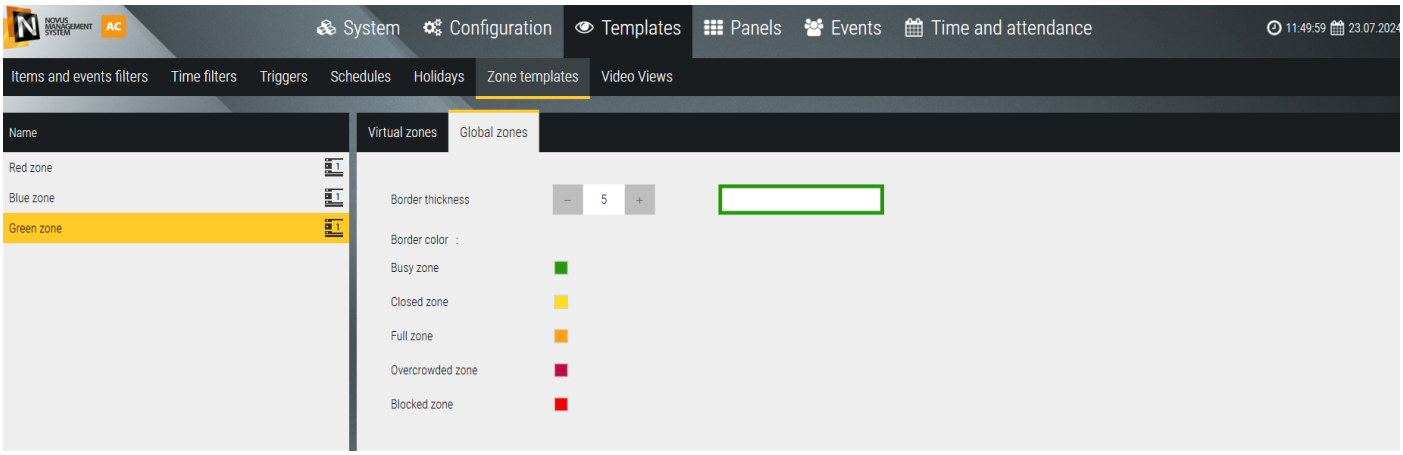
After clicking on the “Add” button, a new item Zone X appears on the list in the left window - we can assign entry and exit readers to it in the right window. After assigning entry and exit readers, go to the left window and assign to each reader from the drop-down list the zone in which the reader is located. This allows you to create a structure of mutual location of zones and transitions between them. After defining the zones and saving to the base to the Panels tab and on the new panel proceed to visualize the defined zones.

Visualize global zones on panels

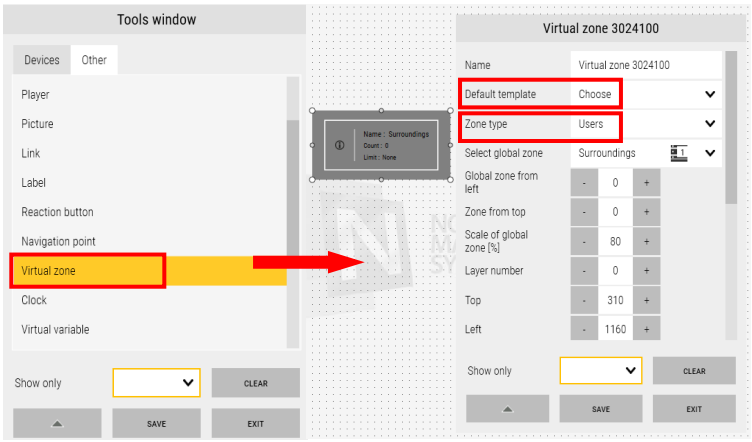
Global zones can be on panels to monitor their status and rewrite users on lists in zones if there is a need to organize their status. On panels, global zones are linked to virtual zone templates. Therefore, you should first define virtual zone templates to which global zones will be assigned on panels.



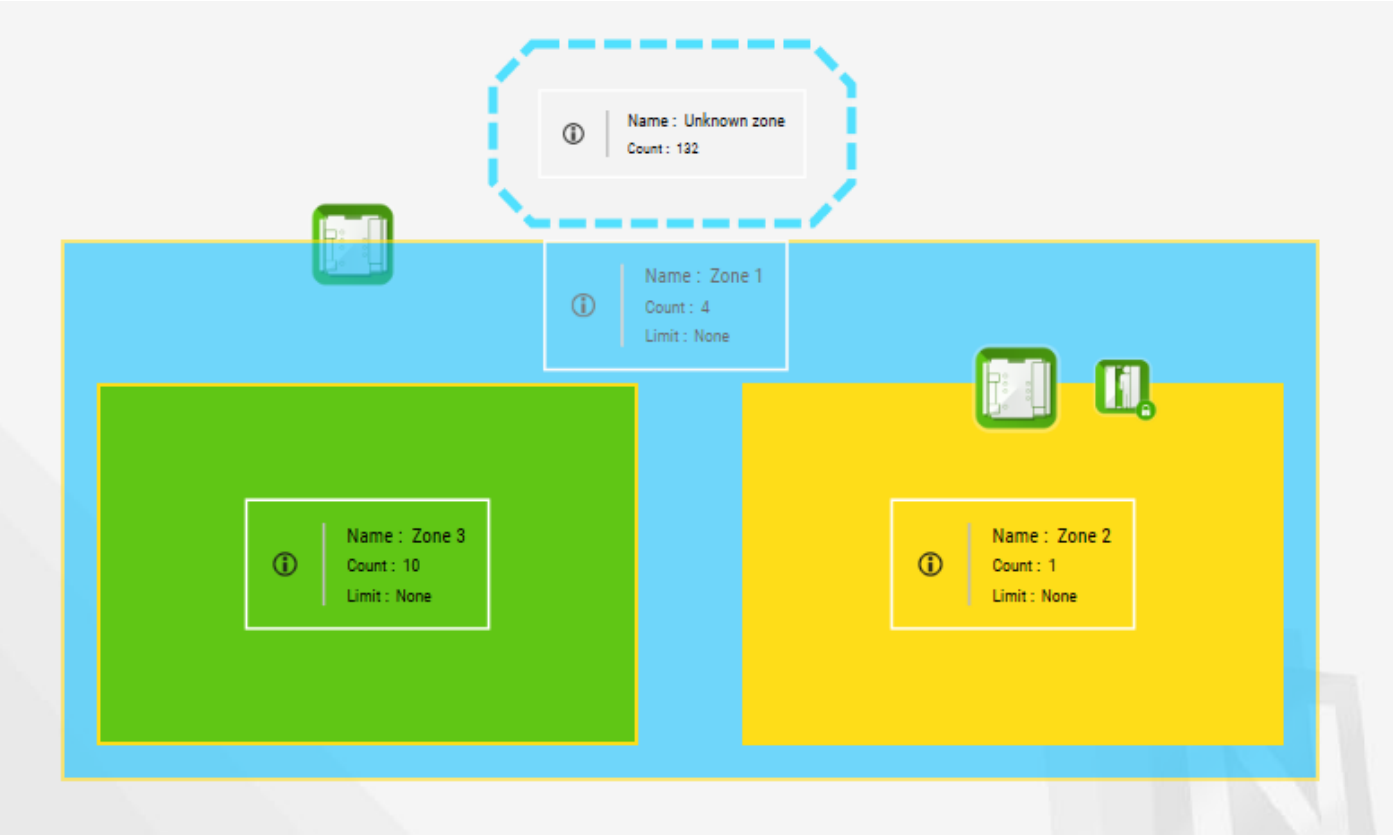
The parameters of the virtual zones are shown above. If you use them to visualize global zones, you need to select a differentiated background color. Next, go to the Global Zones tab and set the thickness of the border on the edge of the virtual zone, the color of which indicates the status of the zone according to the legend. Once on the panel, enter the editing mode and add a virtual zone, assign it a template and global zone

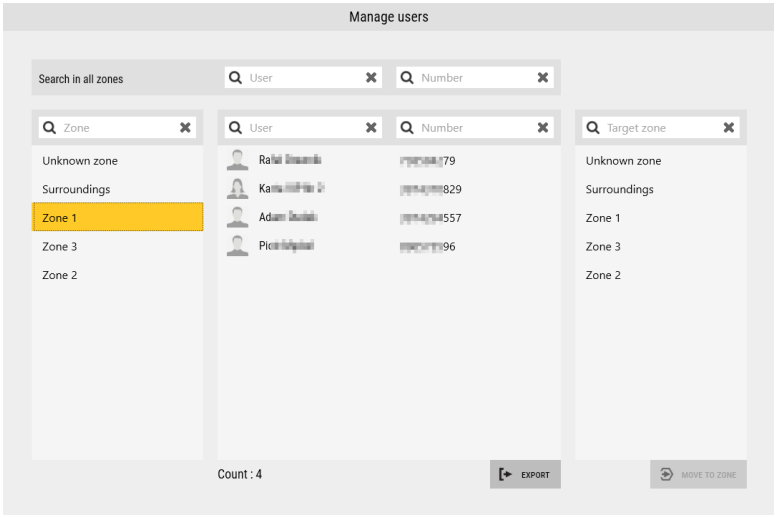


Then modify the parameters of the virtual zone and the global zone (location, size, scale) and save.



An example view after configuring three zones and applying items to them below.
When you left-click on the global zone icon, you will see a window as below:



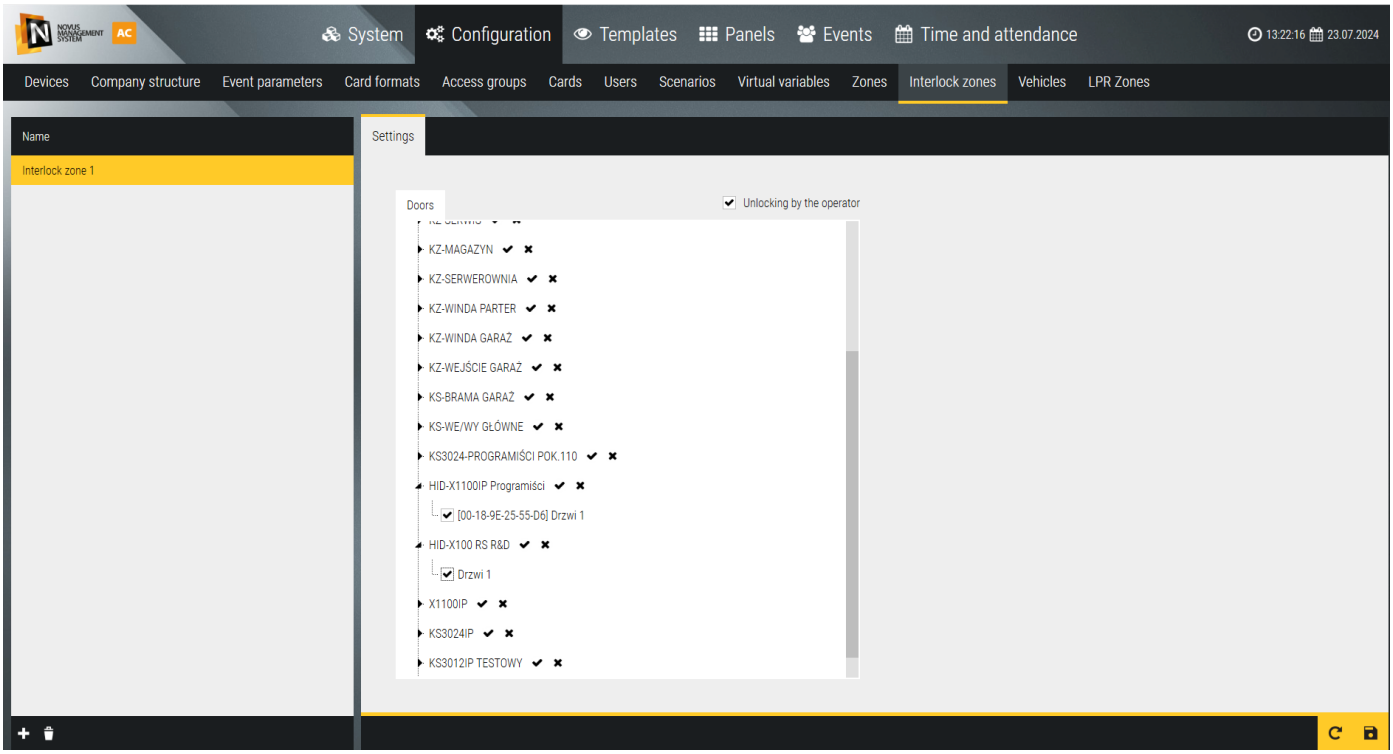


The window displays a list of registered people in the zone. After selecting one or more items in the list (with CTRL) and the zone in the right window, you can rewrite them to this area. You can also export the list of users to a file (*.CSV) and print it.

9.3 Interlock zones

This option is designed to control the closing and locking status of a group of doors. The doors can be controlled by different controllers. The function works only in on-line mode when the NOVUS MANAGEMENT SYSTEM AC server has communication with the controllers.

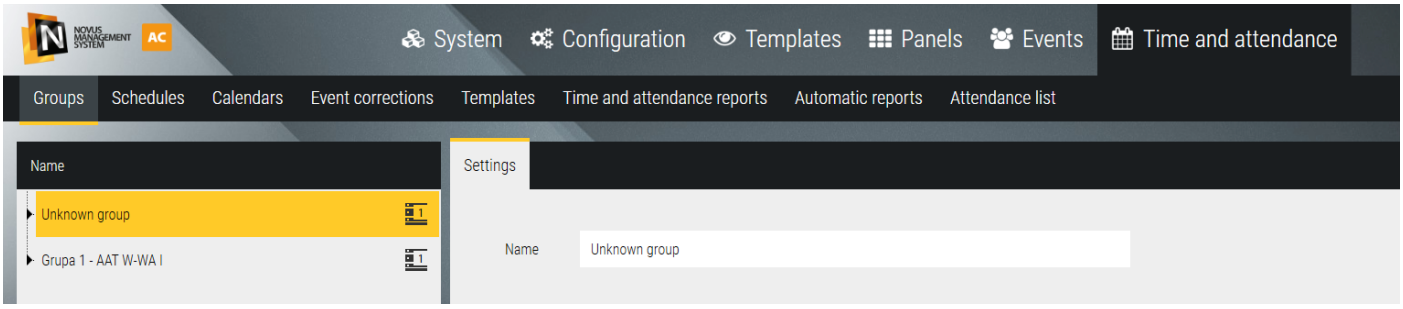
To define a door group for a particular lock, click on the + icon in the lower left corner of the window.



Unlocking by operator - checking this box allows the operator to unlock any door in the lock group even when others in the group are open or unlocked

9.4 Time and attendance

This option is available as a paid license (Trial 60 days available). It is designed for recording and accounting of working time based on events from T&A terminals and KD system readers assigned to T&A groups). To take advantage of this functionality, you need to purchase the appropriate licenses for the functionality itself (NOVUS MANAGEMENT SYSTEM AC RCP v5), the specified number of T&A users (NOVUS MANAGEMENT SYSTEM AC URCP v5) and to add time registration devices to the system (NOVUS MANAGEMENT SYSTEM AC PKT LIC v5). After adding the purchased license to the NOVUS MANAGEMENT SYSTEM AC server, in the Time Registration tab, the possibility of defining T&A groups in terms of assigning input and output terminals and readers to each group is unlocked. The number of such defined groups is not limited. T&A group can include readers from multiple terminals and controllers. Only events from readers assigned to T&A groups are taken into account for accounting working time.

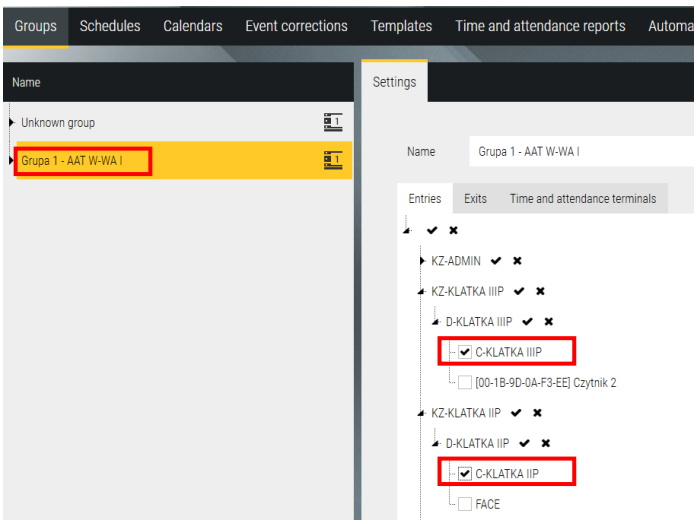


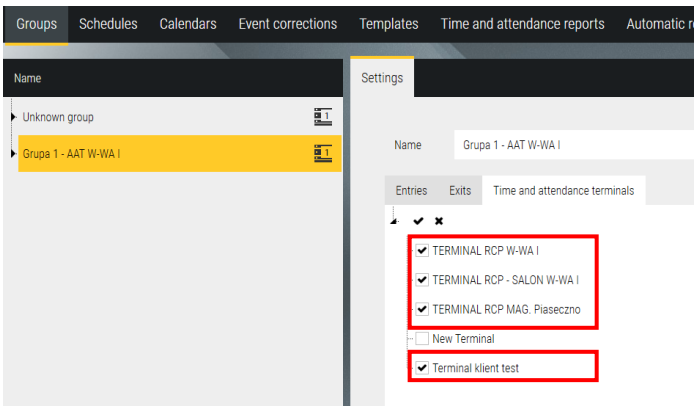
The T&A terminal allows registration of additional I/O during work time: for break, business, private. Registration of these additional I/O during work time is also possible on KD readers - one reader for one type of I/O.

Groups

The list displays the default Unspecified Group, which contains a list of all readers assigned to T&A groups, along with information on which group they belong to. After clicking on the “Add” button on the list in the left window, a new item Group X appears - we can assign input and output terminals and readers to it in the right window. After assigning input and output terminals and readers, they are displayed in the structure in the left window. T&A groups defined in this way are assigned to users in the *Configuration/Users/Time Registration* tab.

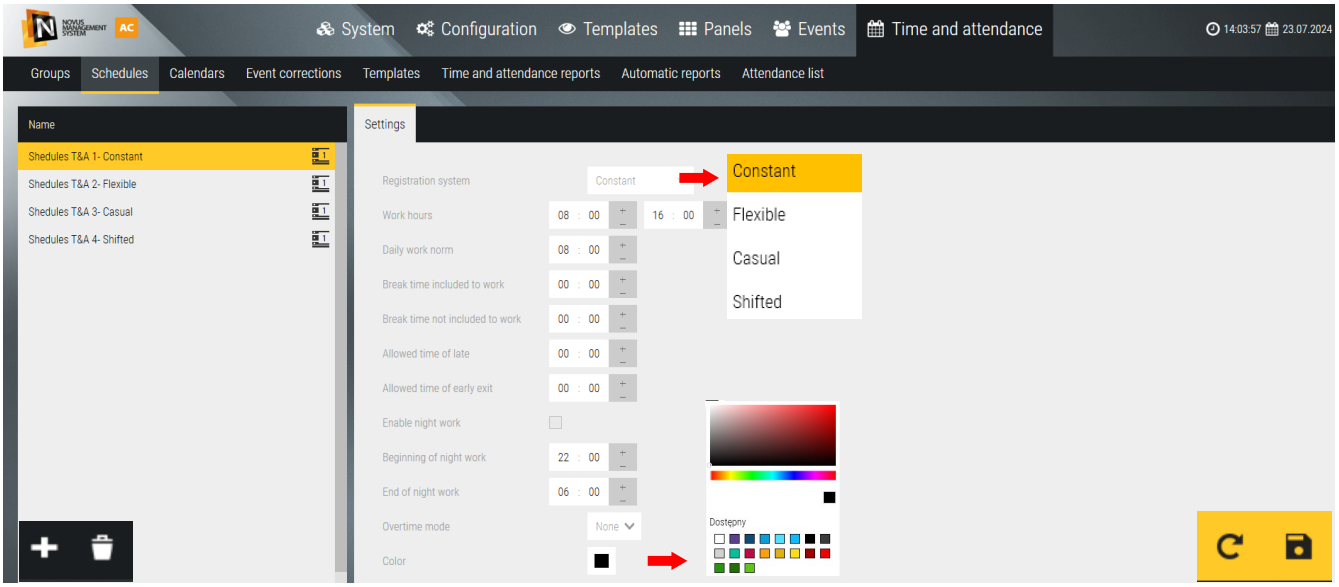
Terminals should be added using the *Time Terminals* tab.



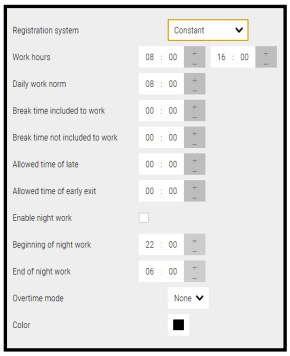


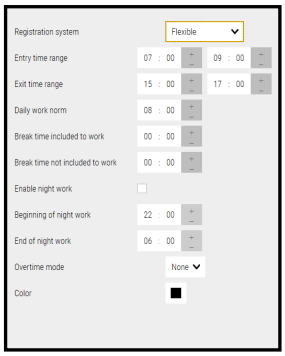
Schedules

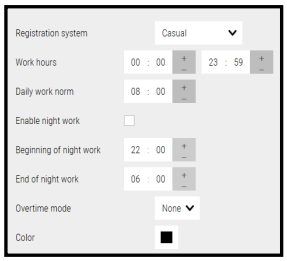
T&A schedules are needed to account for working time in the selected period according to the established daily norm. After clicking on the "+" Add button in the left window, a new schedule appears with a default name that can be edited.

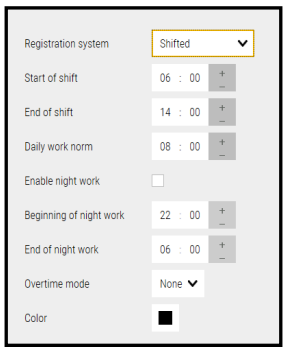


Next, in the Settings tab, select the type of registration system: *Constant, Flexible, Casual, Shift.*









Defining the schedule depends on the choice of registration system:
Constant - means that the employee has fixed working hours with a break.
Daily work norm - daily working time norm.
Break time - the time counted down from the registered work time in the report generation process.
Allowed time of late, of early exit - means that the employer allows late arrivals and early departures.

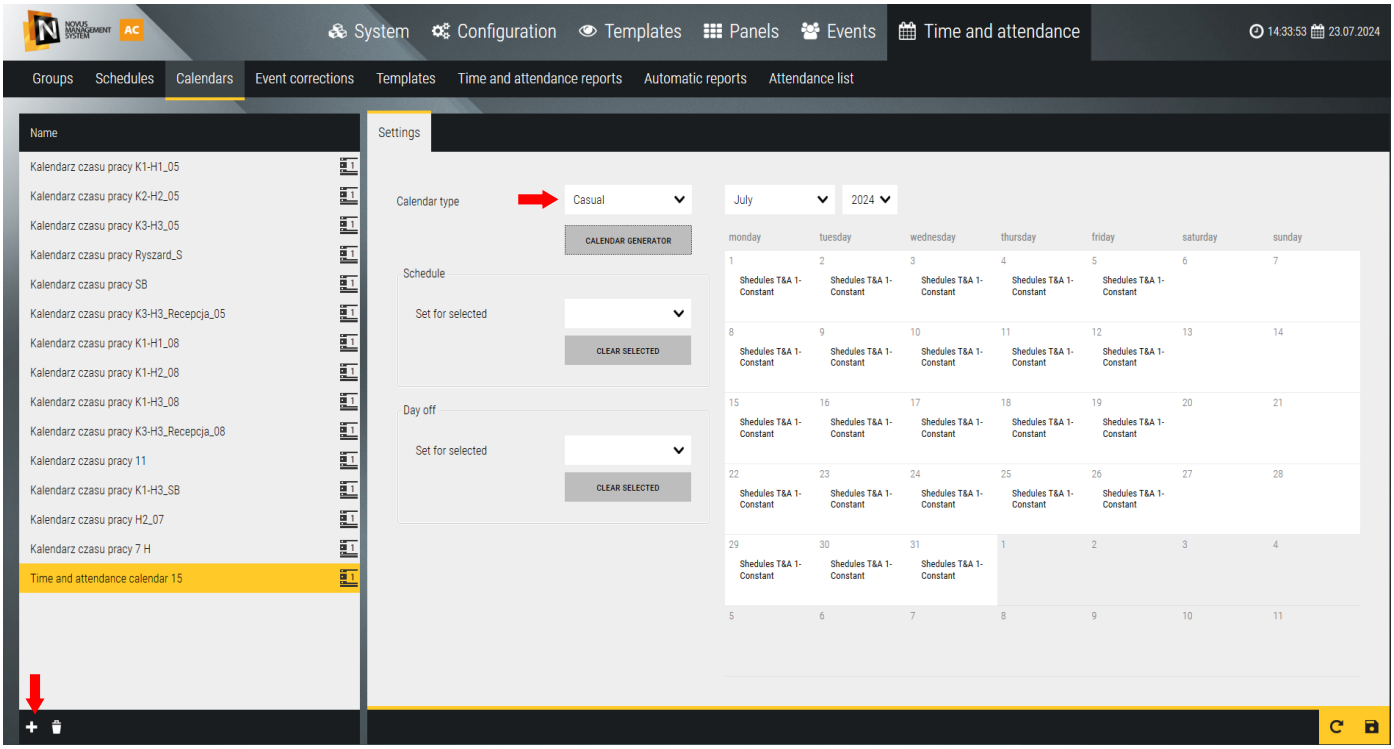
Flexible - means that the employee will have a daily norm of working time to calculate the monthly norm (after multiplying by the number of days to be worked in the month according to the calendar).
Entry time range - set the time range in which the employee should register the start of work. Only registrations from this time range will be included in billing. Earlier registration before the entry time range will result in billing from the beginning of the entry time, later registration (after the end of the entry time) as absence.
Exit time range - set the time range in which the employee should register the end of work. Only registrations from this time range will be included in billing. A later registration (after the end of the exit time) will result in billing at the end of the exit time, an earlier one (before the beginning of the exit time) as an absence.
Daily work norm - is used to calculate the monthly norm based on the calendar, which is displayed in the report
Break time (includet/not includet) to work - the time deducted (or not) from the registered working time in the process of report generation.

Shifted (up to 4 shifts, configuration) - means that the employee will have a set daily working time norm. Configuration of working time for the shift system is done in the Calendars tab. Sample schedule templates for a system with three shifts are shown in items 4, 5 and 6.
Color - color of the schedule description to be displayed in the calendar, important for shift system.

Casual - means that an employee can work any hours and is billed monthly. During each day, he can work for a different number of hours. The hours worked during each day are added up and related to the norm for the period based on the calendar.

Calendars

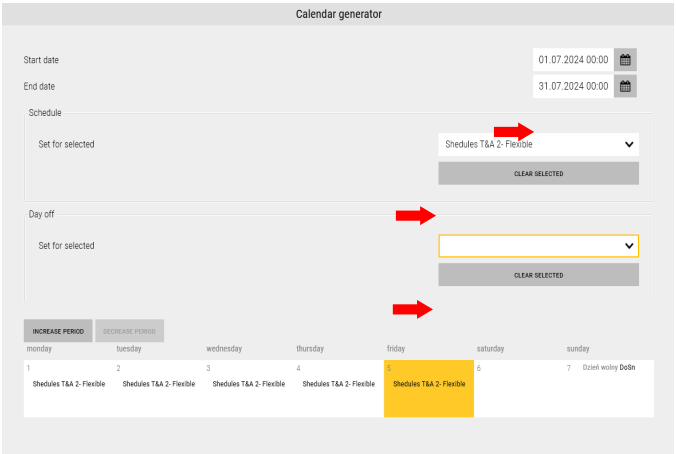
Calendars are needed to account for working time in the set period according to the norm. When defining them, you need to assign a selected schedule to each working day of the week. The calendar is then assigned to the user. After clicking on the "+" *Add button* in the left window, a new calendar appears with a default name that can be edited.



Settings

Type of calendar - Casual or Shifted after selecting Shifted in the Selected schedule item, we can choose defined schedules of Shift type, after selecting Casual schedules of Fixed, Flexible and Casual type. In the field next to it, select the month for which we will generate a calendar with work schedules, and finally the year. The window also displays tiles symbolizing each day of the month.

We can assign schedules to individual days manually or using the report generator.



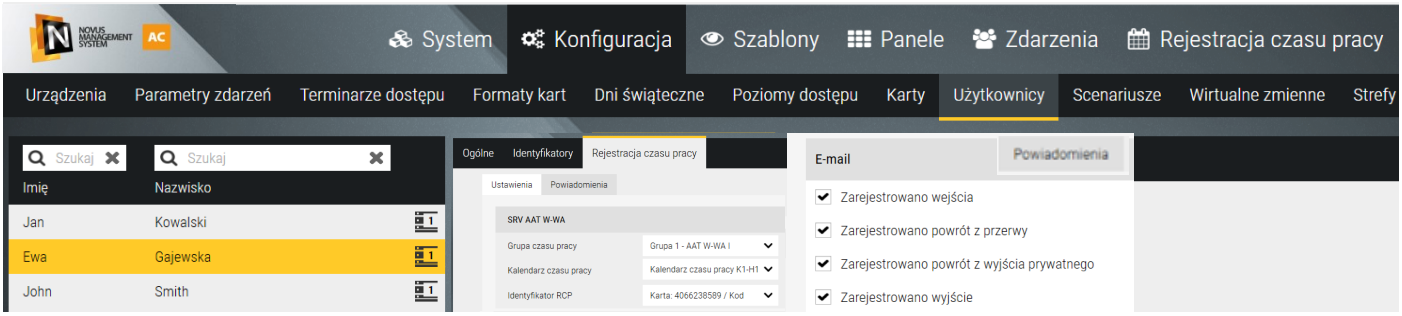
Manual mode - to assign the selected schedule manually, click on a particular day with the left mouse button, with the right one - to remove it

Automatic mode - click on the *Calendar Generator* button.

- set the start and end date of the calendar
- select the schedule from the drop-down list
- by left-clicking on the days of the week add the selected schedule

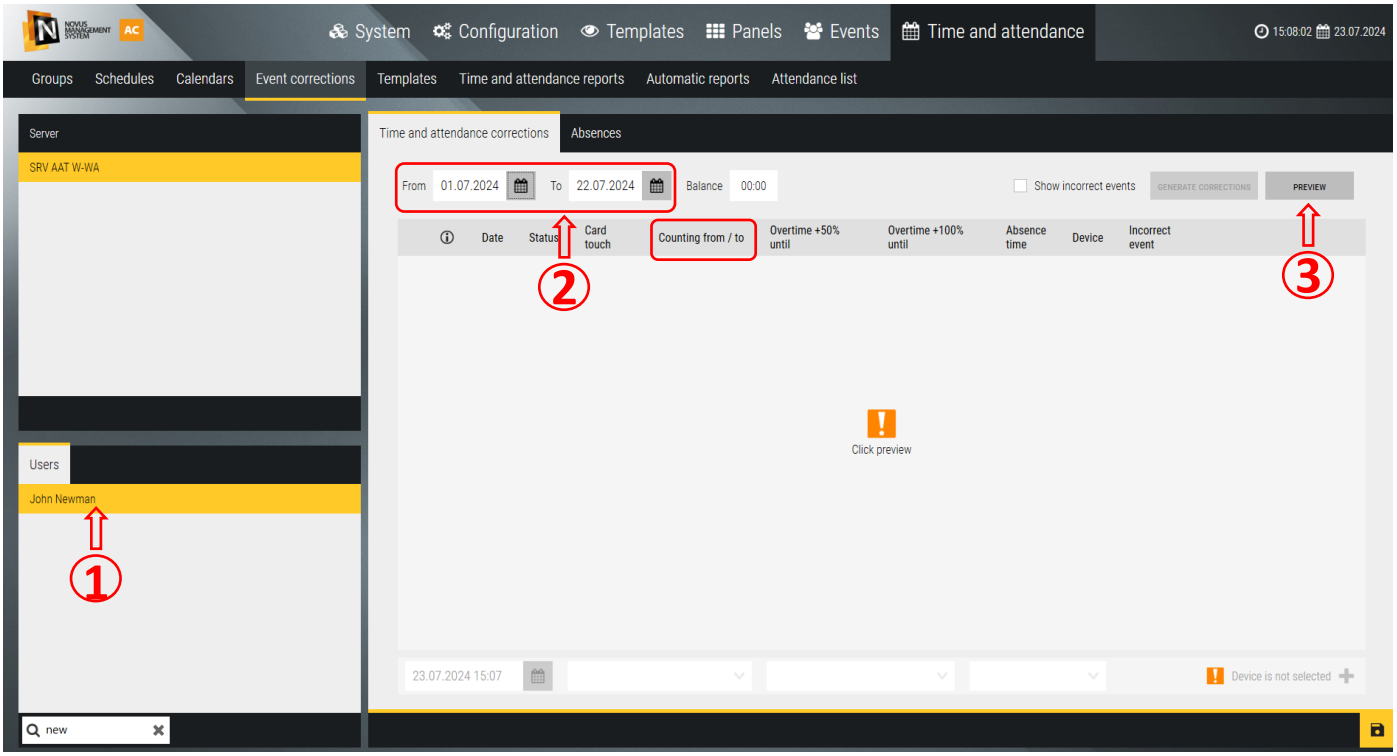
For shift mode, set the cycle according to the number of shifts by clicking on the *Increase/Decrease* cycle buttons. The example opposite shows a cycle for a system with three shifts per day. In the first week, set the schedule for the first shift, in the second week for the second shift, and so on. After clicking OK, the schedules will be automatically assigned in the calendar for the entire period set. It is recommended to choose different color descriptions when defining schedules for the shift system. The Schedules tab contains sample formulas for three shifts. Save the defined calendar.

Users - T&A



In this tab, you can assign a user a group and a working time calendar and notifications. This allows you to register I/O on the terminal or selected readers and generate working time reports. In the notifications tab, you can select T&A events upon occurrence of which an email will be sent to the employee with the current time for working the daily working time norm. This functionality is covered by a paid license.

Event corrections

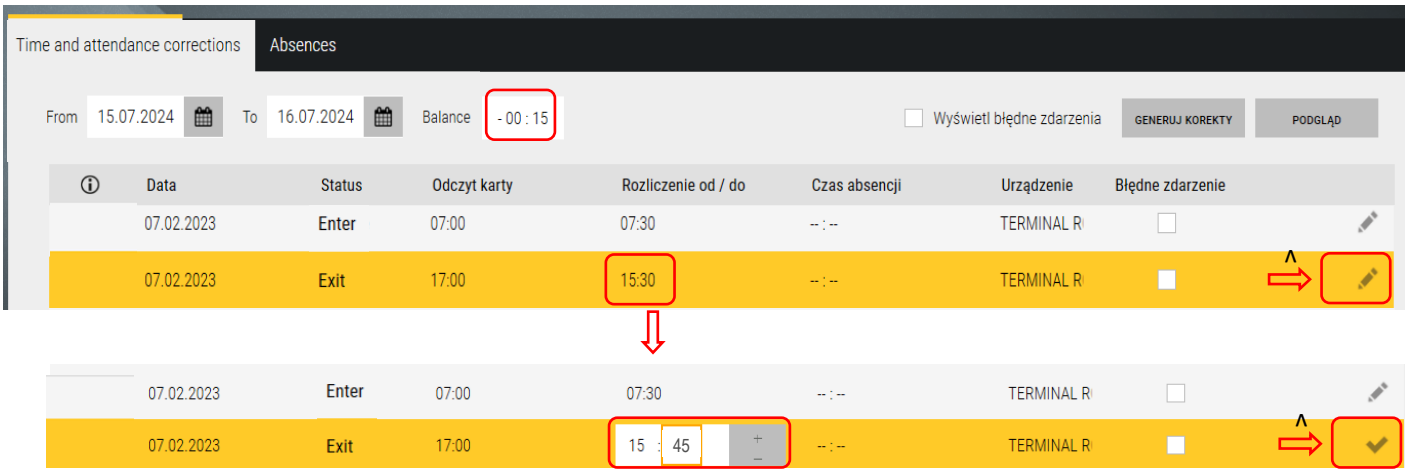


To make changes to the working time of a particular employee, in the *t&A corrections* sub-tab, you need to do it one by one:

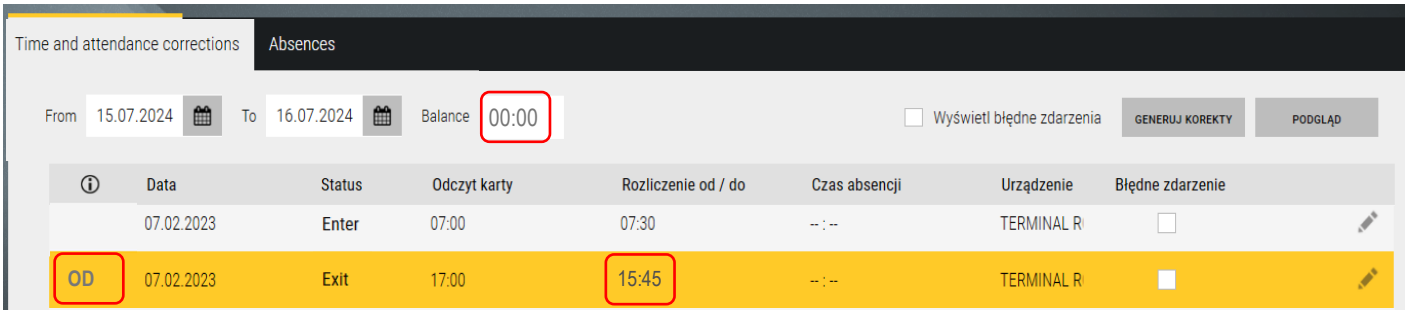
1) select the appropriate user on the left
2) The upper part of the window displays the range of days covering the default accounting period (from the beginning of the month to the end of the previous day) and the balance calculated for this period. You can set a different date range.
3) Click *Preview* in the upper right corner

This will generate a list of all events made by the employee in the set period in chronological order. Each day must start with an entry and end with an exit. Likewise, each exit during the working day must have a return. Only then the balance and the report generated in the next sub-tab will be correct. Missing registrations should be filled in as described below, and erroneous events should be marked in the Erroneous Events column and saved so that they are not displayed and taken into account when accounting for working time. Therefore, after generating the pre-view, review the list for correct enter/exit sequences.

Since version 5 of the program, in this window, in addition to the "Balance" field, there is also a new column Settlement from/to, which is used to adjust working time when a negative balance appears and the employee has worked it off. Only this field is editable and allows you to set the start or end time of working time. This in effect recalculates the working time balance for the specified period. The hours of recording I/O remain unchanged all the time, which allows you to easily analyse the correctness of billing. Edit the field of beginning/end of working time by clicking on the edit icon at the end of the line. After setting the new hour, confirm the operation by clicking on the Confirm icon at the end of the line.
The end-of-work time set in this column must not be later than the WY time in the Card Read column, and must not go beyond the range of working hours set for the department.
If the balance is still negative after the adjustment, search for another day on which to make such an adjustment or ask the employee to work off on subsequent days. After the adjustment is accepted and saved, the **OD** sign - working off - appears at the beginning of the line.
Example of correction:
Balance and time of the end of work before the correction of working off.



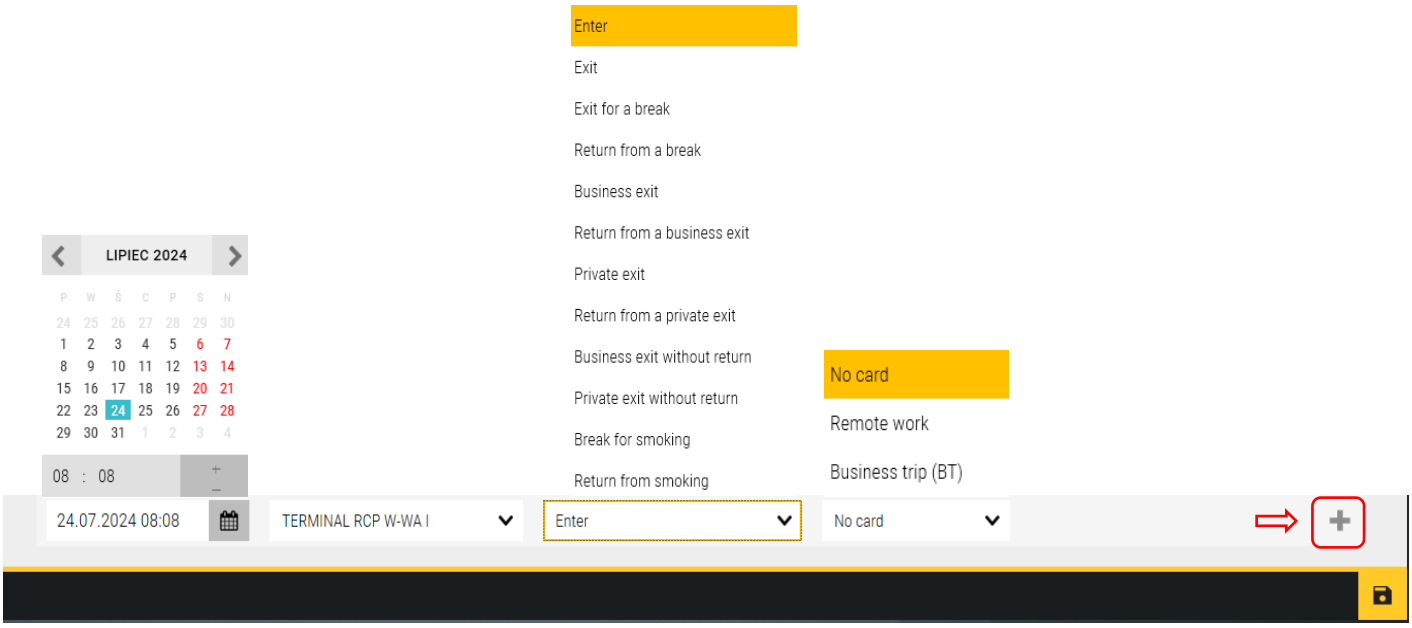
"Reserve" time on exit is 01:30 hours on 07.02.2023.
The balance and the end time of the work after the adjustment of the work-off.



From the "reserve" 00:15 minutes have been used, which is enough to reset the negative balance.
The balance window makes it easier and faster to make adjustments because there is no need to read it from the report.
The time in the Settlement from/to column can be used only for the recording of normal I/O because it refers to the beginning and end of working time for working out the norm.In the case of I/O during the working day, if there are any mistakes (e.g. double reading) or missing registrations then use the option associated with the Erroneous Event column and add the correct registration manually as described later in this manual.

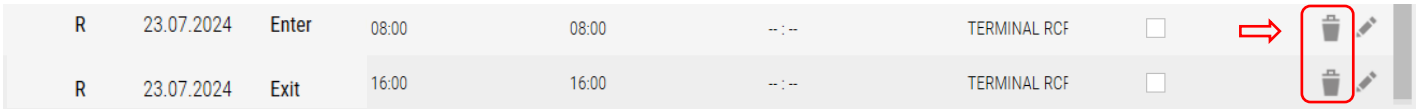
It is possible to make modifications both within the registered event as described on the previous page, as well as to add a completely new event (for example, when an employee fails to read the card in connection with work performed remotely - *R*).
In this case, do the following in the line at the bottom of the window:

1) click on the *Calendar* icon - set the date and time of the entered event
2) select the appropriate terminal for the employee/location
3) specify the type of event to be entered
4) click the '+' icon located at the end of the line



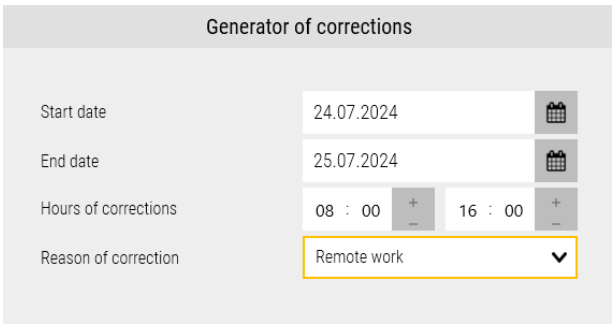
5)

The entered modification will appear in the list of employee events in chronological order with an OK or *R* symbol and a Trash can symbol. Clicking on the Trash icon removes the invalid entry from the list before saving.



If all parameters have been set correctly, the changes made should be saved using the Save icon. After saving, the trash can icon disappears.After adding and saving the input, add the output in the same way.
If the lack of I/O covers several consecutive days, it is worth using the correction generator To do this :

1) click the *Generator of correction* button
2) set the start and end date
3) select the type of absence from the drop-down list
4) click *OK* button



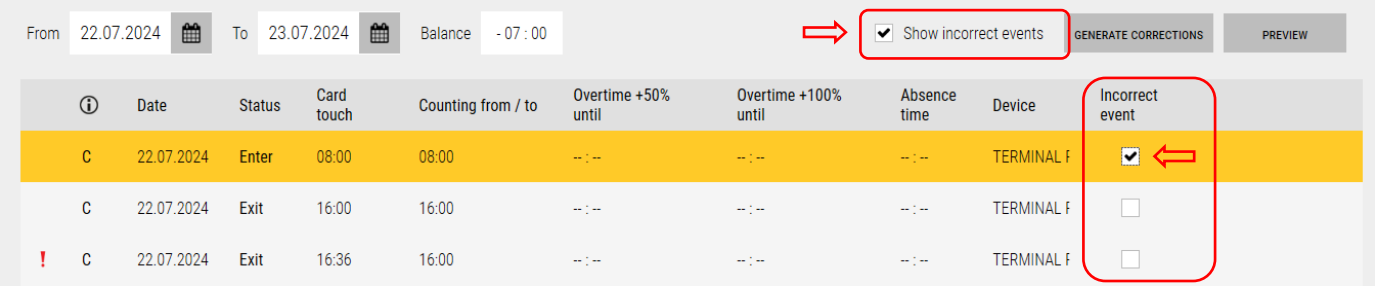
The added *enter/exit* will appear in the list and, after saving and clicking Preview, also on the Time Adjustments tab after selecting the appropriate date range. You can delete it by clicking on the *Trash* icon. The added adjustment requires saving (Diskette).

Note!

Incorrect readings from the terminal or incorrectly recorded C/R manual adjustments can be hiden by checking the box in the *Incorrect Event* column.

In order to do so:

1) check the box for the event in the *Incorrect Event* column



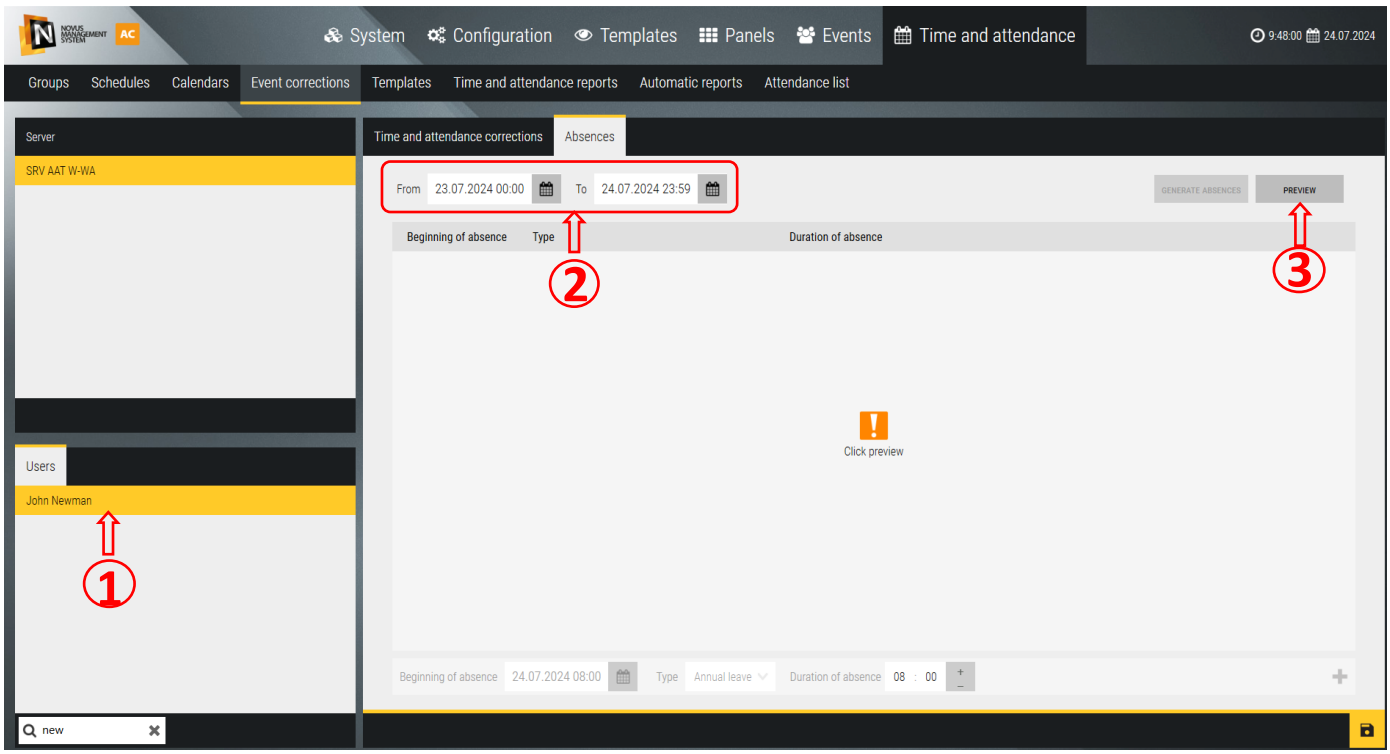
2) Click save *(Floppy disk icon).*

The operation performed in this way will cause the selected line to disappear from the list of events of the employee in question and will not be taken into account in the calculation and in the report. It can be restored by checking the box Display erroneous events and Preview, then uncheck the box and save.

Absences sub-tab

To add or remove an absenteeism for a particular user, in the Absences sub-tab, you need to do the following:

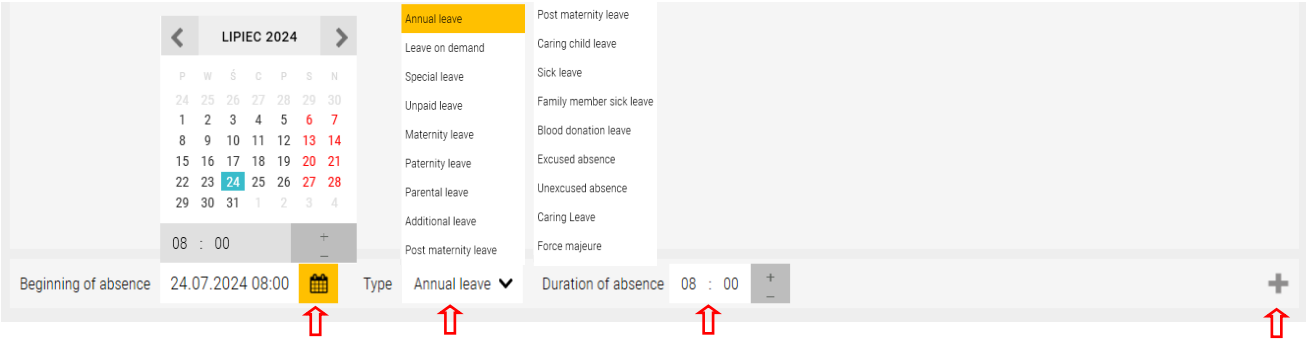
1) on the left, select the appropriate employee
2) select the period within which you want to make modifications
3) Click *Preview* in the upper right corner.



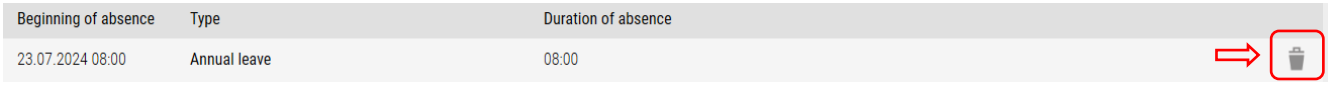
The operations performed above will generate a list of all employee absences in the selected period in chronological order. In case of their absence - the window will remain empty.

To add absences, do the following in the line at the bottom of the window:

1) by clicking on the *Calendar icon* - set the date of the entered event
2) select an absence type from the drop-down list
3) set the time of absenteeism - the daily norm of working time from the schedule or the time, for example, Caring Child Leave
4) click the '+' icon located at the end of the line.



The entered modification will appear on the list of employee absences in chronological order with the Trash icon Clicking on the Bin icon before saving removes the entry from the list. The added absenteeism requires saving *(Diskette icon).*

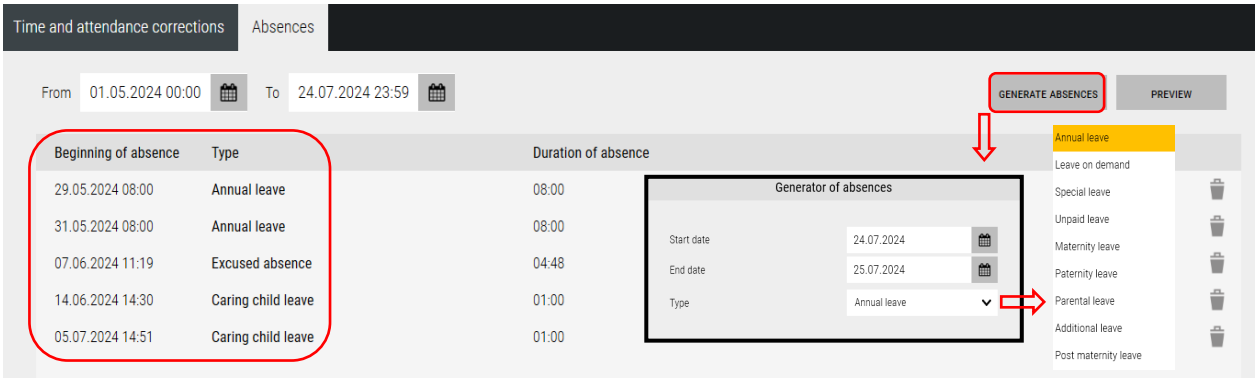


Tip:

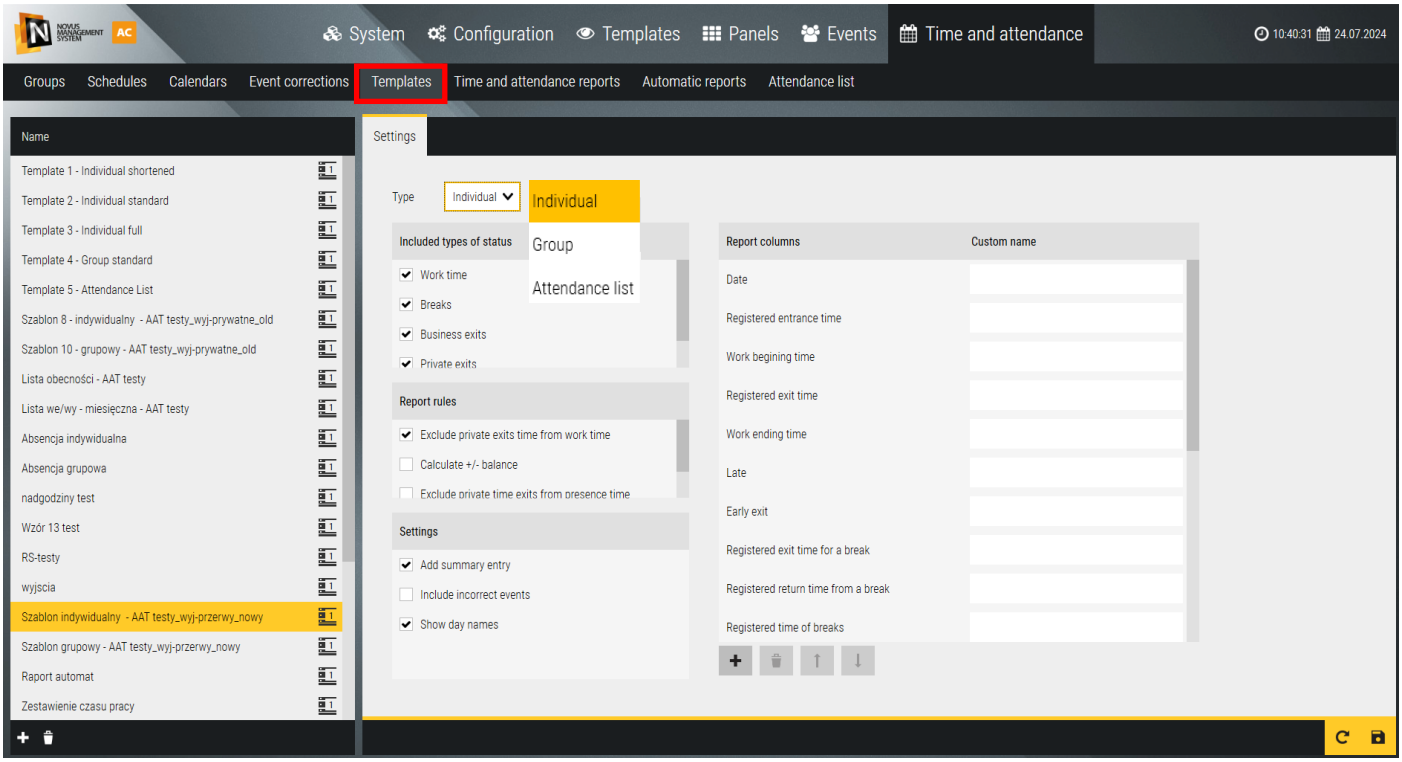
If the absenteeism covers several consecutive days, it is worth using the absenteeism generator. To do this, on the *Absences* tab:

1) click the *Generate Absences* button
2) set the duration of absenteeism - start and end date
3) select the type of absence from the drop-down list
4) click *OK* button.

The added absences will appear in the list and, after saving and clicking Preview, also in the Time Adjustments tab after selecting the appropriate date range. You can delete it by clicking on the Trash icon. The added absenteeism requires saving *(Diskette icon).*



Templates



This tab allows you to define the templates needed to generate T&A reports.
There are three types of templates to choose from for individual, group and attendance list reports.
Each type offers a different set of columns to choose from. The left window contains five templates defined by default for individual, group and attendance list generated reports. These templates cannot be edited - they can be used to generate reports or as examples to define your own reports. To define a new report, click the plus sign in the lower left corner of the window, then select the desired fields in the right window.
The lists in the sections in the right window allow you to select the following template parameters.

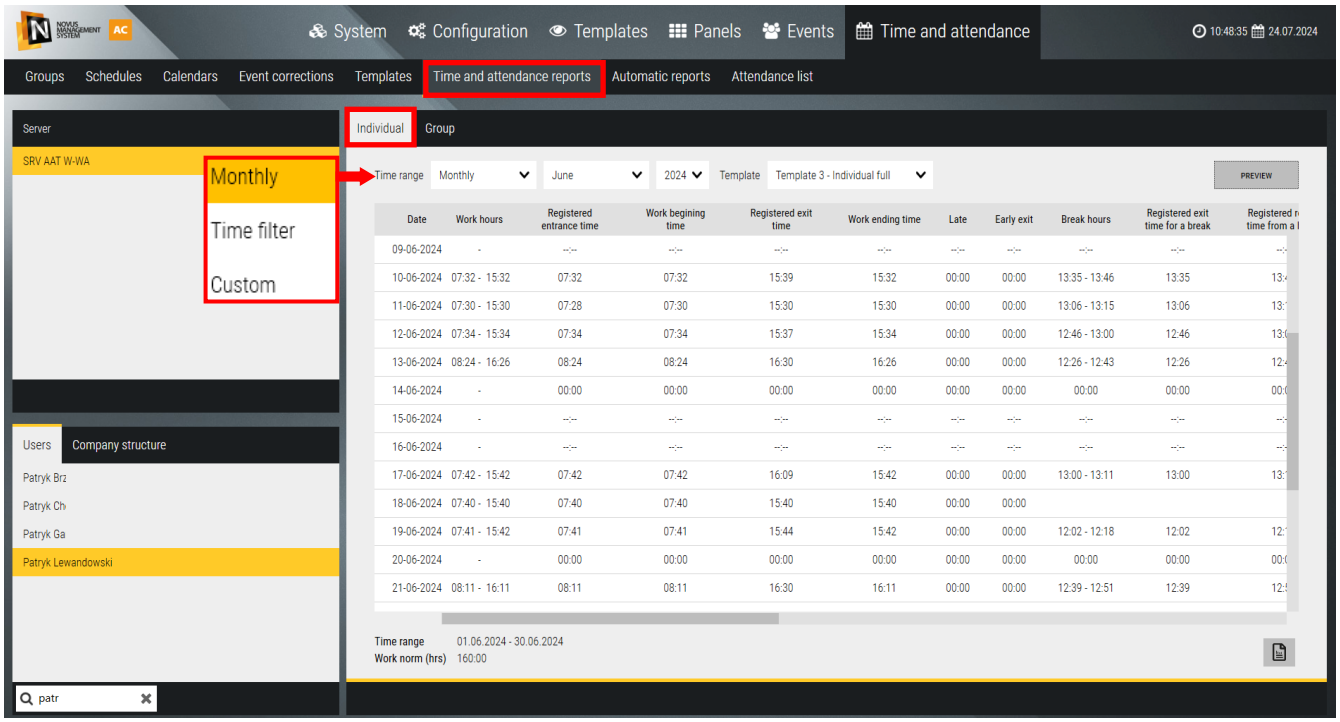
Include type of status - select which types of work status are to be included in the report. These settings affect the appearance and calculation of working time.

Report rules - define whether to include break and private exits in the report calculation.

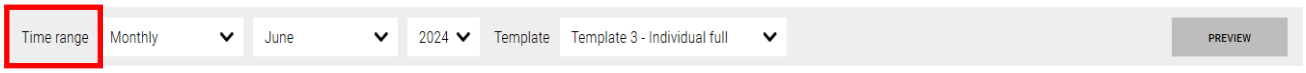
Setting - allow you to specify the appearance of the report form.

Report columns - checkboxes allow you to specify which columns will be displayed in the report. This avoids displaying or printing unnecessary columns. Checked items are set at the top of the list. Depending on the need, the same report can be generated using different templates to get the result in the form you are interested in. The order of columns in the template that have been selected (that is, also in the report) can be changed using the arrows at the bottom of the left window. After selecting the desired item in the list, you can move it up or down.

Time and attendance reports

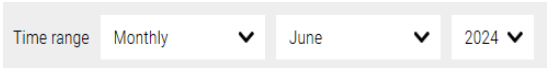


Individual report accounting for employee working time is generated on the basis of events from input/output readers assigned to T&A groups. On the top bar we have filters that allow us to set the parameters of the report:

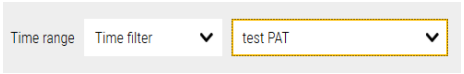


In terms of time, we have a choice of three options:

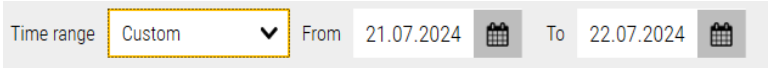
1. From the whole month (previous month by default)



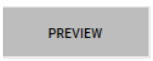
2. From the time range set in the selected time filter



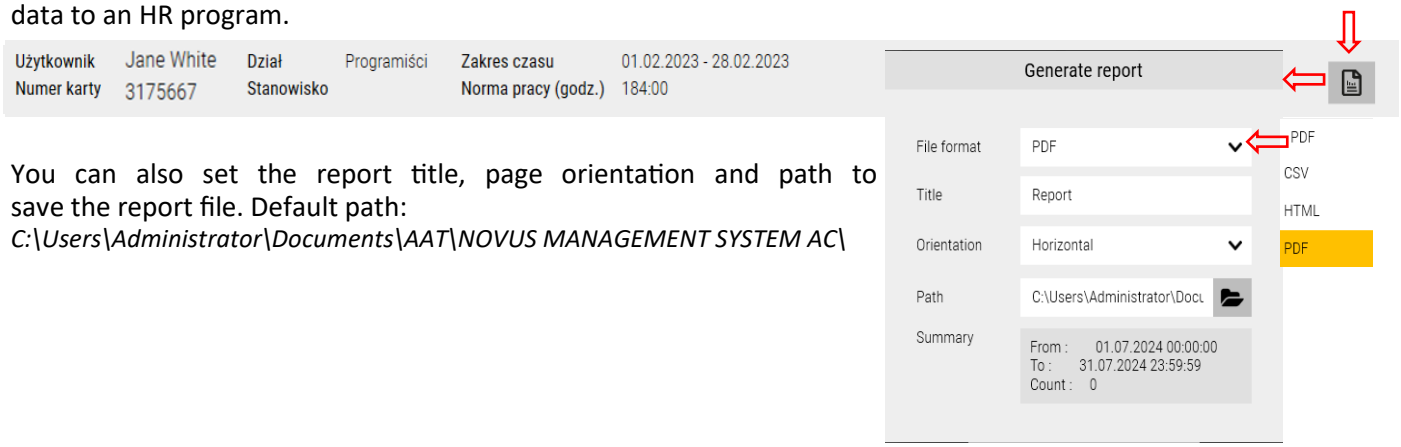
3. From the range defined by the calendar



In a system with multiple servers, select the server (the default is local) and then the department.
You can use the Search field to search for the department name.
Select Report Template from the drop-down list. After setting the filters, click on the *Preview* button.

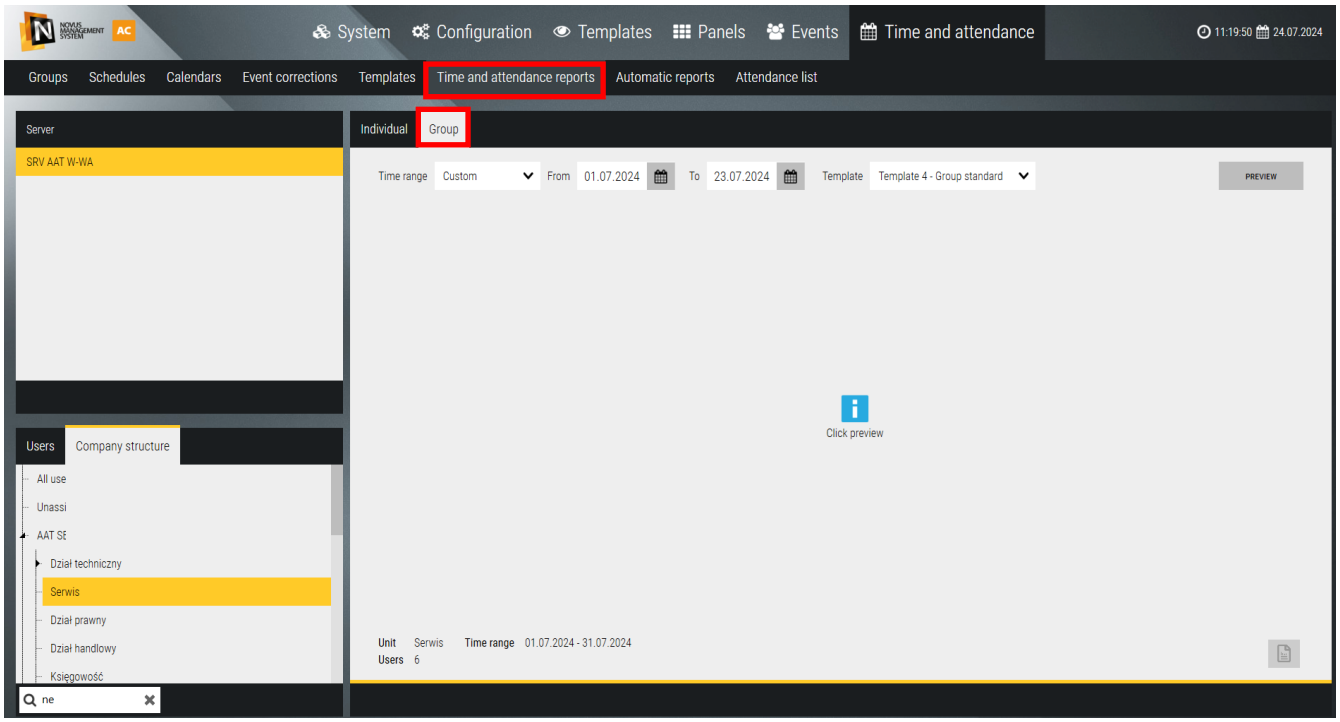


The report will be displayed on the screen. A summary is displayed at the bottom of the report.
The displayed report provides a line-by-line summary of hours worked on a single day, covers the selected date range, and can be saved to a file in HTML, PDF or as an editable file in CSV format. The latter can be used to export data to an HR program.

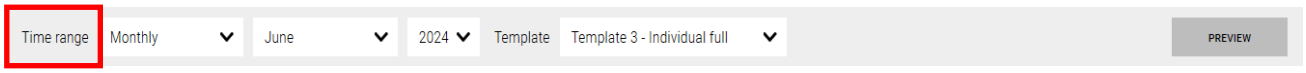


You can also set the report title, page orientation and path to save the report file. Default path:
C:\Users\Administrator\Documents\AAT\NOVUS MANAGEMENT SYSTEM AC

Group report

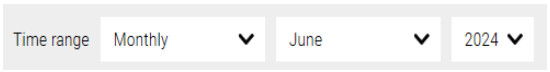


The group report accounting for the working time of the selected department is generated on the basis of events from entry/exit readers assigned to T&A groups. On the top bar we have filters to set the report parameters:

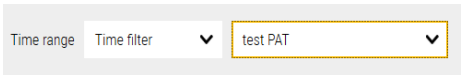


In terms of time, we have a choice of three options:

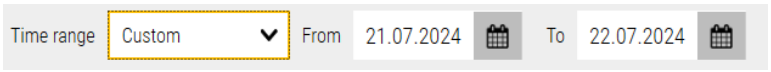
1. From the whole month (previous month by default)



2. From the time range set in the selected time filter

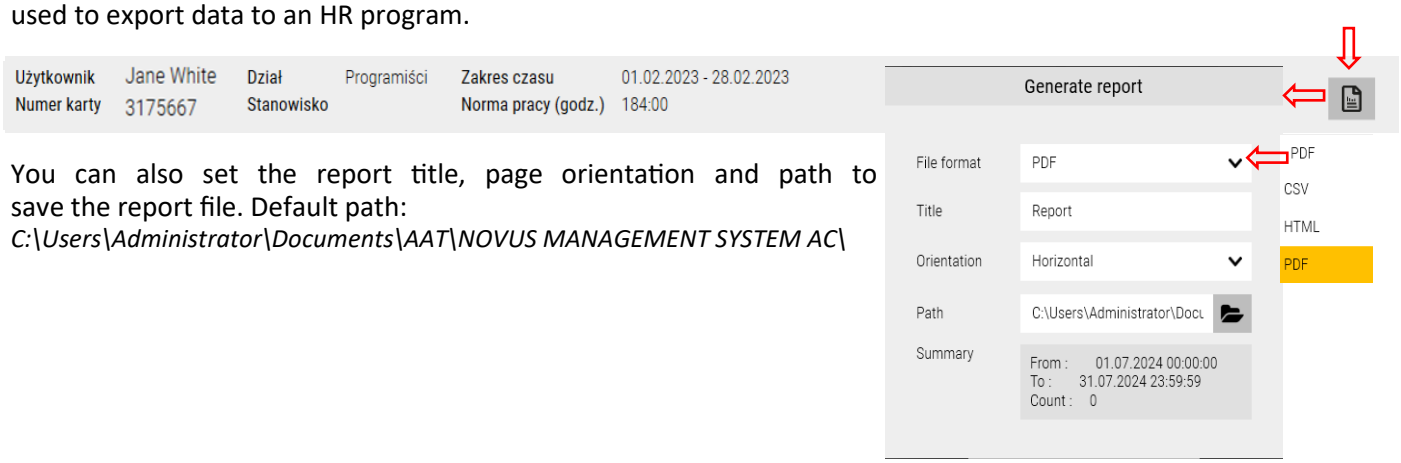


3. From the range defined by the calendar



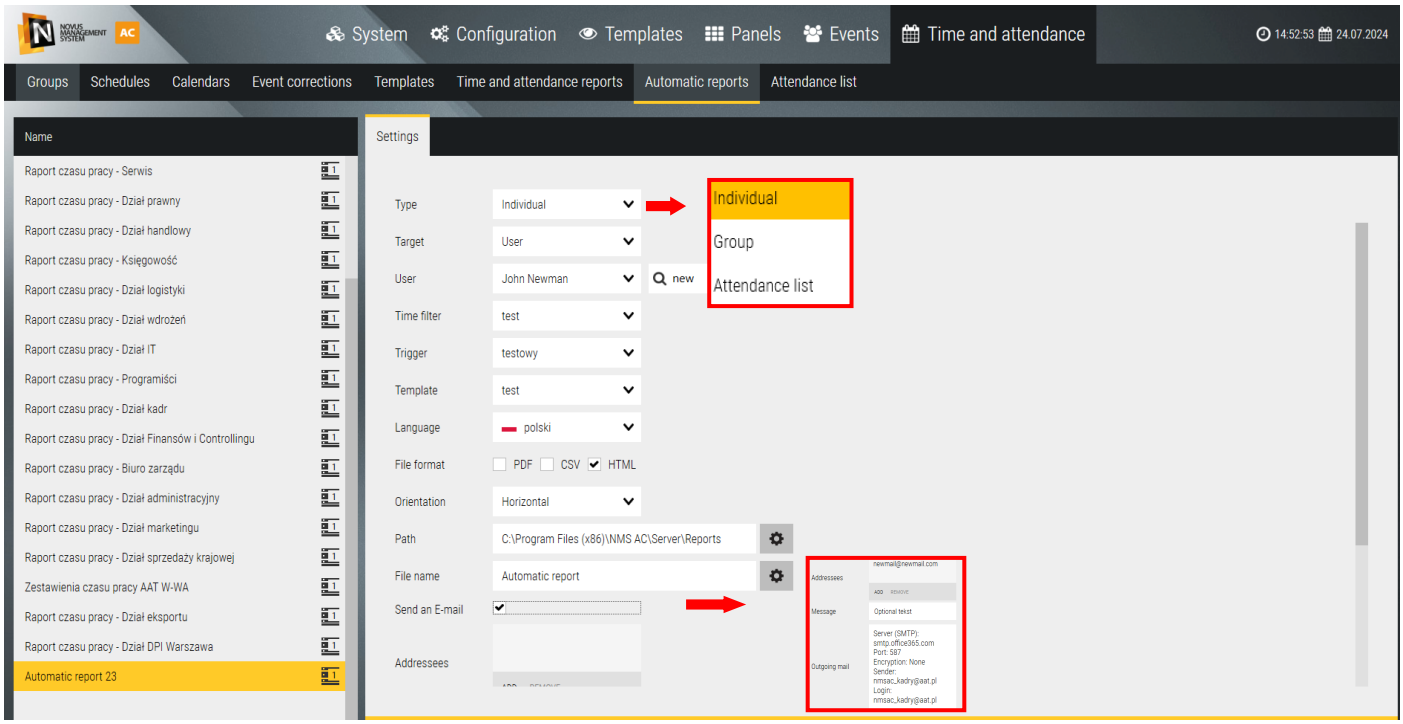
In a system with multiple servers, select the server (the default is local) and then the department.
You can use the Search field to search for the department name.
Select Report Template from the drop-down list. After setting the filters, click on the *Preview* button.

The report will be displayed on the screen. A summary is displayed at the bottom of the report.
The displayed report provides a line-by-line summary of hours worked on a single day, covers the selected date range, and can be saved to a file in HTML, PDF or as an editable file in CSV format. The latter can be used to export data to an HR program.



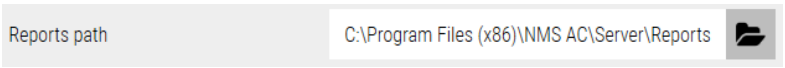
You can also set the report title, page orientation and path to save the report file. Default path:
C:\Users\Administrator\Documents\AAT\NOVUS MANAGEMENT SYSTEM AC

Automatic reports



The time accounting report can be generated manually by the operator as described in the previous section, or automatically according to the set calendar. After clicking on the "+" Add button, a new report template appears in the left window with a default name that can be edited. Then, in the right window, set the filter parameters.
The Time Filter, Trigger and Template need to be predefined in the Templates tab. Time filter allows you to specify the time interval(s) that the report will cover.
Trigger allows you to set the time, day and cycle in which the report generation should be repeated. You can also select the report language, file format and orientation.

Default folder for saving reports:



It can be changed in the *System / General* tab.

The generated report can be sent to email after checking the checkbox and setting the addressee. Correct operation of this option requires setting outgoing mail parameters in the tab: *System / General / Outgoing mail.*

Sample reports

PDF:

Template 4 - Group standard
Serwis
01.07.2024 00:00 - 31.07.2024 23:59

Fullname	Card number	Department	Time range	Real time of work
[redacted]	1[redacted]	Serwis	01.07.2024 - 31.07.2024	32:00
[redacted]	2[redacted]	Serwis	01.07.2024 - 31.07.2024	72:00
[redacted]	2[redacted]	Serwis	01.07.2024 - 31.07.2024	72:00
[redacted]	1[redacted]	Serwis	01.07.2024 - 31.07.2024	72:00
[redacted]	3[redacted]	Serwis	01.07.2024 - 31.07.2024	72:00
[redacted]	4[redacted]	Serwis	01.07.2024 - 31.07.2024	72:00
Summary				392:00

CSV:

W29 --:--

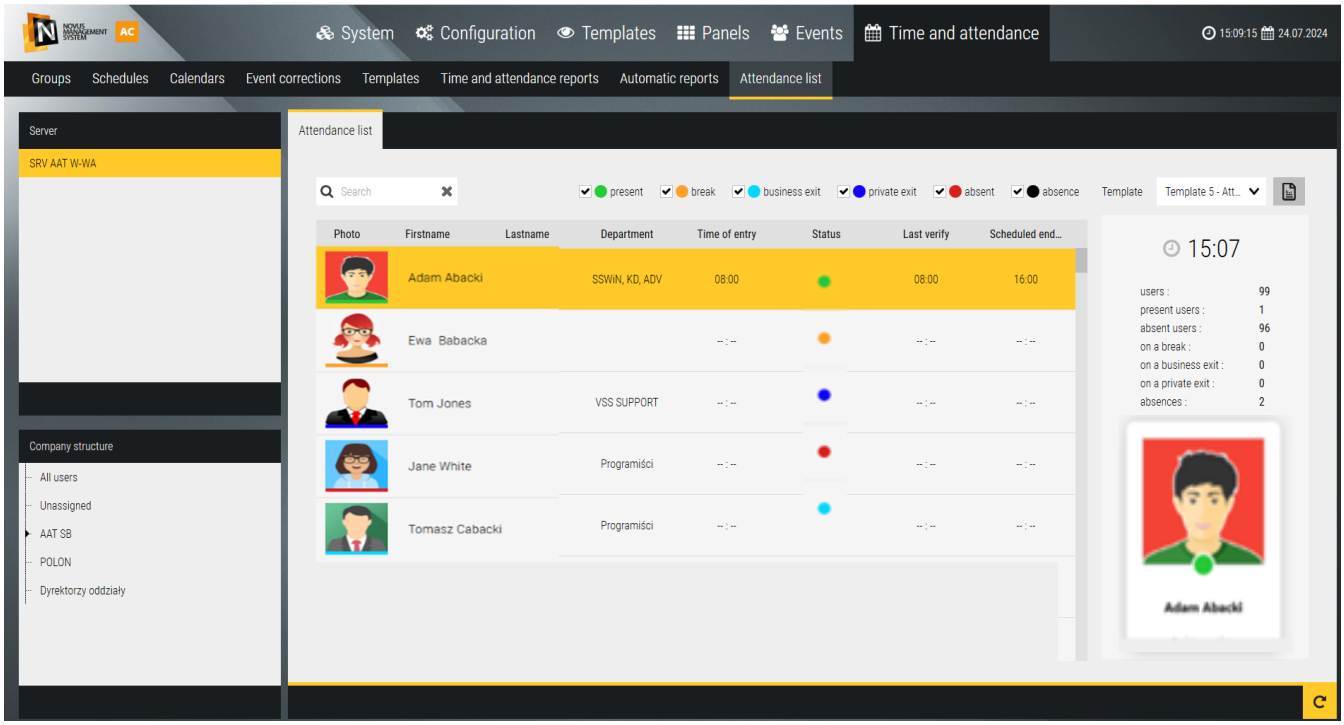
	A	B	C	D	E	F	G	H	I	J	K	L	M
1	John Newman												
2	Template 3 - Individual full												
3	01.07.2024 00:00 - 31.07.2024 23:59												
4	Date	Work hours	Registerec	Work begi	Registerec	Work endi	Late	Early exit	Break hours	Registerec	Registerec	Break time	Registerec
5	01.07.2024	07:32 - 15:32	07:32	07:32	15:32	15:32	00:00	00:00				00:00	
6	02.07.2024	08:05 - 16:05	08:05	08:05	16:05	16:05	00:00	00:00				00:00	
7	03.07.2024	08:24 - 16:24	08:24	08:24	16:30	16:24	00:00	00:00	15:09 - 15:18	15:09	15:18	00:00	
8	04.07.2024	07:46 - 15:45	07:46	07:46	15:45	15:45	00:00	00:01	11:47 - 11:58	11:47	11:58	00:00	
9	05.07.2024	07:57 - 15:57	07:57	07:57	15:57	15:57	00:00	00:00				00:00	
10	06.07.2024	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
11	07.07.2024	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
12	08.07.2024	07:46 - 15:46	07:46	07:46	15:48	15:46	00:00	00:00				00:00	
13	09.07.2024	07:30 - 15:30	07:27	07:30	15:30	15:30	00:00	00:00				00:00	
14	10.07.2024	07:30 - 15:30	07:29	07:30	15:30	15:30	00:00	00:00	13:08 - 13:21	13:08	13:21	00:00	
15	11.07.2024	07:30 - 15:30	07:28	07:30	15:31	15:30	00:00	00:00	11:53 - 11:57	11:53	11:57	00:00	
16	12.07.2024	08:19 - 00:00	08:19	08:19	00:00	00:00	00:00	00:00	12:40 - 12:50	12:40	12:50	00:00	
17	13.07.2024	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
18	14.07.2024	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
19	15.07.2024	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00
20	16.07.2024	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00
21	17.07.2024	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00
22	18.07.2024	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00	00:00
23	19.07.2024	09:18 - 09:25											
24	09:26 - 00:00	09:18											
25	09:26	09:18											

HTML:

Template 3 - Individual full
[redacted]
01.07.2024 00:00 - 31.07.2024 23:59

Date	Work hours	Registered entrance time	Work begining time	Registered exit time	Work ending time	Late	Early exit	Break hours	Registered exit time for a break	Registered return time from a break	Break time by schedule
01-07-2024	07:32 - 15:32	07:32	07:32	15:32	15:32	00:00	00:00				00:00
02-07-2024	08:05 - 16:05	08:05	08:05	16:05	16:05	00:00	00:00				00:00
03-07-2024	08:24 - 16:24	08:24	08:24	16:30	16:24	00:00	00:00	15:09 - 15:18	15:09	15:18	00:00
04-07-2024	07:46 - 15:45	07:46	07:46	15:45	15:45	00:00	00:01	11:47 - 11:58	11:47	11:58	00:00
05-07-2024	07:57 - 15:57	07:57	07:57	15:57	15:57	00:00	00:00				00:00
06-07-2024	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
07-07-2024	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--	--:--
08-07-2024	07:46 - 15:46	07:46	07:46	15:48	15:46	00:00	00:00				00:00
09-07-2024	07:30 - 15:30	07:27	07:30	15:30	15:30	00:00	00:00				00:00
10-07-2024	07:30 - 15:30	07:29	07:30	15:30	15:30	00:00	00:00	13:08 - 13:21	13:08	13:21	00:00
11-07-2024	07:30 - 15:30	07:28	07:30	15:31	15:30	00:00	00:00	11:53 - 11:57	11:53	11:57	00:00
12-07-2024	08:19 - 00:00	08:19	08:19	00:00	00:00	00:00	00:00	12:40 - 12:50	12:40	12:50	00:00

Attendance list

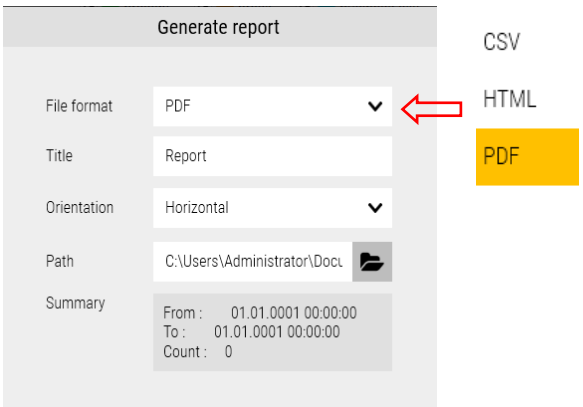


The attendance list allows you to verify the current attendance status of your employees very quickly. When you open the window, it displays a list of employees with photos, as well as the attendance status and the time of registered entry to the company. The status, according to the legend, shows one of five states: presence, absence and exits during working hours.

You can sort the list by clicking on the column headers: Entry Time, Status and Last Reading.

On the right side of the window, the time is displayed - when the window is opened, it is the current time and attendance status for that moment. Refresh the status by clicking on the *Refresh* button.

The icon  in the upper right corner allows you to generate and save the attendance list report for the moment.



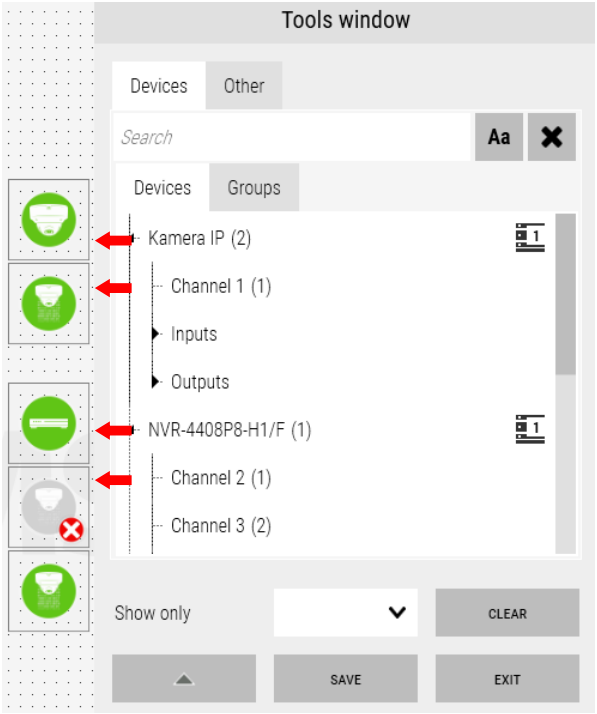
Generating an attendance list report is also possible in automatic mode.

9.5 Integration with VSS devices

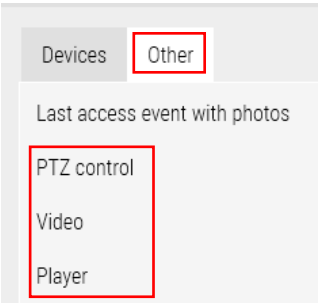
The NOVUS MANAGEMENT SYSTEM AC software enables integration with a video surveillance system. Adding devices of this type is described in chapter **3.10 Devices - Video Surveillance System**.

The connected devices can be operated from the level of *Panels* described in chapter **6. Panels**. The default *Panel 3* includes the *video views* window. You can modify it or create new panels to take full advantage of integration with VSS devices. To do this, enter a panel using  button located in the main bar of the program and select the appropriate panel.

After selecting the panel, you can edit it using the pencil icon  . The *Tools window* appears. You can find there all the elements for panel configuration. The *Devices* tab contains previously added VSS devices. You can move them to the panel by dragging the device or just the video stream. When the panel is saved, clicking the mouse on the device icon displays its event list. Clicking on the video stream icon shows the camera image in a pop-up window.



The *Other* tab in the *Tool Window* shows other panel configuration tools. For the integration of VSS devices, The *Video*, *Player* and *PTZ Control* tools are essential for the integration of VSS devices.



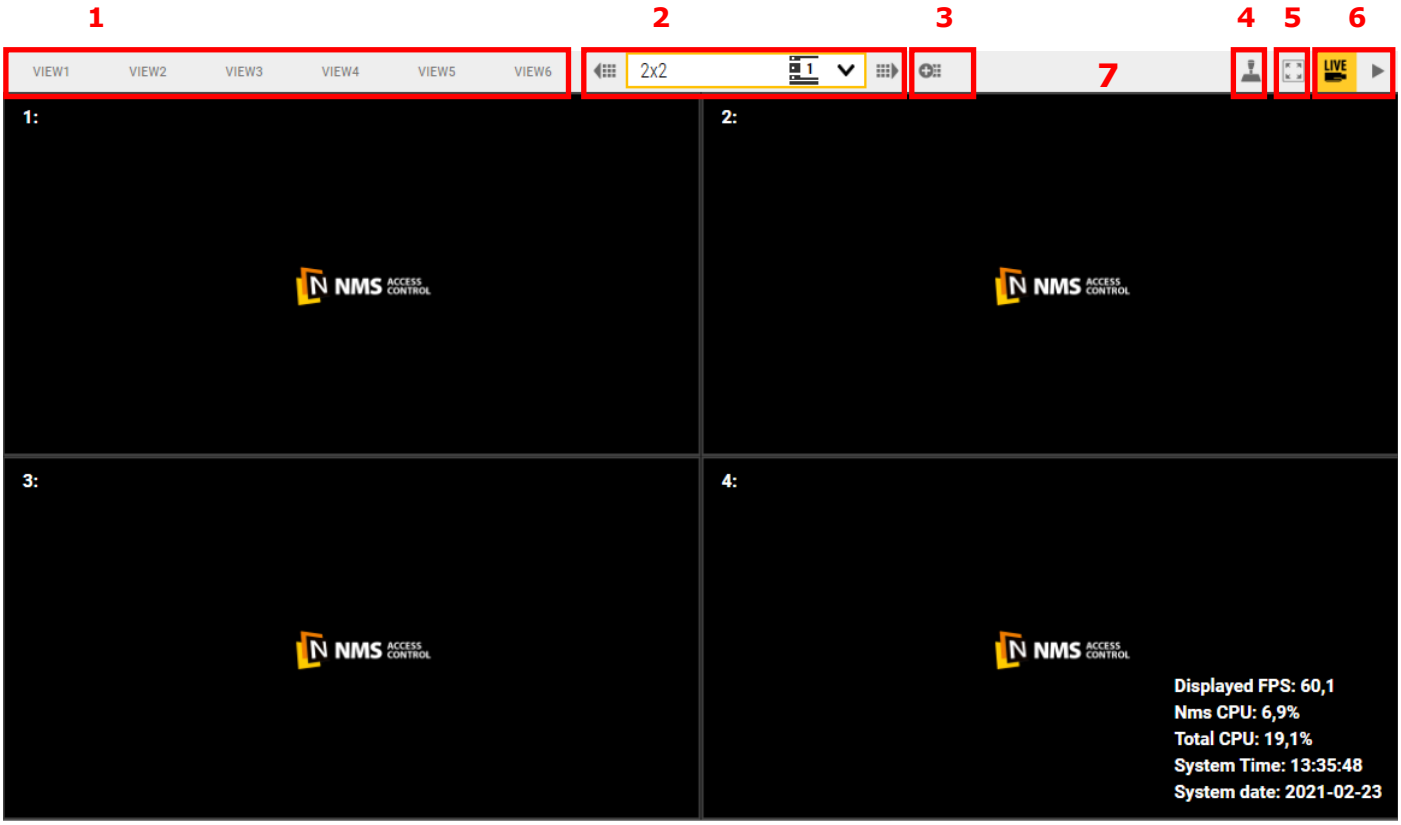
Pay attention to the options that appear after clicking on the stream icon in edit mode:

- Enable OSD—checkbox enabling display of video stream parameters in the image.
- Preview stays open—enabling this checkbox causes the video stream will be displayed until the user closes it with the red cross in the upper right corner of the window. When the option is disabled, the image disappears when you first click on another object
- Preview size—place to define the size of the popup video window.

Another function is to double-click the pop-up video to display the stream in full screen mode. Selecting a part of the image activates the digital zoom function, which can be adjusted using the mouse wheel. Use the right mouse button to exit.

9. 5. 1. VSS integration tools—Video

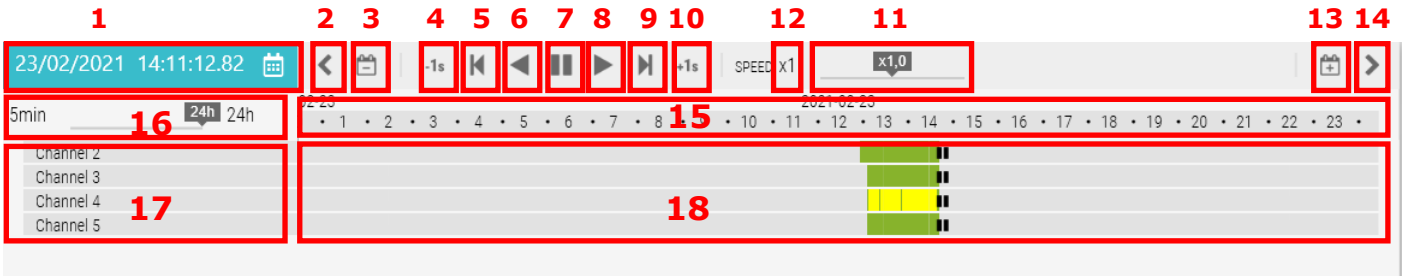
The *Video* window is used to display video streams. It displays cameras previously defined in *Templates*, *Video Views* tab. (described in chapter **5.1 Video Views**). In the top bar of this window there are icons to manage the window.



1. View Buttons—shortcuts to display defined *Video Views*. The buttons do not have any defined views by default. To assign them, press the shortcut using the right mouse button. Then you can add a *Video View* or rename the shortcut button. You can attach multiple views to a defined button. In such a situation, after pressing it, a list of assigned views will appear. If only one view is attached to the button, pressing it will display the view immediately.
2. Buttons that allow to switch views to the next, previous or choose from a list of defined views.
3. The button to add another *Video View*. Pressing it, a window with different divisions appears. Selecting the split, defining the displayed cameras by dragging the stream icons (see the previous page), you can save the *video view* using the floppy disk icon that appears after selecting the split. Then you must enter a name for the saved *Video View*.
4. Joystick icon—enables / disables the ability to control PTZ cameras. When it is enabled, move the cursor over the image of camera, the arrow indicator changes into a control arrow. You can control the dome camera directly on the video image. The zoom ratio can be changed using the mouse wheel.
5. Full screen icon — when pressed, the Panel displays in full screen. The top bar is also visible, it can be removed by right-clicking on any video image and clicking "Hide menu bar".
6. Live view and playback icons. Alternately lit, they indicate which mode is currently displayed. You need the *Player* tool to control the playback material.
7. Right-click on the top bar shows a window where you can add / remove selected icons of the top bar.

9.5.2. VSS integration tools—Player

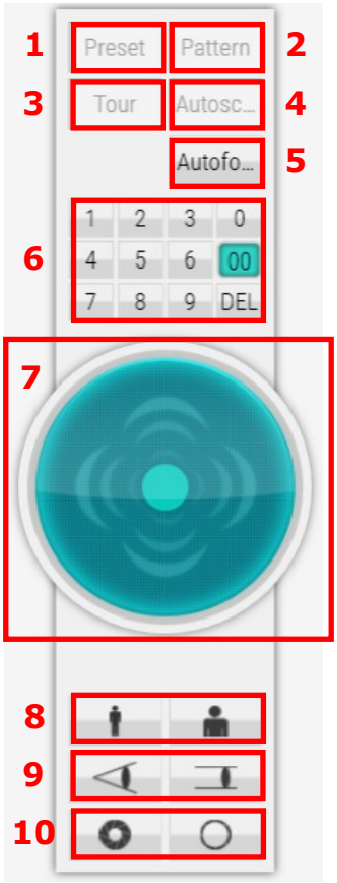
The player tool is necessary to view recordings from VSS recorders. It is blank and grayed while viewing live images. When any *video view* is switched to playback mode, the list of channels of the window is filled in and recordings are displayed on the graph.



1. Date and time of the currently playing video. By pressing the calendar button, you can change the date and time of the material being played.
2. Button to move back the timeline of the panel.
3. Button to move 24 hours back the timeline of the panel.
4. Button to move the recordings 1 second back.
5. Button to move the recordings 1 frame back.
6. Button to play the recordings back.
7. Pause button.
8. Playback button.
9. Button to move the recordings 1 frame forward.
10. Button to move the recordings 1 second forward..
11. Playback speed slider. It enables slow or fast playback of recordings (from x0,1 to x10).
12. „x1” button to set default playback speed (x1).
13. Button to move 24 hours forward the timeline of the panel.
14. Button to move forward the timeline of the panel.
15. Timeline. It shows 24 hours by default, it can be zoomed up to 5 minutes (using mouse scroll or timeline scale). You can move it smoothly using the left mouse button.
16. The timeline scale allows to zoom in the timeline (from 5 minutes to 24 hours).
17. List of playing channels. All cameras that have been switched to playback mode in video views are listed.
18. Recordings presented in the form of a graph and various colors. Clicking on the appropriate point of the graph, you can quickly change the time of the played material.

9. 5. 3. VSS integration tools—Video

You can control PTZ cameras directly on the camera image by pressing the joystick icon in the top bar of the *Video* window. For full control, use the *PTZ Control* tool.

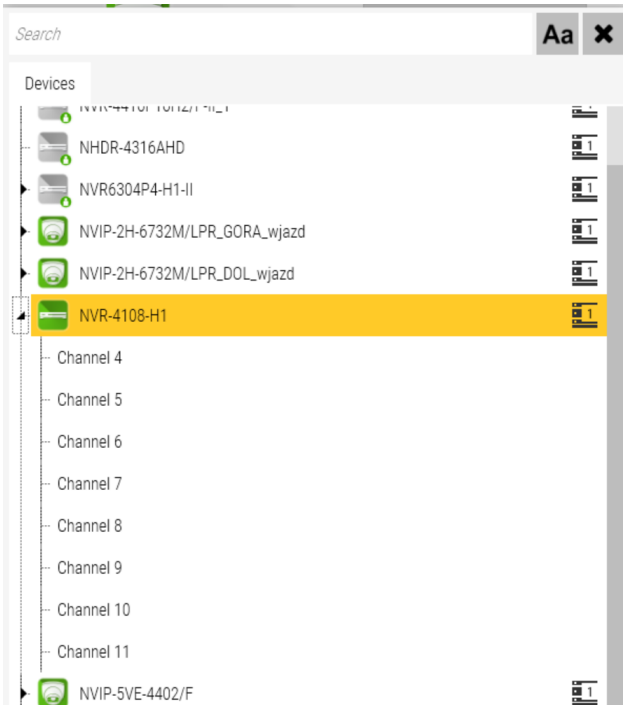


1. Preset button—to call the preset. It is greyed out by default, it activates when you select a number in the lower part of the tool.
2. Pattern button—to call the pattern. It is greyed out by default, it activates when you select a number in the lower part of the tool.
3. Tour button—to call the tour. It is greyed out by default, it activates when you select a number in the lower part of the tool.
4. Auto scan button—to call the auto scan function. It is greyed out by default, it activates when you select a number in the lower part of the tool.
5. Autofocus button—focuses automatically.
6. Numeric keyboard—allows you to select the number of the recalled preset, tour, etc. The highlighted element indicates the selected number.
7. PT control area—allows to move rotating cameras, use different rotation speeds.
8. Zoom buttons—allow to zoom out and zoom in on a camera with a motorzoom lens.
9. Focus buttons—allow to set focus of the image manually in a camera with a motor zoom lens.
10. Iris buttons—allow to manually open or close the iris of the lens.

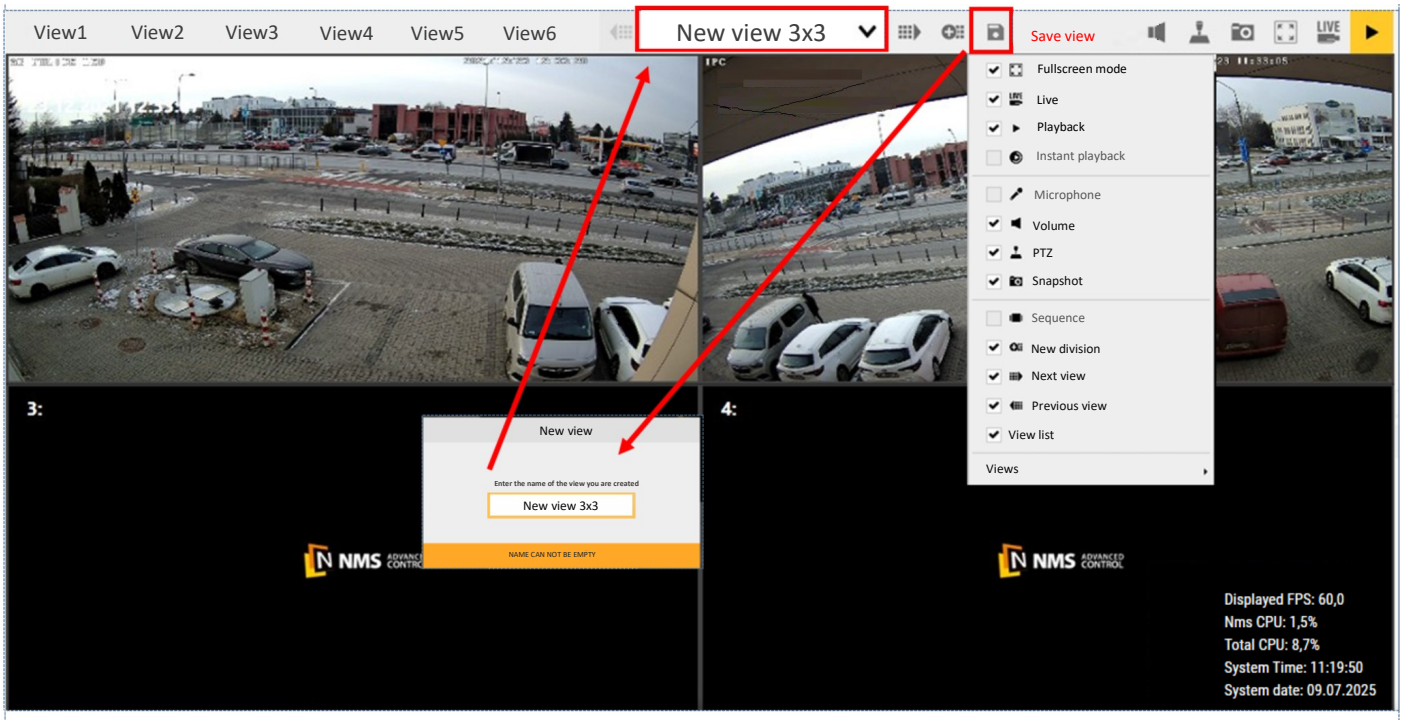
Attention! The availability of particular functions depends on the functionality of the selected camera model.

9. 5. 4. VSS integration tools—Device tree

The Device Tree tool functions as a browser for the CCTV system structure, displaying all surveillance devices added to the system in a list format – including both individual cameras and recorders with their assigned video channels.

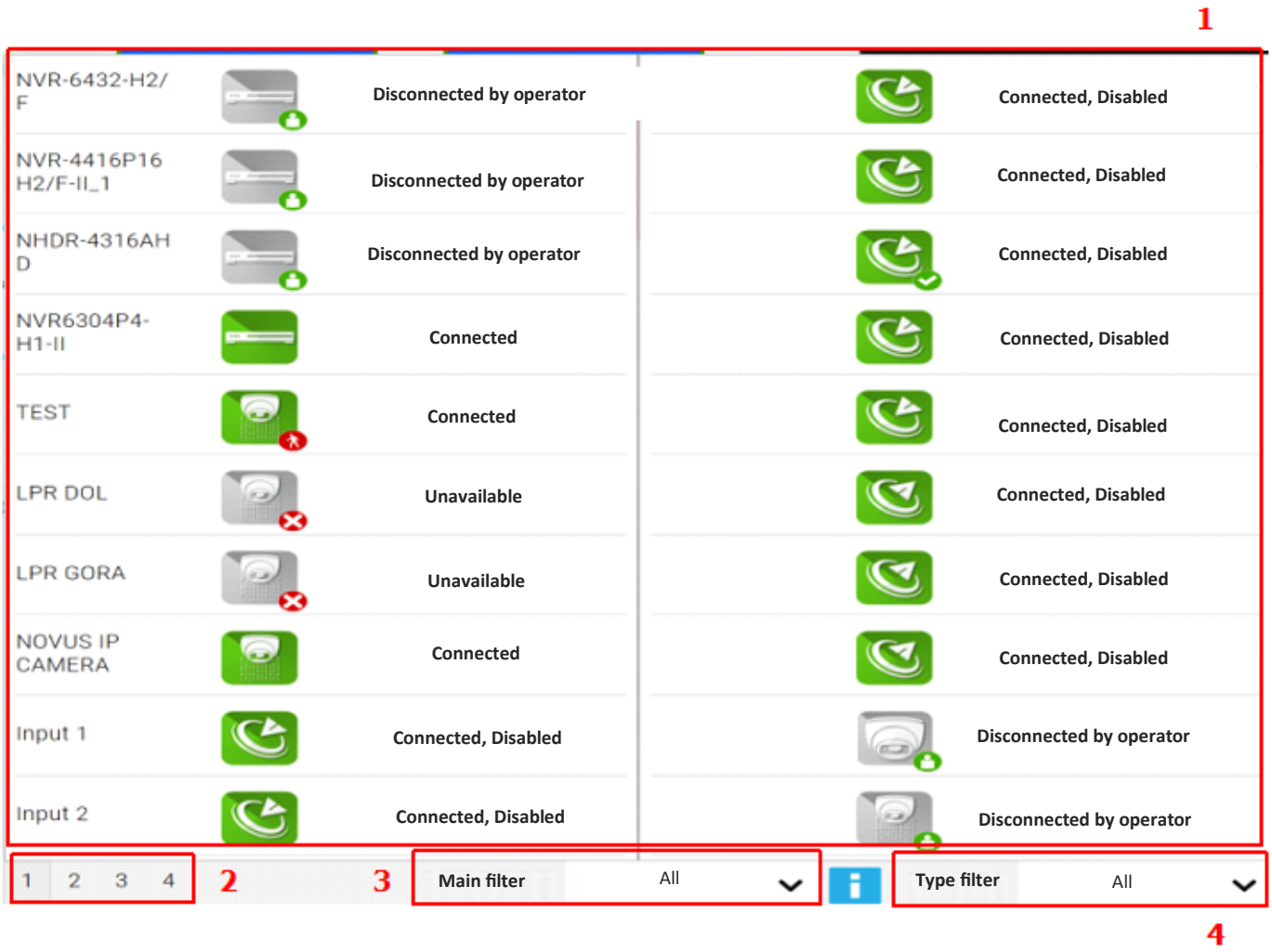


To create a temporary view in the Video tool and optionally save it, drag a device or channel from the list onto the selected view in the Video tool, holding the cursor over the desired element.



9. 5. 5. VSS integration tools—Synoptic board

The Synoptic Board tool is used to display devices and monitor their statuses.
Users can observe device statuses in real time, such as: Normal communication, Event detected, Unavailable, or Disconnected by operator.



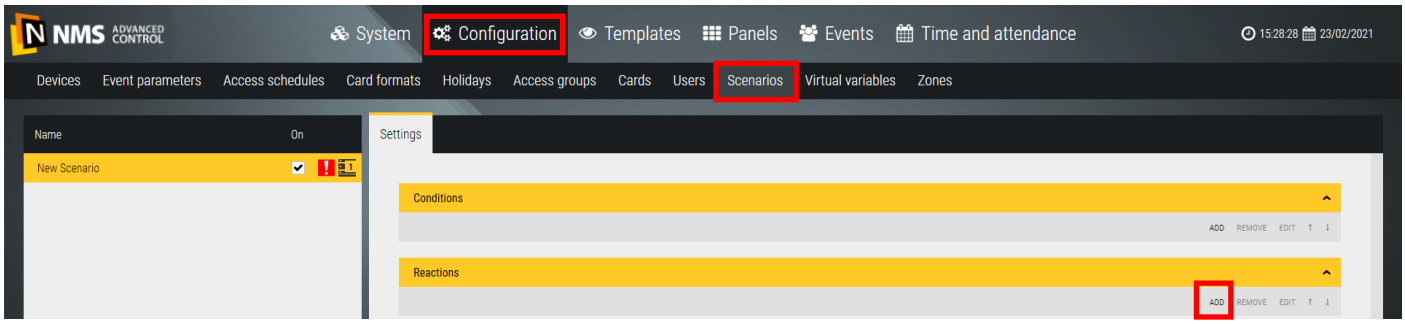
1. Device window – displays all devices, channels, inputs, and outputs available in the system.
2. Page selection – allows switching between pages with lists of devices and system elements.
3. Main filter – enables selection of filters previously defined in the *Element and Event Filters* tab.
4. Type filter – allows narrowing the list to selected categories, including:

- All
- Controllers
- Cameras
- Readers
- Surveillance lines

To view the video from a specific device, hold the cursor over the channel icon and drag it to the selected view in the Video tool.
IMPORTANT! This function works only on channel icons, not on entire devices.

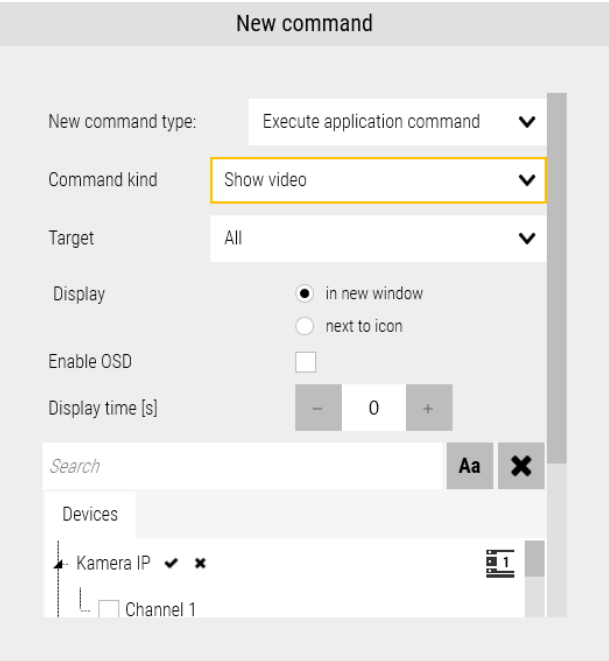
9. 5. 6. View video streams in response to the scenario

The integration of NMS AC software with VSS devices also applies to displaying video streams as a reaction to any events available in the system. Reaction settings can be set in the Configuration menu, Scenarios tab.



After creating a new scenario and its launch conditions, click the *Add* button in the Reactions section. *New command* window appears, select the command type *Execute application command*. Further options will appear, you must set *Show Video* as the command type.
There are additional display options:

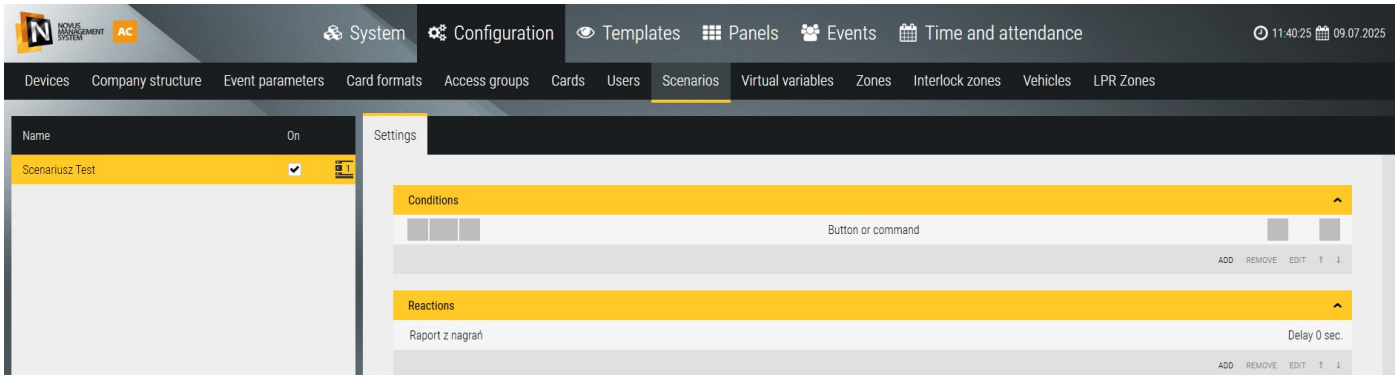
- Target — video display can be set for a specific operator or group of operators.
- Display — display can be set in a new window or in the pop-up window next to the video stream icon. In the first case, a single camera will occupy the entire window. By increasing the number of streams, it will automatically divide into 4, 9 or 16 streams. For more than 16 streams, the streams displayed first disappear.
- Enable OSD — displaying a video in a new window, you can enable the OSD of that window
- Display Time — the default value of 0 means that the stream, after calling, will be displayed until the operator disables it. By specifying a different value, we make the streams indicated in this scenario disappear after a written number of seconds while displaying subsequent streams.



- Devices — list of added video devices, you can select any streams from cameras and recorders.
- Delay time— response delay time.

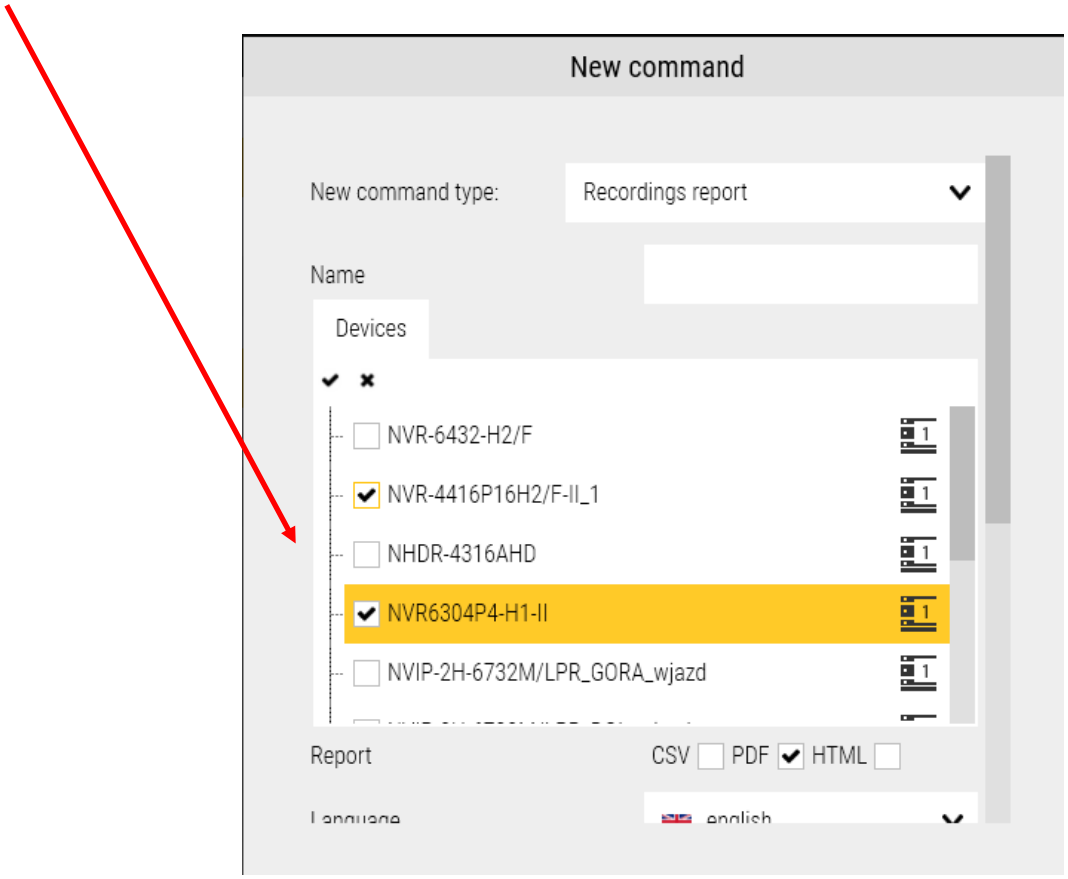
9. 5. 7. Generating recorder reports via scenario response

A new feature has been added that allows generating reports by defining a scenario.
The generated report includes key information about the status of recorders, such as:
device IP address, disk status, total recording time, recording time range, time difference between the recorder and the server, and software or firmware version.

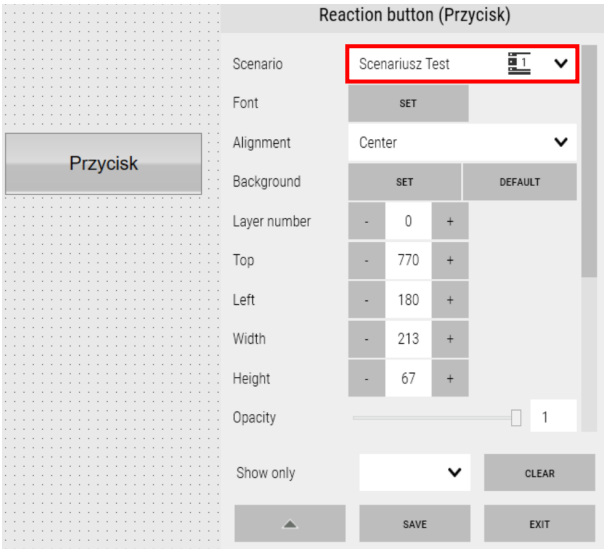


To generate a recording report, create a new scenario in which the operating conditions are defined.
In this case, select a command type such as Button or Command, which will initiate the report generation.

Next, in the Responses tab, choose the command type Recording Report. The report will be generated only for the recorders selected in the list.

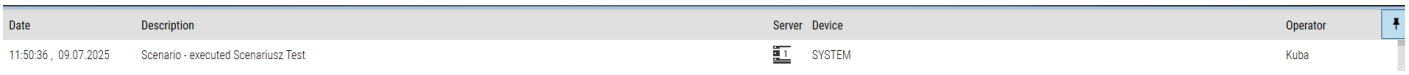


In the Reaction Button tool editing window, you must select the newly created scenario that will trigger the report generation process.



Once the scenario is executed, the report is automatically saved using the button available on the panel. The file is saved to the location previously defined in the system configuration – under the System > General tab, where the save path is specified.

Successful implementation of the report generation process results in an entry in the log window confirming that the operation was completed. For channels that were not being recorded, the recordings are unavailable.



EXCEL:

A	B	C	D	E	F	G	H	I
Device name	Channel name	IP	HDD Status	Total recording time	Recordings from	Recordings to	Device time difference	Firmware
NVR-4108-H1		192.168.40.27	OK				-0d 00:03:57	V8.1.0-20201216
NVR-4108-H1	Channel 4 Main		OK	7d 02:48:40	02.07.2025 08:59	09.07.2025 11:48		
NVR-4108-H1	Channel 4 Division		OK	0d 00:00:00	Unavailable	Unavailable		
NVR-4108-H1	Channel 5 Main		OK	20d 23:33:34	18.06.2025 12:14	09.07.2025 11:48		
NVR-4108-H1	Channel 5 Division		OK	5d 02:47:22	18.06.2025 12:14	23.06.2025 15:02		
NVR-4108-H1	Channel 6 Main		OK	20d 23:33:35	18.06.2025 12:14	09.07.2025 11:48		
NVR-4108-H1	Channel 6 Division		OK	5d 02:47:22	18.06.2025 12:14	23.06.2025 15:02		
NVR-4108-H1	Channel 7 Main		OK	7d 02:48:33	02.07.2025 08:59	09.07.2025 11:48		
NVR-4108-H1	Channel 7 Division		OK	0d 00:00:00	Unavailable	Unavailable		
NVR-4108-H1	Channel 8 Main		OK	5d 20:54:24	18.06.2025 12:45	24.06.2025 09:40		
NVR-4108-H1	Channel 8 Division		OK	5d 02:16:22	18.06.2025 12:45	23.06.2025 15:02		
NVR-4108-H1	Channel 9 Main		OK	0d 00:00:00	Unavailable	Unavailable		
NVR-4108-H1	Channel 9 Division		OK	0d 00:00:00	Unavailable	Unavailable		
NVR-4108-H1	Channel 10 Main		OK	0d 00:00:00	Unavailable	Unavailable		
NVR-4108-H1	Channel 10 Division		OK	0d 00:00:00	Unavailable	Unavailable		
NVR-4108-H1	Channel 11 Main		OK	0d 00:00:00	Unavailable	Unavailable		
NVR-4108-H1	Channel 11 Division		OK	0d 00:00:00	Unavailable	Unavailable		

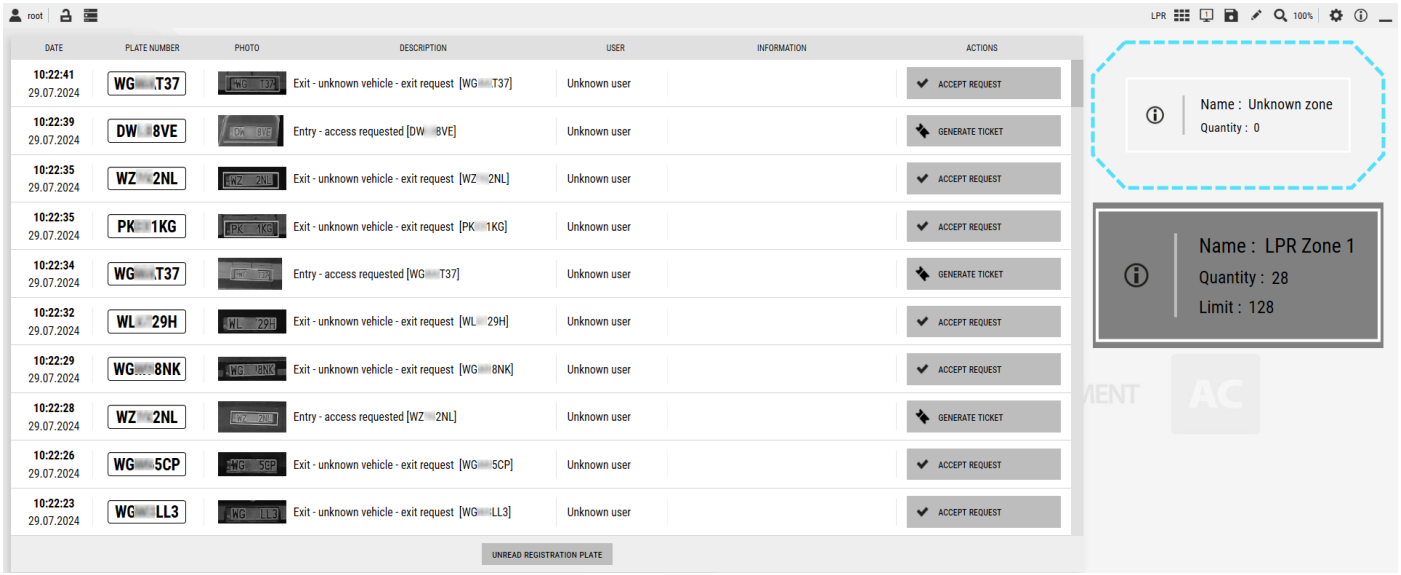
HTML:

Device name	Channel name	IP	HDD Status	Total recording time	Recordings from	Recordings to	Device time difference	Firmware
NVR-4108-H1		192.168.40.27	OK				-0d 00:03:57	V8.1.0-20201216
NVR-4108-H1	Channel 4 (Main)		OK	7d 02:48:40	02.07.2025 08:59:40	09.07.2025 11:48:20		
NVR-4108-H1	Channel 4 (Division)		OK	Unavailable	Unavailable	Unavailable		
NVR-4108-H1	Channel 5 (Main)		OK	20d 23:33:34	18.06.2025 12:14:47	09.07.2025 11:48:21		
NVR-4108-H1	Channel 5 (Division)		OK	5d 02:47:22	18.06.2025 12:14:48	23.06.2025 15:02:10		
NVR-4108-H1	Channel 6 (Main)		OK	20d 23:33:35	18.06.2025 12:14:46	09.07.2025 11:48:21		
NVR-4108-H1	Channel 6 (Division)		OK	5d 02:47:22	18.06.2025 12:14:48	23.06.2025 15:02:10		
NVR-4108-H1	Channel 7 (Main)		OK	7d 02:48:33	02.07.2025 08:59:51	09.07.2025 11:48:24		
NVR-4108-H1	Channel 7 (Division)		OK	Unavailable	Unavailable	Unavailable		
NVR-4108-H1	Channel 8 (Main)		OK	5d 20:54:24	18.06.2025 12:45:47	24.06.2025 09:40:11		
NVR-4108-H1	Channel 8 (Division)		OK	5d 02:16:22	18.06.2025 12:45:48	23.06.2025 15:02:10		
NVR-4108-H1	Channel 9 (Main)		OK	Unavailable	Unavailable	Unavailable		
NVR-4108-H1	Channel 9 (Division)		OK	Unavailable	Unavailable	Unavailable		
NVR-4108-H1	Channel 10 (Main)		OK	Unavailable	Unavailable	Unavailable		
NVR-4108-H1	Channel 10 (Division)		OK	Unavailable	Unavailable	Unavailable		
NVR-4108-H1	Channel 11 (Main)		OK	Unavailable	Unavailable	Unavailable		
NVR-4108-H1	Channel 11 (Division)		OK	Unavailable	Unavailable	Unavailable		

9.6 LPR - license plate recognition

General description of the functionality of the parking system implemented using the LPR license plate recognition function:

- cooperation with Novus LPR cameras connected to NMS AC directly or via NMS software
- control of vehicle access to defined zones in accordance with specific schedules
- the ability to define parking zones and assign them different levels of access
- defining limits on the number of vehicles in defined zones
- visualization of vehicles in defined zones
- assigning license plate numbers as user IDs
- defining the database of vehicle license plate numbers along with additional information about the vehicle, vehicle owner and expiry date
- recording the history of recognized license plate numbers with the possibility of subsequent export
- the possibility of cooperation with thermal transfer printers in order to print tickets containing such information as, m.in, recognized license plate number, allowed time in the zone, date and time of ticket printing and others



9.6.1 LPR - License plate recognition

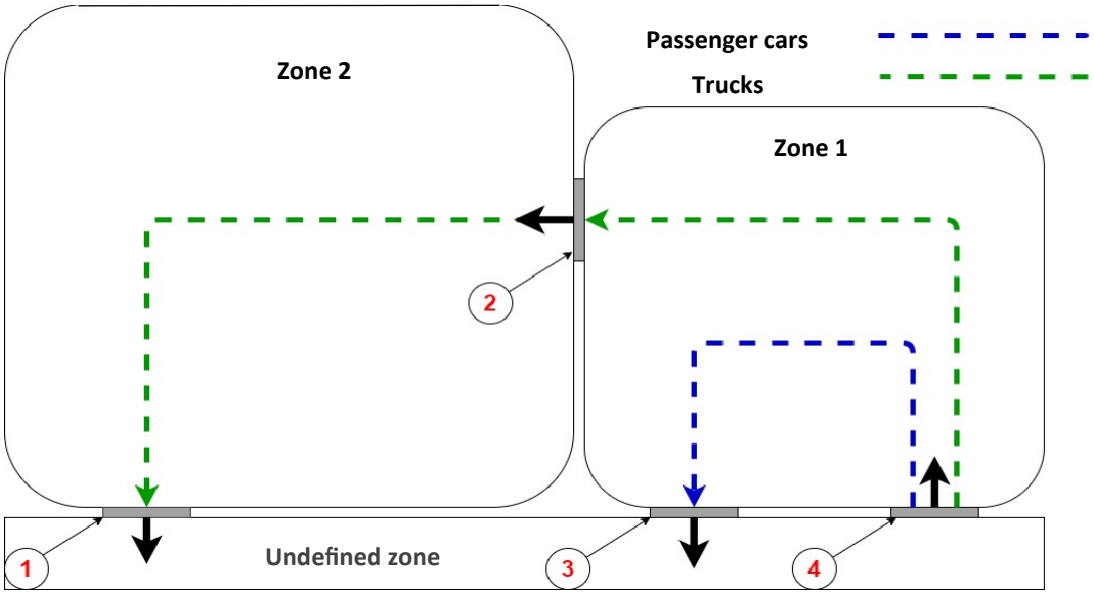
NMS AC software integrated with IP cameras equipped with LPR functions allows you to control the access of vehicles to pre-defined zones.

Assuming that:

You want to have control over two separate zones, as in the figure below.

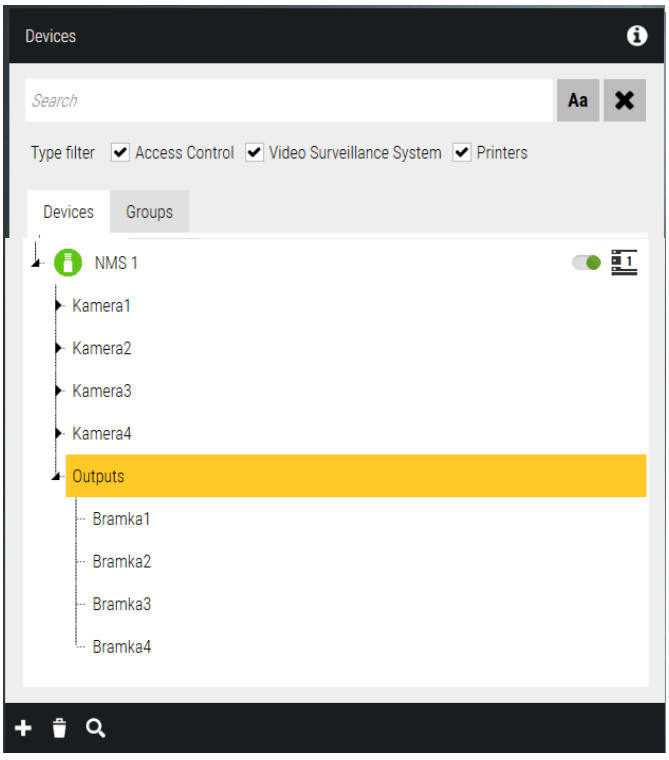
Zone 1 can be accessed by the group": "Passenger cars" and the group "Trucks".

Zone 2 can be accessed by the "Trucks" group.



The numbers 1-4 indicate both the numbers of mounted cameras and relays controlling devices such as barriers or gates.

The program should be configured as follows:



9.6.2 Adding Devices

In order to ensure control over vehicles entering and leaving specific zones, cameras equipped with license plate recognition functions should be installed when entering/leaving the zone, and then adding them to the NMS AC program.

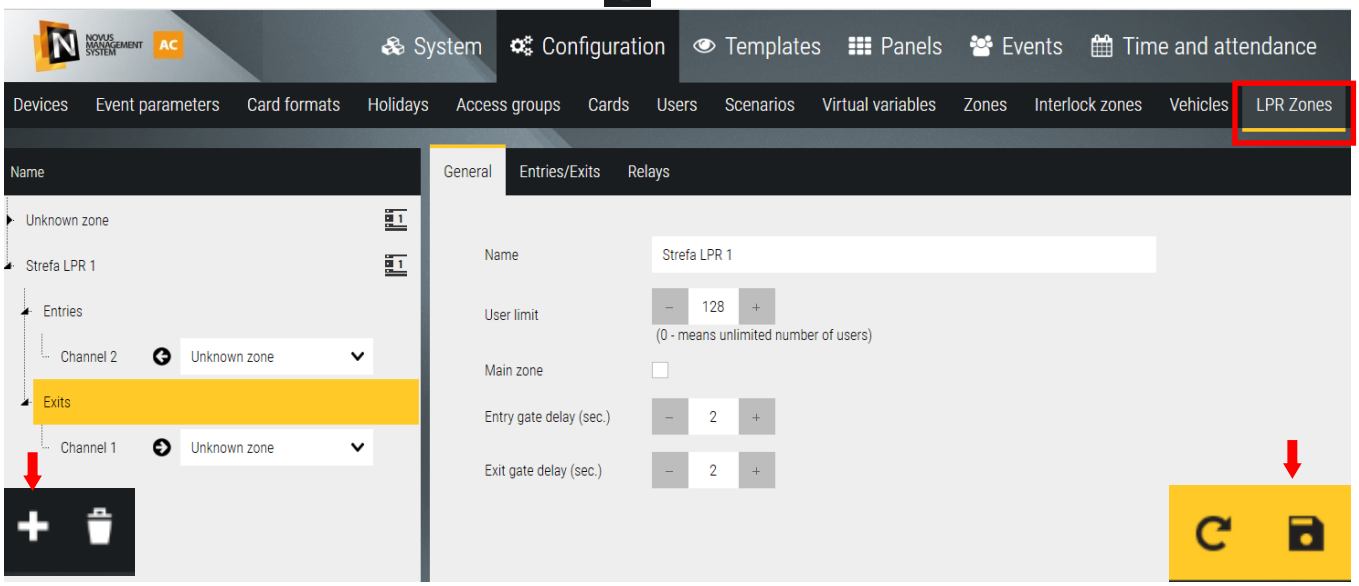
The process of adding VSS devices is described in Chapter 3.10 CCTV. In the example above, the cameras added to the system were named according to the figure next to it.

IMPORTANT! To ensure proper operation of an LPR camera, go to the Devices > Details tab of the selected LPR camera and set the Event Method field to **LongPolling**. This setting must be applied individually for each camera.

9.6.3 LPR Zones

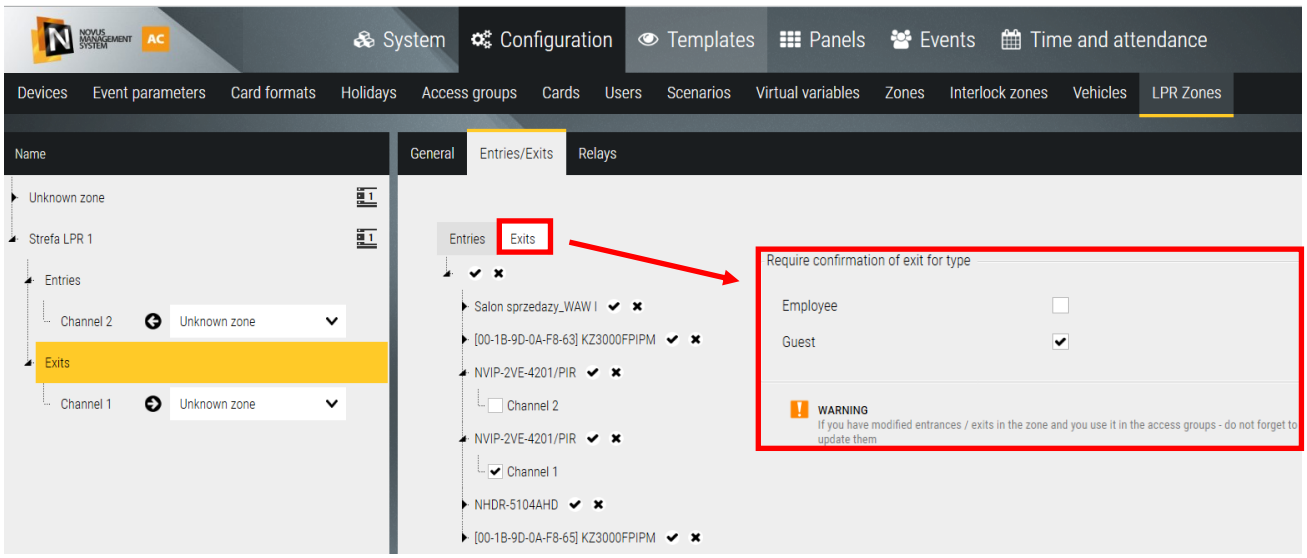
9.6.3.1 Configuration Zones

After you add devices to NMS AC, you must create virtual zones in the program. To do this, go to the Configuration tab > LPR Zones and click on the icon with the plus symbol, add the required number of zones.



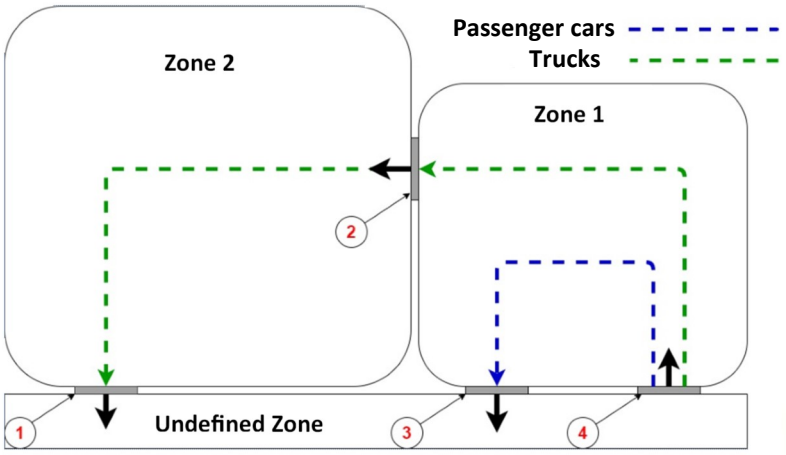
After clicking on the selected zone, in the "General" tab there are fields:

Name - allows you to name the zone
User limit - determines the maximum number of vehicles that can be in the zone at the same time
Main zone - after leaving the main zone to the unspecified zone, the ticket expires
Delay of the entrance / exit gate - this is the time of delaying the operation of the relay output controlling the entrance / exit gate.



In the "**Entries/Exits**" tab, you can assign individual cameras according to the entries and exits from the zone marked in yellow.
Buttons are used to select and deselect multiple channels at once.

The button is used to delete individual zones after selecting them.
After clicking "**Departures**", in addition to the possibility of assigning appropriate cameras to trips, you can also define for which of the 4 special groups (Employee, Guest, Administrator, Security) the trip to the unspecified zone will require confirmation by the operator (departure request).



Entries/Exits

According to the figure:

At the entrance to **Zone 1** there is a **camera 4**.

On two departures from **Zone 1** there are **cameras 2 and 3**.

Therefore, the entrances and exits for **Zone 1** should be set as in Figure(1).

Entry to **Zone 1**:

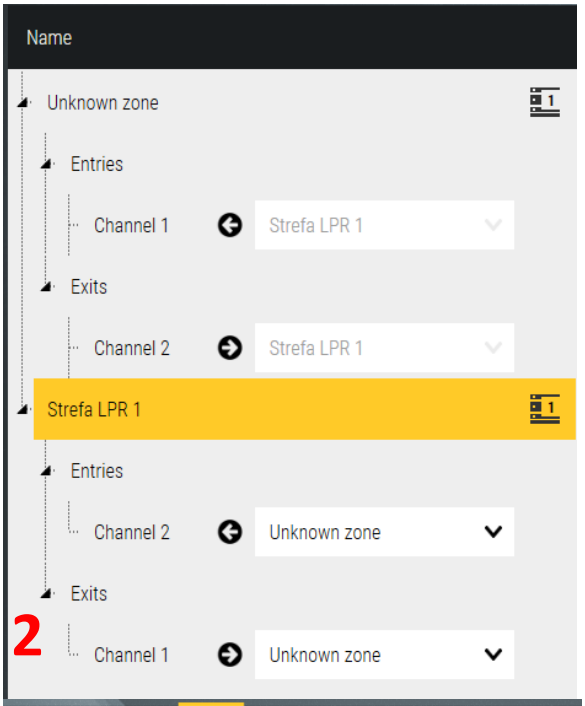
From the "Indeterminate Zone" monitors **camera 4**

Departure from **Zone 1**:

To the "Indeterminate Zone" monitors **camera 3**

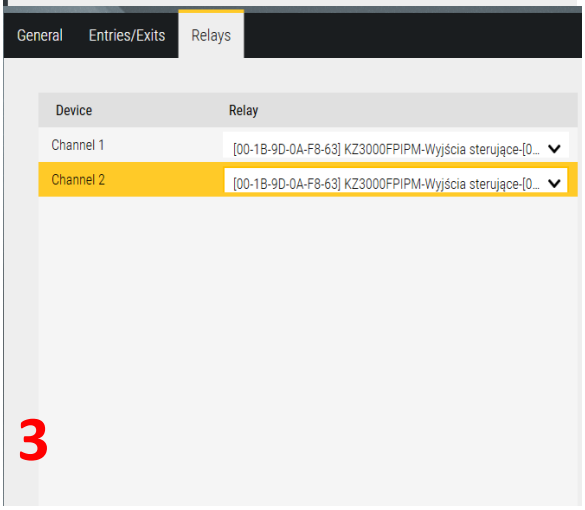
For "Zone 2" monitors **camera 2**

Thus, the drop-down menu on the left side of the panel should be configured as in Figure (2).



Relays

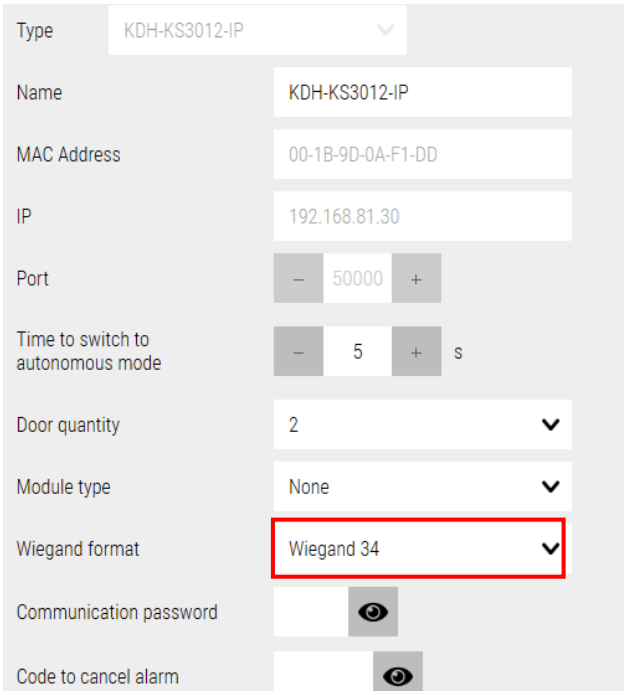
The LPR Zones configuration step can be completed by assigning relays to the appropriate devices. The names of the devices and relays were previously defined when adding devices in section 9.5.1. Due to the fact that in the adopted project, each camera is to control the gate at which it is placed, the relays should be configured in the same way as in the figure (3).

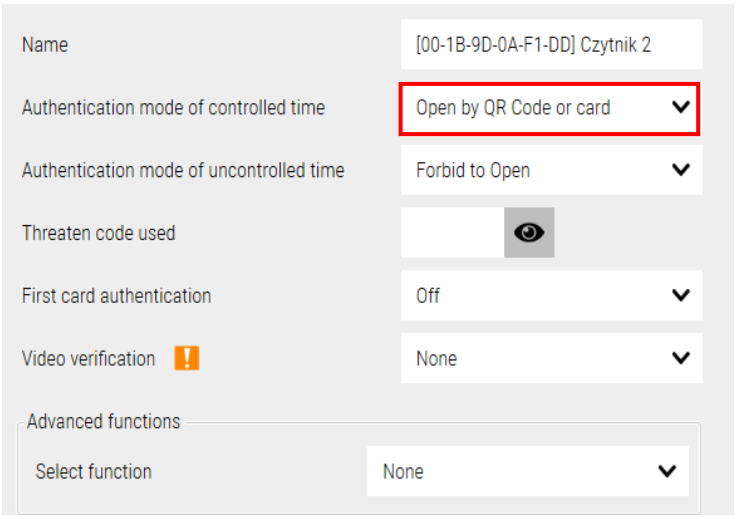


9.6.3.2 Guest Exit Handling Using Controller, Reader, QR Printer, and LPR Camera

To exit the LPR zone, the guest must scan the issued ticket at the reader, which automatically opens the barrier and records the event in the system. The LPR camera captures the vehicle's license plate number, which is then linked to the issued ticket, enabling later verification and exit control.

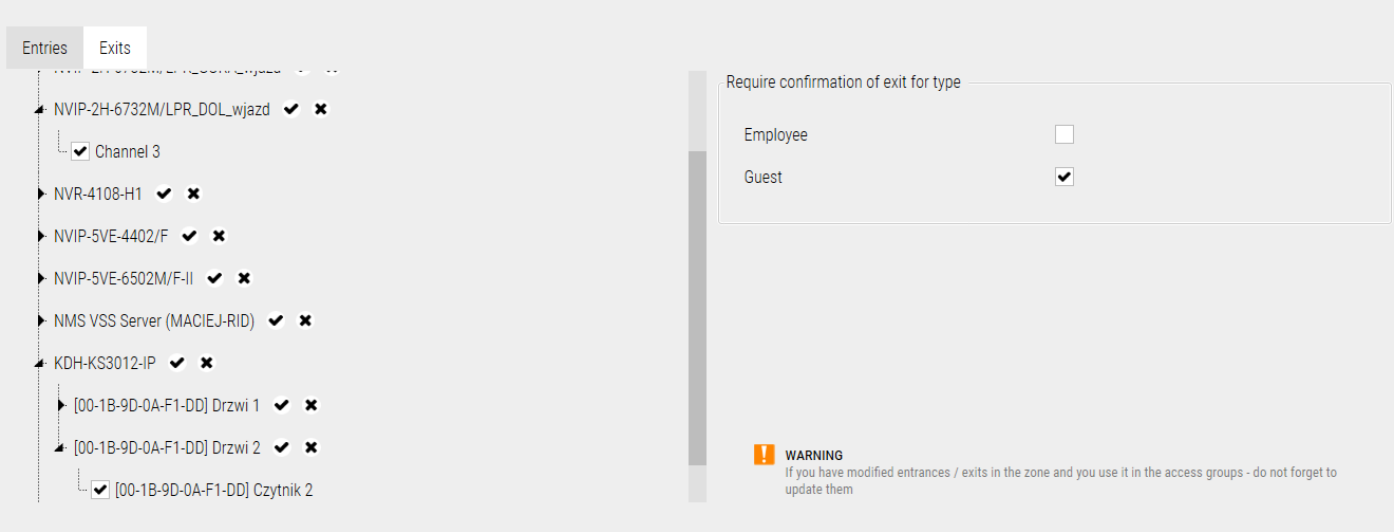
An example configuration of the reader for the selected Access Control device — in this case, the KDH Series 3000 — is shown in the images below:





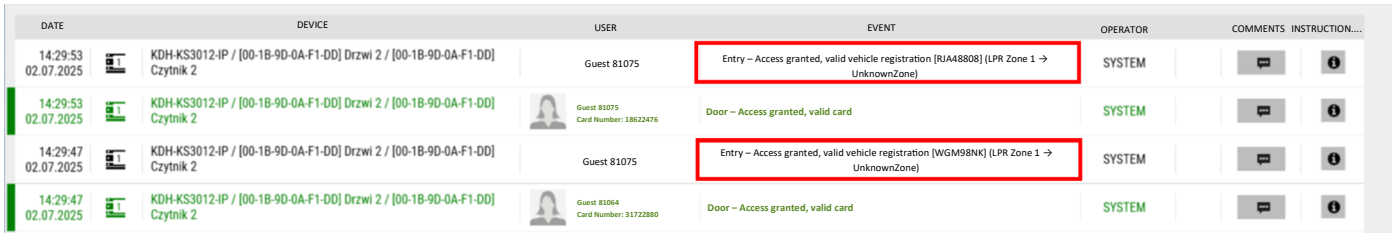
IMPORTANT! For the reader to correctly read QR codes from tickets, the Wiegand format must be set to Wiegand 34 in the Access Control device configuration.
Additionally, in the Details tab of the selected reader, the Identification Mode during Active Time field must be set to QR Code or Card.

Additionally, in the LPR Zones tab, you must select the next device as the exit point—in addition to the selected LPR camera, also add the Reader, and enable the option requiring exit confirmation for the Guest type.



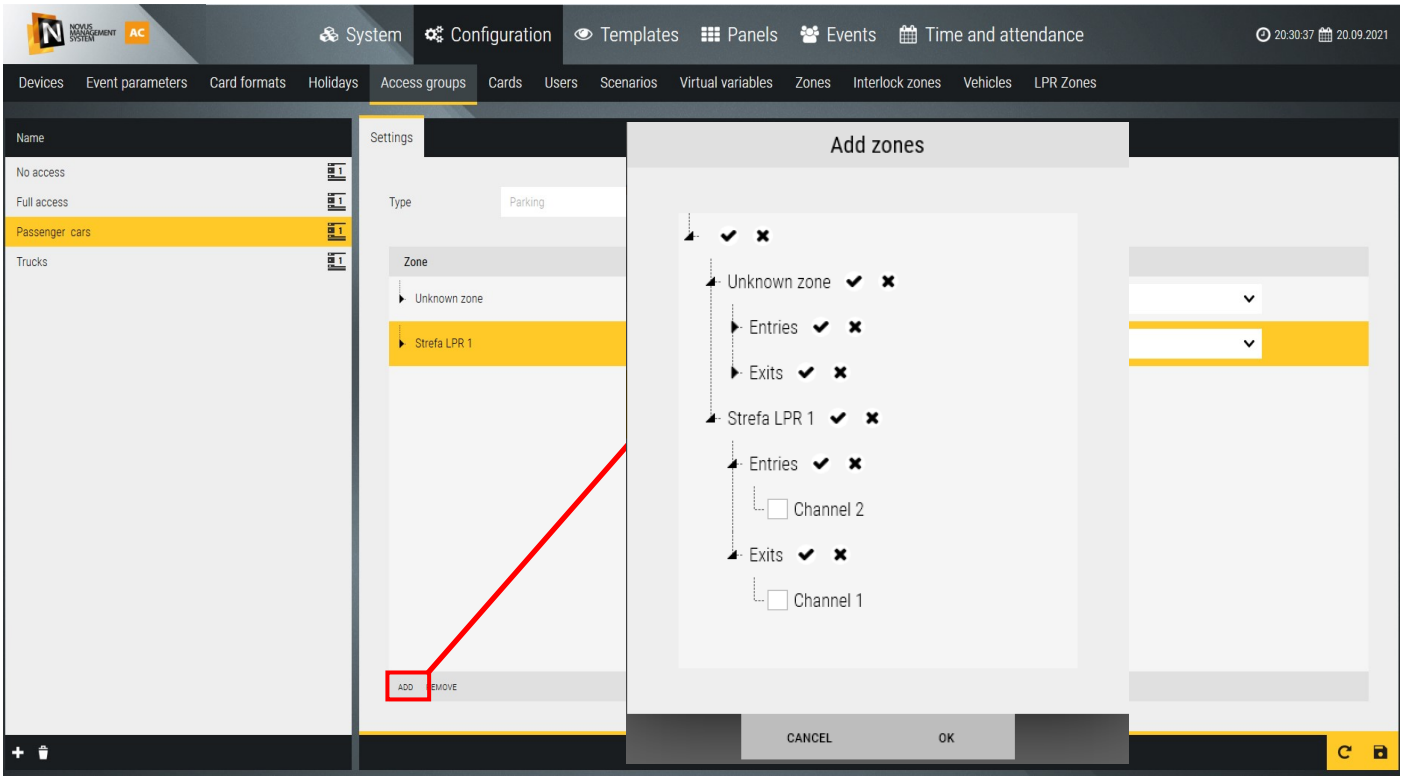
In the Relays tab, assign the newly created outputs to the previously configured output responsible for actions such as raising the barrier during exit from the zone—similarly to how the LPR camera is assigned to the exit.

As a result, after presenting the QR ticket to the reader, log entries should appear confirming a successful exit from the LPR zone with a valid ticket.



9.6.4 Access levels - parking

The access level menu is described in Chapter 4.2 Access Levels, using the example of defining access to doors and elevators. In the case of LPR, instead of doors and elevators, the user has to deal with zones to which access is



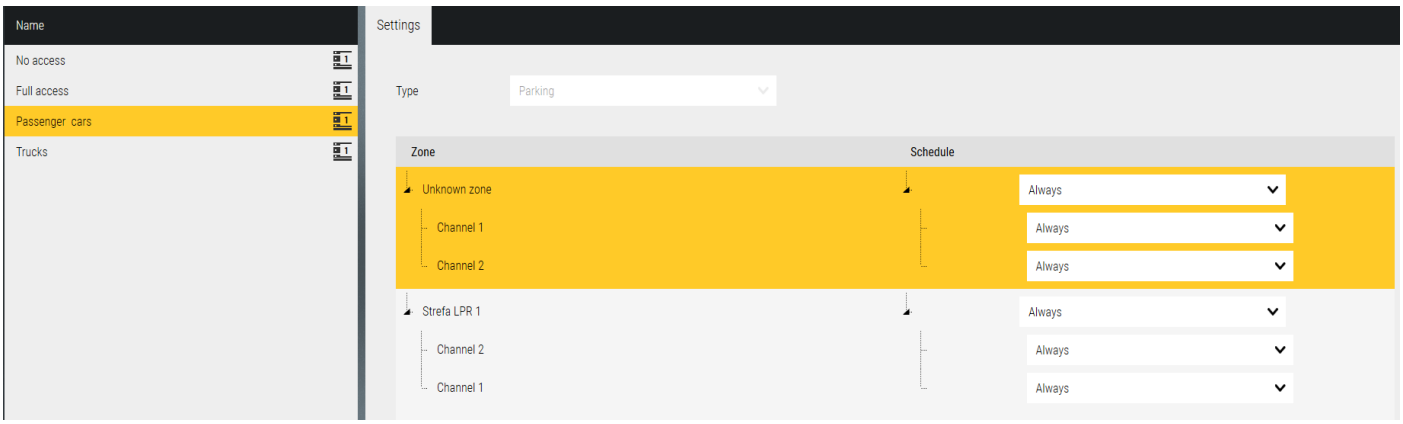
controlled m.in by LPR cameras.

In the example project, you need to create two levels of access:

Passenger cars—who will have access to Zone 1 and will be able to pass through Gates 3 and 4.

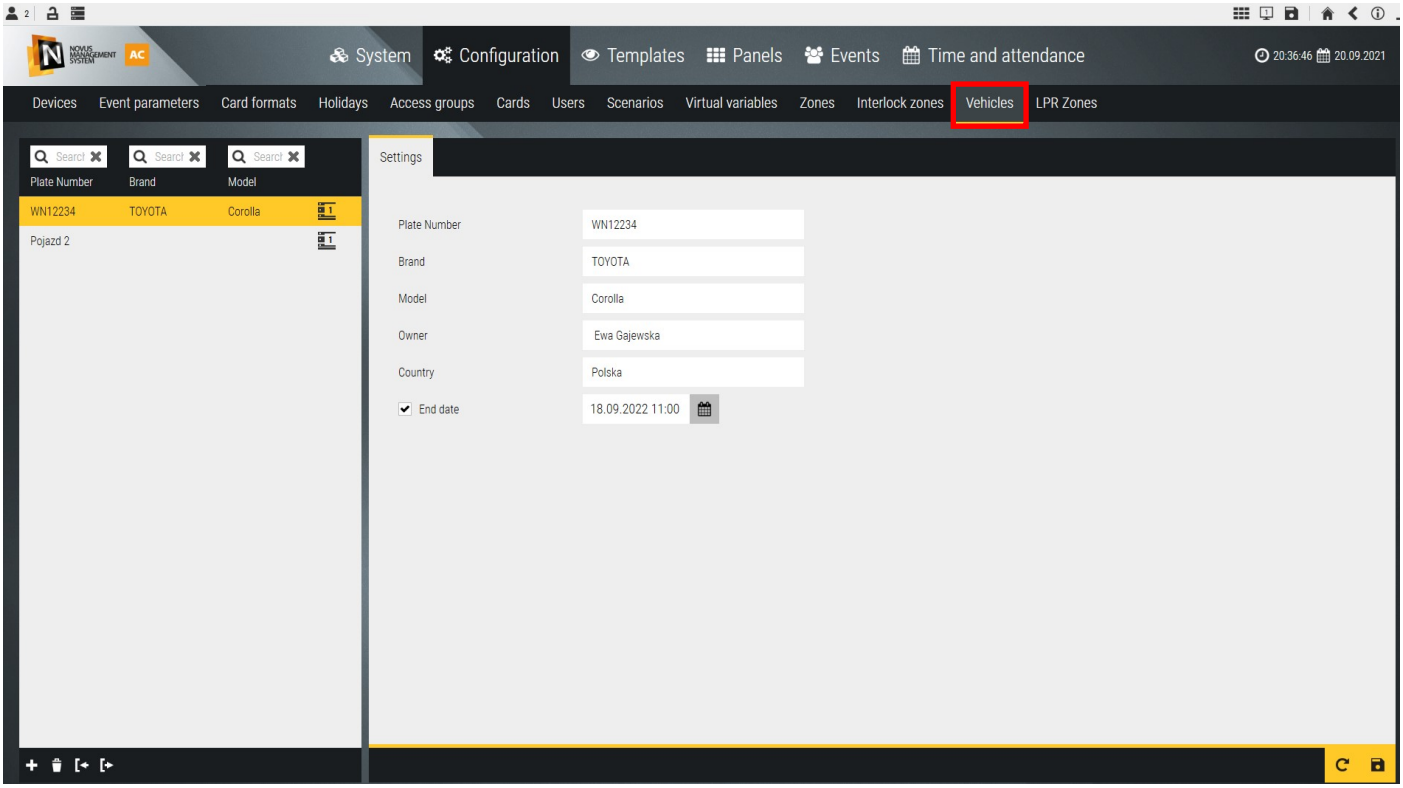
Trucks – which will have access to Zone 1 and Zone 2 and will have the opportunity to pass through gates **1,2,4.**

To do this, click on the + icon and add the two levels of access above. To rename newly created access levels, double-click it. After naming and clicking on the newly created level, it will light up in yellow, in the Settings tab you need to change the type to Parking. Then, by clicking the Add button, you will be able to define access to individual entries and exits for each of the levels separately. According to the project assumptions on page 85, access to the zones by trucks should be configured as in the figure below. Finally, in the schedule column, change Never to Always for each zone.



9.6.5 Vehicles

The Vehicles tab is used to create a vehicle base. Information such as registration number, make, model, owner and country are stored there. The program also allows you to define the time after which the vehicle will be removed from the base. To add a vehicle to the database, click the + icon, then to complete the information about the vehicle, click on the newly created field and in the Settings tab fill in the relevant information.

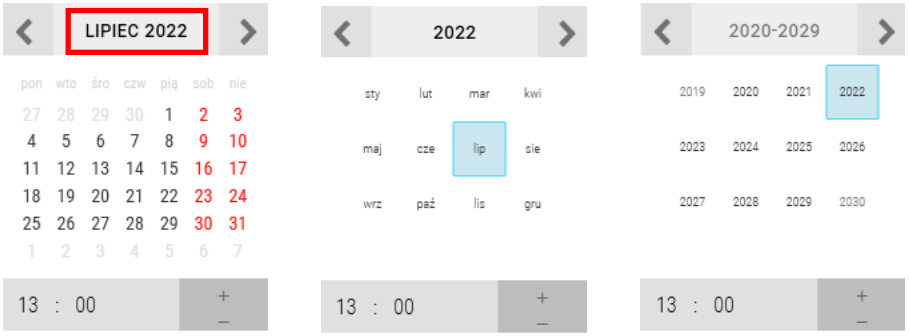


Buttons:

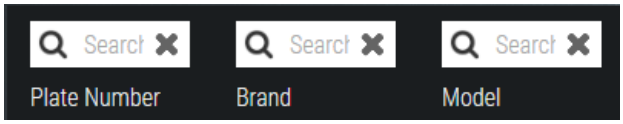
- is used to import the vehicle database in .csv format,

- is used to export the vehicle database in .csv format,

The **End Date** field is used to specify the expiration date of an item in the vehicle database. If this box is unchecked, the vehicle will not be automatically removed from the base. The date and time can be set by clicking on the calendar icon. To go to the month selection and then to the years selection, click the box selected in the figure below. Below the calendar is a time checkbox, you can type it from the keyboard or use the buttons. +/-

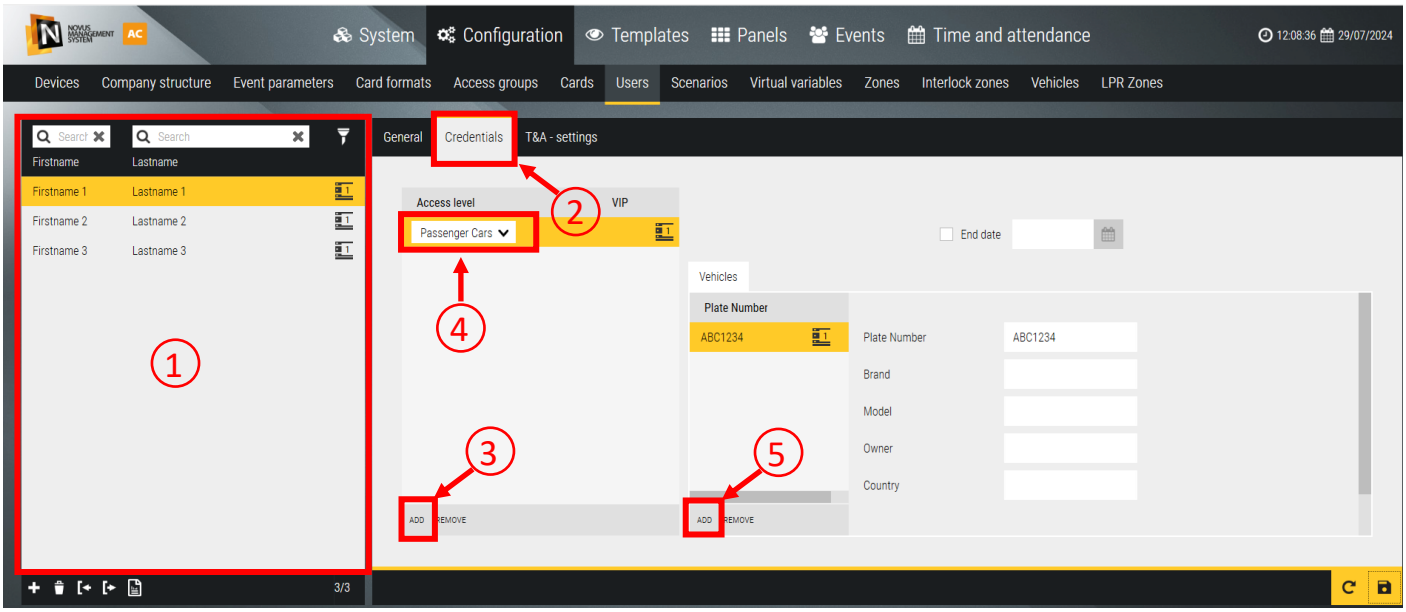


Above the list of added license plates there is a search engine that allows you to narrow down the list of license plates by license plate number, make and model of the car.



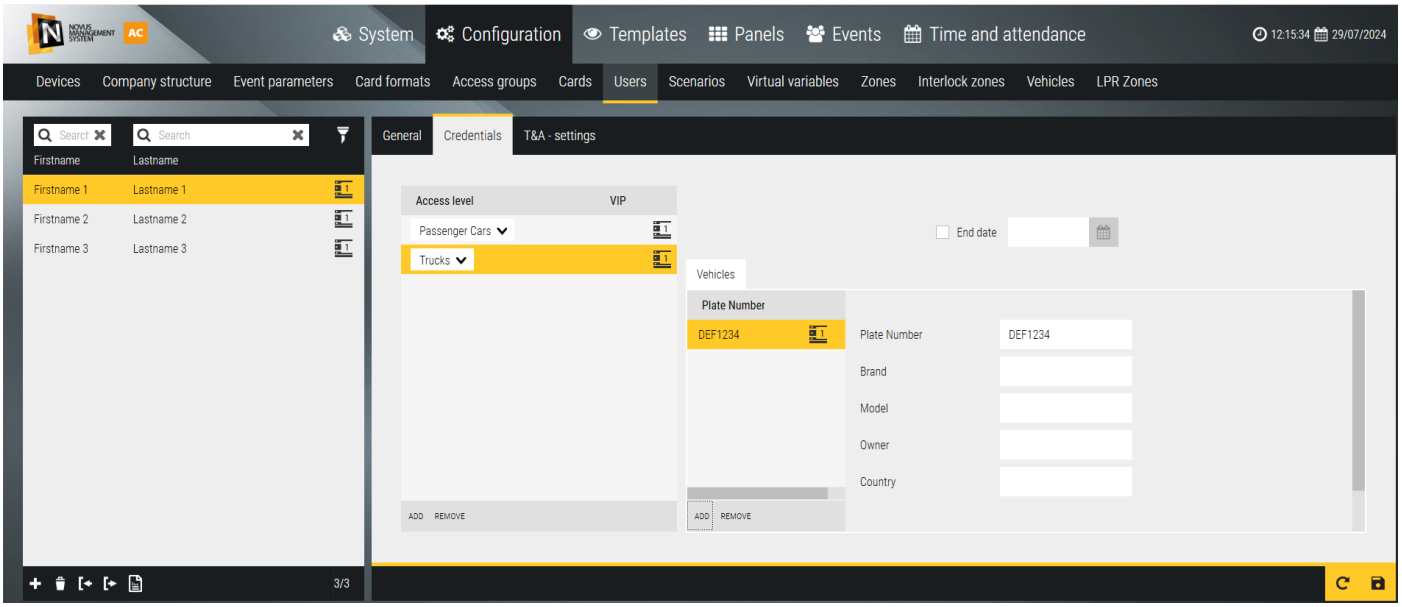
9.6.6 Users - Identifiers

Granting users permission to enter specific zones is carried out using the Users>Identifiers tab. This involves assigning a vehicle to the user (from a previously created vehicle database) and giving it a specific level of access. A full description of the Users tab is available in this manual in **section 4.4 Users.**



Assuming that the user should have access to the "Passenger Cars" zone by car with ABC 1234 registration, and to the "Trucks" zone - by car with DEF 1234 registration, first select it from the menu on the left (1) and go to the Credentials tab (2). In the Access Levels field, click the Add button (3), then the "No access" level will be set by default, in the (4) field it should be changed to "Passenger cars". Then, after clicking Add (5), a list of vehicles assigned to this user (defined earlier in the Vehicles tab) will be displayed, you need to add a vehicle with registration ABC 1234. The above method has been configured bookmark in the figure above.

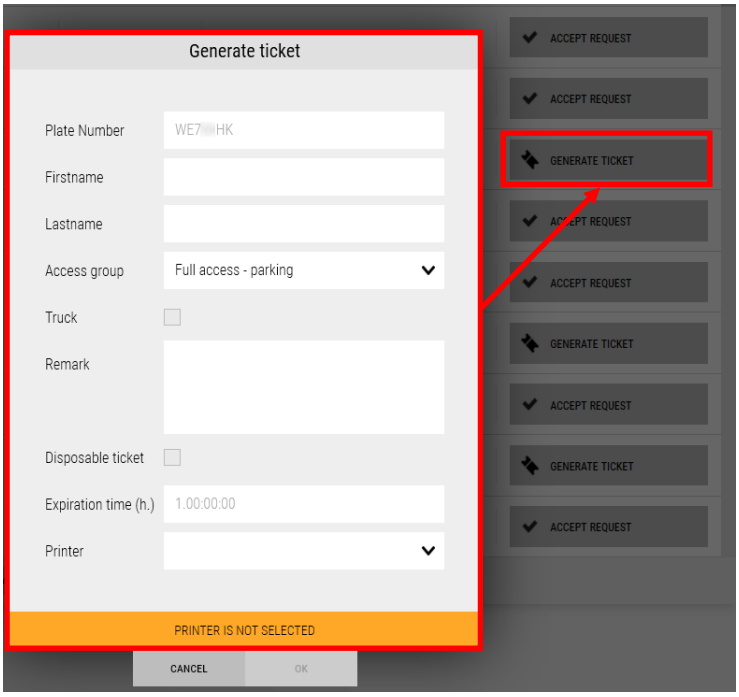
In the case of access to the second zone, the access level "Trucks" should be added and the action repeated, with the difference that in field (5) a vehicle with registration DEF 1234 should be added, as in the figure below.



9.6.7 Tools in the LPR panel

To gain insight into the operation of the vehicle license plate recognition system, NMS AC software allows you to create panels tailored to the user's needs. The process of adding panels and their configuration is described in more detail in **Chapter 6. Panels. In order to properly operate the vehicle access control system, it is best to use at least two tools.**

The most important tool is the **LPR Events** window. It is used to display events related to the recognition of license plate numbers and to manually manage the entry and exit of cars from individual zones. When a license plate is detected, the system displays the time of the event, the photo of the plate, the license plate number and the description of the event in the window. The description may include, inter alia: information on the mixing of vehicles between zones; information on whether or not vehicles have been granted access to the zones; information on the validity of tickets; access requests.



A special event is the **access request**, which is displayed when an unknown vehicle wants to enter from an unspecified zone to zones under access control. The person supervising the operation of the system can click the **Generate Ticket** button, then a window will be displayed in which you must provide information related to the vehicle entering. The person generating the ticket can assign the vehicle the appropriate level of access and define the validity time of the ticket. In case the ticket printout fails, the **Reprint button** appears after the ticket is generated.

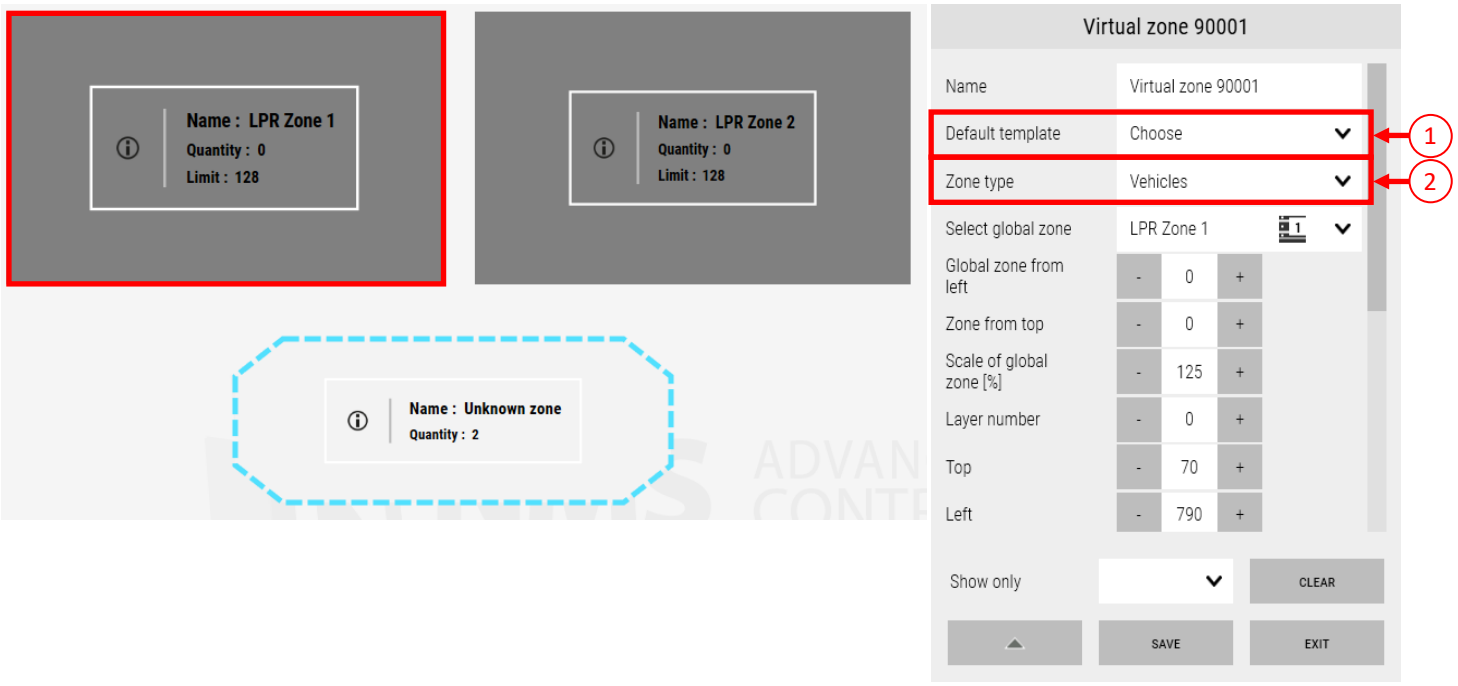
To print a ticket, a dedicated printer should be added to the system. This can be done in the Configuration> Devices tab. For more information on adding devices to NMS AC, see Chapter **3.System Configuration.**

An example ticket for a vehicle with registration "ABC 1234" is shown in the figure next to it. The ticket, in addition to the information supplemented when generating it, has a unique QR code.

Virtual Zone

Another tool used in the LPR panel is the **virtual zone.**

The process of adding zones to the panel is already described in this manual **in Chapter 9.2 Global Zones.**



A Special type is the Unspecified Zone, it represents the area outside the zones covered by access control (e.g. the street from which you enter the object covered by the access control system). The other zones added to the panel can be assigned previously created (ch. 9.5.2) LPR Zones. To do this, in edit mode, left-click on the newly created zone and in the edit window select **Zone Type** (1) :

Vehicles and in the **Select global zone** field (2) select the LPR zone or the unspecified zone. The rest of the settings concern the appearance and location of the zone in the panel.

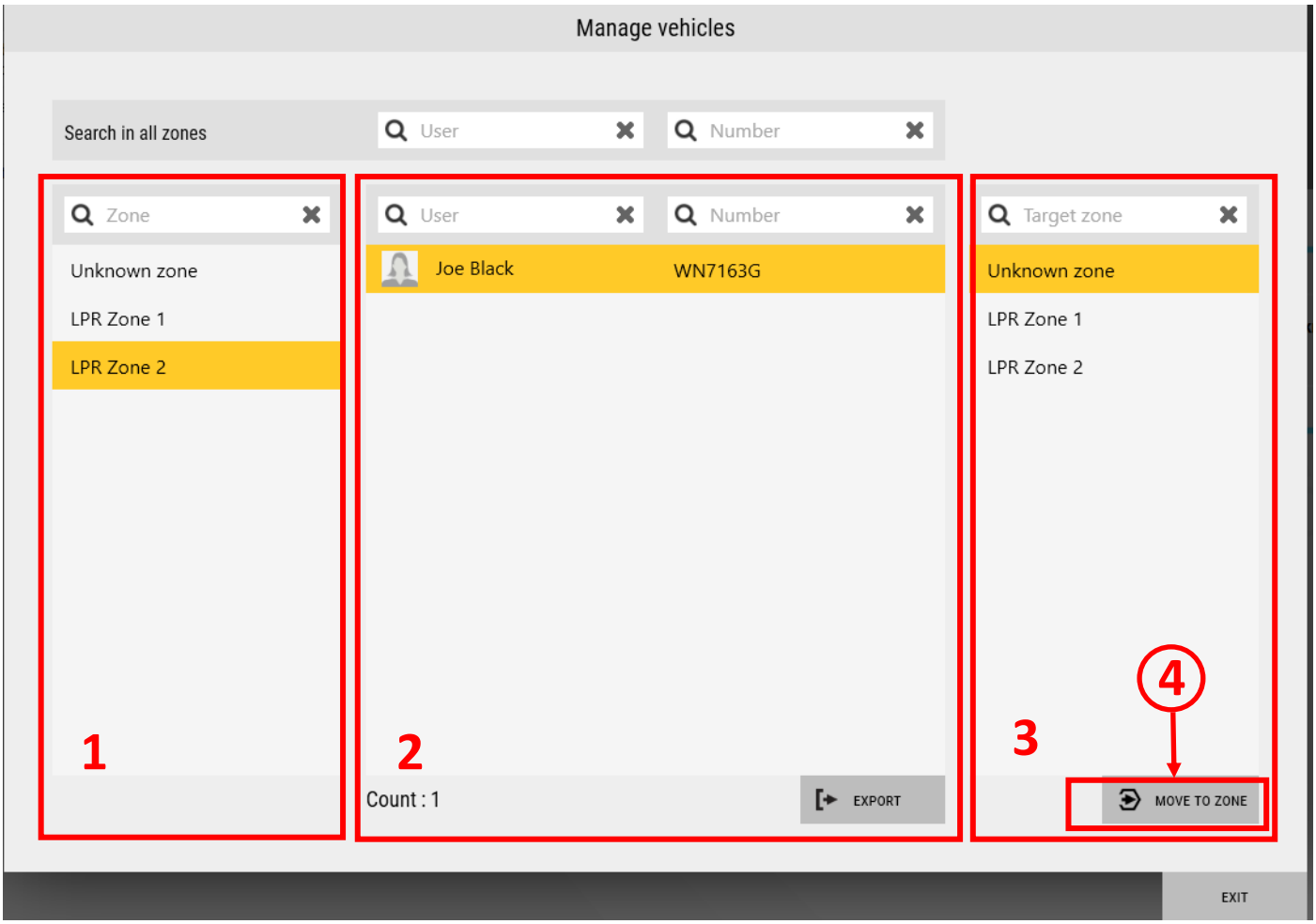
After configuring the newly created zone, information such as:

- name
- number of vehicles currently in the zone the
- limit of people who can be in the zone at the same time.

After right-clicking on the virtual zone, a list will be displayed next to it with the license plate numbers of the vehicles in the zone and the names of their users.

Management of vehicles located in zones

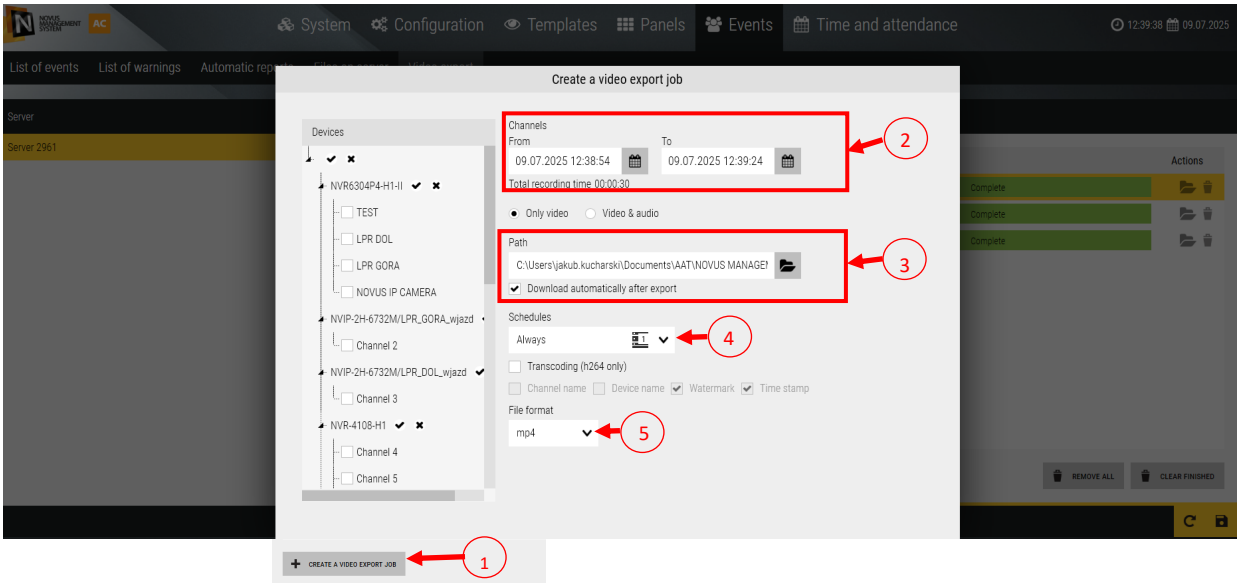
After clicking the left mouse button on any zone, the user has the option to go to the vehicle management window. Field (1) is used to select the zone from which the preview is displayed in the middle field (2). Field (2) is used to view which users are currently in a given zone. In the event of non-compliance of information on vehicles in the zone with the actual state of affairs, the user has the possibility to transfer vehicles from that zone to the target zone (3). To do this, select the selected user and the target zone and click the **Move to Zone button** (4).



9.7 Exporting Recordings

9.7.1 Exporting Recordings from the Main Menu

To export recordings stored on network recorders connected to the system (e.g., NMS, NVR, NHDR NOVUS), go to the Events tab, then select Video Export, and click the Create Export Task button (1).
A window will appear where you must first select the cameras from which the recordings are to be exported. This can be done on the left side of the window by checking the desired video channels.



In field (2), click the calendar icon to select the time range for the recordings to be exported.
Below that, you can choose whether the exported recording should include video and/or audio (this feature will be available in the future).
Note that recordings are exported from the recording devices to the NOVUS MANAGEMENT SYSTEM AC server.

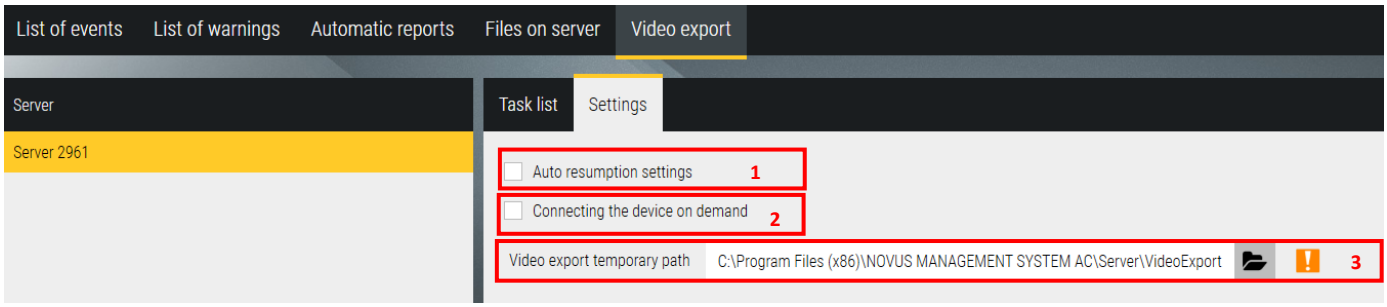
To have the recordings automatically downloaded and saved to a selected path on the workstation where the NOVUS MANAGEMENT SYSTEM AC client is installed, check the box “Download automatically after export” in field (3).
Otherwise, the recordings will be exported to the server and will be available for manual download by clicking the button  next to the blue status bar labeled “Ready to download.”

The Schedules function (4) is used for periodic export of recordings and will be available in the future.
You can also choose the format in which the recordings will be exported (5); available formats are AVI and MP4.

After clicking OK, the settings will be saved. To export and download the recordings, click the floppy disk icon  located in the bottom-right corner of the window. Once the recordings are successfully downloaded, the status Completed will be displayed.

The folder icon  opens the folder where the downloaded recordings were saved, while the trash icon  removes the selected item from the list.

Additionally, new options have been added in the Settings tab: Automatic reconnection to devices and On-demand device connection. These features help optimize system performance, especially in environments with a large number of cameras and recorders.



1. **Auto resumption settings** - The system automatically attempts to retrieve recordings again in the event of temporary connection loss or other technical issues.

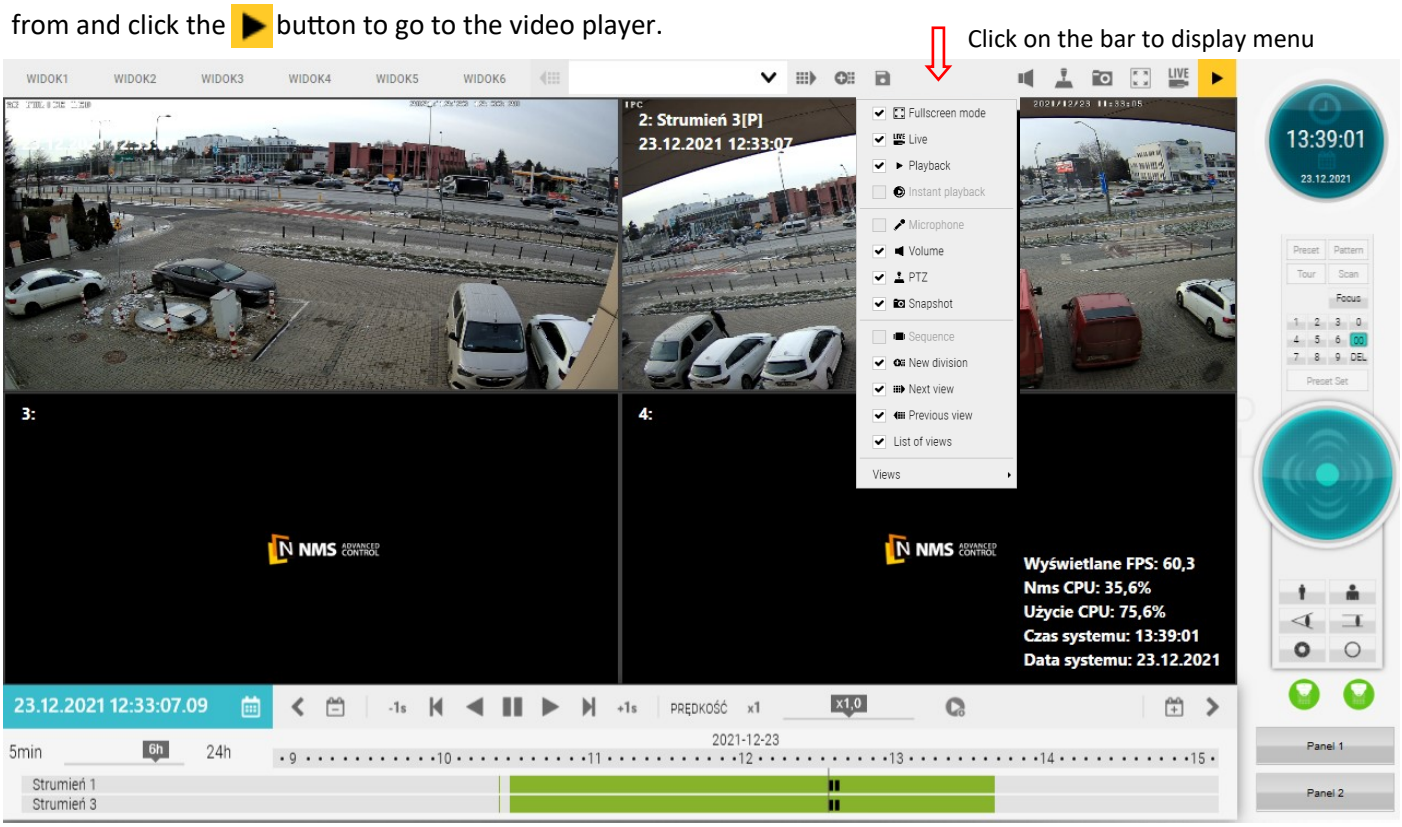
2. **Connecting the device on demand** - This option allows the system to automatically establish a connection with a device when a video export request is made. If this option is disabled, the user must manually connect to the device.

3. **Video export temporary path** - The system uses a local temporary path to store files before they are finalized or downloaded.

Thanks to these options, it is possible to reduce network and server load while maintaining full system functionality.

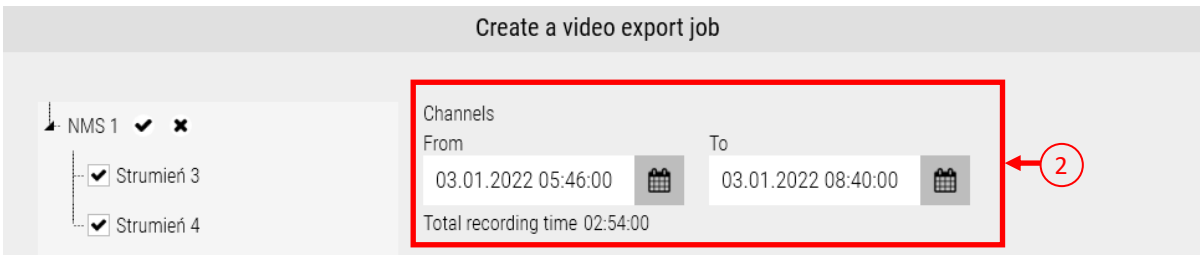
9.7.2 Export recordings from the video player

The second way to export recordings from NMS server consist in go to the panel where the player and video window are placed. It can be done by going to the default defined panel 3. To do this, click on the icon located on the right side of the top interface bar. Next, select the view with the cameras you want to export recordings from and click the button to go to the video player.



To export recordings, first select the desired time period. There are two ways to define the time period from which the recordings are exported. One of them was mentioned on the previous page. The second way is to drag the mouse cursor along the timeline while holding the right mouse button.

So firstly select area on the timeline and click the export icon **(1).** Next, the **Create a video export job** window appears and the field **(2)** is automatically filled in for each selected channel according to the selection on the timeline.

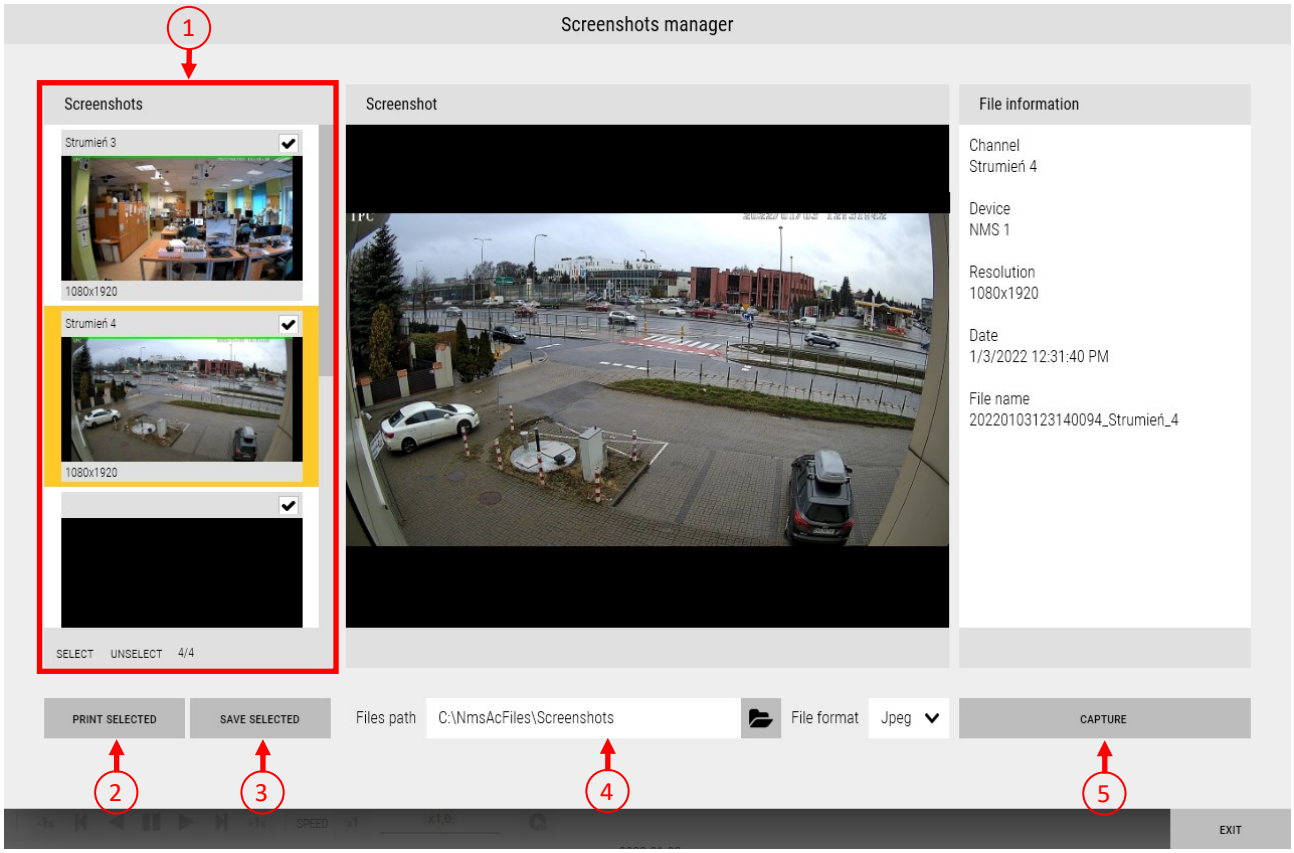


At the end to export and download selected recordings, follow the same procedure as described in the section **Export recordings from the main menu** on the previous page.

9.8 Downloading screenshots

To make a screenshots go to the panel where the video window is located. It can be done by going to the default defined panel 3. To do this, click the icon located on the right side of the top interface bar. Then, in the video window select the view with the cameras you want to make a screenshot. Depending on whether you want to take a screenshots from, click the appropriate icon (live view and video player) in the upper right corner of the video window.

To go to the screenshot manager, click the camera icon .



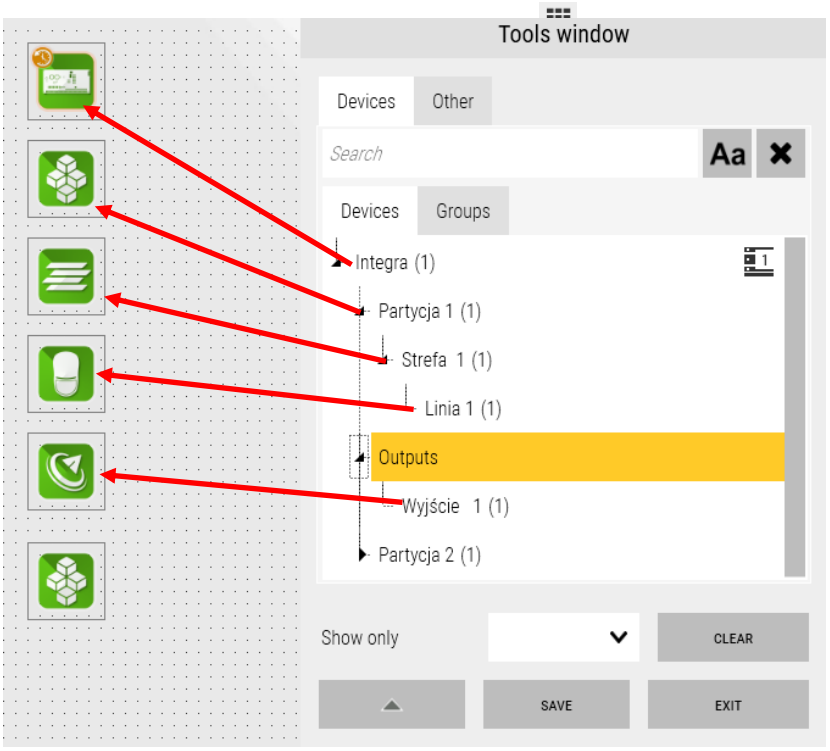
In the screenshots manager field **(1)** is possible to select channels from which images are captured. Use the **Capture** button **(5)** to capture the image currently displayed on the player, if the player is set to "live" mode, the current camera view is captured. The path to the folder where captured images are saved can be entered in the field **(4)** or indicated manually by clicking the icon, next to it is a **File Format** field where you can choose from a drop-down list the format in which the image should be saved (Jpeg, Png or Bmp). Click the **Print Selected (2)** button to print the photos directly without saving them on the computer, the **Save Selected (3)** button saves the photos to a designated file directory.

9.9 - Integration whith Intrusion & hold-up alarm systems

The NOVUS MANAGEMENT SYSTEM AC program enables integration with the Intrusion and Hold-Up alarm system. Adding devices has been described in this chapter **3.13Devices — Intrusion and Hold-Up alarm system (I&HAS)**.

Connected devices can be operated from the Panels described in chapter **6. Panels**.

Modifications or creation of new operator panels allows you to take full advantage of the possibilities of integration with the Intrusion and Hold-Up alarm system . To do this, select a operator panel using the button in the main bar of the program, then select the appropriate operator panel.



After selecting a operator panel, you can edit it using the pencil icon.

Tools Window displaying all elements for alarm panel configuration are located.

In the Devices tab, you can find previously added I&HAS devices. They can be moved to the operator panel by dragging the panel itself, object, partition, zone or output.

After exiting the edit mode, clicking the mouse left button on the device icon allows you to display its list of events.

The list of events for the panel, object or partition corresponds to the operation from the chapter 3.XX Devices — Intrusion and Hold-Up alarm system (I&HAS) — Operations.

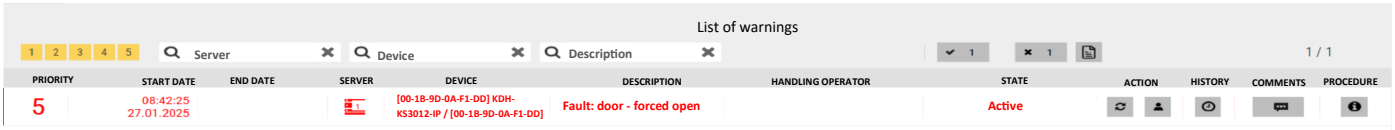
Actions that can also be performed include bypassing/unbypassing inputs and controlling the activation and

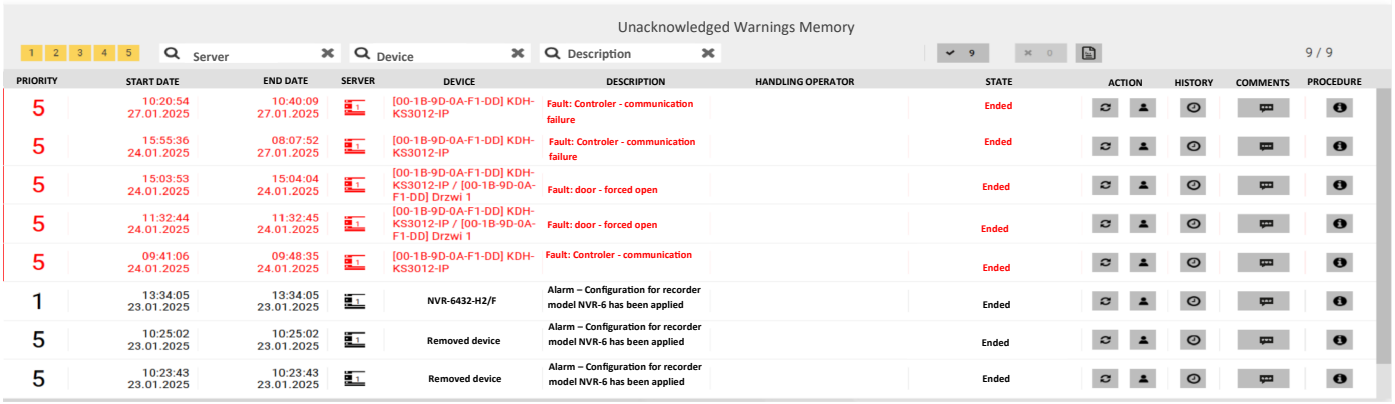
9.10 - Warning management tool: visualization and reporting

The Warnings tool provides a visual overview of the status of system components operating on-site, focusing on potential failures and alarms (warnings). When the require comments option is enabled, every event defined as an alarm or failure must be commented on by the system operator.

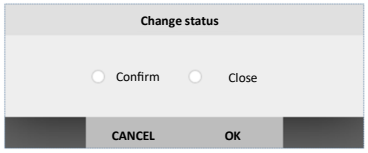
It is possible to generate reports that show the current status of alarms/failures (warnings) on the site, as well as the history of their occurrence along with operator comments.

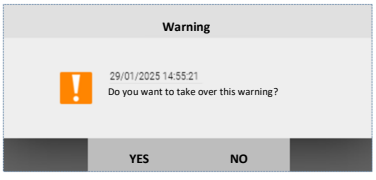
The tool is divided into two parts. The first part is a list of current warnings, which are those that are currently active. The second part is a memory of unacknowledged warnings, which refers to warnings that are no longer active but have not yet been confirmed.



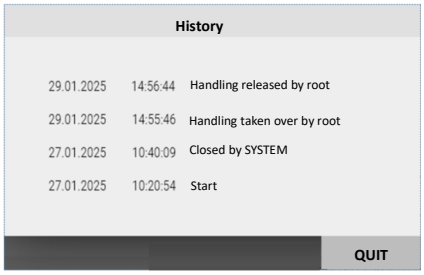


In the ACTIONS column, users have several options. They can mark a warning as acknowledged, close a current warning, or take over the handling of a specific warning.

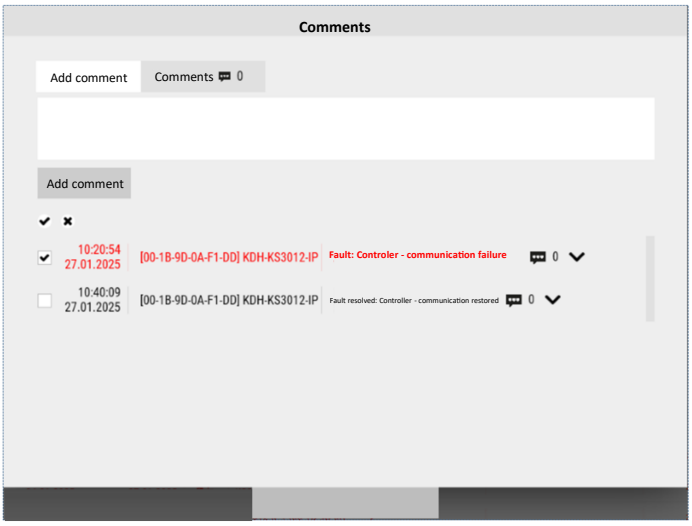




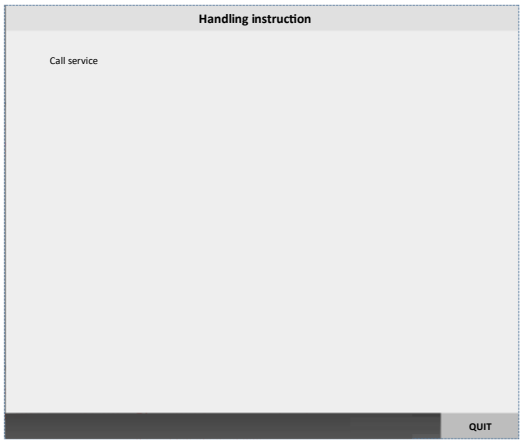
The HISTORY column allows users to view the event history associated with a given warning.



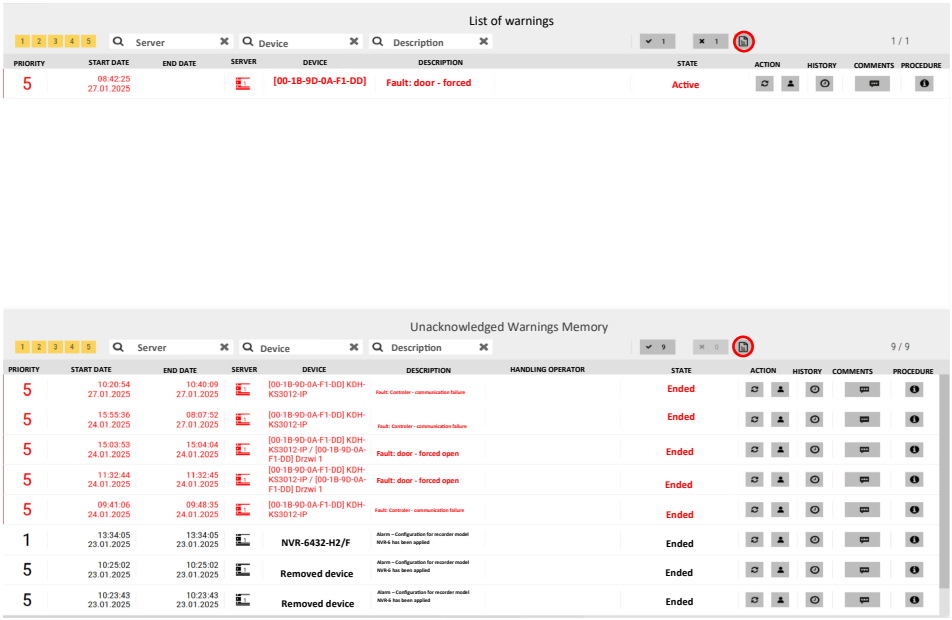
The COMMENTS column allows users to add or view a comment related to the warning and its resolution.

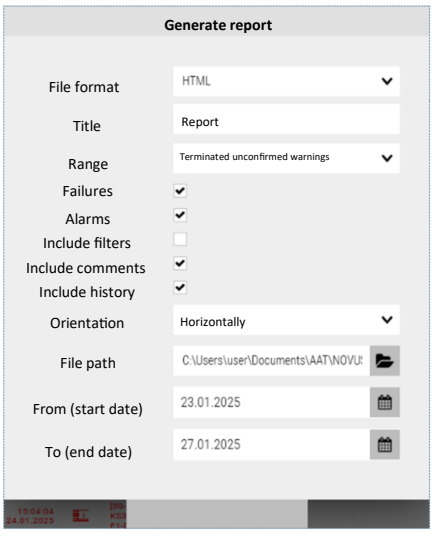


The INSTRUCTION column provides access to a procedure prepared by the installer for handling a specific warning. This instruction is added in the Configuration → Event Parameters menu.



It is also possible to generate reports for both current and unacknowledged warnings.





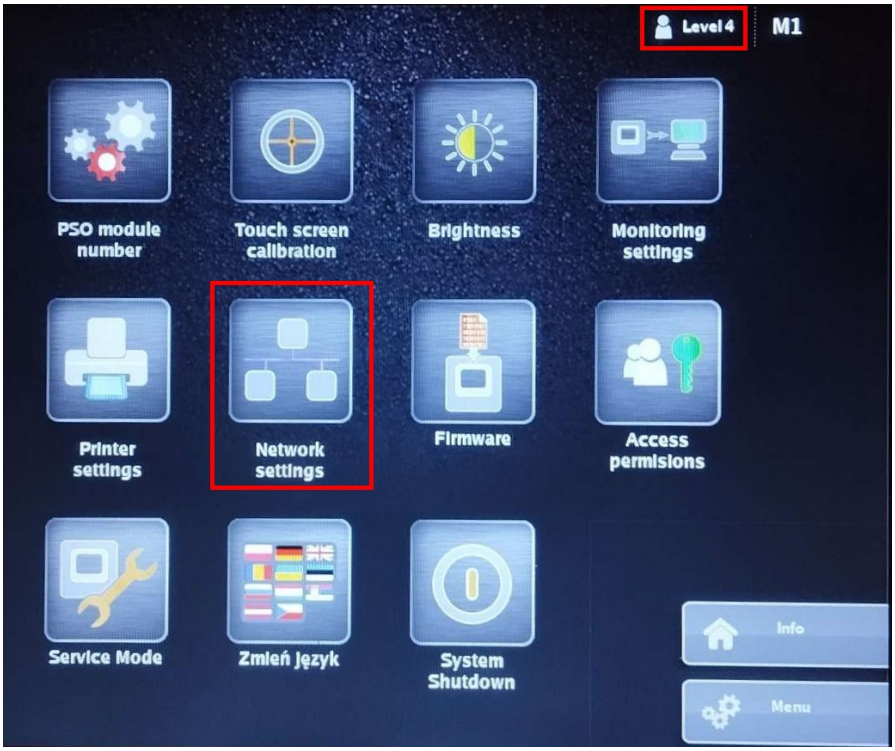
9.11 - Fire alarm system integration (visualization) Polon 6000

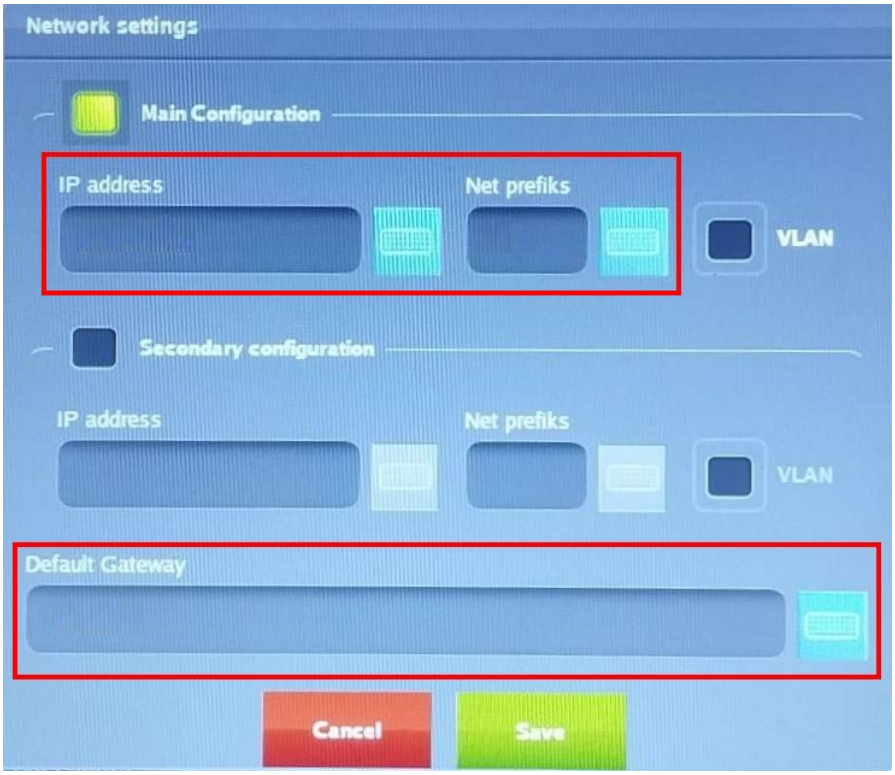
Configuration of the Polon 6000 fire alarm main panel to work with NOVUS MANAGEMENT SYSTEM AC software.

In order to configure Polon 6000 main panel to communicate with NOVUS MANAGEMENT SYSTEM AC software proceed as follows:

- Log in to the Polon 6000 main panel with P4 level (default P4 level password)
- Set proper IP address and other necessary network parameters as shown below:

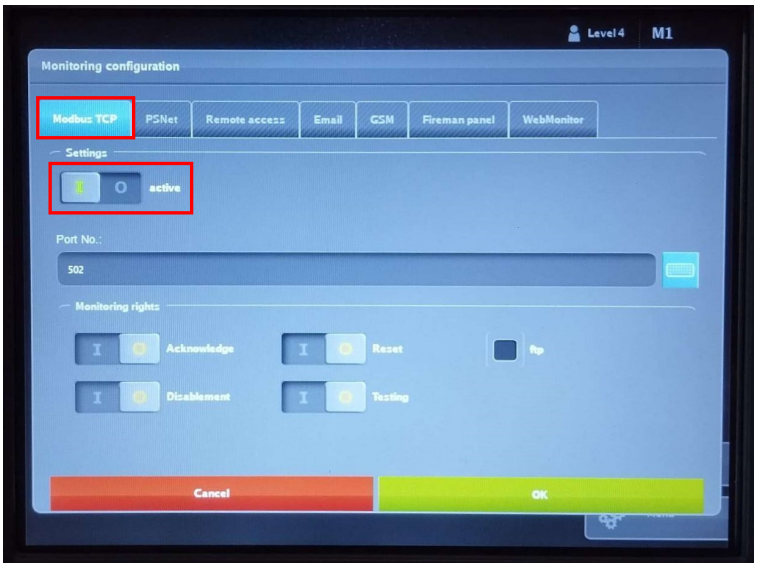
  Menu -> PSO Configuration-> Network setting





- Go to

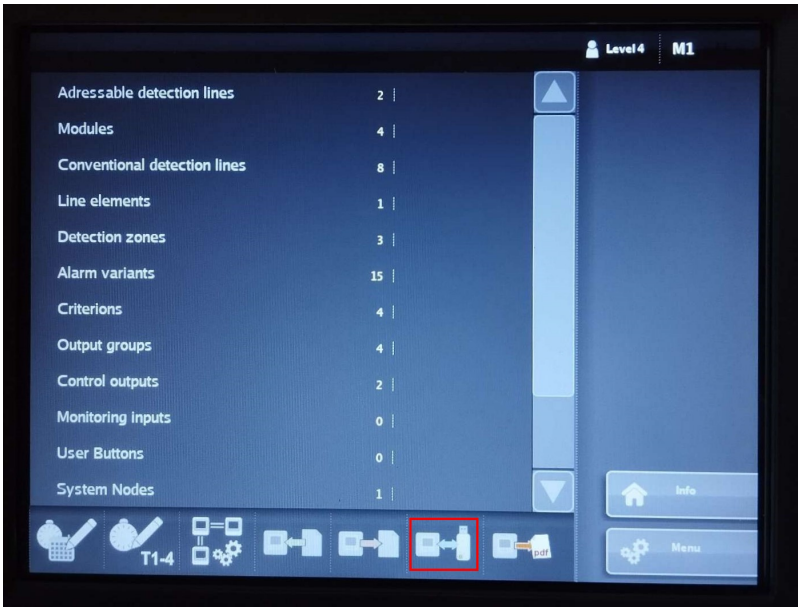
  Menu -> PSO Configuration-> Monitoring configuration
  MODBUS TCP -> enabled



WARNING! After enabling the Modbus function, the PSO module must be restarted.

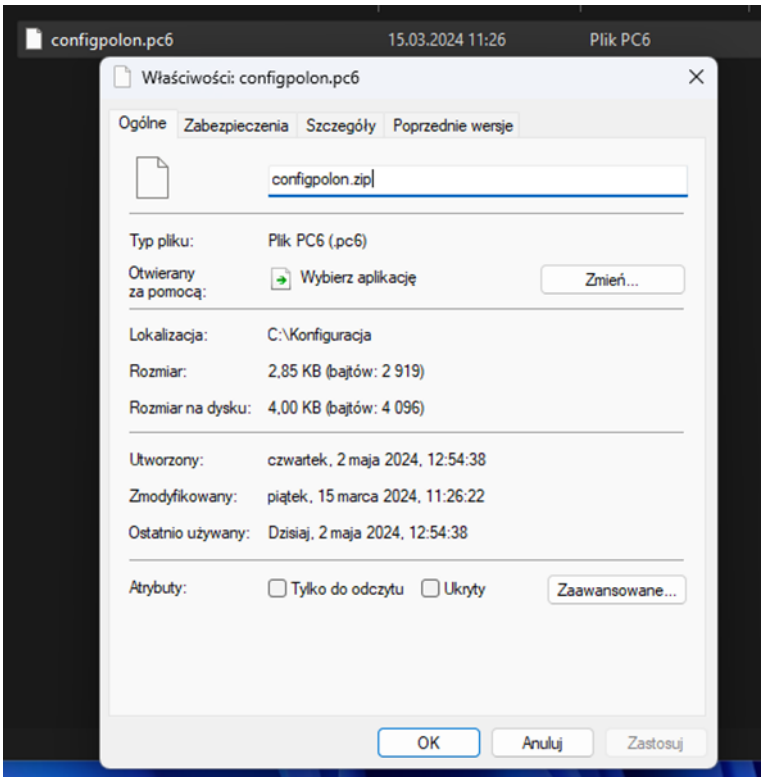
Export configuration from Polon 6000 main panel and import to the NOVUS MANAGEMENT SYSTEM AC software.

- After log in to the Polon 6000 main panel go to the system configuration (copying configuration as shown below)

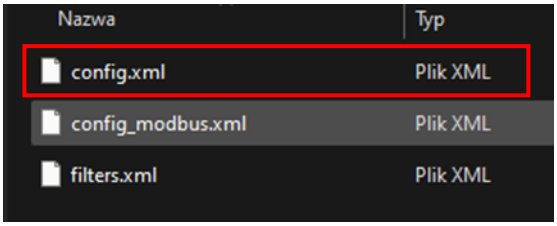


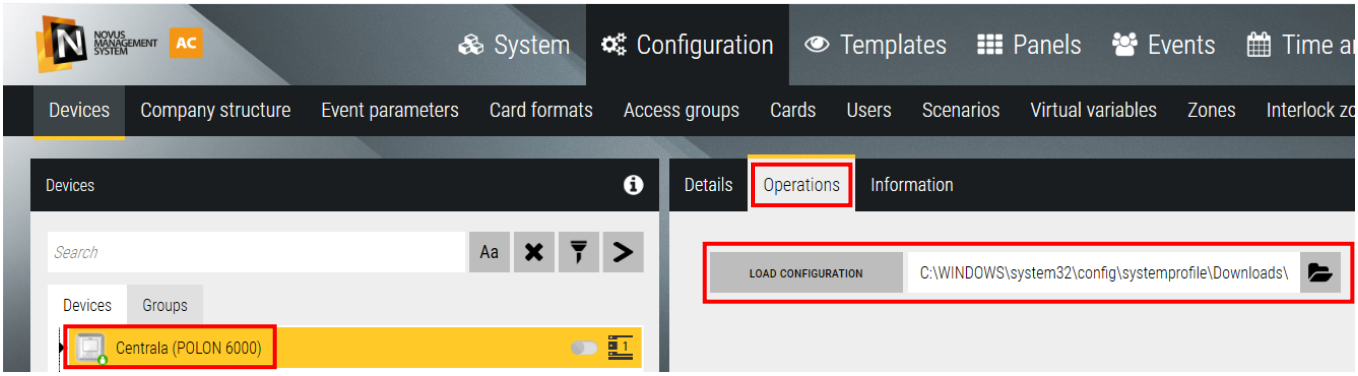
- We export the configuration to a Pendrive.

- After exporting the configuration we get a *.pc6 file, we need to change its extension to *.zip and then extract its contents.



- We get a config.xml file that needs to be imported in the NOVUS MANAGEMENT SYSTEM AC software for the selected Polon 6000 main panel



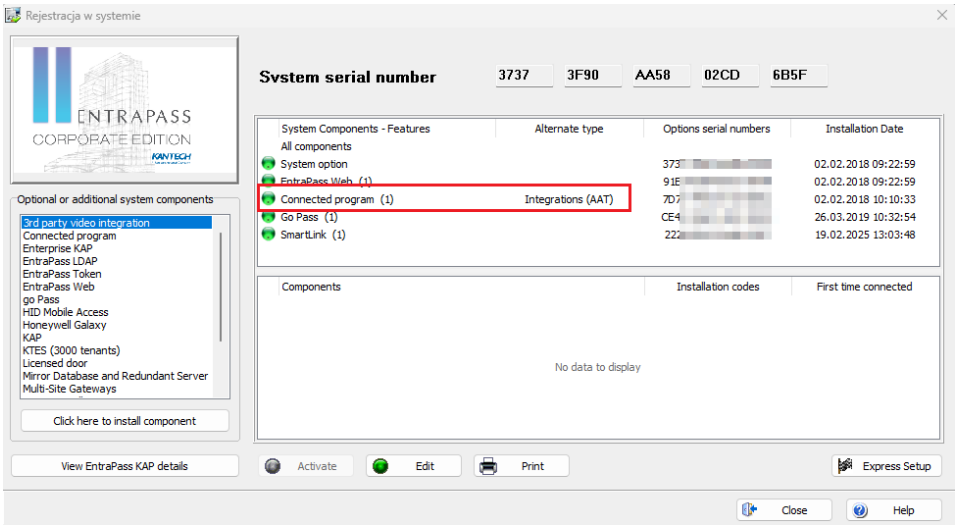


9.12 - Integration (visualization) with KANTECH access control system

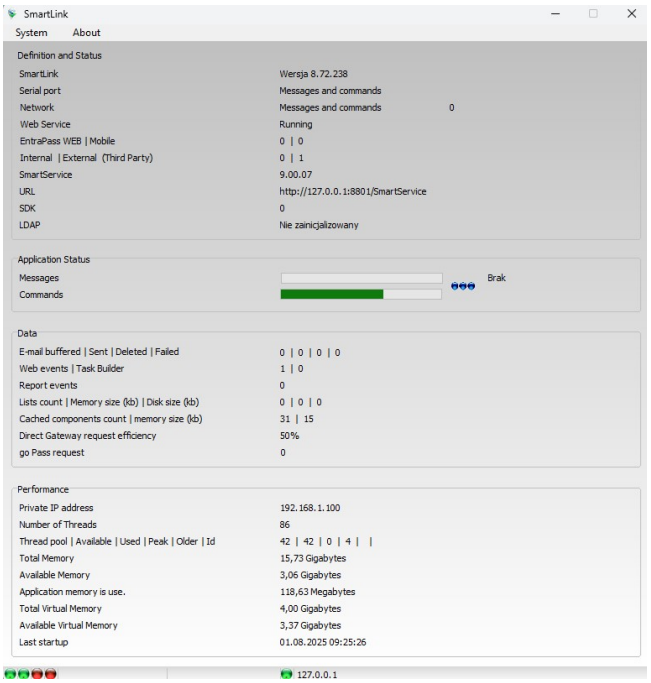
Configuring EntraPass software for cooperation with NOVUS MANAGEMENT SYSTEM AC software

To configure Kantech's EntraPass software for the NOVUS MANAGEMENT SYSTEM AC program, make sure that:

The EntraPass software is available in **Corporate** or **Global** versions and has an active **CONNECTED PROGRAM** license for integration with the client application:



The SmartLink application is installed and active, and is connected to the EntraPass server:

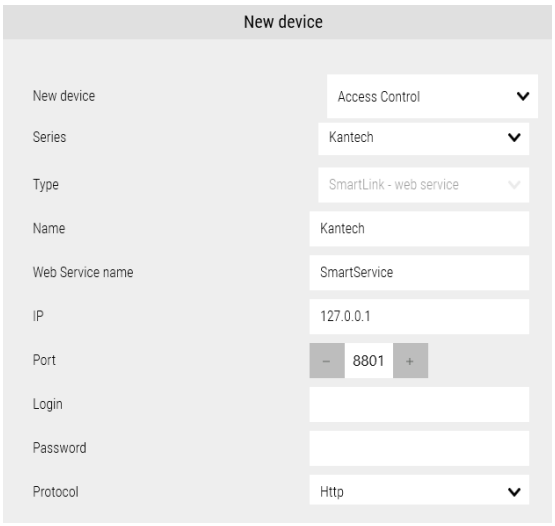


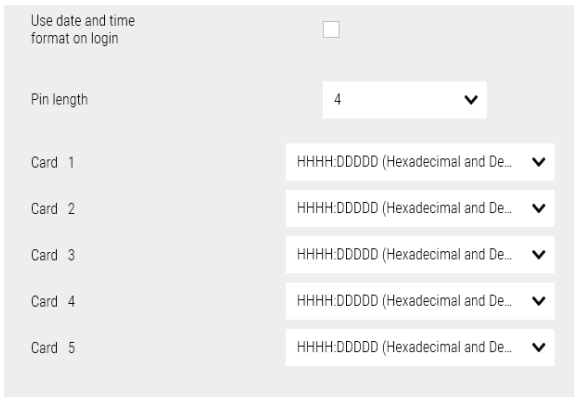
Configuration of NOVUS MANAGEMENT SYSTEM AC software for cooperation with KANTECH EntraPass program:

- Make sure that the NOVUS MANAGEMENT SYSTEM AC software is the correct version supporting integration - minimum 6.01.XX
- There are enough license points *(System/Licenses/Licenses tab)* - minimum 60 points

Adding KATECH controllers to NOVUS MANAGEMENT SYSTEM AC software:

In the Configuration tab, add a new device using the "+" icon and select Access Control - Series - Kantech





Name - editable text field describing the connection to KANTECH controllers

Web Service name - editable text field, to be completed as configured for the *SmartLink* application name in the *Smartlink Web and API tab* in the EntraPass software

IP - SmartLink application IP address field

Port - SmartLink application port configured in the *Smartlink Web and API tab* in EntraPass software - Web Service Port

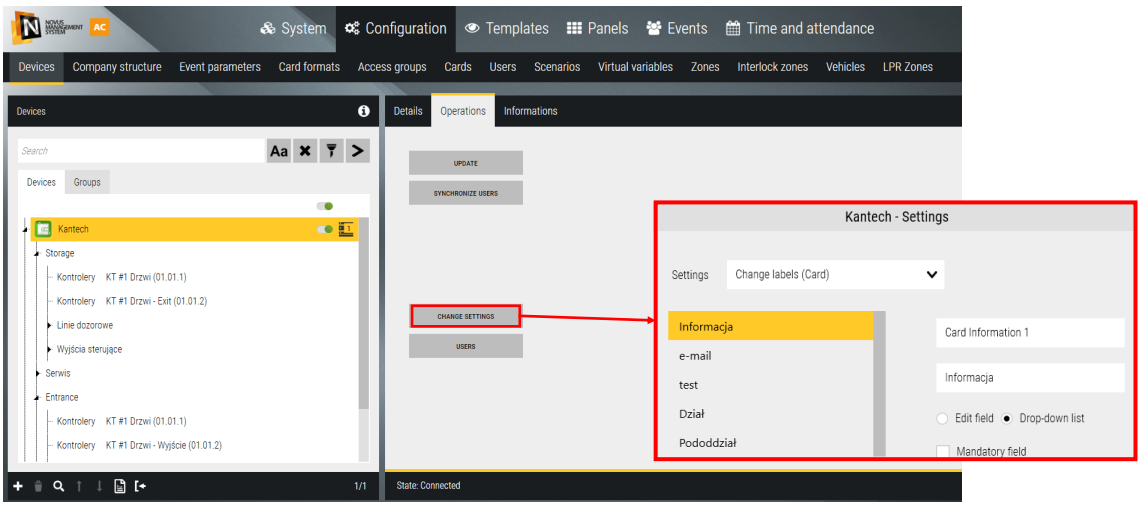
Login - username/operator name for the Entrapass system

Password - user/operator password for the Entrapass system

Protocol - communication protocol configured in the *Smartlink Web and API* tab in the EntraPass software - select http or https

Use date and time format on login, PIN lenght, Card 1,2 … - The tabs should be completed according to the settings in the EntraPass software, tab *Options - Display format*

After saving and configuring correctly, the connection icon should display green, and the status should change to - *State: Connected*

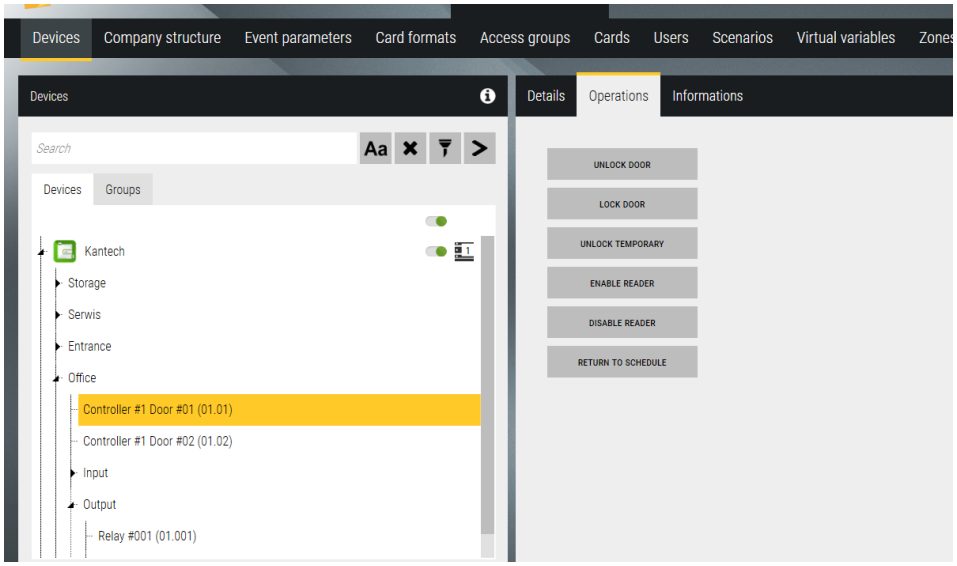


Update - Downloads information about all controllers, doors, alarm lines, and control outputs located in the EntraPass software and displays their list and status in a tree view in the device tab.

Synchronize Users - Synchronizes changes that apply to users

Change settings - Allows you to change the names of labels for fields in the “Card information” tab in the Cards section.

In the operations tab, we can execute commands related to added devices, inputs, and outputs:

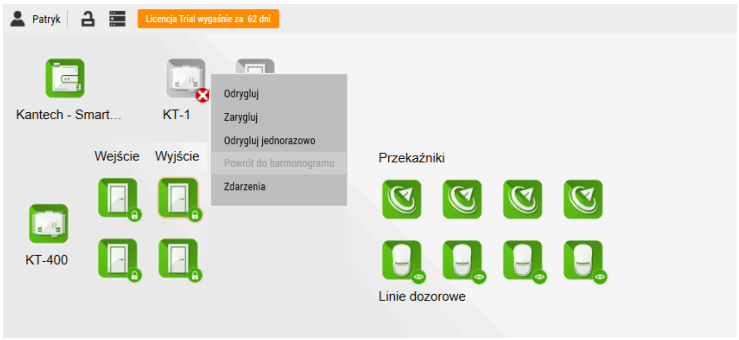


Door - unlock/lock door/unlock temporary/enable/disable reader/return to shedule

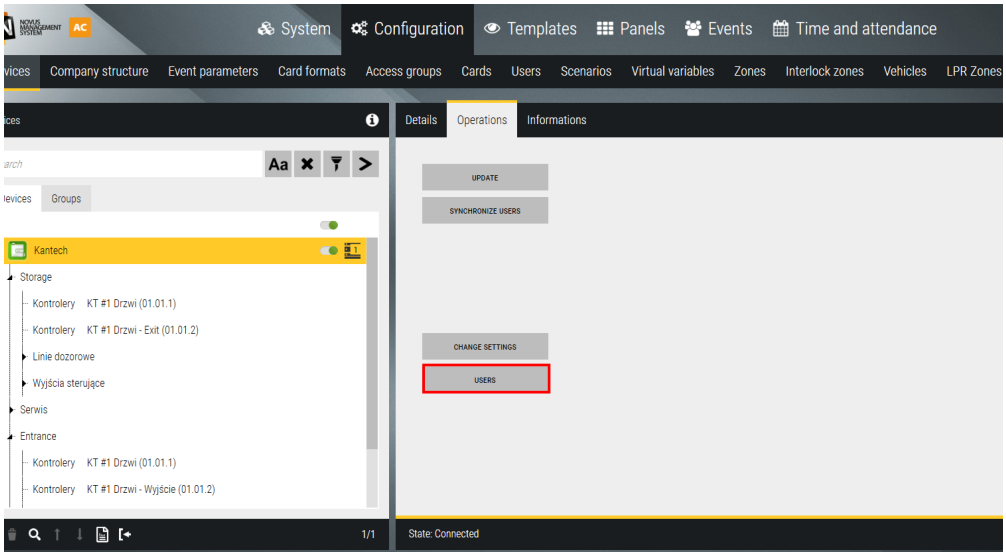
Output - turn on/turn off/turn on temporary/return to shedule

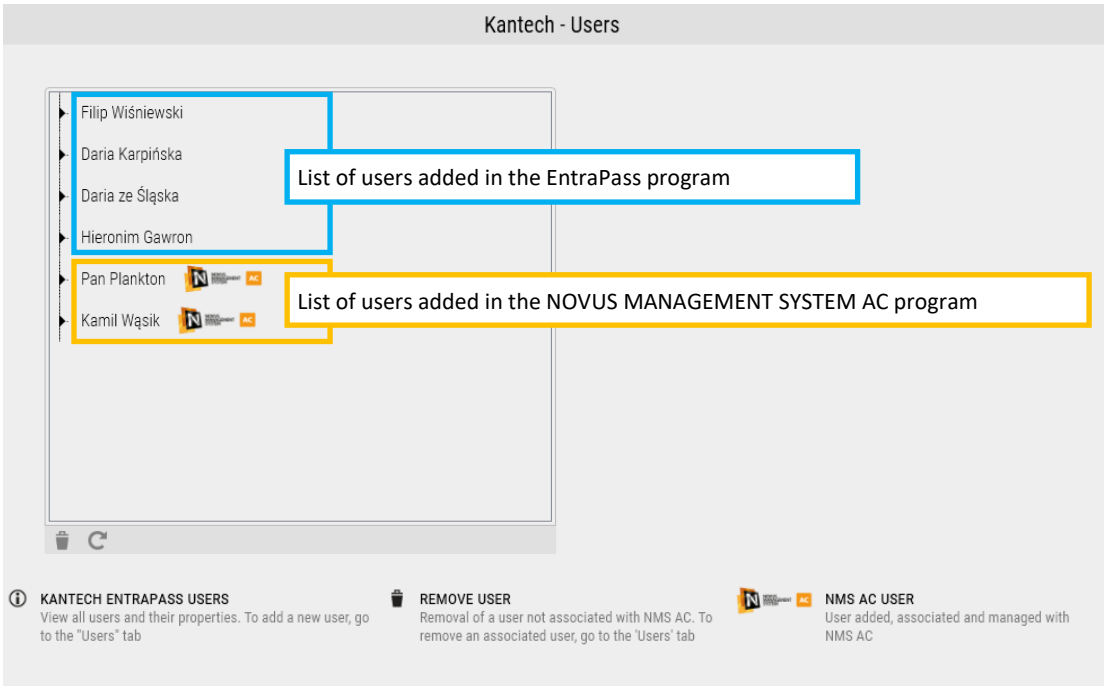
Input - active security/dismiss return to shedule

All elements displayed on the devices can be placed on panels and controlled from the operator's position.

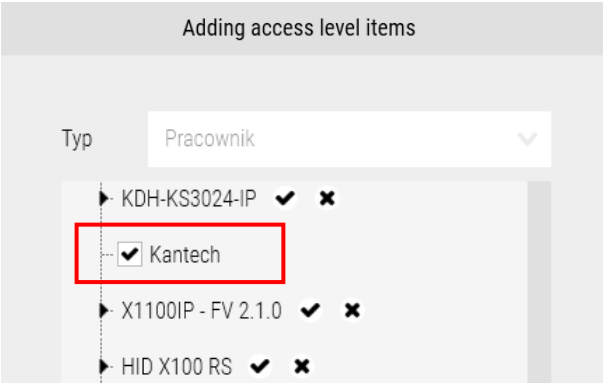


Users - displays a list of users assigned to EntraPass software

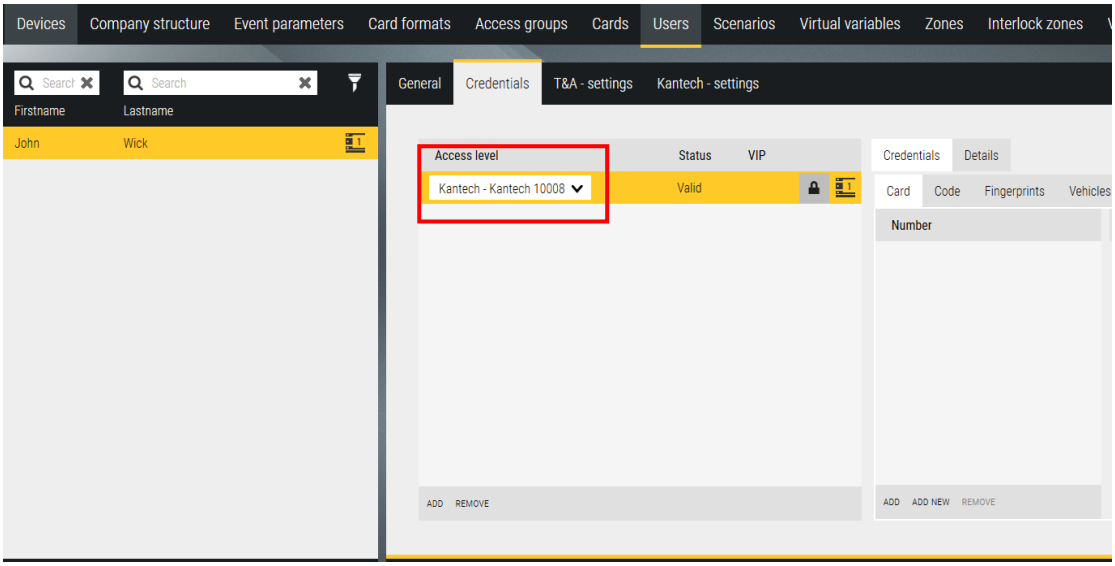




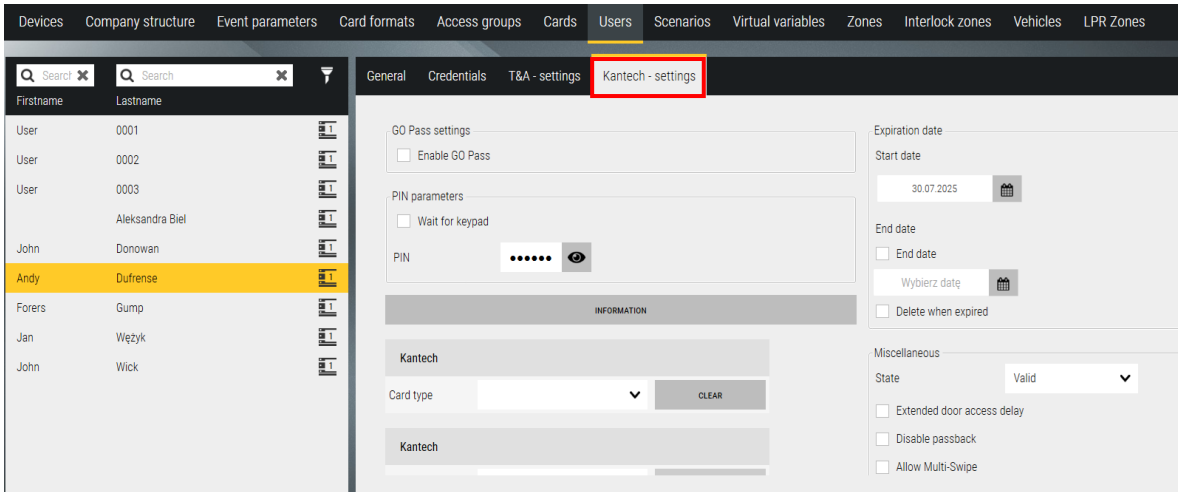
Adding users - To add a new user for the Kantech EntraPass system, we must first create an access level for the added system from the *Configuration/Access groups* menu.



(From Version 6.04.xx, the access level for Kantech is created automatically after configuring the system)



Next, add the user in the same way as for other system users, via the *Configuration/Users* tab. In the Access Level field, select the level you created earlier for the Kantech system.



Kantech - settings - In this window, we can configure the card parameters for the Kantech system

GO Pass setting - enable functionality for GO Pass applications (Kantech virtual cards)

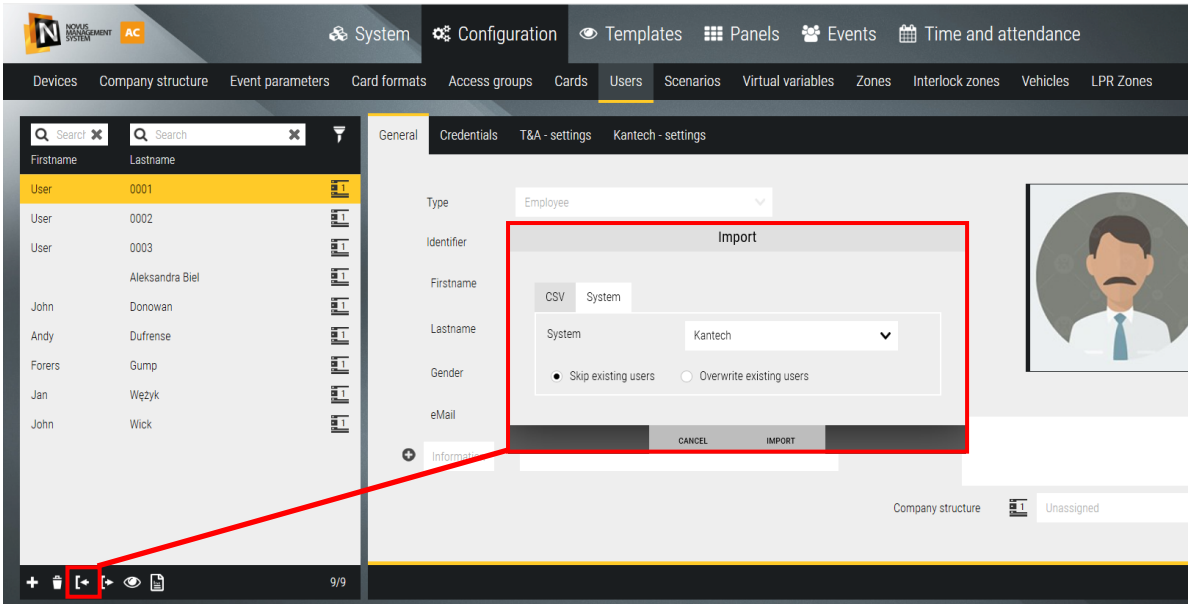
PIN parameters - wymuszenie używania PIN przez użytkownika, ustawienie kodu PIN

Card type - In this section, you can select the card type set in the EntraPass software. The card type contains the access level assigned to selected doors for Kantech controllers. The card type must be configured in the EntraPass software.

Expiration date - setting the start and end dates for the card, it is also possible to remove cards that have expired from the system.

State - Card status information *Valid/Invalid/Stolen lost/Expired*

Enabling additional functionalities for the ID: Extended door acces delay, Disable passback, allowing multi-swipe



Import users - You can import or update users from the Kantech system. Go to the Configuration/Users tab, select the import icon, and go to the System tab. From the list, select the Kantech integration from which you want to download users along with their configuration, card numbers, PIN codes, photos, etc.

List of functionalities of the **NOVUS MANAGEMENT SYSTEM AC** integration with **Kantech EntraPass** software

Commands	Events	User management
Update	Alarm	Preview users and cards configured with EntraPass
Lock/unlock the door	Controller failure	Adding and removing users and cards from NMS AC
Temporarily unlock the door	Door locked/unlocked	
Return to the schedule	Door held open	
Enable/disable the reader	Door in normal condition	
Enable/disable the relay	Door forced open	
Temporarily enable the relay	Reader active/inactive	
Enable/disable monitoring of surveillance lines	Access permitted/prohibited	
	Alarm line monitoring enabled / disabled	
	Relay enabled / disabled	
	Communication lost	
	Communication restored	
	Disconnected by operator	

9.13 - Integration with NOVUS MANAGEMENT SYSTEM AC software using API

General information

API is a set of HTTP/HTTPS commands. The assumption is that almost everything that can be configured and almost all information that can be downloaded from the NOVUS MANAGEMENT SYSTEM AC server from the client application interface will theoretically also be configurable, downloadable from the API level. The set of commands available in the API will be developed depending on the integration needs reported by customers, it will be a matter of individual approach. Currently, a number of commands related to LPR systems and access control users are supported.

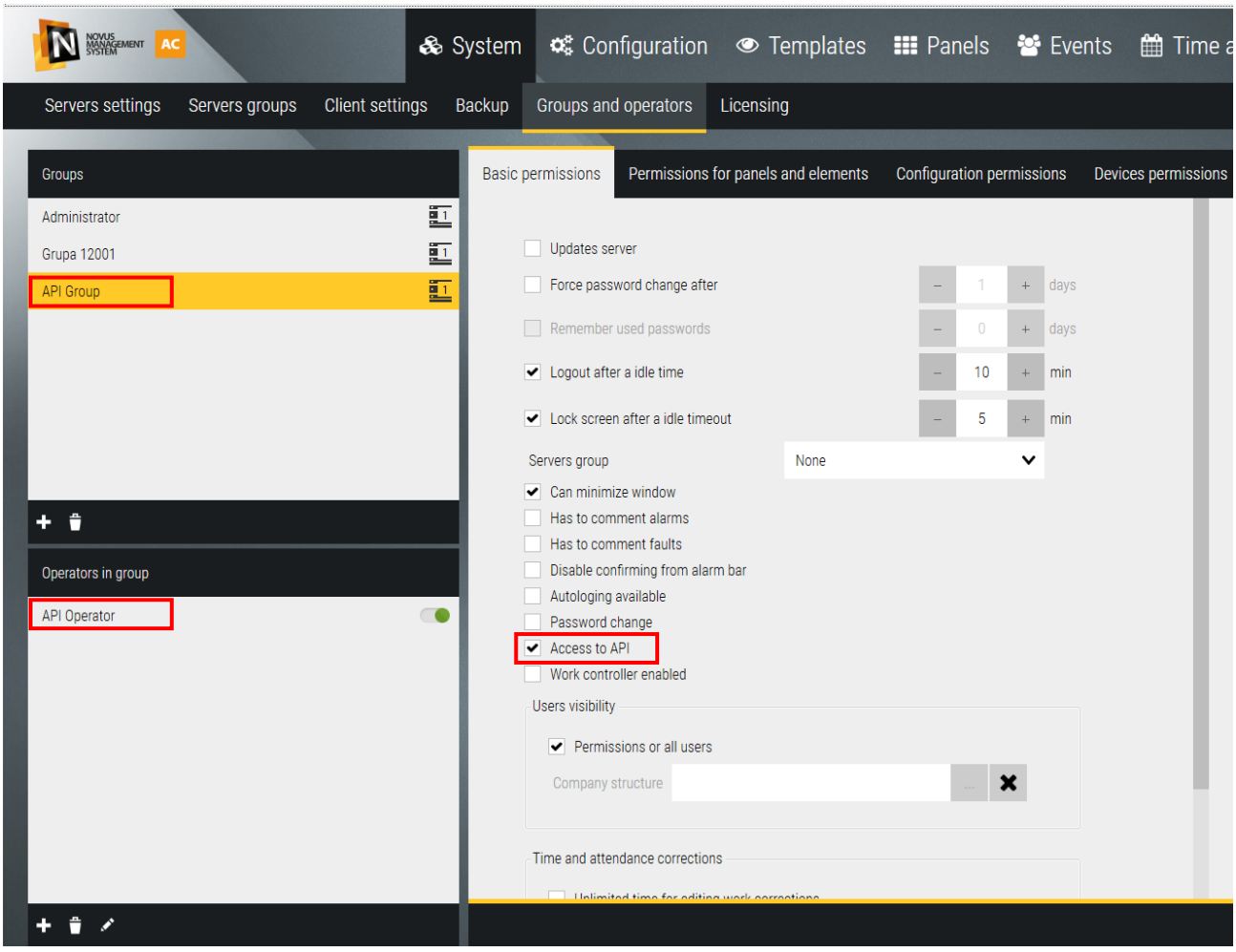
To use the API functionality, it is necessary to purchase a dedicated license for the NOVUS MANAGEMENT SYSTEM AC server (NOVUS MANAGEMENT SYSTEM AC API v5).

For example, if you want to create access that allows you to open doors, you need to create a card that will open them and a user to whom this card will be associated. Then you need to create an identifier in which you pass the user ID, card ID and access level ID specifying where the user will have access. The association (identifier) created in this way will allow the card to be used and the door to be opened.

The same applies to vehicles when opening the entrance, except that the identifier will not be the card but the vehicle registration number. In the case of vehicles, the appropriate access level configured for vehicles should also be used.

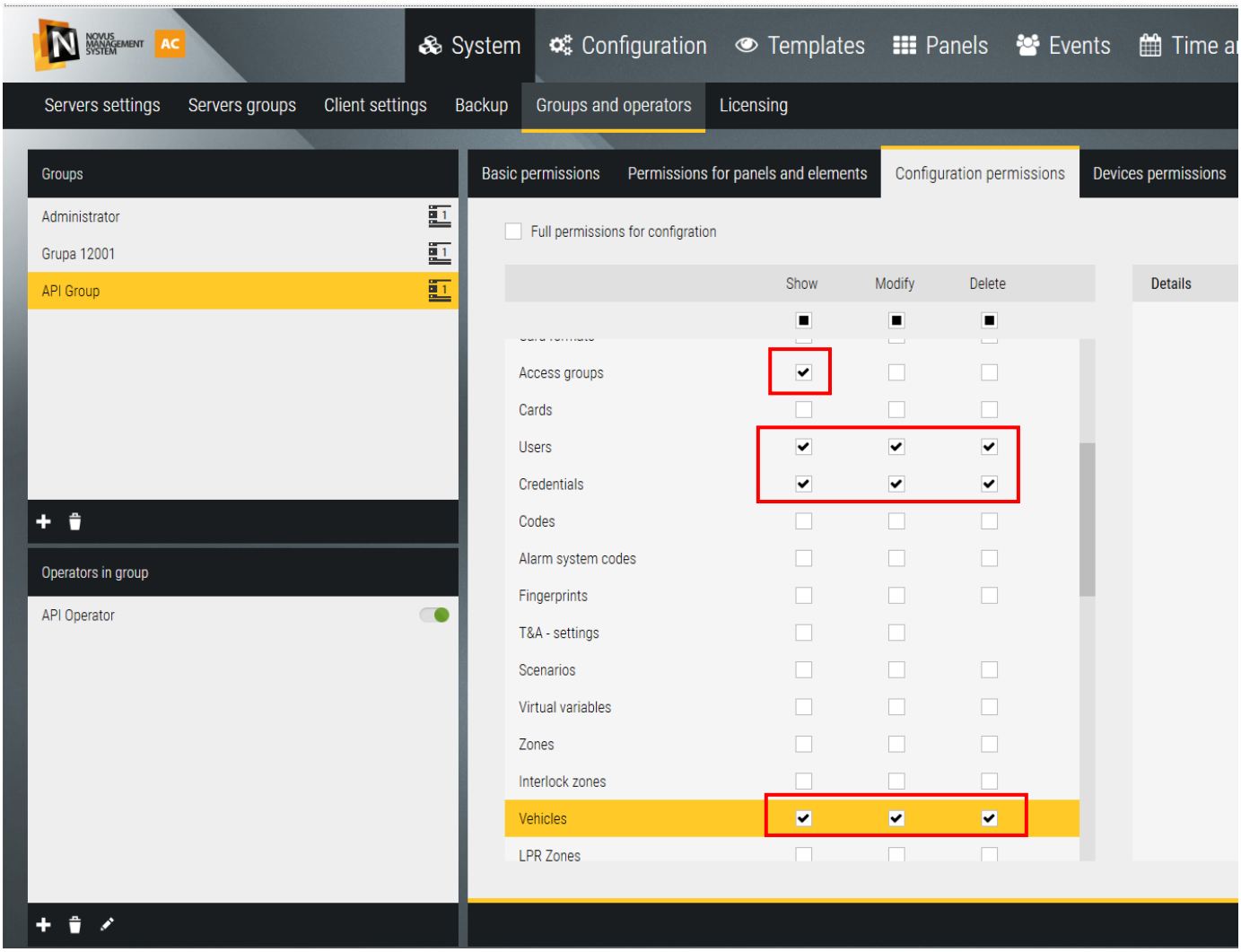
Sample initial configuration

After logging into the software, in the System/Groups and operators tab, add a new group and give it access to the API and create an operator account with a password.

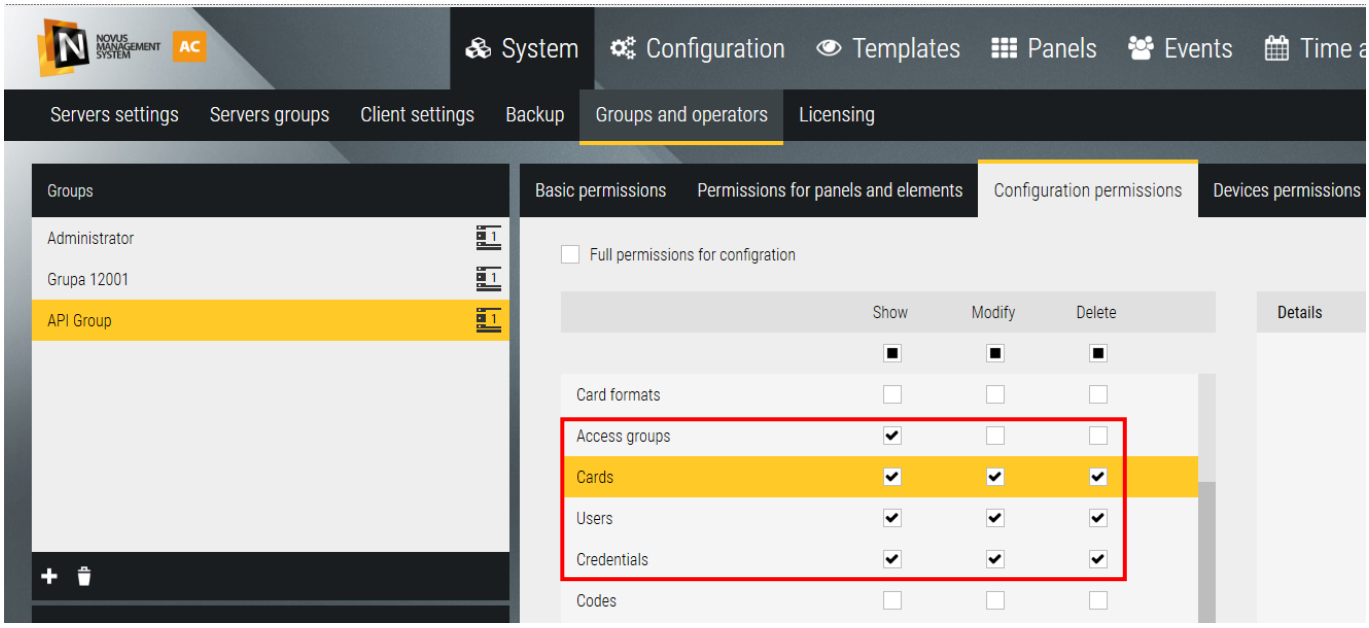


In addition, this group should be given appropriate permissions for the resources that will be modified.

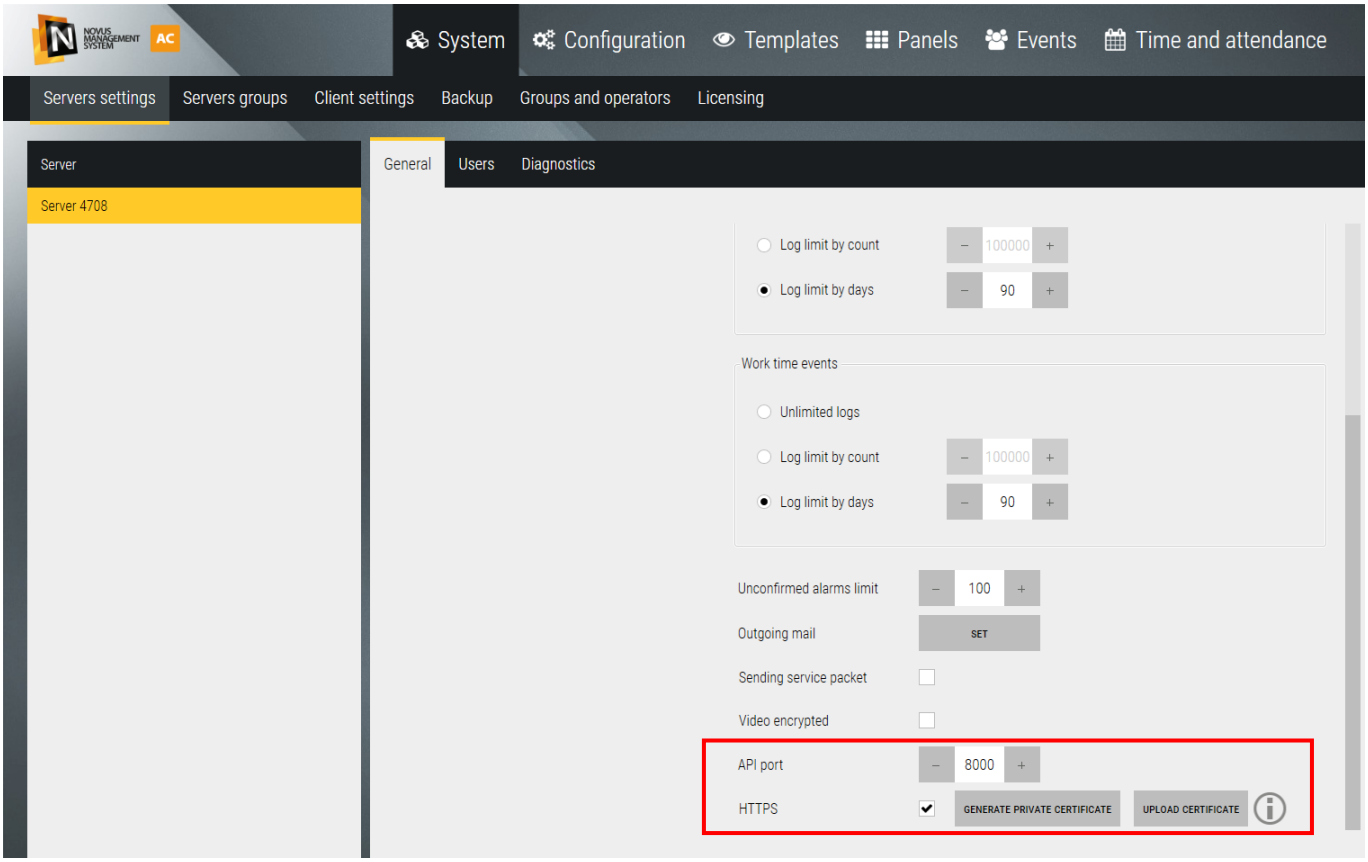
In the case of vehicles:



In the case of cards:



You should also check the API port in the System/Server Settings tab and the HTTPS settings. By default, the port is set to 8000 and the HTTPS option is checked.



API documentation web is available under address:

https://localhost:8000/api/docs

To use the API you need to download a token GET https://localhost:8000/api/auth

Authorization: Basic Auth and use the login and password of the operator who has access to the API.

The token should be included with each subsequent request. When the token expires, a new token should be generated.

If you use the HTTPS protocol and have problems connecting to the API due to the certificate, you should generate a new private certificate from the program configuration by entering the IP address of the NOVUS MANAGEMENT SYSTEM AC server. A certificate file will be created in the application's main directory, which should be added to trusted certificates on the client computer.

Examples:

Adding new vehicle:

POST https://localhost:8000/api/vehicles

JSON BODY

```
{
 "id": 0,
 "plateNumber": "WF2222",
 "owner": "Kowalski",
 "brand": "Audi",
 "model": "A4",
 "country": "Poland"
}
```

In response, the details of the created vehicle with the assigned vehicle ID

Adding new card:

POST https://localhost:8000/api/cards

JSON BODY

```
{
 "number": 6898221,
 "type": "Employee",
 "remark": "description",
 "id": 0
}
```

In response, the details of the created card with the assigned ID

New user adding

POST https://localhost:8000/api/users

JSON BODY

```
{
 "id": 0,
 "firstName": "Jan",
 "lastName": "Kowalski",
 "remark": "description",
 "email": "kowalski@firma.pl",
 "male": true,
 "type": "Employee"
}
```

In response, the details of the created user with the assigned user ID

Listing of the Access groups

GET https://localhost:8000/api/accesslevels

In response, list of the Access groups with assigned ID

Associating a user with an identification element and access level

For vehicles in the "vehicles" list add the vehicle ID:

POST https://localhost:8000/api/credentials

JSON BODY

```
  {
    "accessLevel": 3,
    "userId": 10008,
    "expirationDate": "0001-01-01T00:00:00",
    "cards": [],
    "codes": [],
    "fingerPrints": [],
    "alarmSystemCodes": [],
    "qrCodes": [],
    "vehicles": [10005]
  }
```

However, in case of associating cards in the "cards" list, add the card id

POST https://localhost:8000/api/credentials

JSON BODY

```
{
   "accessLevel": 2,
   "userId": 10008,
   "expirationDate": "0001-01-01T00:00:00",
   "cards": [10045],
   "codes": [],
   "fingerPrints": [],
   "alarmSystemCodes": [],
   "qrCodes": [],
   "vehicles": []
}
```

Removing access

DELETE https://localhost:8000/api/credentials/{ID}

DELETE https://localhost:8000/api/users/{userID

DELETE https://localhost:8000/api/vehicles/{vehicleID}

or

DELETE https://localhost:8000/api/cards/{cardID}

Application events

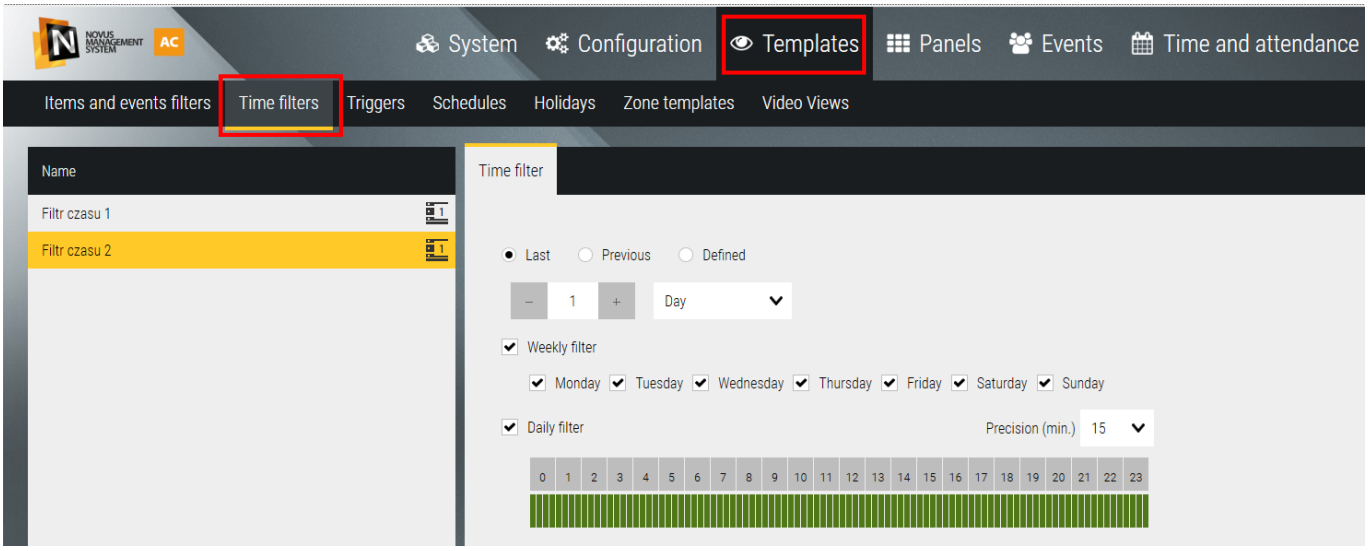
Getting events

GET https://localhost:8000/api/events?From=0001-01-01T00:00:00.555&To=2201-01-01T00:00:00.664&TimeFilterId=0&ItemsAndEventsFilterId=0&Limit=30&language=pl

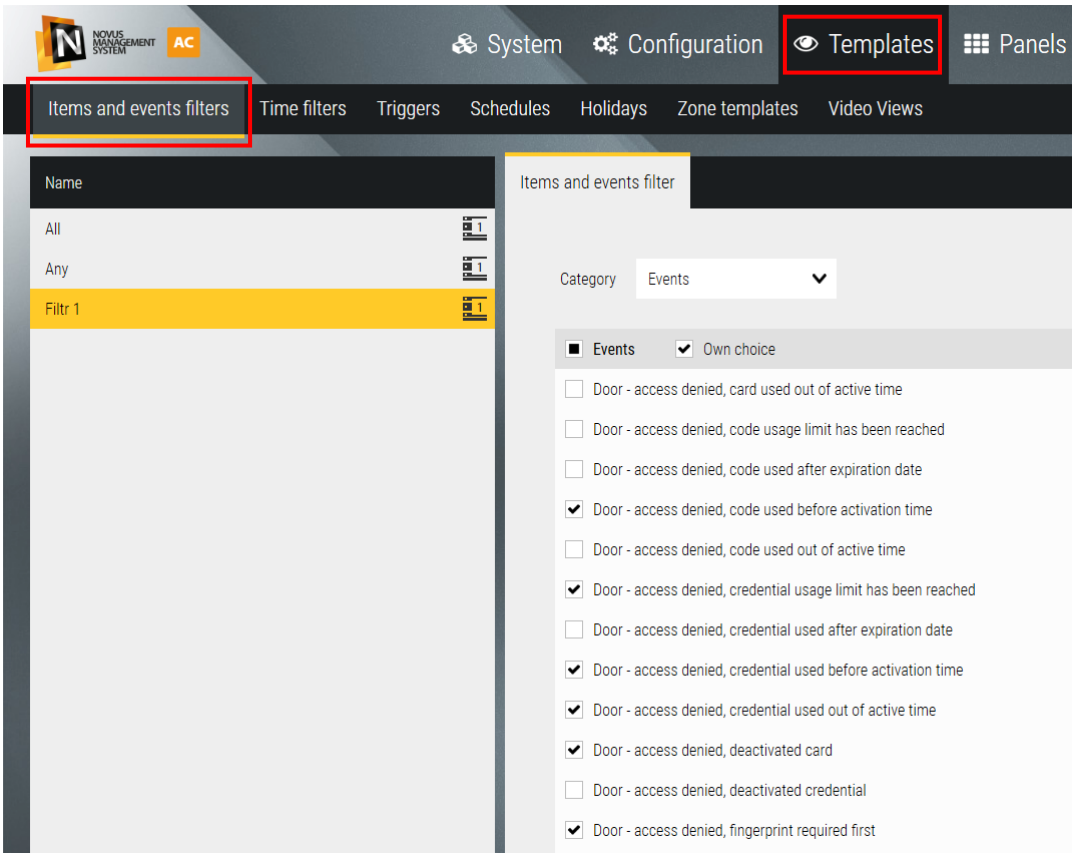
Parameters used to getting events

- Time range from—to
- Optionally, you can use time filters defined in the software

- Optionally, you can use time filters defined in the software



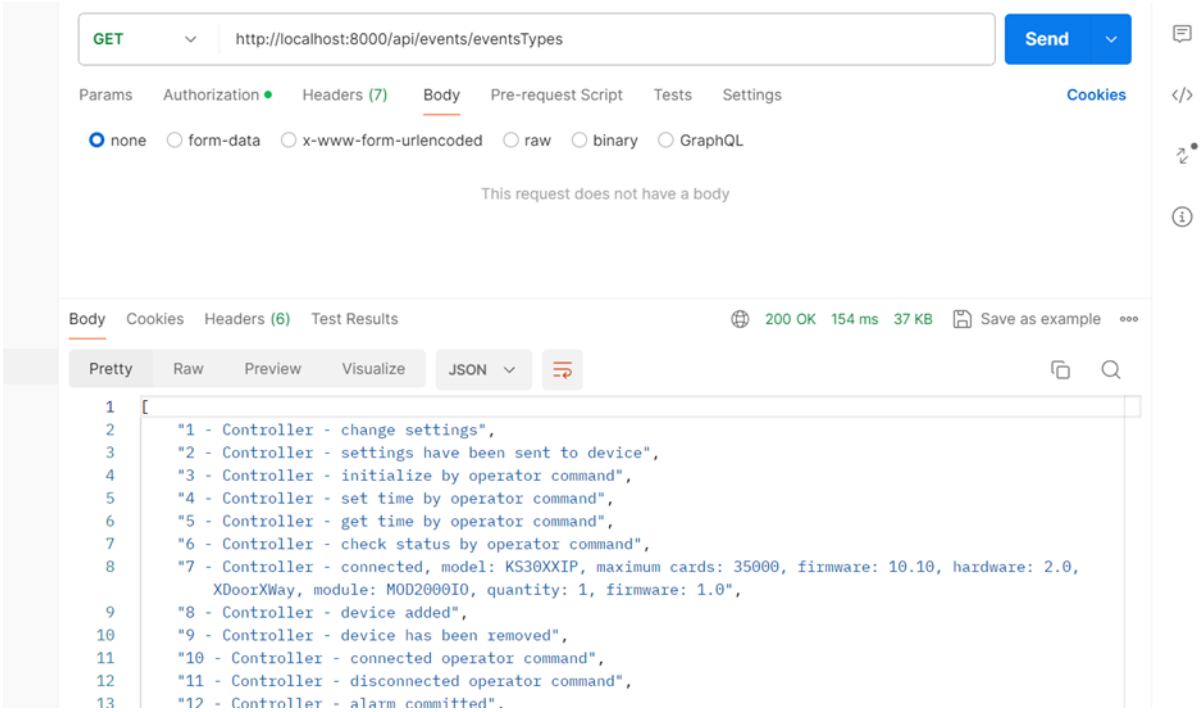
- Optionally, you can use Items and events filters defined in the software



Above elements can be listed by using:
https://localhost:8000/api/itemsAndEventsfilters

A list of all possible event identifiers (EventTypeID) along with their descriptions (Details) can be listed using:

https://localhost:8000/api/events/eventsTypes



FEE-BASED LICENCE AGREEMENT
for "NOVUS MANAGEMENT SYSTEM" AC version

We hereby inform that the installation and use of "Novus Management System" AC version software indicates automatic acceptance of the terms of this Licence Agreement on behalf of the Licensee – User. The Manufacturer informs that the use of the Software may not be available in certain countries and languages. If you do not agree to the terms of this License Agreement, discontinue use of the Software immediately, uninstall it and remove it from your device.

1. DEFINITIONS

1.1. "**Agreement**" – this licence agreement which the User concludes with the Manufacturer in order to be able to use the Software.

1.2. "**Copyright and Related Rights**" – each individually and all together the copyright and related rights, including – in particular – copyright, rights to patents, trademarks, logos, as well as know-how and trade secrets, included in or related to the Software, owned by the Manufacturer. Copyright and related rights are protected in particular by the Act of 4 February 1994 on Copyright and Related Rights (Journal of Laws of 1994, No. 24, item 83, as amended).

1.3. "**Manufacturer**" – AAT SYSTEMY BEZPIECZEŃSTWA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ with its registered seat in Warsaw, ul. Puławska 431, 02-801 Warsaw, entered into the register of entrepreneurs kept by District Court for the capital city of Warsaw, 13th Commercial Division of the National Court Register under number: KRS 0000838329, NIP 9512500868, REGON 385953687, with share capital amounting to: PLN 17,005,000.00.

1.4. "**User**" – a natural person, a self-employed person, a legal person and an organisational unit that is not a legal person but to which the law confers legal capacity, which installs or uses the Software. The User may not be a natural person who is a consumer within the meaning of the Civil Code Act (Journal of Laws of 23 April 1964 (Journal of Laws, no. 16, item 93 as amended).

1.5. "**Software**" – computer software, comprising the entire contents of files delivered electronically or on a medium, constituting a Work within the meaning of the Copyright and Related Rights Act, developed by the Manufacturer or for which the Manufacturer is the owner of the property rights, which may be used by the User under the terms of the Agreement.

1.6. "**Licence Key**" – the numerical code generated by the Manufacturer, provided to the User, necessary for the use of the Software or additional functionalities or extensions Licence Key can be used only once and on only one device.

1.7. "**Licence Points**" – points that allow the User to add integrated devices to the Software.

2. GENERAL PROVISIONS

2.1. The User may only install and use the Software in the manner and under the conditions provided for in the Agreement, in accordance with the Software user manual.

2.2. The Agreement does not transfer copyright and related rights to the User, nor does it grant the User these rights. The User is only entitled to use the Software to the extent specified in the Agreement.

2.3. The User acknowledges that the purchase of the Licence obliges the User to comply with the provisions of the Agreement.

2.4. The Manufacturer hereby grants the User a non-exclusive licence for their own use only, without the right to grant licences to others, in the territory indicated in the registration form, to download, install and use the Software on a stationary or portable computer.

2.5. The licence is granted to the User against payment. The licence fee is set out in the sales document.

2.6. The licence fees may be shaped differently depending on the location, the way the Software is used or the functionalities or extensions added. In particular, the licence fee may be a one-off fee, a periodic fee, depending on the number of Licence Points or additional functionalities or extensions.

3. LICENCE AND RESTRICTIONS

3.1. The Manufacturer grants the User a licence authorising them to use the Software in the fields of exploitation indicated in point 4 below.

3.2. The User has the right to install and activate the Software only once and only on one computer workstation designated for that purpose (on one computer) and to make one backup copy.

3.3. The User may not in any way lend, resell, transfer, publish, distribute or in any way make available the Software or any part of it, as well as the License Key, to third parties or infringe any rights relating to the Software or any part of it.
3.4. The User shall not be authorised and agree that they will not attempt, cause, permit or authorise any third party to modify, edit, create derivative works from, decompile, disassemble or break the code of the Software, any part thereof, or any files and their contents comprising or attached to the Software.
3.5. The User is not authorised to use the Software to create or develop a competitive product.
3.6. The Manufacturer reserves the exclusive right to make modifications, extensions, updates, translations or repairs to the Software at its sole discretion.
3.7. The Manufacturer is not obliged to inform the User about the modifications made, additional functionalities, extensions, updates, translations or subsequent versions of the Software.
3.8. The Manufacturer is not obligated to provide the User with subsequent versions of the Software, its additional functionalities, extensions, updates, translations, and may discontinue doing so at any time.
3.9. The provision of newer versions of the Software can be performed by activating the update option directly from the Software, provided that the computer is connected to the Internet. The User may also download and install modifications, additional functionalities, extensions or updates to the Software made available by the Manufacturer on their website under the conditions indicated in such updates.
3.10. The Manufacturer is not obliged to provide any services related to the Software, in particular technical assistance or support.

4. FIELDS OF EXPLOITATION

4.1. The Manufacturer grants the User a licence exclusively covering the following fields of exploitation:
1) entering the Software or parts thereof into the memory of a computer or other device intended for the use of the Software, including downloading the Software from the Manufacturer's website or other carrier and installing it;
2) making a single backup copy, if this is necessary for the use of the Software;
3) using the Software under the terms and conditions indicated in the Agreement, including its registration, integration with devices and use of additional functionalities or extensions of the Software.

5. SOFTWARE REGISTRATION

5.1. The Manufacturer shall make available to the User free of charge a trial version of the Software ("**Trial**") for a limited period of time of 60 days, which can be activated after registration of the Software. During this period, the User should purchase a Licence Key and activate the Software. In the event of failure to purchase a licence, register the Software and activate it, the licence automatically expires and the User loses the right to use the Software.
5.2. Registration of the Software takes place directly from the Software level or via the Manufacturer's website. The User shall then activate the Software.
5.3. Registration of the Software consists of providing data concerning the User, i.e. data of the installer and data of the licence user.
5.4. Registration of the Software requires access to the Internet.
5.5. Activation of the Software consists of entering the License Key.
5.6. The User may add functionalities or extensions available in the Manufacturer's offer ("**Functionality**") to the Software. The activation of a Functionality consists in the payment of an additional licence fee (purchase of the respective License Key) and its entry in the appropriate place in the Software.
5.7. The Manufacturer may request access to the location of the Software, as well as control its use.

6. TERM OF THE AGREEMENT

6.1. The Agreement is concluded by the User's acceptance of its terms when the User clicks the "I accept" button during the installation of the Software or its update. In any case, it is assumed that the start of the use of the Software constitutes acceptance of this Agreement.

6.2. In the case of activation of the Trial version, the Agreement is concluded for a fixed period of 60 days. The Agreement is transformed into an Agreement for an indefinite period of time, provided that the License Key is purchased and the Software is registered and activated.
6.3. The Agreement is concluded for an indefinite period of time on the condition that the User purchases a Licence Key, registers and activates the Software.
6.4. The Agreement may be terminated by either Party with one month's notice, except that the User may terminate the Agreement without one month's notice – by deleting the Software and its backup copy.
6.5. The Manufacturer may terminate the Agreement without notice if the User breaches the provisions of the Agreement.
6.6. The Manufacturer may terminate the Agreement immediately, without notice, in the event of the User's failure to pay the licence fee in full (in the case of a one-off payment) or its subsequent part (in the case of additional, periodic or spread out payments) in accordance with the deadline indicated in the sales document. In such a situation, the Manufacturer shall be entitled to exclude and block the User from using the Software or its respective Functionality.
6.7. Upon termination of the Agreement, all the User's rights to the Software granted by the Agreement shall expire. The User shall then stop using the Software and remove the Software and its backup copy from any media or devices.
6.8. The Manufacturer is not responsible for any damage incurred due to the termination of the Agreement.

7. WARRANTIES AND LIABILITY OF THE MANUFACTURER

7.1. The Manufacturer warrants that it has the capacity to conclude and perform the Agreement.
7.2. The User warrants that it has the capacity to conclude and perform the Agreement.
7.3. The Manufacturer shall deliver the Software on an "as is" basis without any warranties and shall not be held liable for any functional deficiencies of the Software or the consequences of using the Software, in particular in cases of faulty operation of the computer system caused by hardware defects, improper installation or configuration of the software and hardware, and in cases of improper operation of the Software.
7.4. The warranty for defects specified in the provisions of the Civil Code is excluded.
7.5. The Manufacturer is not liable for any warranty with respect to the Software.
7.6. The Manufacturer shall not be held liable for the manner in which the User uses the Software, and in particular for using the Software contrary to the Agreement or the User Manual, and for the resulting damage.
7.7. The Manufacturer is not responsible for the infringement of Copyright and Related Rights, as well as for claims of third parties, resulting from the User's use of the Software contrary to the Agreement.
7.8. Should it not be possible to exclude the liability indicated in this item 7, it shall be excluded to the maximum extent possible. In particular, the Manufacturer's liability for damage that could be caused intentionally is limited to EUR 500 and does not include the right to claim reimbursement of lost profits or liability for indirect damage.
7.9. The above provisions also apply to all functionalities of the Software.

8. USER'S RISK

8.1. The User acknowledges and agrees that the entire risk arising from the use of the Software in the manner specified in this Agreement and in the user manual accompanying the Software lies with the User to the fullest extent permitted by law. Furthermore, in the event of circumstances preventing the operation of the Software – provided that the direct cause of such circumstances is attributable to the Software – the User should immediately inform the Manufacturer, under pain of exclusion of any liability of the Manufacturer which may arise on this account.
8.2. The User acknowledges that the entire risk arising from the installation and activation of the Software on a given device, as well as the integration of the Software with other programs or devices, their use and their installation rests with the User to the fullest extent permitted by law. This Agreement does not set out the terms and conditions for the use of such programs or devices and their use should be in accordance with the relevant licence terms.

8.3. The User acknowledges that use of the operating system on which the Software runs should be in accordance with the licence terms of that system.
8.4. The User understands that the Software may not implement all of their individual requirements and that the Manufacturer is not obliged to assess the suitability of the Software to the User's expectations. The User accepts the entire risk of the appropriate selection of hardware and the proper design of the Software to meet their needs.
8.5. The User acknowledges that the entire risk arising from the integration of the Software with the Functionalities, the use of the Functionalities and their activation rests with the User to the fullest extent permitted by law.

9. TRADE MARKS/LOGO

9.1. The Manufacturer is the sole proprietor of the trade mark NOVUS MANAGEMENT SYSTEM – legally protected national trade mark entered in the Register of Trade Marks kept by the Patent Office of the Republic of Poland under No. 213634 and appearing under the number 1008732 of World Intellectual Property Organization (WIPO) an international trade mark designed to designate products in Class 9 of the International Nice Classification of Goods and Services.
9.2. The aforementioned trade mark, as well as the name of the Software and the logo, are legally protected and may not be used by third parties without the Manufacturer's consent.
9.3. The aforementioned trade mark or logo may not be altered, in particular this applies to their size, proportions, colours or otherwise modified in appearance.
9.4. The aforementioned trade mark may not be used in publications, websites and other materials the content of which may disparage the Manufacturer or the Software, infringe intellectual property or other rights, or is contrary to the law of a given country or international law.

10. FORCE MAJEURE

10.1. The Parties shall not be liable for non-performance or undue performance of their obligations under the Agreement only in the situation where such non-performance or undue performance is a consequence of force majeure.
10.2. Force majeure shall be understood by the Parties as an event that could not have been foreseen with due diligence, which is external both to and independent of the Manufacturer and the User, and which the Parties could not have prevented by acting with due diligence. In particular, force majeure shall be deemed to include earthquakes, floods, fires, hurricanes, natural disasters, epidemics, other events caused by natural forces, strikes, military actions, export and import restrictions.
10.3. If the events referred to in item 10.2 are of a temporary nature, the Parties undertake to perform the provisions of the Agreement, whereby the time provided for the fulfilment of the obligations under the Agreement shall be extended by the duration of the circumstances causing the delay.

11. DISPUTES SETTLEMENT

11.1. The Parties undertake to resolve any disputes which may arise from the performance of the Agreement amicably.
11.2. In the event that it is not possible to amicably resolve a dispute arising from the Agreement, the Parties accept Polish law as applicable to resolve the dispute, which they shall submit to the court having jurisdiction over the Manufacturer's registered office.
11.3. Any infringement of the Manufacturer's Copyrights and Related Rights may result in civil and criminal liability of the infringer.

12. FINAL PROVISIONS

12.1. This Agreement does not transfer to the User the proprietary copyrights in whole or in part to the Software or its Functionality, but only grants the right to use the Software, including its Functionality, under the conditions indicated herein.
12.2. The User agrees to make their personal data available to the Manufacturer in the Software registration form and to have it processed by the Manufacturer. The information clause is included in the Software registration form.
12.3. The Manufacturer may assign the rights to the Software, or parts thereof, to third parties of their choice, without notifying the User.

12.4. The User may not assign the rights obtained under the Agreement to third parties without the consent of the Manufacturer.
12.5. The User declares that they have familiarised themselves with the content of the Agreement before using the Software and do not raise any objections to it.
12.6. If any provision of the Agreement is found to be unlawful or to lead to a circumvention of the law, it shall be deemed null and void. The remaining provisions of the Agreement shall remain in force, unless the circumstances indicate that the Agreement would not have been concluded without them. The Parties undertake that, in such a situation, they will enter into negotiations to replace the invalid provisions, with provisions that will achieve the closest possible economic purpose.
12.7. All changes to this Agreement require written form in order to be valid. The Parties declare that they have read the Agreement, understand it and are aware of their rights and obligations.
12.8. In the event that other language versions of this Licence Agreement are created and there is a linguistic discrepancy between them, the Polish language version shall prevail.

List of changes in the software

Version 6.03.032
Date: 9.05.2025

1. Improved the mechanism for deleting access cards in HID® Aero® devices and KaDe series 3000 controllers.
2. Fixed issues with assigning access levels to users and sending them to HID® Aero® devices and KaDe series 3000 controllers.
3. Improved system performance when handling a large number of NOVUS series 4000 recorders.
4. Increased system responsiveness when managing a large number of devices and highly complex configurations.
5. Enhanced T&A (Time and Attendance) functionalities – night shift mode, attendance list behavior, accurate work time calculation, correct generation of daily summary emails, and compensatory time entry.
6. Added the Device Tree tool – placed on the panel, it displays a list of all CCTV devices added to the system. It allows creating new video views directly from the panel by dragging video channels or entire devices into the Video tool window.
7. Added the ability to drag items from the Synoptic Board tool into the Video tool on the CCTV panel, enabling the creation of new video views directly from the panel.
8. Added the ability to generate reports from recorders of series 4000, 6000, and NMS VSS containing the following information: IP address, disk status, total recording time, recording range, time difference on the device (compared to the server generating the report), and software or firmware version.
9. Added a button in the Operations tab to open device configuration in a web browser.
10. Fixed an issue with automatic backup creation.
11. Optimized the database protection mechanism to prevent overflow.
12. Added on-demand connection functionality for CCTV devices.
13. Modified the connection method for Satel alarm control panels (authentication using administrator code).
14. Added support for single-stream CCTV devices (enabling, for example, two-way audio communication for Zenitel ELSII-10LHM and ELSII-10HM speakers).
15. Improved the display of the device tree.

Version 6.00.004
Date: 27.06.2024

1. Added visualization of the POLON 6000 fire alarm system
2. Added the ability to build an access control system based on HID® Aero® X1100 controllers and X100, X200, X300 expansion modules
3. Added an encrypted OSDP connection for HID® devices
4. Added time-based anti-passback for zones
5. Changed icon appearance
6. Added the ability to exempt VIPs from time-based anti-passback mode
7. Added licenses (extensions): NOVUS MANAGEMENT SYSTEM AC KaDe OP v6, NOVUS MANAGEMENT SYSTEM AC ULPR OP v6, NOVUS MANAGEMENT SYSTEM AC HID OP v6

Version 5.00.107

1. Extended ability to configure permissions for operators
2. Added new absences
3. Added API access support
4. Modification of delegation generation method
5. Improved night hours settlement
6. Improved overtime settlement
7. Changes in generating work time reports
8. Improved updating in multi-server mode
9. Fixed problem with video export paths
10. Fixed problem with trigger configuration
11. Fixed problem with RCP passwords starting from zero
12. Fixed problem with setting video verification

Version 5.00.90

1. Added support for modified method of calculating license points
2. Added support for NOVUS MANAGEMENT SYSTEM AC NMS VSS OP extension
3. Added ability to filter days in triggers
4. Improved deleting logs+

Version 5.00.71

1. Possibility to change the order of devices in the device window
2. Added the ability to permanently collapse the event window to disable
3. Improved remembering the event window pin
4. Improved scrolling in the video split selection window
5. Improved display on 4K screens
6. Improved the hot spot function
7. Improved the email sending function
8. Added the ability to clone access levels
9. Improved validation when creating automatic RCP reports
10. Improved the problem with editing automatic RCP reports
11. Improved the panel opening scenario
12. Added the ability to filter archived events by entered query
13. Improved the automatic cursor jump from the hour field to the minute field when entering the time
14. Changed the default RCP template names
15. The schedule breaks field increases minutes by default after use +
16. Added a message about an incompatible version in multiserver mode
17. The license status field moves to the license window after clicking
18. Improved the problem with registering a license in a country other than Poland
19. Added information about the Trial license
20. Improved the translation of some information messages
21. RCP - Configuration/RCP Terminals / Operations - synchronization - downloading events from the terminal from a specified date by the operator's command.
22. A condition was added in the "Image analysis - license plate recognition" scenarios
23. The method of adding channels for NMS and Novus Management System VSS was changed
24. The property fields of date of birth, position, telephone, address and education were removed
25. The possibility of limiting the editing time of event correction was added
26. The default time range for RCP reports was changed
27. RCP: new statuses were added: Private exit without return and Business exit without return
28. Improved user export and import
29. License modifications
30. RCP - Sorting columns in the RCP template definition window.
31. RCP - Possibility of defining proper names for columns in the RCP report template
32. RCP - Custom reports - the sum of individual reports for the entire department or company in one file.
33. RCP - Settlement of shift work time system - from 1 to 4 shifts per day.
34. RCP - Modification of the method of communication with work time registration terminals.
35. Building automation - integration with the LANKON-008 device

Version 5.00.035

1. Diagnostic Window tab moved to Server Settings tab
2. Changes in Backup window: creating, deleting and restoring copies are now in one place
3. Diagnostic Logs moved to Client Settings tab
4. Licenses Tab Changes: Registration form and GDPR clause added to Registration sub-tab
5. Licenses sub-tab displays currently used keys, number of license points, maximum number of LPR vehicles and RCP users, displaying multi-server and hardware identifier
6. Ability to activate and deactivate license keys.
7. Added button to synchronize with the license server
8. Added button to export license information to a pdf file
9. Added button to activate the trial license
10. Added integration with the Satel alarm control panel
11. Changed organization of user identifiers in the Users tab
12. Added button “Generate Import Template” in the Users tab
13. Added cloning button in the scenarios and panels tab
14. Changed organization in the Holidays tab
15. Added search field in the Video Views tab
16. Added a third state of the notification pin button, you can now lock the notification window so that it does not expand on an event.
17. Video export now has two tabs, “Task List” and “Settings”
18. Added Custom work time report

AAT SYSTEMY BEZPIECZEŃSTWA Sp. z o.o.

ul. Puławska 431, 02-801 Warszawa
tel. 22 546 05 46, faks 22 546 05 01
e-mail: aat.warszawa@aat.pl, www.aat.pl — Warszawa

ul. Kolejowa 12C lok. 4/2, 15-701 Białystok
tel./faks 85 688 32 33, 85 688 32 34
e-mail: aat.bialystok@aat.pl, www.aat.pl — Białystok

ul. Fordońska 183, 85-737 Bydgoszcz
tel./faks 52 342 91 24, 52 342 98 82
e-mail: aat.bydgoszcz@aat.pl, www.aat.pl — Bydgoszcz

ul. Ks. W. Siwka 17, 40-318 Katowice
tel./faks 32 351 48 30, 32 256 60 34
e-mail: aat.katowice@aat.pl, www.aat.pl — Katowice

ul. Prosta 25, 25-371 Kielce
tel./faks 41 361 16 32, 41 361 16 33
e-mail: aat.kielce@aat.pl, www.aat.pl — Kielce

ul. Biskupińska 14, 30-737 Kraków
tel./faks 12 266 87 95, 12 266 87 97
e-mail: aat.krakow@aat.pl, www.aat.pl — Kraków

90-019 Łódź, ul. Dowborczyków 25
tel./faks 42 674 25 33, 42 674 25 48
e-mail: aat.lodz@aat.pl, www.aat.pl — Łódź

ul. Racławicka 82, 60-302 Poznań
tel./faks 61 662 06 60, 61 662 06 61
e-mail: aat.poznan@aat.pl, www.aat.pl — Poznań

Al. Niepodległości 606/610, 81-855 Sopot
tel./faks 58 551 22 63, 58 551 67 52
e-mail: aat.sopot@aat.pl, www.aat.pl — Sopot

ul. Zielona 42, 71-013 Szczecin
tel./faks 91 483 38 59, 91 489 47 24
e-mail: aat.szczecin@aat.pl, www.aat.pl — Szczecin

ul. Na Niskich Łąkach 26, 50-422 Wrocław
tel./faks 71 348 20 61, 71 348 42 36
e-mail: aat.wroclaw@aat.pl, www.aat.pl — Wrocław

NIP: 9512500868, REGON: 385953687, Nr BDO: 000433136

Wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m.st. Warszawy w Warszawie,
XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000838329,
kapitał zakładowy wpłacony w całości w wysokości:17 005 000 zł