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

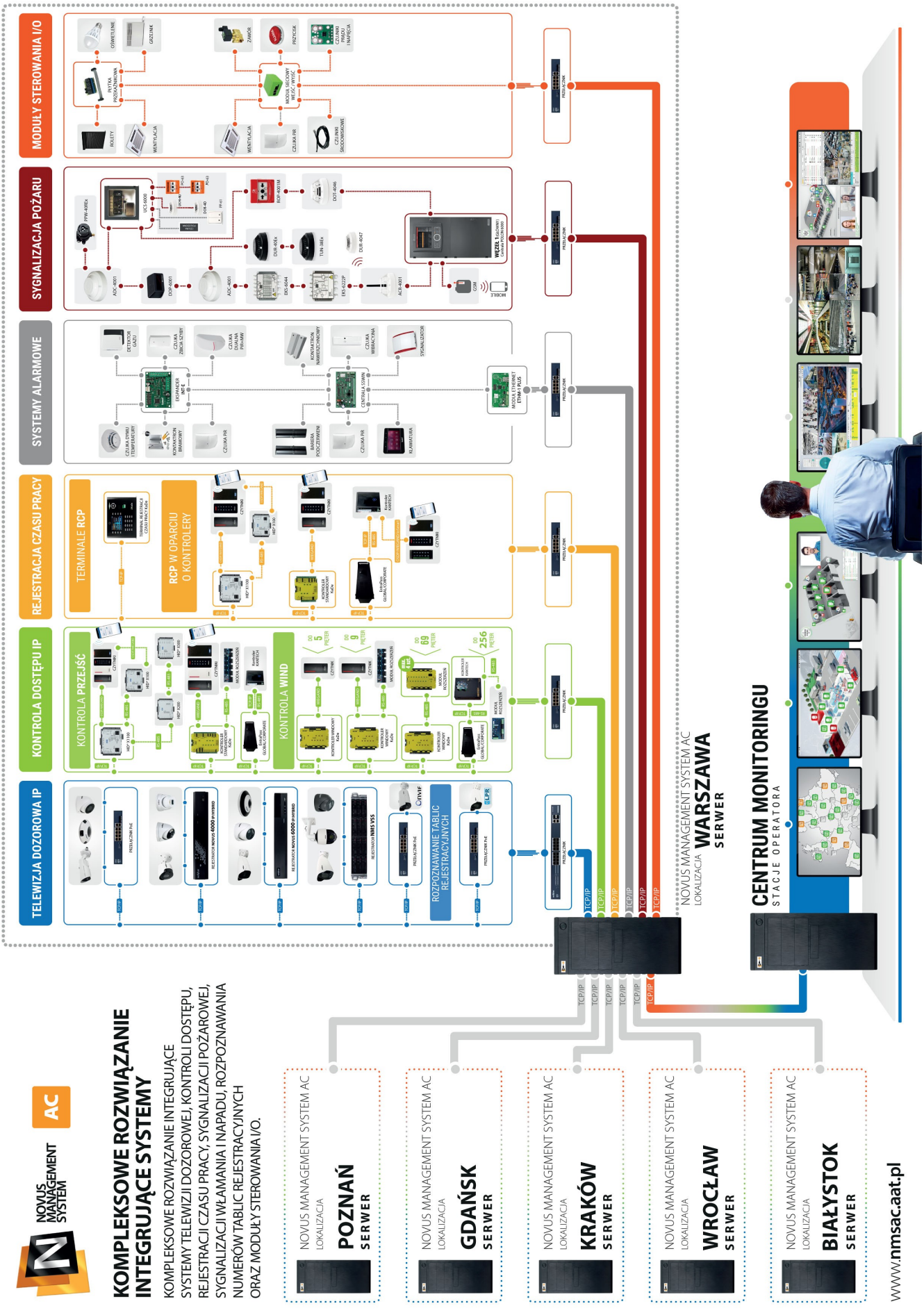
License plate recognition (LPR)	
Parameter or function name	**Parameter or function value**
Supported devices	IP cameras Novus NVIP-2H-6732M/LPR / NVIP -4H-6732M/LPR connected directly or via an NOVUS MANAGEMENT SYSTEM VSS IP recorder
Number of cameras supported	No program limitations
Support for QR 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.

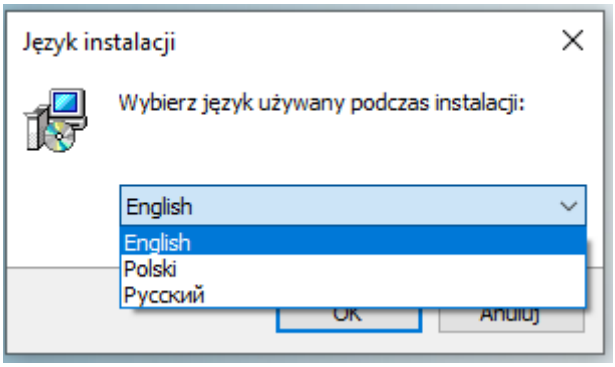
A trial license for the program (**TRIAL**) is also available, its duration is 60 days. It includes full functionality and a limit of 500,000 license points, 500,000 RCP users, 500,000 LPR vehicles and 100 operator stations. For detailed information, please contact the sales department of AAT SYSTEMY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

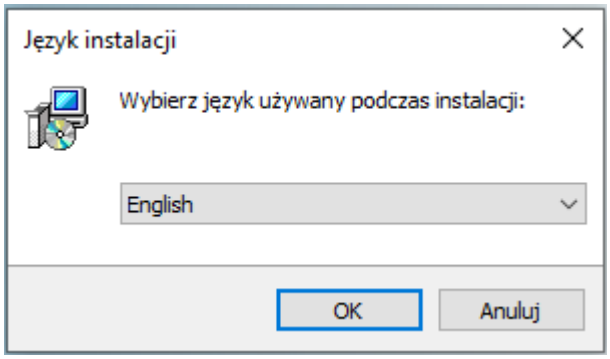
2.3 Software installation

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).

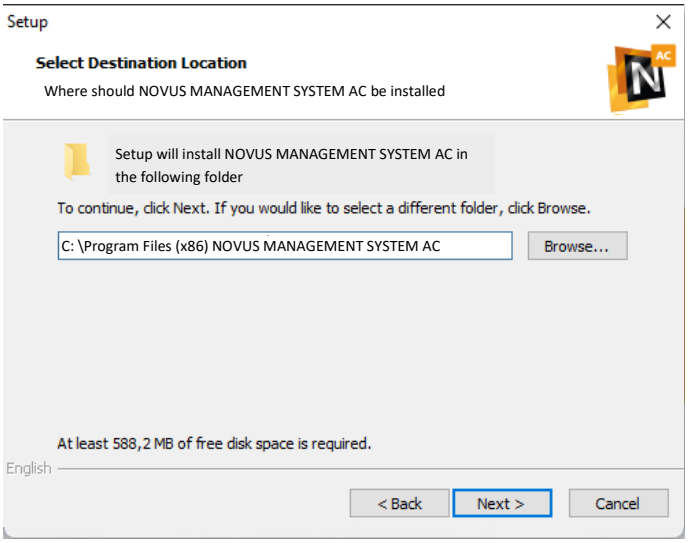
After running the **NOVUS MANAGEMENT SYSTEM AC installer**, the window shown below will appear on the screen. Select the language of the installer from the drop-down list and confirm with **OK**.

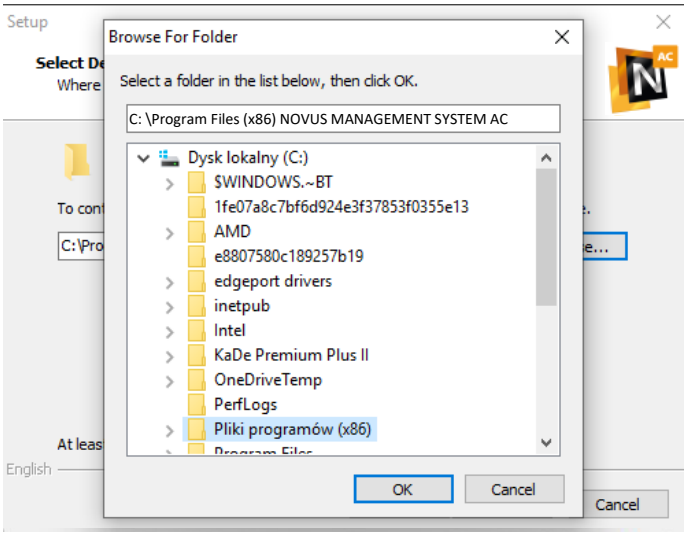




User License will be displayed, which need confirmation after reading to pass to the next installation step. After checking ***I accept the agreement*** checkbox click ***Next***.

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.

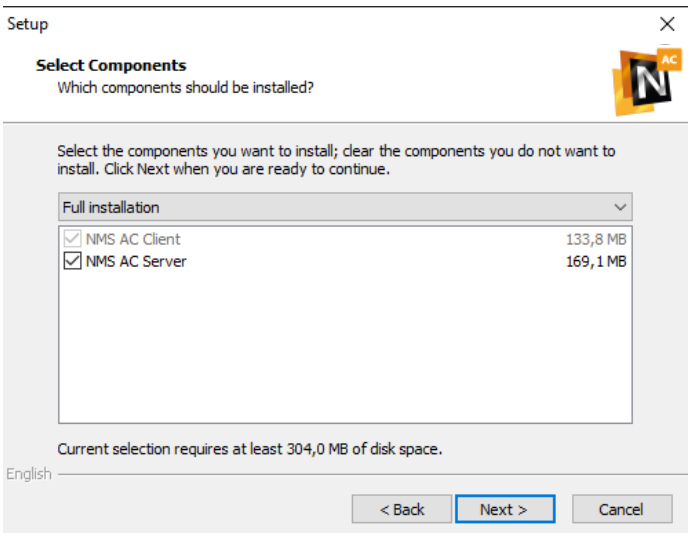


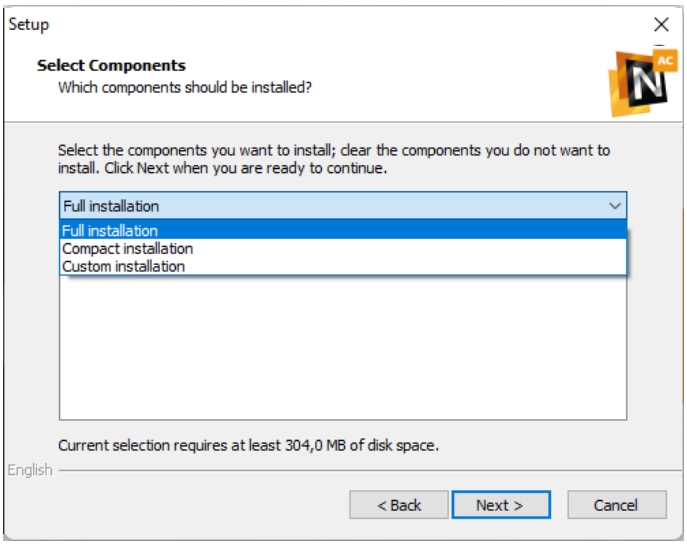


At this stage of the software installation, select its range. There are three options available in the drop-down list:

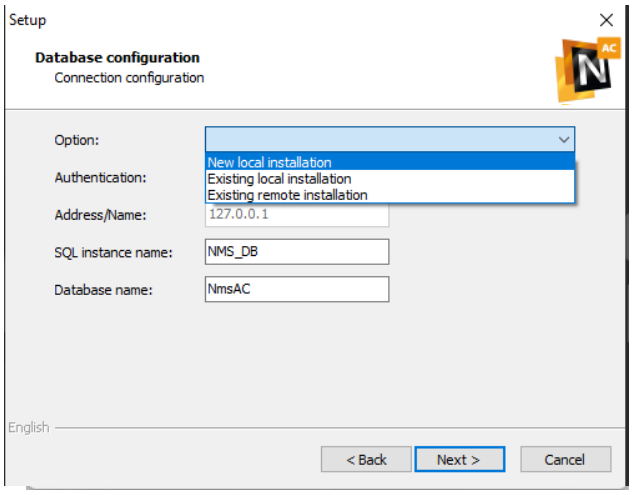
- ***Full installation*** - installs both NOVUS MANAGEMENT SYSTEM AC server and the client application
- ***Basic installation*** - installs only the client application which must be connected to the NOVUS MANAGEMENT SYSTEM AC server on another computer
- ***User installation*** - installs the components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

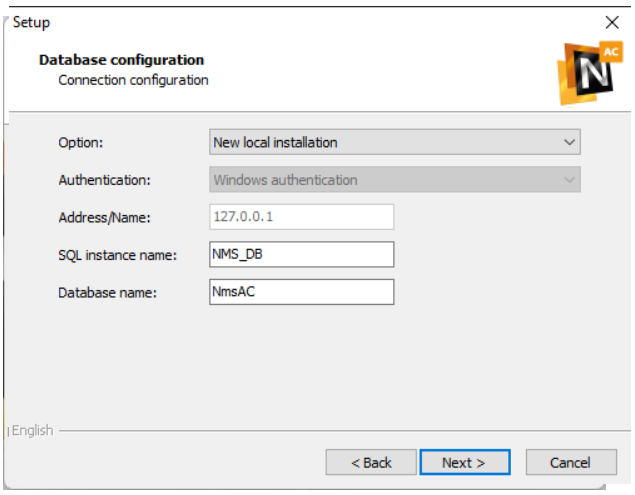
After selecting the installation range, click ***Next***.

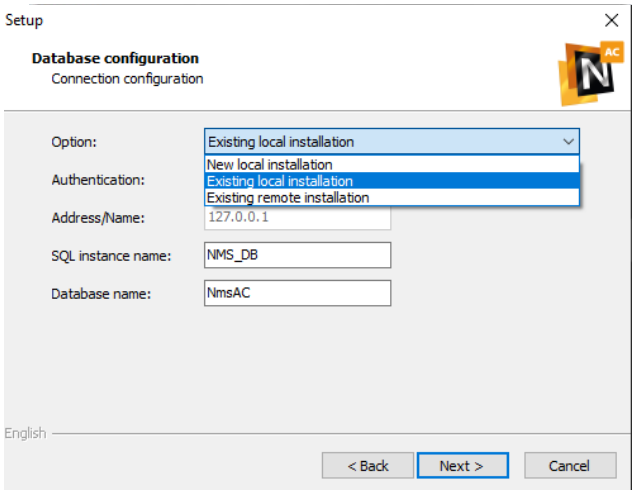


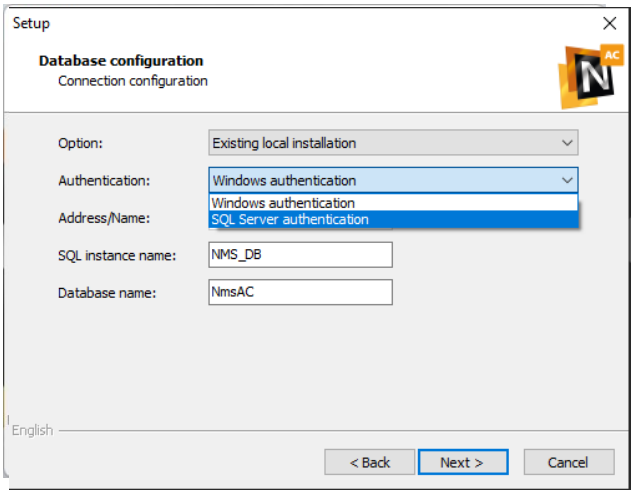


At the database configuration stage, select one of three options from the drop-down list below.





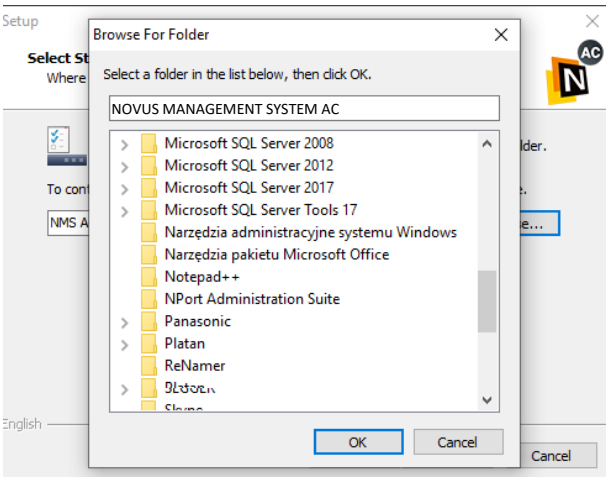




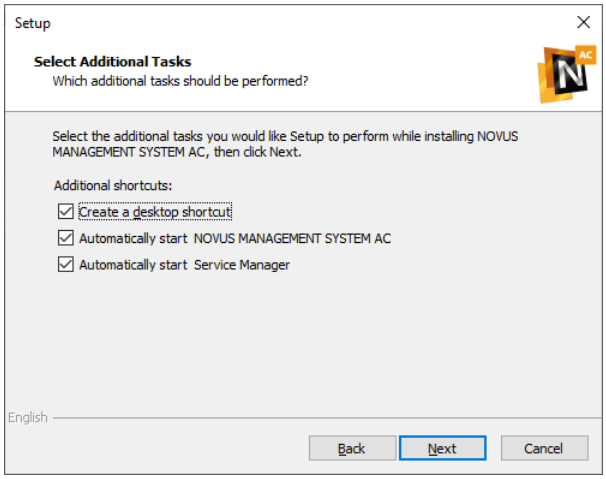
The new local installation - installs the SQL Server on the computer, creates a new SQL instance and database with the names specified in the text boxes.

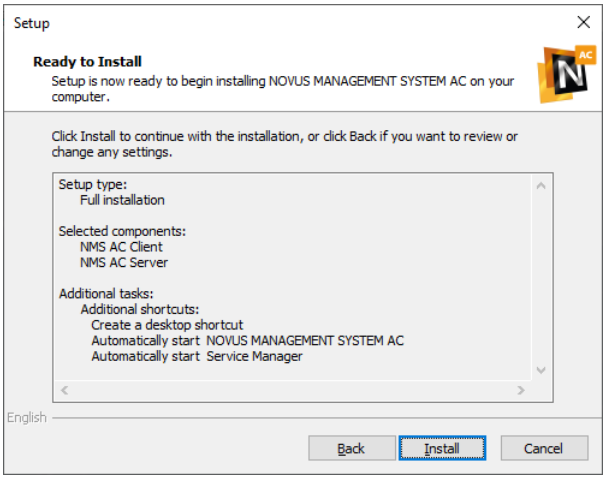
Existing local installation - this option can be selected if SQL Server is already installed on the computer; creates a new SQL instance and database with the names specified in the text boxes; if you choose to authenticate through SQL server, you must provide the login information used to confirm access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

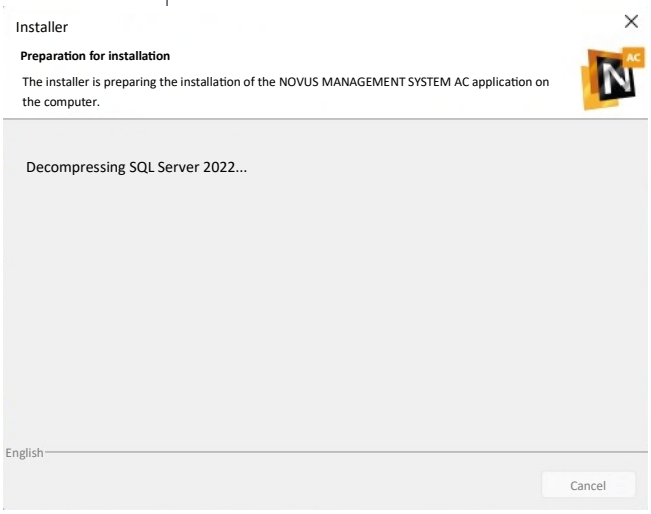


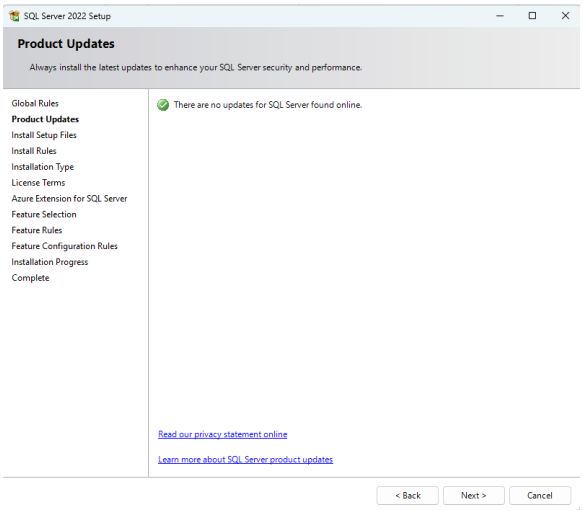


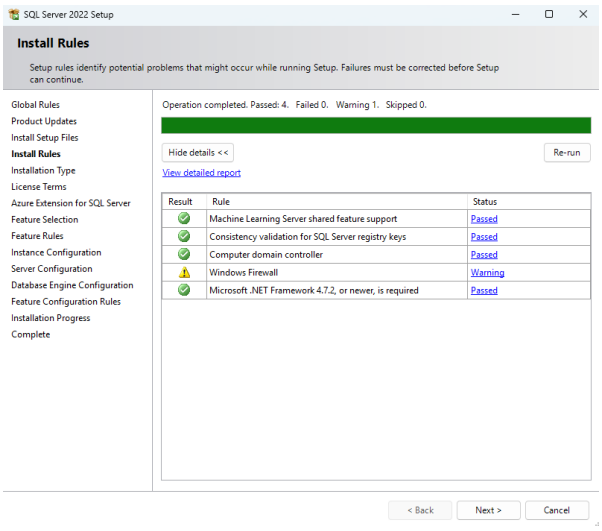
After pressing ***Next*** button, you will see the installation summary window with previously selected settings. Until this step you can go back to the previous steps of configuring the installation using ***Back*** button. If the summary settings are correct, click ***Install***.

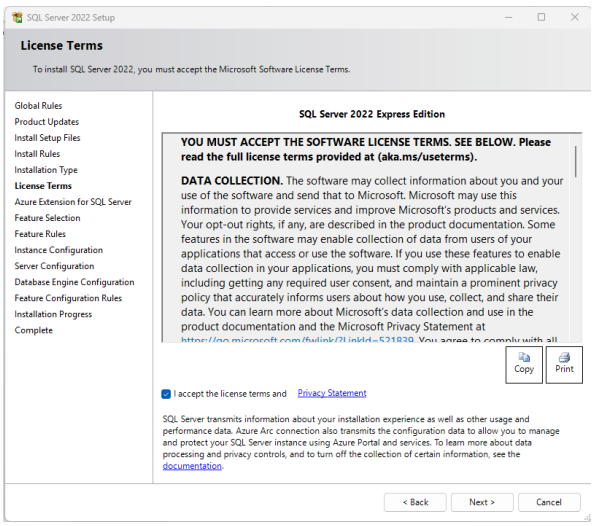
At this point, after selecting the location and names, the proper software installation process begins.

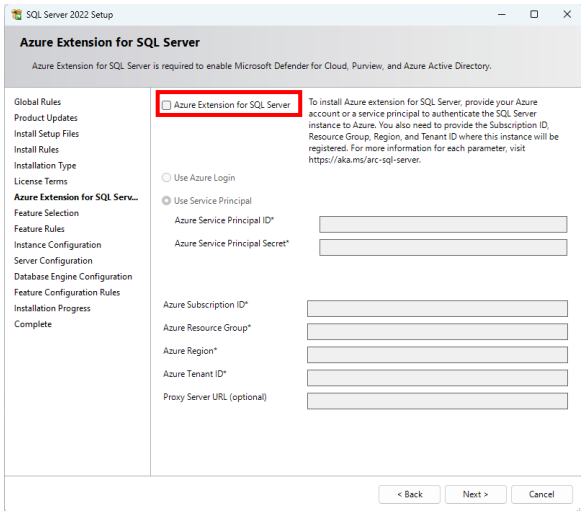
At the beginning, the SQL database will be installed according to the option you chose, and then the **NOVUS MANAGEMENT SYSTEM AC** application. If your computer is not connected to the Internet, you may be prompted to check for available updates during the installation of the SQL database, and then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

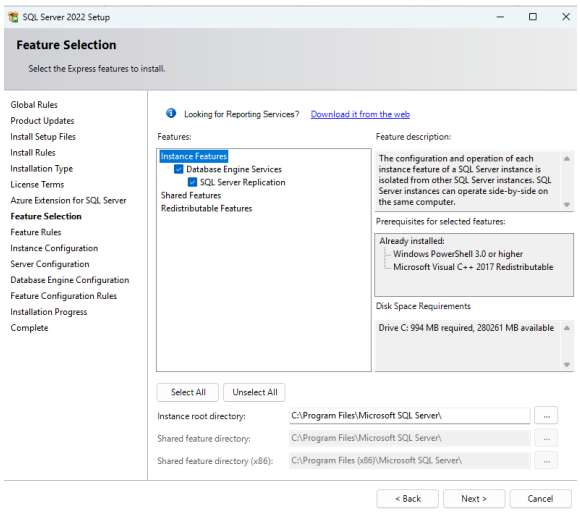




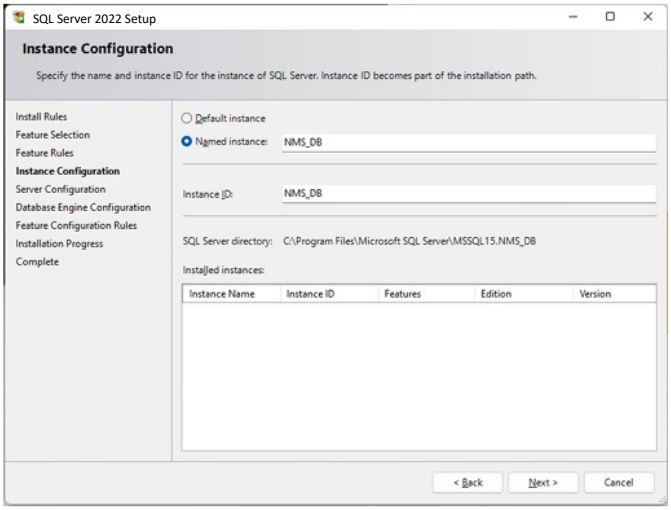


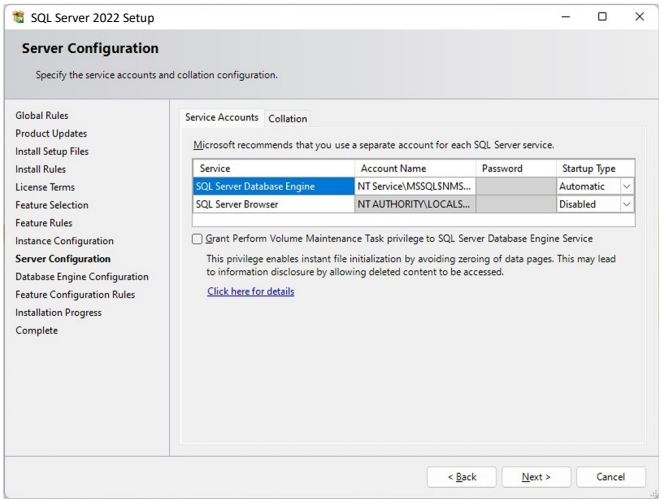


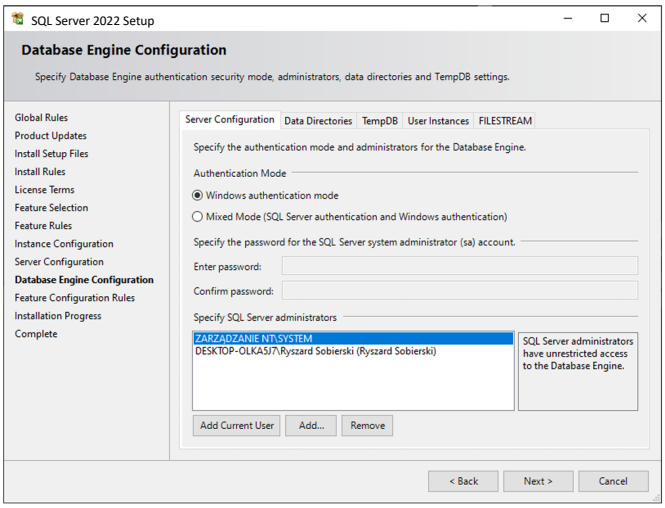


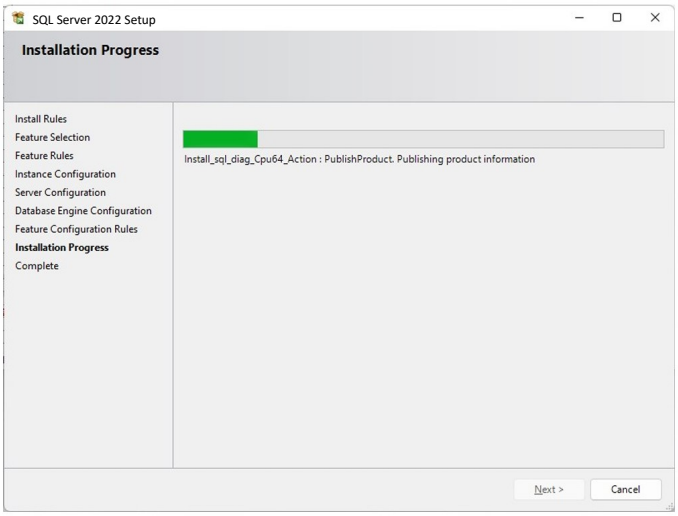


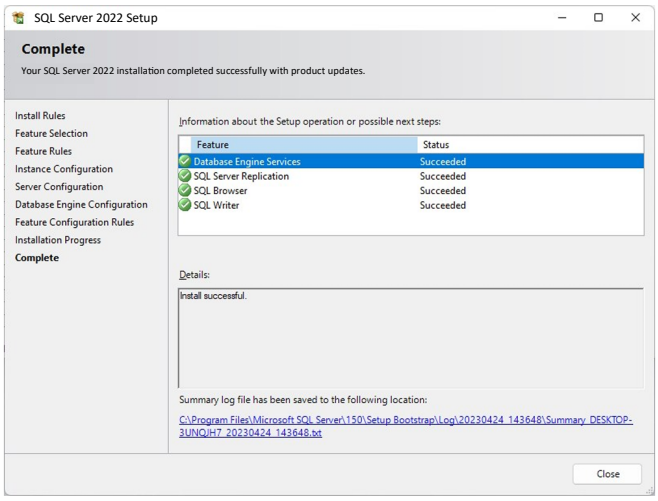
At this stage, in the next windows, click Next button and in the License Terms window, check the box for acceptance of the license (I accept the license terms and Privacy Statement).







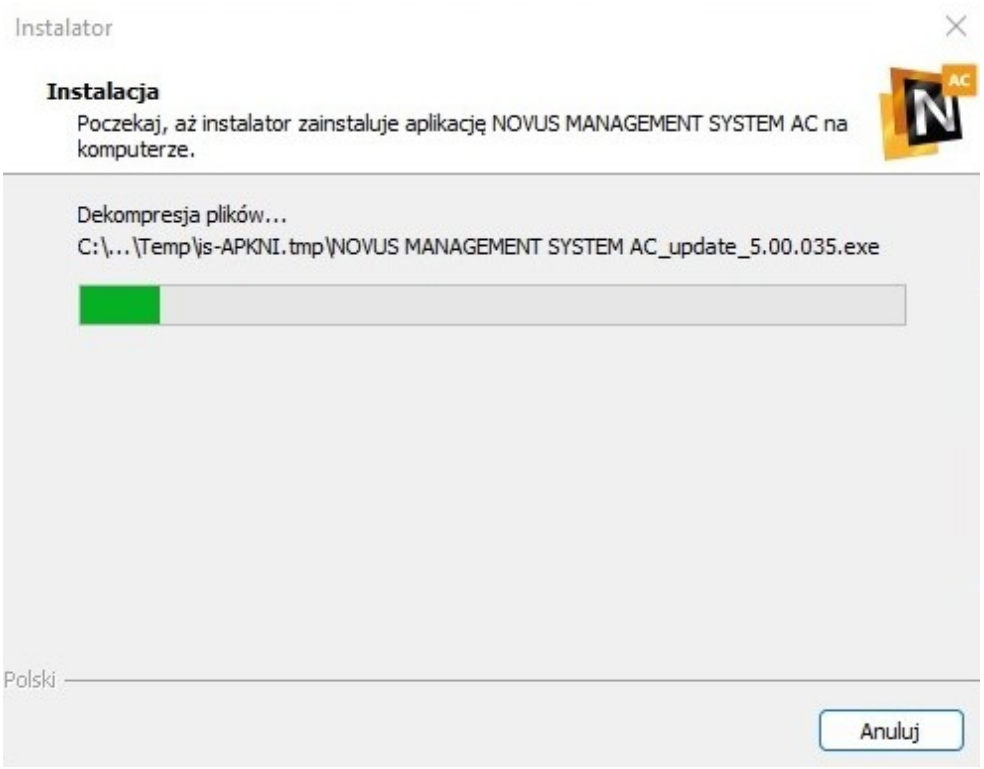




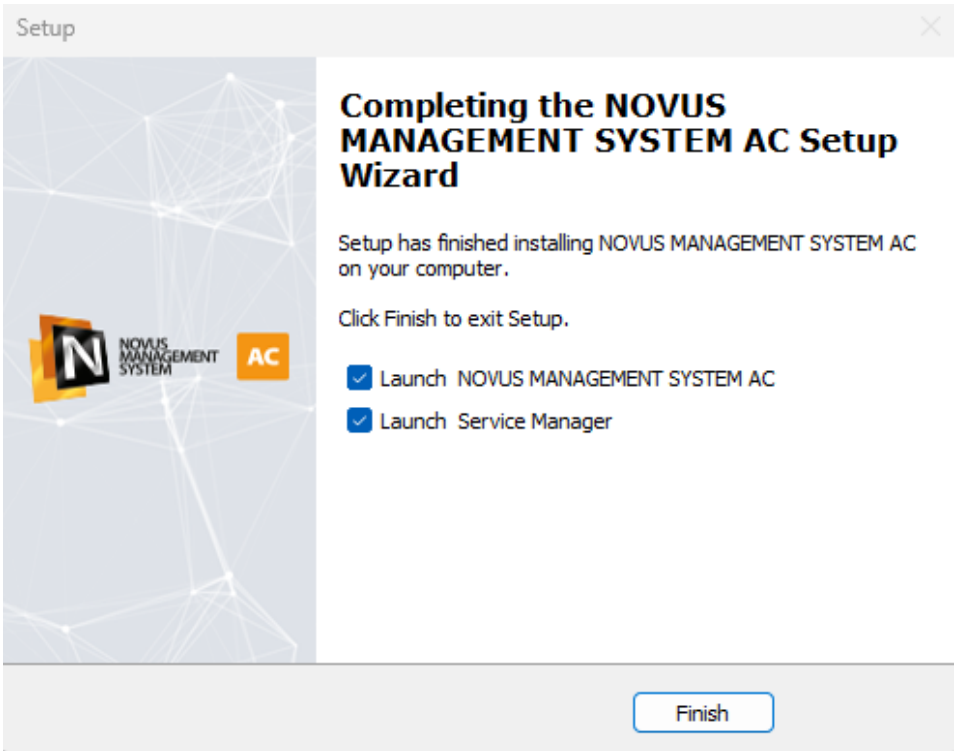
In the next steps of the installation, steps are performed according to the list on the right side of the window.

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.*

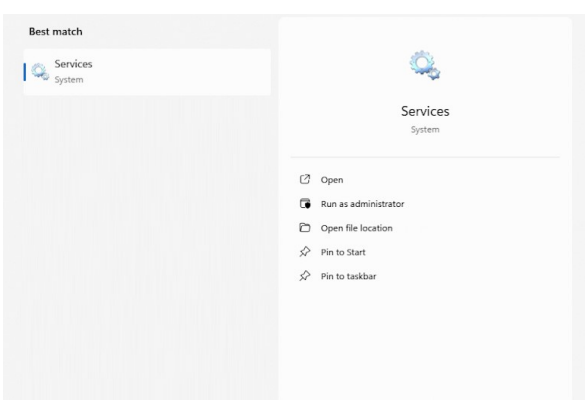
The installer will go through the process of installing the required components of NOVUS MANAGEMENT SYSTEM AC, which takes a few moments.

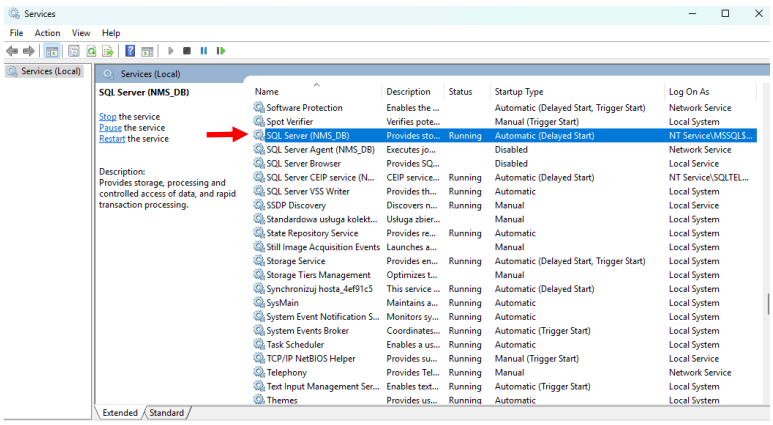


After installing the application, the information window shown below appears. You can start NOVUS MANAGEMENT SYSTEM AC immediately by clicking the ***Close*** button with the Run **NOVUS MANAGEMENT SYSTEM AC** application checkbox checked at the same time. Unchecking this box and clicking the button 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.

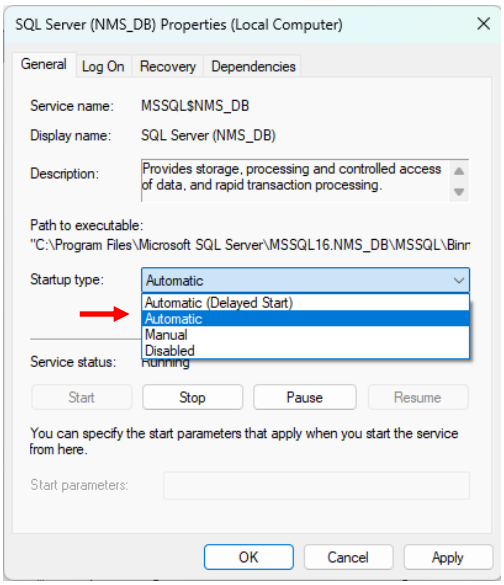


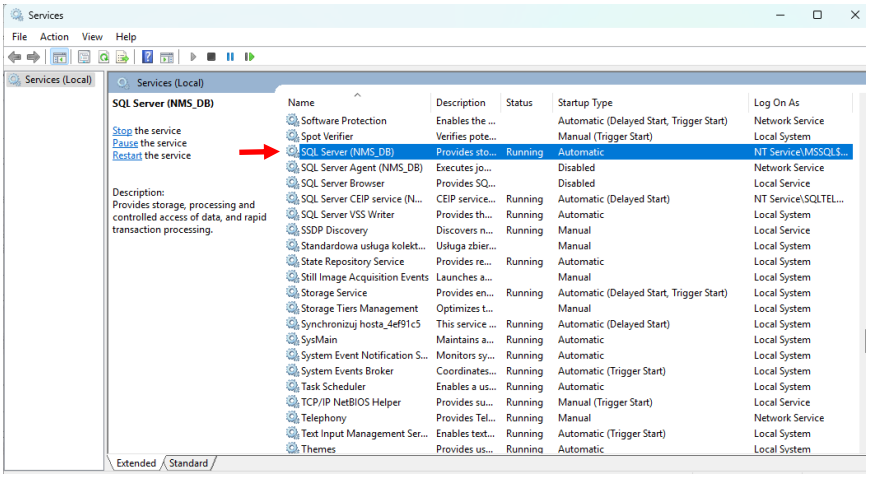
WARNING!
After installing the program server, you need to change the startup type of the SQL Server. To do this, search for “Services” in the search bar on the Windows 10/11 taskbar.





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.

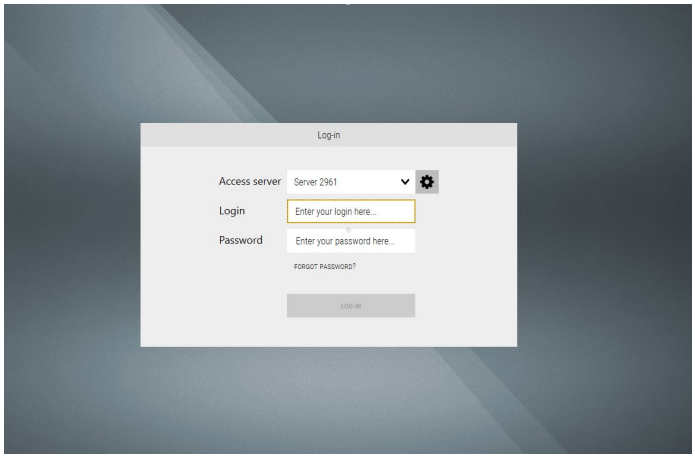
To perform the upgrade, follow the same steps as described in the section on program installation.

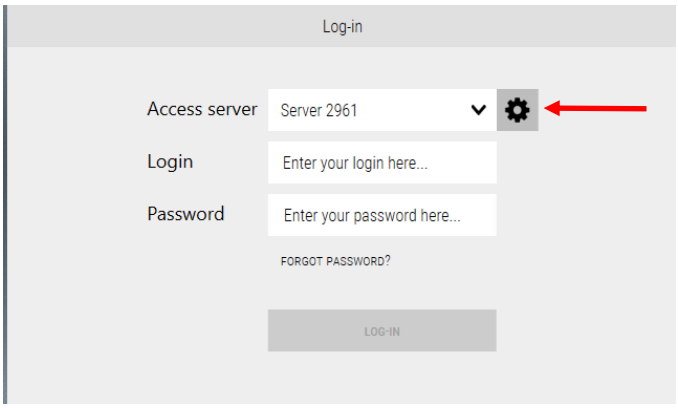
Before updating from version 6.00.004 to version 6.01.039 or later, an intermediate update to version 6.00.012 must be performed.

2.5 Running the program

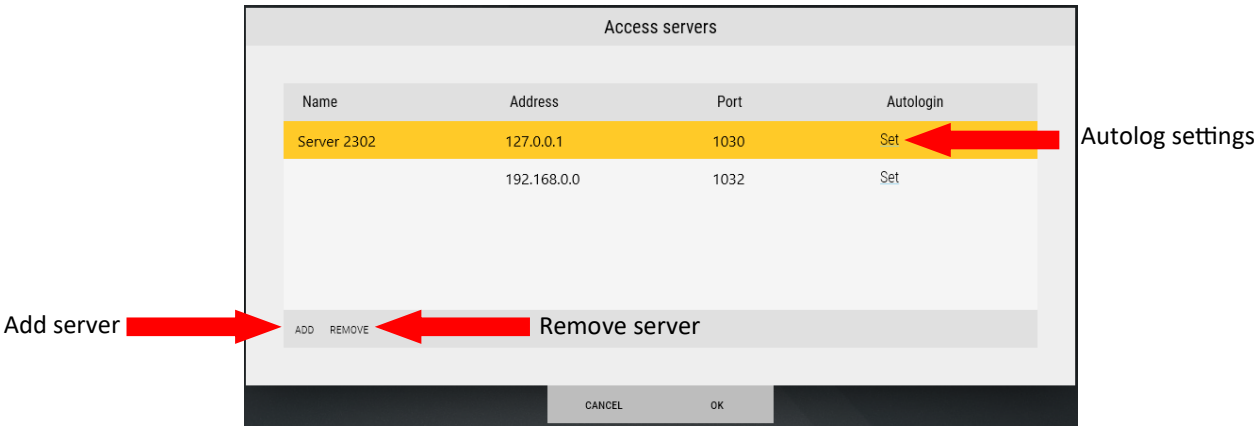
After installing **NOVUS MANAGEMENT SYSTEM AC** software, the icon shown below will appear on the desktop by default, and the **NOVUS MANAGEMENT SYSTEM AC** group will be created in the Windows start menu. You can use them to launch the program.

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.

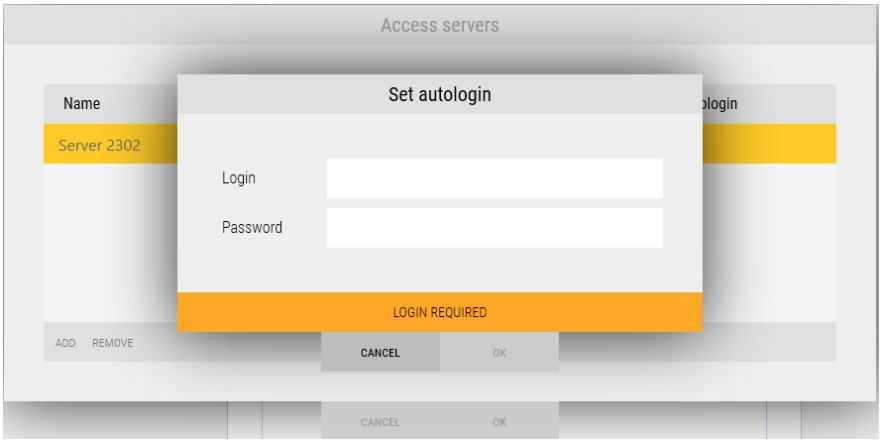




The access server list window allows you to add, delete and configure **NOVUS MANAGEMENT SYSTEM AC** servers to which the operator station can be connected. When adding a server, enter its IP address and port number (default is 1030). The server name will be downloaded automatically after the connection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

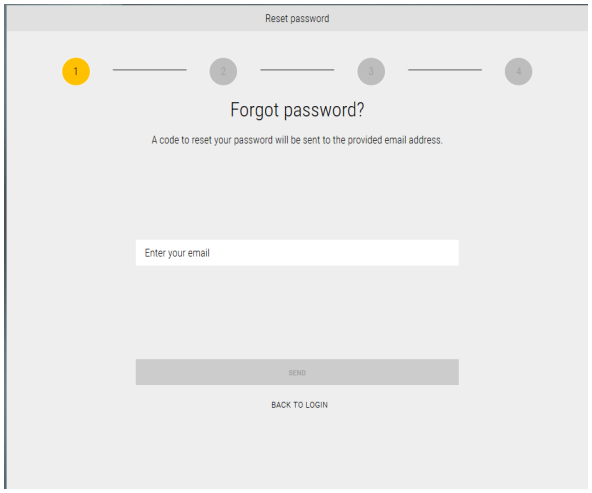


After clicking the **Set/Autologin button,** it is possible to set the name of the operator and the password for the automatic login of the operator added to the system immediately after starting the program.

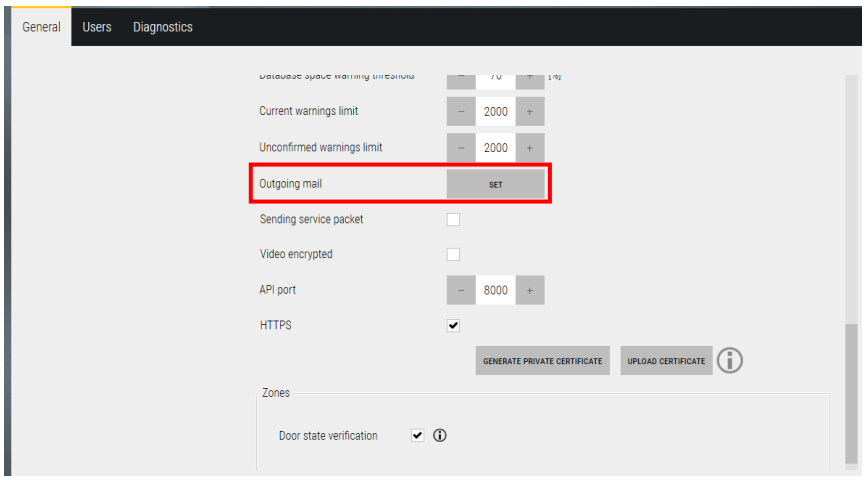


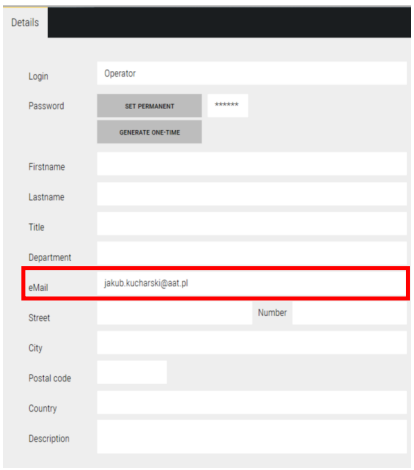
Please note that the autolog function is only available to operators assigned to groups with the "Autolog available" permission.

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

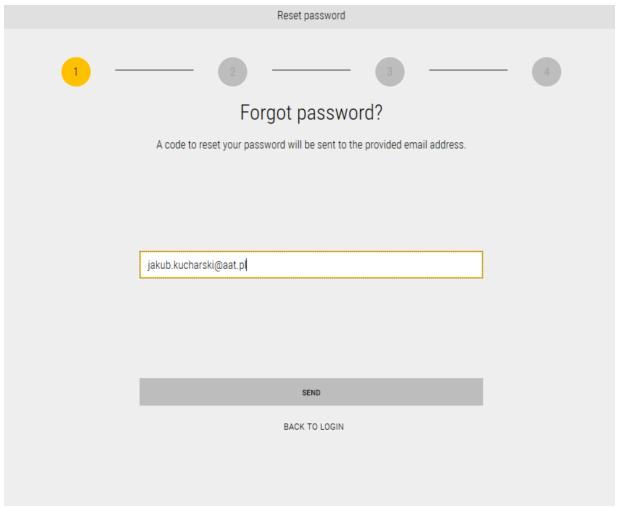


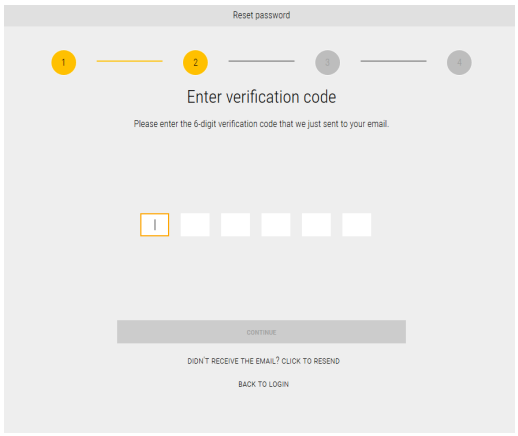
WARNING! This function works only after configuring the outgoing mail server in the **System > Server Settings** tab and setting the operator's email address in the **System > Groups and Operators** tab.

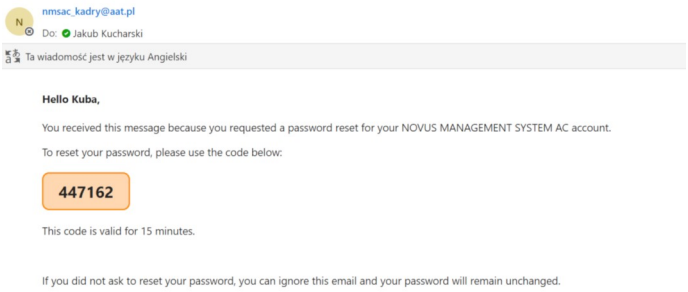


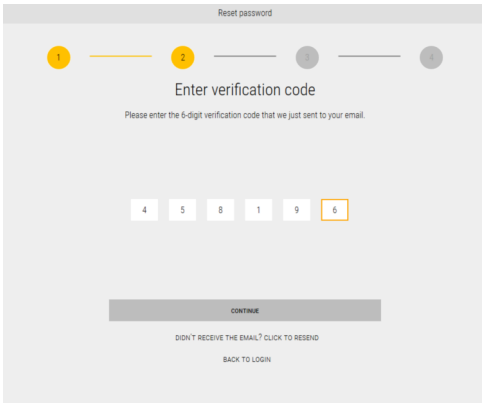


The operator recovers the password by entering their assigned email address, to which a six-digit code will be sent. The email is sent automatically after proceeding to the code entry window.

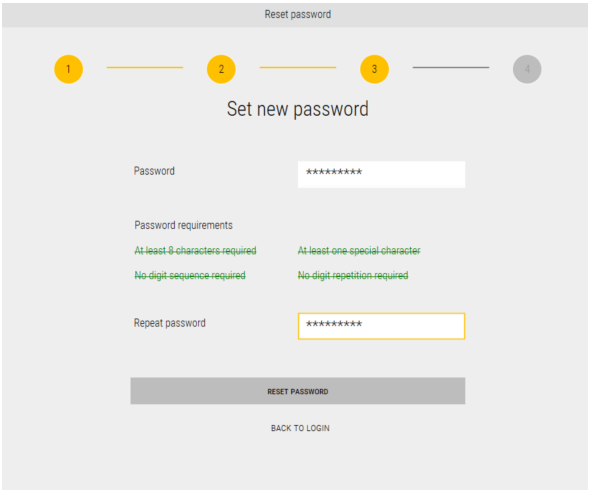


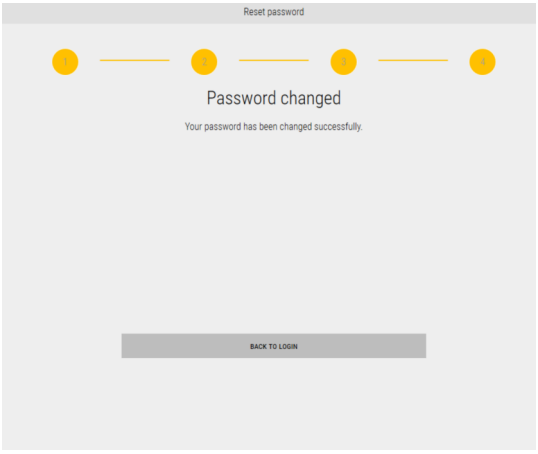






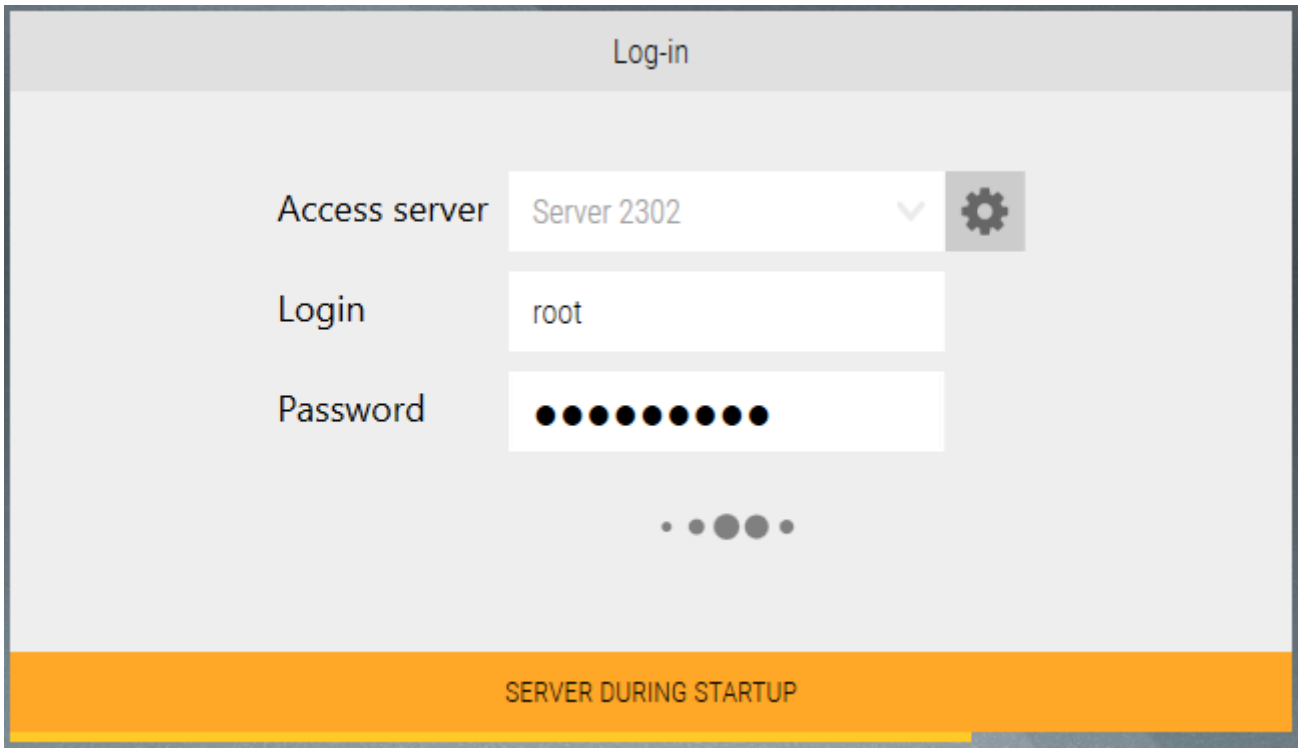
After correctly entering the six-digit code, the operator can change their password according to the specified requirements.
Once confirmed, the password is updated.



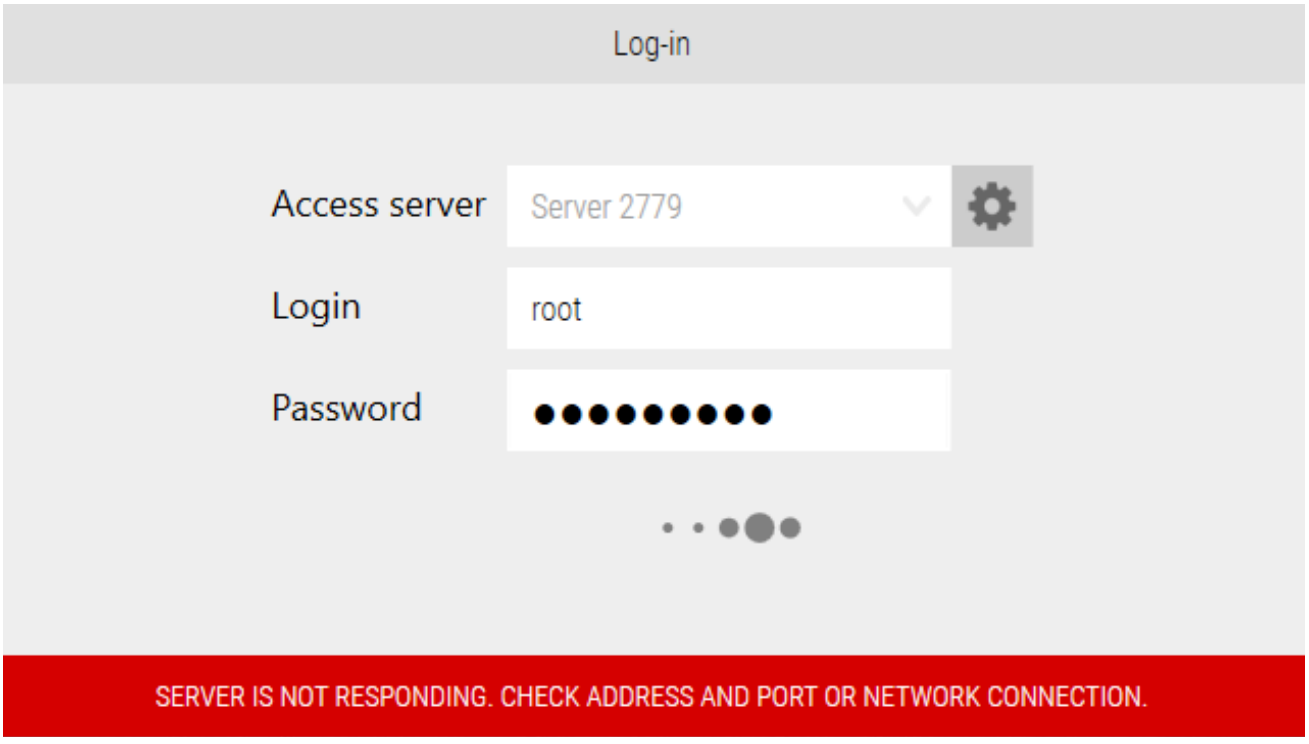


WARNING! If the email with the code is not delivered, click **"DIDN'T RECEIVE THE EMAIL? CLICK TO RESEND."**
If the email still does not arrive, check the **SPAM** folder in your mailbox.

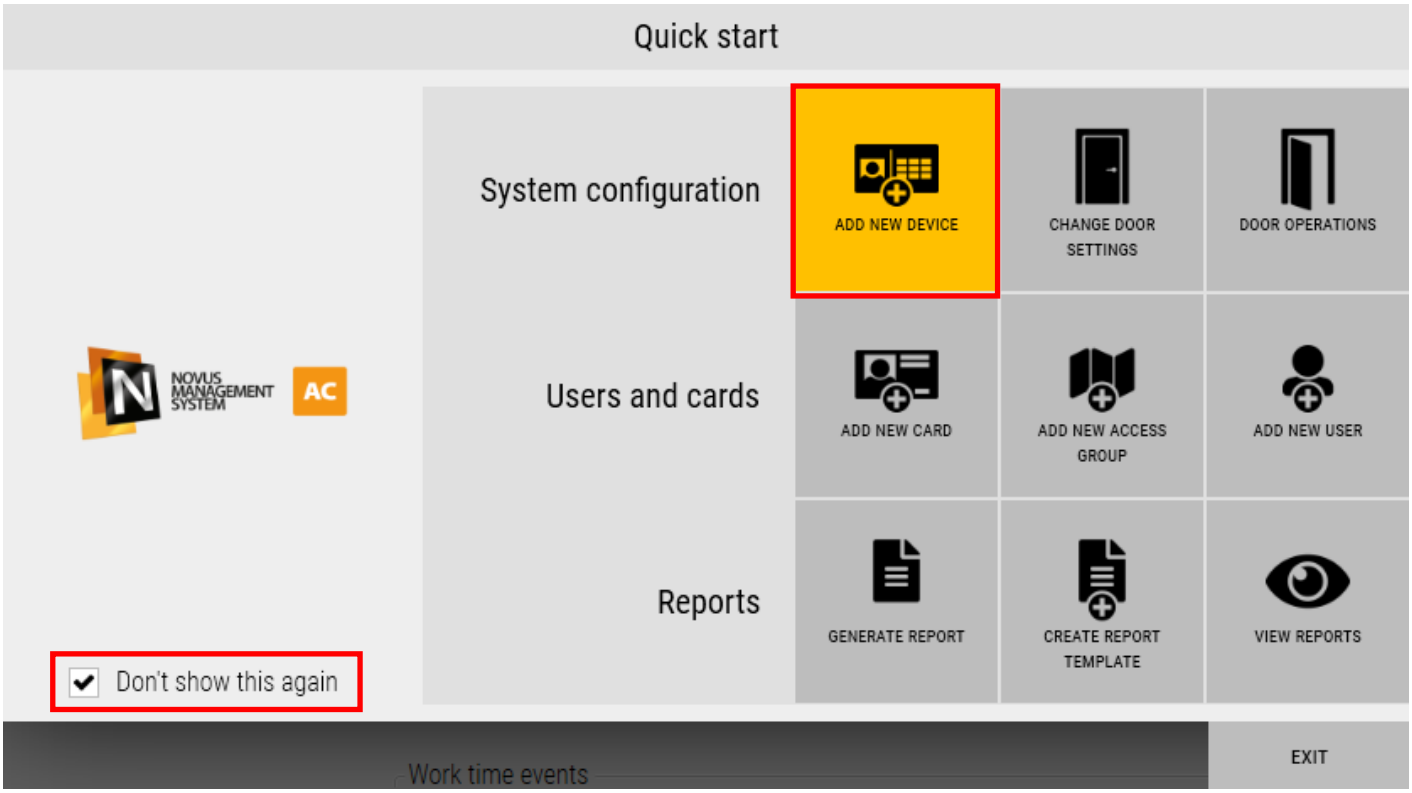
After you enter your name and password and click on the LOGIN button, you may see the message SERVER IN STARTING UP at the bottom of the window. This means that you should wait as the server service is starting up (e.g. after a reboot).



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

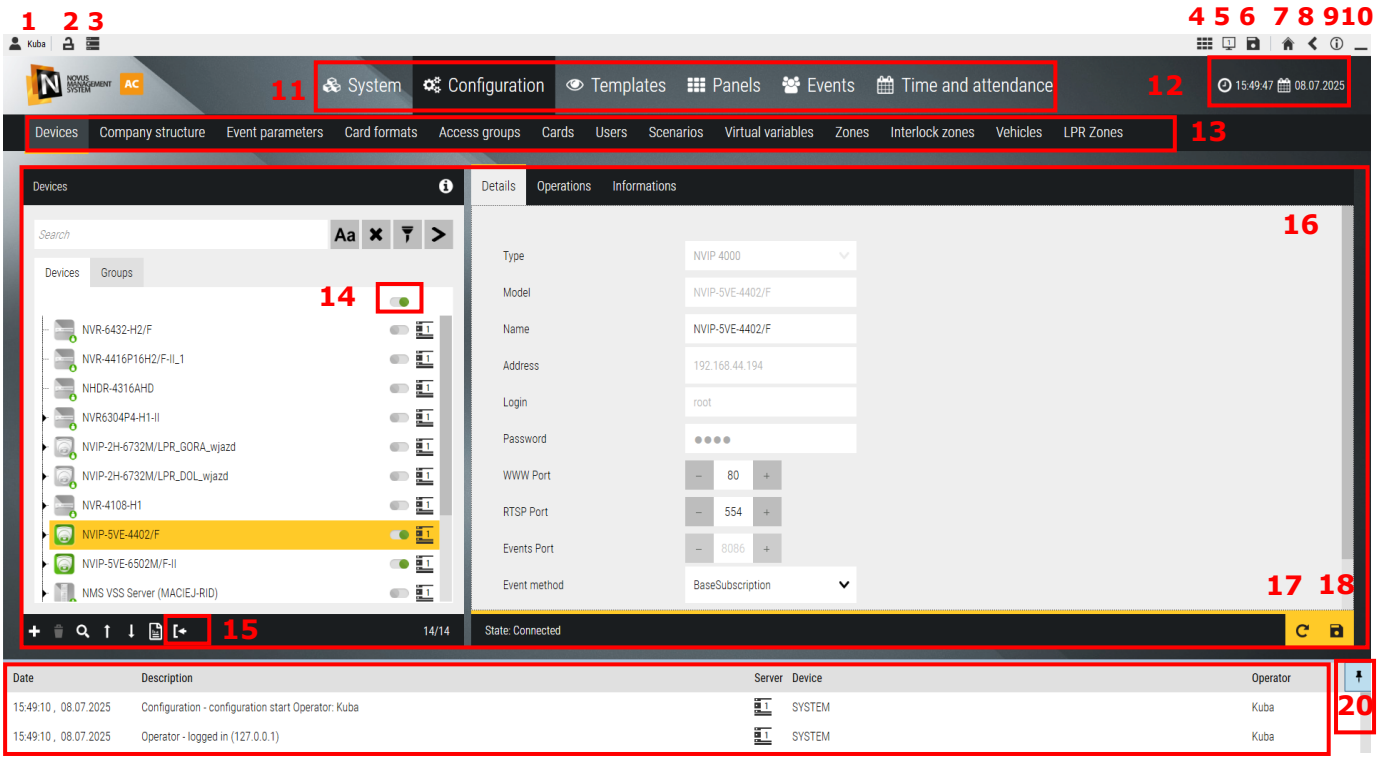
3. Reports

- ***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

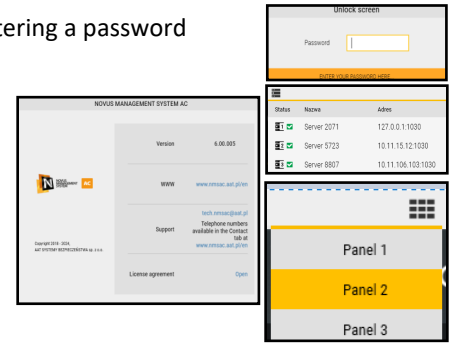
Selecting the **Don't show this again** checkbox detailed in the above figure causes the **Quick Start** window not to be automatically displayed when **NOVUS MANAGEMENT SYSTEM AC is** started. The Exit button closes the **Quick Start** window.

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



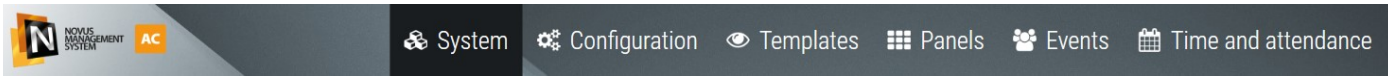
10. **Minimize** button - minimizes the program NOVUS MANAGEMENT SYSTEM AC window.
11. Section selection bar - click on the appropriate section to configure or preview options.
12. Current server time and date.
13. Tab bar - allows you to move between the various tabs of the selected section.
14. Button 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.

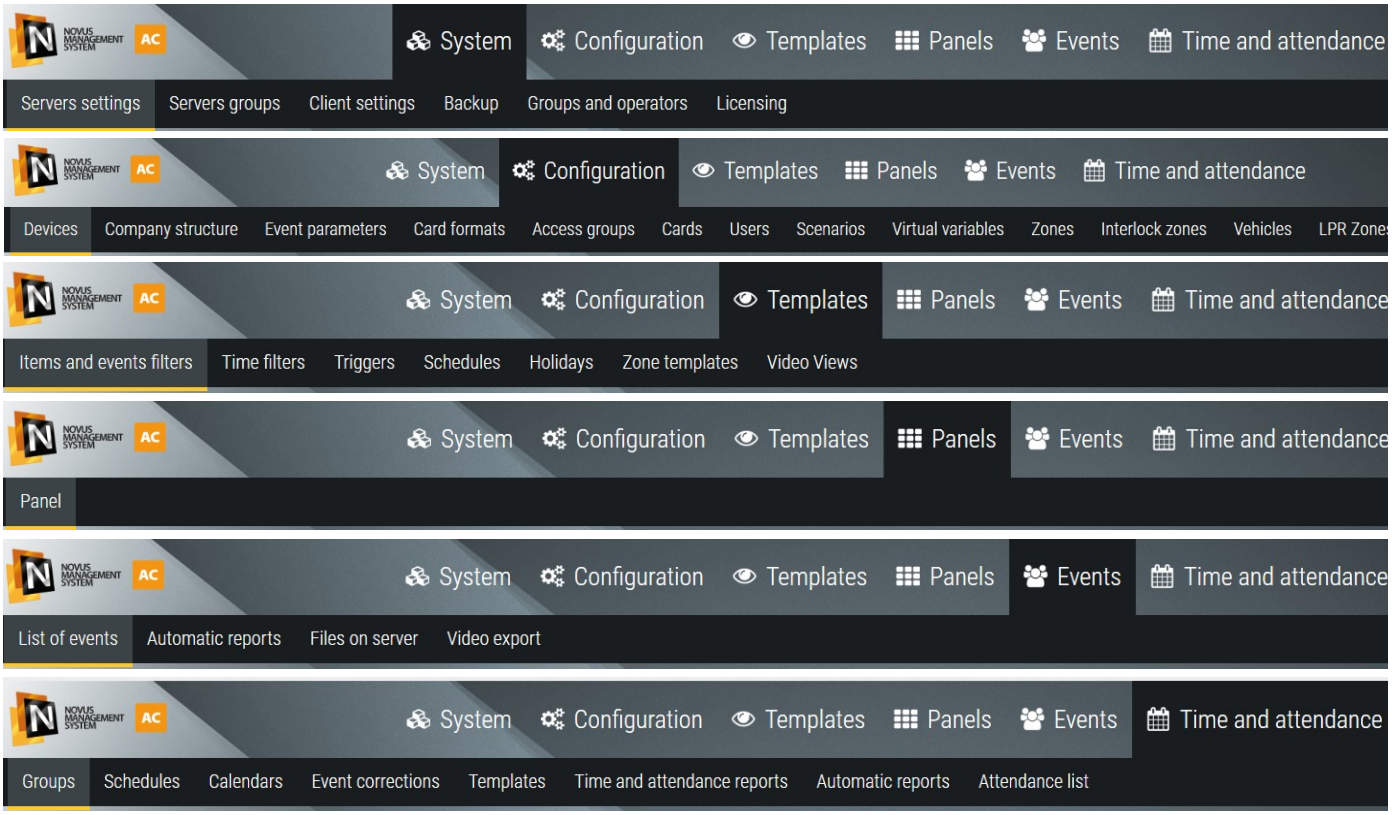
2.7 Program menu

The program menu contains two bars.

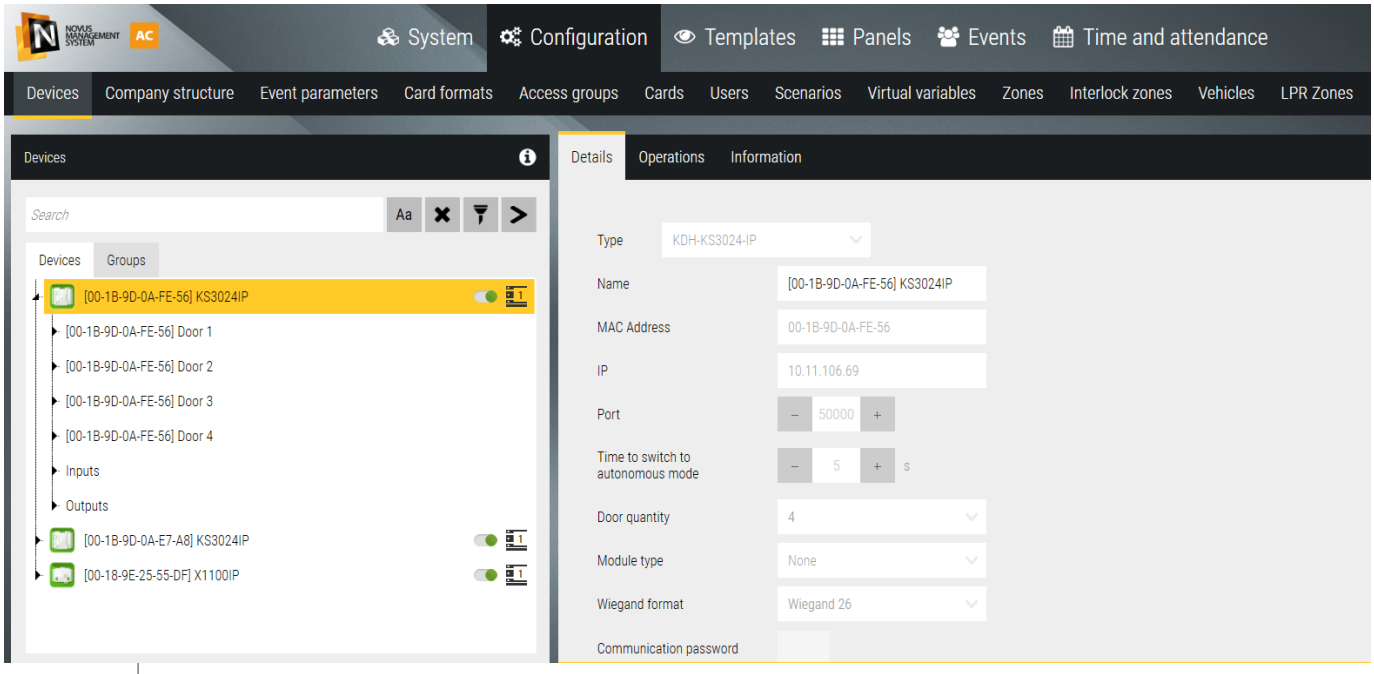
Main bar:



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	-

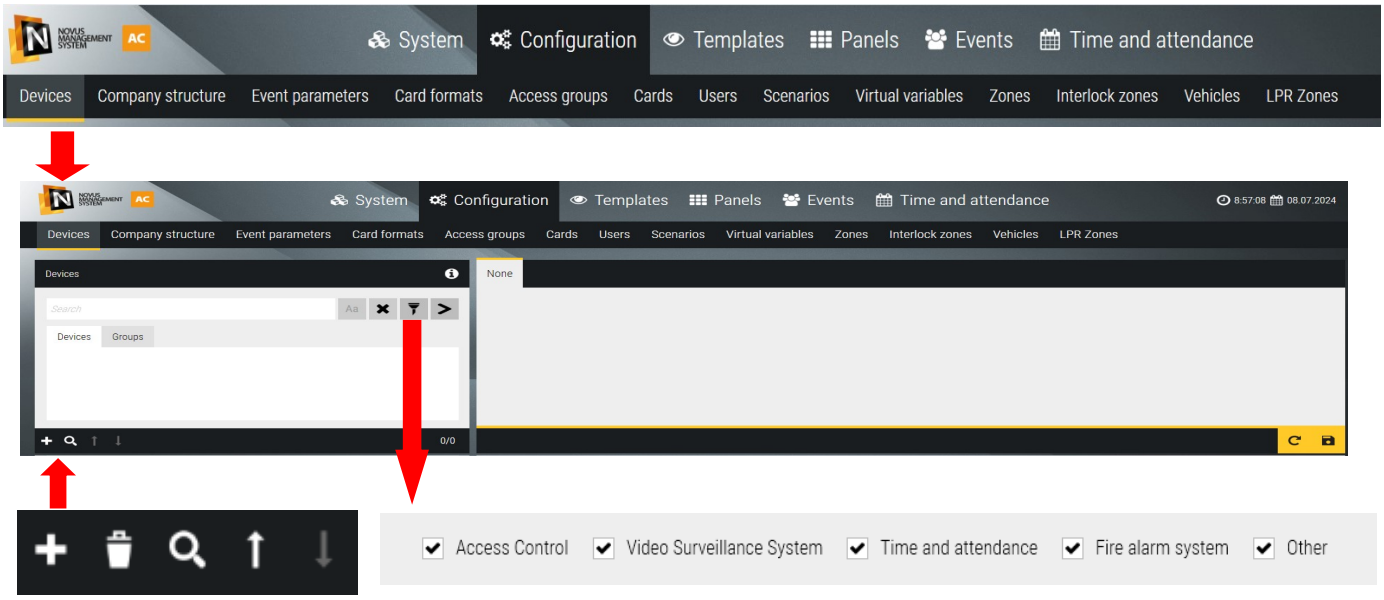
Icon symbol	Description	Location
	Report in CSV	Events
	Report in HTML	Events
	Auto report.	Events
	Alarm deletion	-
	Alarm	-
	Size of letters	-
	Error / info	-
	Refresh	Configuration
	Save	Configuration
	Add	Configuration
	Delete	Configuration
	Import list	Configuration
	Export list	Configuration
	Search	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.



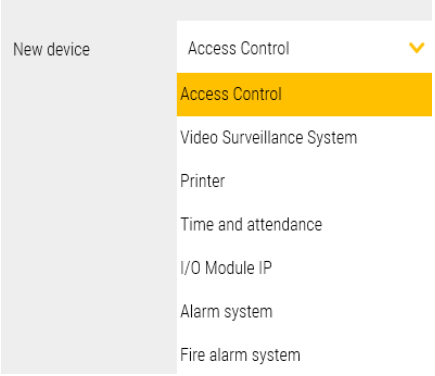
- add new device
- remove
- search
- change order of devices up/down

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

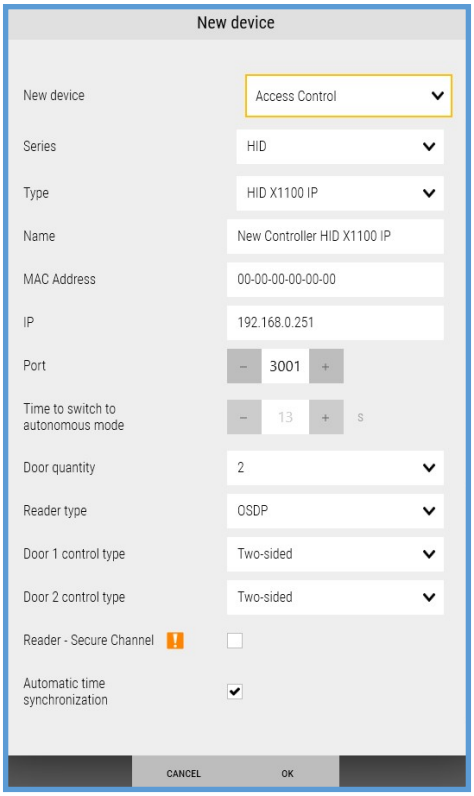
The system can be configured off-line before connecting to the system at the site, but it is much faster to configure the process on-line when we have the devices already installed, connected to the power supply and Ethernet network. We can then use a search engine, which, after searching the network, 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

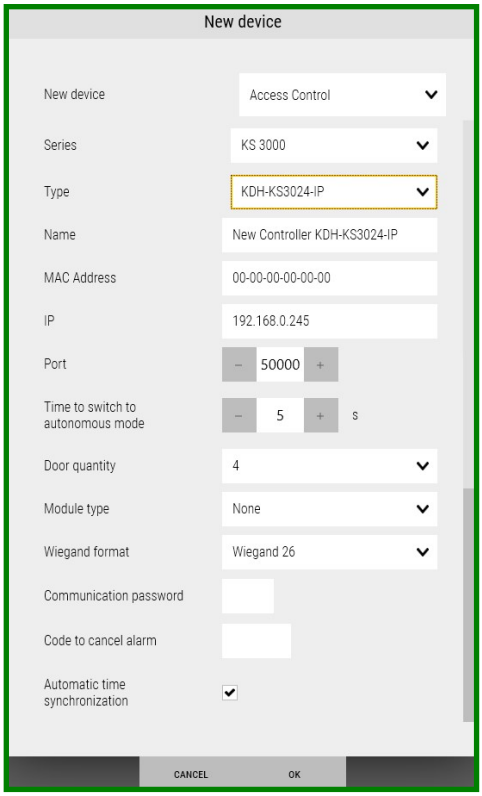
This option allows us to add a new device off-line when we cannot use the search engine. After clicking on this button, a window will appear as on the next page, where we can select the type of device we want to add:



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)

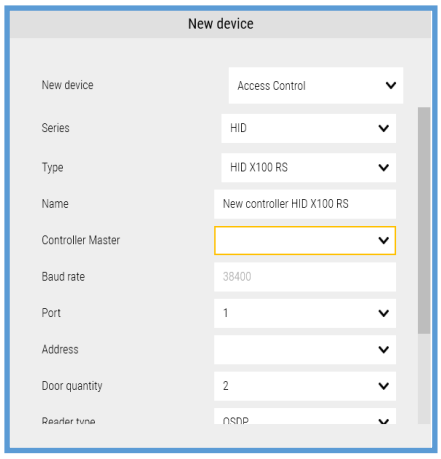
Configuration of the door, only for **HID® Aero® series** - X1100 i X100:

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

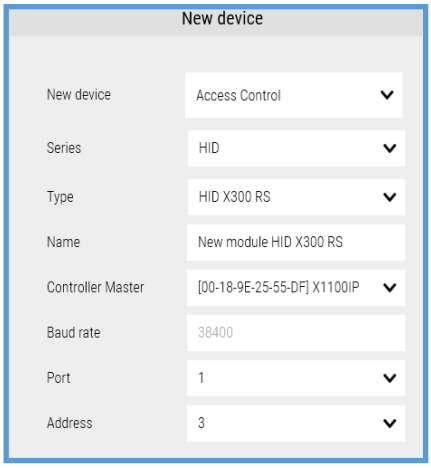
Reader type - OSDP or Wiegand, depending on the method of communication between the controller and the readers.

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

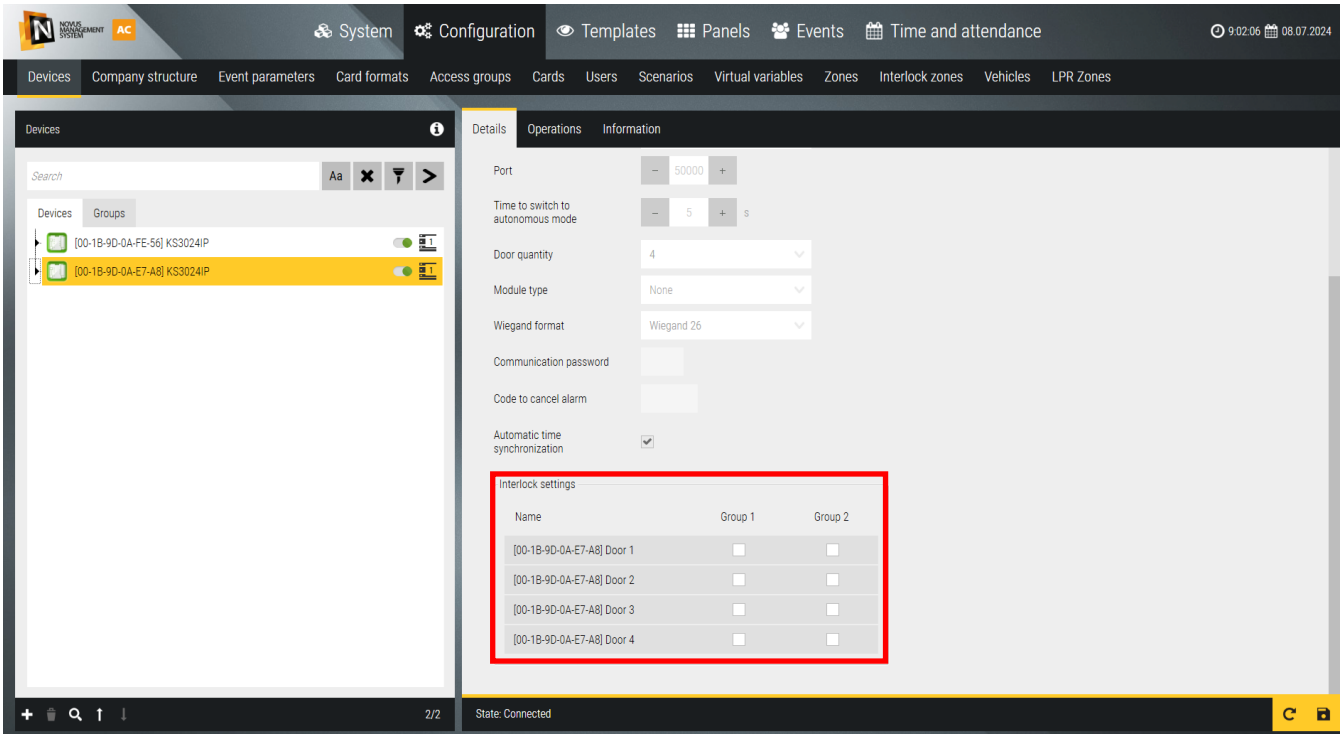
Automatic time synchronization - when this box is checked, the time in the controller will be synchronized from the server every 4 hours

Options for integrated controllers:

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

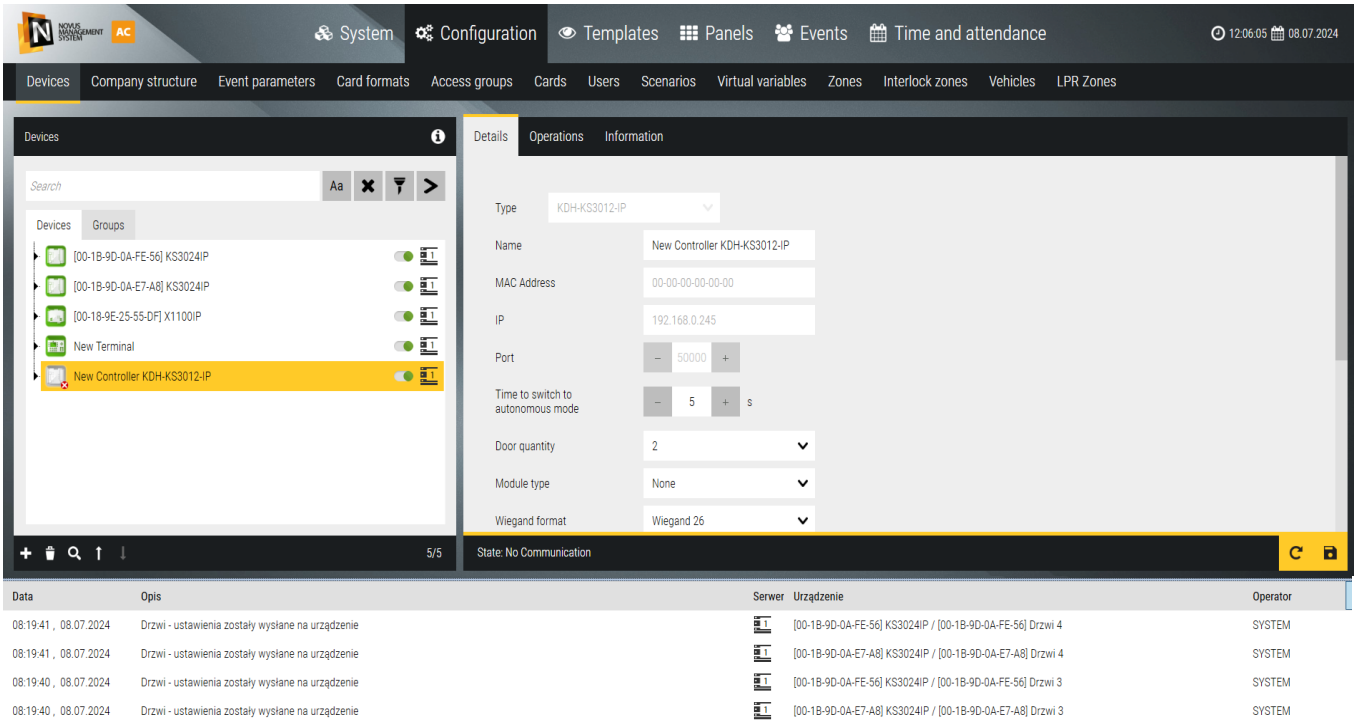
Enabled tamper alarm - activation/deactivation of the tamper alarm (concerns KDH-KZ3000-IP-U and M)

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.



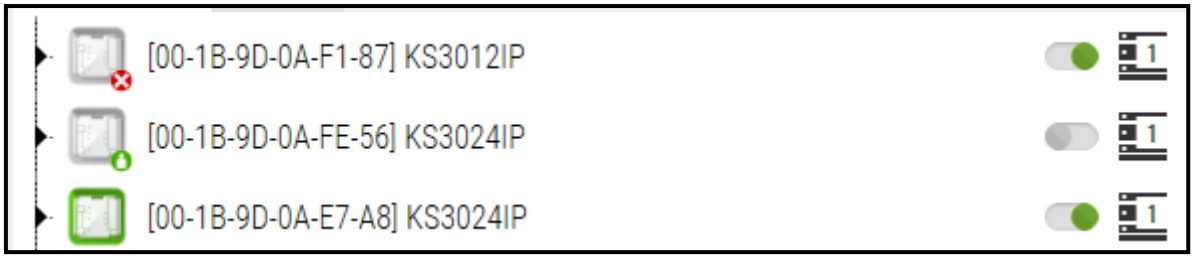
For KDH-KS3012/24-IP controllers, additional fields appear in the lower right window to add the controller's doors and readers to one or two groups. This applies to the lock function (i.e. mutual control of door leaf status) . These fields do not appear for the elevator controller.

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.

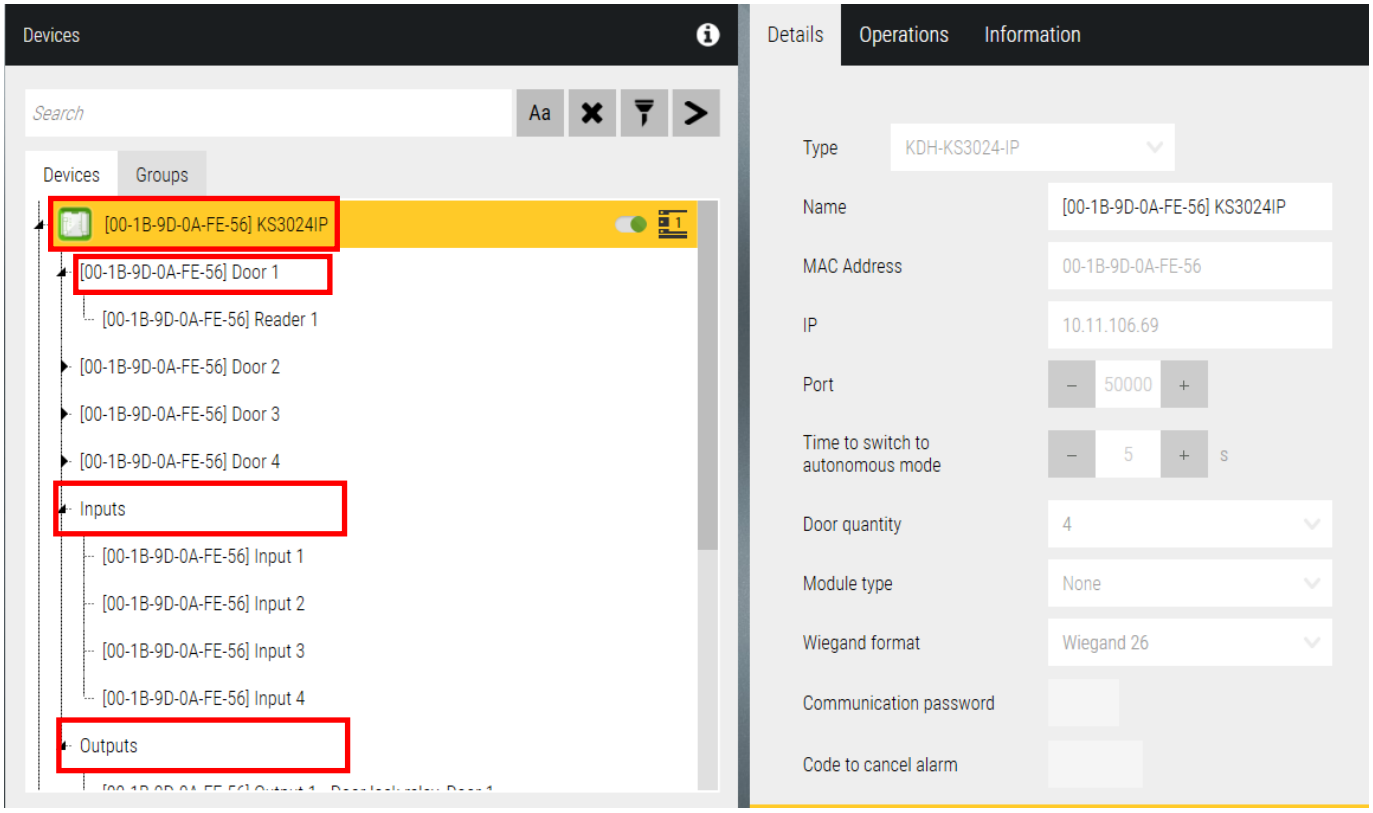


After saving the settings, the icon status can show one of three situations:

- 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



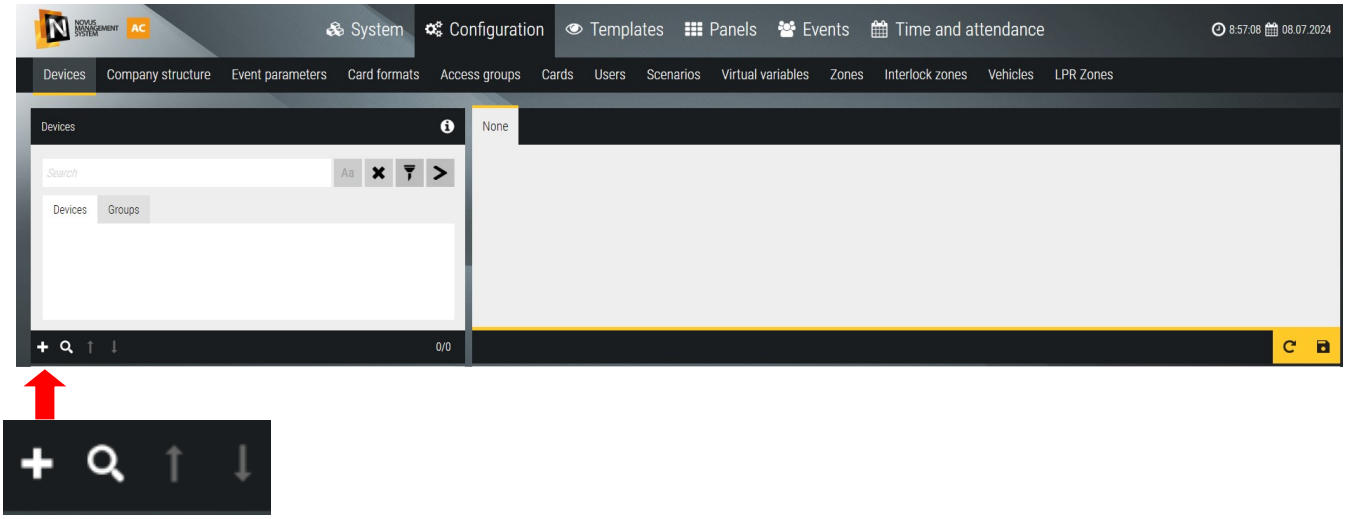
The controller icon can be expanded by clicking on the black triangle on the line of the main tree and display the cooperating elements. By selecting the desired element in the expanded list, we can edit its settings



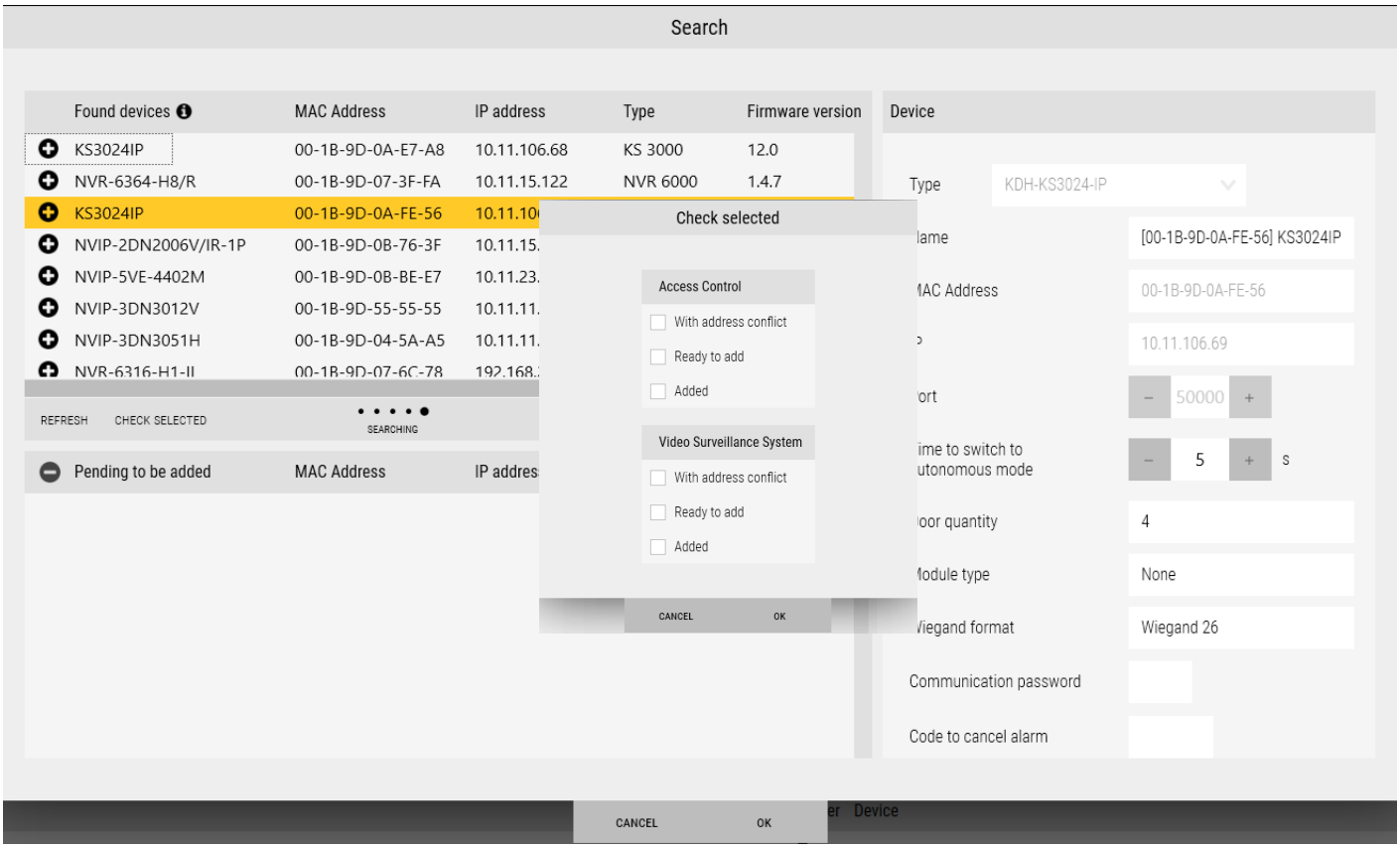
This includes such elements as doors, readers, input lines and control outputs. After selecting a selected element, its settings are displayed in the right window and can be edited. The selected element is highlighted in yellow. After changing the settings, save them by clicking on the floppy disk in 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



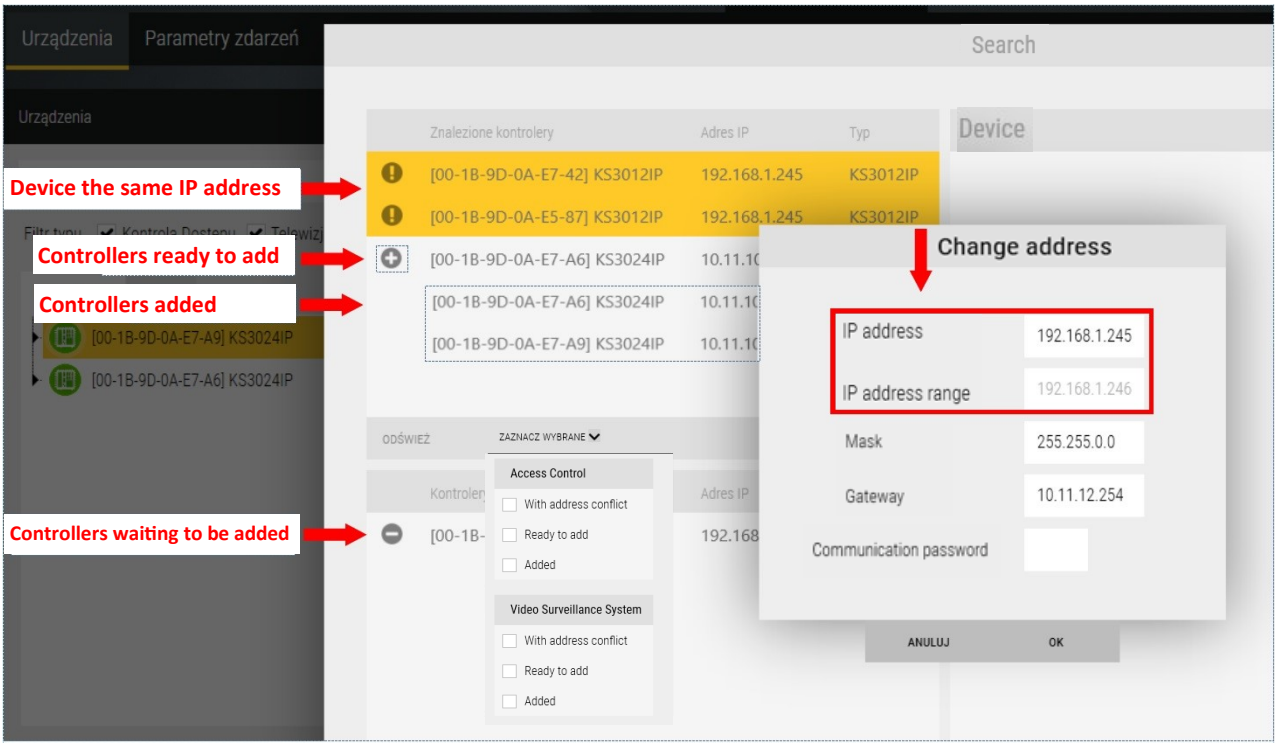
When the controllers have been installed on the site, connected to Ethernet and power, it is recommended to use the search engine available in the program to add them to the system database. This speeds up the process considerably. To start the search engine, click on the Search button at the bottom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



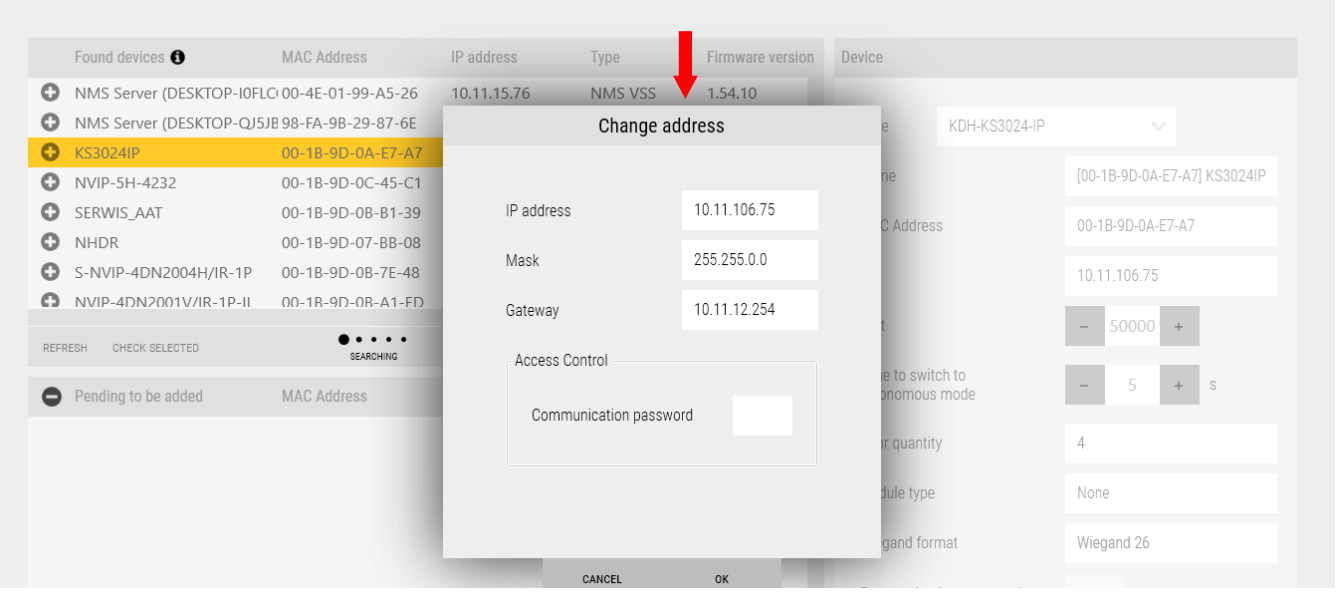
Statuses of searched controllers displayed in top left window:

- - 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.



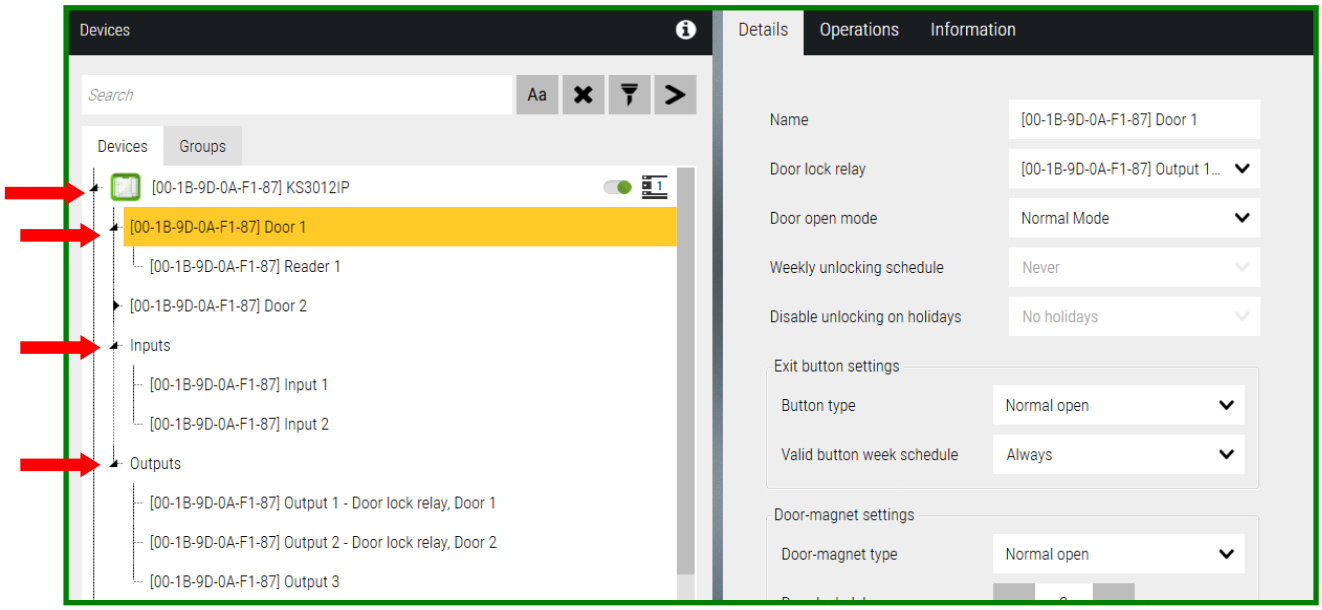
In the drop-down list, we can choose which group of controllers we want to select. In case we want to change the address of one retrieved controller, we select it in the list in the upper window and click on the *Change Address* button.



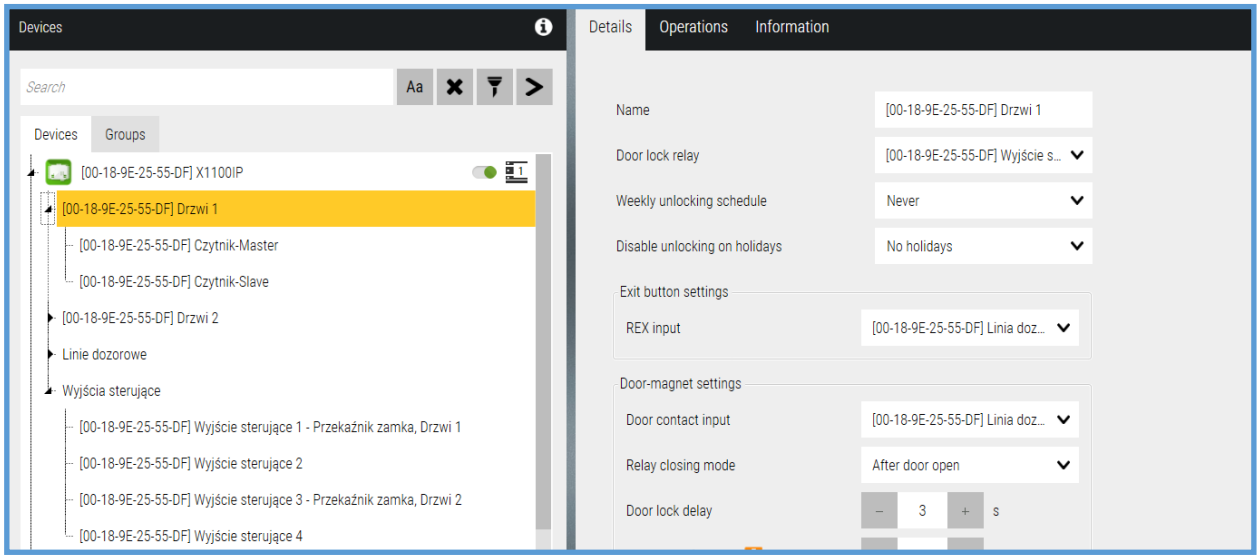
After setting the addresses and adding all controllers to the list in the bottom window, click on the OK button. The added controllers will appear in the *Devices* window.

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



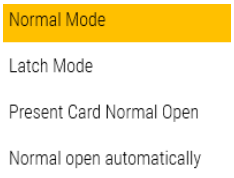
HID® series

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.

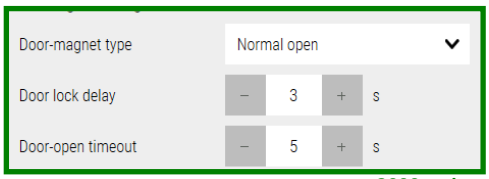
Door-magnet settings

3000 series:

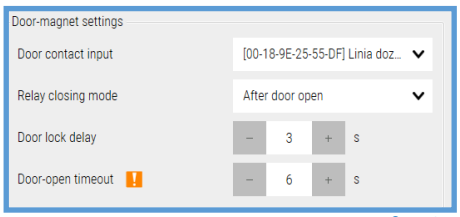
Door-magnet tpe - NO or NC type can be selected from the drop-down list

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.

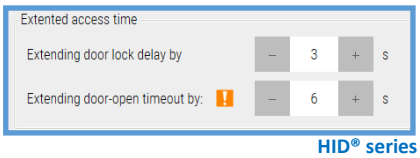
Door-open timeout - editable field for entering the time (s) for closing the door leaf. After the expiration of the time, which is the sum of the times for closing and unlocking, a Door Held alarm will be generated - default is 8 sec. (3+5). The time can also be set by clicking on the - or + buttons.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

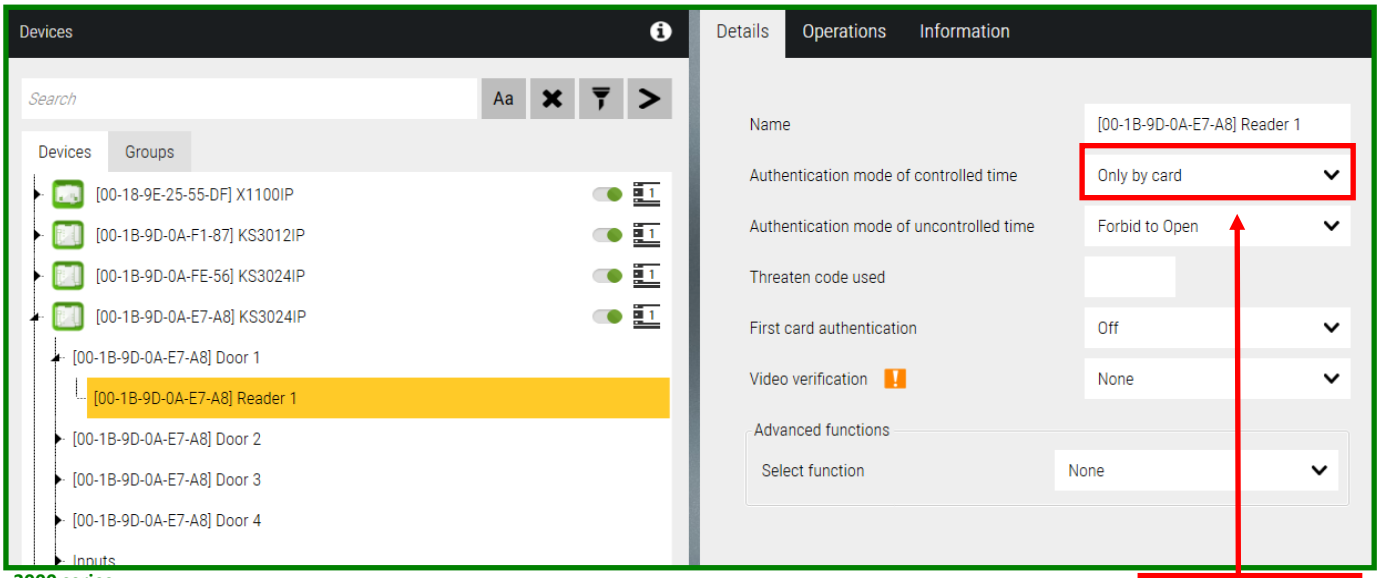
Door open timeout - editable field for entering the time (s) for closing the door leaf. After the expiration of the time, which is the sum of the times for closing and unlocking, an alarm Door Held , configurable only in the range of even numbers from 2 (s) to 512 (s), will be generated.

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

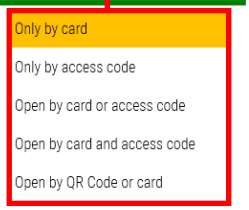
Extending door lock delay by - extends the unlocking time of the lock by the set time in seconds

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).

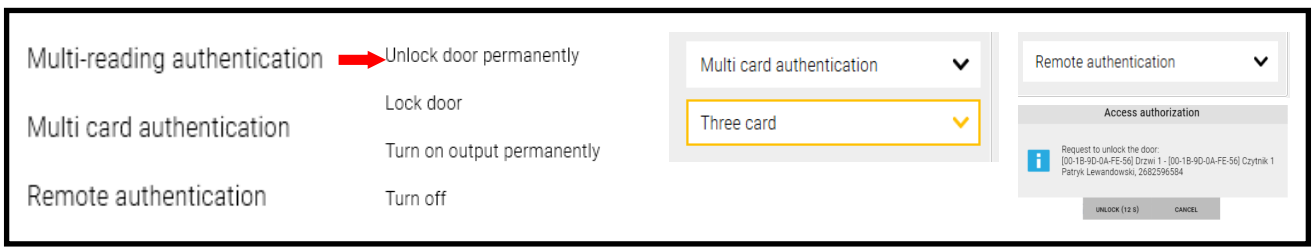
Video verification - allows you to assign a camera installed above (or built-in) the reader to record a freeze frame when the card is read. The freeze frame is attached to the event in the stack and in a report on the screen.

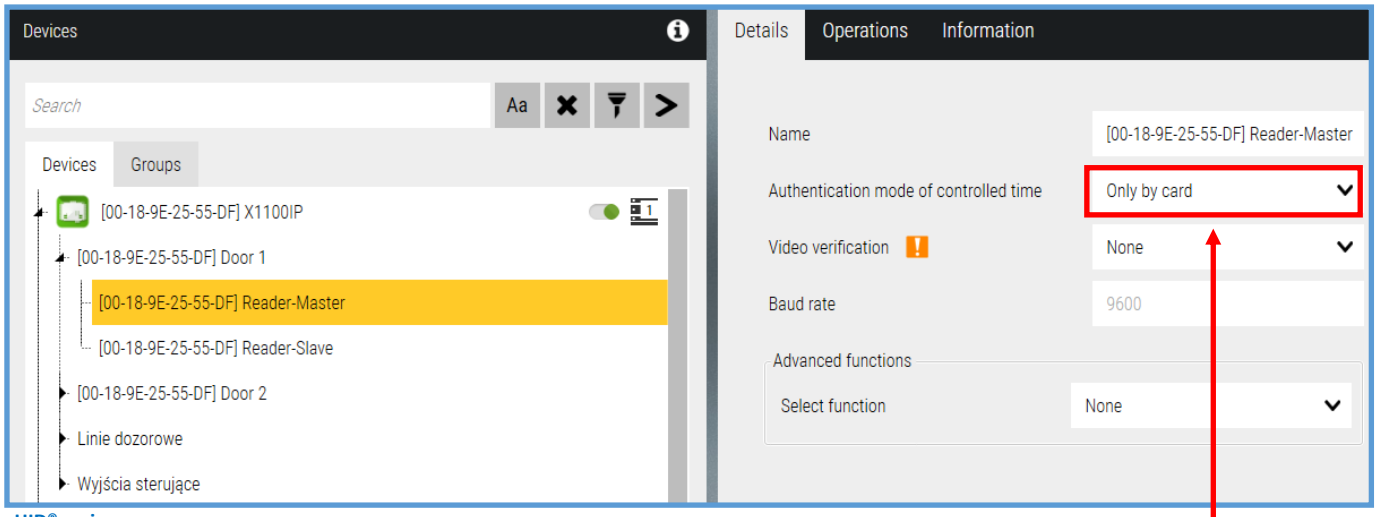
Advanced functions: - selection as in the window below:

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.

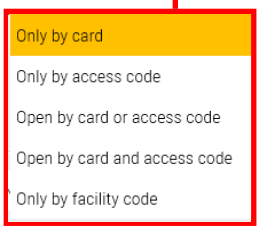
Multi card authentication - gaining access requires the use of one to four valid cards consecutively. Special option for rooms requiring greater security.

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:

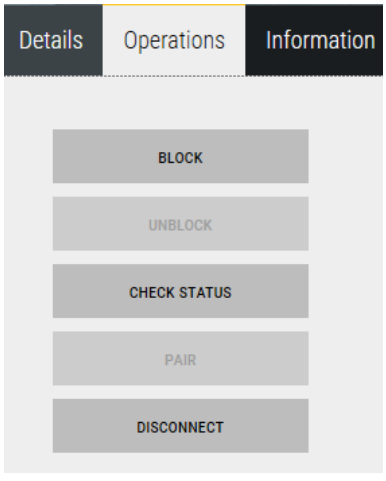
Reader-Master - Reader connected via OSDP protocol with address set to 0
Reader-Slave - Reader connected via OSDP protocol with address set to 1
Name - an editable field for entering the reader's name in place of the default name.
Authentication mode of controlled time - from the drop-down list, you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

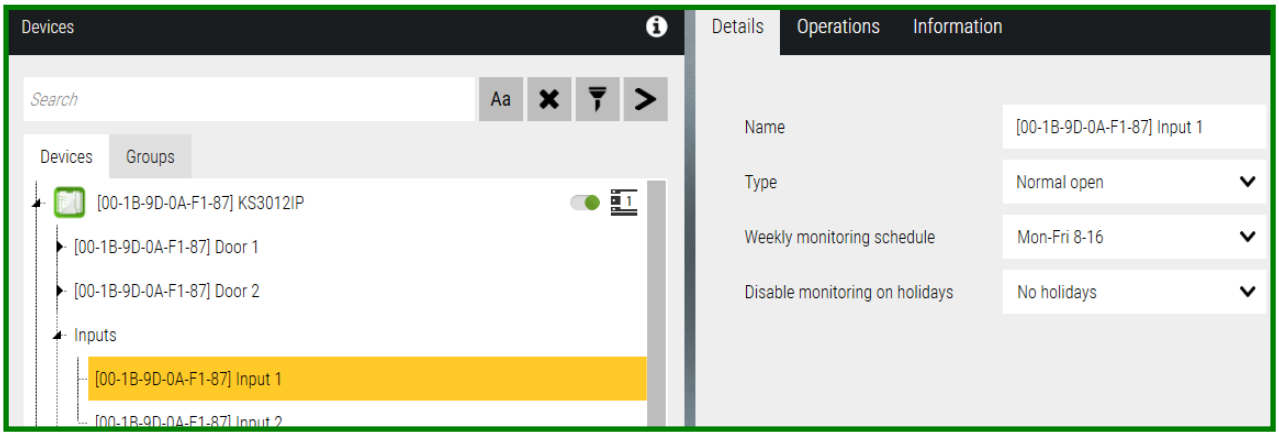
Block/ Unblock reader - allows locking/unlocking of the reader by the operator

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.

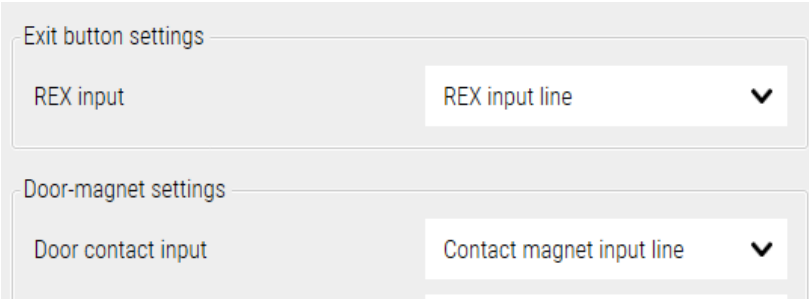
Type - NO or NC type can be selected from the drop-down list - NC is recommended.

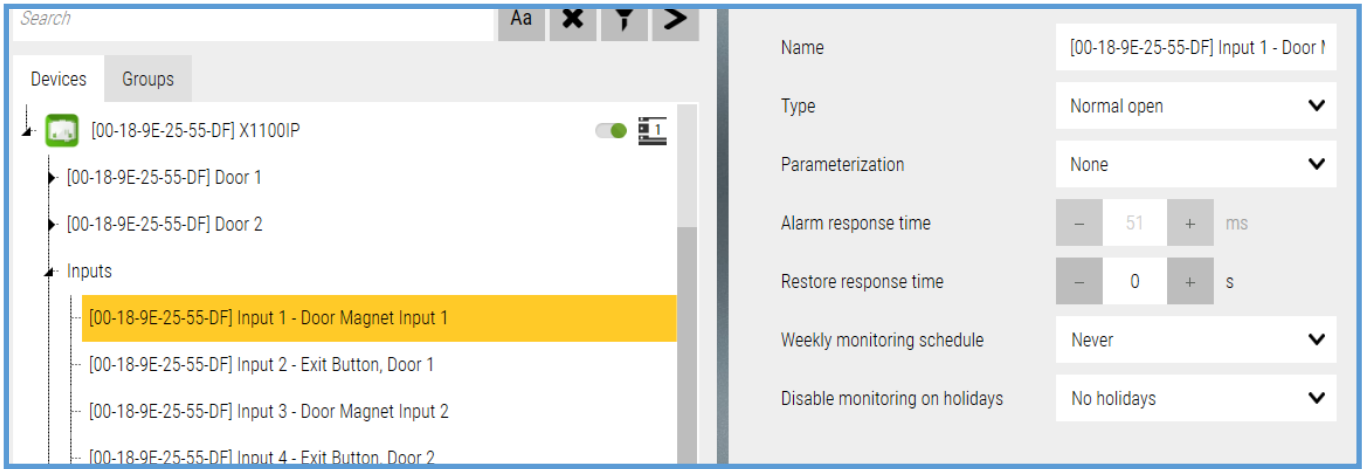
Weekly monitoring shedule - from the drop-down list, you can select a predefined schedule according to which the line will be monitored and then alarms will be generated.

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

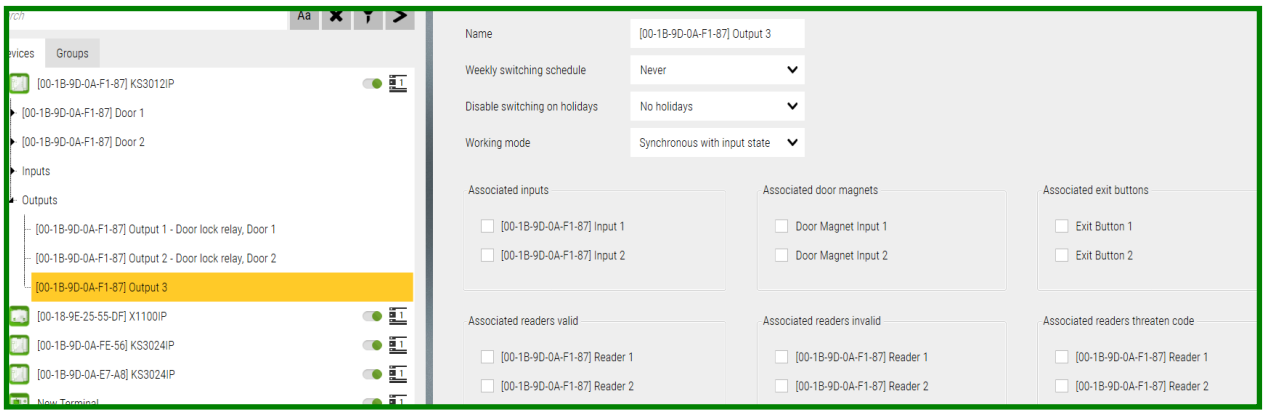
- normal state

Alarm

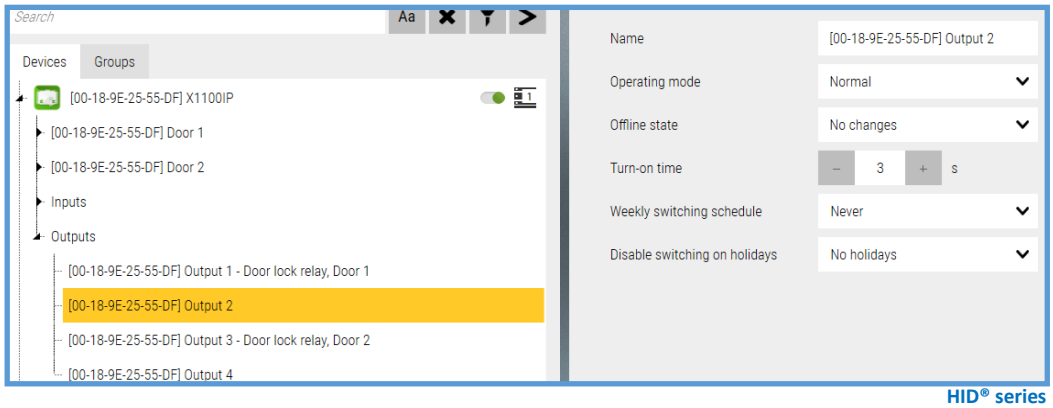
Fault/short circuit

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.

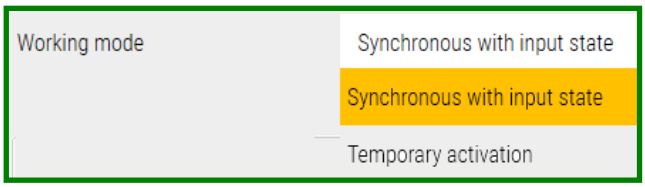
Weekly switching shedule - From the drop-down list, you can select a predefined schedule according to which the output will be automatically switched.

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

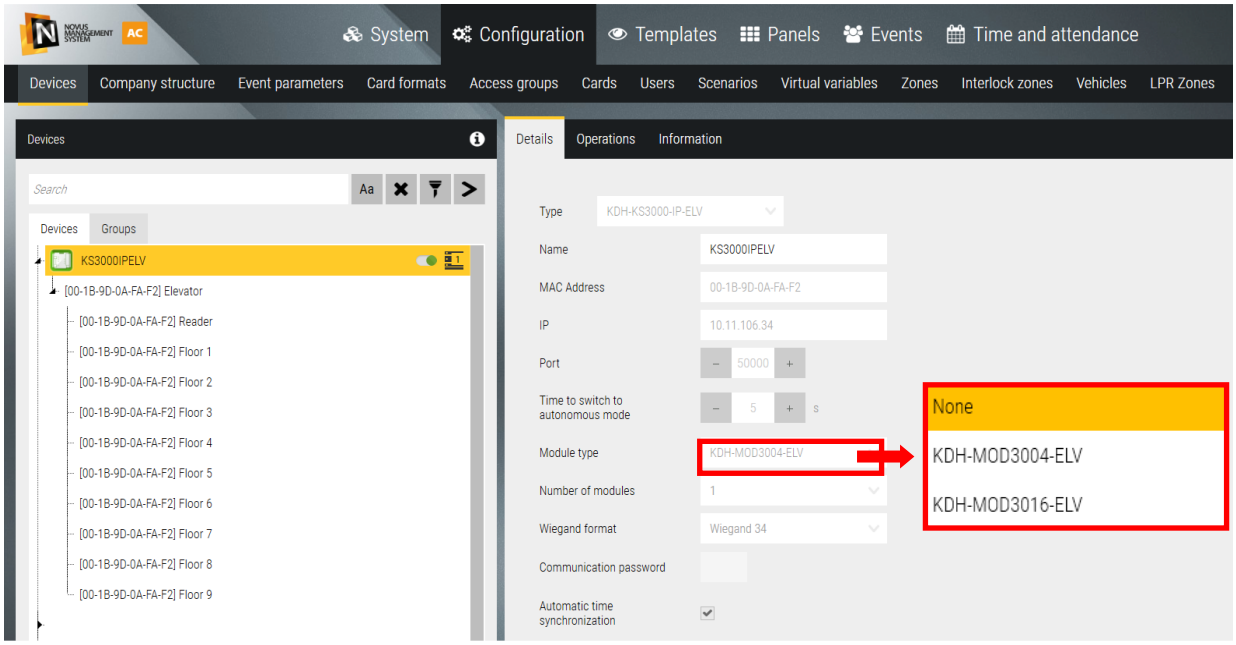
Offline state - For **HID® series** controllers only, status after the controller goes offline, selectable:

- No change
- Inactive
- Active

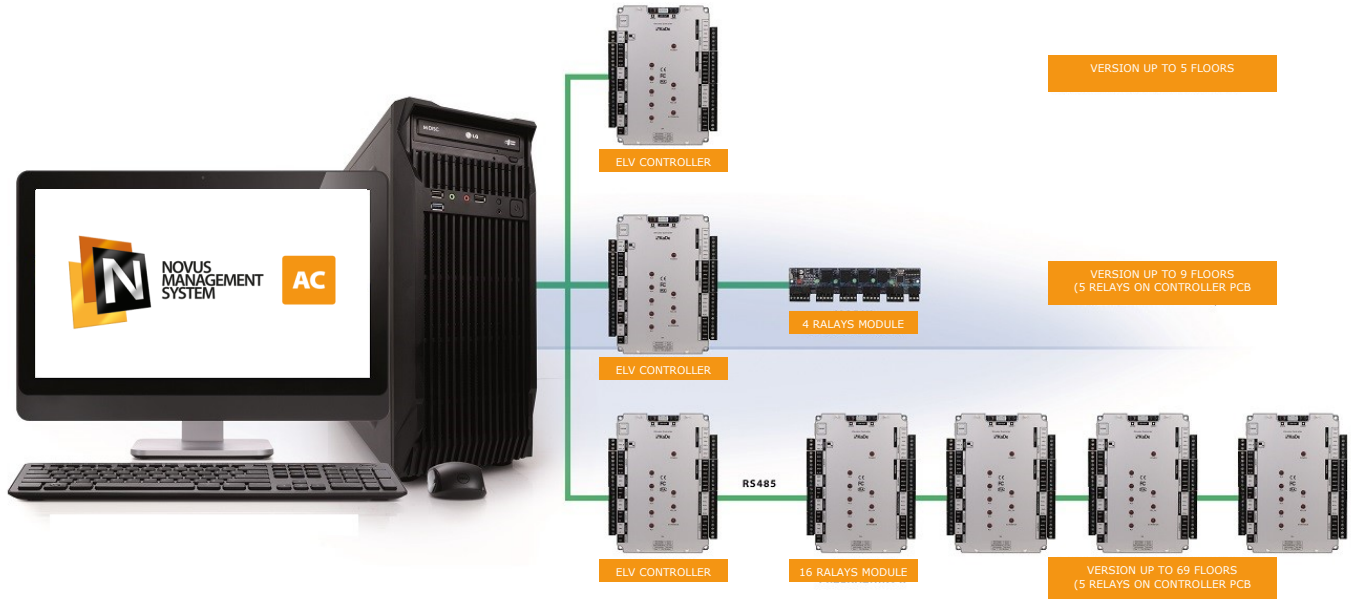
Turn-on time - switches to the time set in the field below

HID® series

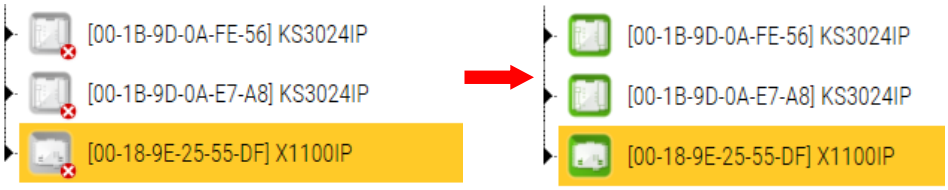
3.6 Devices - Access control - Elevator controller



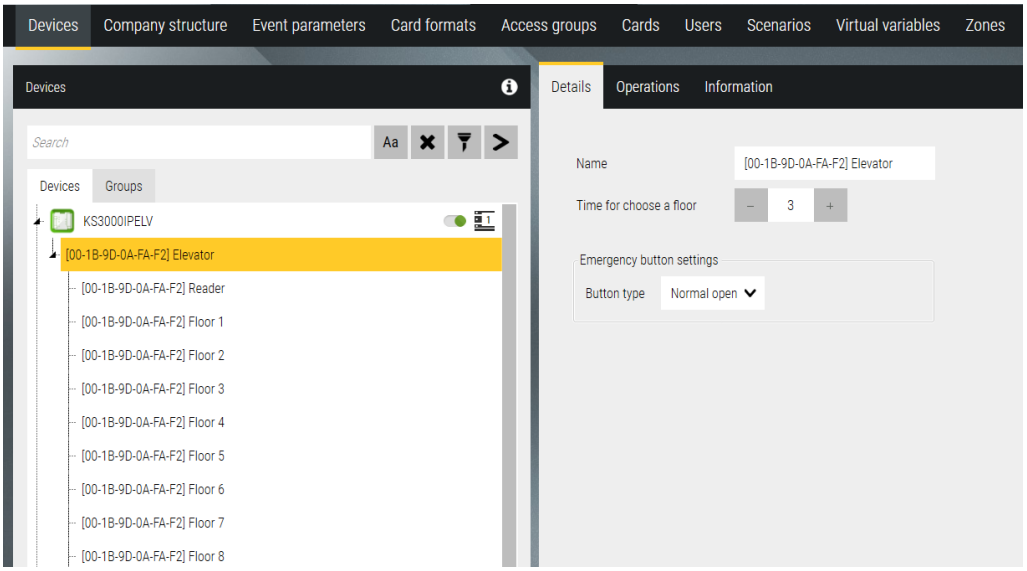
With the KDH-KS3000-IP-ELV controller, you can also add expansion modules. There are two types of modules to choose from. Depending on the number of floors to be served by the elevator, we have the following combinations.



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:



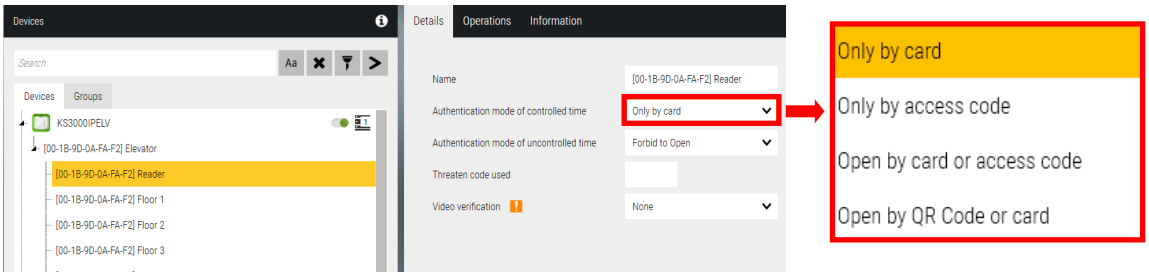
3.7 Devices - Access control - Elevator controller - Elevator



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

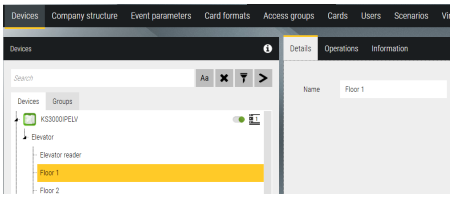
3.8 Devices - Access control - Elevator controller - Elevator—Reader



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

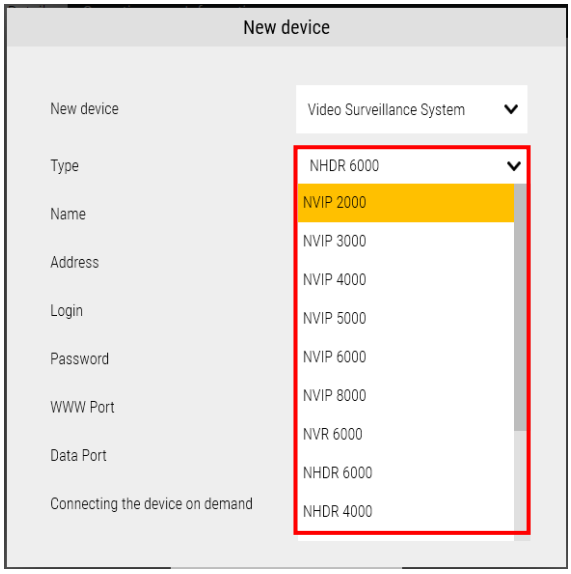


3.10 Devices - Video Surveillance System

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.

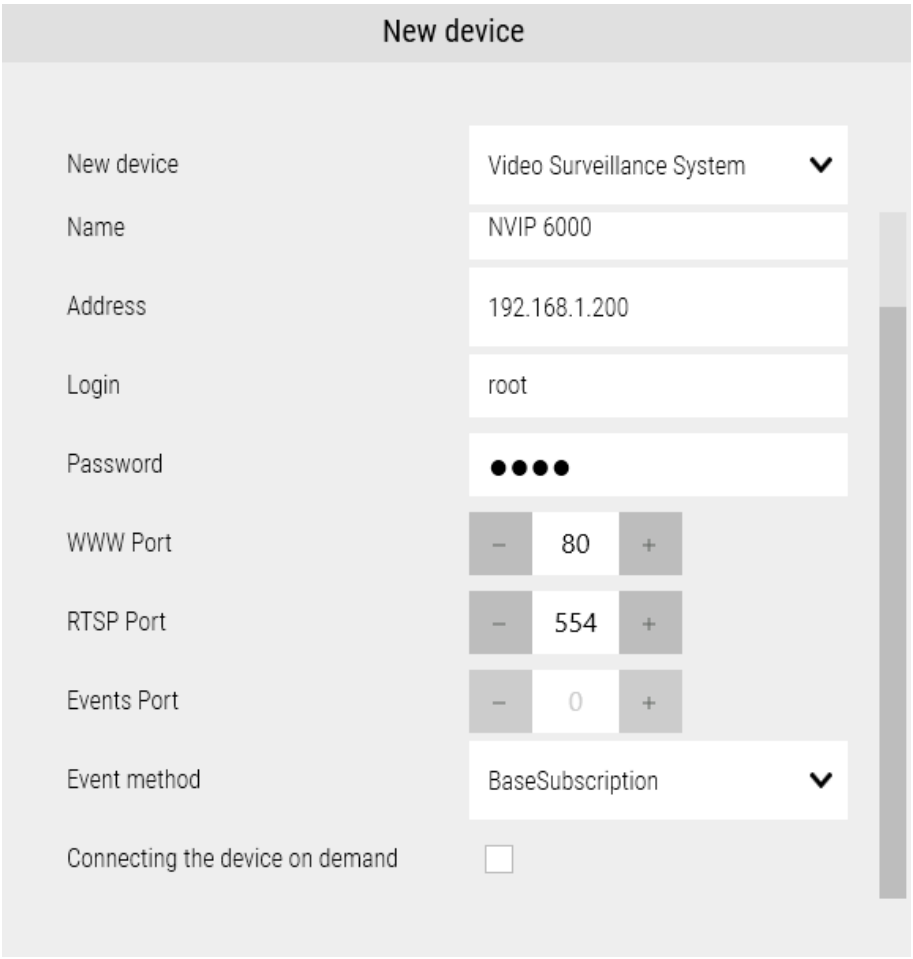
Name - editable field to type the name of the video device in place of the default name if you want. This field will be filled automatically when camera is connected.

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



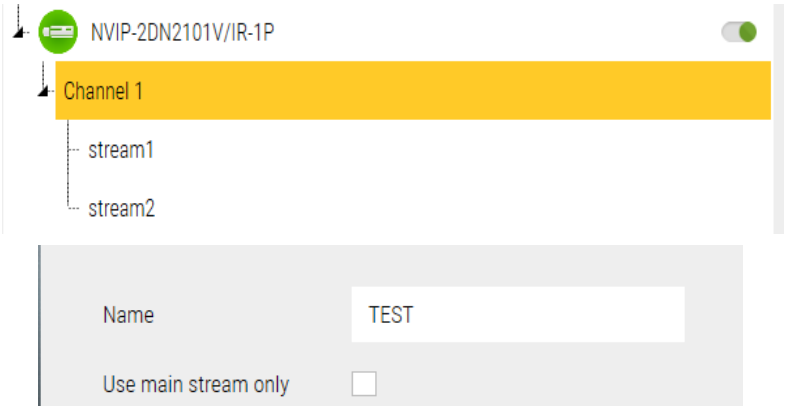
User - editable field to type a user name that matches the settings of the video device.

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:

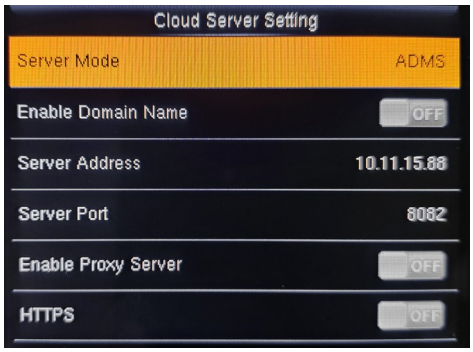
Time and Attendance terminal configuration

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.

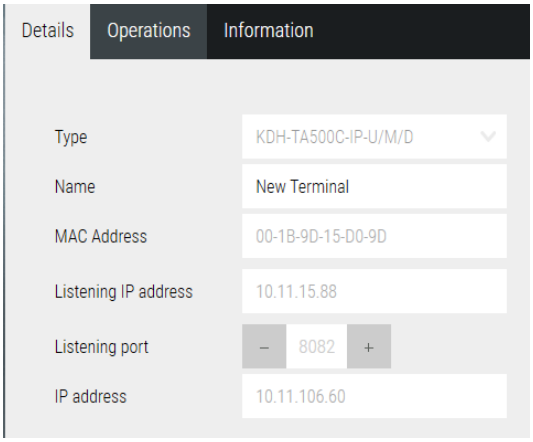
Terminal IP address settings

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*).

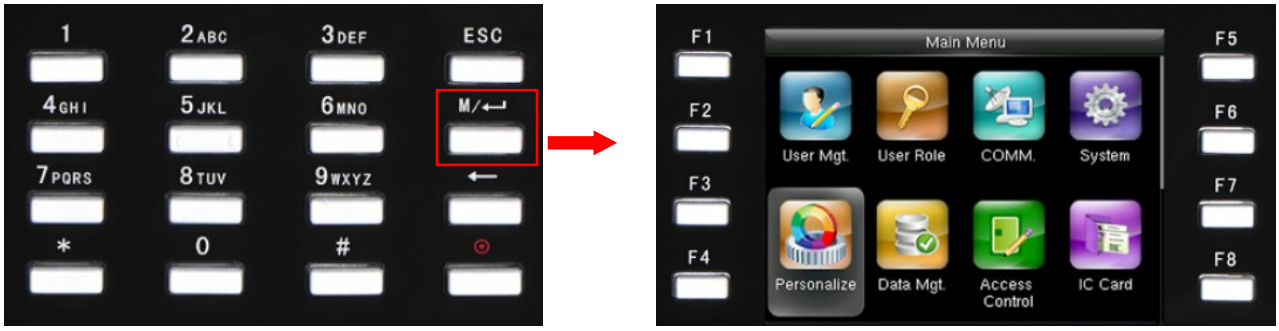


If you are upgrading from version **5.00.035** to version **5.00.071,** after completing the configuration process, perform an initialization operation on the terminal (in the Configuration - > Devices , select the terminal from the list and then the **Initialization** option from the Operations menu). 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.

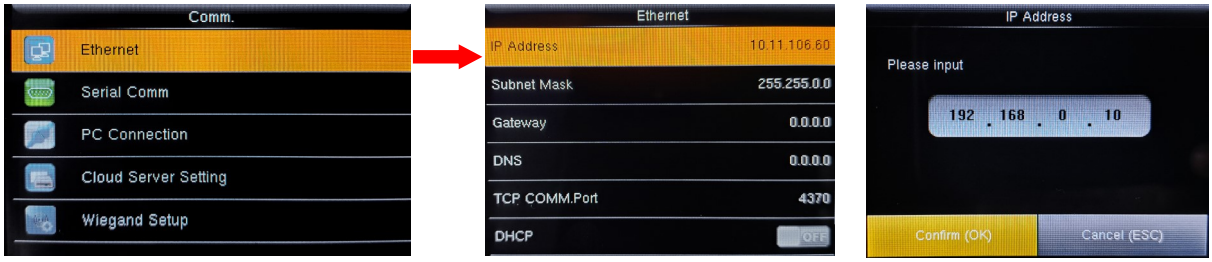
NOVUS MANAGEMENT SYSTEM AC program allows integration with time and attendance registration system. From version 4.02.XX and higher, these functions can be realized in cooperation with T&A terminals of KDH-TA500C-IP-UMD and KDH-TA500CFP-IP-UMD types, which offer registration of different types of I/O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

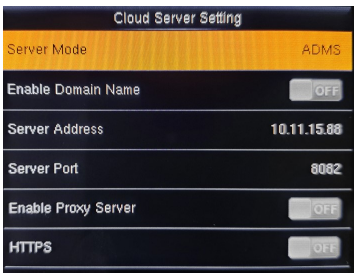
Selection of items with cursors. (upper right corner of the terminal)



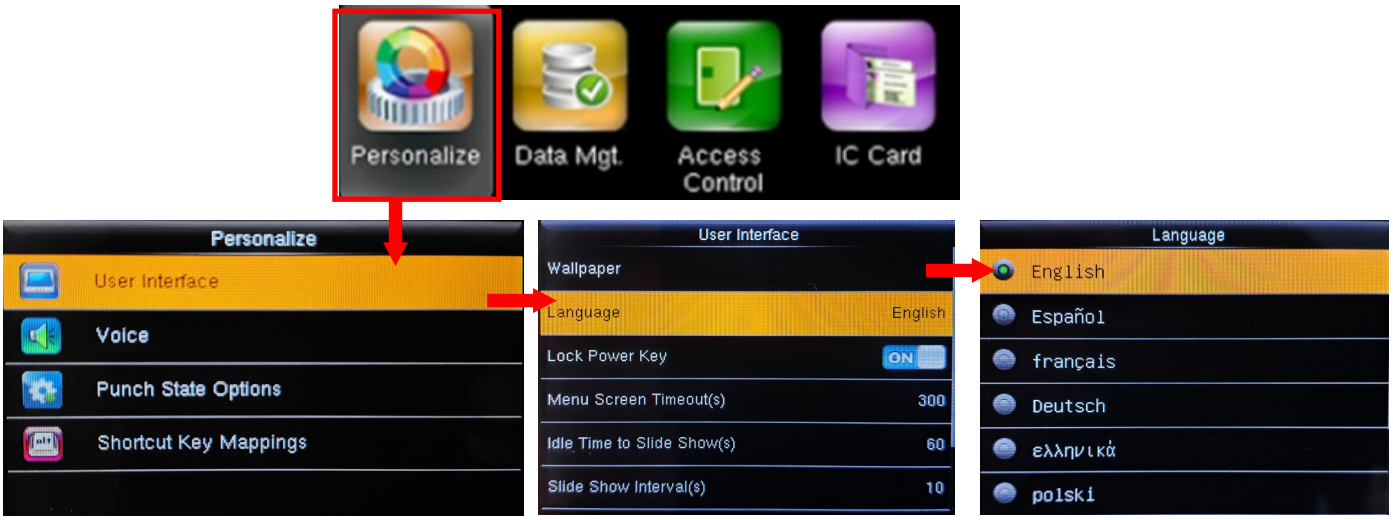
After clicking on the *Comm* icon, select *the Ethernet* item and click OK in the cursor field - upper right corner of the terminal. Fill in the first 4 fields - After selecting the field, click OK and enter the address-port values without changes. If you are using DHCP network, just select the last 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

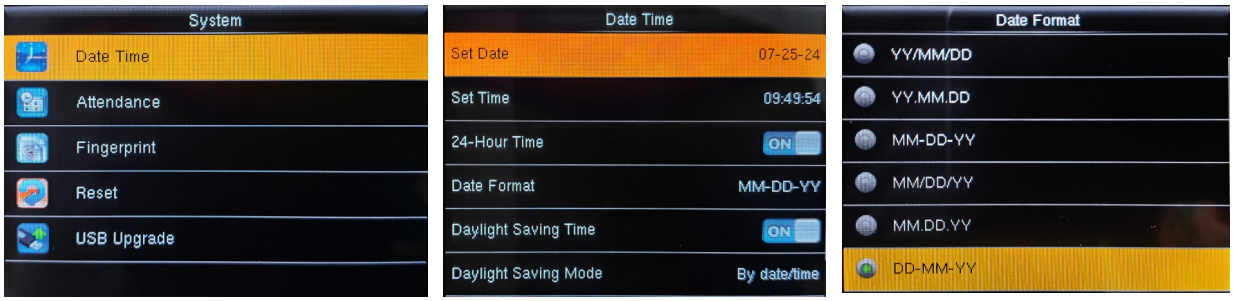


Choice of language



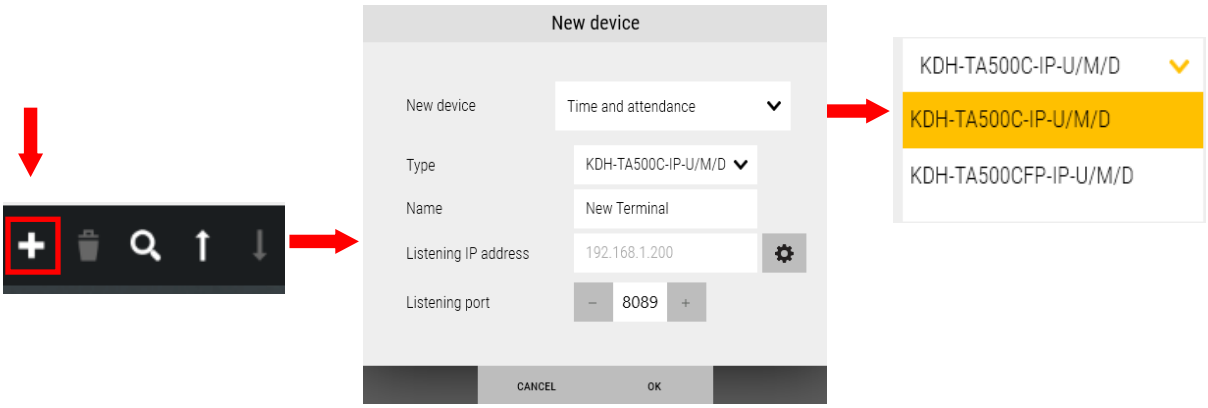
After clicking on the Personalization icon, select the User Interface item and in the next window Language.
Set the Polish language and exit the menu with the ESC button.

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:

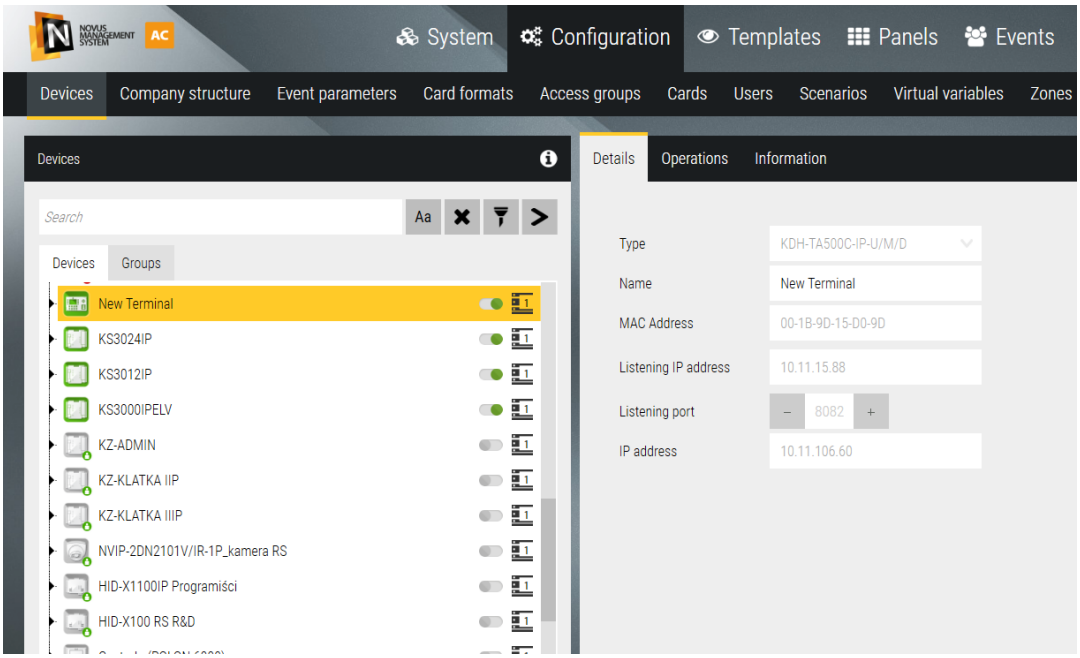
Model: **KDH-TA500C-IP-UMD** or **KDH-TA500CFP-IP-UMD** with biometrics scanner.

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.

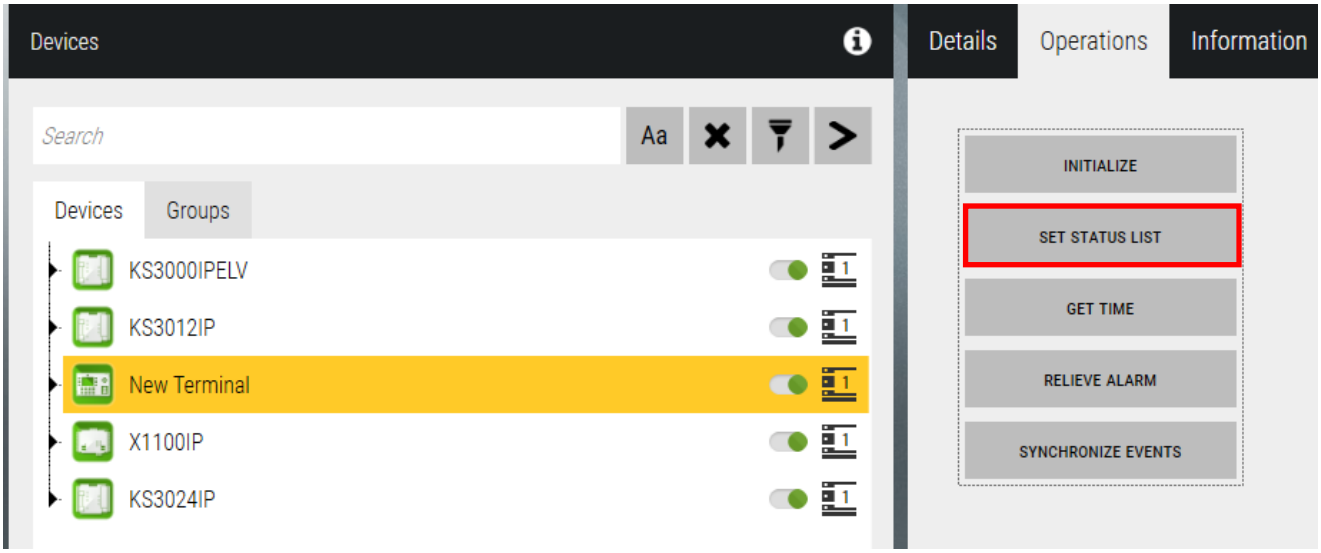


From this point on, entering the terminal menu requires the admin password. Default login: type admin ID - 1 and OK, Verify **password: 1 2 3 4 5 6 7 8** and Ok.

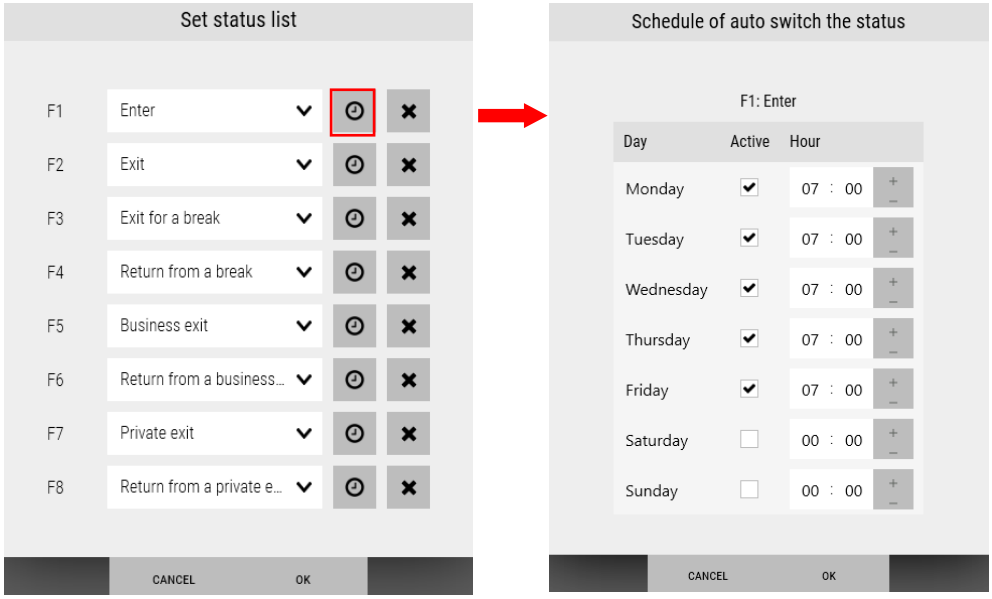
The default password must be changed after logging in the menu Manage user. By editing the Admin user.

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

Set enter/exit registration statuses



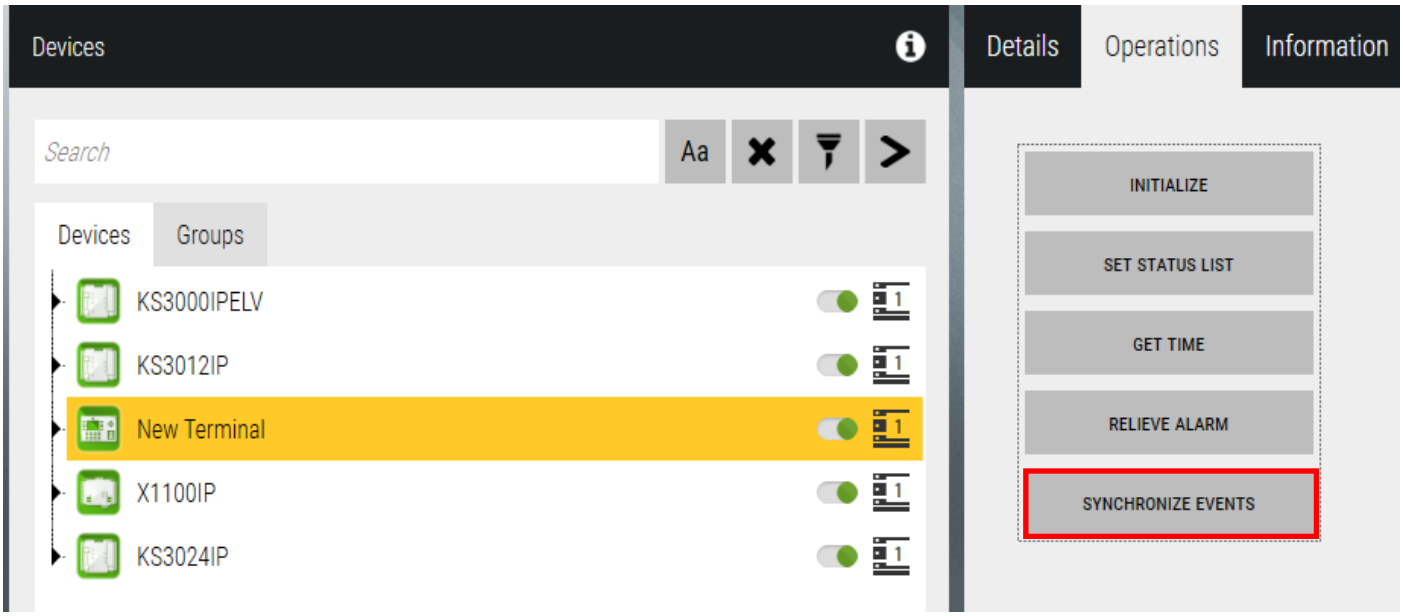
On the Operations tab, click on the Set Status List button. You can leave the default settings or set your own order by selecting a status from the drop-down list next to each button.
By clicking on the clock icon next to each button, you can set a schedule to automatically switch registration status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

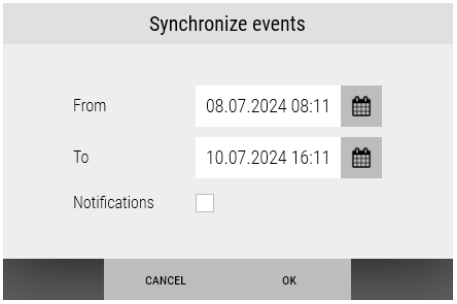


After completing the settings, confirm OK, and then click the Save button in the lower right corner of the configuration window. This will upload the correct registration status descriptions. This process can take up to several minutes. During this process, a description will appear on the terminal display 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.

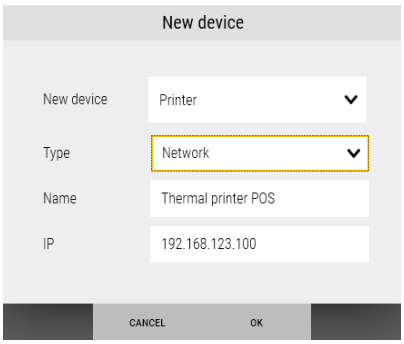




After clicking on the Synchronize Events button, the following window will be displayed:
Choose the date and time range from which you want to download events. Optionally, you can enable email notifications, but if there are a lot of undownloaded events, it is better not to use it in order not to fill 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.*

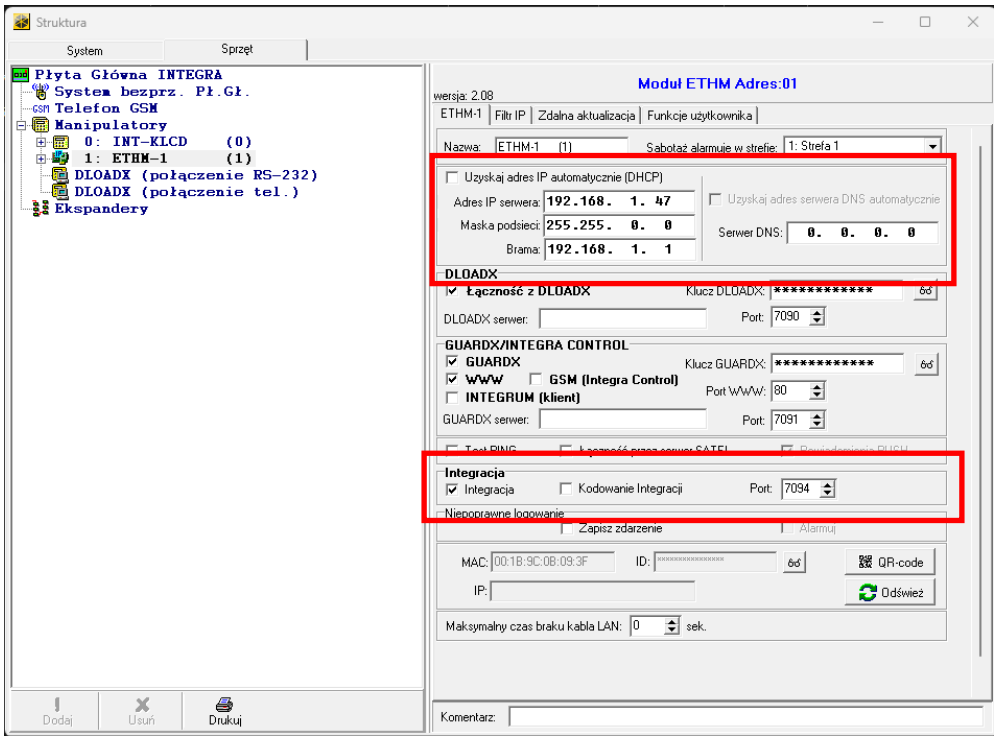


3.13 Devices — Intrusion and Hold-Up alarm system (I&HAS)

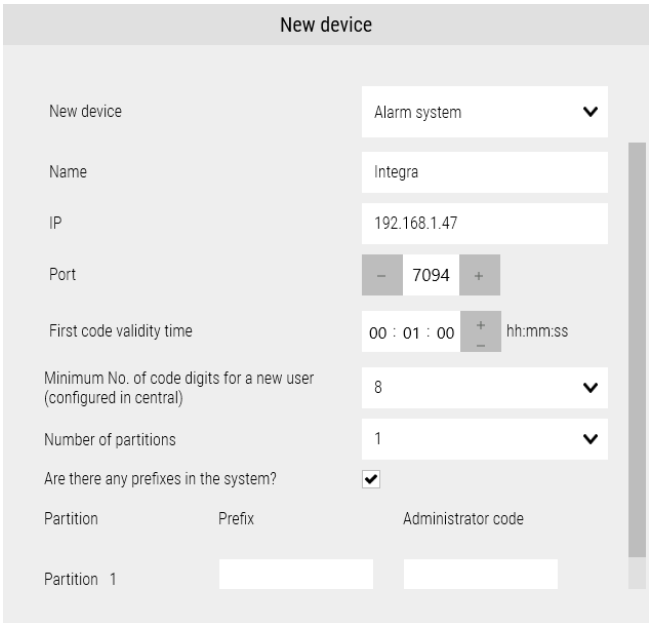
NOVUS MANAGEMENT SYSTEM AC program in version 5 or higher, enables in addition to access control, video surveillance and time attendance systems integration with intrusion and hold-up alarm system.

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.

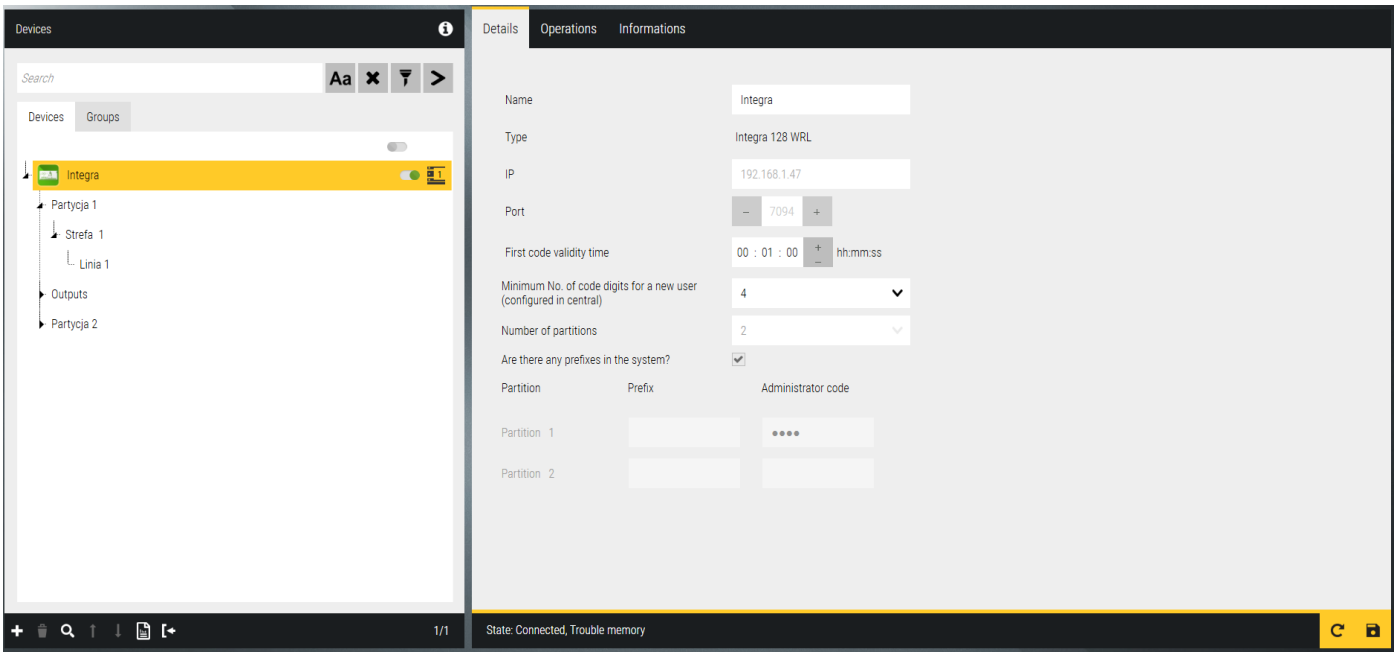
Minimum code length for a new user— minimum number of user code digits programmed in the panel.

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.

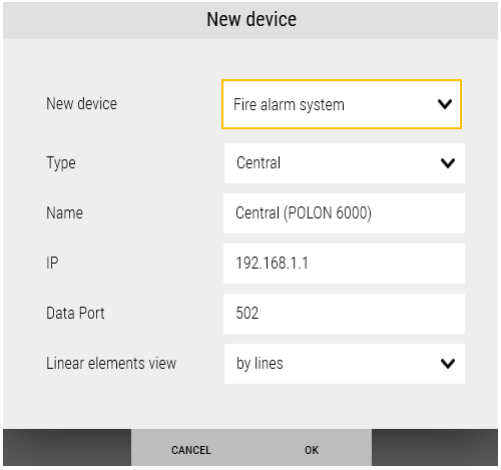


3.14 Devices - POLON 6000 Fire alarm system

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.

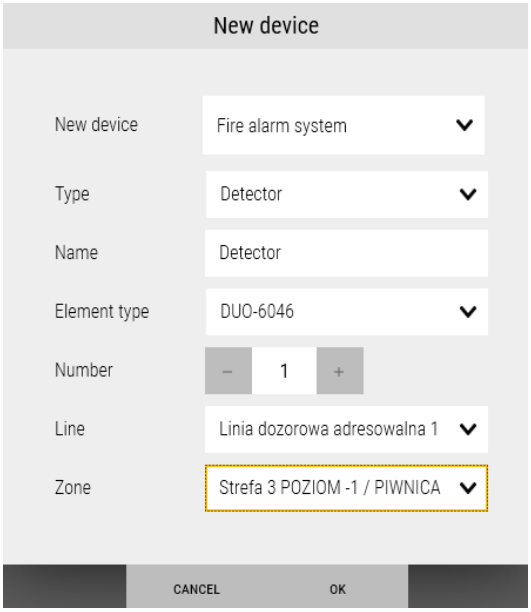
Note: To establish a connection with the Polon 6000 main panel, it must be properly configured. The description of the main panel configuration can be found in chapter 9.10 of this user manual.

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

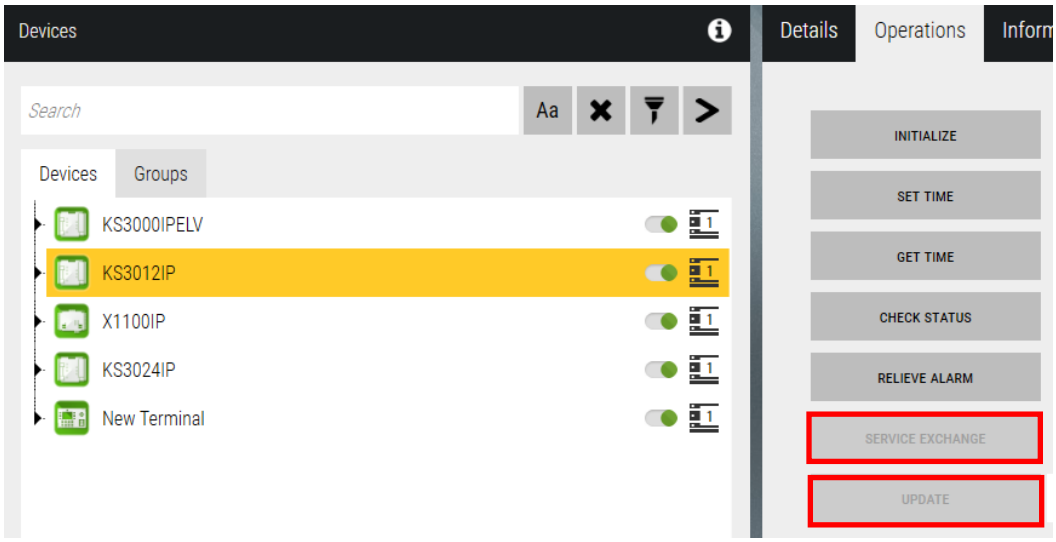
B) Loading the configuration exported from the main panel

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

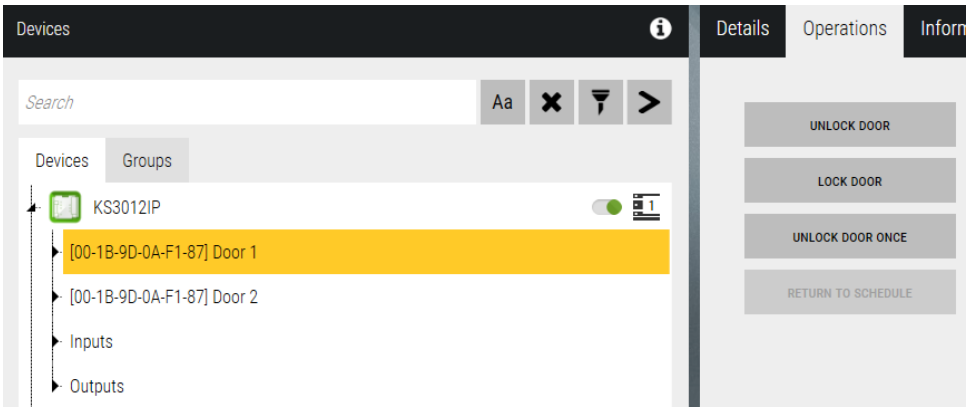


New buttons:

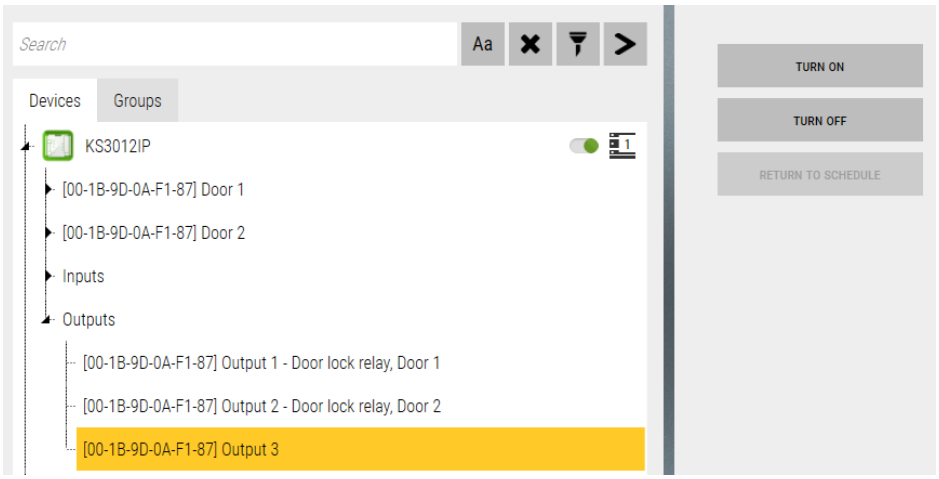
SERVICE EXCHANGE - allows you to replace the controller with a new one, which should be connected with the same IP address

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

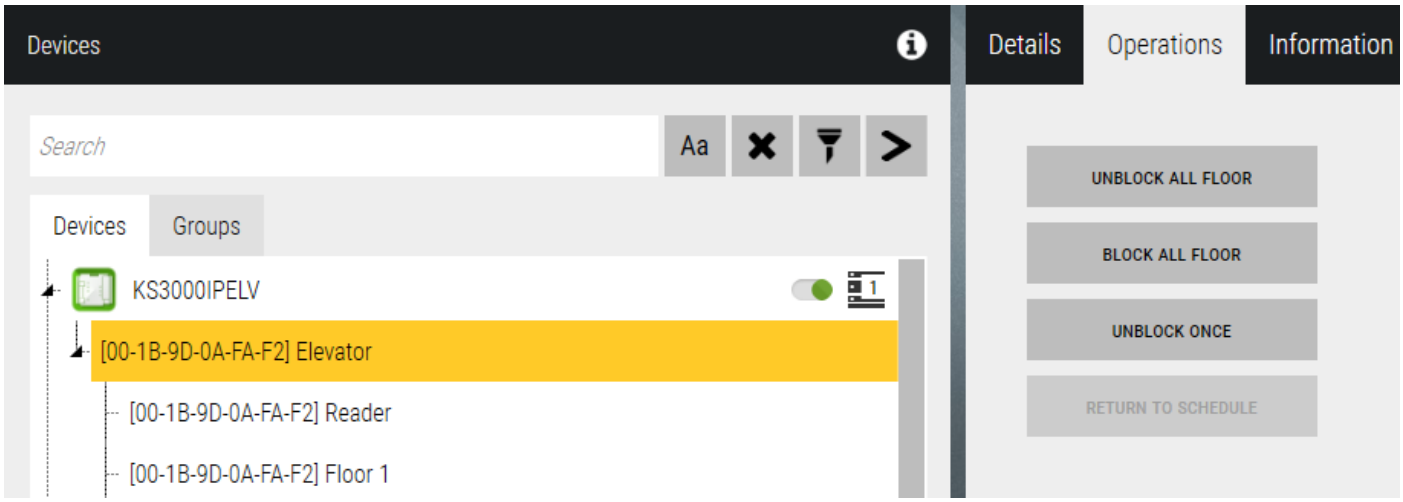
Door



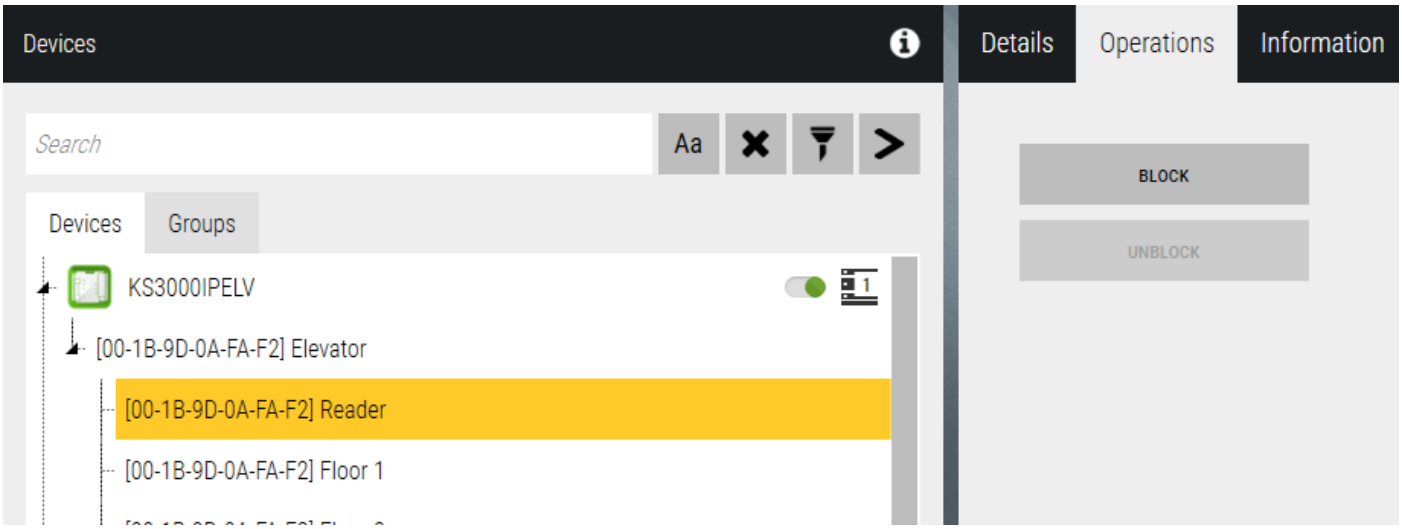
Outputs (only not assigned to the lock)



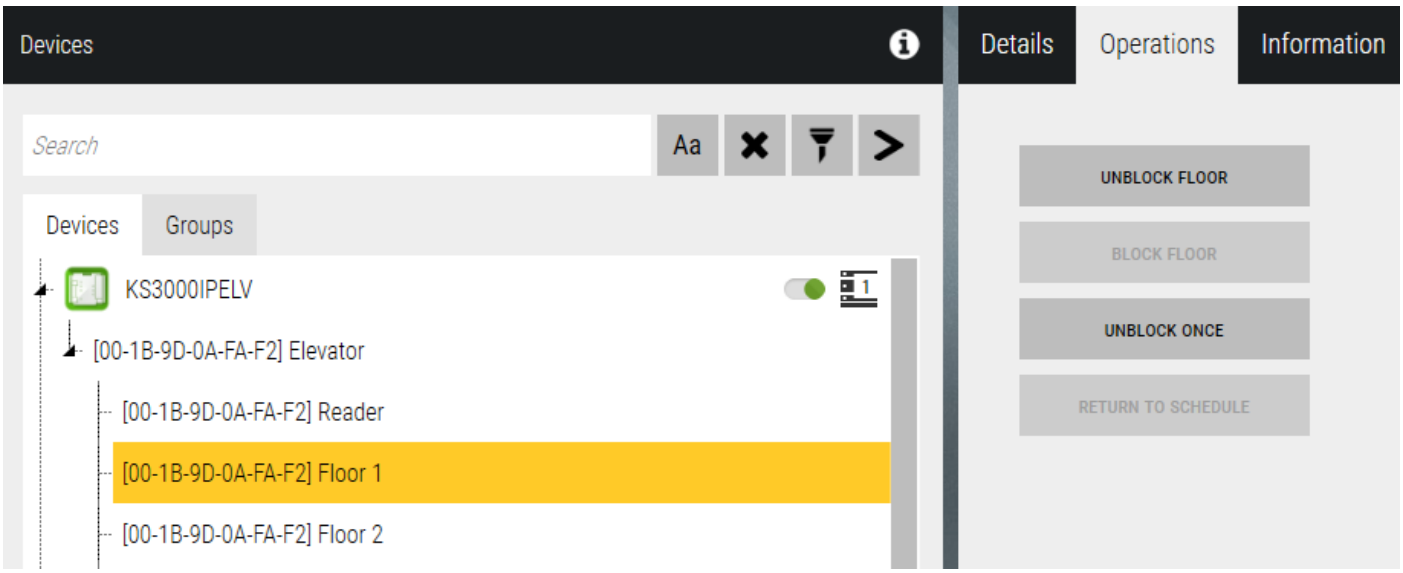
Elevator



Reader

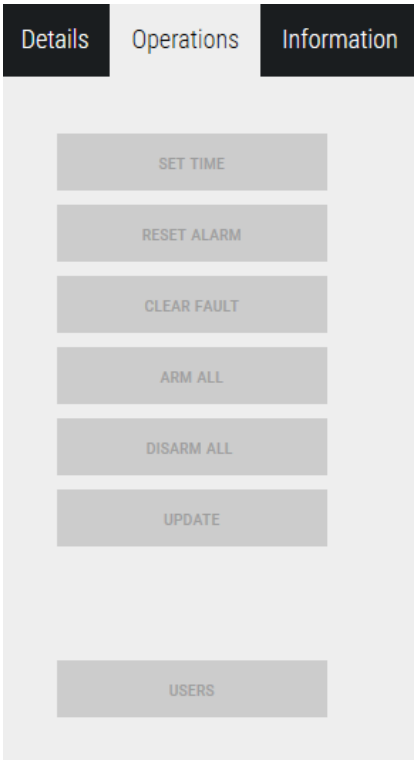


Floor



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.

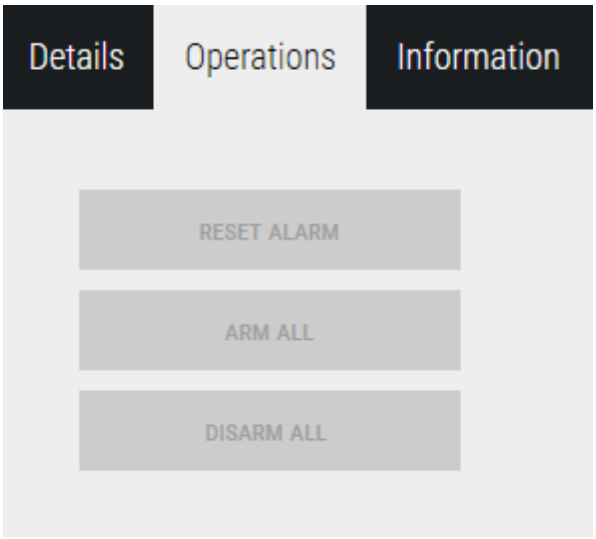
Arm all — button allows you to arm all disarmed objects and partitions in the system with status allow arming.

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

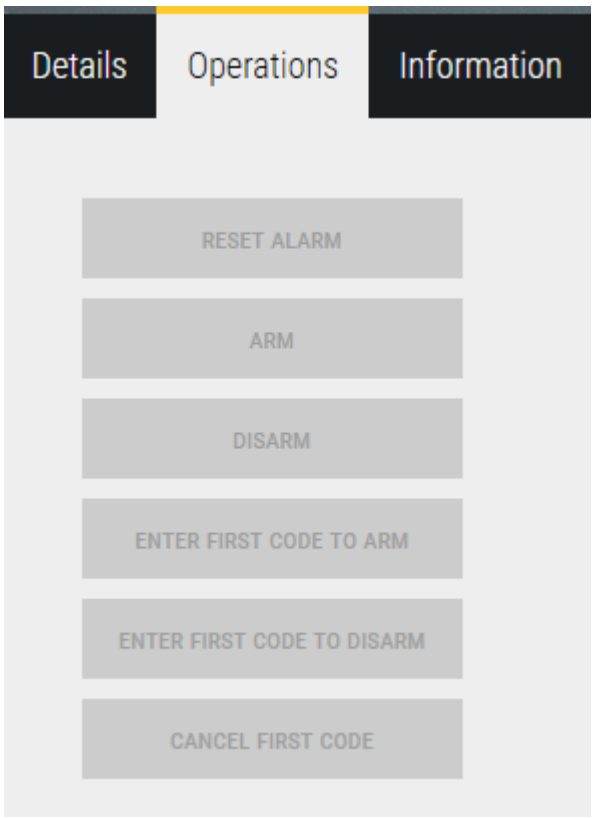


Reset alarm — if an alarm occurred on the object and it is saved in the alarm memory, this button clears the alarm memory.

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.

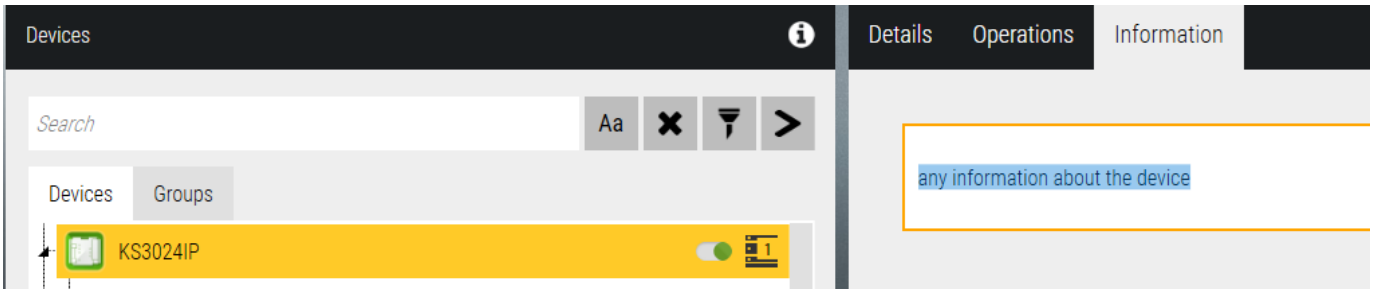
Enter first code to arm — button enters the first code to arm for a properly configured partition. The validity time of the first code is set when adding the control panel to NMS ADVANCED CONTROL.

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

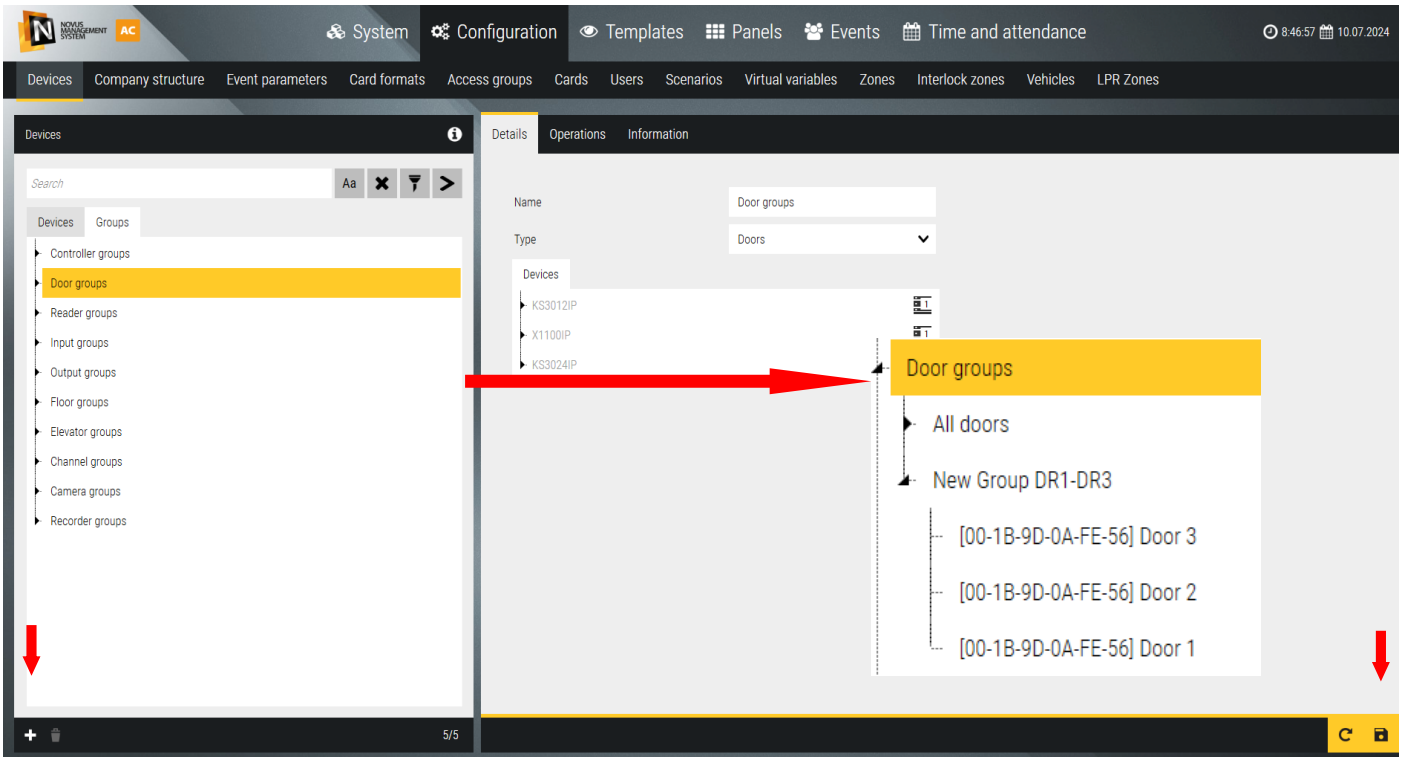
Each item has an Information tab, where you can put any description you want.



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.



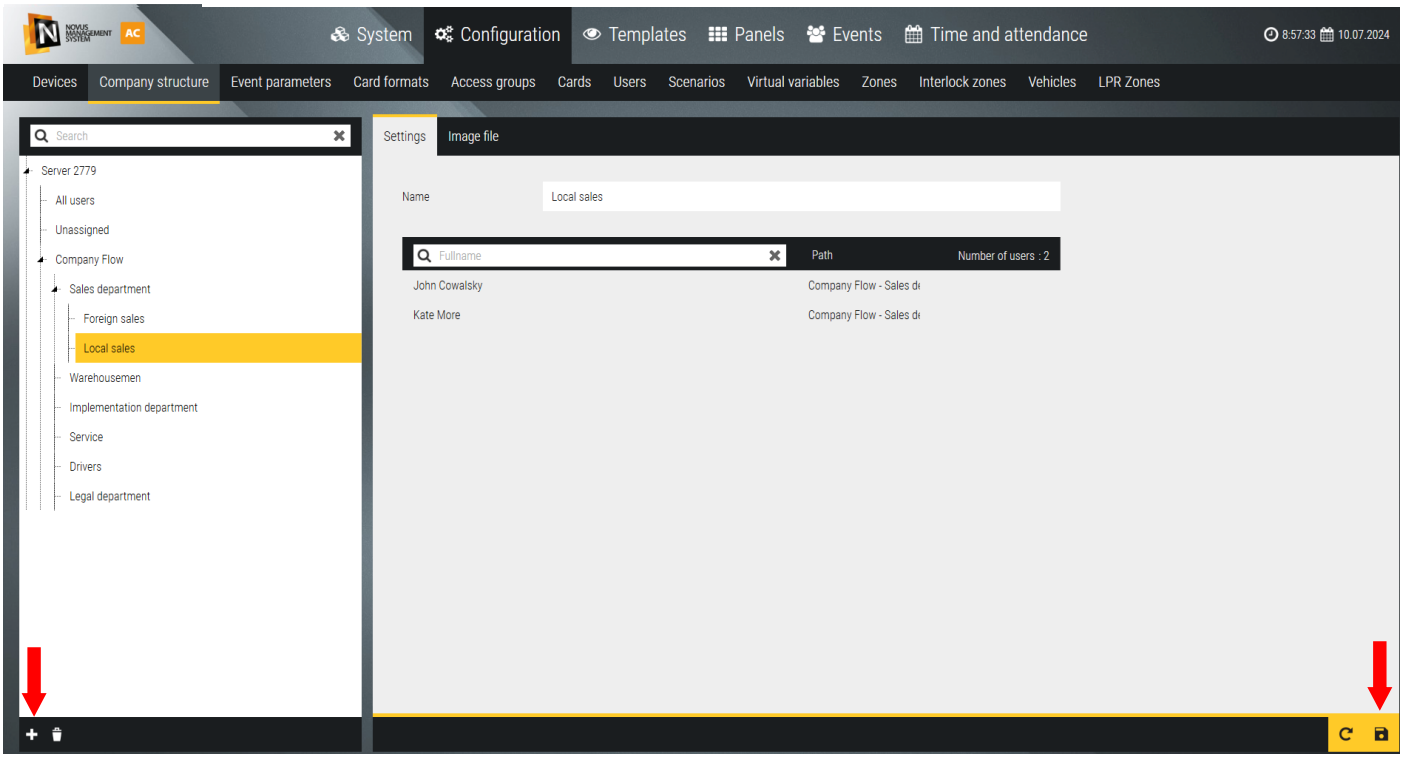
In addition to default groups containing all elements of a given type, we can define subgroups that contain only selected elements of a given type. To do this, select the default group of a given type and click the *Add* button at the bottom of the window. A new subgroup will appear in the group tree,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

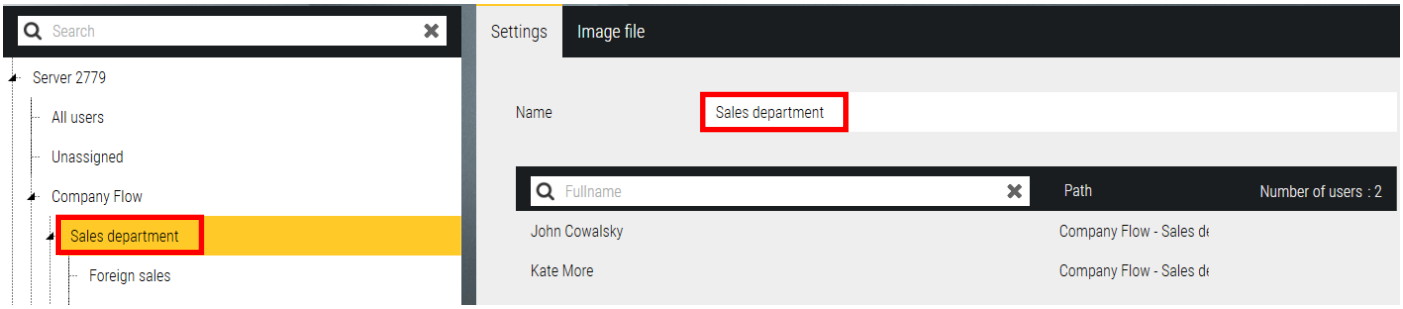
A defined group can be edited or deleted by selecting it in the list and clicking on the *Delete* button in the lower left corner of the window.

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:



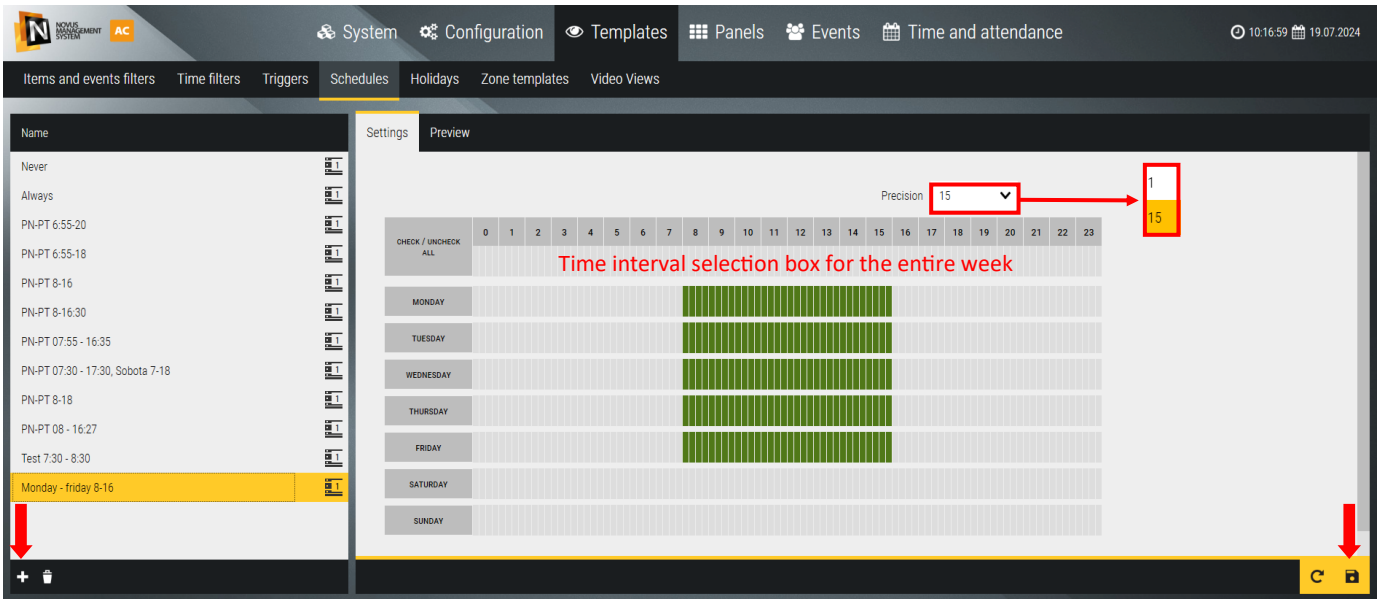
All users- displays in the right window a list of all users added to the database
Unassigned- displays in the right window a list of users not assigned to the structure
After adding users (manually or by import), both lists are the same.
To add a company structure, click on the Add button in the lower 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.



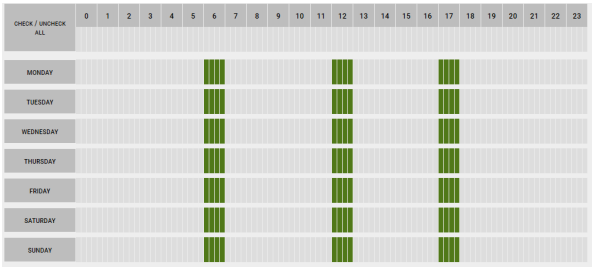
Section 4. Users, cards and access groups

4.1 Schedules

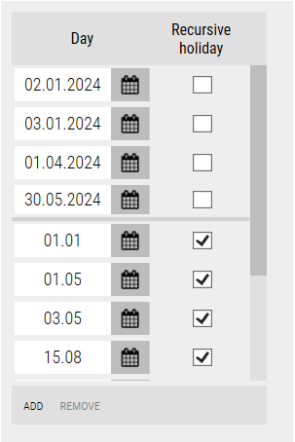
The Templates / Schedules tab allows you to define schedules intended in the KD system for access levels, automatic unlocking of doors, monitoring of guard lines at specific time intervals, and activation of control outputs and scenarios.

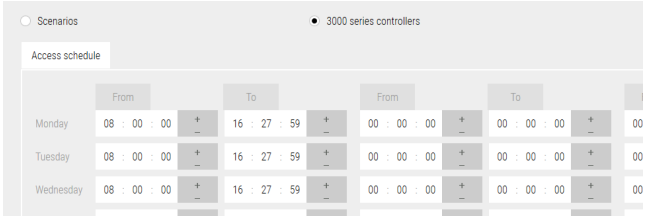


By default, two schedules are defined, *Never* and *Always*, which cannot be deleted or edited.
To add a new schedule, click on the Add button in the lower left corner of the screen. The default name in the yellow box can be changed to your own.
By clicking or dragging in the interval selection box with 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.

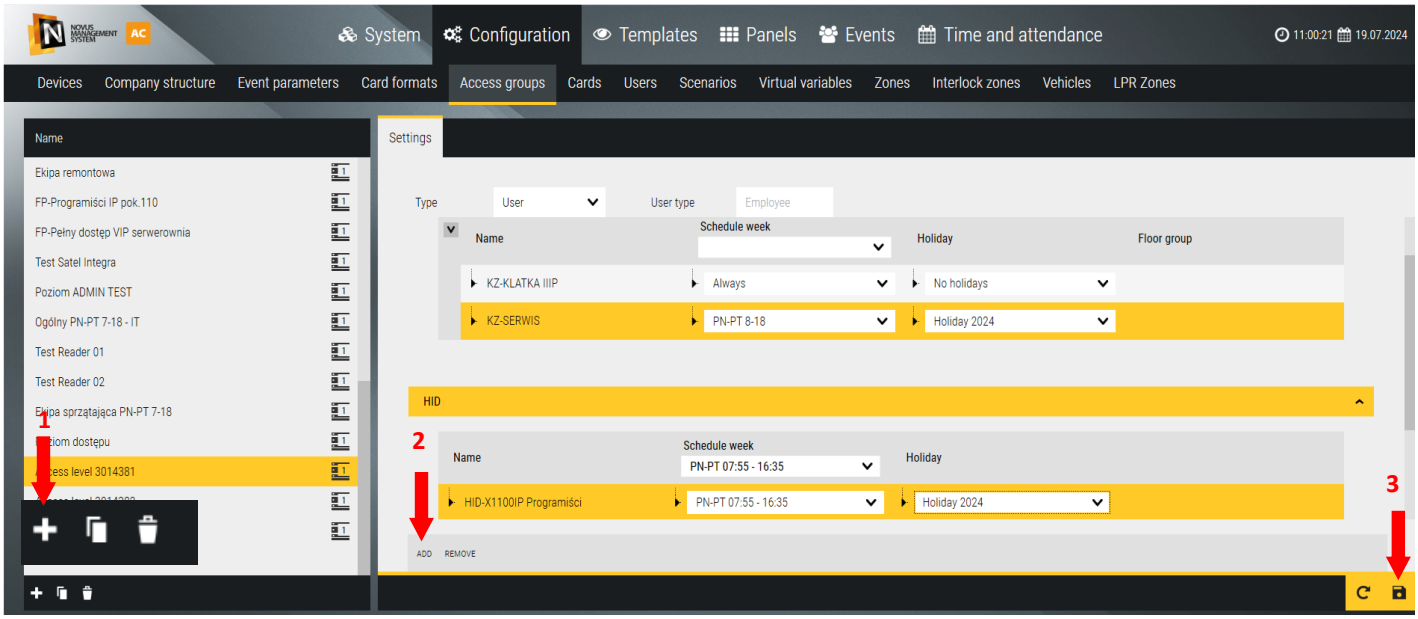


Holidays can be defined for the operation of scenarios by clicking on the button on the right side of the window. In the date fields, set the date of the holiday with the cursors in the order: year, month day. Then check the Special day checkbox. If the holiday is recurring, check the checkbox Repeat 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.

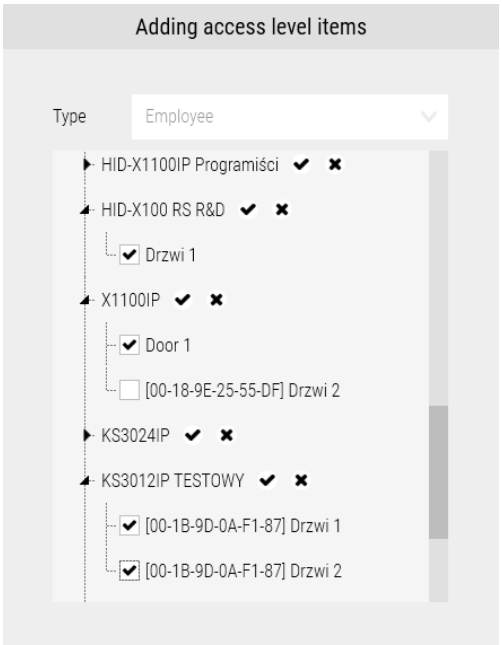




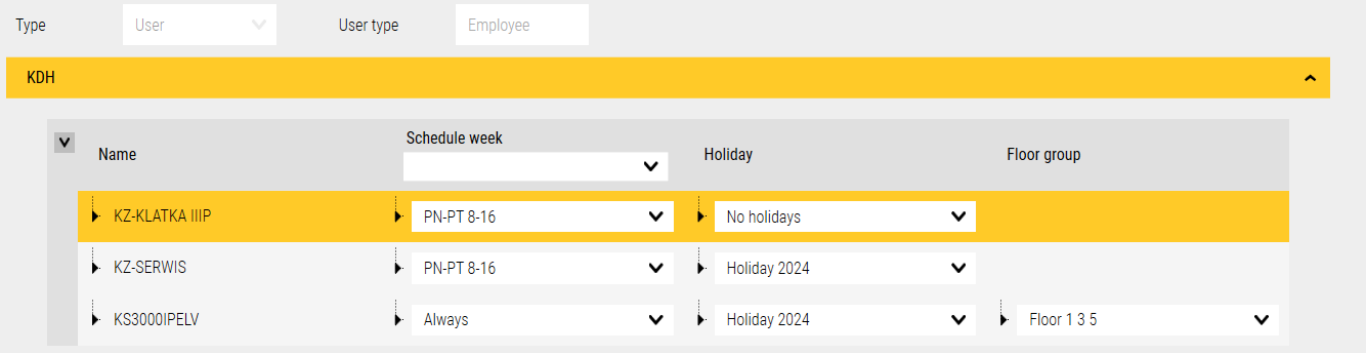
4.2 Acces groups



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.

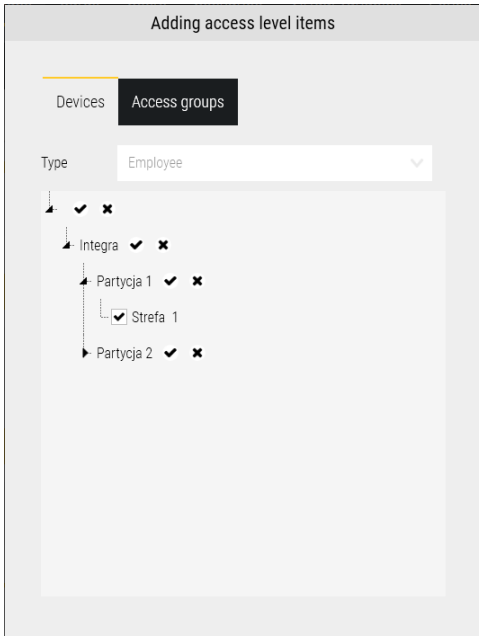
In the third column (Holiday), select a holiday from the drop-down list according to the expected access rights.

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.

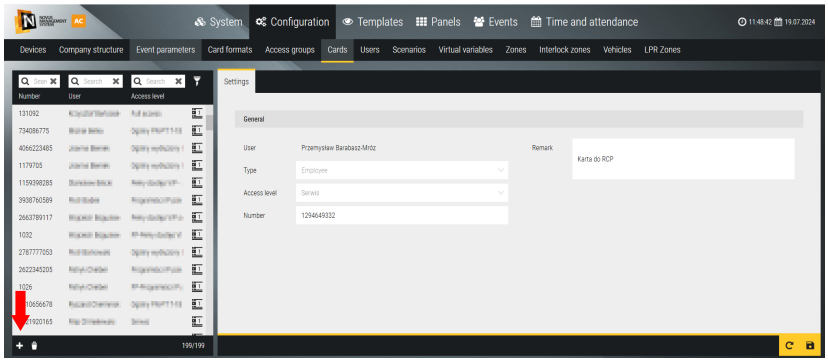
A window with a list of all previously added devices will be displayed.

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

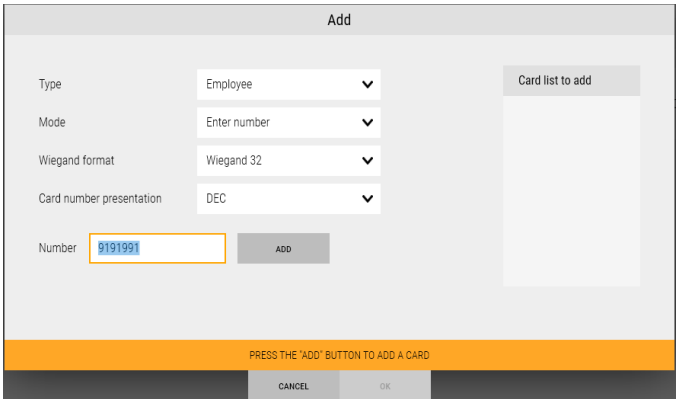
Checkboxes allow you to quickly check and uncheck and mark all items.

4.3 Cards

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



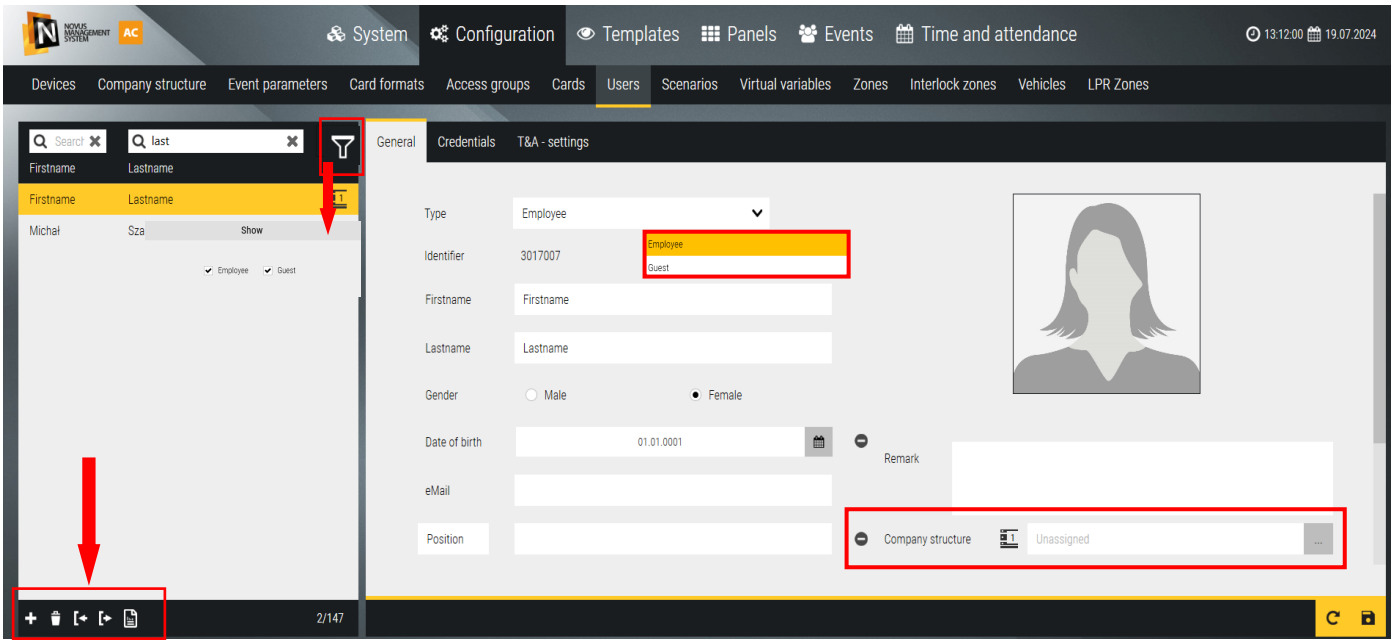
After clicking on the *Add* button, a window is displayed as below:



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.

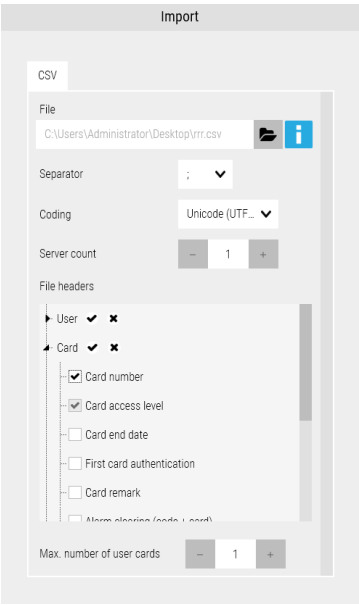
4.4 Users

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).

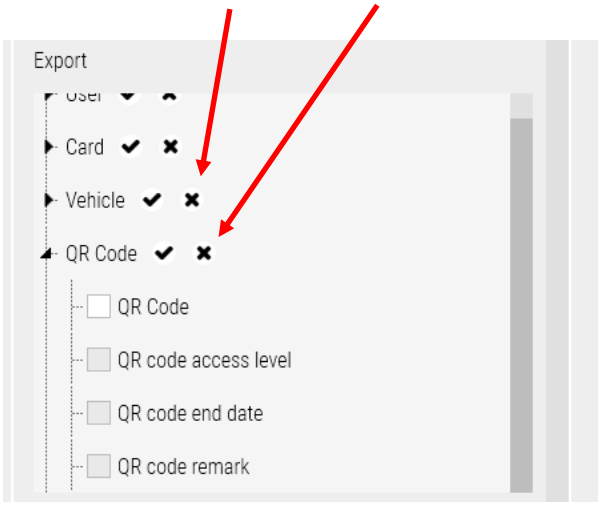


An example of an exported file with selected part of the options available for the User and Card items:

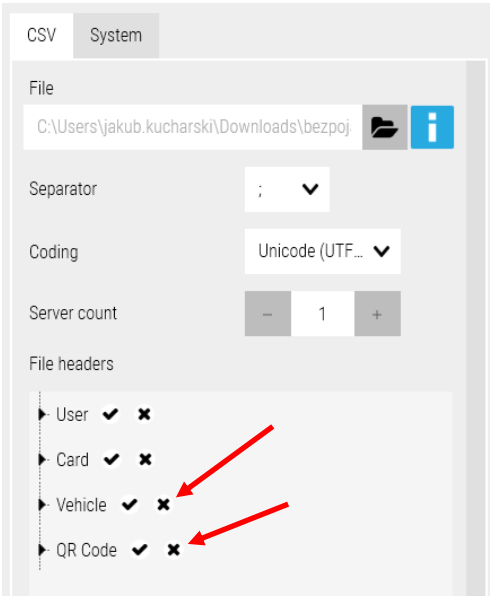
	A	B	C	D	E	F	G
1	Identifier	User type	Server name	Firstname	Lastname	Male	Card number
2	3006540	Employee	SRV AAT W-WA	Rafał	Nowak	Yes	755151267

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.



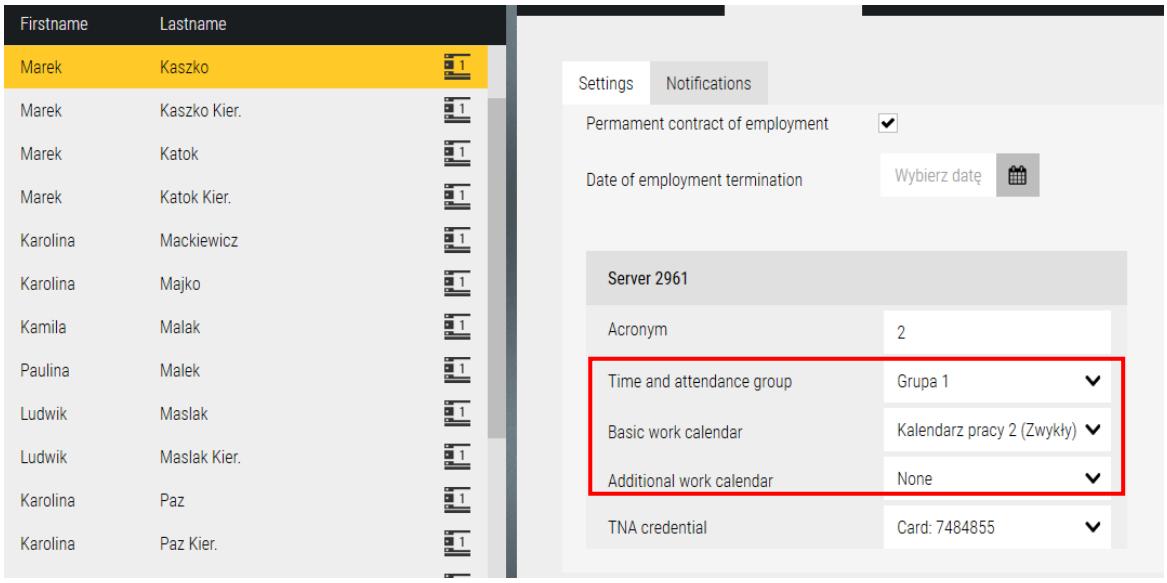
To import a file containing user data, select the icon
A window like the one shown below will appear.



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).

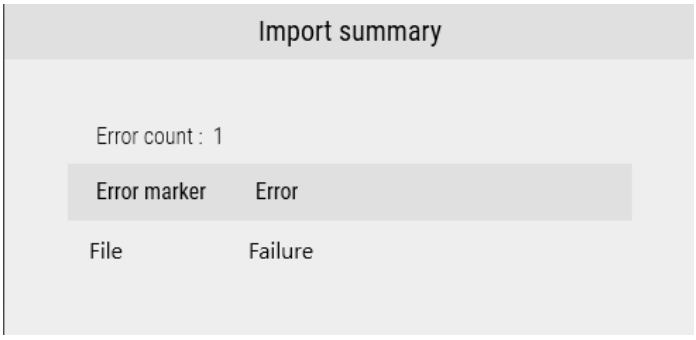


If the data in the columns are to be imported: Type, Work Calendar, Work Time Group, Access Level and Company Structure then these items must first be defined in the program and then their names copied and pasted into the appropriate columns. If, after the first import, you want to continue working on 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.

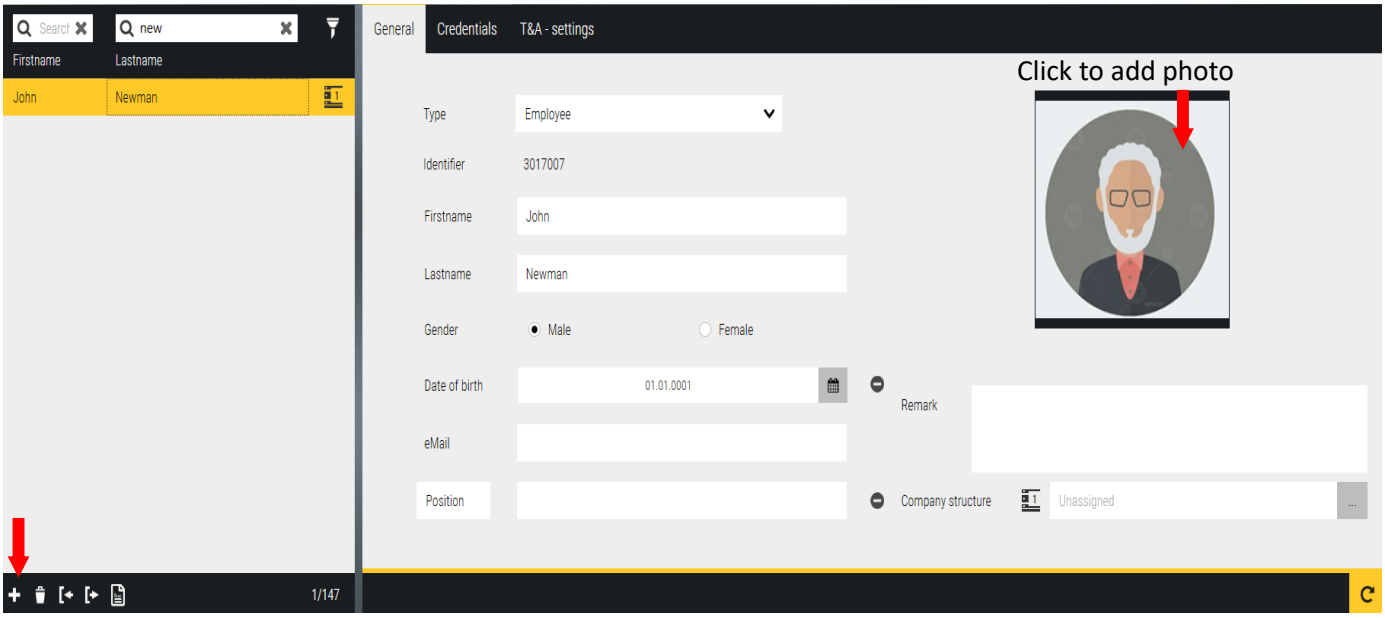
View of the exported CSV file:

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:



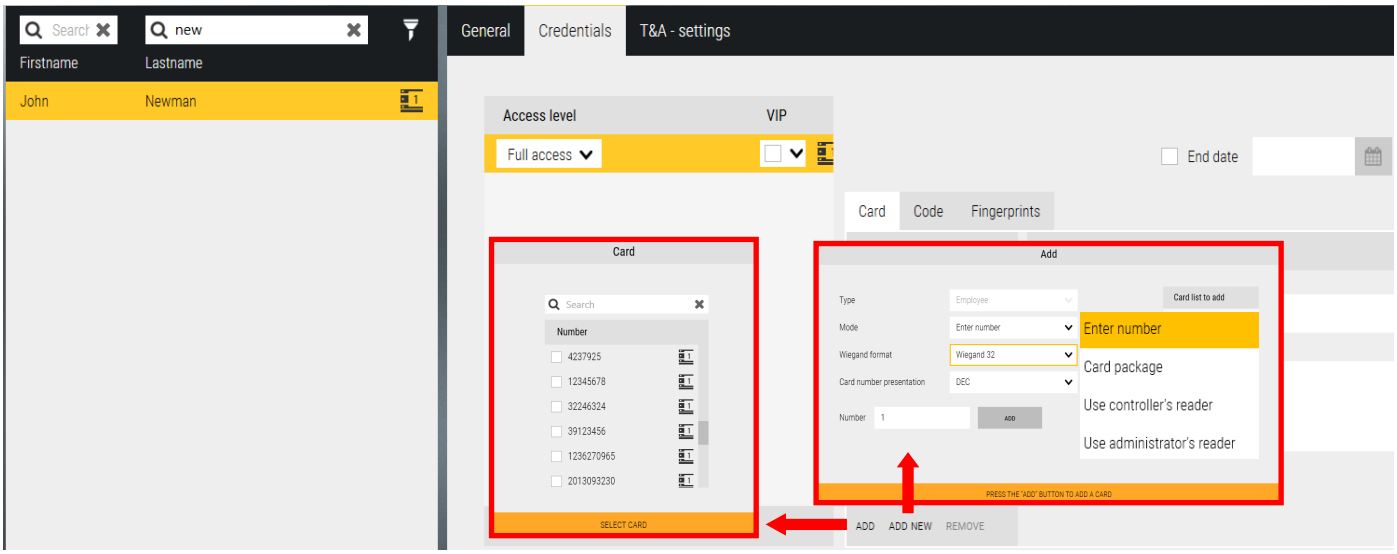
Adding a new user - click on the Add (+) button in the lower left corner of the window (to delete, select and click Delete). Then fill in the form fields in the right window. Except for the first and last name field, the other fields are not mandatory. You can also add a photo of the user from a file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

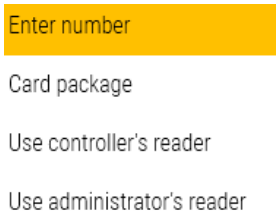


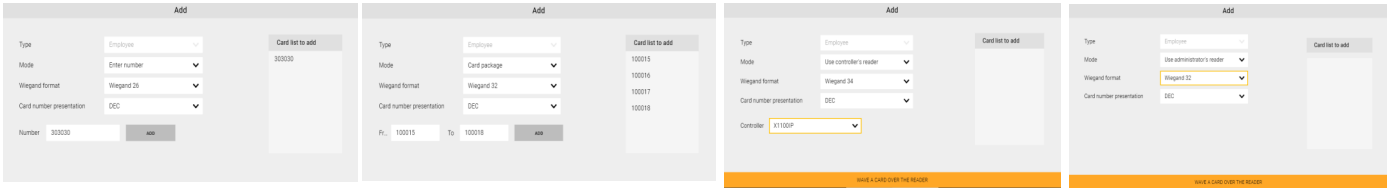
In the window on the previous page, we have two ways to assign a new card to a user. A user can have more than one card.

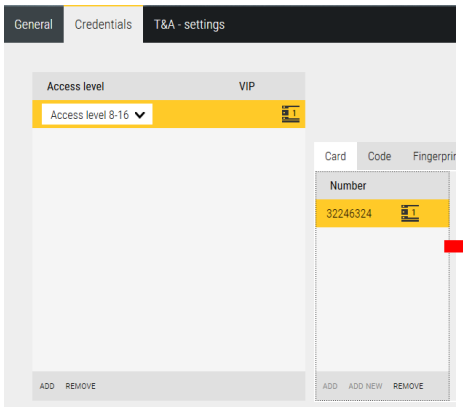
After clicking on the *Add* button, a window pops up as on the left with a list of cards added earlier through the Cards tab. Select the card numbers you want to assign to the user.

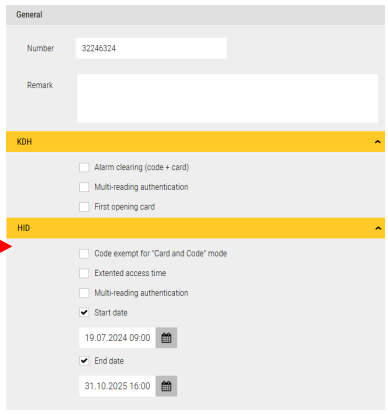
After clicking on the *Add New* button, a window pops up as on the right. In this window, we can choose one of four options for entering the card number in the list:

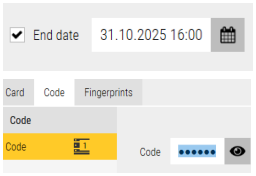
- Manual entry of the number in the editable field (when we know the card number) The entered number is subject to verification, if it already exists in the system database it is highlighted in red and cannot be added.
- Manual entry of the first number from the card pack (pack with consecutive numbers) 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:

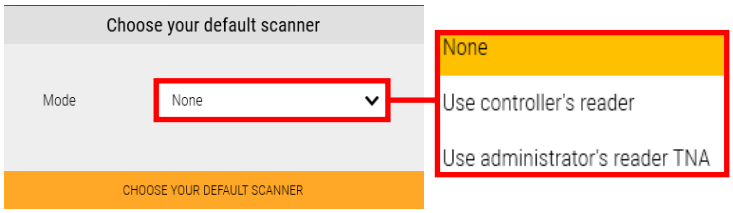
Code exempt for „Card and code" mode - transitions set in the "c&c" mode will not require entering a PIN.

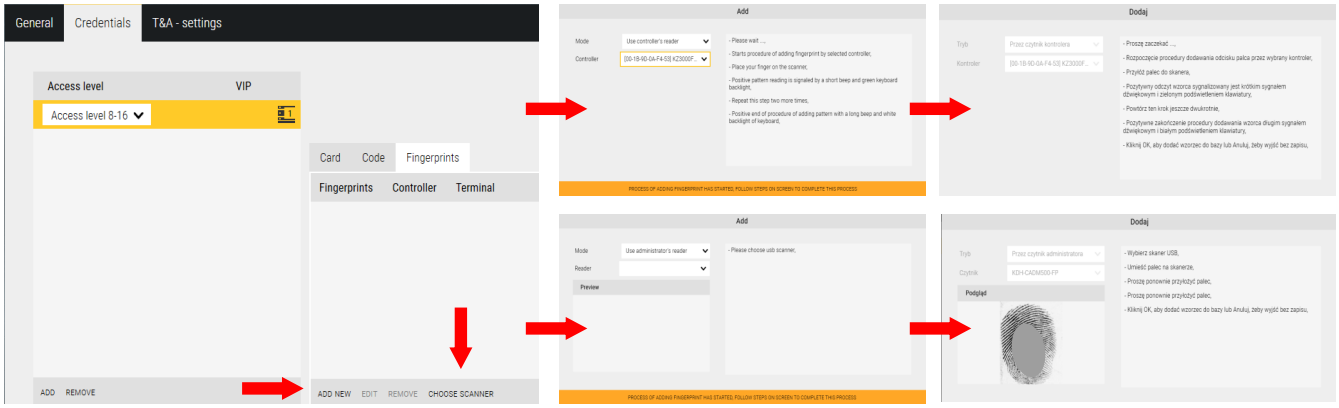
Extendet access time - Door unlatching and opening time will be as in the *Door/Extended Access Time* setting

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.

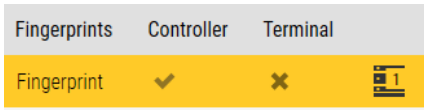
Adding fingerprints - applies **KDH-KS3000FP-IP-U_M i KDH-TA500CFP-IP-UMD**.
To start the procedure of adding fingerprints, click on the *Choose Scanner* button in the *Fingerprints* section.
For KDH-KS3000FP-IP-U_M models, add by selecting a controller from the list - Use controller's reader
For KDH-TA500CFP-IP-UMD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

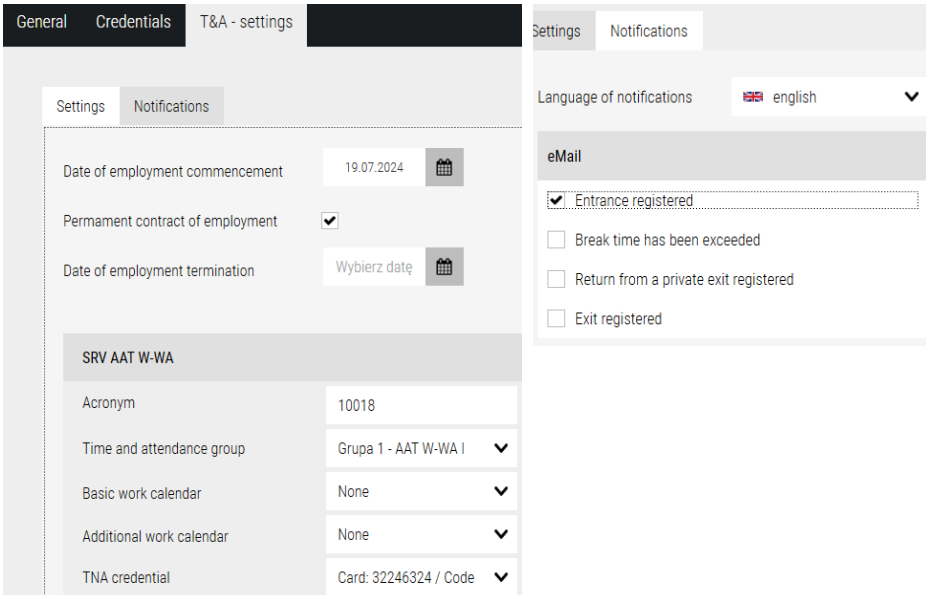
After completing the procedure (3 finger touchdowns), click OK, and after closing the window, you can add fingerprints from more fingers in the same way. Then click Save to save the user data to the database and send it to the controllers.



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

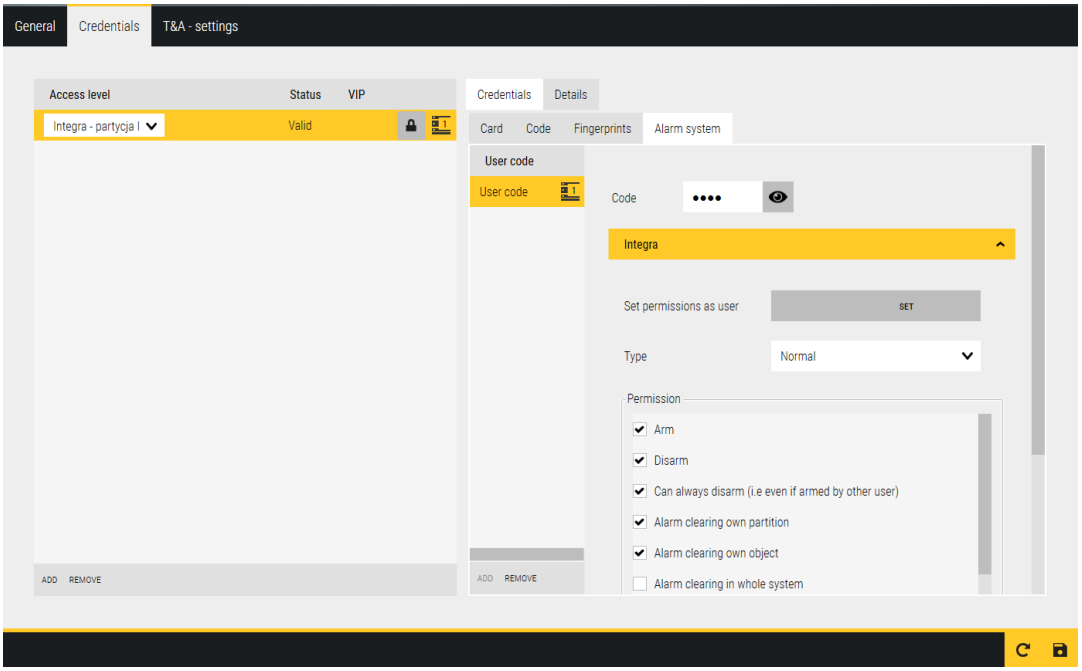
T&A settings - In this tab, you can define the user's start and end date of employment, assign group and working time calendars, and select an ID for time registration. You can also define an Acronym which is the user's identification number. This allows you to register *enter/exit* on the terminal or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

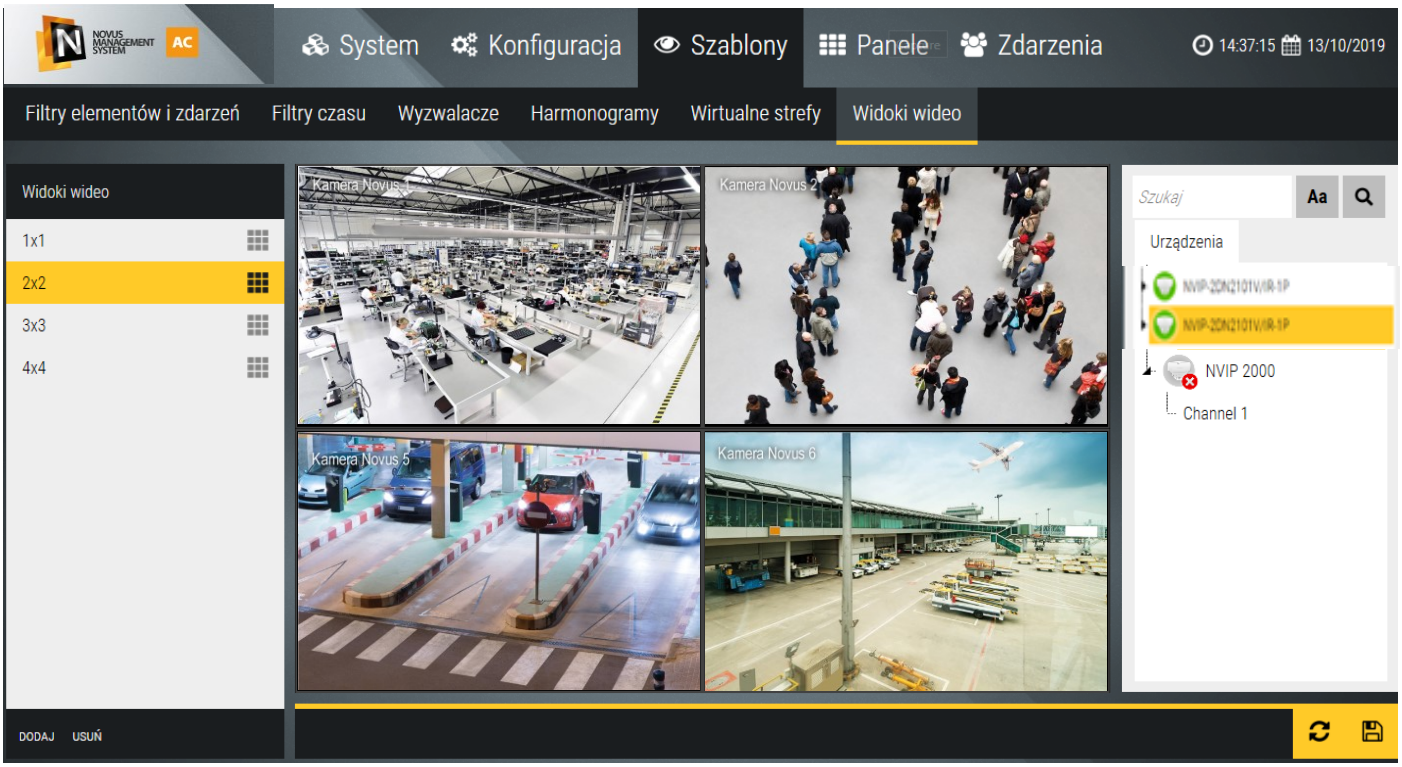


After clicking the Add button, define the user's password and its permissions (or copy from another user).
The password’s number of digits is defined when adding the new panel to NOVUS MANAGEMENT SYSTEM AC program.

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.

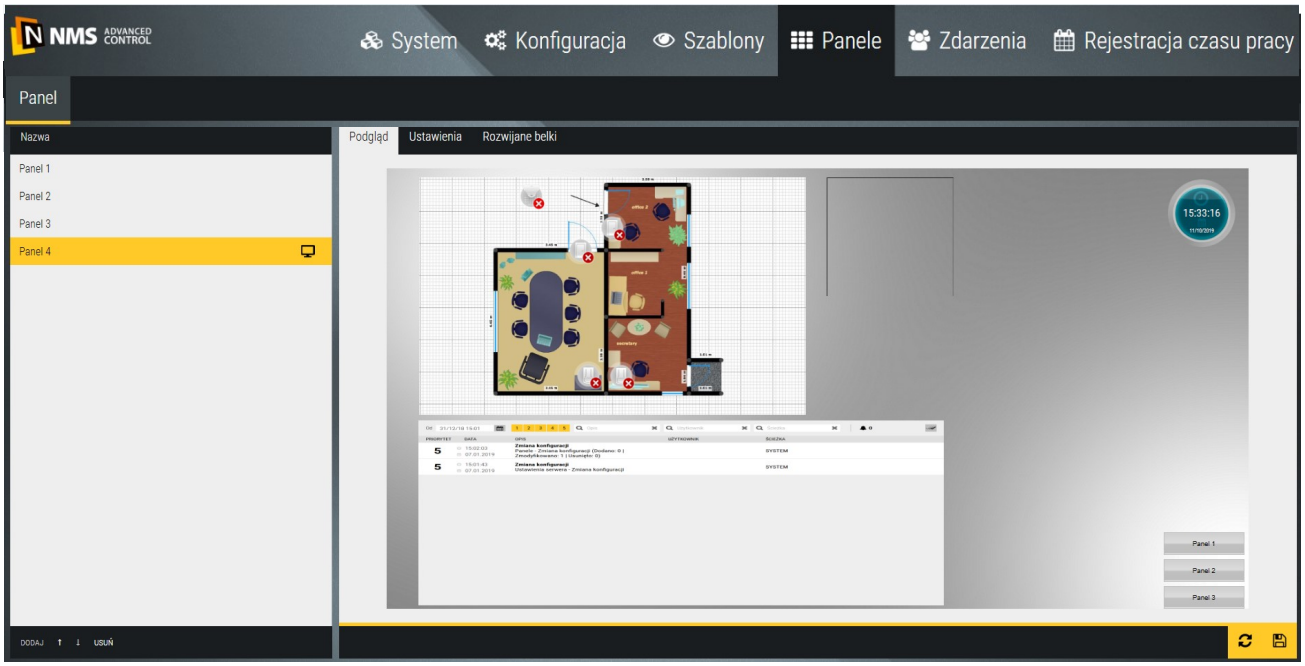
By right clicking on one of the split screens it can be set as a HOTSPOT window. This window will not have a permanently assigned camera. It will display the camera that the user click with the mouse wheel (middle button).

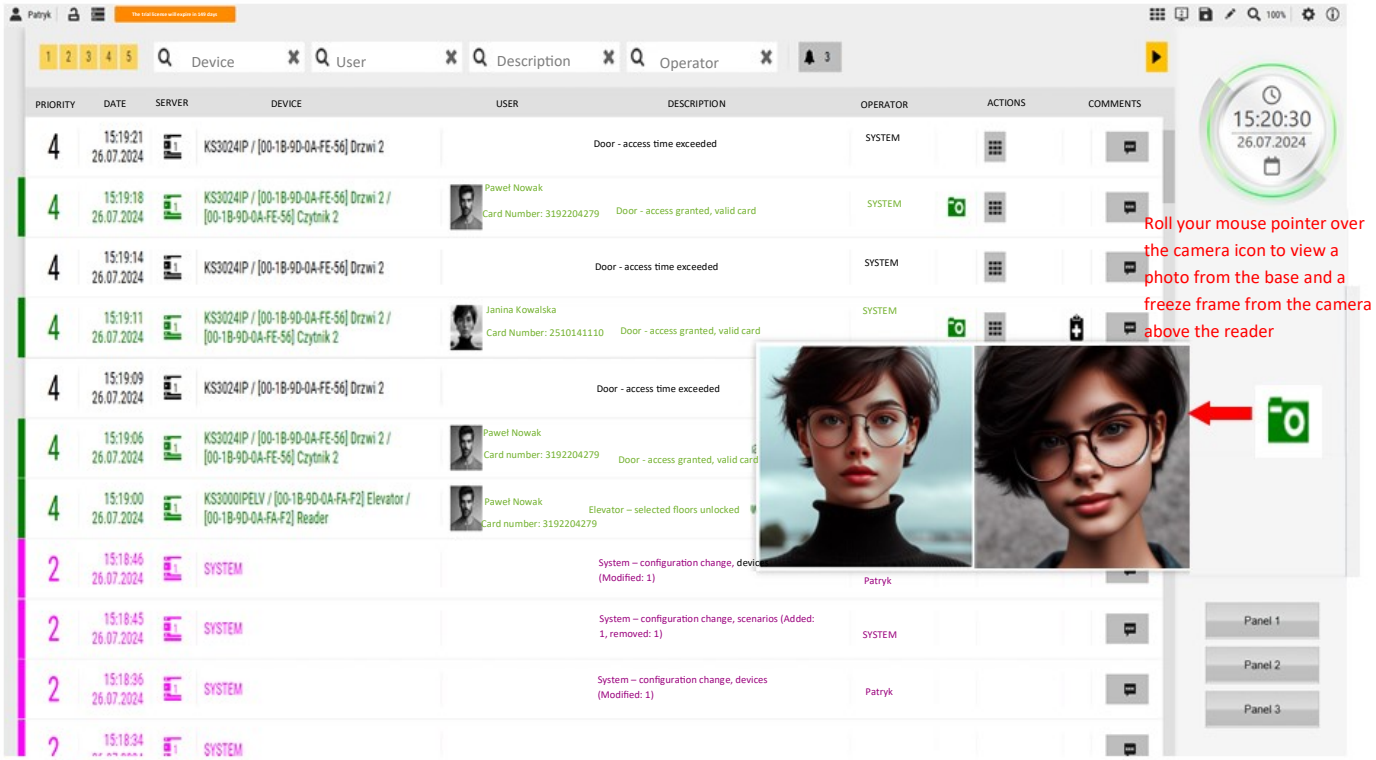
After you define the video views, click the Save button in the lower-right corner.
You can view defined video views on panels in video windows. Default Panel 3 includes this view window.

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.

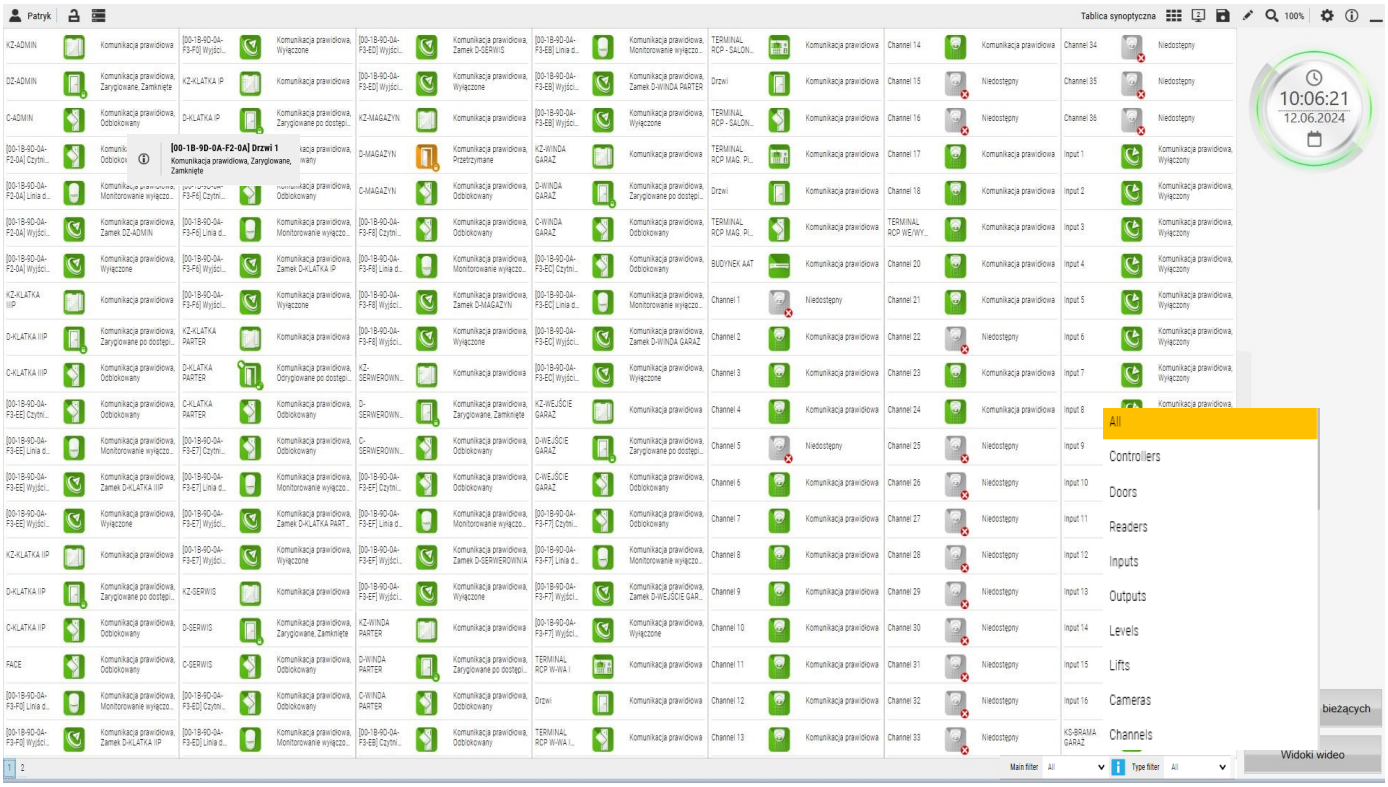




See the table on page 30 for a description of the icons on the top bar.

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.

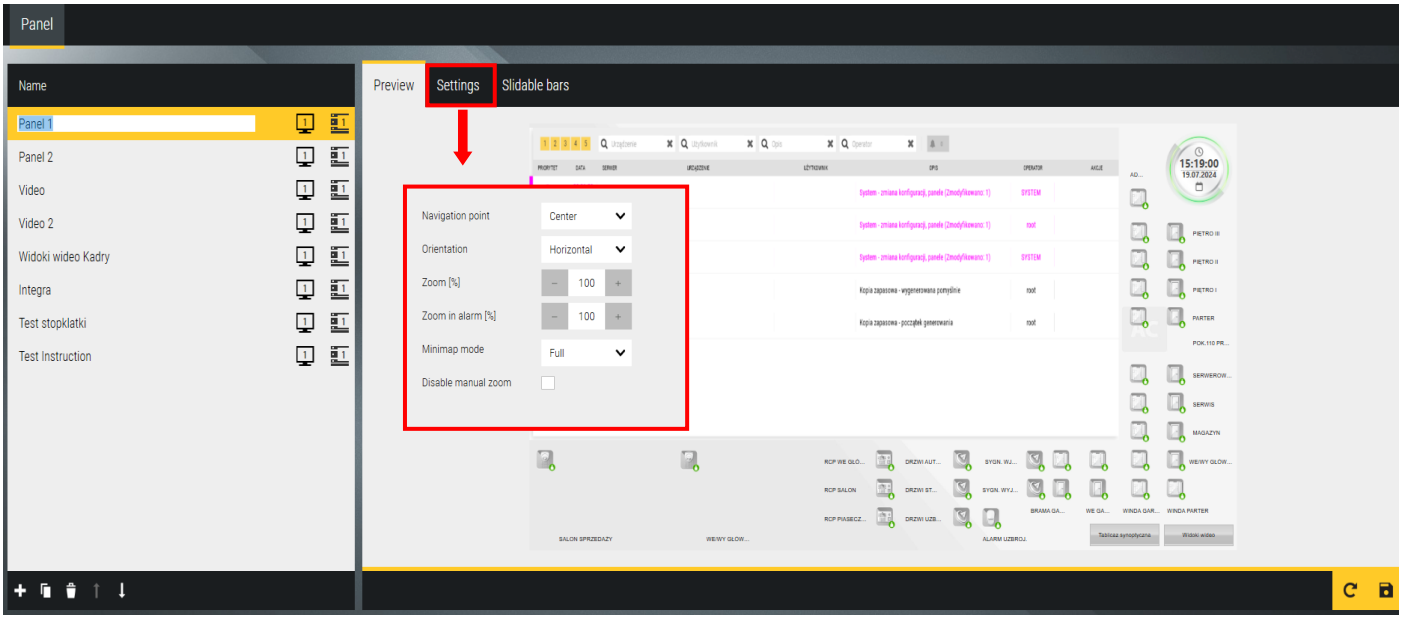


Panel 2 contains a synoptic table, to which successive added controllers are automatically added, along with associated elements (doors, supervisory lines, control outputs, elevators, floors) and CCTV devices in the form of icons showing their current status. The status of the icons is updated in real 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

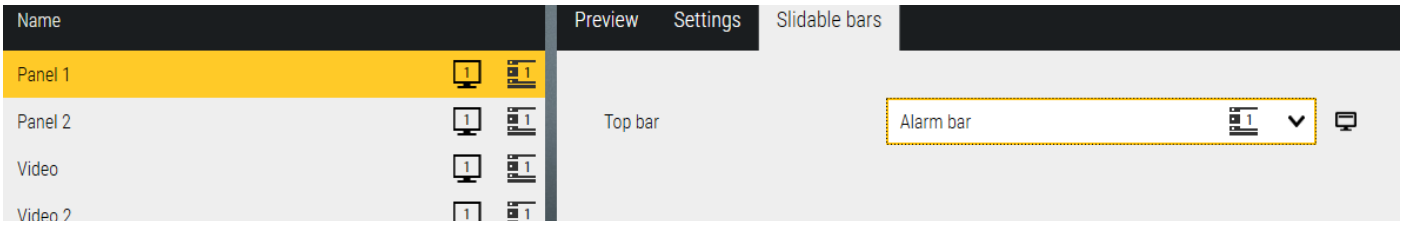
Zoom [%] - allows you to set the magnification value on the panel

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



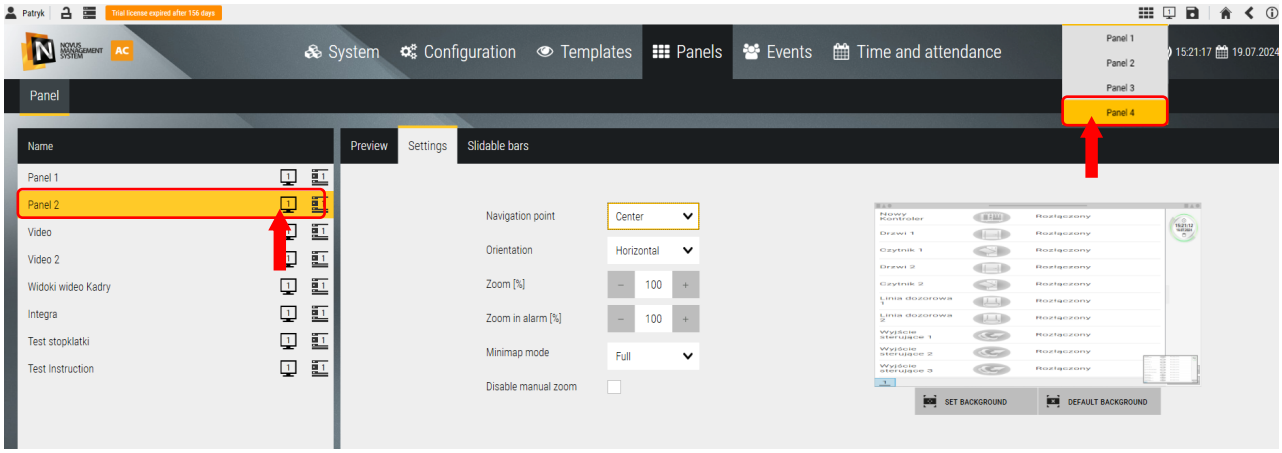
Tab *Slidacle bars*

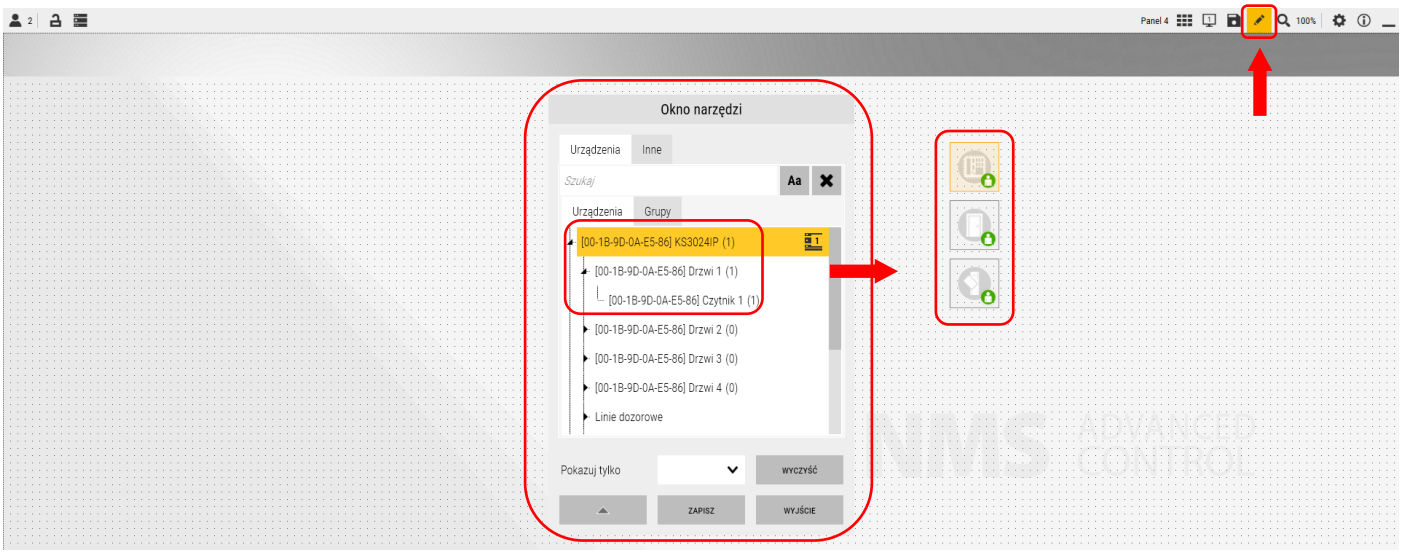
Top bar - to choose from the drop-down list: alarm bar or none

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

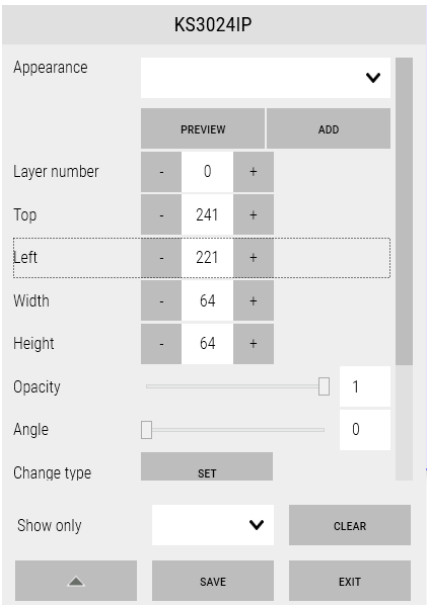
By clicking on the panel name in the left window, we can enter display mode and verify the settings.

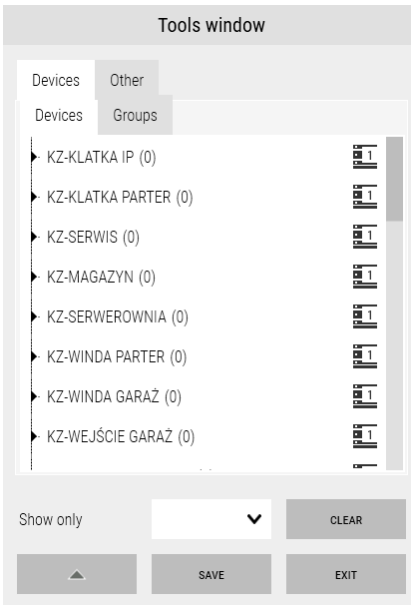
Configuration of the defined panel

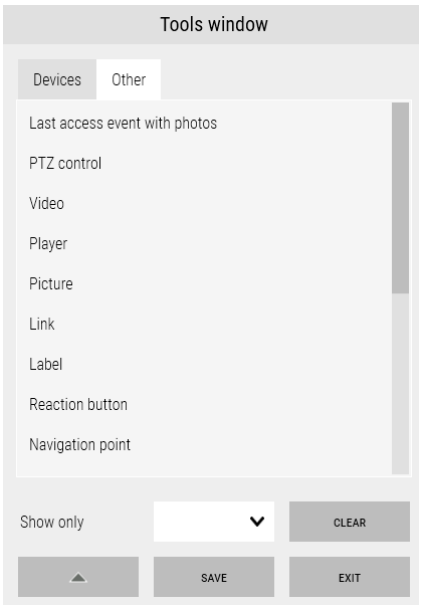




When you click on the list in the left window or in the upper right corner on the selected monitor, a window will appear as below. Clicking on the *Edit* icon in the upper right corner opens the Tools Window. The *Devices* tab displays a list of devices added to the system database, which can be dragged 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



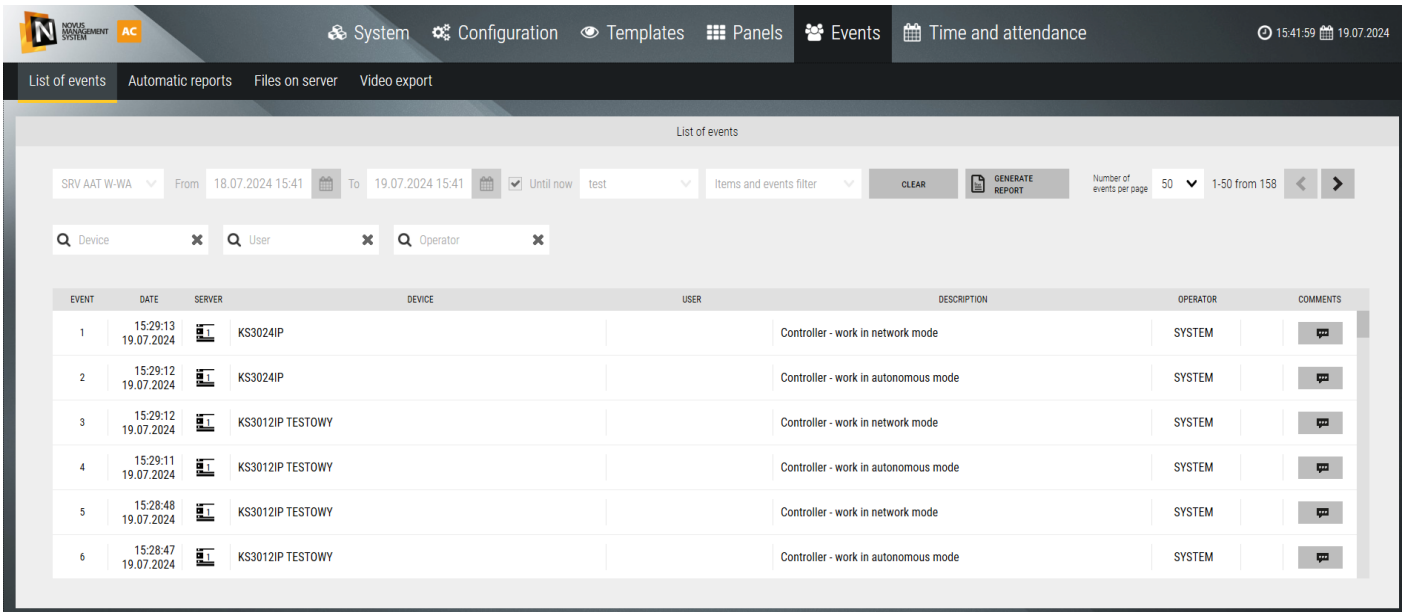




Section 7. Events and reports

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.

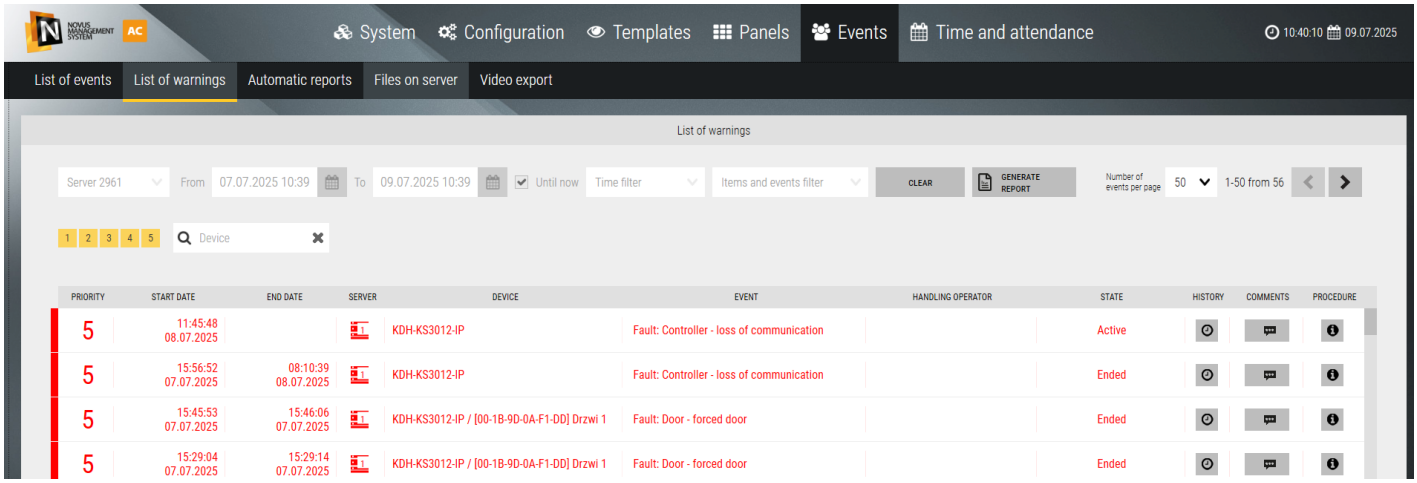
At the top of the window are filter windows for date, time interval (last 24 hours back by default), and items and events. This allows for easier analysis of events on the object

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).



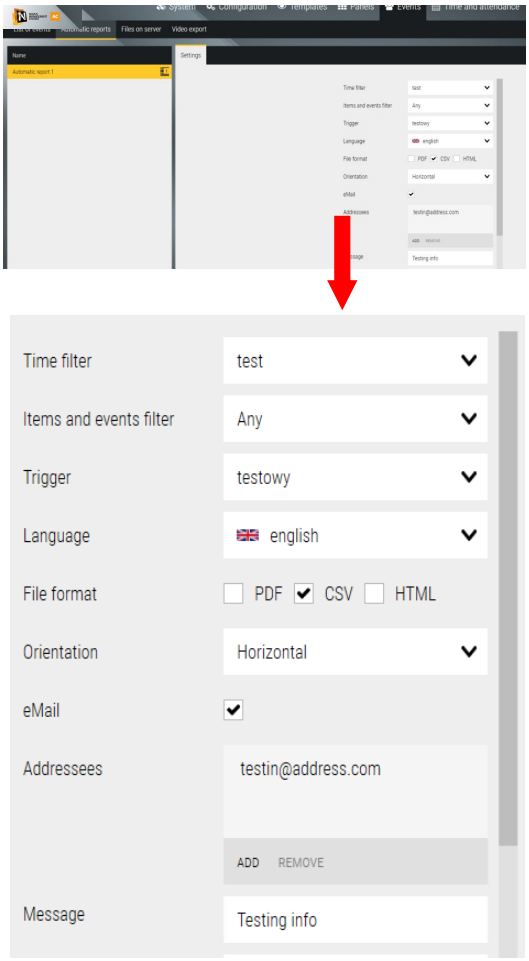
Each line in the report includes a timestamp indicating the date and time, a description of the event, associations with the operator or card user, and the physical system component related to the warning.

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

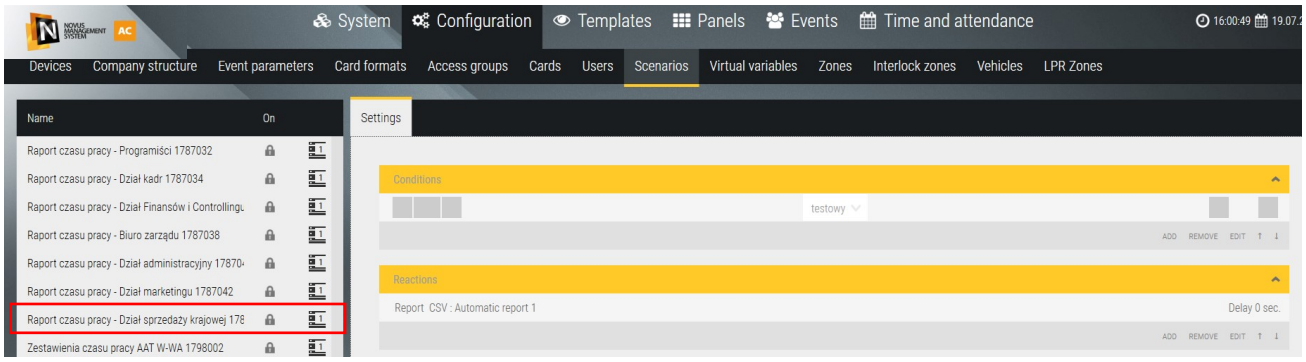
Note: Each of the above three options, when expanded, contains an "Add" item that opens a window to define a new filter or trigger

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.

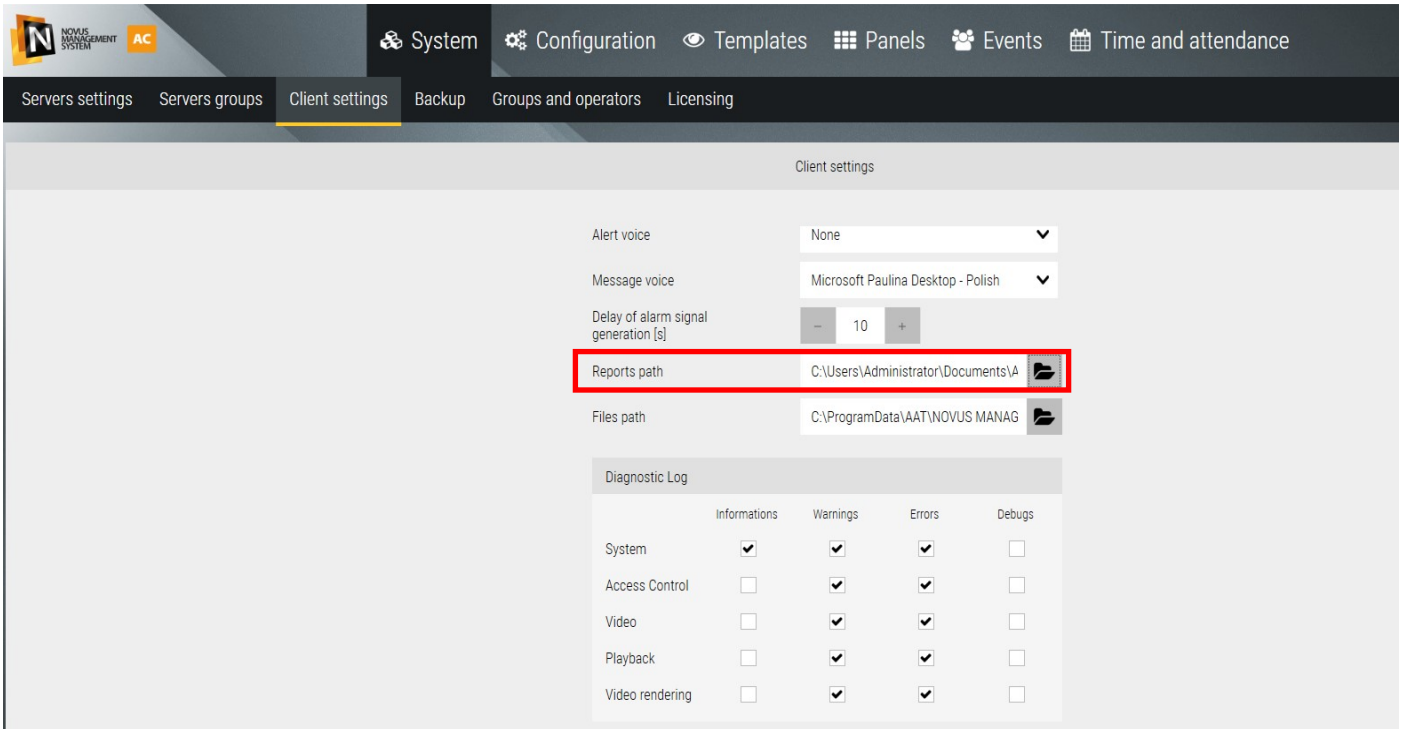
Email - A box to check if the report is to be sent as an email. Once checked, fields for entering email addressees and subject are displayed below. To add an addressee, click on the add button at the bottom of this field and enter the email address in the box that appears.



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

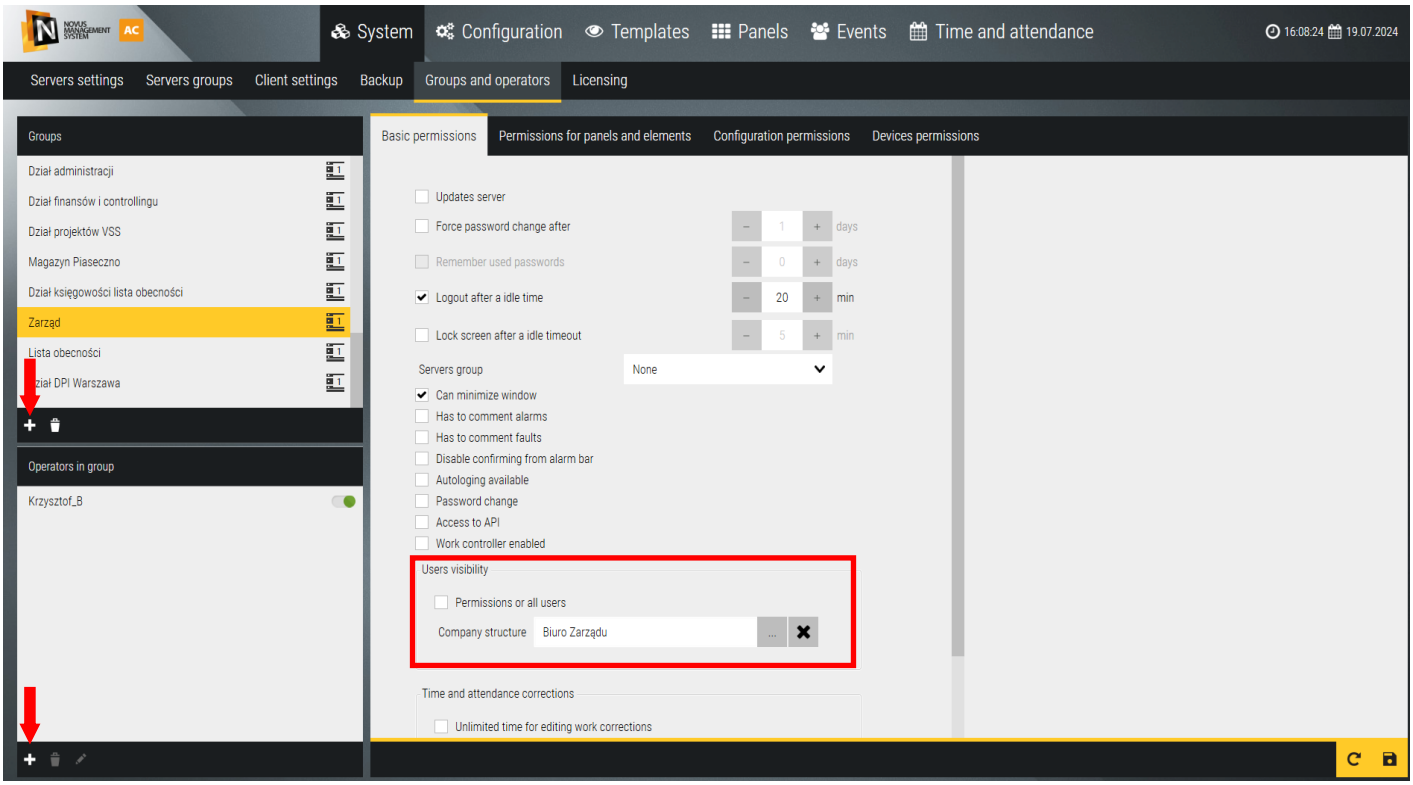
Reports generated automatically according to the trigger assigned in the template are saved in the report archive on the computer where the NOVUS MANAGEMENT SYSTEM AC server service is installed. You can change this path in the *System* tab.



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.

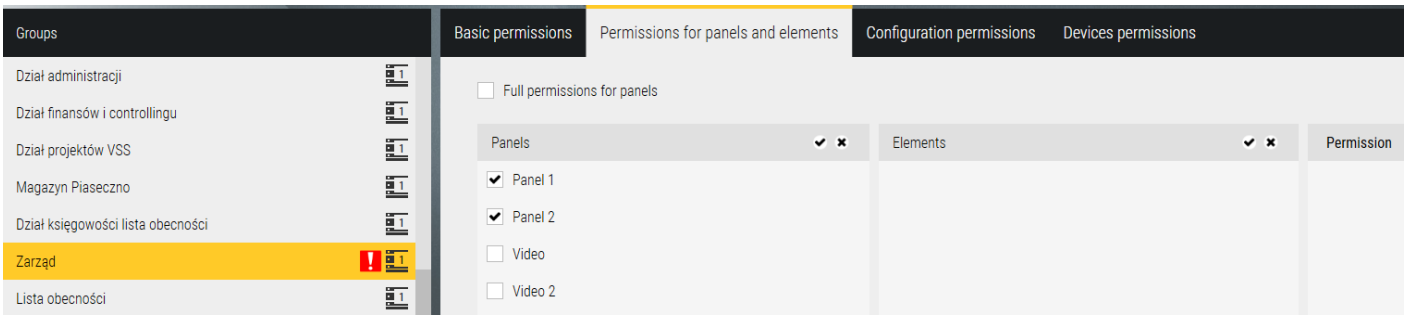
After selecting a group in the upper window, operators can be added to it. By default, one root operator with full privileges is defined in the Administrator group. Permissions are defined for the group (not for individual operators), for a new group of operators you should set them in the following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

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

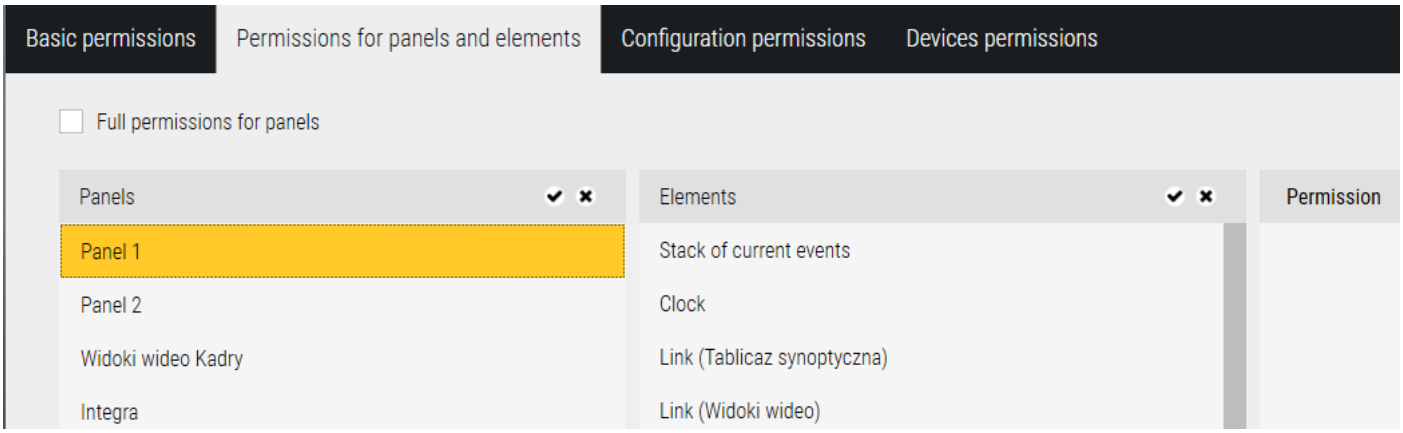
Info:

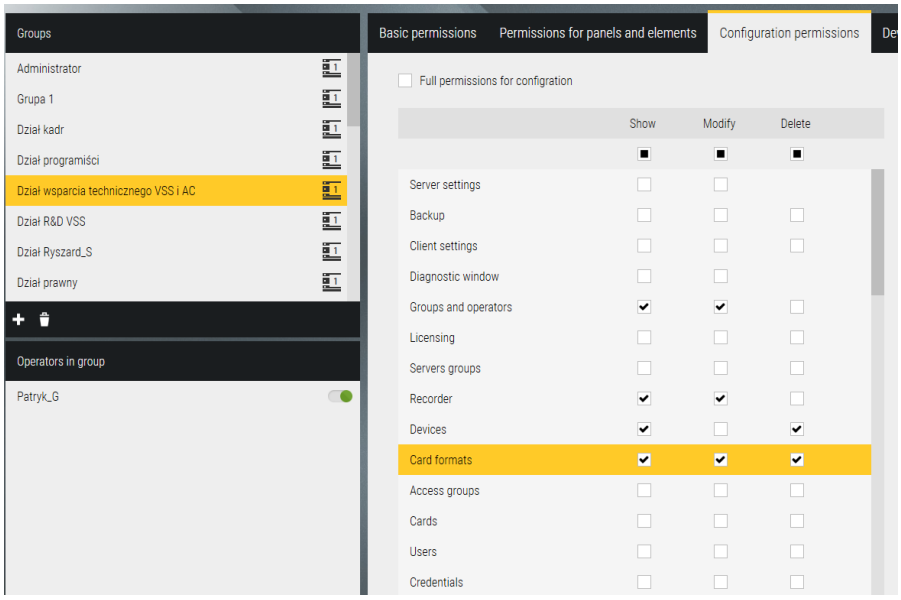
By default, no users are assigned for the newly created group. To change this, select All users or select users according to the company structure.

Permmision for panels and elements



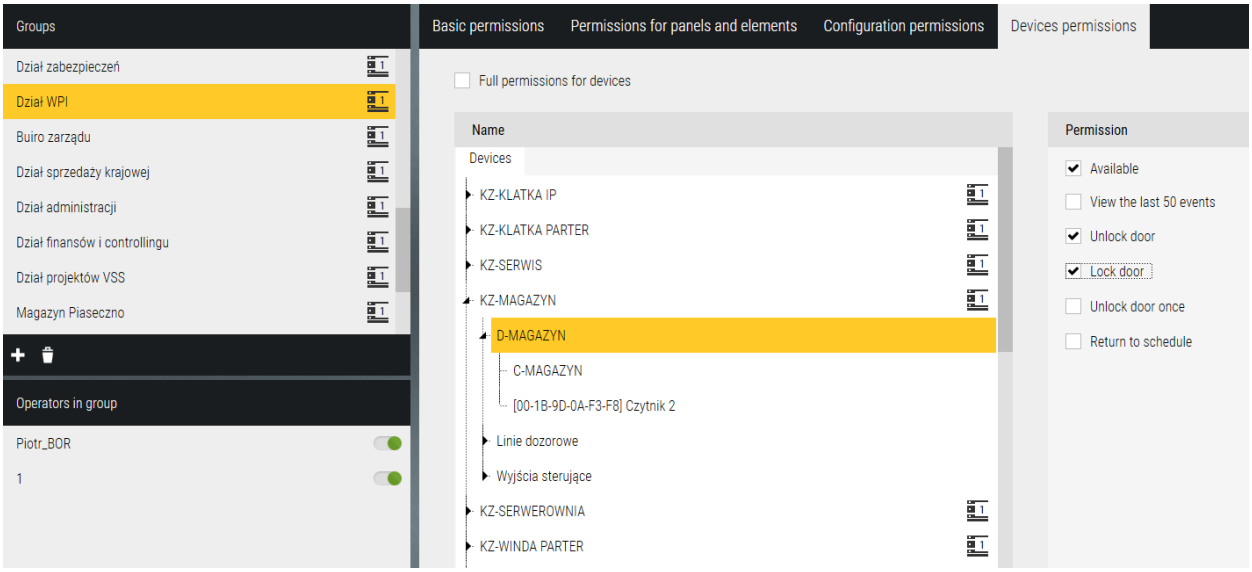
After clicking on the button at the bottom of the window, a list of available panels is displayed in the first column - select those to which operators from this group are to have access and OK.
The second column (Elements) displays a list of elements embedded on this panel. After selecting a selected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





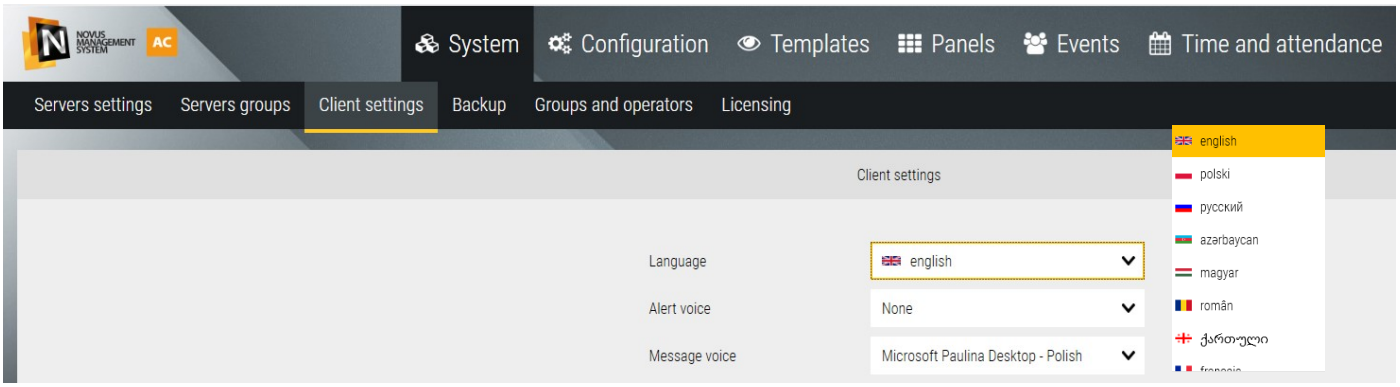
In this tab, set which items from the program's menu will be accessed by operators from this group. The administrator has full read, modify and delete access. For the *Security* group, most often only selected menu items with the *Show* attribute are left.

Devices permissions



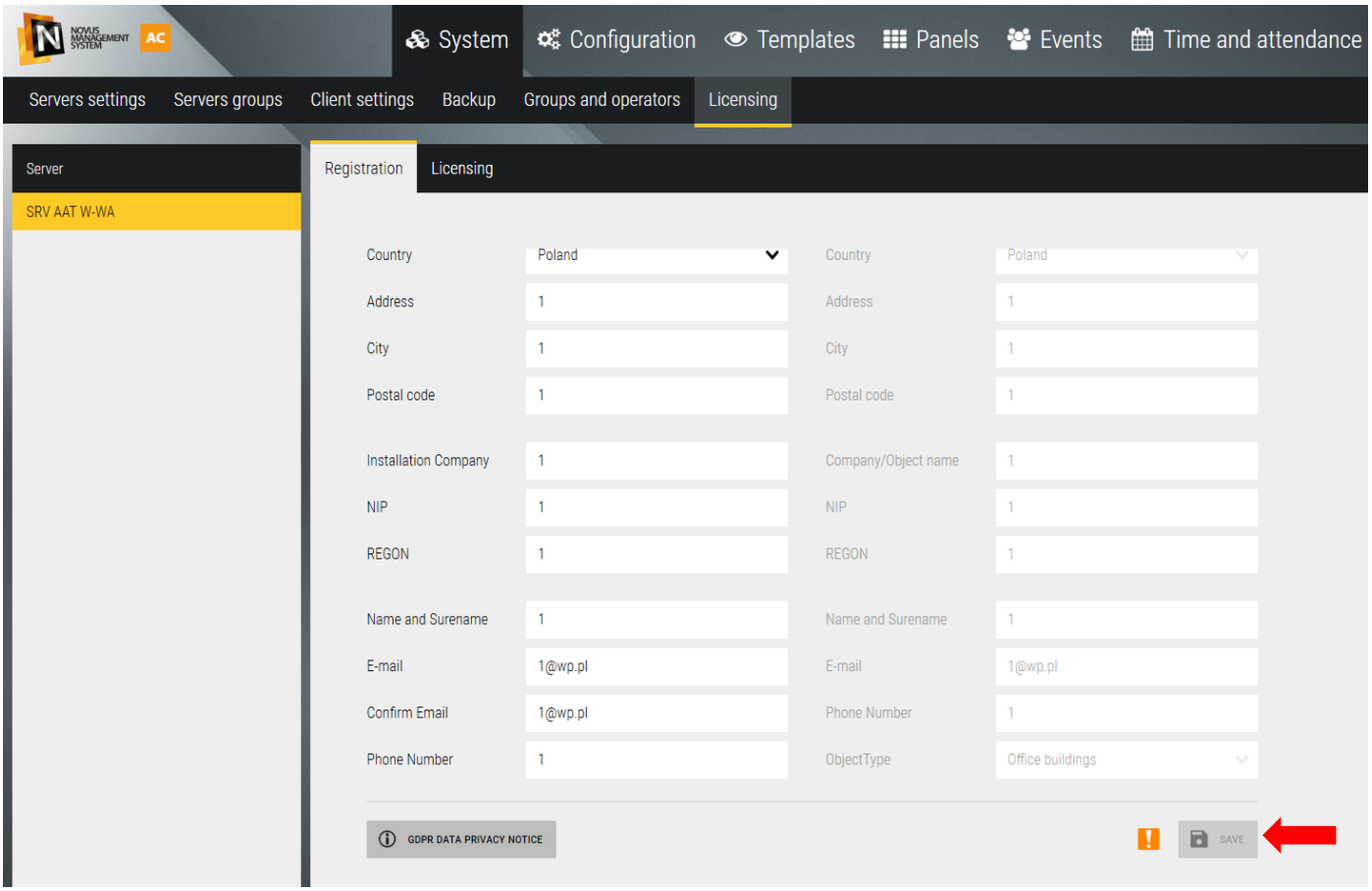
In this tab, set which system devices operators from this group will have access to perform certain operations on them. The administrator has full access to all operations. For the Security group, most often only selected items related to basic operations are left, e.g. Unlocking/locking doors.

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

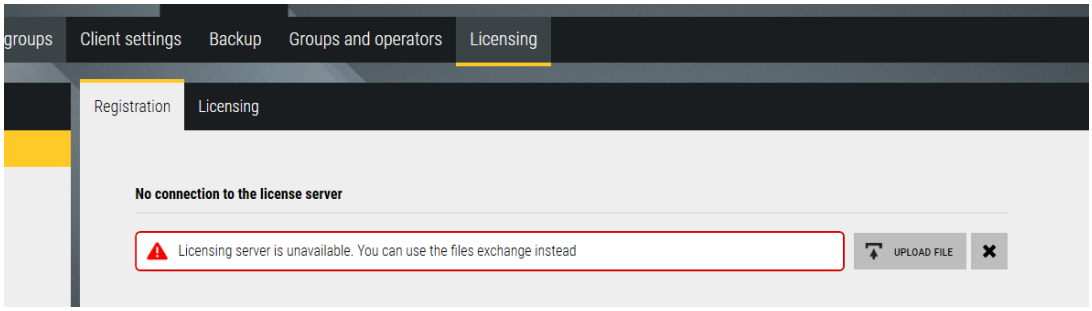


The use of NOVUS MANAGEMENT SYSTEM AC requires its registration and activation of the corresponding licenses. Activation of licenses is possible only after registering the program.
To register the program, fill in all the required fields shown in the image above.

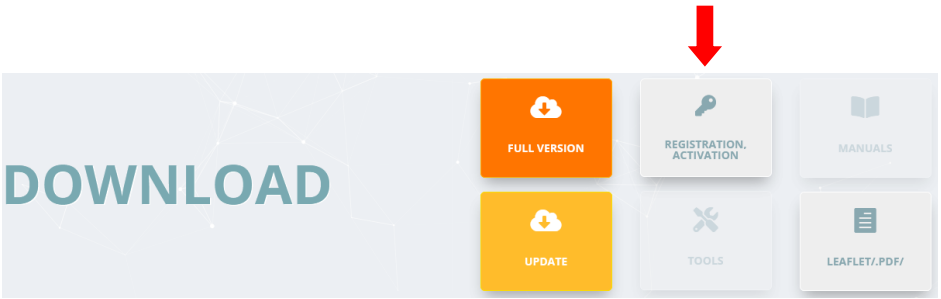
NOTE!
Once the registration process is completed, editing the data in the License User Data section will not be possible. In order to modify these data, please contact AAT SECURITY SYSTEMS Ltd. via e-mail address: kontakt@aat.pl.

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

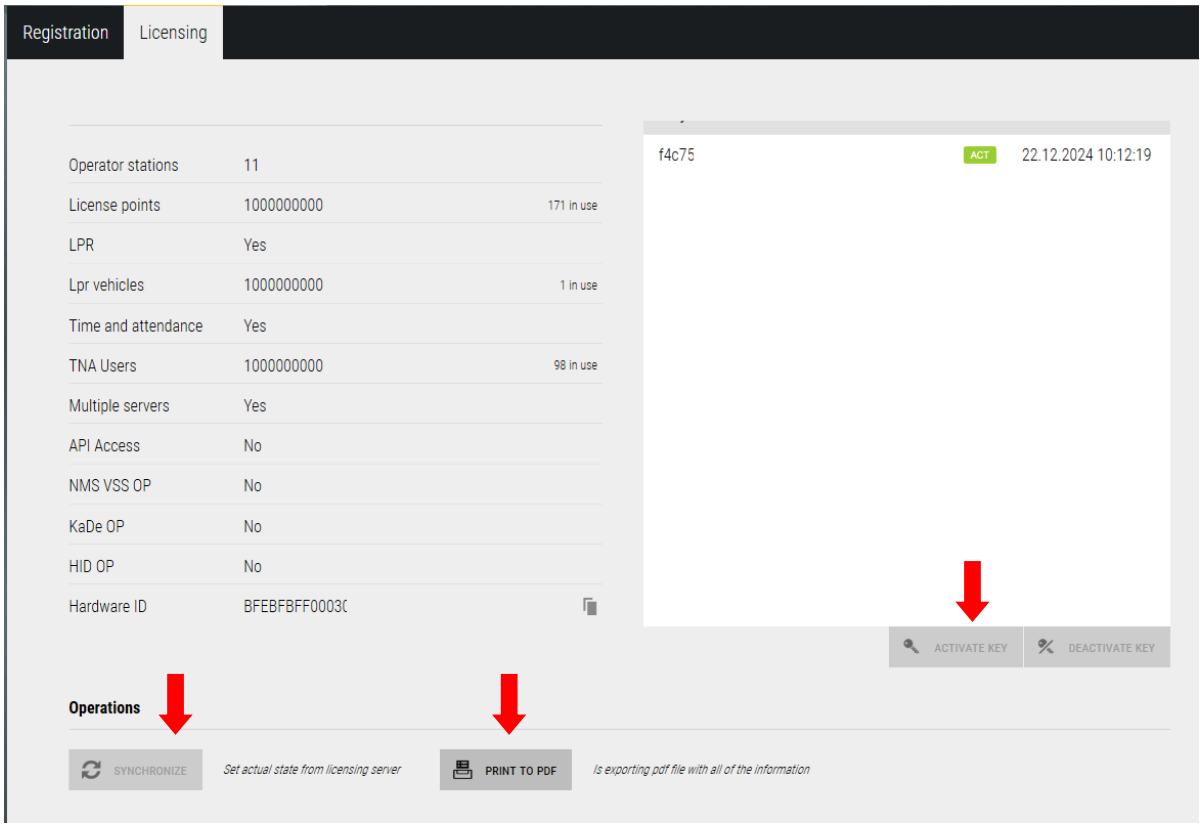
If you register from a computer without Internet access, the following option will appear in the *Upload File* window.



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.



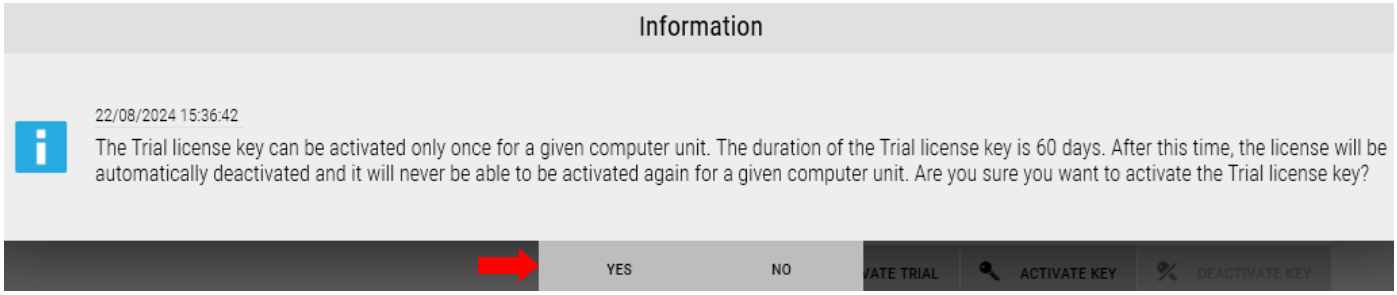
Selecting the SYNCHRONISE option downloads information about the computer unit from the license server (if the computer on which you are synchronizing has access to the Internet. Otherwise, a request.nlic file will be generated. To complete the synchronization process, follow the same steps as described 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.

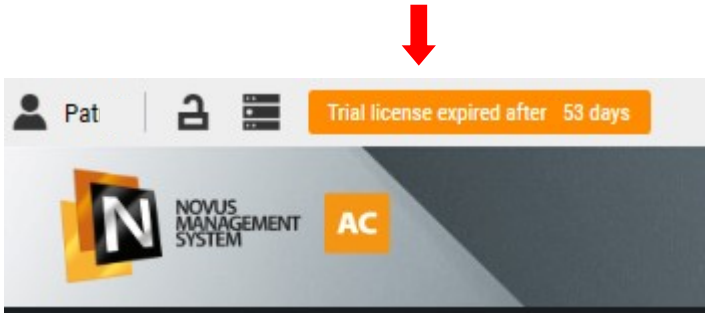
TRIAL license activation

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.

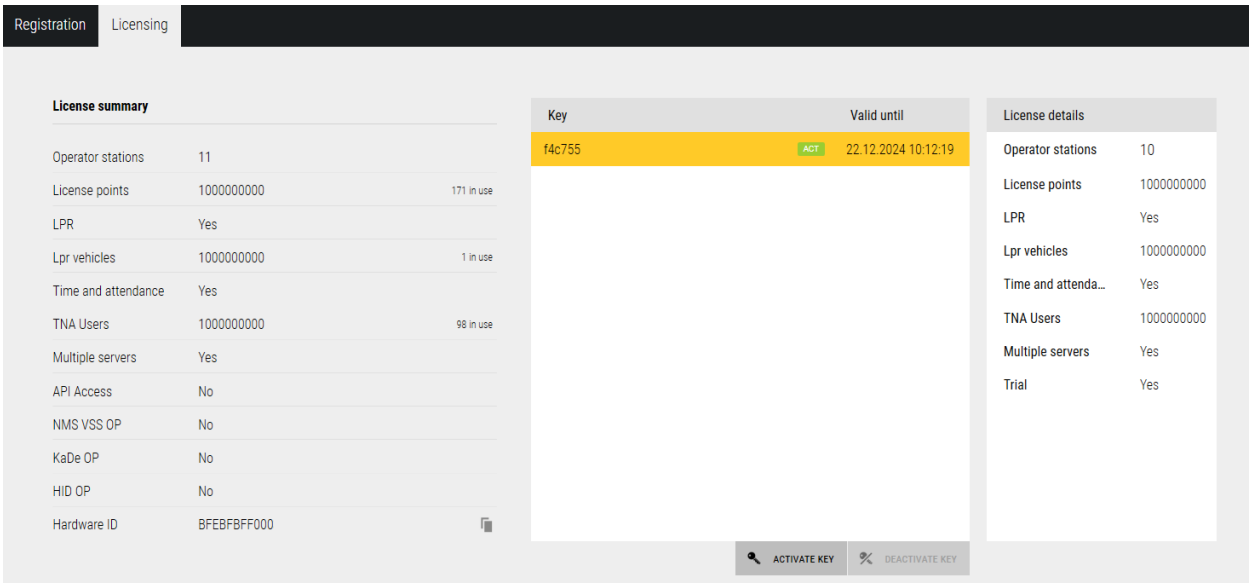


If paid licenses have not been activated, after the expiration of the TRIAL license period, all devices added to the system will be disconnected, but the system configuration will not change. Once the corresponding paid licenses have been purchased and activated, the ability to establish communication 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.



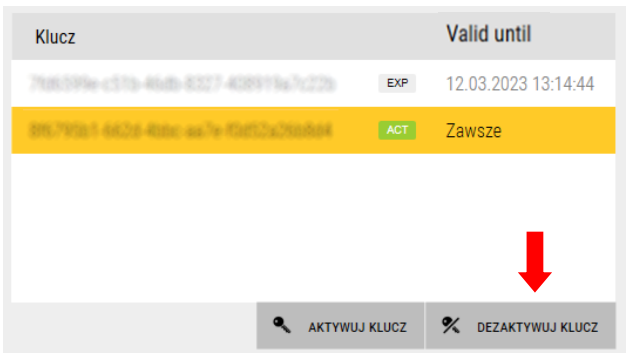
Activation of paid license key

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.

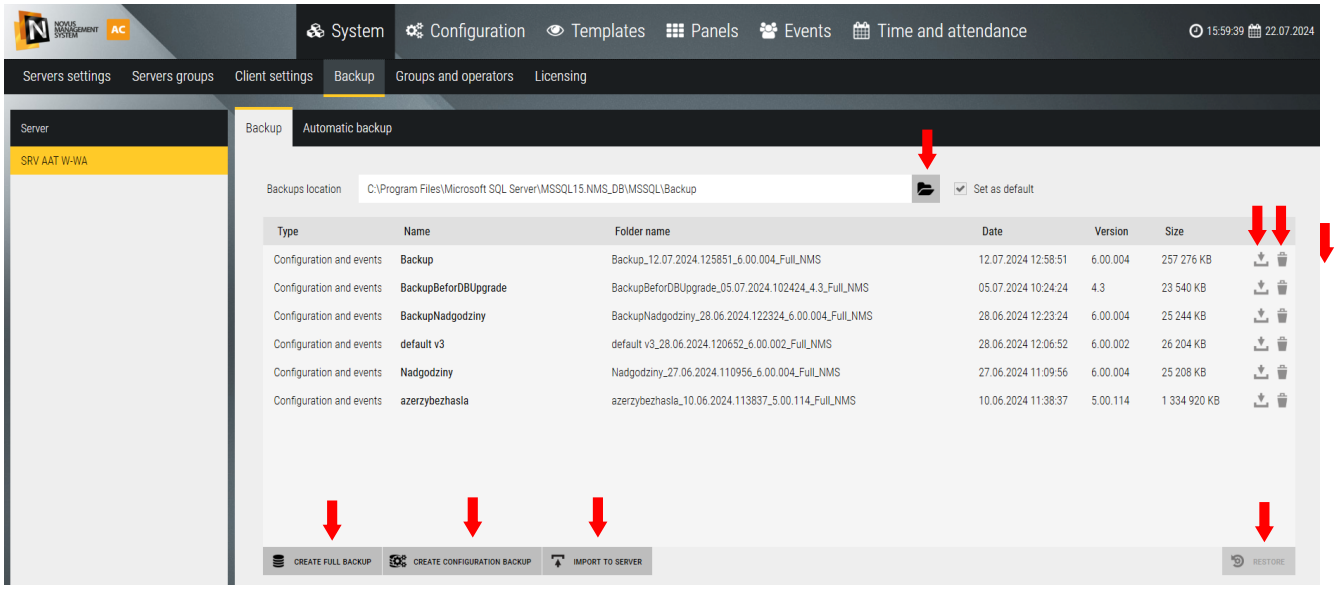


Deactivation of paid license key

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.



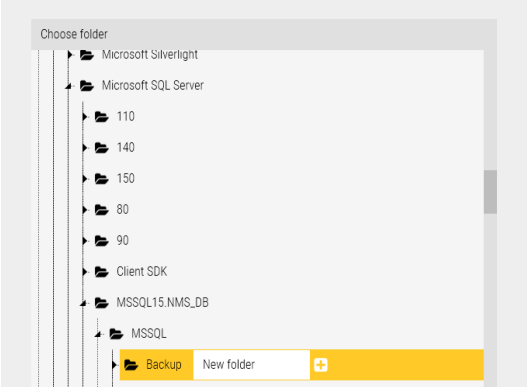
8.4 System backup



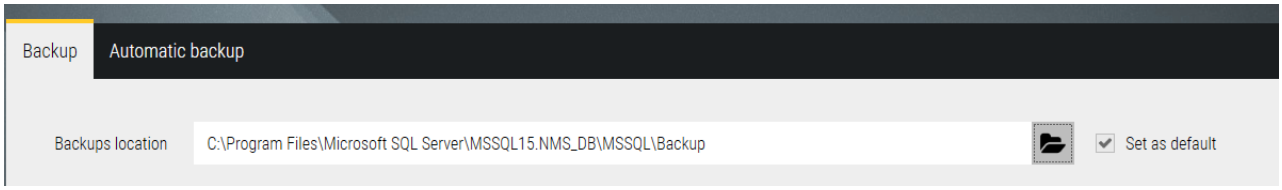
In this tab you can make or restore a backup of the system.

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

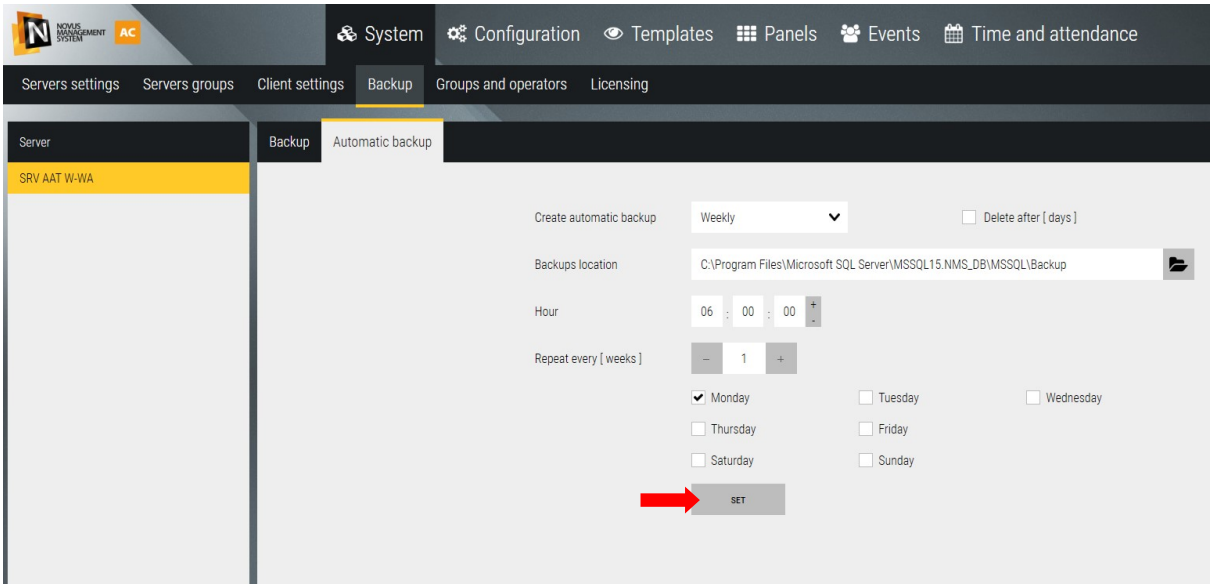
To restore a copy of the system, select it from the list (if the copy file is not on the list, use the IMPORT TO SERVER option), and then select the RESTORE button.

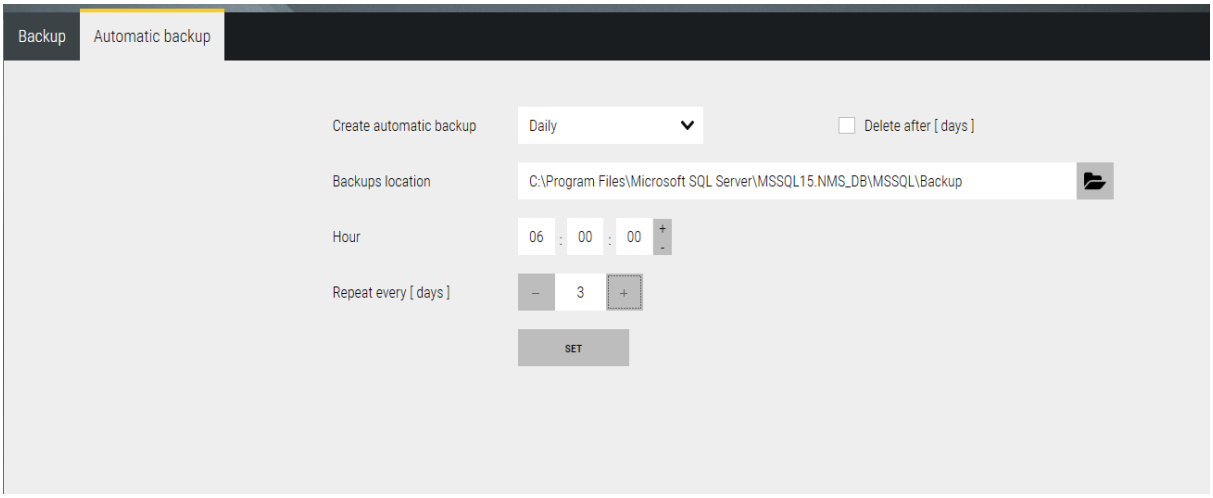
It is also possible to restore the initial state of the system (clearing the database) - for example, after testing the system. To do this, restore the backup under the name Default Settings, which is automatically generated after installing the system.

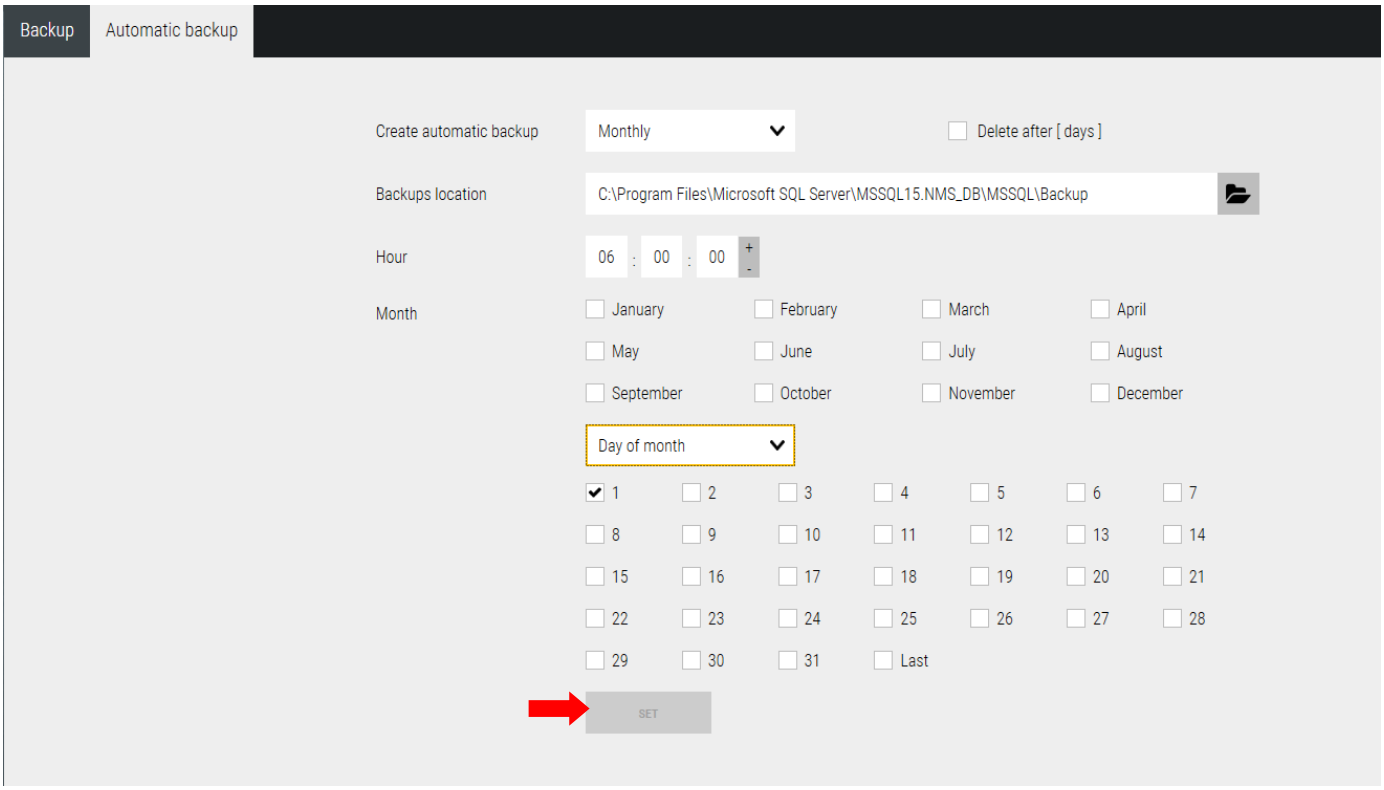
Automatic backup

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

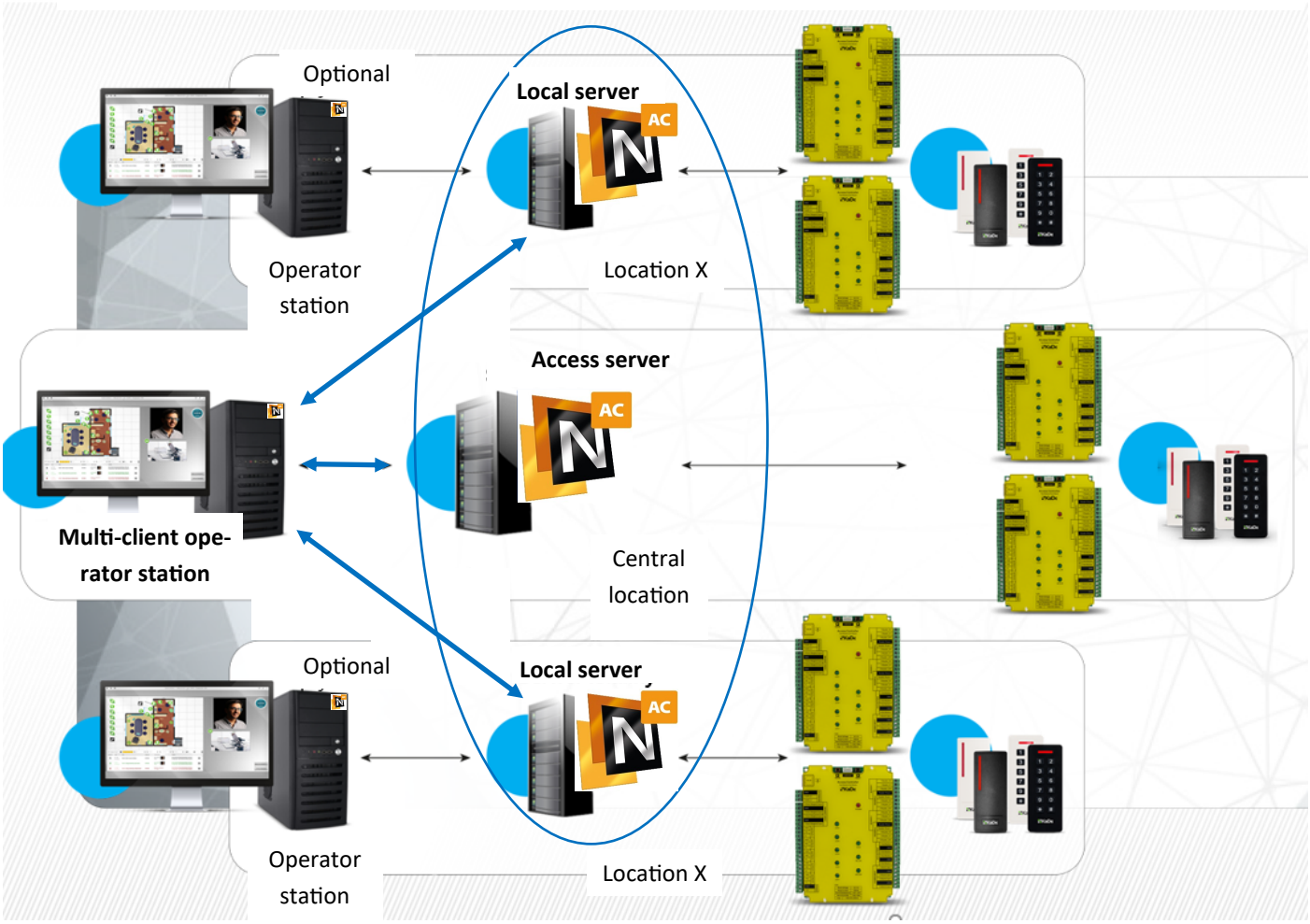
This options is available as a paid license in 4.0 version or higher. It is mainly designed to support systems in multiple locations, but can also be used to support large systems in one location especially if a large number of VSS devices are installed.

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:

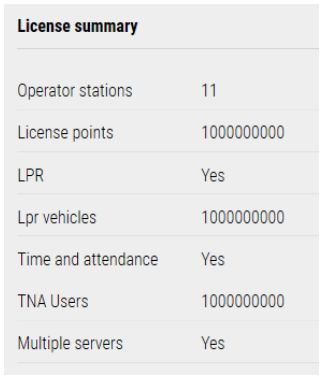
Access server - one server in system with a multi-servere license added, where is group made of local servers (each of them must have an added multi-server license). In the system and even within one group there can be more than one access server.

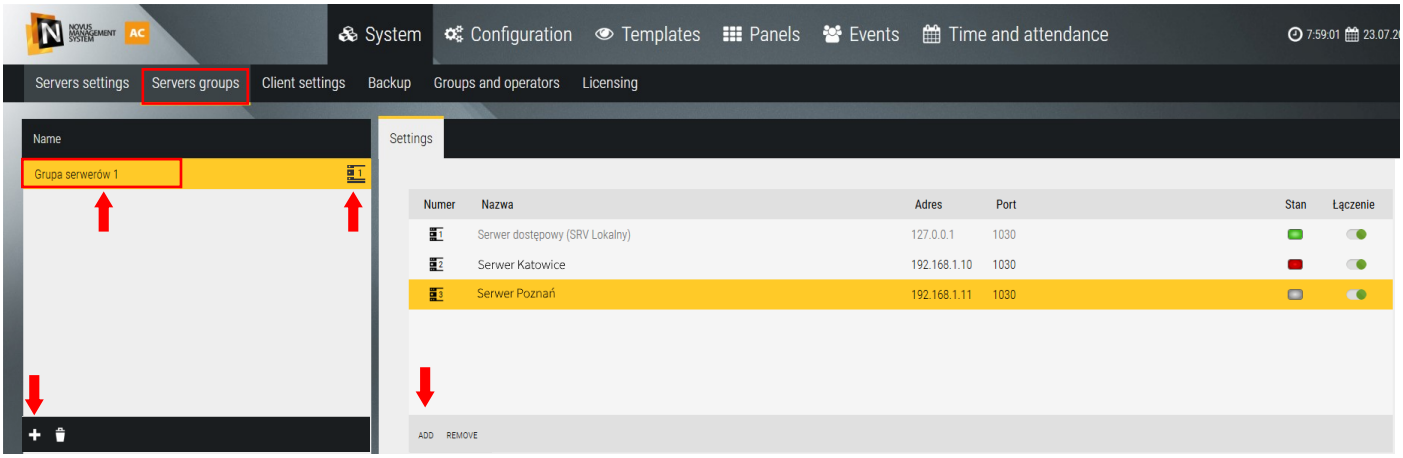
Multi-client - operator station (NOVUS MANAGEMENT SYSTEM AC Client) logged into the access server by an operator with a common login to all servers in the group.

NOVUS MANAGEMENT SYSTEM AC - system with multiple servers



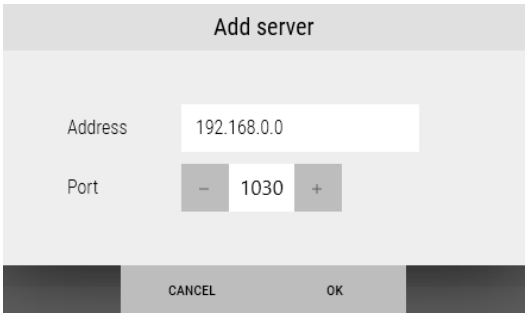
If you want to create a group of servers then the purchase of an additional NOVUS MANAGEMENT SYSTEM AC SRV v5 license is required for each of them . After adding the purchased license to the NOVUS MANAGEMENT SYSTEM AC server, a new tab - Server Groups - will appear in the SYSTEM tab and new icons in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

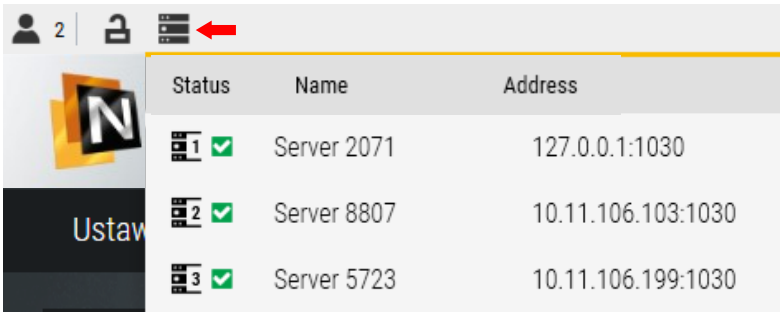




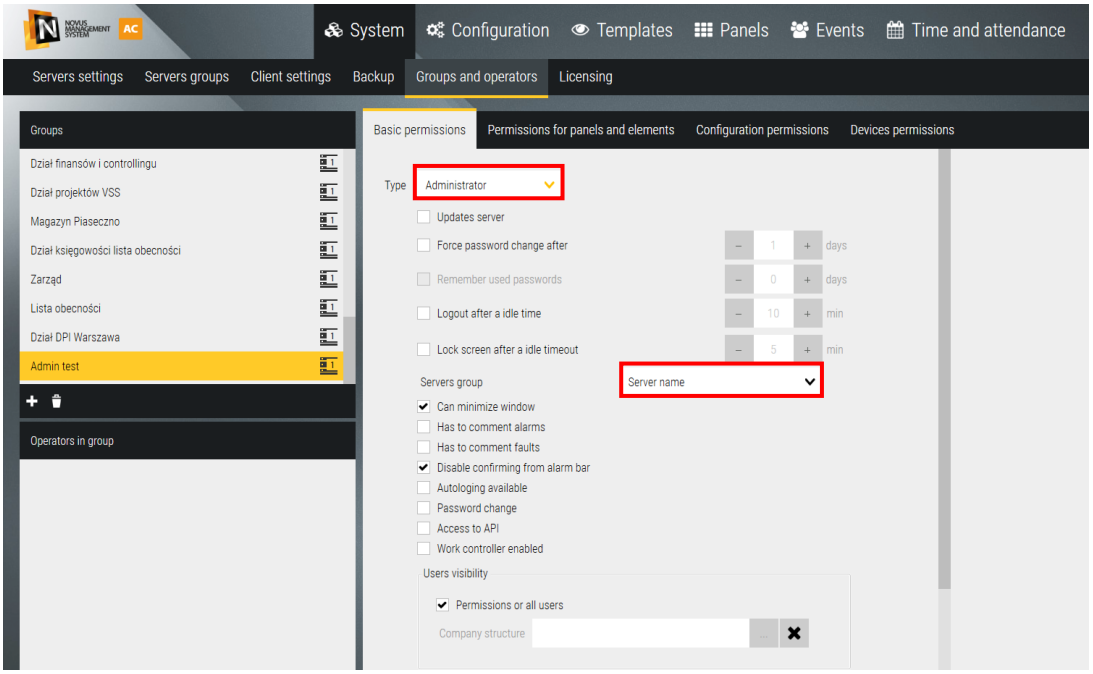
Add - To create a server group, click on the “+” (Add) button in the lower left corner of the window.
Then enter the name of the defined server group in the name field.

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.

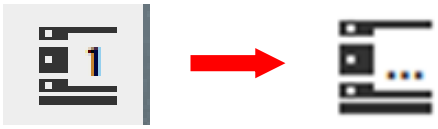


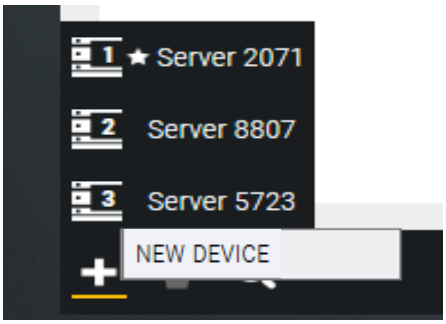


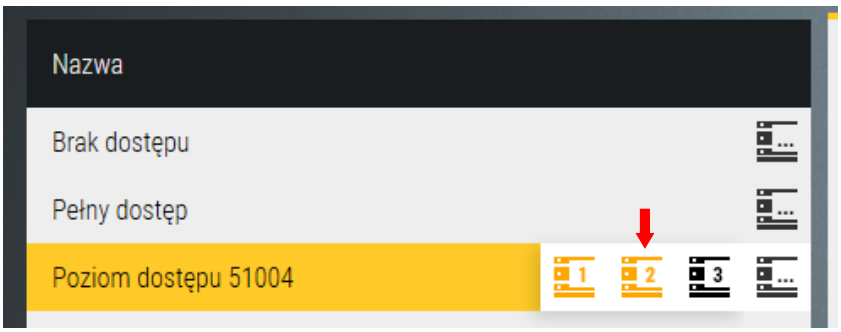
After creating a group of servers, define an operator assigned to that group on each server. This will allow you to access subsystems within the group after logging on to one of the client stations within the group. After adding a multi-server license, a new option - *Server Group* - appears in the defining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

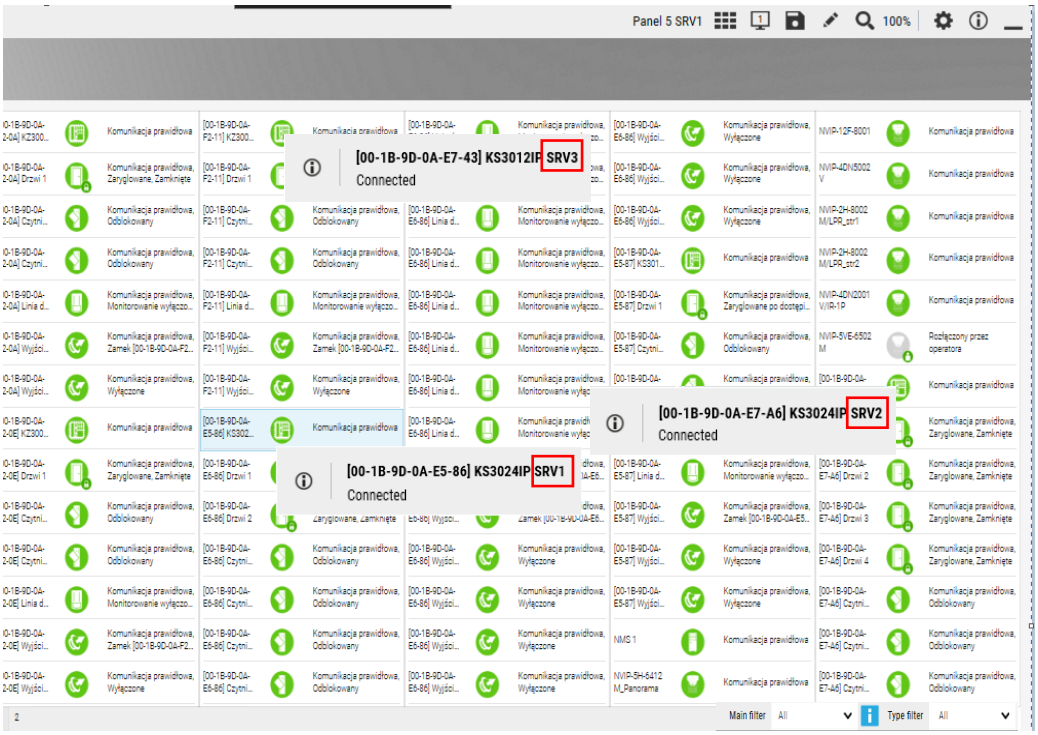






Selected default system items that are the same on servers are in the lists in the left window only once regardless of the number of servers in the group. This applies, for example, to schedules, access levels, holidays.

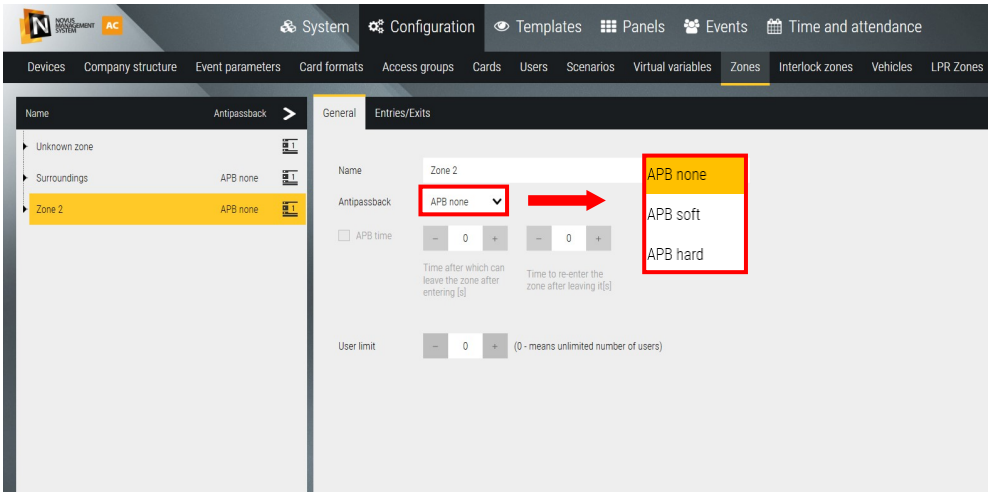
Similarly, this is the case with the synoptic table.



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

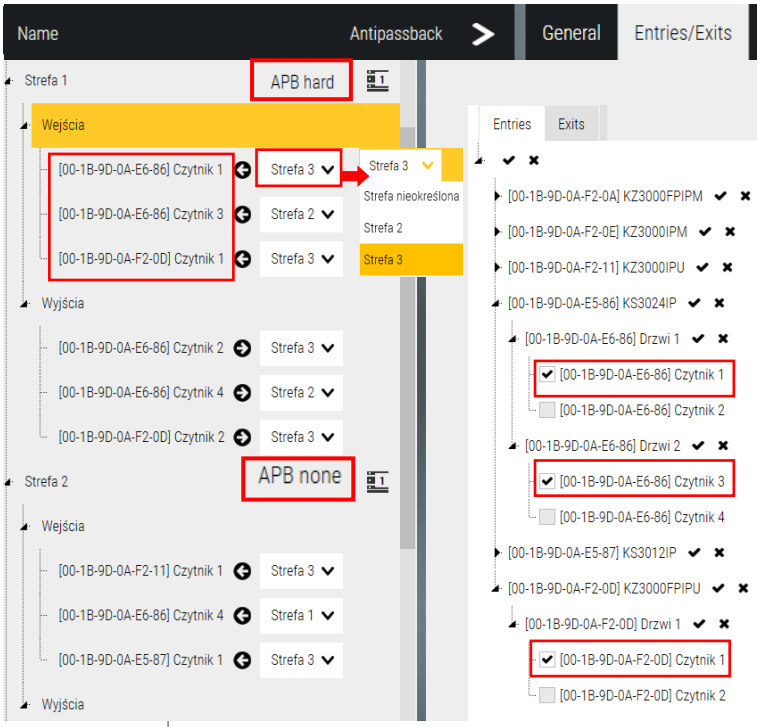
This option is designed to control the status of people and vehicles in areas covered by two-way access control. The global zone can include readers from many controllers, supports both hard, soft and timed antipassback. The function works only in online mode when the NOVUS MANAGEMENT SYSTEM AC server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

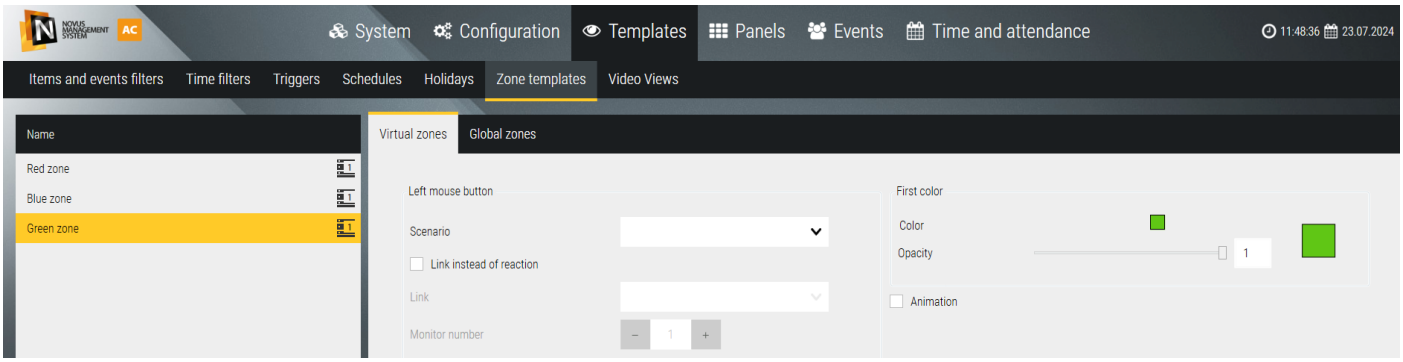
Before defining the zones, it is advisable to make a sketch on the plan of the facility or site, marking the periphery of the zones and the location of the entry/exit readers.



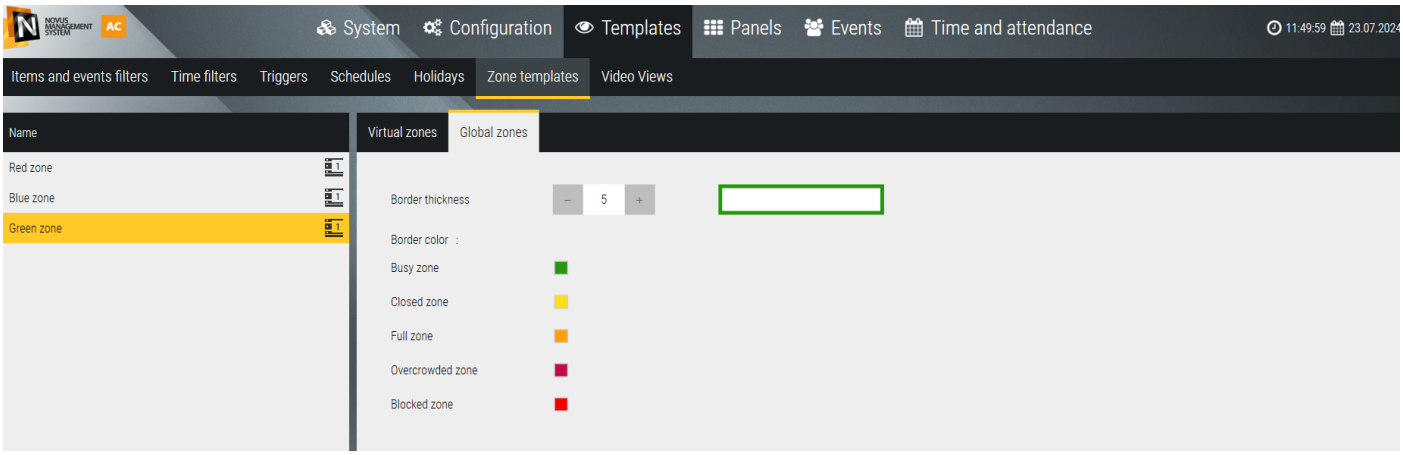
After clicking on the “Add” button, a new item Zone X appears on the list in the left window - we can assign entry and exit readers to it in the right window. After assigning entry and exit readers, go to the left window and assign to each reader from the drop-down list the zone in which the reader is 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

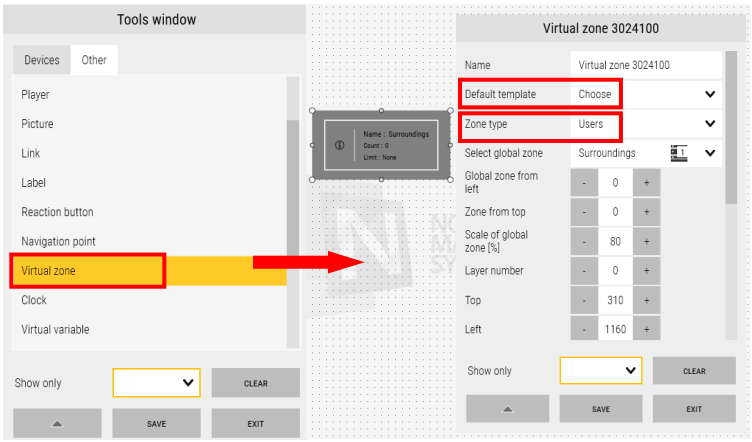
Global zones can be on panels to monitor their status and rewrite users on lists in zones if there is a need to organize their status. On panels, global zones are linked to virtual zone templates. Therefore, you should first define virtual zone templates to which global zones will be assigned on panels.



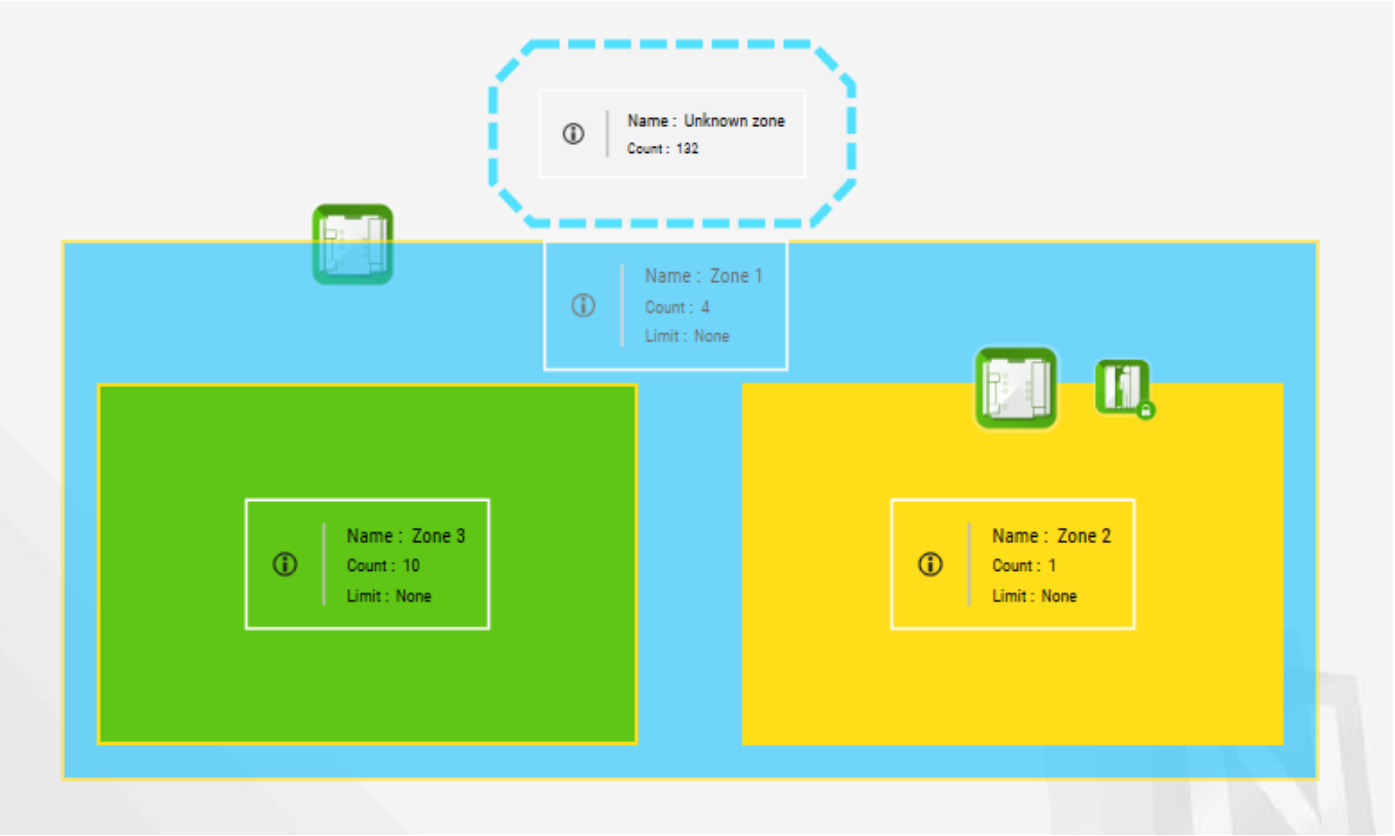
The parameters of the virtual zones are shown above. If you use them to visualize global zones, you need to select a differentiated background color. Next, go to the Global Zones tab and set the thickness of the border on the edge of the virtual zone, the color of which indicates the status of the zone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

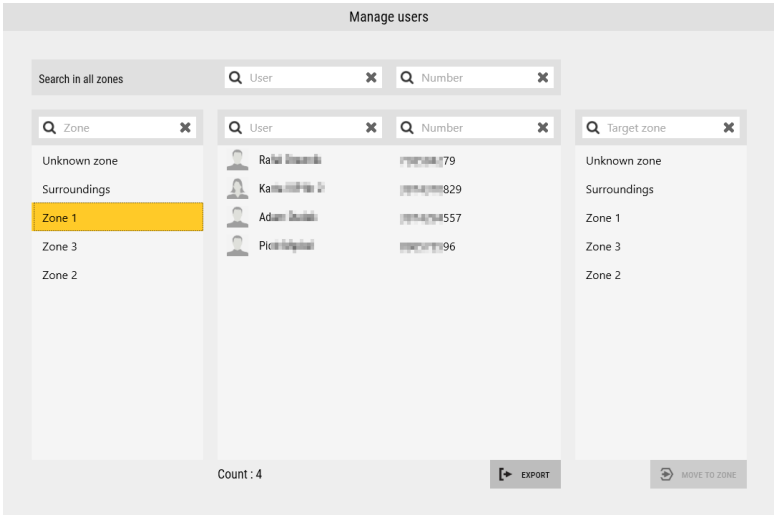


Then modify the parameters of the virtual zone and the global zone (location, size, scale) and save.



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:



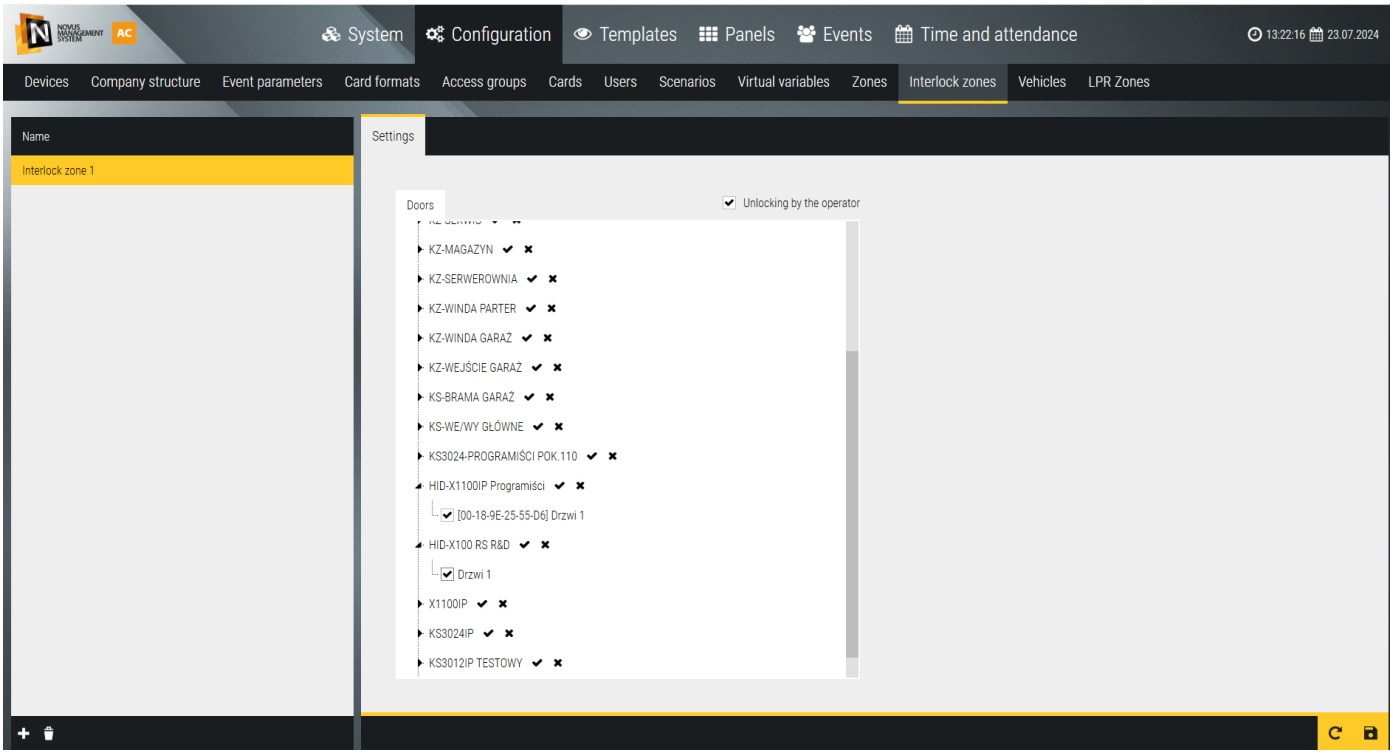


The window displays a list of registered people in the zone. After selecting one or more items in the list (with CTRL) and the zone in the right window, you can rewrite them to this area. You can also export the list of users to a file (*.CSV) and print it.

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.

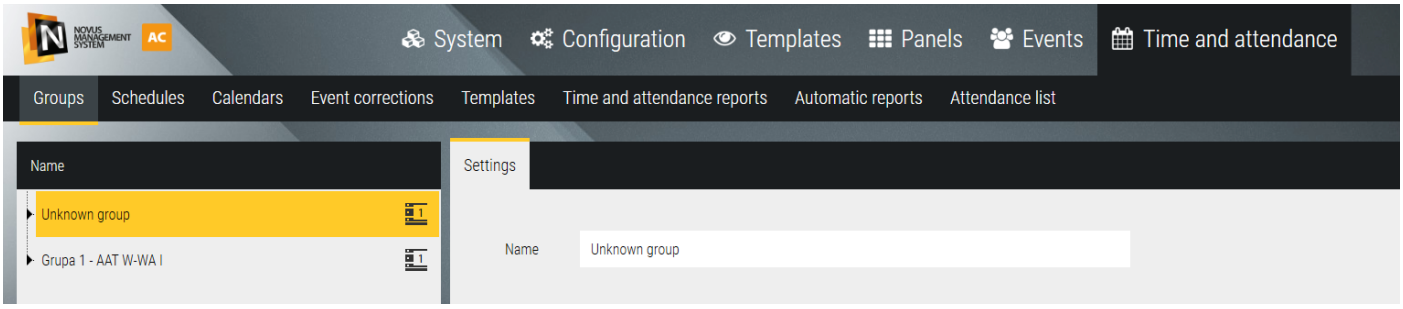
To define a door group for a particular lock, click on the + icon in the lower left corner of the window.



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.

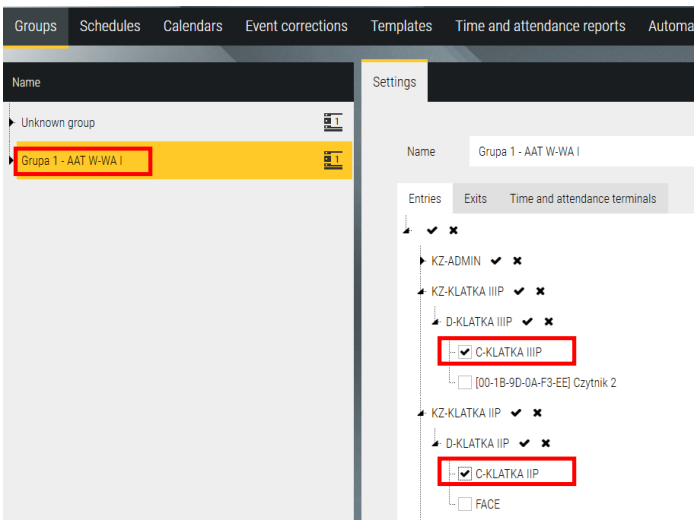


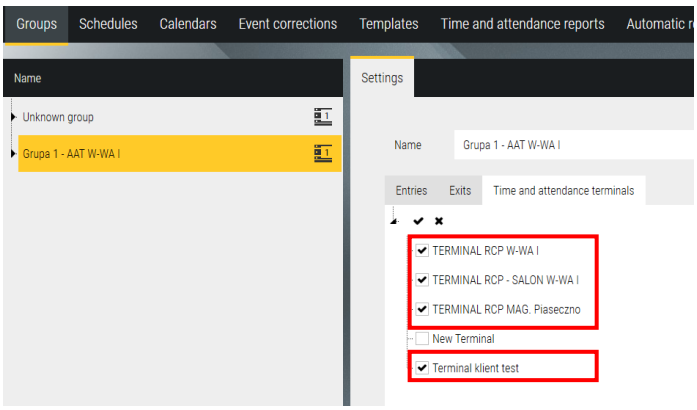
The T&A terminal allows registration of additional I/O during work time: for break, business, private. Registration of these additional I/O during work time is also possible on KD readers - one reader for one type of I/O.

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.

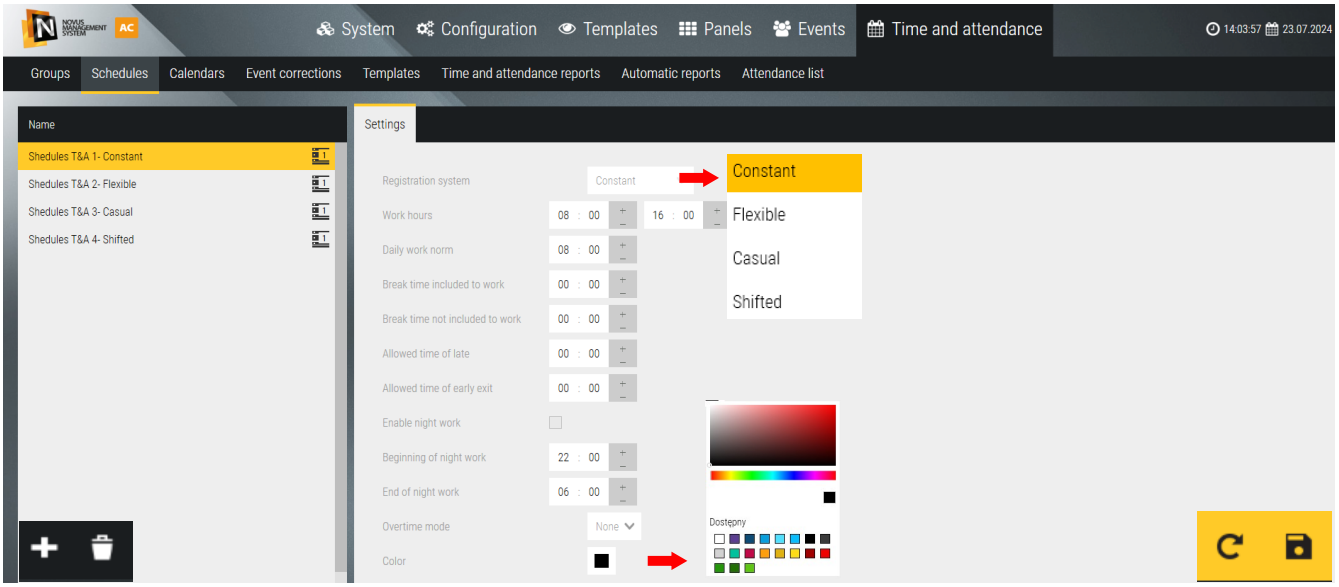
Terminals should be added using the *Time Terminals* tab.



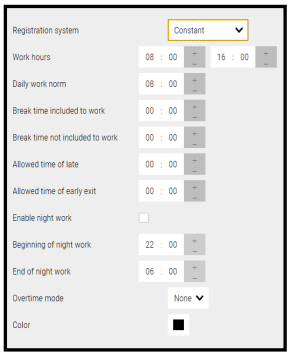


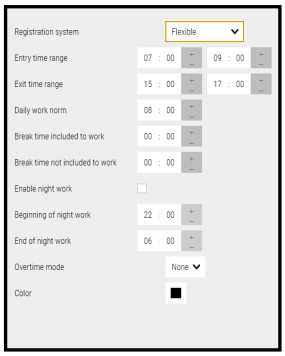
Schedules

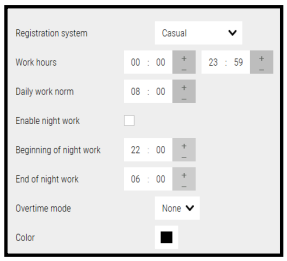
T&A schedules are needed to account for working time in the selected period according to the established daily norm. After clicking on the "+" Add button in the left window, a new schedule appears with a default name that can be edited.

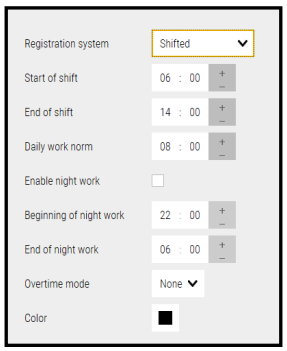


Next, in the Settings tab, select the type of registration system: *Constant, Flexible, Casual, Shift.*









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.

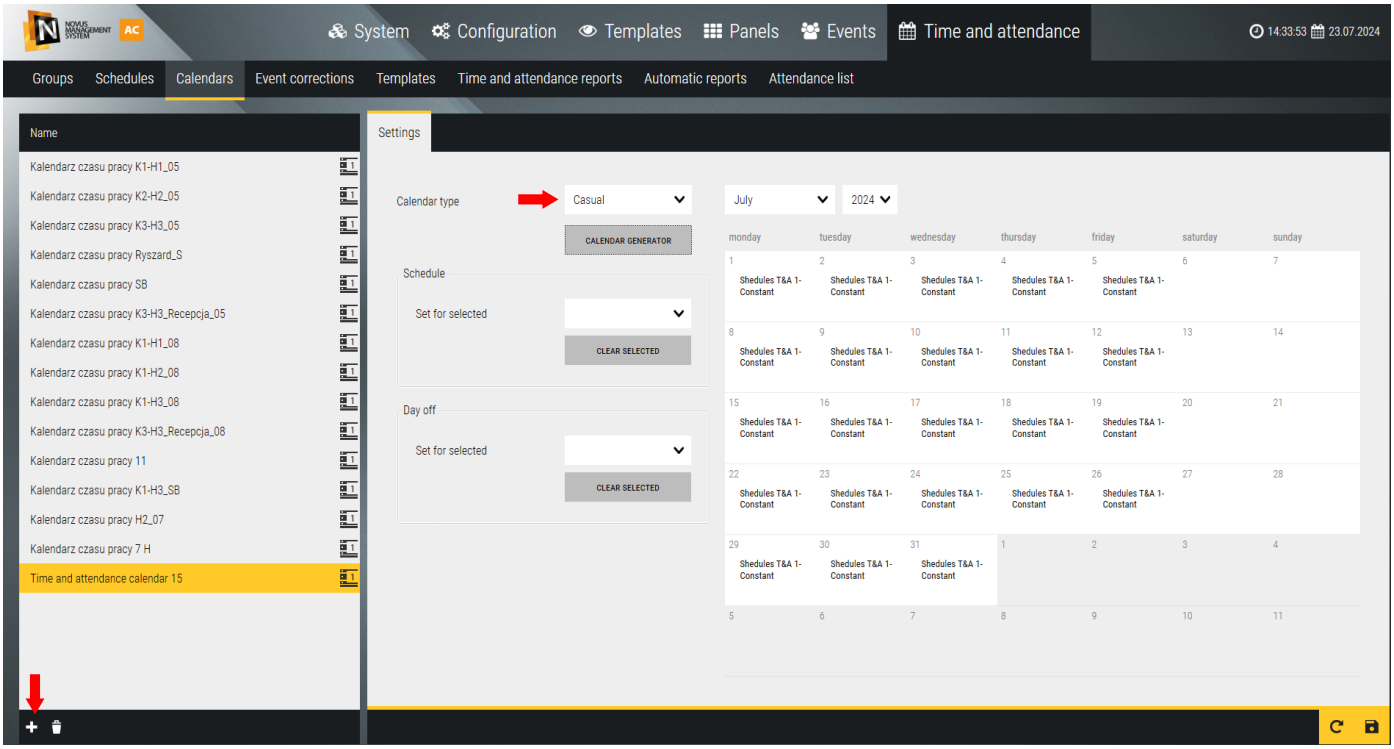
Flexible - means that the employee will have a daily norm of working time to calculate the monthly norm (after multiplying by the number of days to be worked in the month according to the calendar).
Entry time range - set the time range in which the employee should register the start of work. Only registrations 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

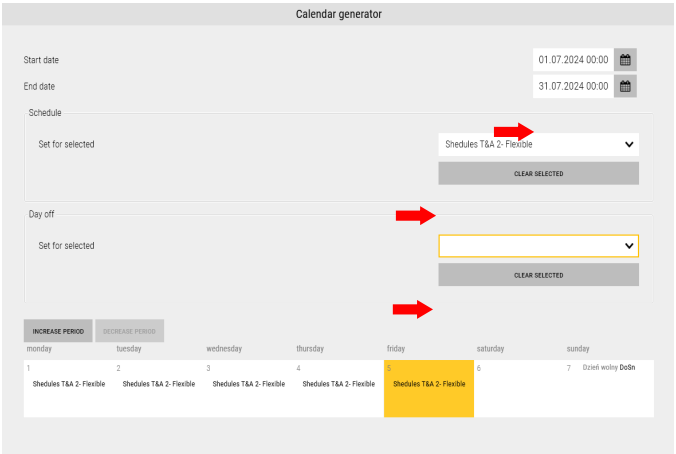
Calendars are needed to account for working time in the set period according to the norm. When defining them, you need to assign a selected schedule to each working day of the week. The calendar is then assigned to the user. After clicking on the "+" *Add button* in the left window, a new calendar appears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



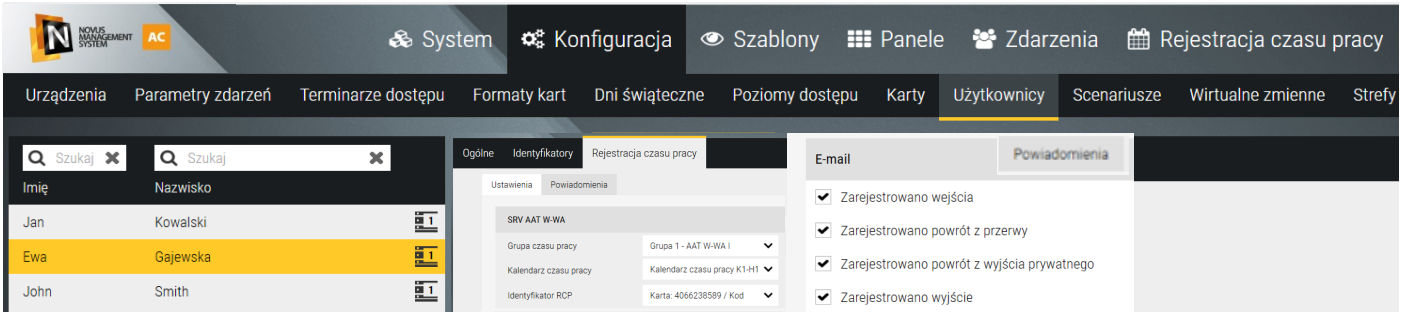
Manual mode - to assign the selected schedule manually, click on a particular day with the left mouse button, with the right one - to remove it

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

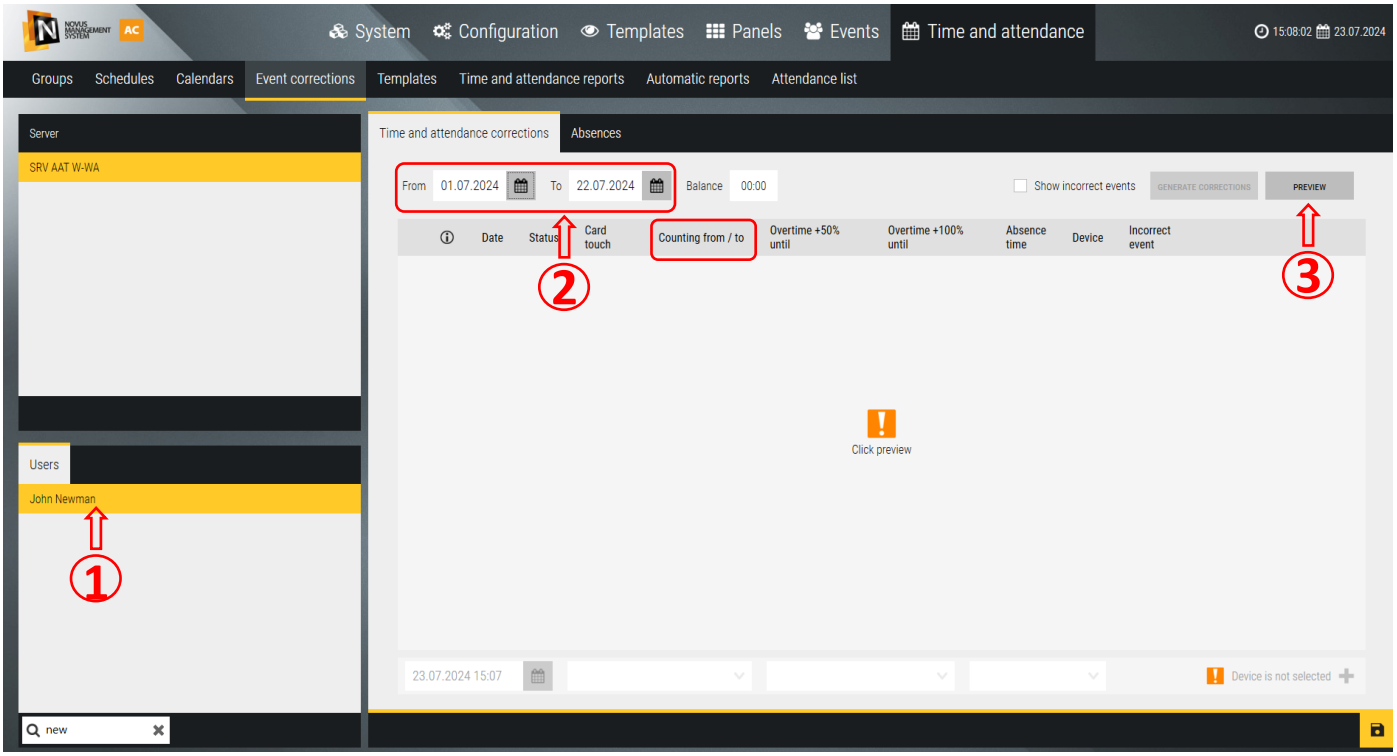
For shift mode, set the cycle according to the number of shifts by clicking on the *Increase/Decrease* cycle buttons. The example opposite shows a cycle for a system with three shifts per day. In the first week, set the schedule for the first shift, in the second week for the second shift, and so on. 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

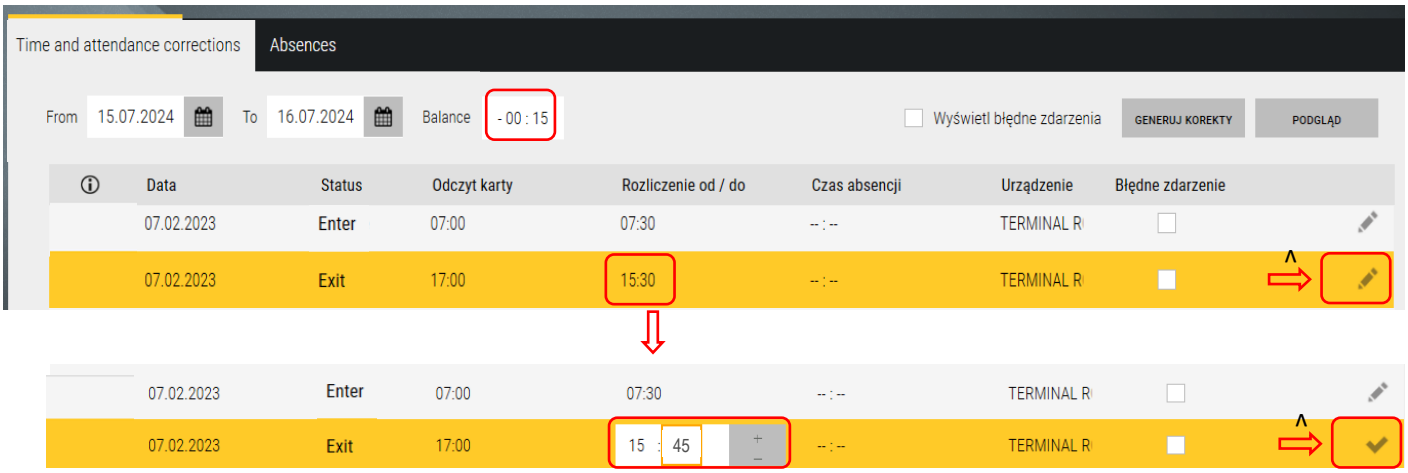


To make changes to the working time of a particular employee, in the *t&A corrections* sub-tab, you need to do it one by one:

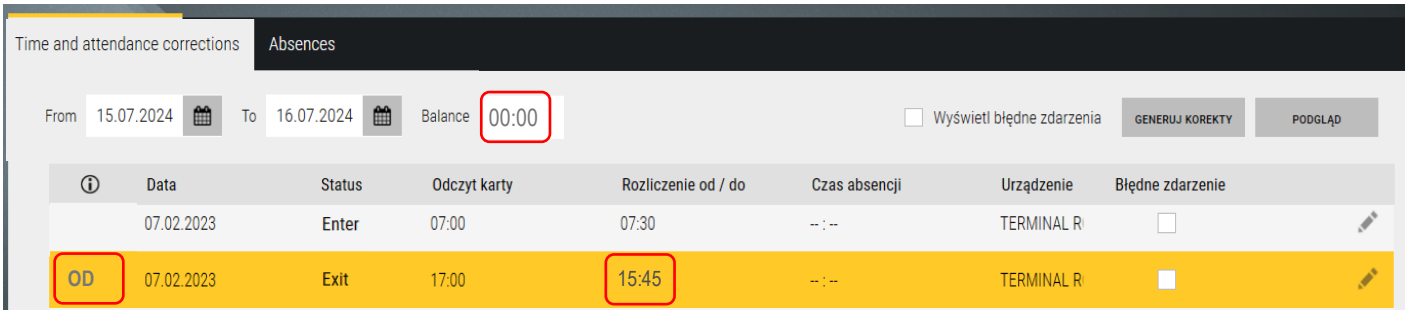
1) select the appropriate user on the left
2) The upper part of the window displays the range of days covering the default accounting period (from the beginning of the month to the end of the previous day) and the balance calculated for this period. You can set a different date range.
3) Click *Preview*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



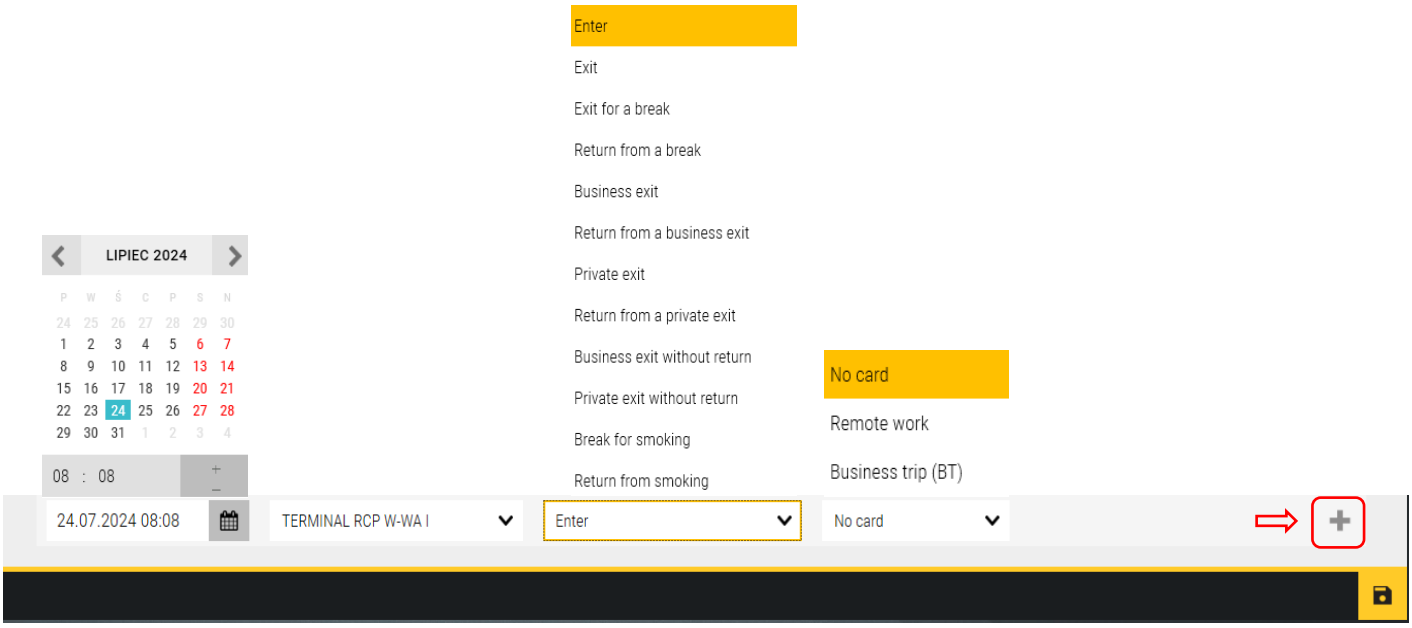
"Reserve" time on exit is 01:30 hours on 07.02.2023.
The balance and the end time of the work after the adjustment of the work-off.



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.

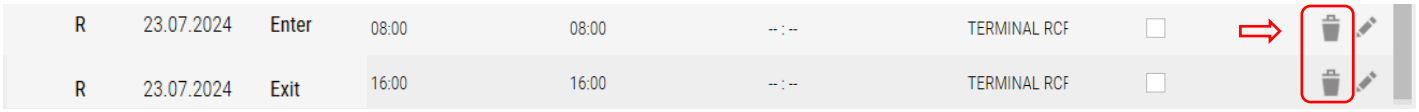
It is possible to make modifications both within the registered event as described on the previous page, as well as to add a completely new event (for example, when an employee fails to read the card in connection with work performed remotely - *R*).
In this case, do the following in the line at the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



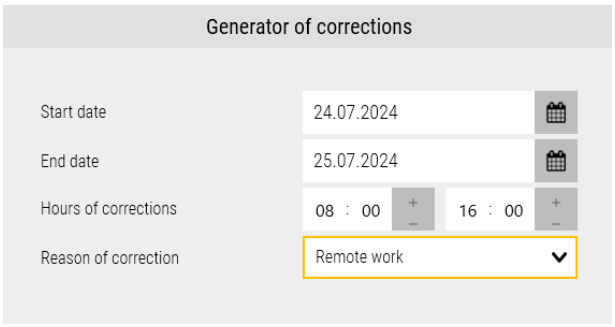
5)

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



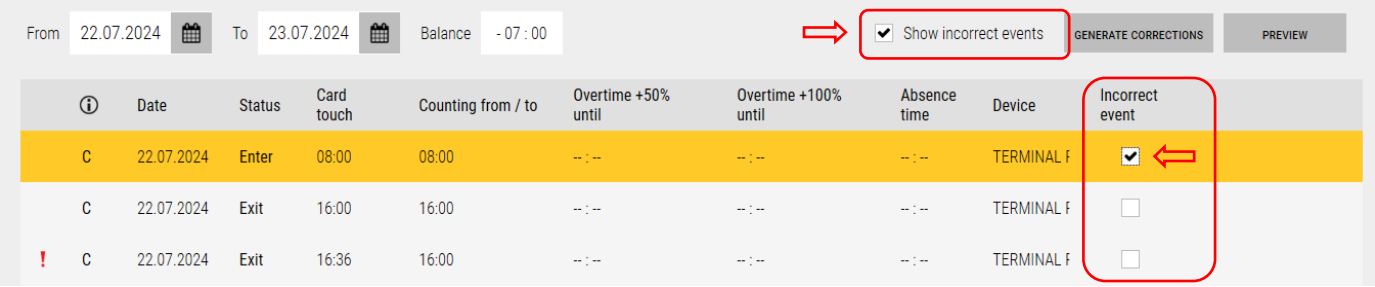
The added *enter/exit* will appear in the list and, after saving and clicking Preview, also on the Time Adjustments tab after selecting the appropriate date range. You can delete it by clicking on the *Trash* icon. The added adjustment requires saving (Diskette).

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



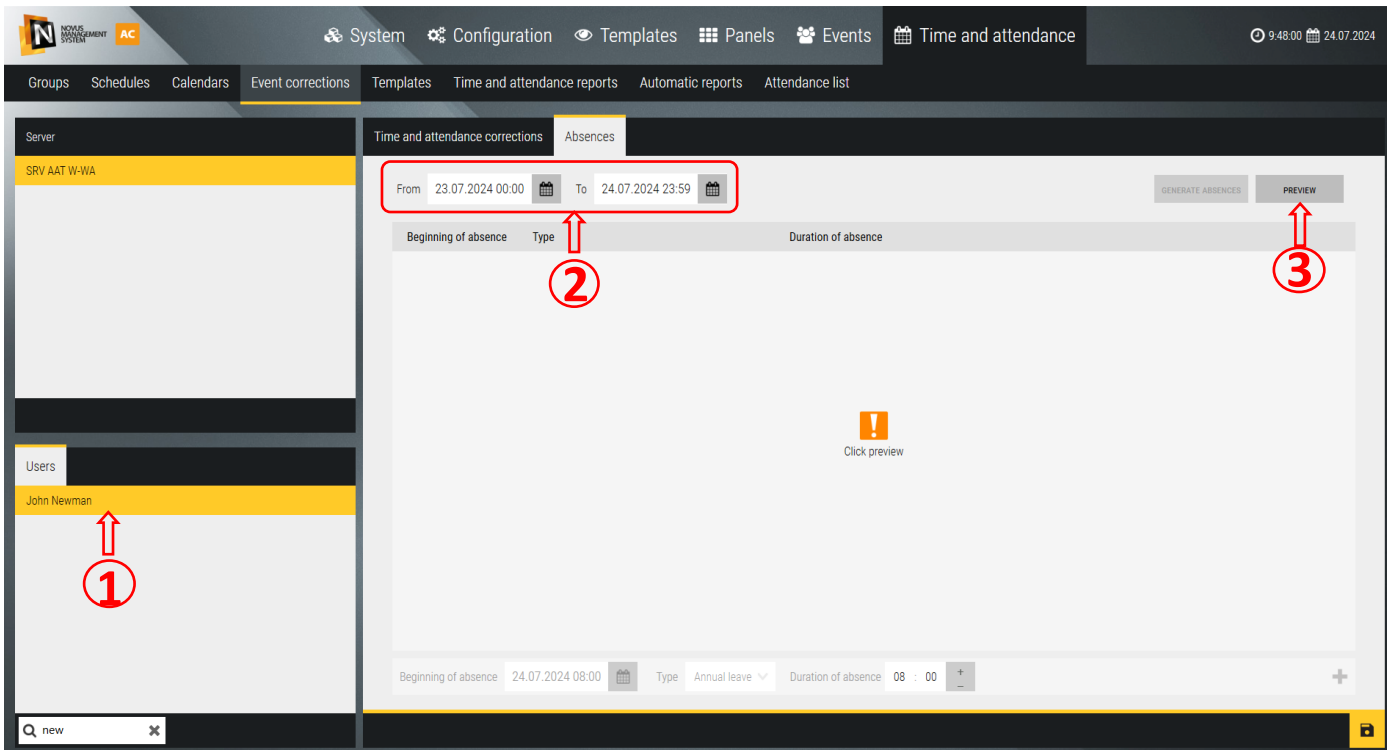
2) Click save *(Floppy disk icon).*

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:

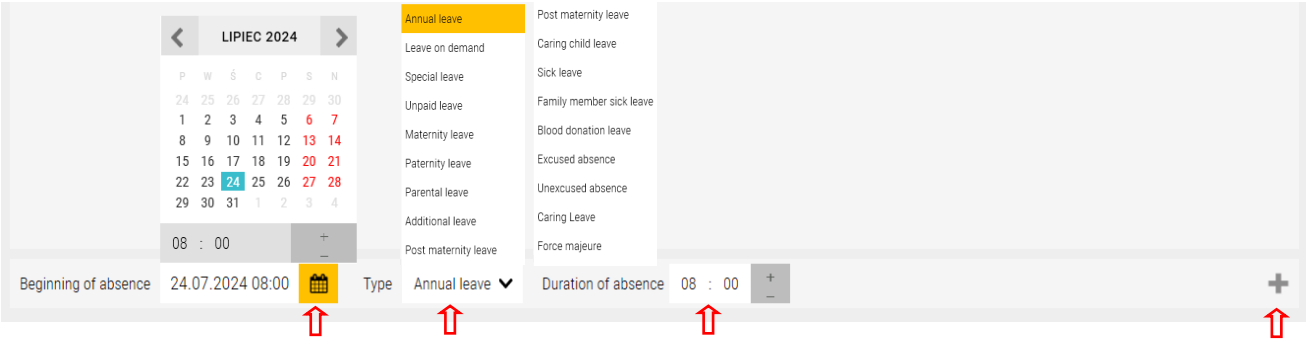
1) on the left, select the appropriate employee
2) select the period within which you want to make modifications
3) Click *Preview* in the upper right corner.



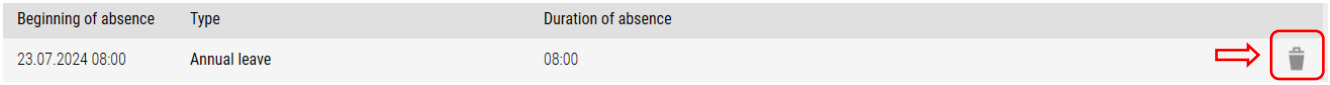
The operations performed above will generate a list of all employee absences in the selected period in chronological order. In case of their absence - the window will remain empty.

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).*

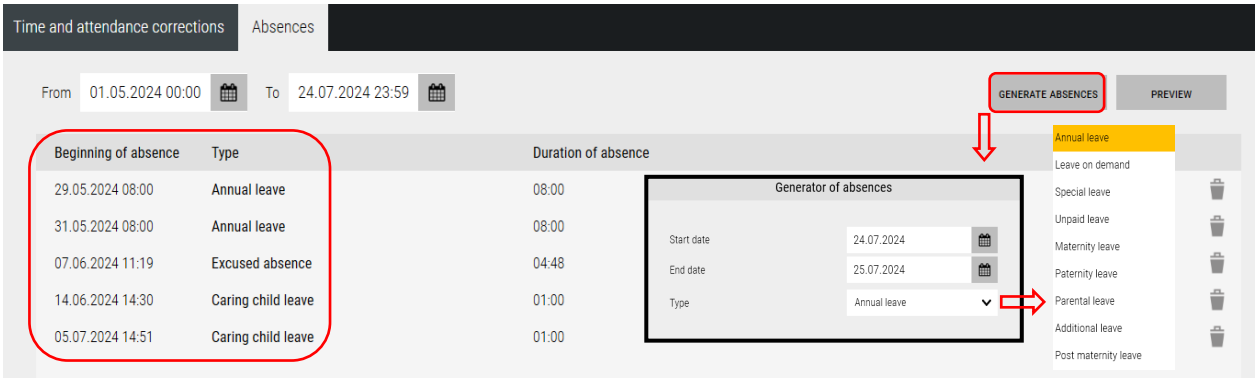


Tip:

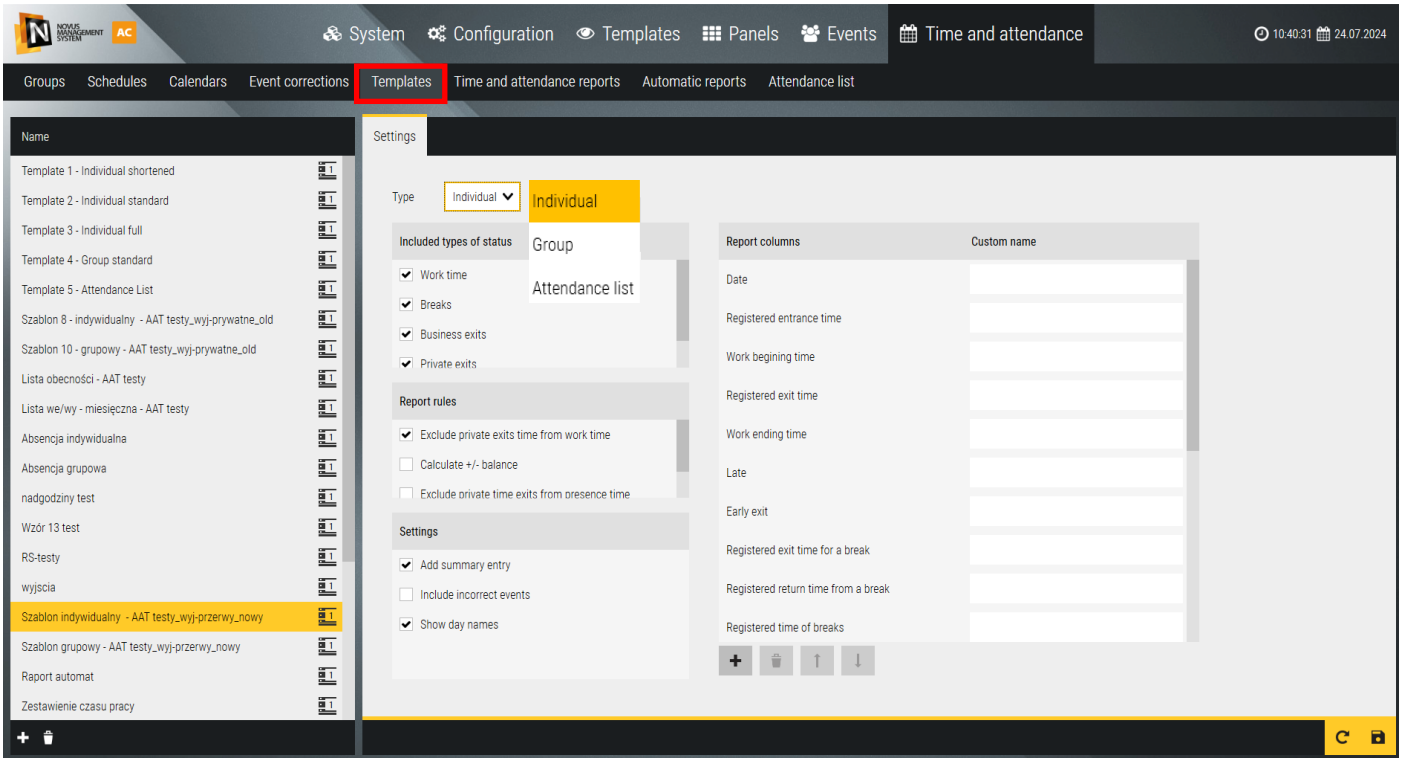
If the absenteeism covers several consecutive days, it is worth using the absenteeism generator. To do this, on the *Absences* tab:

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.

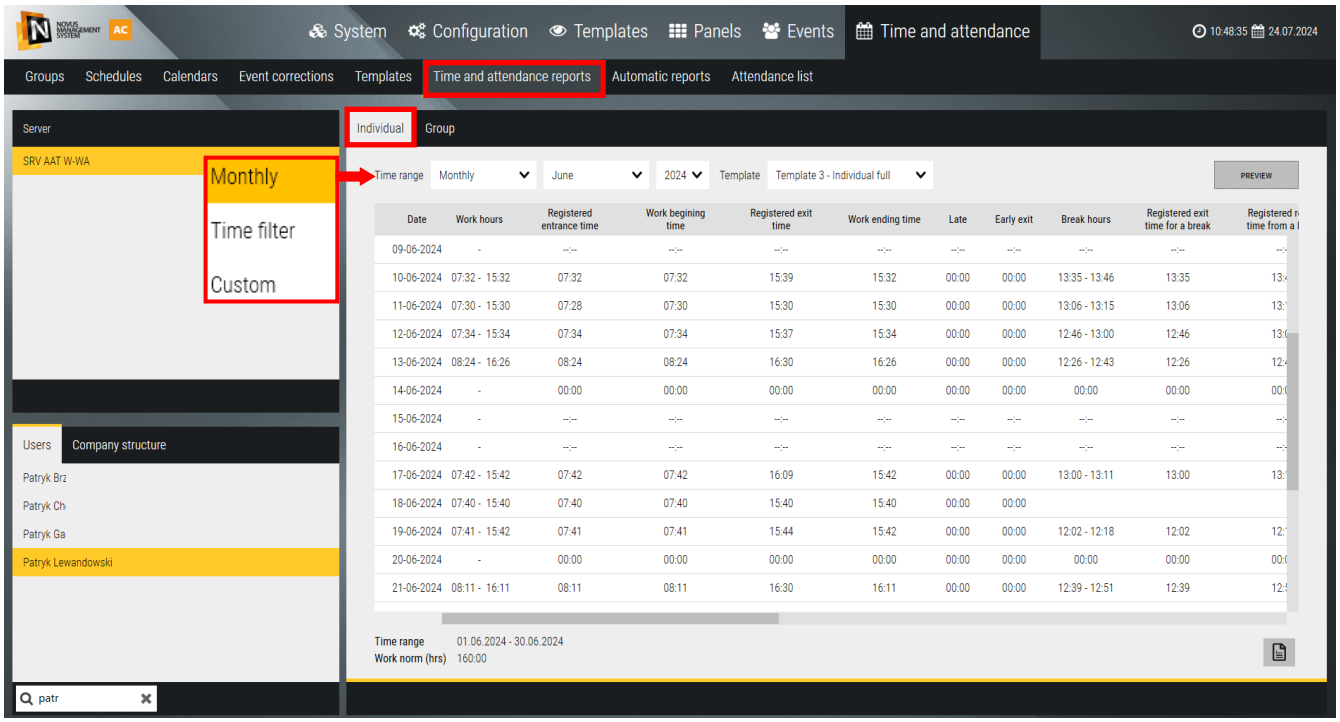
Include type of status - select which types of work status are to be included in the report. These settings affect the appearance and calculation of working time.

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

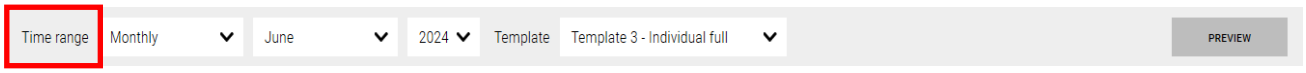
Setting - allow you to specify the appearance of the report form.

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

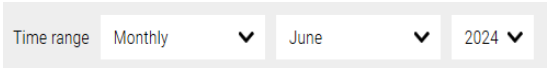


Individual report accounting for employee working time is generated on the basis of events from input/output readers assigned to T&A groups. On the top bar we have filters that allow us to set the parameters of the report:

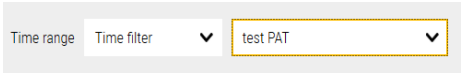


In terms of time, we have a choice of three options:

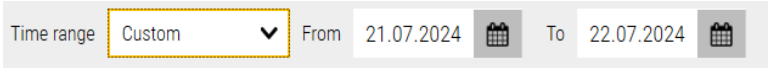
1. From the whole month (previous month by default)



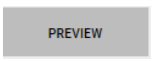
2. From the time range set in the selected time filter



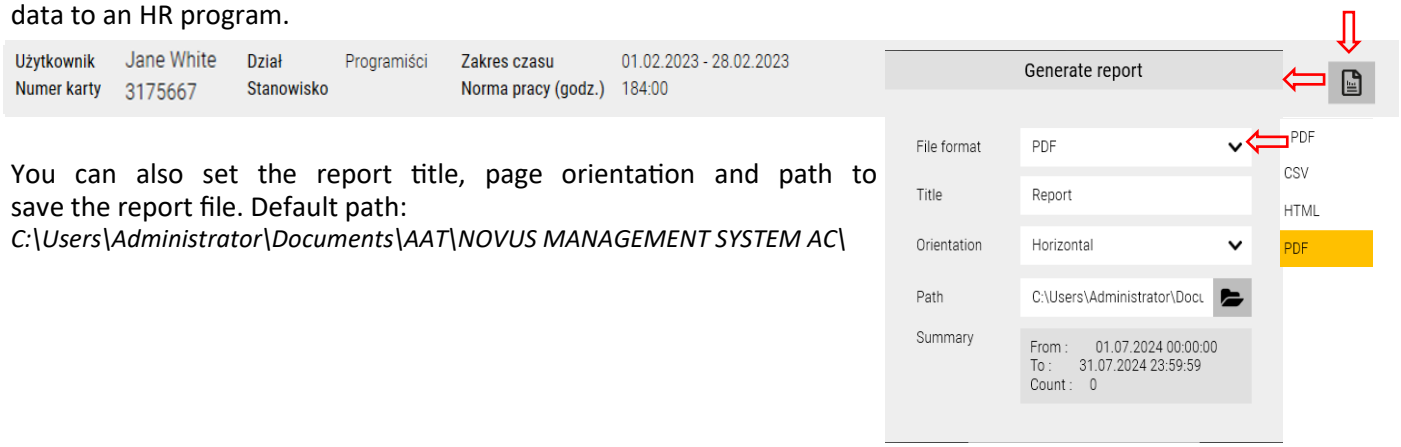
3. From the range defined by the calendar



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.

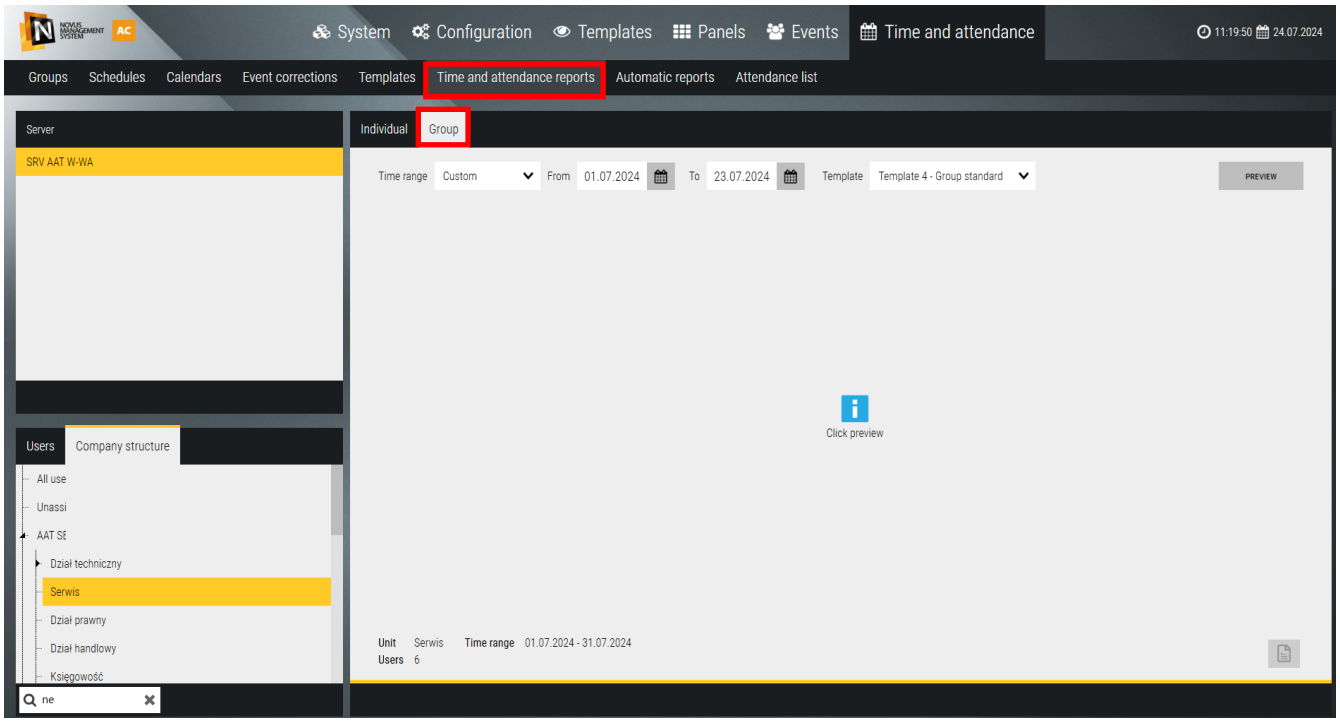


The report will be displayed on the screen. A summary is displayed at the bottom of the report.
The displayed report provides a line-by-line summary of hours worked on a single day, covers the selected date range, and can be saved to a file in HTML, PDF or as an editable file in CSV format. The latter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

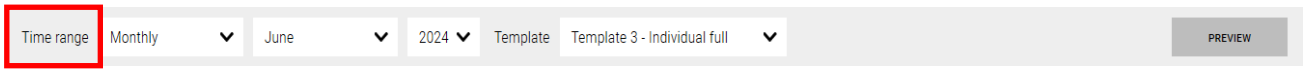


You can also set the report title, page orientation and path to save the report file. Default path:
C:\Users\Administrator\Documents\AAT\NOVUS MANAGEMENT SYSTEM AC

Group report

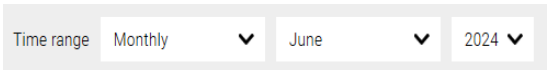


The group report accounting for the working time of the selected department is generated on the basis of events from entry/exit readers assigned to T&A groups. On the top bar we have filters to set the report parameters:

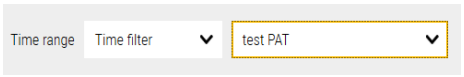


In terms of time, we have a choice of three options:

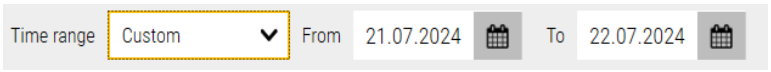
1. From the whole month (previous month by default)



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

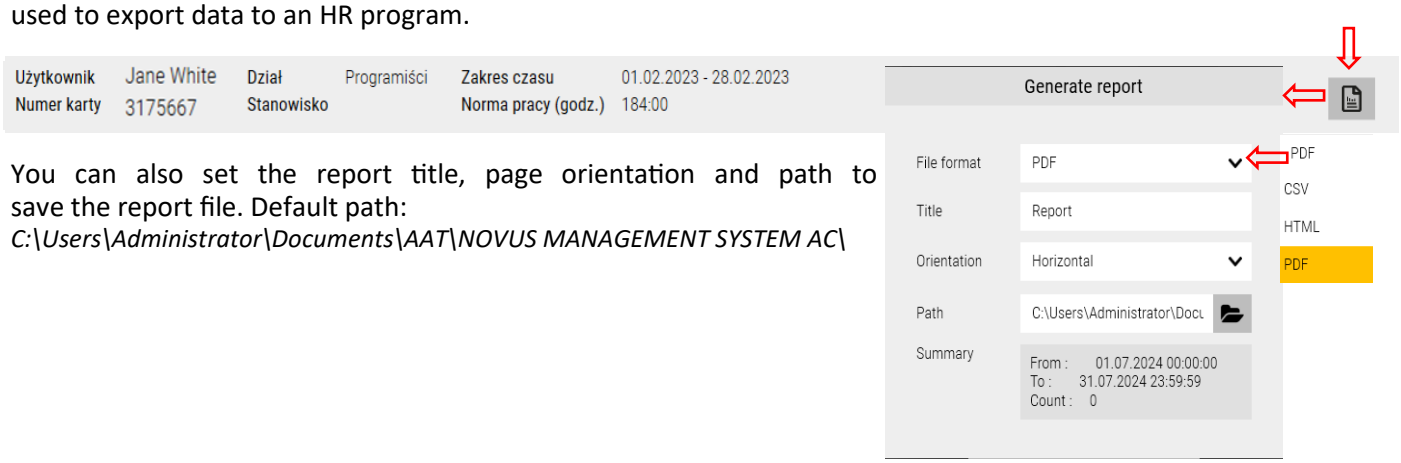


3. From the range defined by the calendar



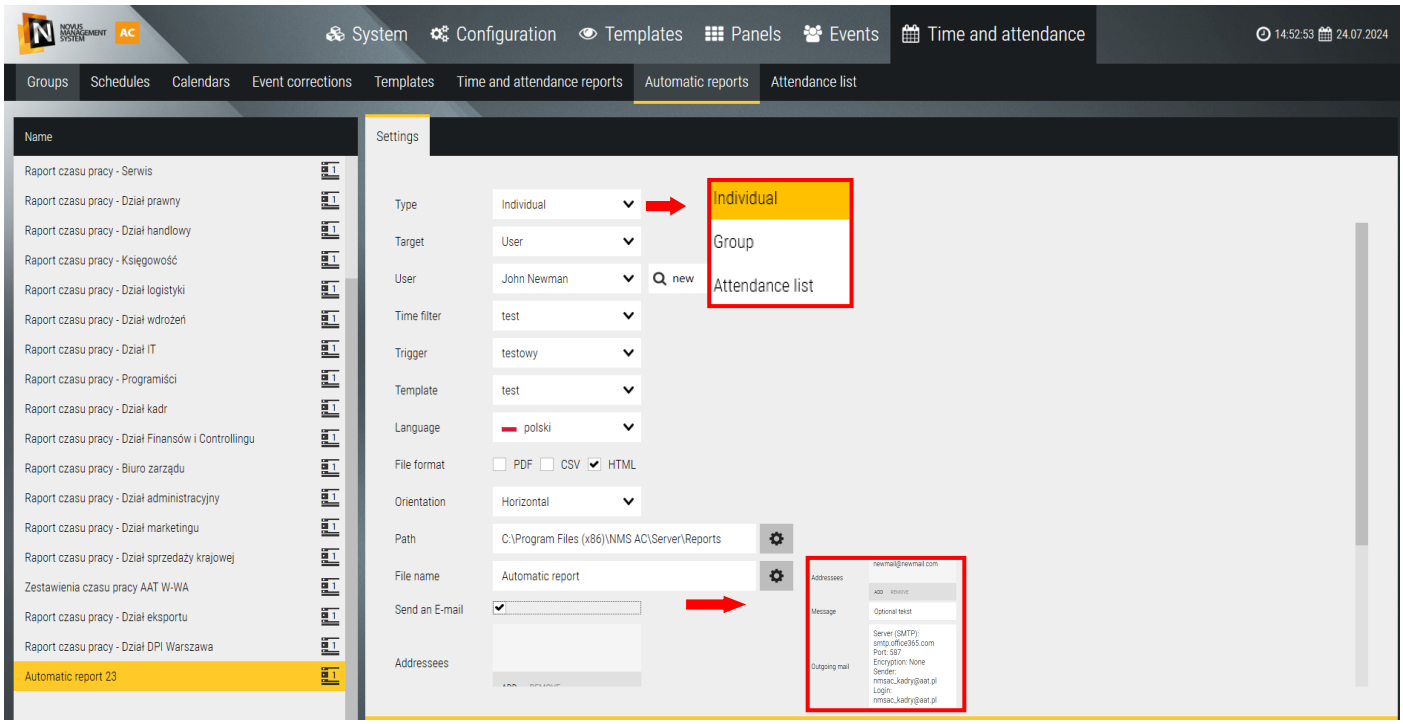
In a system with multiple servers, select the server (the default is local) and then the department.
You can use the Search field to search for the department name.
Select Report Template from the drop-down list. After setting the filters, click on the *Preview* button.

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.



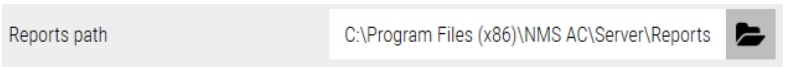
You can also set the report title, page orientation and path to save the report file. Default path:
C:\Users\Administrator\Documents\AAT\NOVUS MANAGEMENT SYSTEM AC

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 --:--

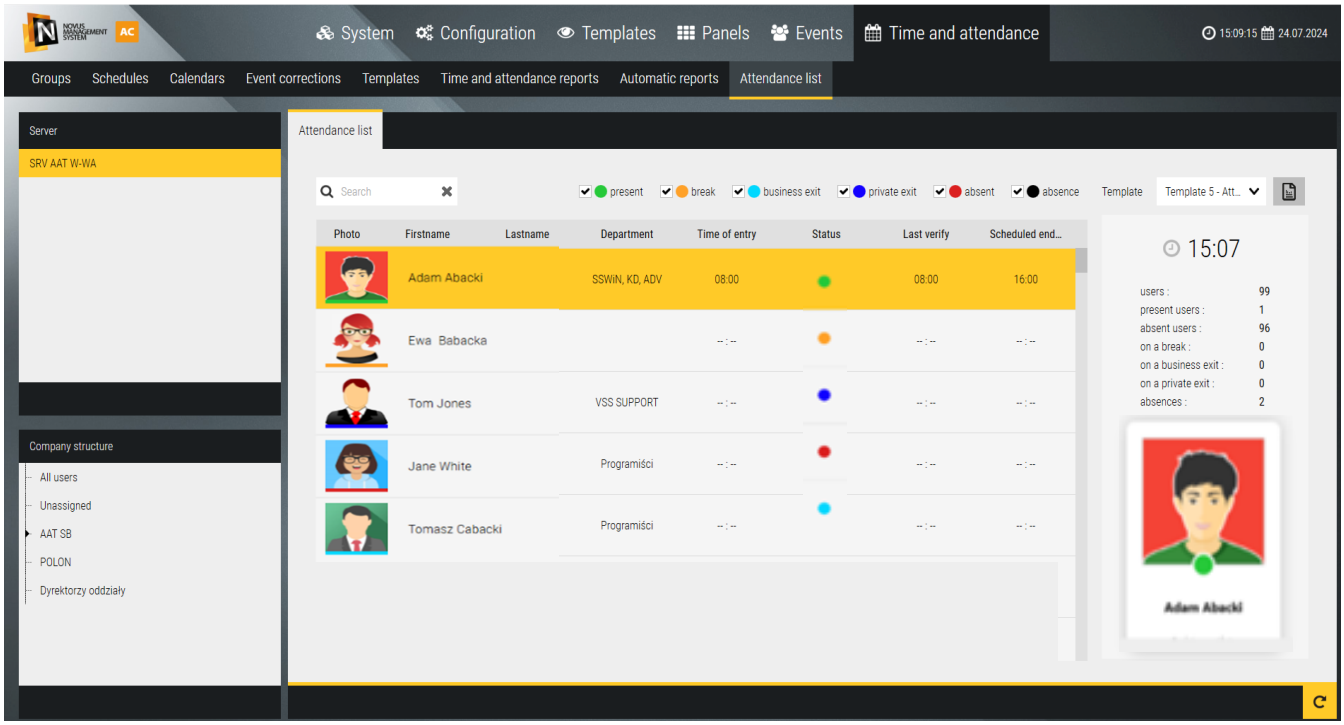
	A	B	C	D	E	F	G	H	I	J	K	L	M
1	John Newman												
2	Template 3 - Individual full												
3	01.07.2024 00:00 - 31.07.2024 23:59												
4	Date	Work hours	Registerec	Work begi	Registerec	Work endi	Late	Early exit	Break hours	Registerec	Registerec	Break time	Registerec
5	01.07.2024	07:32 - 15:32	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

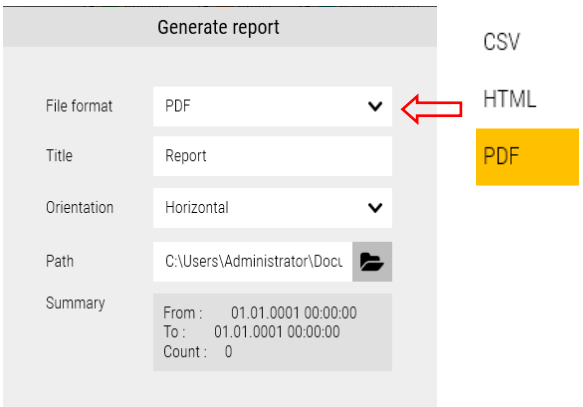


The attendance list allows you to verify the current attendance status of your employees very quickly. When you open the window, it displays a list of employees with photos, as well as the attendance status and the time of registered entry to the company. The status, according to the legend, shows one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



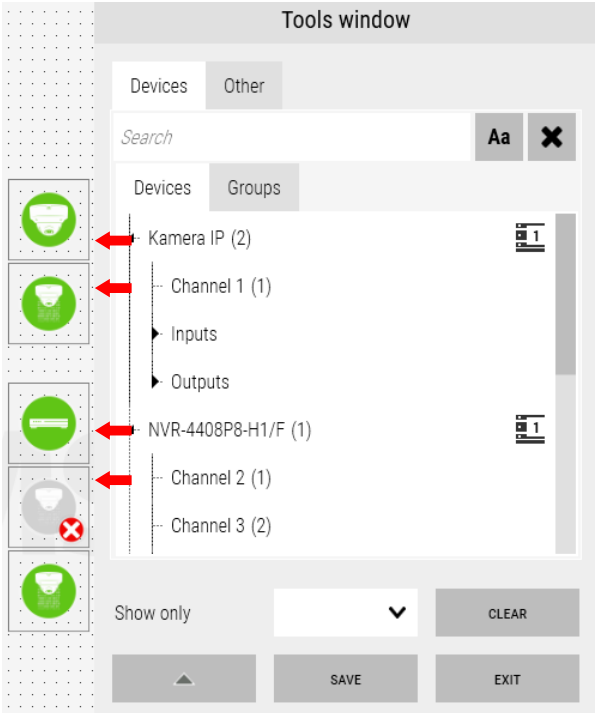
Generating an attendance list report is also possible in automatic mode.

9.5 Integration with VSS devices

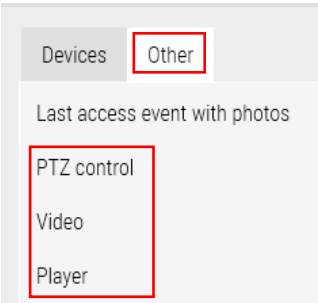
The NOVUS MANAGEMENT SYSTEM AC software enables integration with a video surveillance system. Adding devices of this type is described in chapter **3.10 Devices - Video Surveillance System**.

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.



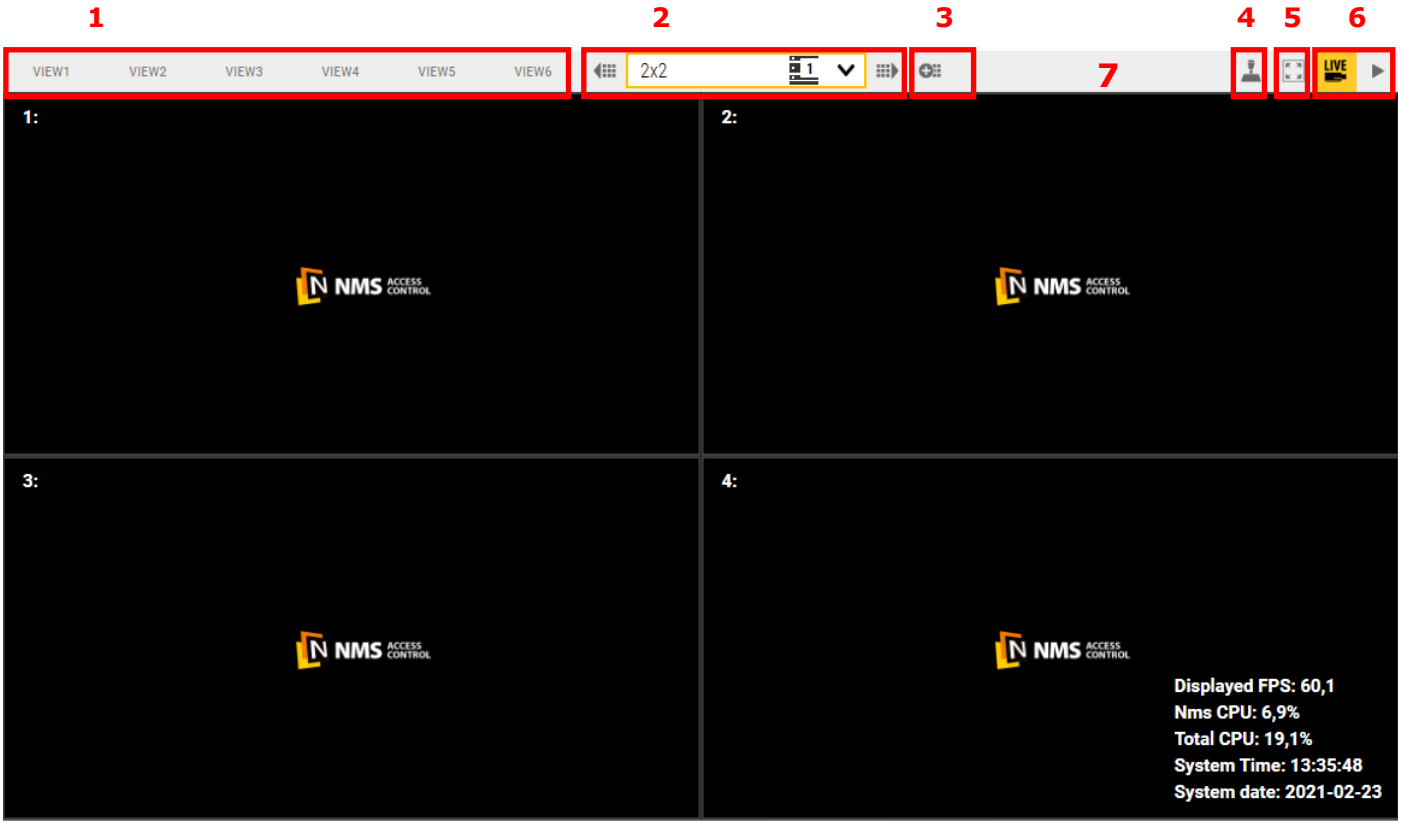
Pay attention to the options that appear after clicking on the stream icon in edit mode:

- 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

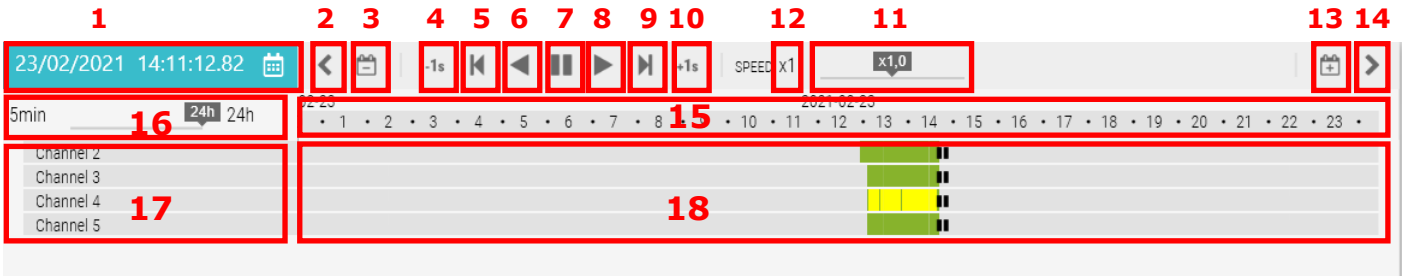
The *Video* window is used to display video streams. It displays cameras previously defined in *Templates*, *Video Views* tab. (described in chapter **5.1 Video Views**). In the top bar of this window there are icons to manage the window.



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

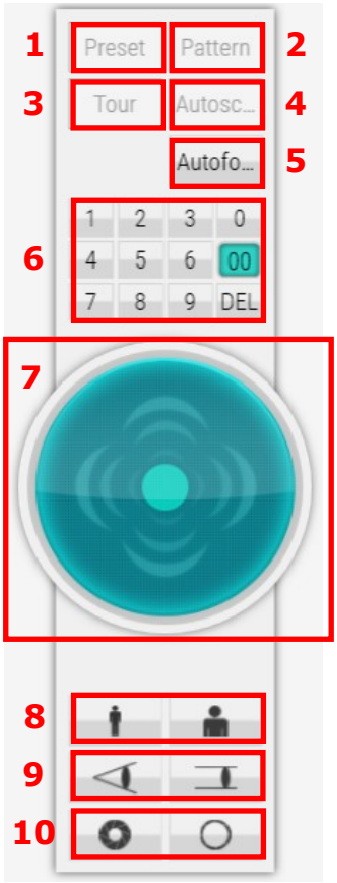
The player tool is necessary to view recordings from VSS recorders. It is blank and grayed while viewing live images. When any *video view* is switched to playback mode, the list of channels of the window is filled in and recordings are displayed on the graph.



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.

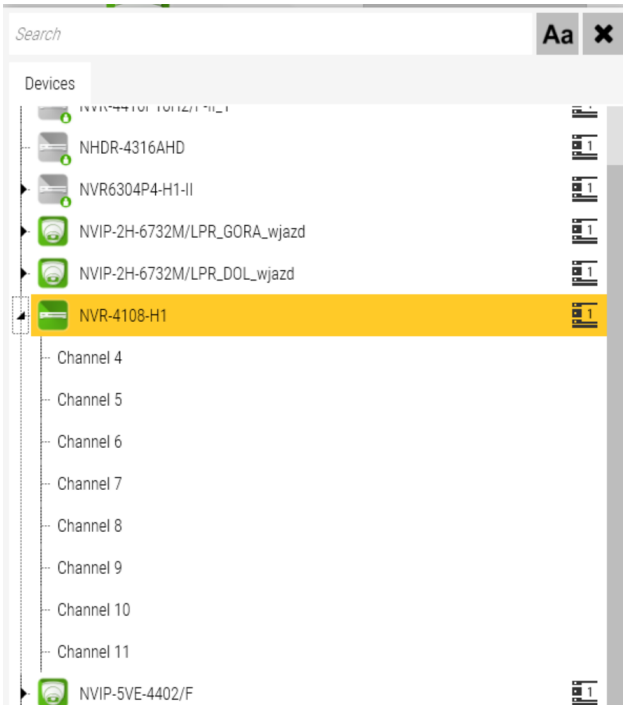


1. Preset button—to call the preset. It is greyed out by default, it activates when you select a number in the lower part of the tool.
2. Pattern button—to call the pattern. It is greyed out by default, it activates when you select a number in the lower part of the tool.
3. Tour button—to call the tour. 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.

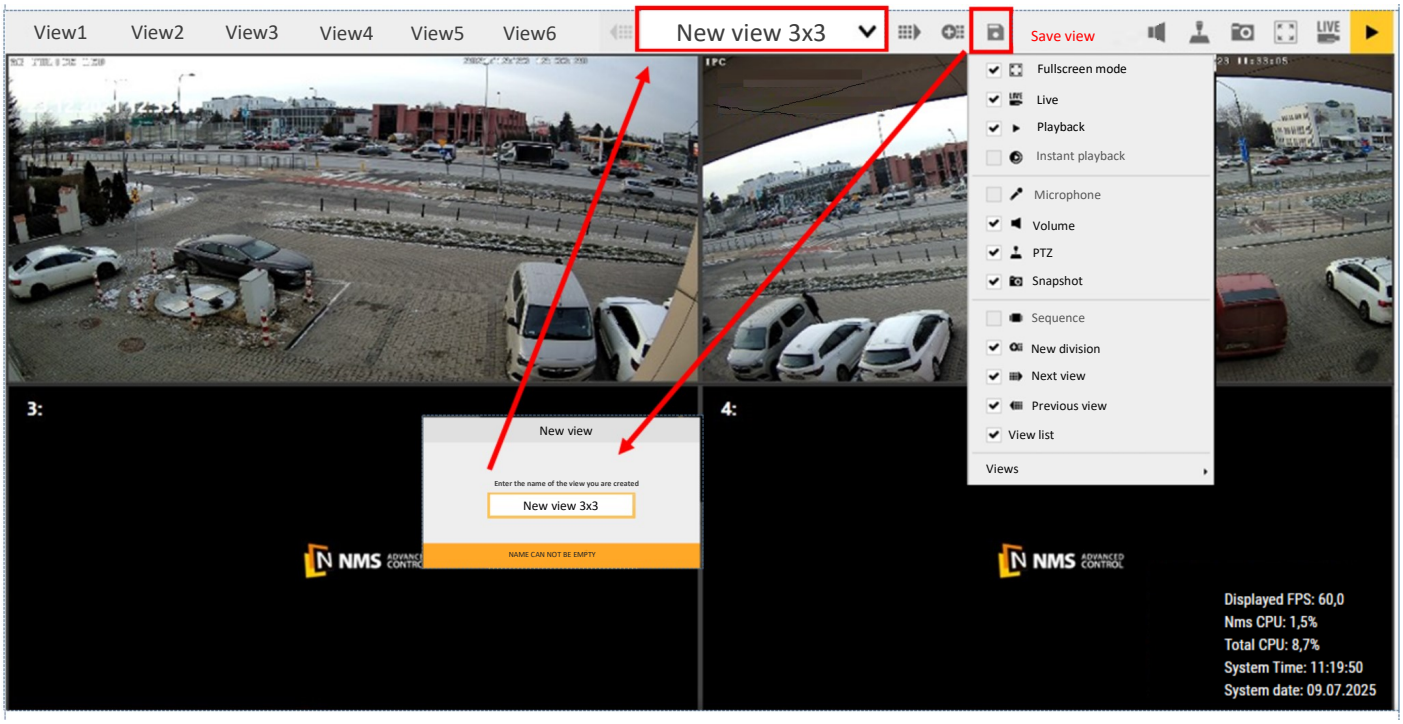
Attention! The availability of particular functions depends on the functionality of the selected camera model.

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.

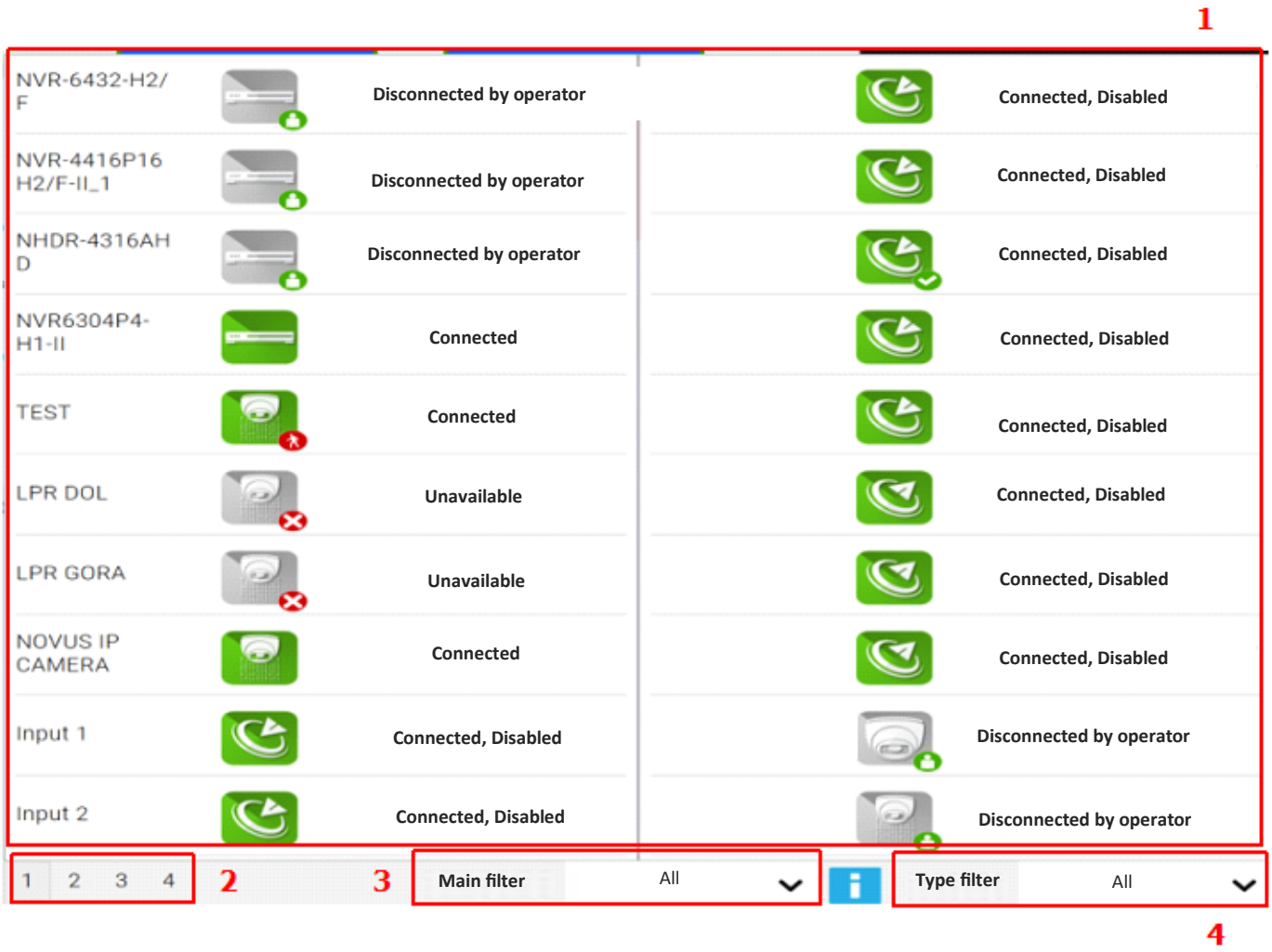


To create a temporary view in the Video tool and optionally save it, drag a device or channel from the list onto the selected view in the Video tool, holding the cursor over the desired element.



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.



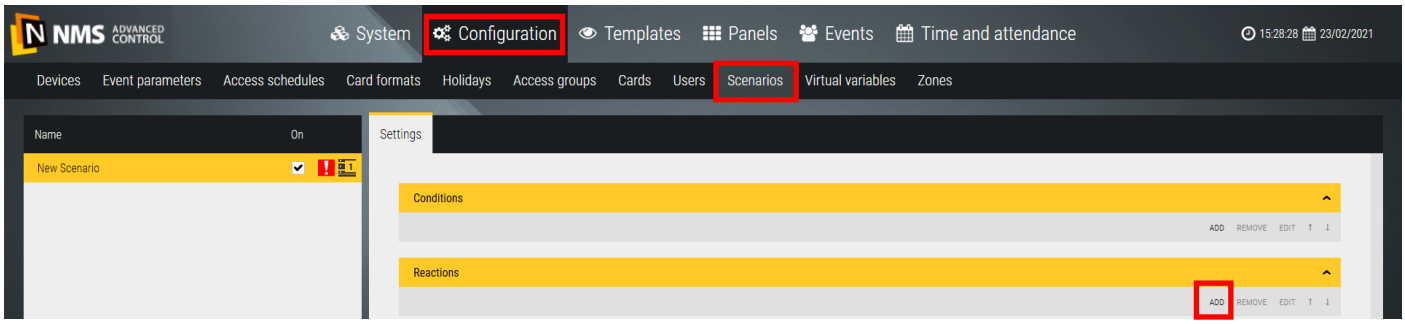
1. Device window – displays all devices, channels, inputs, and outputs available in the system.
2. Page selection – allows switching between pages with lists of devices and system elements.
3. Main filter – enables selection of filters previously defined in the *Element and Event Filters* tab.
4. Type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

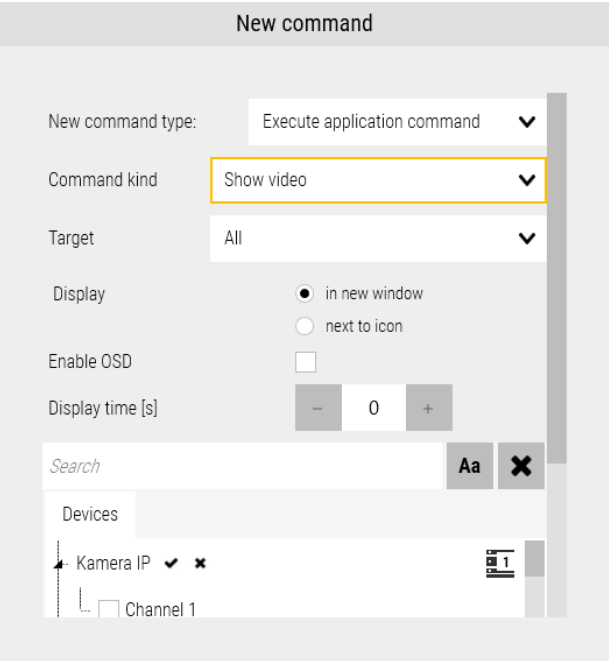
9. 5. 6. View video streams in response to the scenario

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:

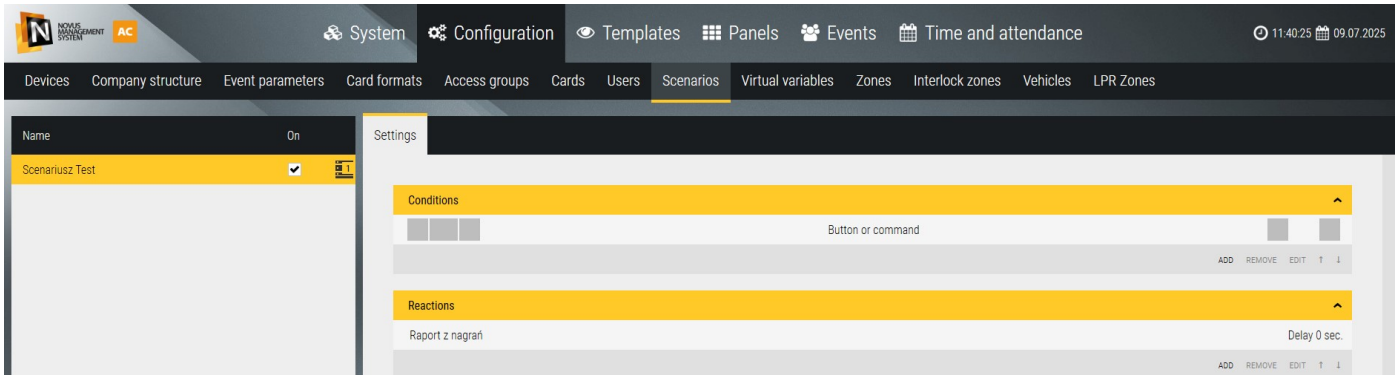
- Target — video display can be set for a specific operator or group of operators.
- Display — display can be set in a new window or in the pop-up window next to the video stream icon. In the first case, a single camera will occupy the entire window. By increasing the number of streams, it will automatically 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.

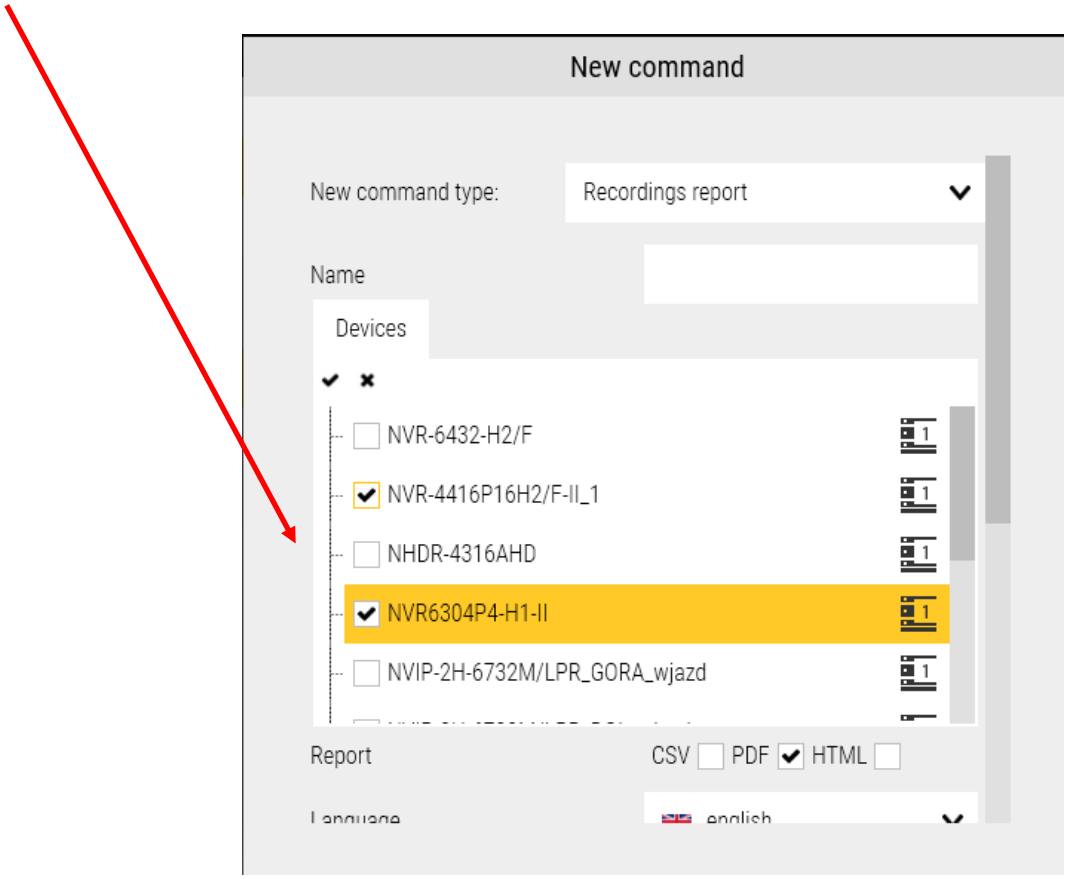
9. 5. 7. Generating recorder reports via scenario response

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.

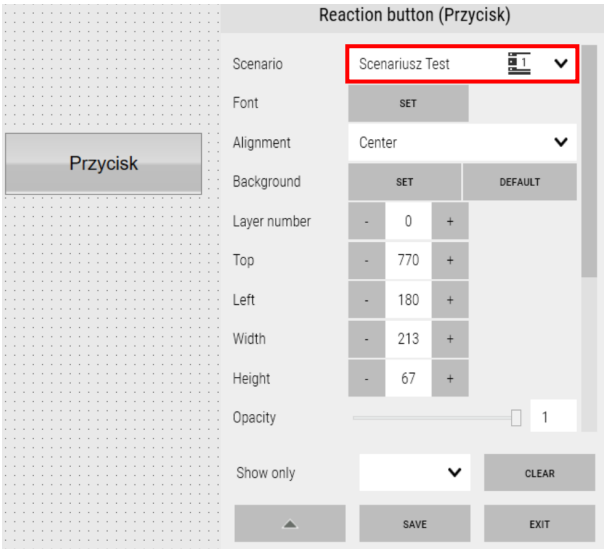


To generate a recording report, create a new scenario in which the operating conditions are defined.
In this case, select a command type such as Button or Command, which will initiate the report generation.

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

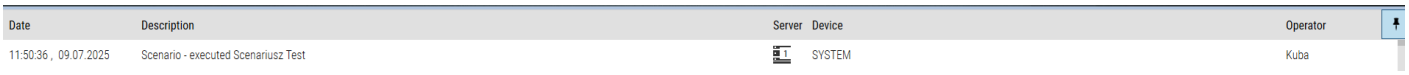


In the Reaction Button tool editing window, you must select the newly created scenario that will trigger the report generation process.



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		

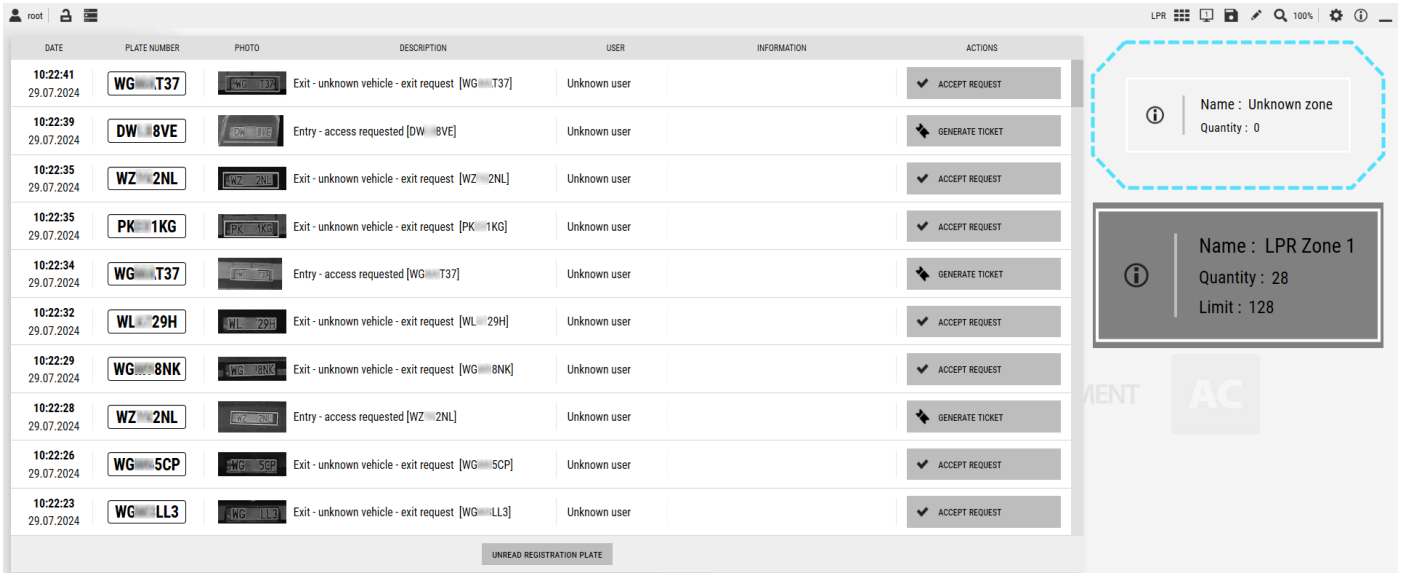
HTML:

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

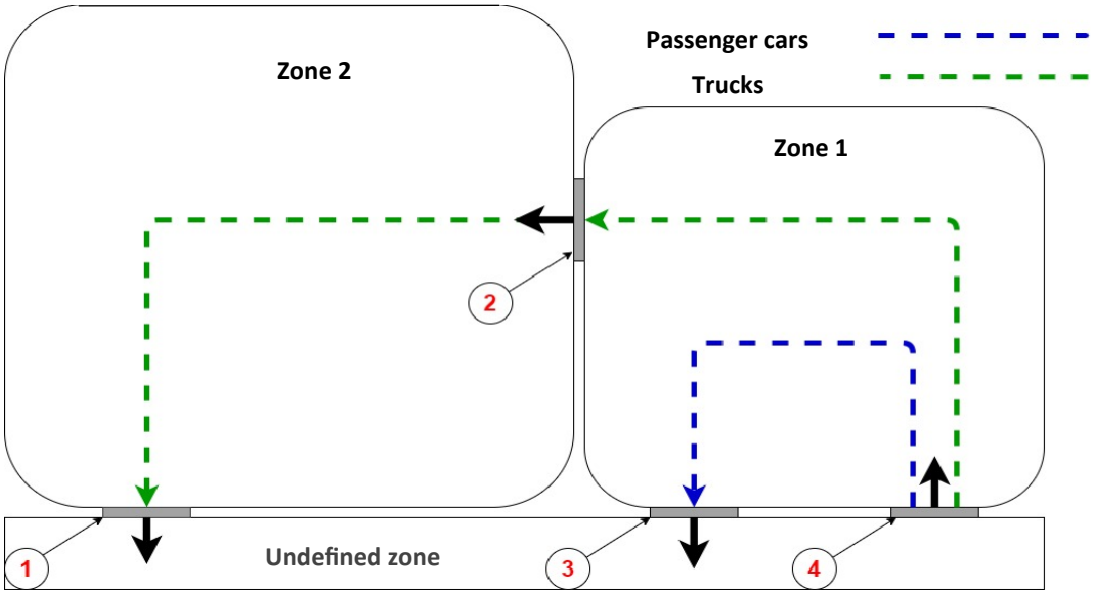
NMS AC software integrated with IP cameras equipped with LPR functions allows you to control the access of vehicles to pre-defined zones.

Assuming that:

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

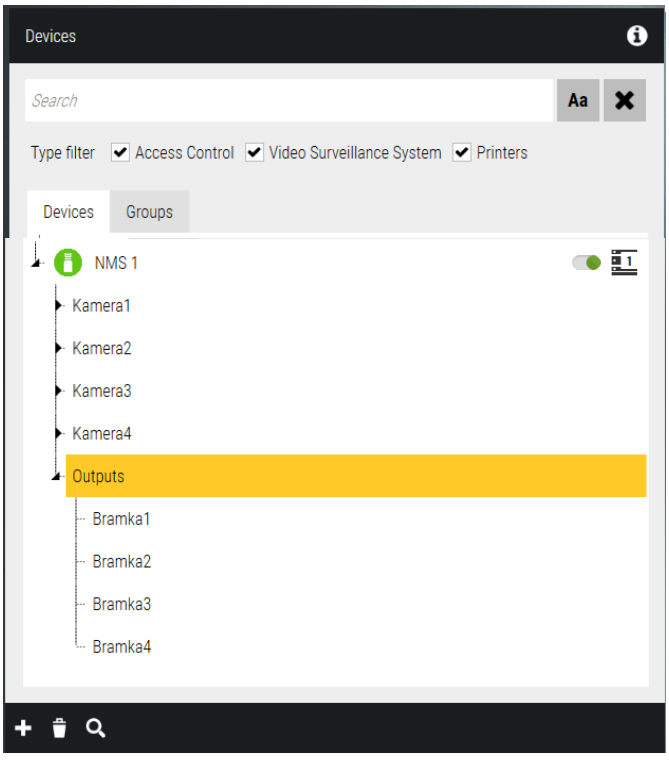
Zone 1 can be accessed by the group": "Passenger cars" and the group "Trucks".

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.

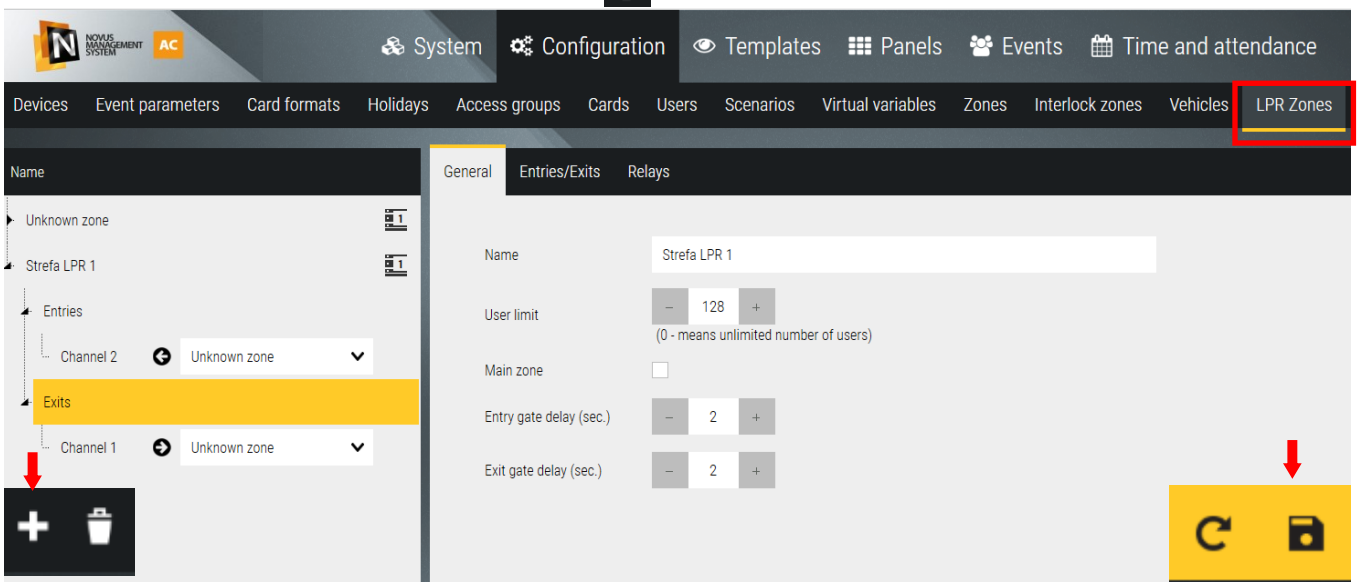
The process of adding VSS devices is described in Chapter 3.10 CCTV. In the example above, the cameras added to the system were named according to the figure next to it.

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

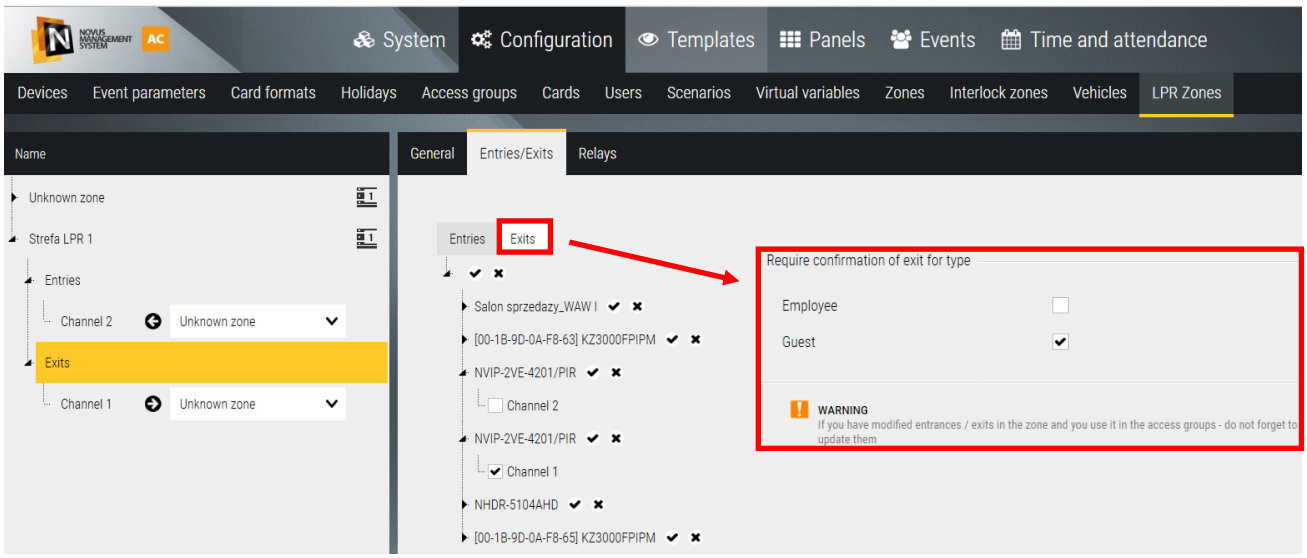
9.6.3.1 Configuration Zones

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.



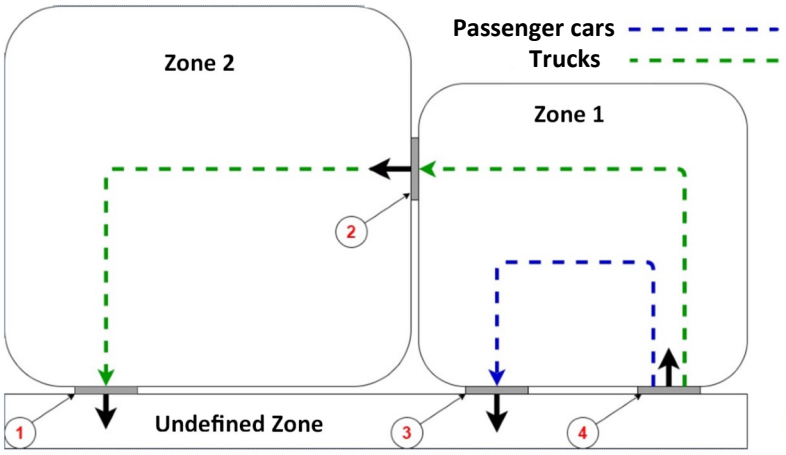
After clicking on the selected zone, in the "General" tab there are fields:

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**:

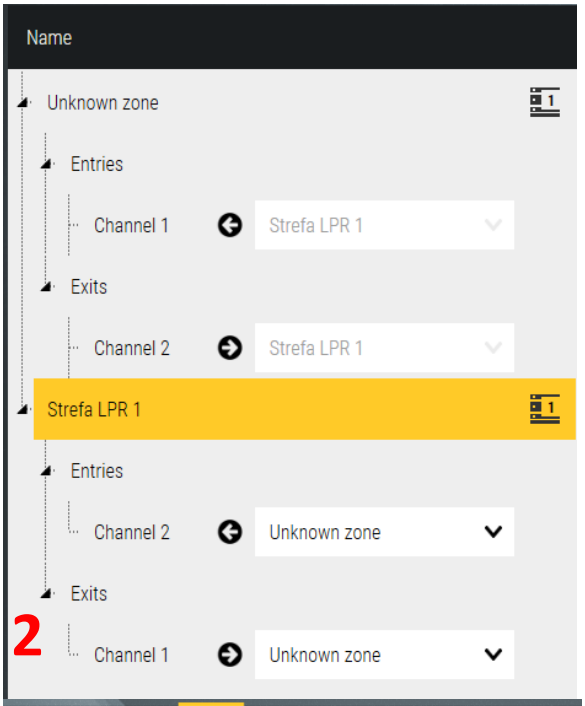
From the "Indeterminate Zone" monitors **camera 4**

Departure from **Zone 1**:

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

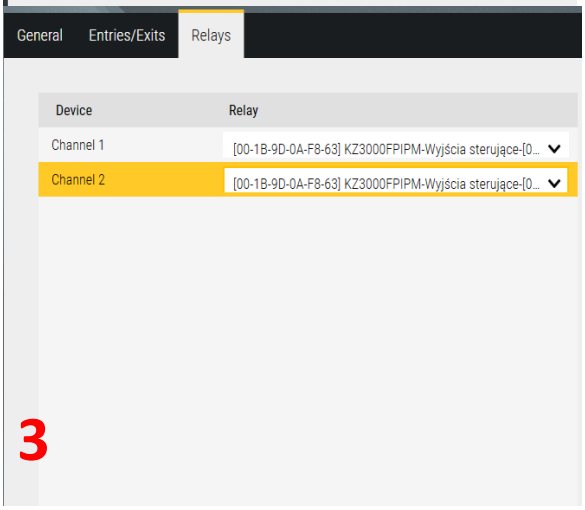
For "Zone 2" monitors **camera 2**

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



Relays

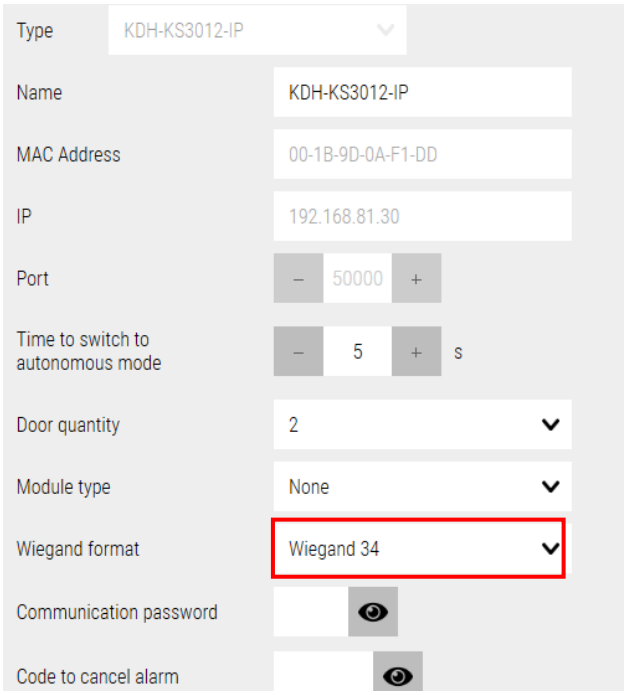
The LPR Zones configuration step can be completed by assigning relays to the appropriate devices. The names of the devices and relays were previously defined when adding devices in section 9.5.1. Due to the fact that in the adopted project, each camera is to control the gate at which it is placed, the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

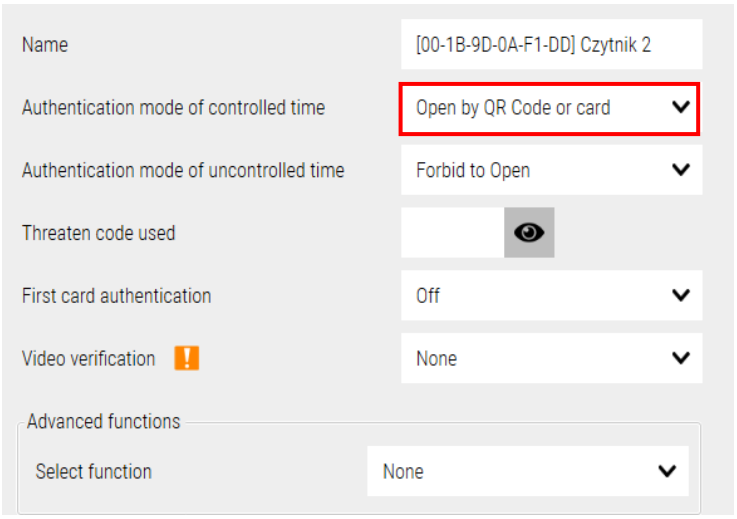


9.6.3.2 Guest Exit Handling Using Controller, Reader, QR Printer, and LPR Camera

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.

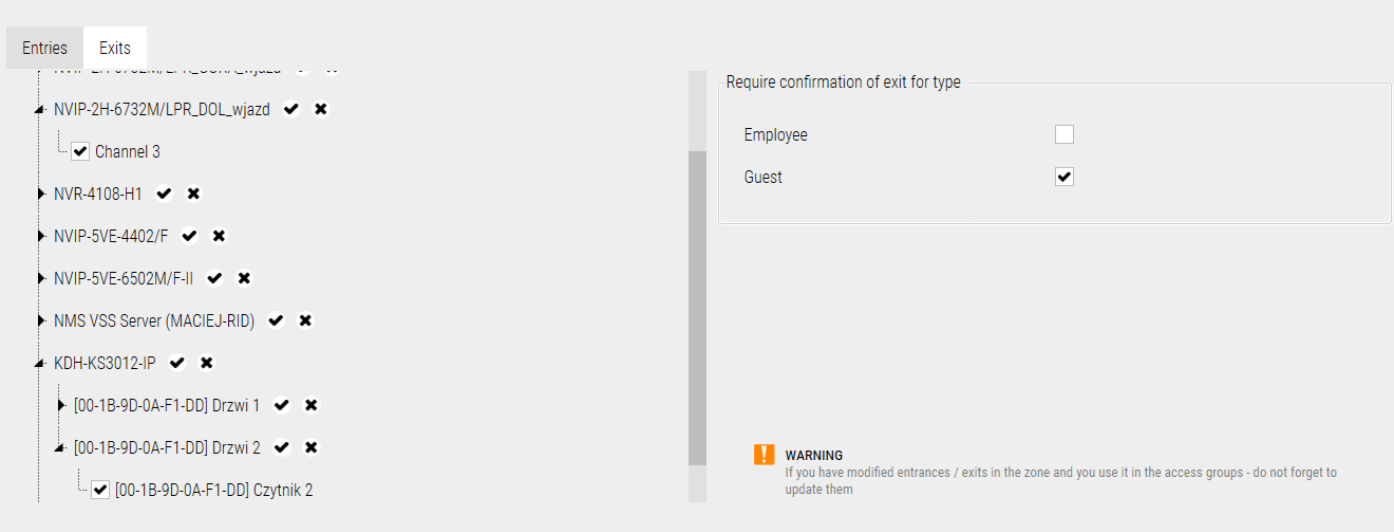
An example configuration of the reader for the selected Access Control device — in this case, the KDH Series 3000 — is shown in the images below:





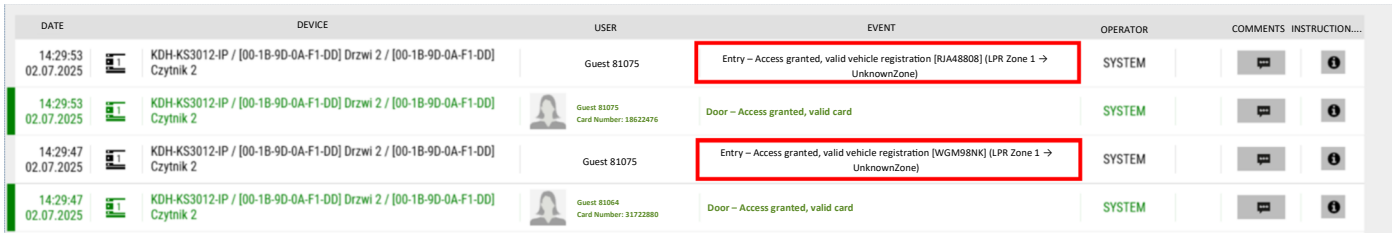
IMPORTANT! For the reader to correctly read QR codes from tickets, the Wiegand format must be set to Wiegand 34 in the Access Control device configuration.
Additionally, in the Details tab of the selected reader, the Identification Mode during Active Time field must be set to QR Code or Card.

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.



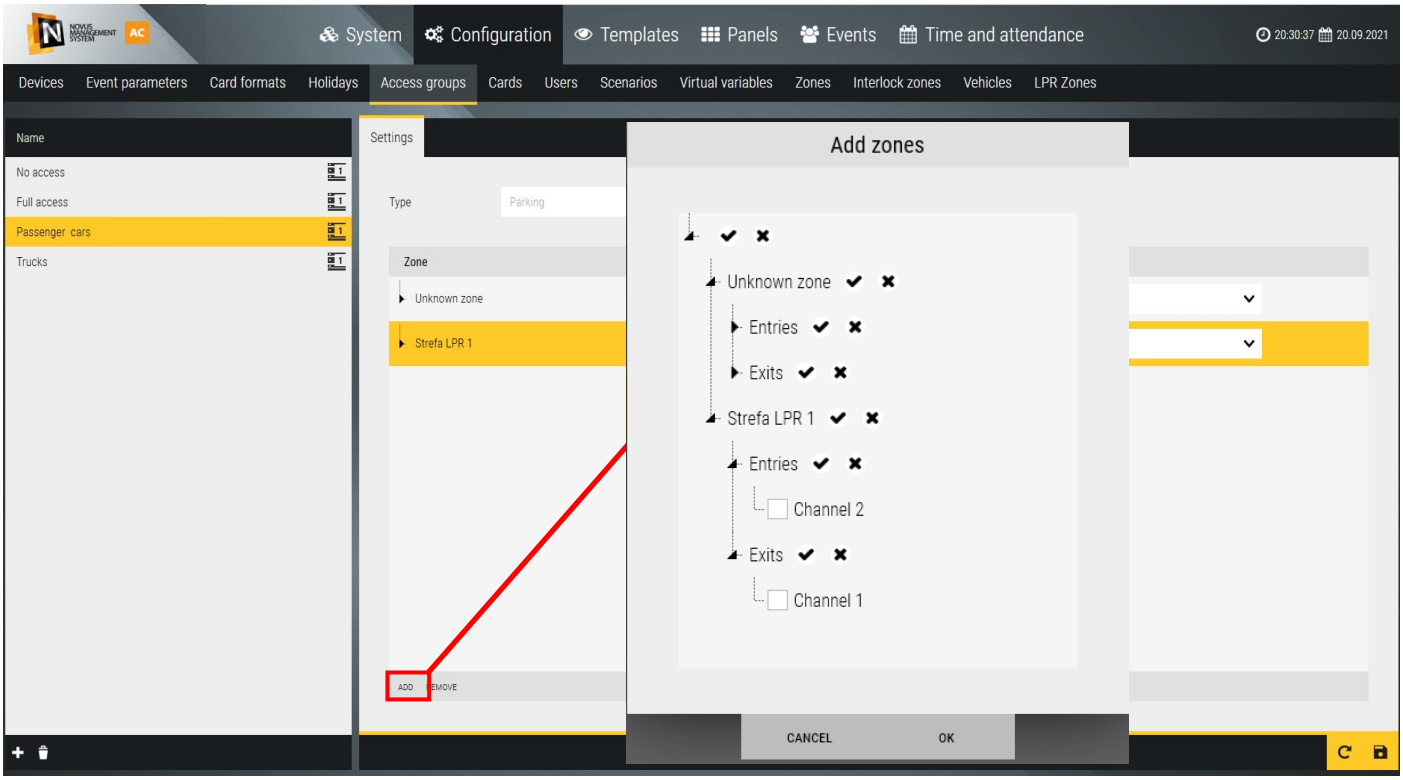
In the Relays tab, assign the newly created outputs to the previously configured output responsible for actions such as raising the barrier during exit from the zone—similarly to how the LPR camera is assigned to the exit.

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



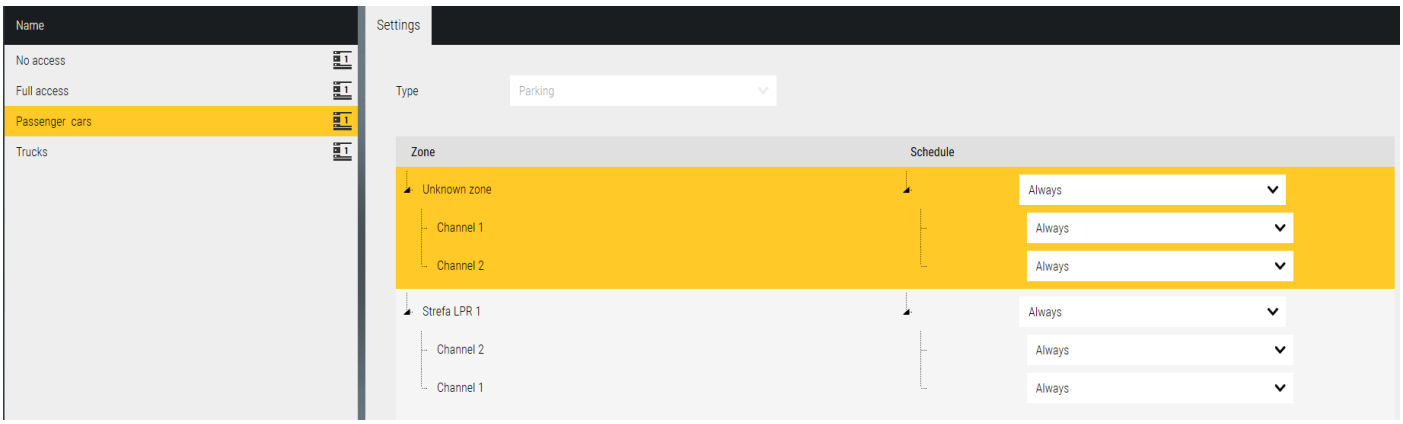
controlled m.in by LPR cameras.

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.

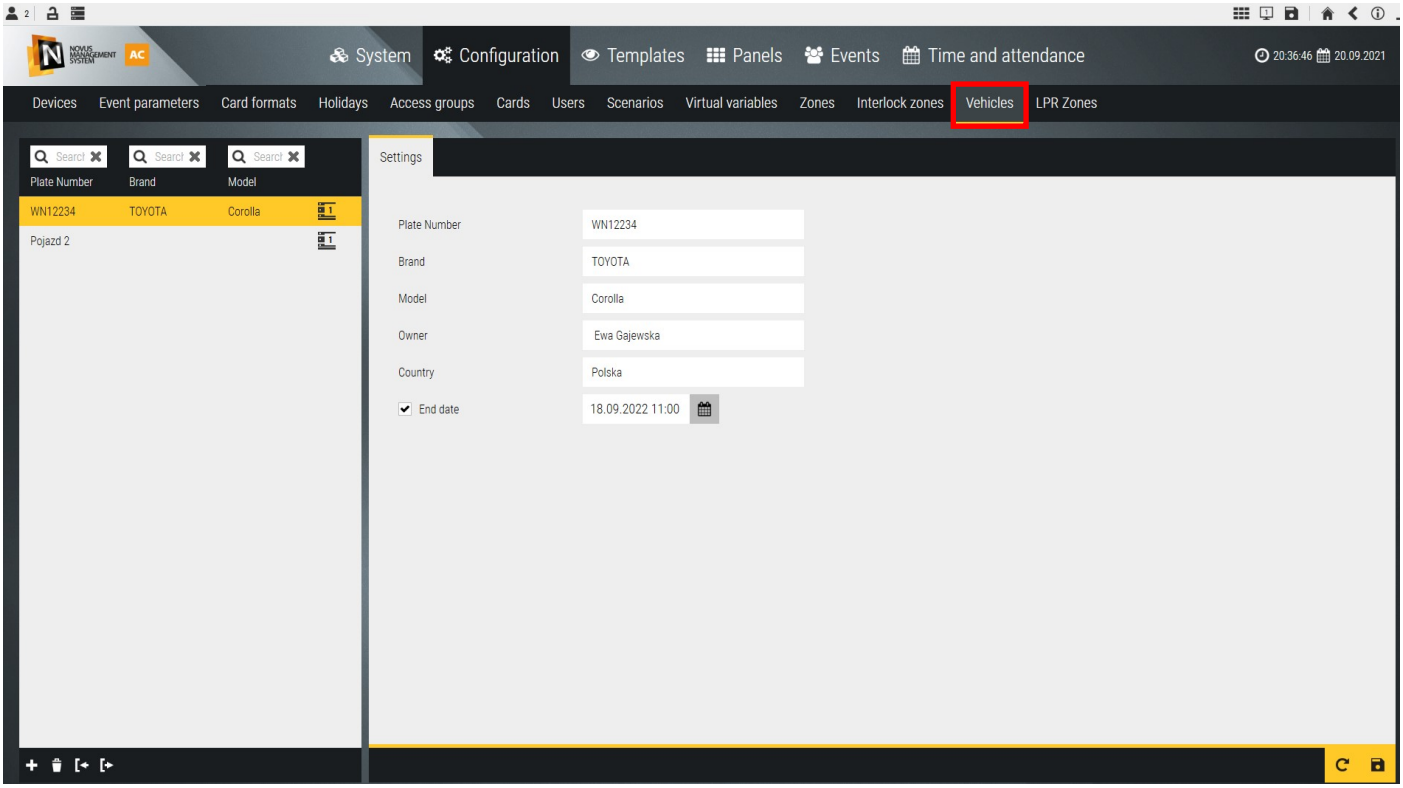
Trucks – which will have access to Zone 1 and Zone 2 and will have the opportunity to pass through gates **1,2,4.**

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.

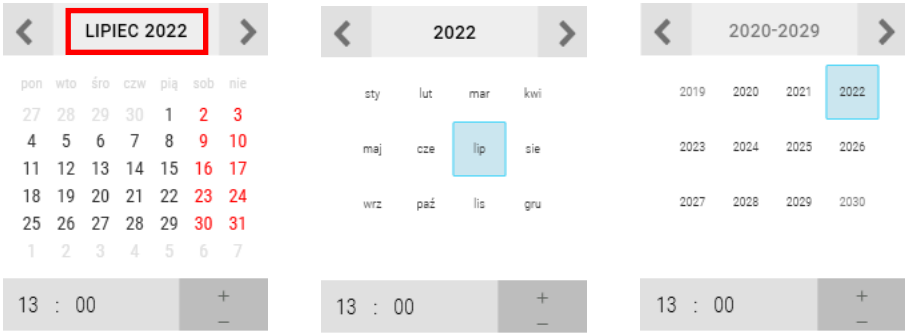


Buttons:

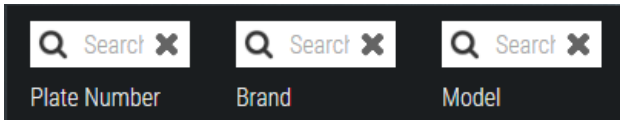
- is used to import the vehicle database in .csv format,

- 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. +/-

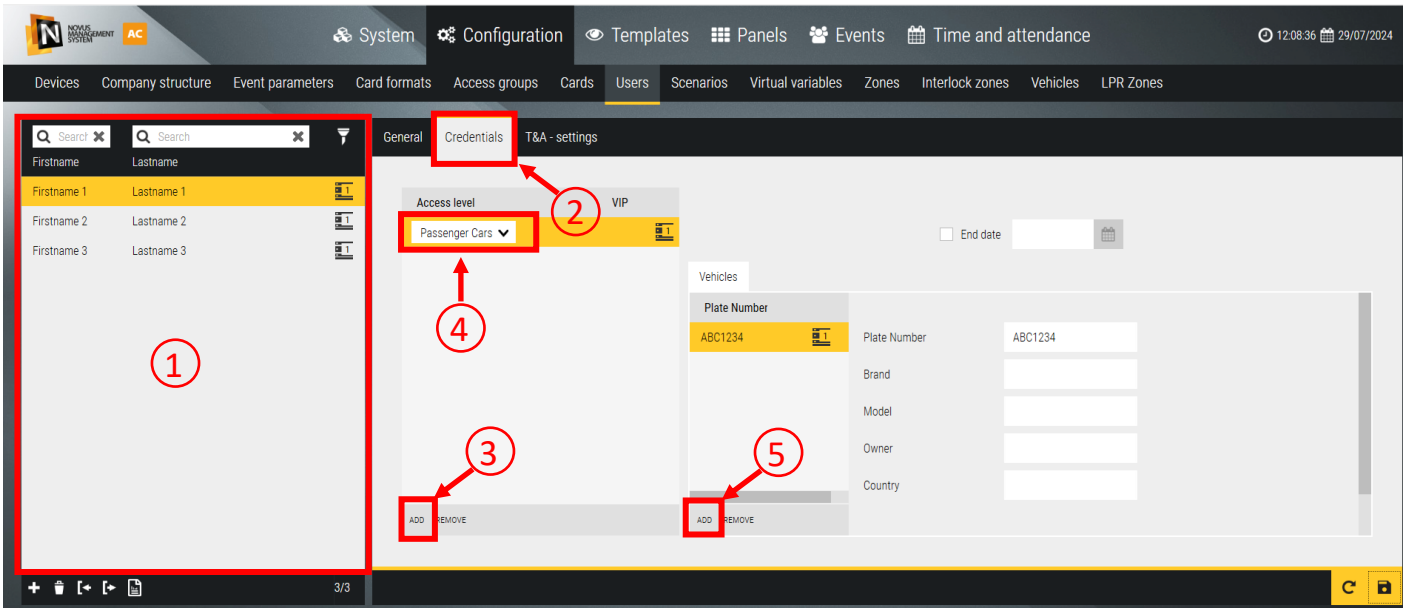


Above the list of added license plates there is a search engine that allows you to narrow down the list of license plates by license plate number, make and model of the car.



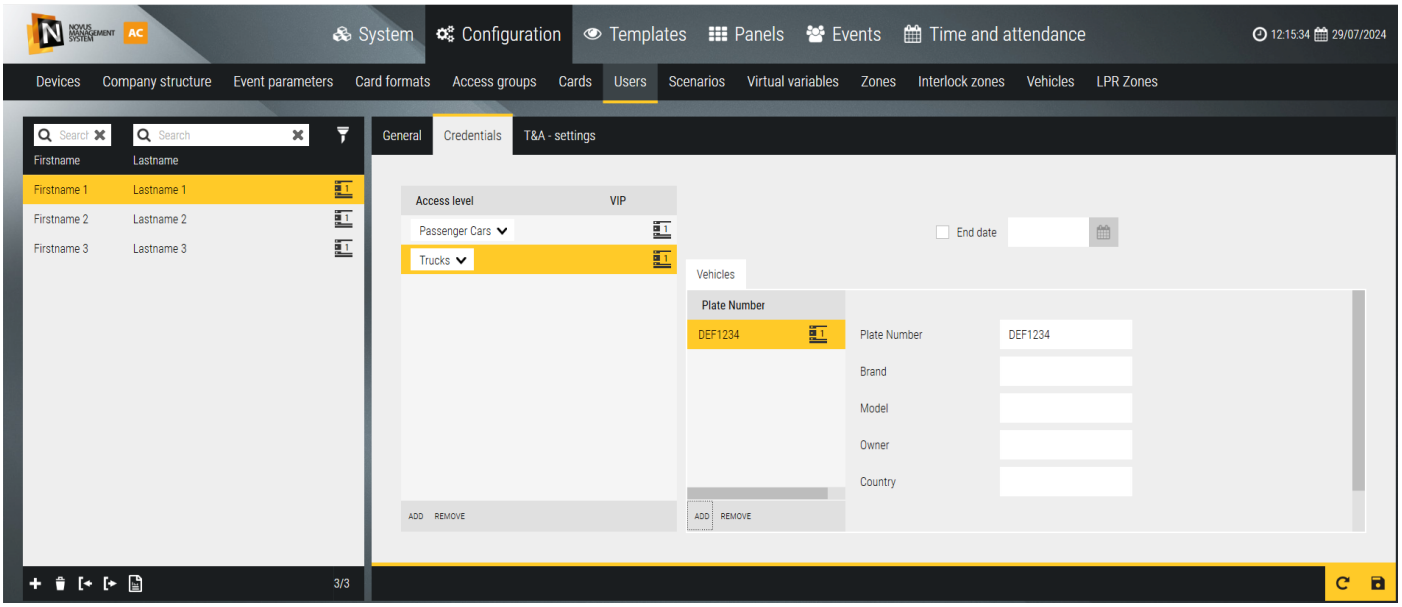
9.6.6 Users - Identifiers

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.

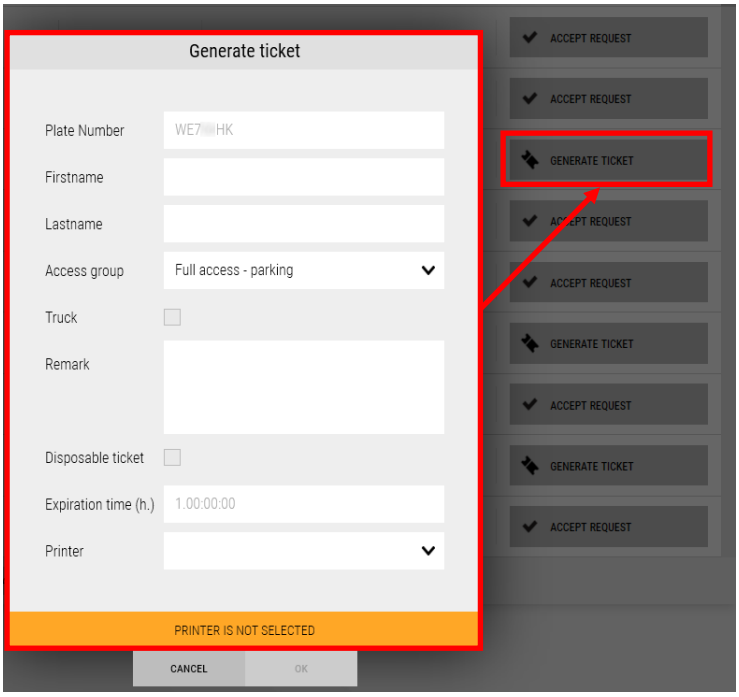
In the case of access to the second zone, the access level "Trucks" should be added and the action repeated, with the difference that in field (5) a vehicle with registration DEF 1234 should be added, as in the figure below.



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.

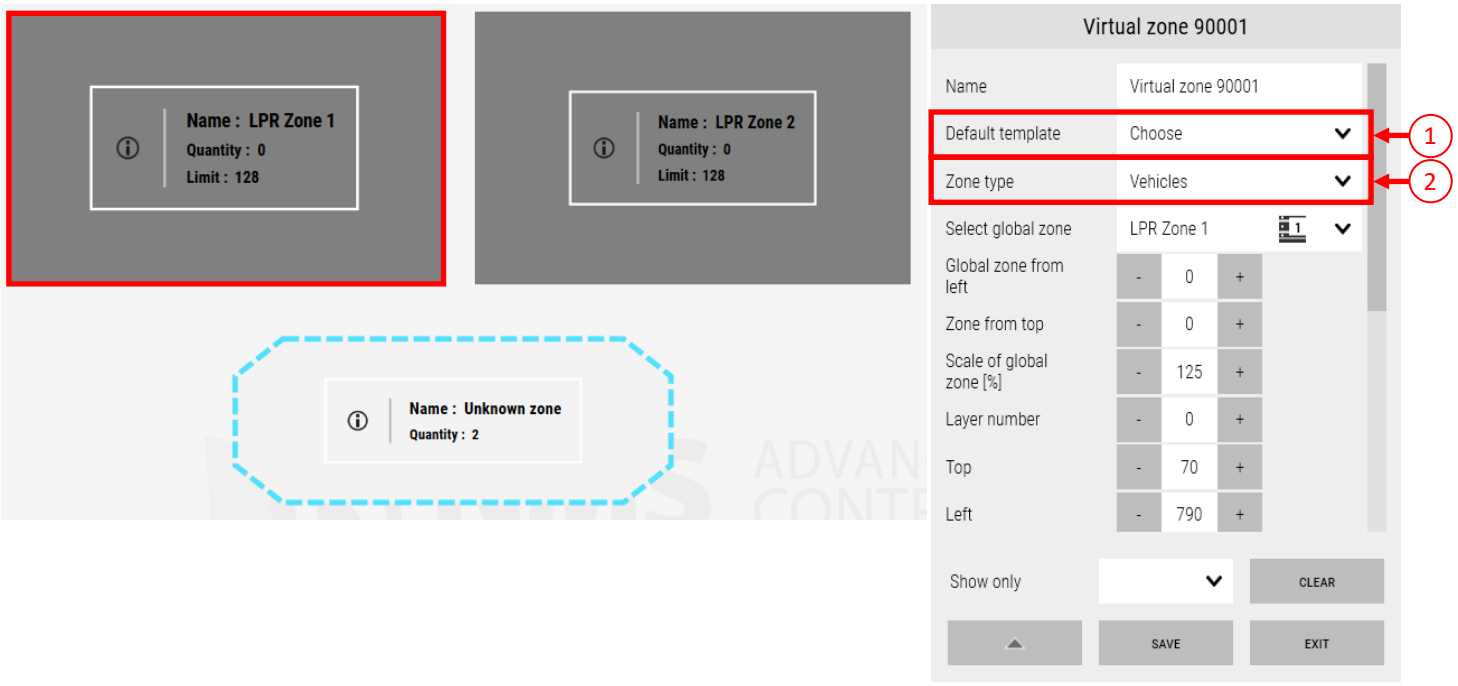
To print a ticket, a dedicated printer should be added to the system. This can be done in the Configuration> Devices tab. For more information on adding devices to NMS AC, see Chapter **3.System Configuration.**

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.

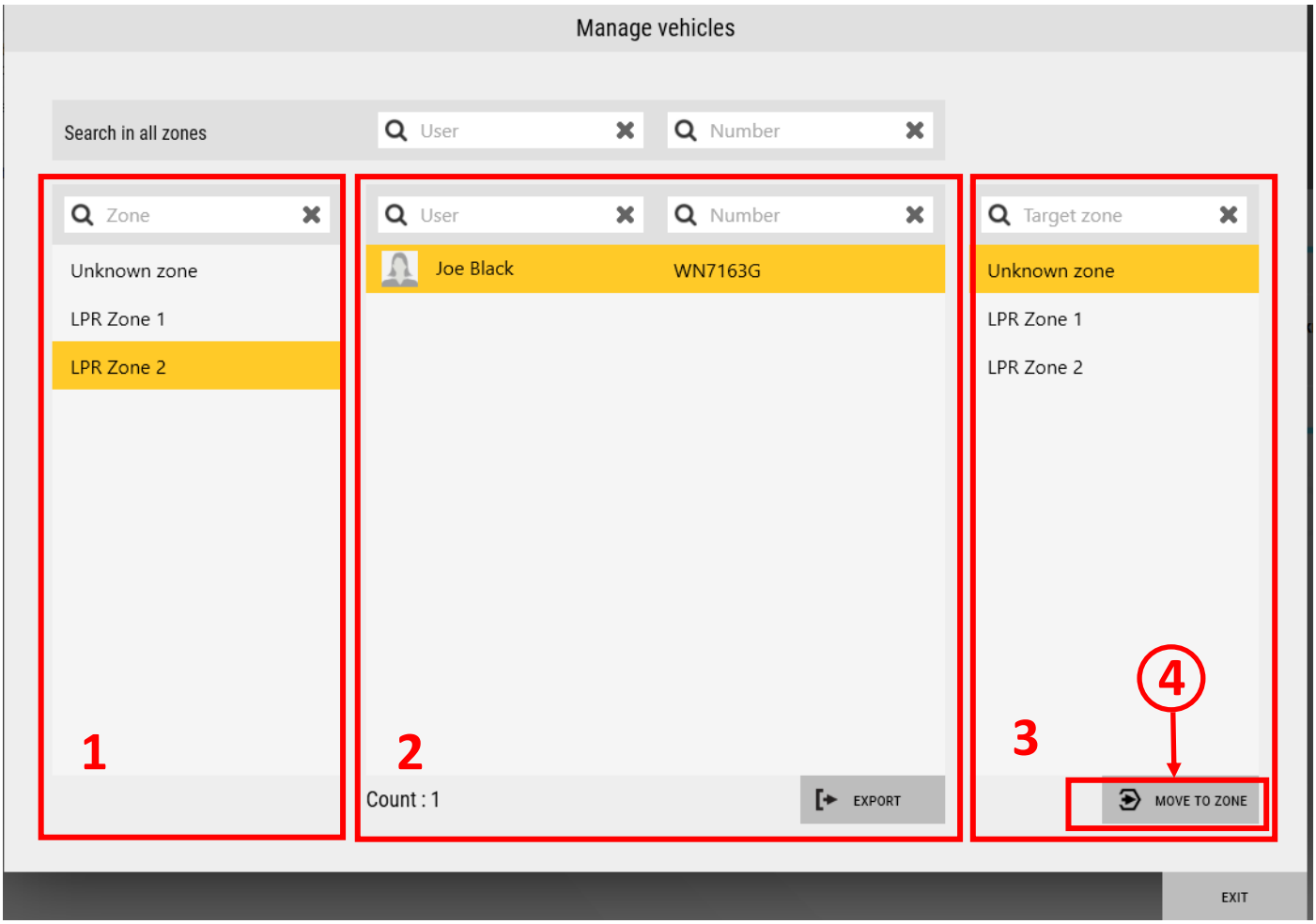
After configuring the newly created zone, information such as:

- 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

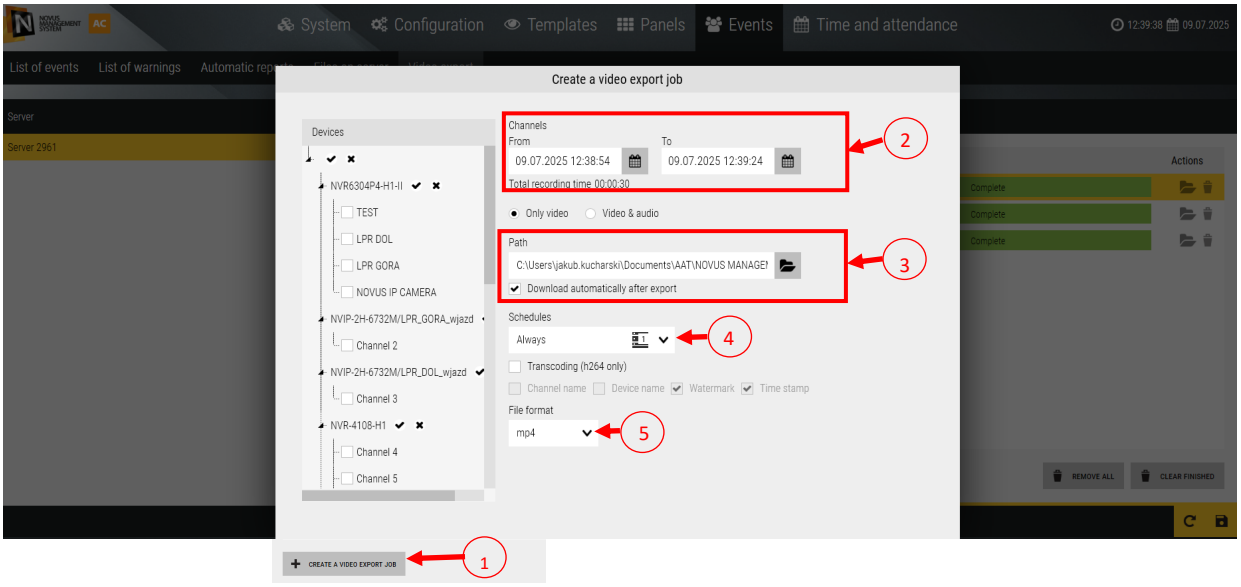
After clicking the left mouse button on any zone, the user has the option to go to the vehicle management window. Field (1) is used to select the zone from which the preview is displayed in the middle field (2). Field (2) is used to view which users are currently in a given zone. In the event of non-compliance 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.

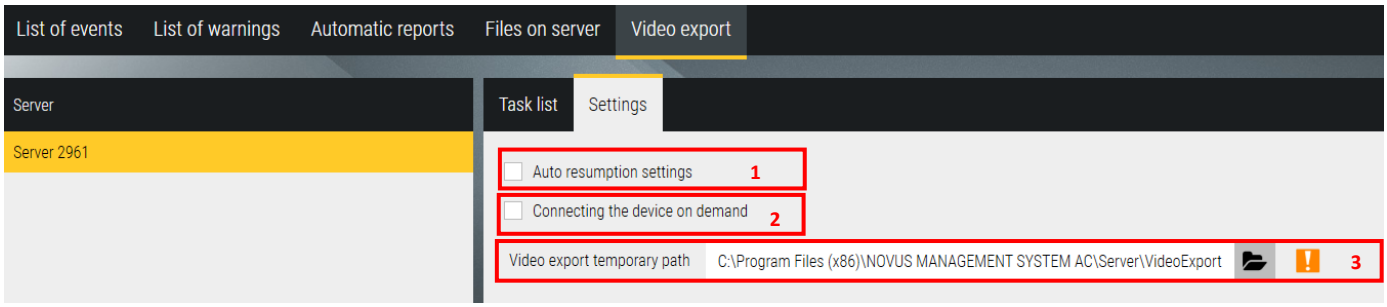
To have the recordings automatically downloaded and saved to a selected path on the workstation where the NOVUS MANAGEMENT SYSTEM AC client is installed, check the box “Download automatically after export” in field (3).
Otherwise, the recordings will be exported to the server and will be available for 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.

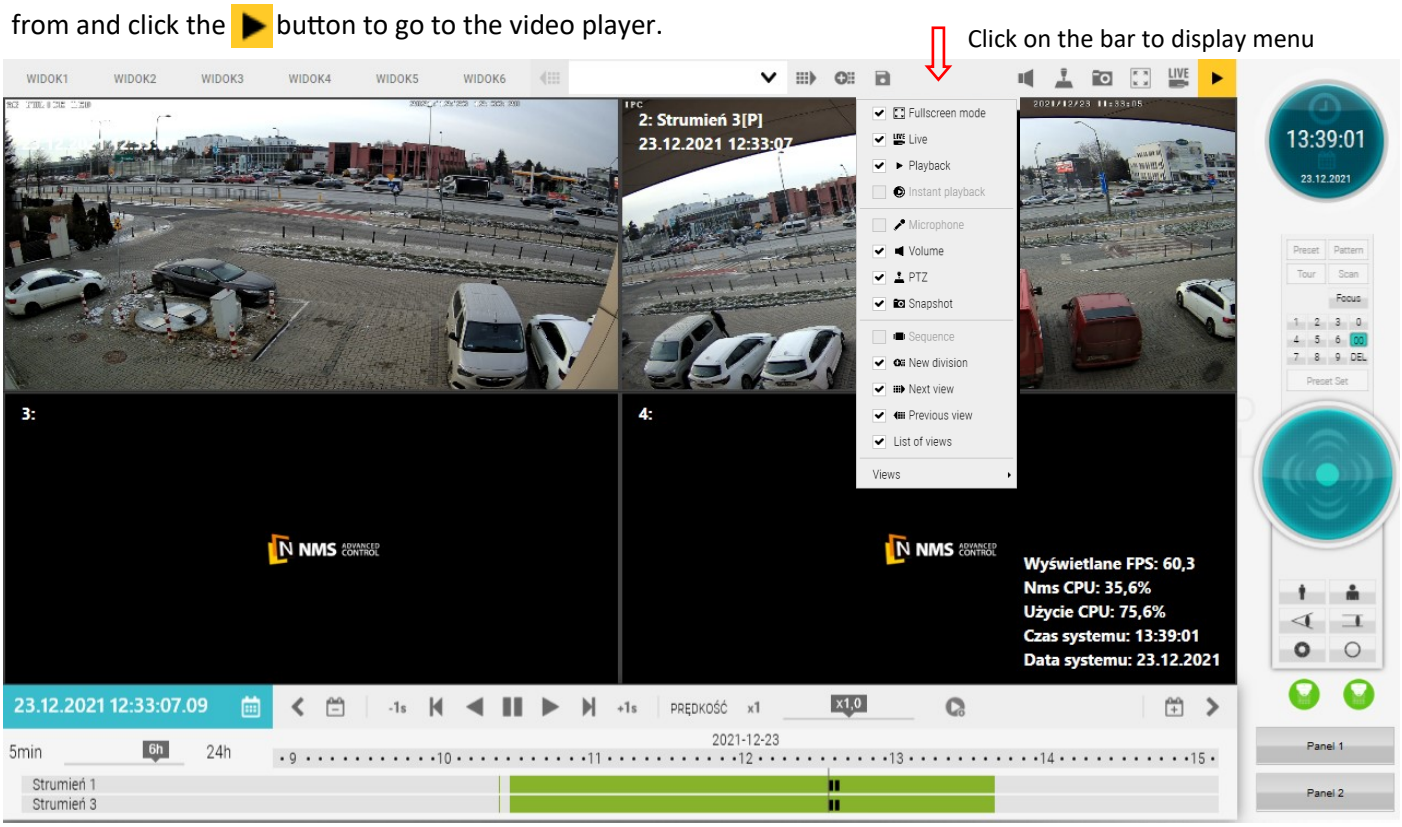
2. **Connecting the device on demand** - This option allows the system to automatically establish a connection with a device when a video export request is made. If this option is disabled, the user must manually connect to the device.

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.

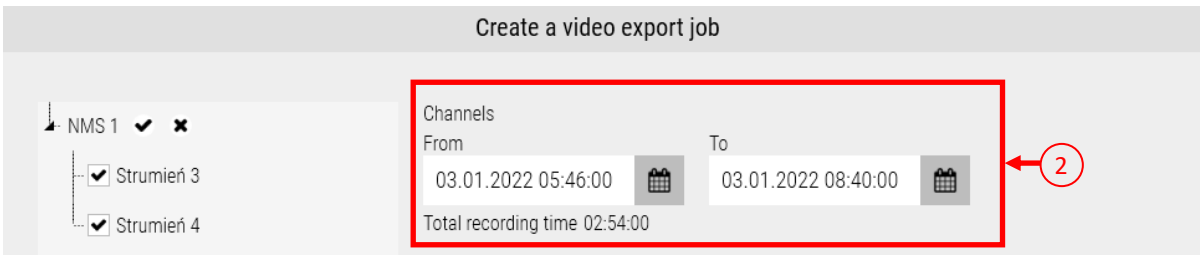
9.7.2 Export recordings from the video player

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.

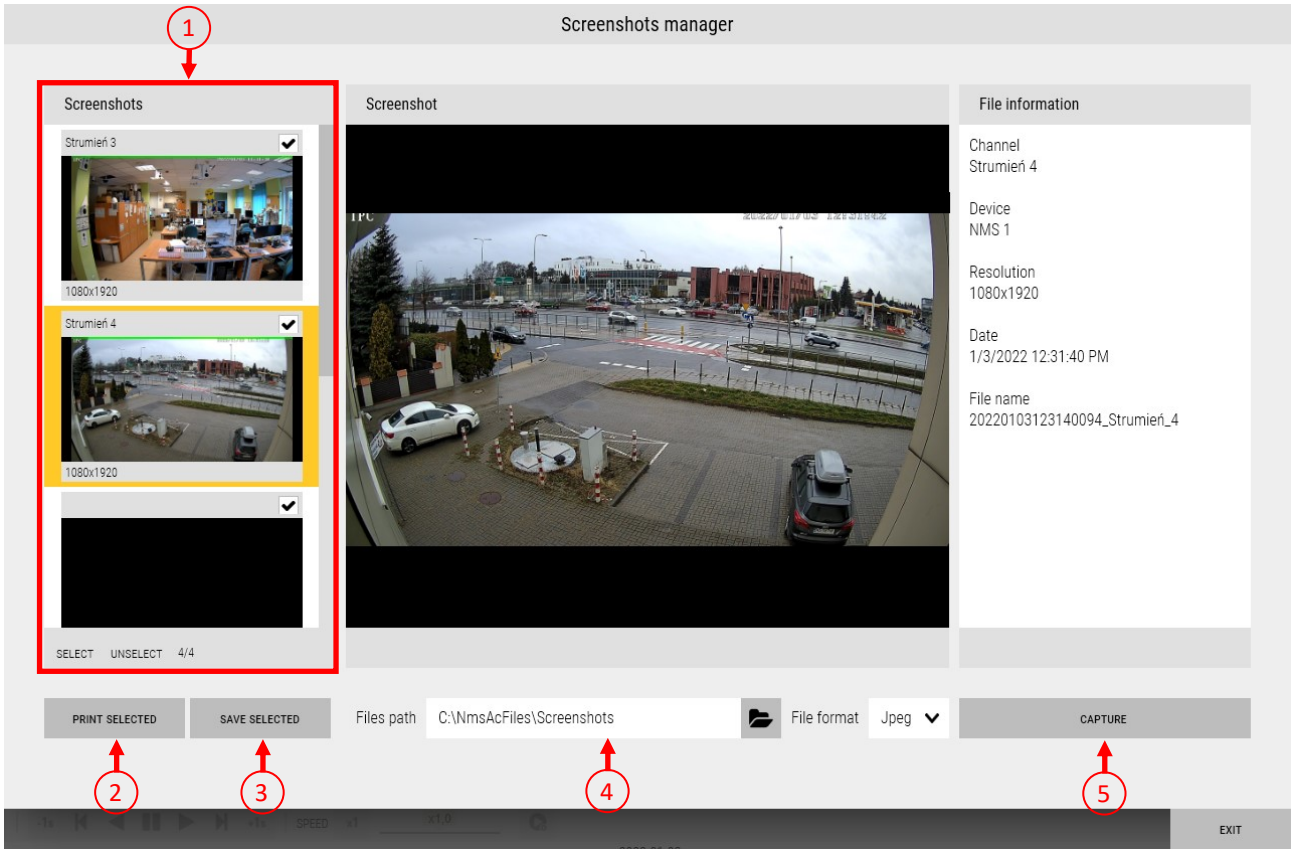


At the end to export and download selected recordings, follow the same procedure as described in the section **Export recordings from the main menu** on the previous page.

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 .



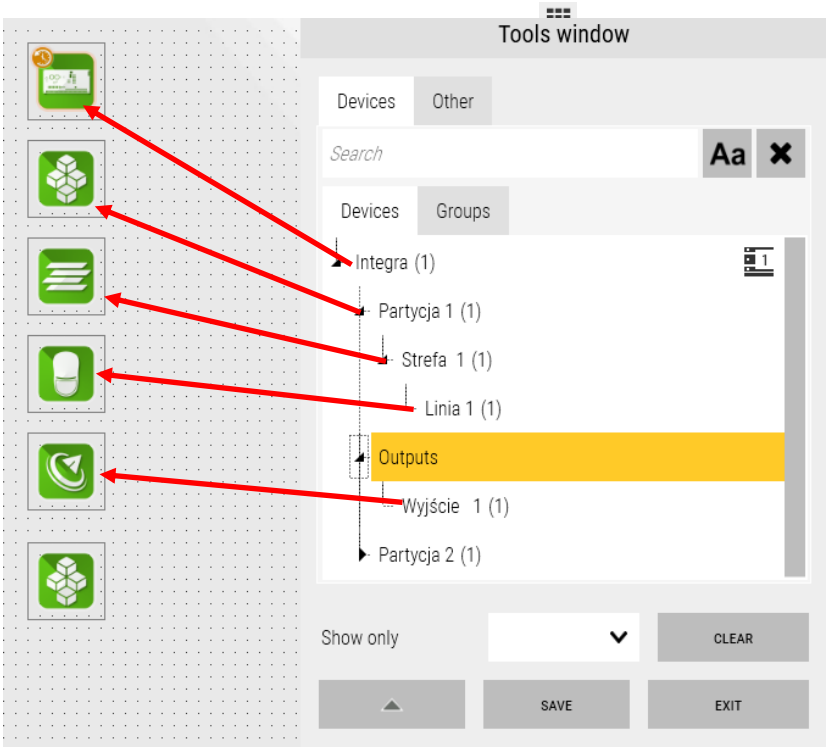
In the screenshots manager field **(1)** is possible to select channels from which images are captured. Use the **Capture** button **(5)** to capture the image currently displayed on the player, if the player is set to "live" mode, the current camera view is captured. The path to the folder where captured 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.

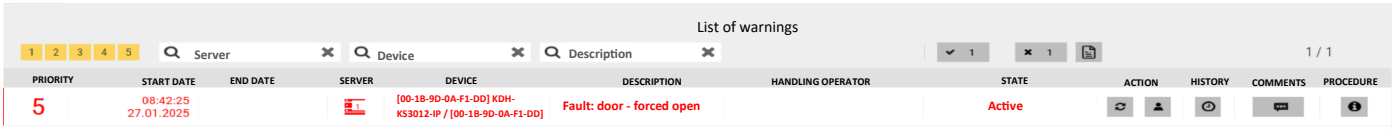
Actions that can also be performed include bypassing/unbypassing inputs and controlling the activation and

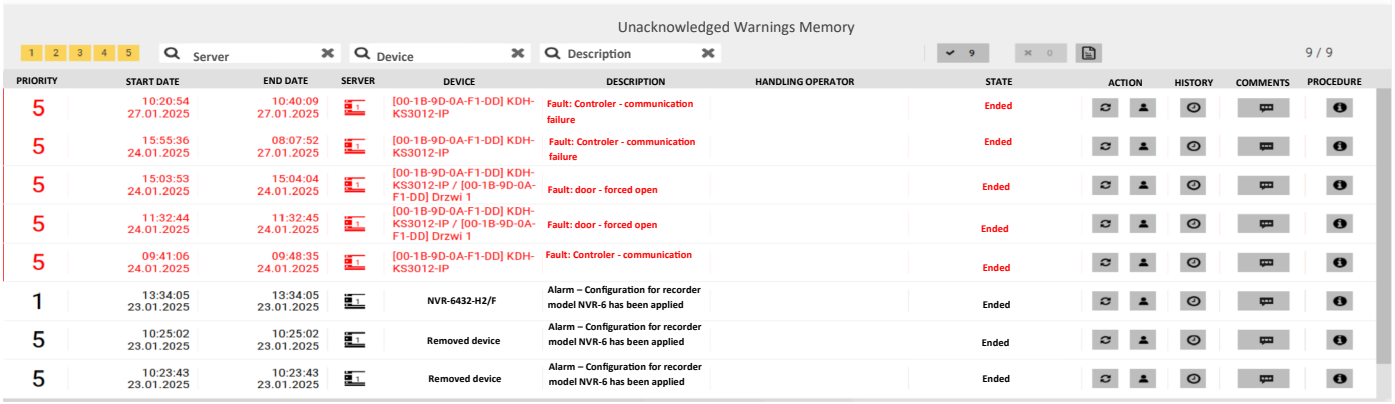
9.10 - Warning management tool: visualization and reporting

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.

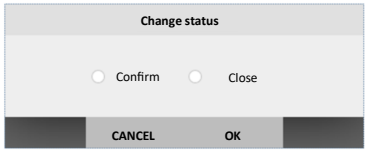
It is possible to generate reports that show the current status of alarms/failures (warnings) on the site, as well as the history of their occurrence along with operator comments.

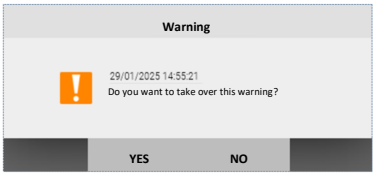
The tool is divided into two parts. The first part is a list of current warnings, which are those that are currently active. The second part is a memory of unacknowledged warnings, which refers to warnings that are no longer active but have not yet been confirmed.



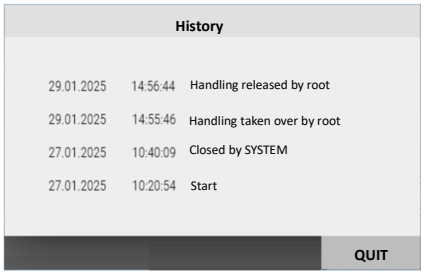


In the ACTIONS column, users have several options. They can mark a warning as acknowledged, close a current warning, or take over the handling of a specific warning.

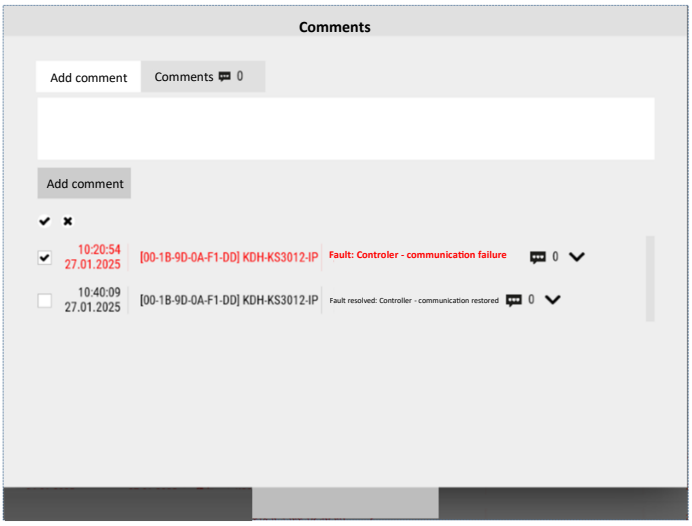




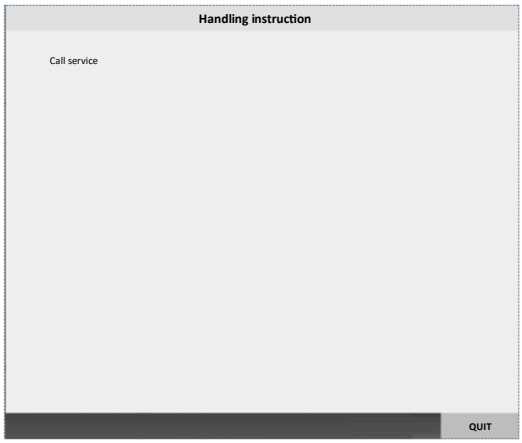
The HISTORY column allows users to view the event history associated with a given warning.



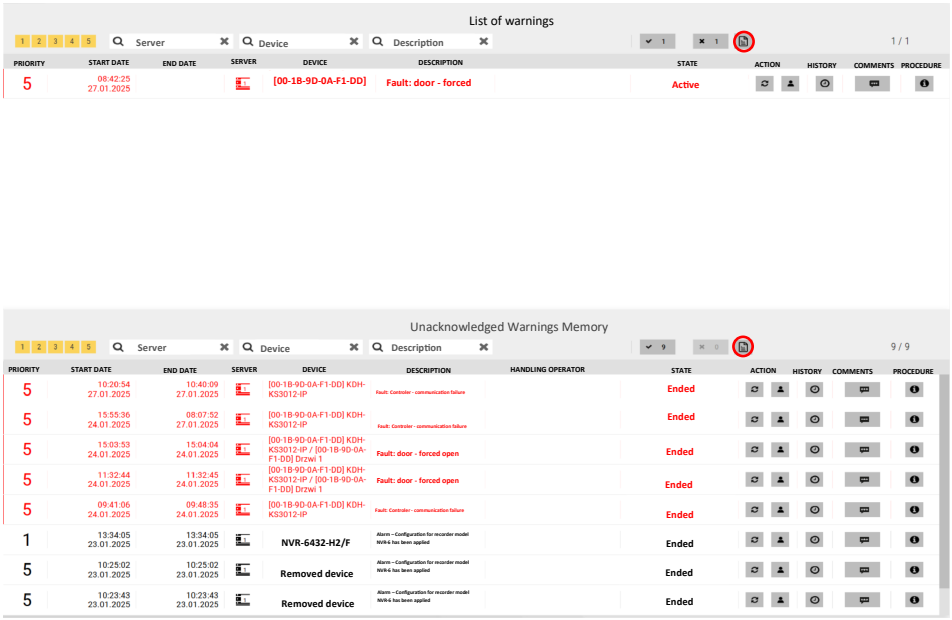
The COMMENTS column allows users to add or view a comment related to the warning and its resolution.

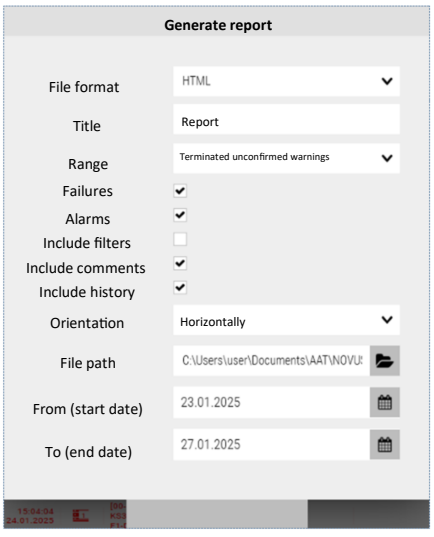


The INSTRUCTION column provides access to a procedure prepared by the installer for handling a specific warning. This instruction is added in the Configuration → Event Parameters menu.



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





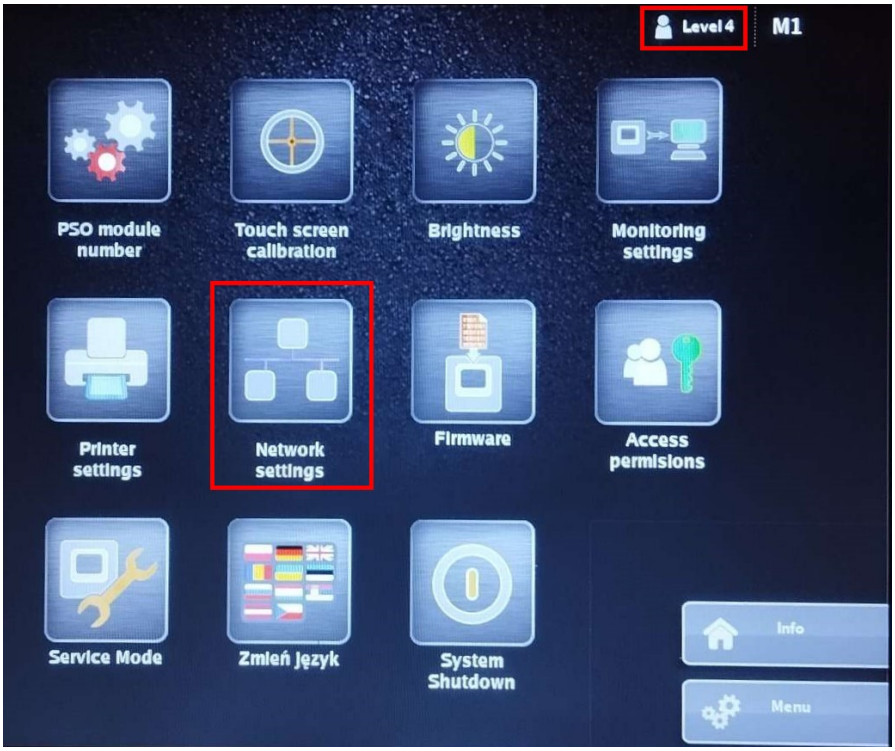
9.11 - Fire alarm system integration (visualization) Polon 6000

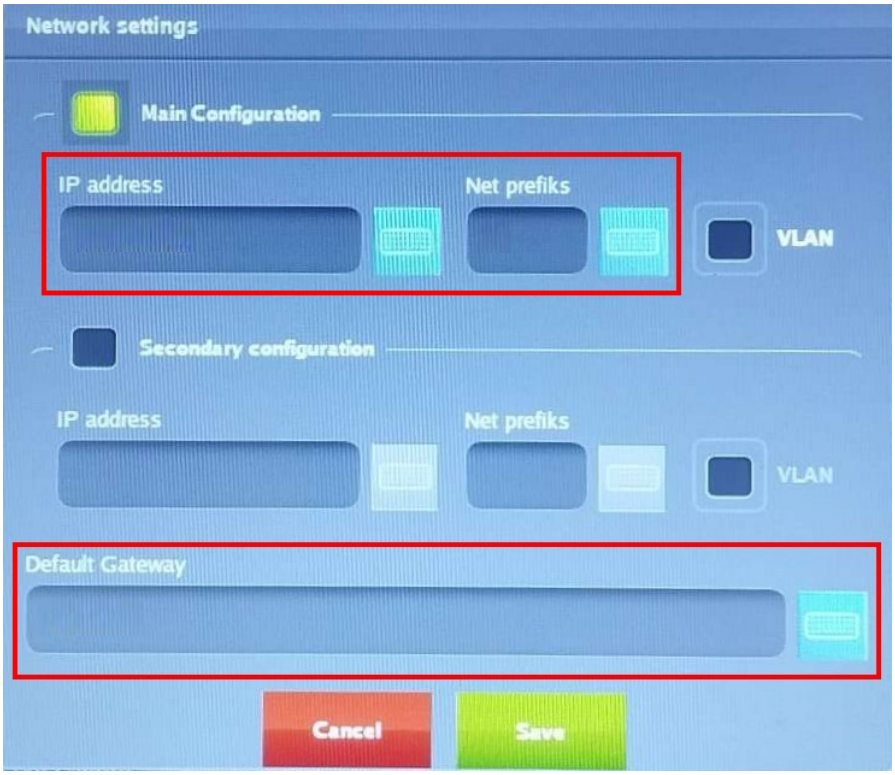
Configuration of the Polon 6000 fire alarm main panel to work with NOVUS MANAGEMENT SYSTEM AC software.

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:

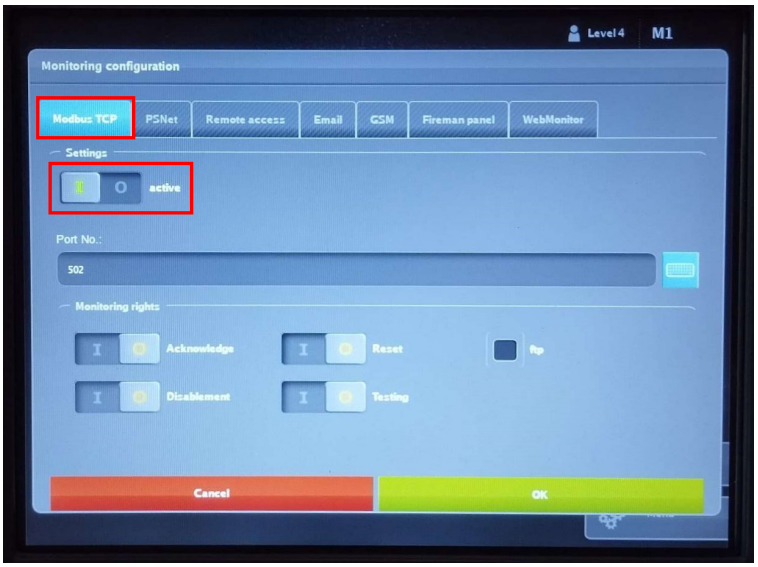
  Menu -> PSO Configuration-> Network setting





- Go to

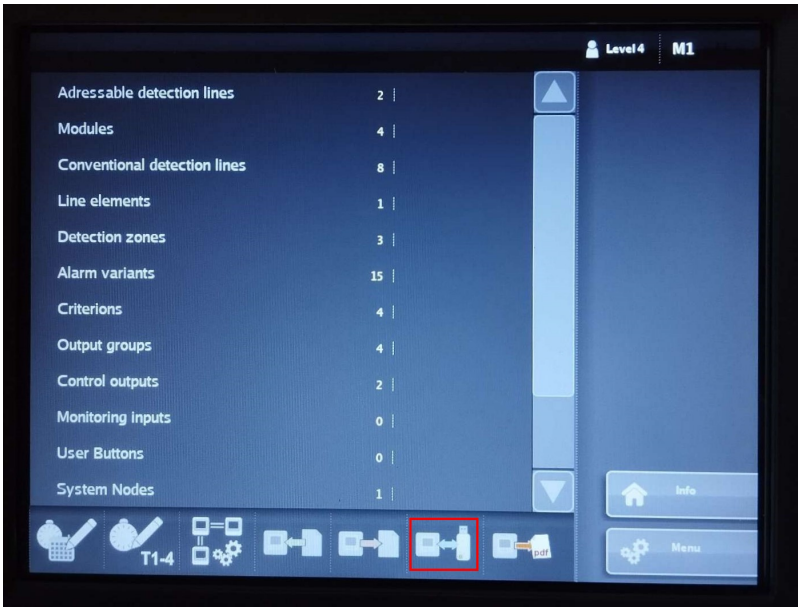
  Menu -> PSO Configuration-> Monitoring configuration
  MODBUS TCP -> enabled



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

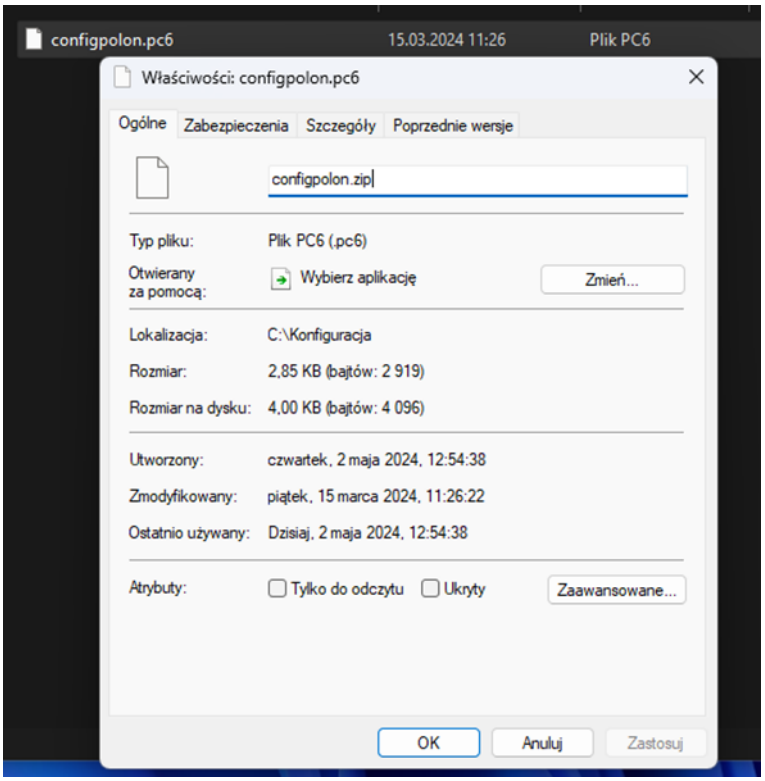
Export configuration from Polon 6000 main panel and import to the NOVUS MANAGEMENT SYSTEM AC software.

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

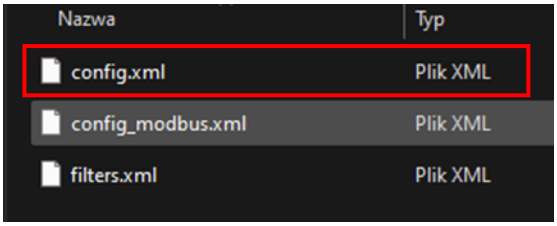


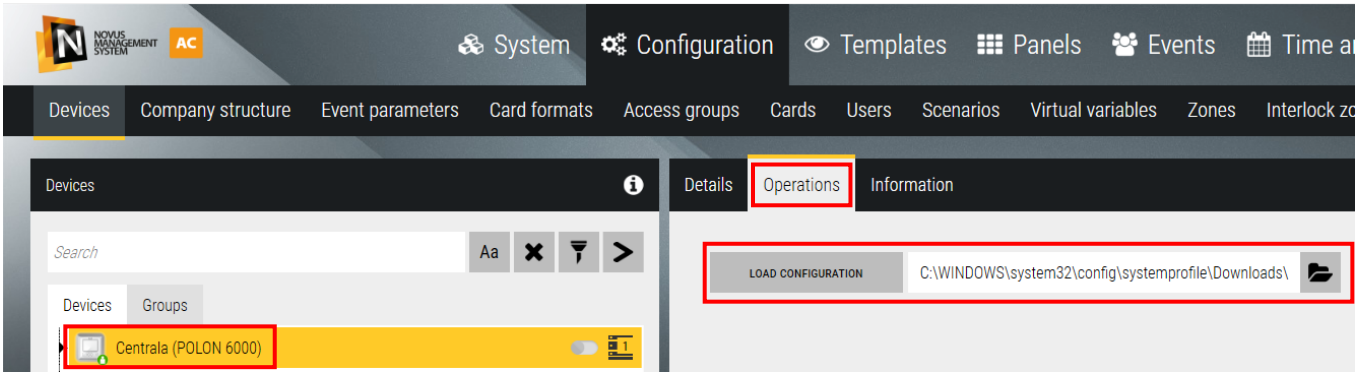
- We export the configuration to a Pendrive.

- 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



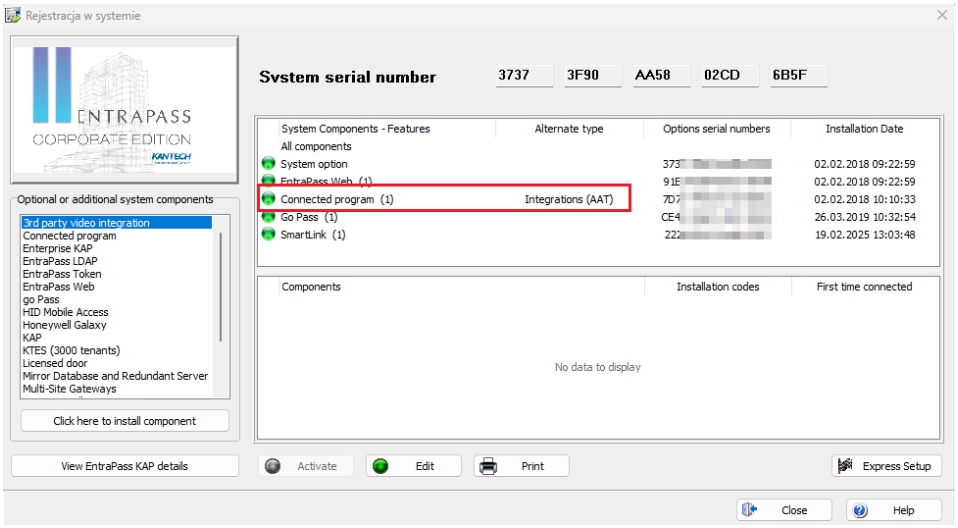


9.12 - Integration (visualization) with KANTECH access control system

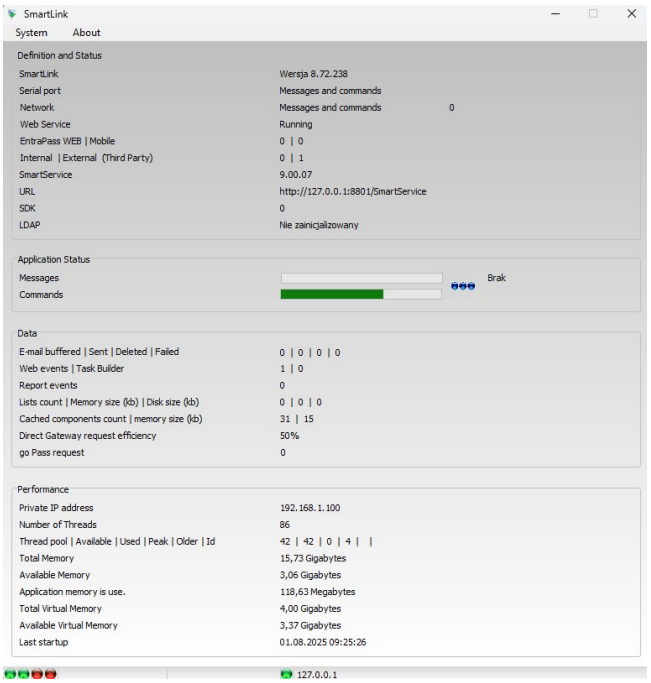
Configuring EntraPass software for cooperation with NOVUS MANAGEMENT SYSTEM AC software

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:

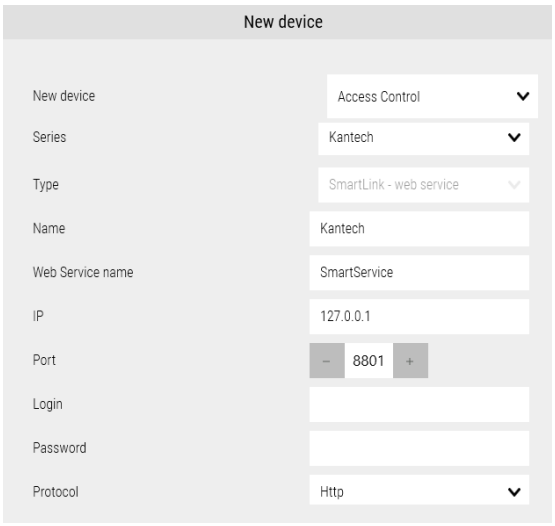


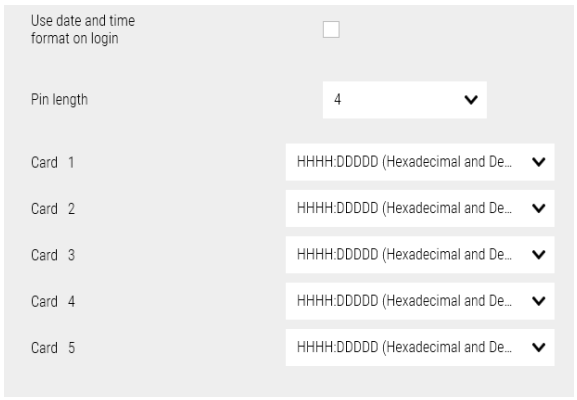
Configuration of NOVUS MANAGEMENT SYSTEM AC software for cooperation with KANTECH EntraPass program:

- 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

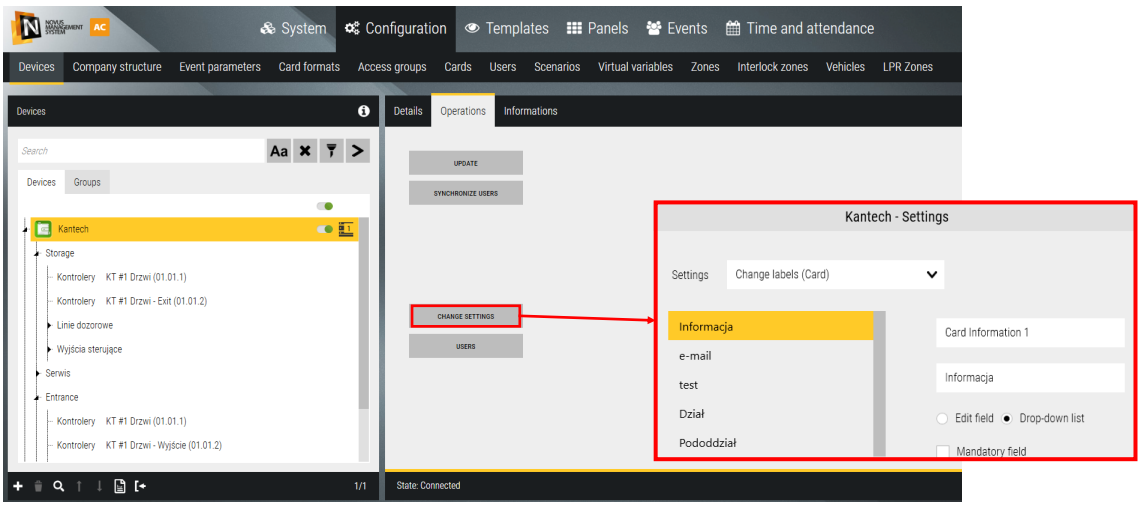
Login - username/operator name for the Entrapass system

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*

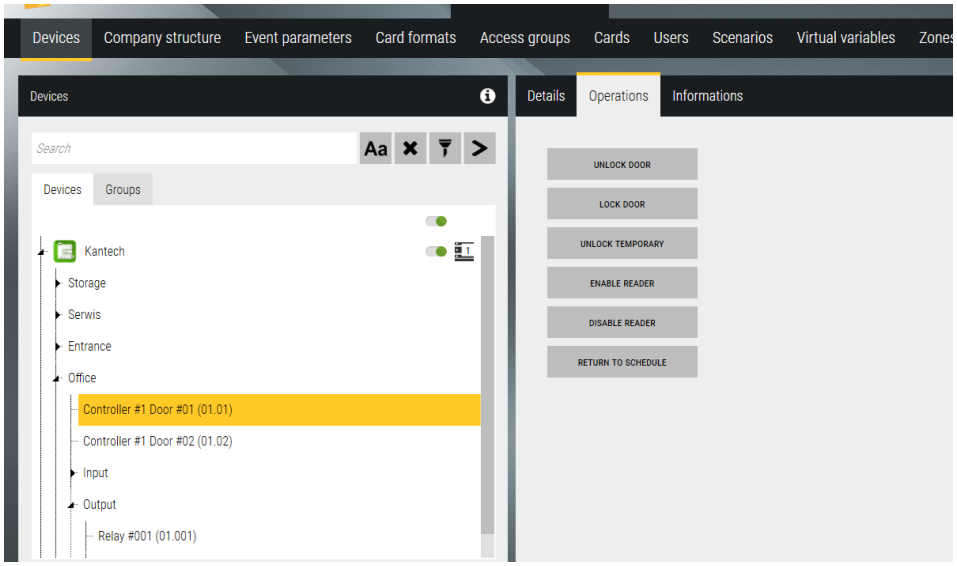


Update - Downloads information about all controllers, doors, alarm lines, and control outputs located in the EntraPass software and displays their list and status in a tree view in the device tab.

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:

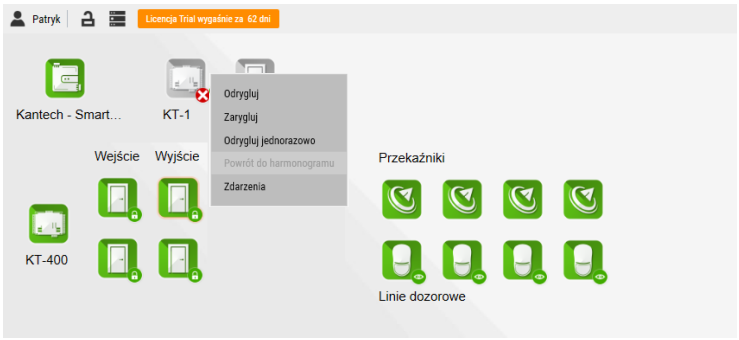


Door - unlock/lock door/unlock temporary/enable/disable reader/return to shedule

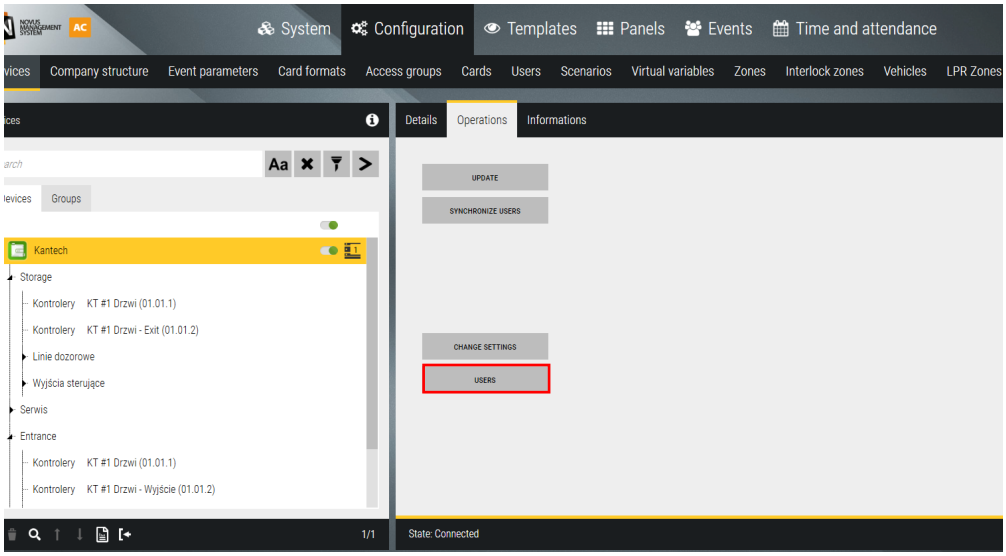
Output - turn on/turn off/turn on temporary/return to shedule

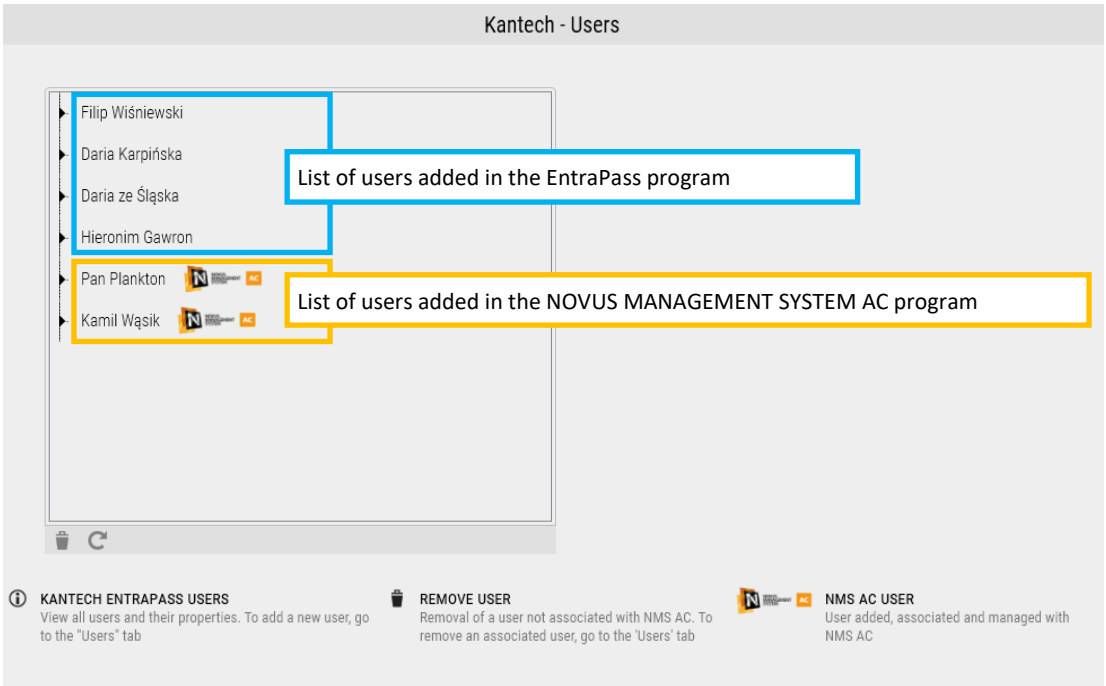
Input - active security/dismiss return to shedule

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

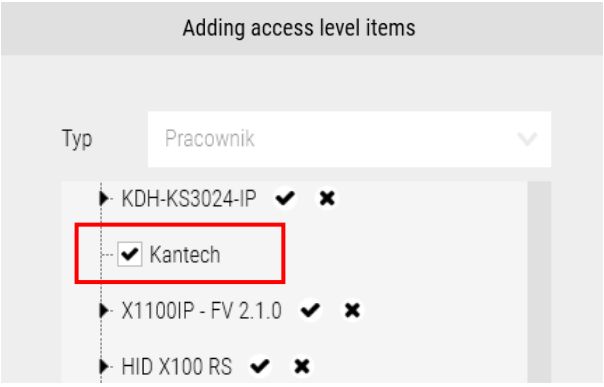


Users - displays a list of users assigned to EntraPass software

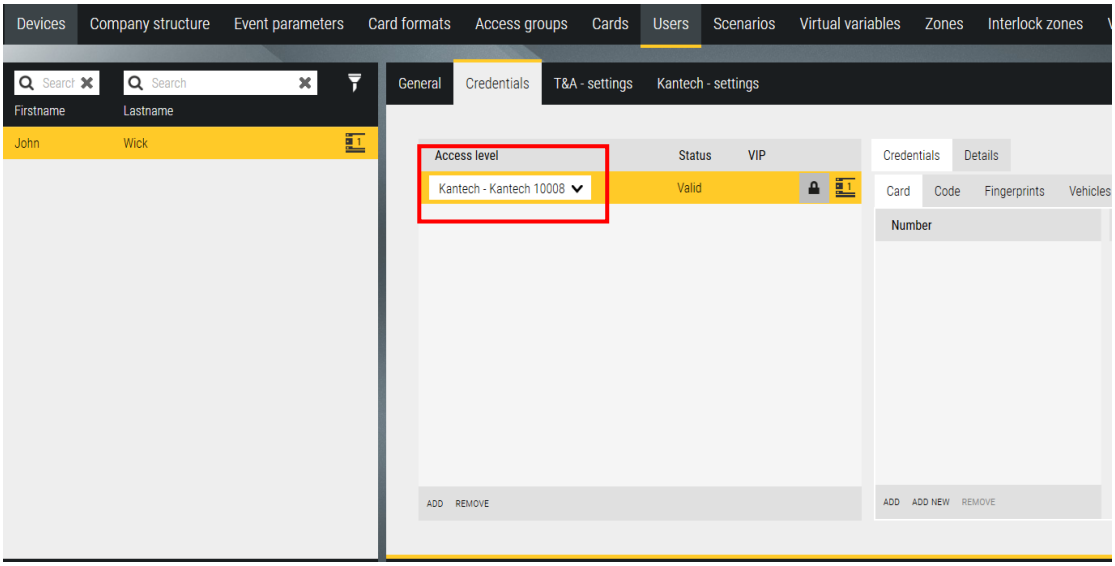




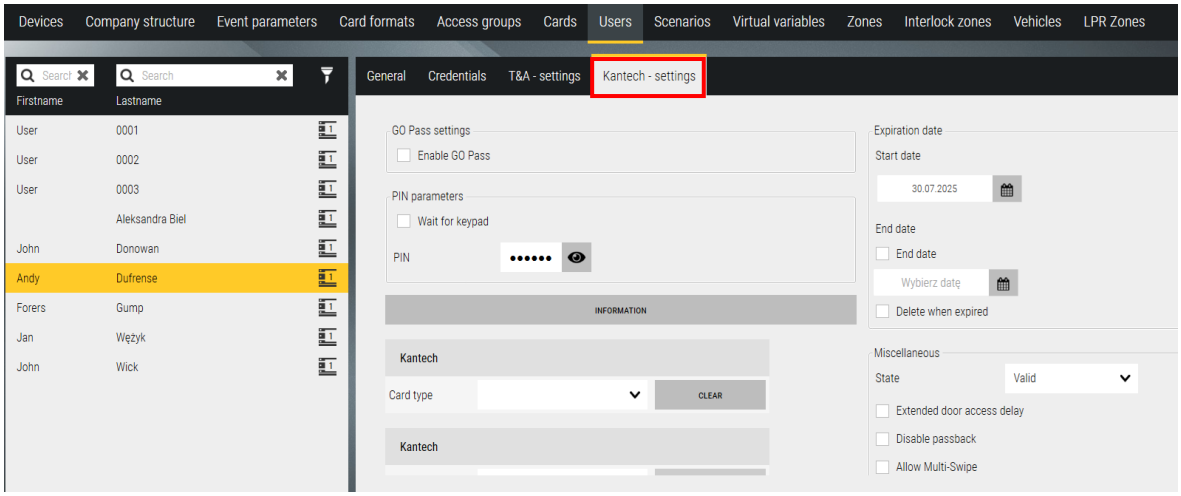
Adding users - To add a new user for the Kantech EntraPass system, we must first create an access level for the added system from the *Configuration/Access groups* menu.



(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)

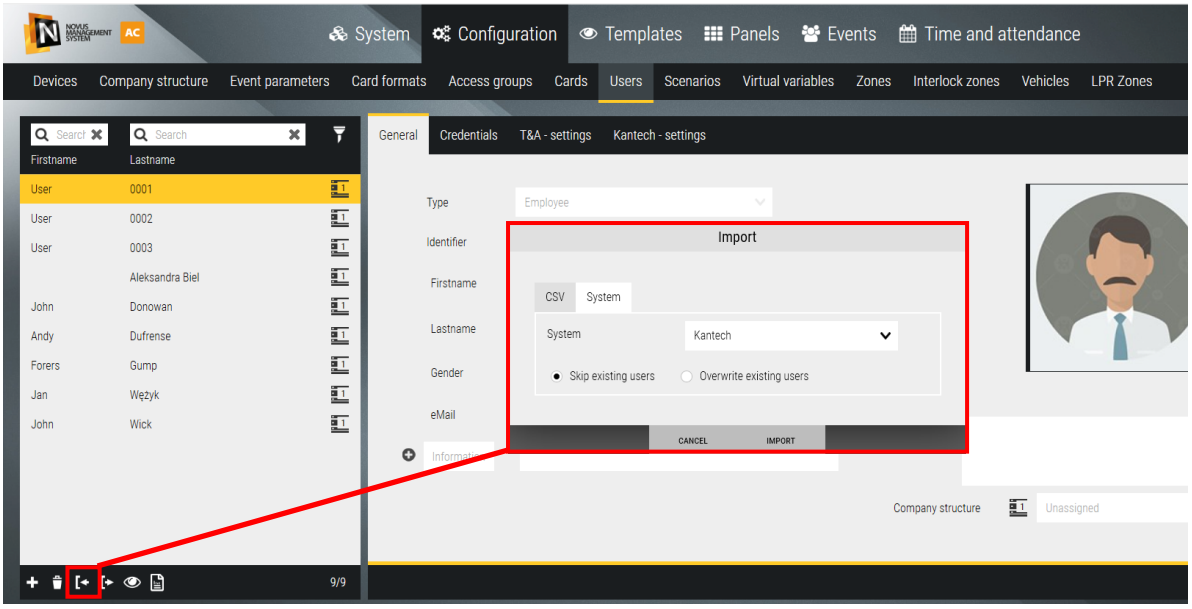
PIN parameters - wymuszenie używania PIN przez użytkownika, ustawienie kodu PIN

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.

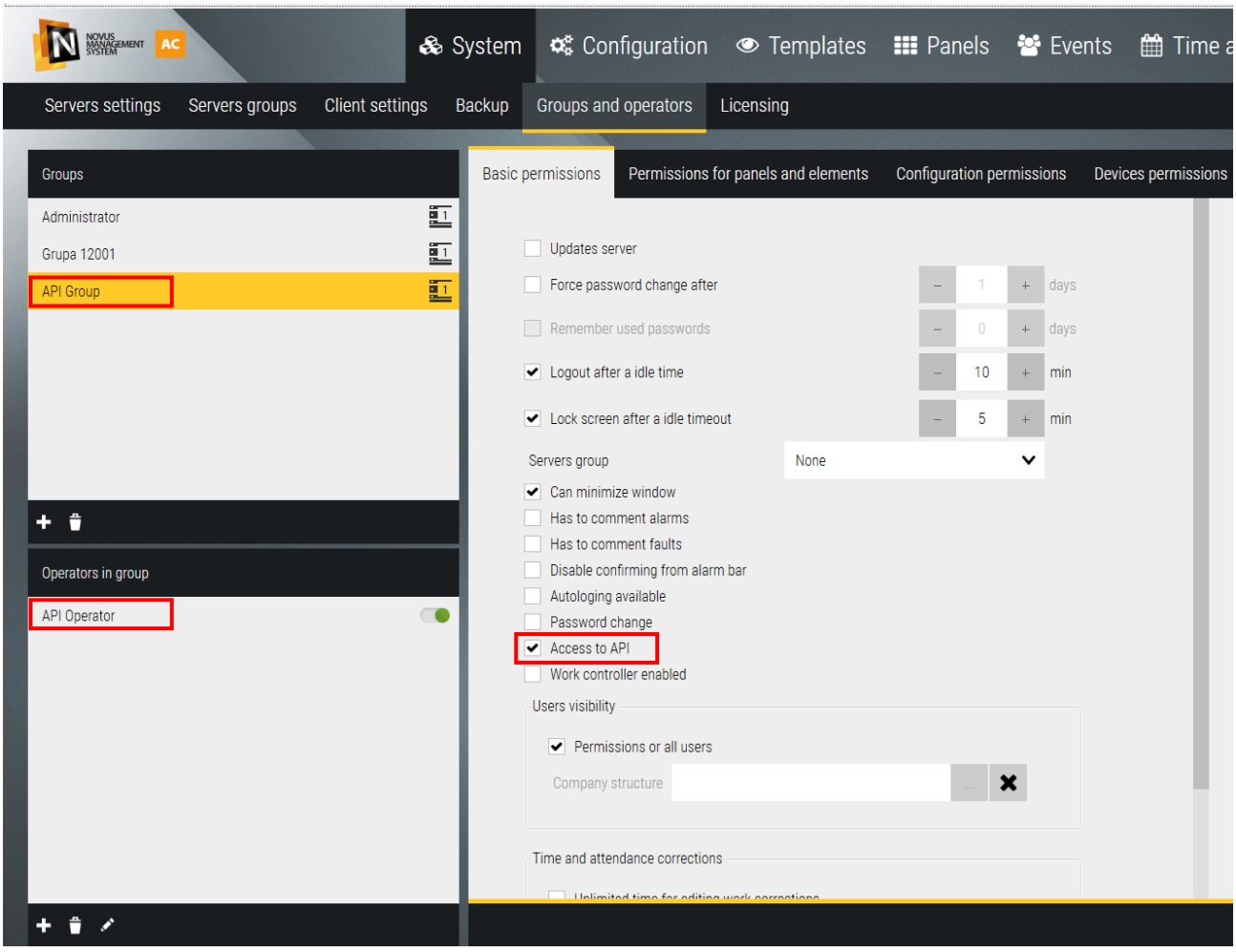
To use the API functionality, it is necessary to purchase a dedicated license for the NOVUS MANAGEMENT SYSTEM AC server (NOVUS MANAGEMENT SYSTEM AC API v5).

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.

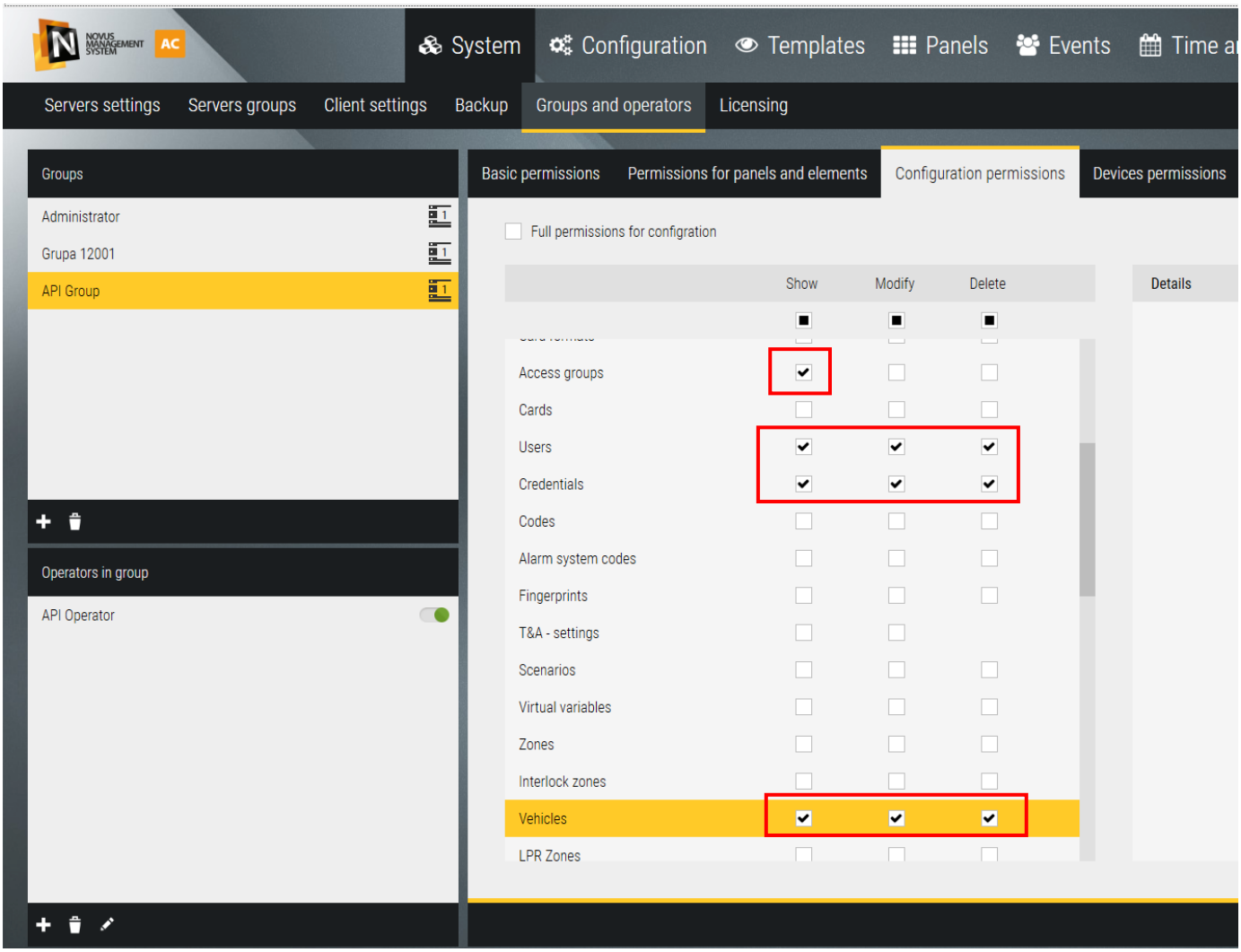
Sample initial configuration

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.

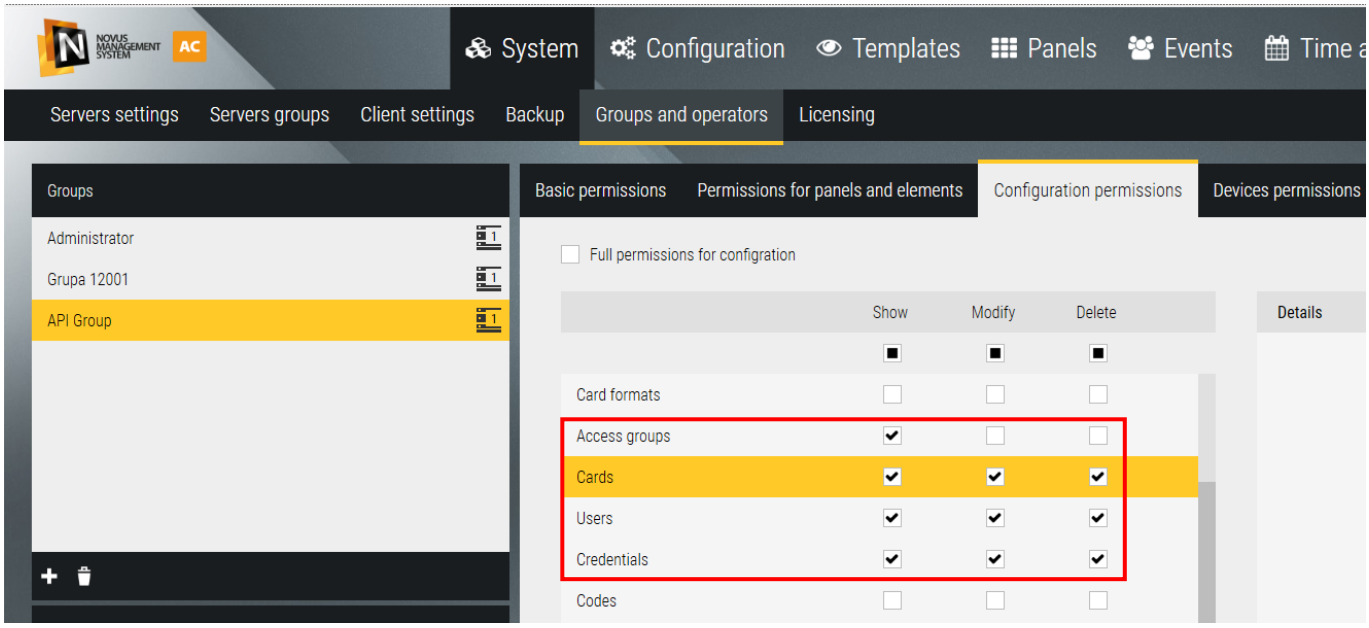


In addition, this group should be given appropriate permissions for the resources that will be modified.

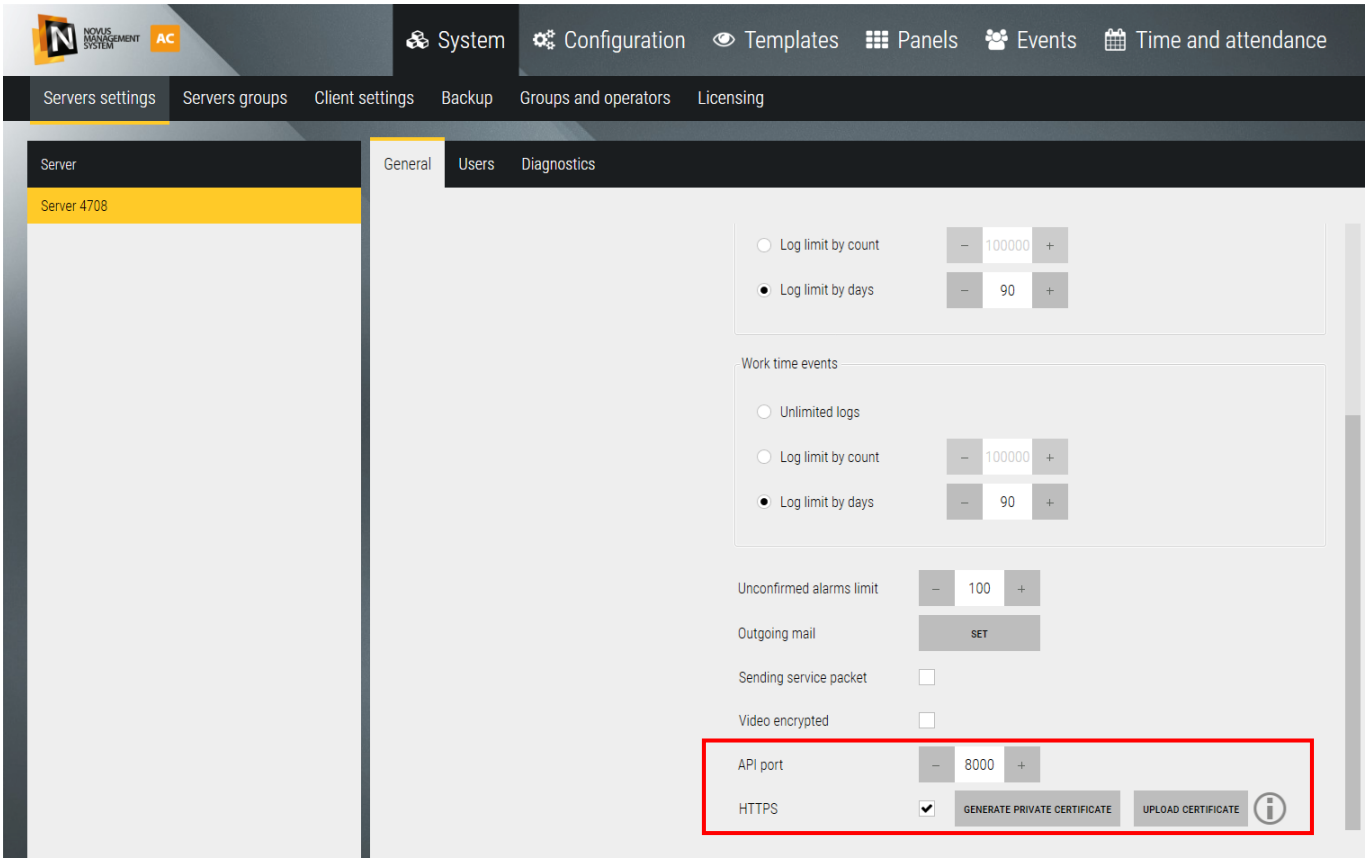
In the case of vehicles:



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

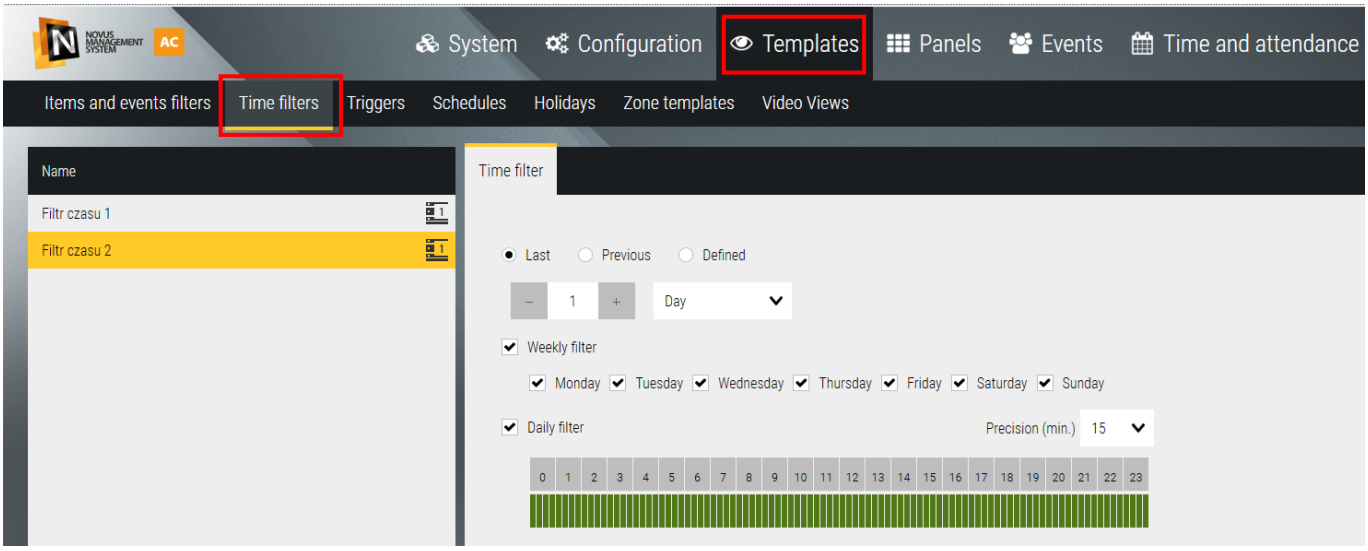
Getting events

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

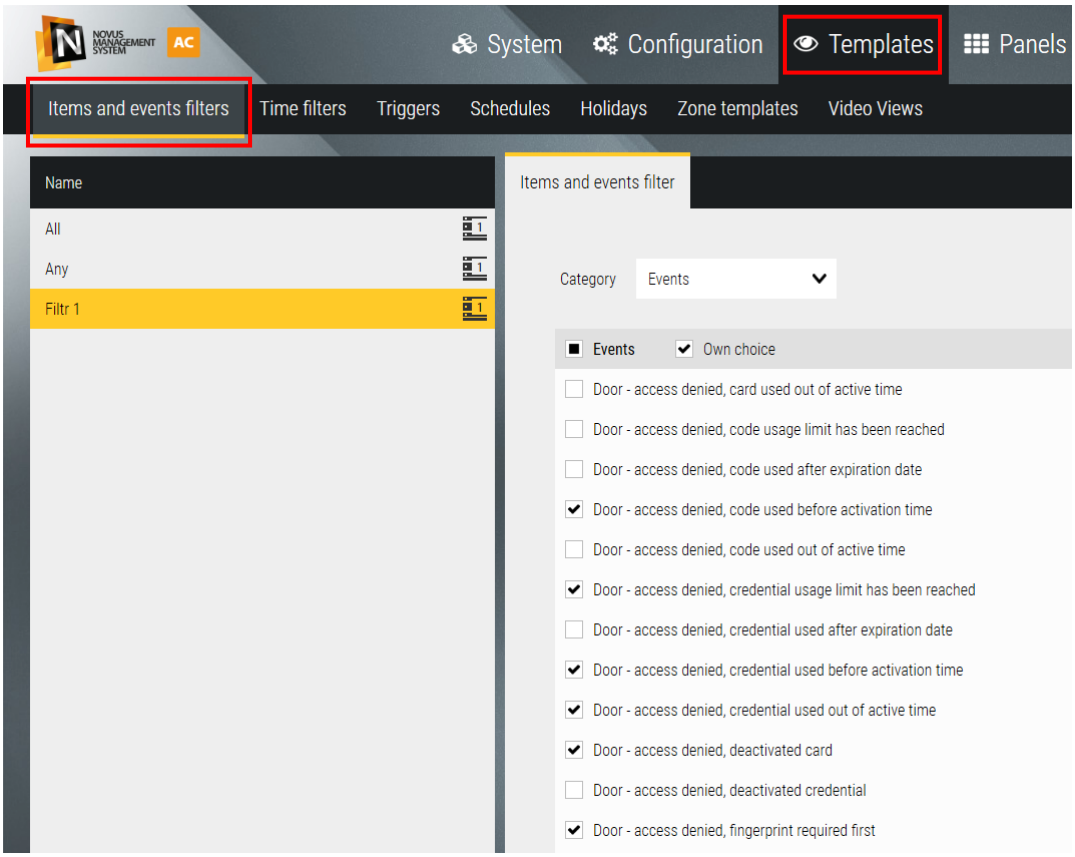
Parameters used to getting events

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

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



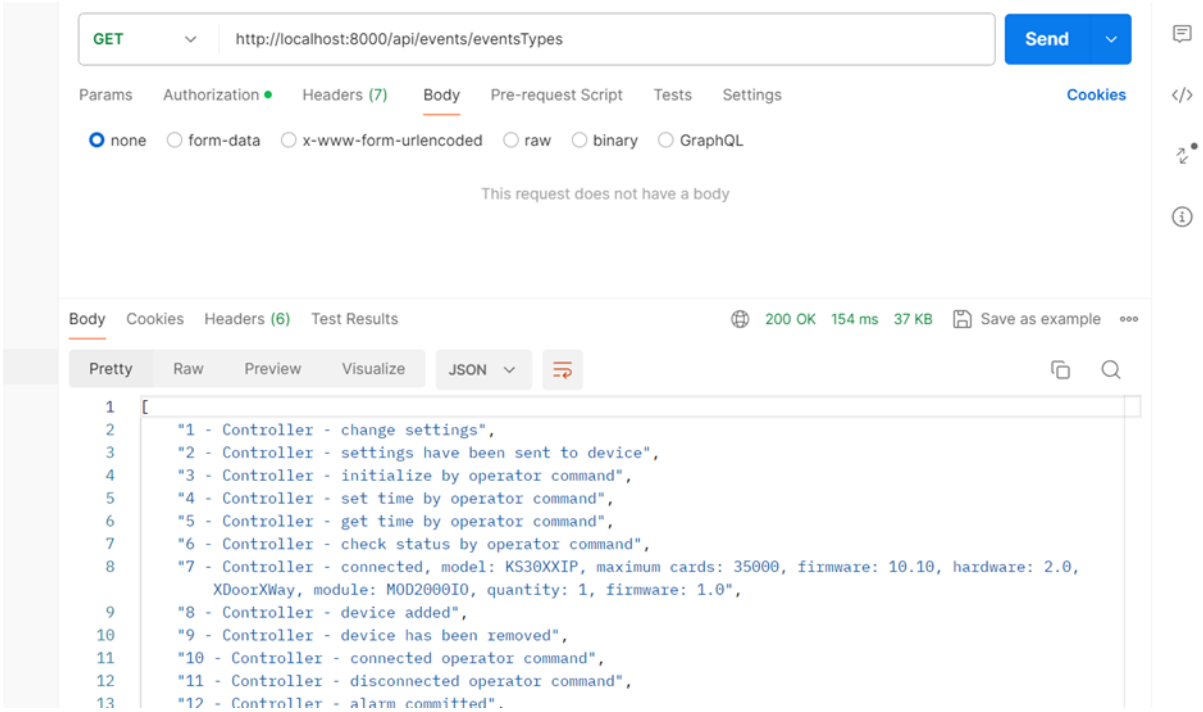
- Optionally, you can use Items and events filters defined in the software



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

Instrukcja instalacji i programowania

NOVUS MANAGEMENT SYSTEM AC

OPROGRAMOWANIE DO INTEGRACJI, KONFIGURACJI I WIZUALIZACJI SYSTEMÓW BEZPIECZEŃSTWA

Wersja programu 6.05.044 Aktualizacja: 08-05-2026

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

SPIS TREŚCI

Do czego służy i dla kogo jest przeznaczona niniejsza instrukcja.

Niniejsza instrukcja przeznaczona jest dla instalatorów oraz osób, które chcą się zapoznać z procesem instalacji programu NOVUS MANAGEMENT SYSTEM AC, programowania systemu oraz sprawdzenia poprawności jego działania pod względem komunikacyjnym oraz użytkowym. Dlatego opisane są w niej kolejne kroki jakie należy wykonać, żeby to zrealizować. Instrukcja ogranicza się w swojej treści do najważniejszych czynności jakie trzeba w tym celu wykonać. Kolejne kroki opisane są w zalecanej kolejności wykonywania. Powinno to stanowić znaczne ułatwienie dla osób, które potrzebują wykonać tylko podstawowe czynności związane z konfiguracją urządzeń wchodzących w skład systemu, dodaniem kart i użytkowników wraz z uprawnieniami w zakresie dostępu do pomieszczeń oraz sprawdzeniem stanu systemu i generowaniem podstawowych raportów.

Rozdział 1. WSTĘP

1.1 Informacje wstępne

NOVUS MANAGEMENT SYSTEM AC to oprogramowanie stanowiące kompleksową platformę do centralnego zarządzania systemami bezpieczeństwa, zaprojektowaną w oparciu o podział na systemy natywne oraz systemy zintegrowane. Takie podejście umożliwia elastyczne dopasowanie systemu do wymagań obiektu oraz istniejącej infrastruktury technicznej.

Systemy natywne

W ramach systemów natywnych NOVUS MANAGEMENT SYSTEM AC zapewnia pełną, bezpośrednią obsługę i zarządzanie następującymi rozwiązaniami:

Kontrola dostępu (KD): kontrolery standardowe typu KDH-KS3012-IP, KDH-KS3024-IP, KDH-KS3012-IP-II, KDH-KS3024-IP-II, KDH-KS3000-IP-ELV, biometryczne KDH-KZ3000FP-IP-U, KDH-KZ3000FP-IP-M, zintegrowane KDH-KZ3000-IP-U, KDH-KZ3000-IP-M, windowy KDH-KS3000-IP-ELV, kontrolery marki HID®Aero® - X1100, moduły rozszerzeń marki HID®Aero® - X100, X200, X300, system kontroli dostępu Kantech.

Rejestracja czasu pracy (RCP): terminale RCP typu KDH-TA500C-IP-U/M/D i KDH-TA500CFP-IP-U/M/D. W ramach integracji KD z RCP do jednego czytnika kontroli dostępu może zostać przypisana jedna funkcja systemu rejestracji czasu pracy.

Rozpoznawanie numerów tablic rejestracyjnych (LPR): kamery IP NVIP-2H-6732M/LPR, NVIP-4H-6732M/LPR, NVIP-2H-6732M/LPR-II, NVIP-4H-6732M/LPR-II serii 6000 marki NOVUS.

Systemy zintegrowane

NOVUS MANAGEMENT SYSTEM AC umożliwia także integrację i centralny nadzór nad systemami zewnętrznymi, do których należą:

Telewizja dozorowa (VSS): kamery IP NOVUS serii 4000/6000/8000, rejestratory IP NOVUS serii 4000/6000, rejestratory multistandard NOVUS serii 4000/6000 rejestratory IP NOVUS MANAGEMENT SYSTEM VSS, NMS oraz poprzez protokół ONVIF/RTSP z ze sprzętem innych producentów.

Sygnalizacja włamania i napadu (SSWiN): centrale alarmowe Integra firmy SATEL.

System sygnalizacji pożaru (SSP): centrale Polon 6000.

Sterowanie modułami I/O: Moduł sieciowy wejść/wyjść LANKON-008, który umożliwia realizację funkcji automatyki oraz sterowanie urządzeniami peryferyjnymi.

Dzięki strukturze typu multi-klient, multi-serwer możliwa jest obsługa systemu z wielu stanowisk (1 stacja operatora w standardzie, dodatkowe po zakupie licencji rozszerzających). System jest prosty w instalacji i posiada przyjazny interfejs graficzny dla operatora. Dzięki wprowadzeniu kilku zaawansowanych funkcji może znaleźć również zastosowanie w systemach z wieloma lokalizacjami.

Interfejs operatora umożliwia:

- definiowanie parametrów systemu (uprawnień dla operatorów, licencji, kopii)
- konfigurację parametrów fizycznych elementów systemu (kontrolery, drzwi, czytniki)
- konfiguracja i wizualizacja systemów w z wielu lokalnych serwerów jednocześnie (multi-klient)
- definiowanie elementów logicznych (terminarze, poziomy dostępu, karty)
- definiowanie scenariuszy reagujących automatycznie na zdarzenia w systemie
- monitorowanie stanu systemu „on-line" za pomocą ikon elementów systemu zlokalizowanych na mapach obiektu na tablicy synoptycznej i poprzez komunikaty wyświetlane na stosie zdarzeń
- wyświetlanie zdjęć użytkownika po użyciu karty wraz ze stopklatką z kamery
- wyświetlanie obrazu z kamer zlokalizowanych w kontrolowanych przejściach - automatycznie po zdarzeniu lub po kliknięciu na ikonie
- kontrola dostępu do pięter poprzez czytnik umieszczony w kabinie windowej z opcją odblokowania wszystkich lub wybranych pięter przez operatora lub terminarz; (*opcja dostępna wkrótce)
- generowanie filtrowanych raportów zdarzeń (automatycznie lub na żądanie) i zapis w formacie csv lub html (z opcją drukuj do pdf)
- generowanie raportów RCP na postawie harmonogramów czasu pracy oraz wyświetlanie listy obecności
- definiowanie struktury firmy
- wysyłanie powiadomień dotyczących rozliczenia czasu pracownika pracy na jego służbowy email
- podgląd, odtwarzanie oraz eksport nagrań wideo/audio
- wizualizację oraz obsługę systemów alarmowych SATEL opartych o centrale Integra
- obsługę parkingu z kontrolowanym wjazdem

Program NOVUS MANAGEMENT SYSTEM AC oferuje również szereg funkcji opisanych szczegółowo w dalszej części instrukcji, które umożliwiają spełnienie wymagań stawianych często przez administratora systemu jak przykładowo: dostęp po użyciu 2, 3 lub 4 kart, pierwsze otwarcie kontrolowanego przejścia za pomocą tzw. „pierwszej karty" ze specjalnymi uprawnieniami, multi-odczyt, dostęp po potwierdzeniu przez operatora, śluza i anti-passback w obrębie kontrolera, wizualizacja stref globalnych oraz generator raportów RCP. Program będzie sukcesywnie rozbudowywany o nowe funkcje.
Lista najważniejszych funkcji i parametrów systemu przedstawiona jest w załączonych tabelach, a struktura systemu pokazana jest na załączonym schemacie blokowym. Kontrolery z portami IP komunikują się z usługą serwera poprzez sieć Ethernet.

1.2 Funkcje i parametry systemu NOVUS MANAGEMENT SYSTEM AC

Ogólne	
Nazwa parametru lub funkcji	**Wartość parametru lub opis funkcji**
System operacyjny PC	Windows 10/11 Pro 64 Bit Windows 10/11 IoT 64 Bit
Baza danych	Microsoft SQL 2022
Język	angielski, polski, azerski, węgierski
Monitoring „on-line”	TAK
Multi-serwerowość (systemy rozproszone)	TAK
Struktura klient-serwer	TAK
Obsługa wielu monitorów	TAK, do 6 monitorów
Wizualizacja systemu na panelach	TAK
Definiowane scenariusze zadziałania	TAK
Definiowanie grup elementów	TAK
Import danych użytkowników z pliku	TAK
Komunikacja	
Wbudowane porty IP	poprzez sieć Ethernet
Raporty zdarzeń	Filtrowane, zapis w formacie csv, html, pdf
Systemy natywne	
Kontrola dostępu (KD)	TAK, KaDe, HID®Aero®
Rejestracja czasu pracy (RCP)	TAK, KaDe, HID®Aero®,Kantech
Rozpoznawanie tablic rejestracyjnych (LPR)	TAK, NOVUS
Systemy integrowane	
Kontrola dostępu (integracja/wizualizacja)	Tak, Kantech
Telewizja dozorowa (VSS)	TAK, NOVUS, ONVIF, RTSP
Sygnalizacja włamania i napadu (SSWiN)	TAK, SATEL Integra
Moduły sterowania I/O	TAK, Tinycontrol
System sygnalizacji pożarowej (SSP)	TAK, POLON 6000

Kontrola dostępu (KD) marki KaDe	
Nazwa parametru lub funkcji	**Wartość parametru lub opis funkcji**
Monitoring „on-line”	TAK
Wyświetlanie zdjęć użytkowników	TAK
Funkcje związane z dostępem	
- tryb identyfikacji użytkownika	Karta, PIN, Karta lub PIN, Karta + PIN, Odcisk palca i kombinacje z kartą lub PIN
- anti-passback lokalny	TAK
- anti-passback globalny, multi-śluza globalna	TAK
- „pierwsza karta otwierająca”	TAK
- dostęp po potwierdzeniu przez operatora	TAK
- dostęp po użyciu wielu kart (od 2 do 4)	TAK
- multi-odczyt karty (2 i 3)	TAK
- sekwencyjne odryg./zaryglow. drzwi kartą	TAK
- odryglowanie zgodnie z terminarzem po od-czycie ważnej karty lub automatycznie	TAK
Funkcje alarmowe	
- kod dyskretnego alarmu	TAK
Import danych użytkowników z pliku	TAK
Kontrolery	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
Pojemność pamięci kontrolera KaDe	
- pamięć kart	20 000
- pamięć zdarzeń	50 000
Komunikacja	
Wbudowane porty IP	- poprzez sieć Ethernet
Czytniki i karty	
- format kart	Zgodny z formatem 26-40 bit Wiegand
- typ kart	Dowolna technologia zgodna z czytnikiem
Raporty zdarzeń	Filtrowane, zapis w formacie csv, html (pdf)
Raporty RCP (z terminali lub z czytników KD)	Rozliczanie czasu pracy na podstawie harm.
Obsługa wind	Z wykorzystaniem kontrolera KDH-KS3000-IP-ELV oraz modułów rozszerzeń KDH-MOD3016-ELV, KDH-MOD3004-ELV
Maks. ilość obsługiwanych pięter	Do 69

Kontrola dostępu (KD) marki HID®Aero®	
Nazwa parametru lub funkcji	**Wartość parametru lub opis funkcji**
Monitoring „on-line”	TAK
Wyświetlanie zdjęć użytkowników	TAK
Funkcje związane z dostępem	
- tryb identyfikacji użytkownika	Karta, PIN, Karta lub PIN, Karta + PIN, Odcisk palca i kombinacje z kartą lub PIN
- anti-passback lokalny	TAK
- anti-passback globalny, multi-śluza globalna	TAK
- „pierwsza karta otwierająca”	TAK
- dostęp po potwierdzeniu przez operatora	TAK
- dostęp po użyciu wielu kart	TAK
- multi-odczyt karty (2-krotny)	TAK
- odryglowanie zgodnie z terminarzem po odczycie ważnej karty lub automatycznie	TAK
- obsługa funkcji kodu lokalizacji (FC)	TAK
Import danych użytkowników z pliku	TAK
Kontrolery oraz moduły rozszerzeń	Inteligentny kontroler IP HID® Aero® X1100, kontroler rozszerzeń przejść RS HID® Aero® X100, moduł rozszerzeń wejść RS HID® Aero® X200, moduł rozszerzeń wyjść RS HID® Aero® X300
Pojemność pamięci kontrolera HID® Aero® X1100	
- pamięć kart	250 000 (kontroler master)
- pamięć zdarzeń	50 000
Komunikacja	
Wbudowane porty TCP/IP	Poprzez sieć Ethernet (do kontrolera master)
Wbudowany port RS-485	Do szyfrowanej komunikacji z modułami rozszerzeń
Czytniki i karty	
- format kart	Wieloformatowy
- typ kart	Dowolna technologia zgodna z czytnikiem
- czytnik	Zgodne z WIEGAND lub OSDP
Raporty zdarzeń	Filtrowane, zapis w formacie csv, html (pdf)
Raporty RCP (z terminali lub z czytników KD)	Rozliczanie czasu pracy na podstawie harm.
Obsługa wind	Z wykorzystaniem inteligentnego kontrolera IP HID® Aero® X1100, modułu rozszerzeń wyjść RS HID® Aero® X300 oraz modułu rozszerzeń wejść RS HID® Aero® X200
Maks. ilość obsługiwanych pięter	Do 128
Potwierdzenie wyboru piętra	Tak, z wykorzystaniem modułu rozszerzeń wejść RS HID® Aero® X200

Kontrola dostępu (KD) marki KANTECH	
Nazwa parametru lub funkcji	**Wartość parametru lub opis funkcji**
Komendy	Aktualizuj Zarygluj / odrygluj drzwi Odrygluj drzwi czasowo Powrót do terminarza Włącz / wyłącz czytnik Włącz / wyłącz przekaźnik Włącz przekaźnik czasowo Włącz / wyłącz monitorowanie linii dozorowych
Zdarzenia	Alarm Uszkodzenie kontrolera Drzwi zaryglowane / odryglowane Drzwi przetrzymane Drzwi w stanie normalnym Drzwi sforsowane Czytnik aktywny / nieaktywny Dostęp zezwolony / zabroniony Monitorowanie linii dozorowej włączone / wyłączone Przekaźnik włączony / wyłączony Utrata komunikacji Powrót komunikacji Rozłączony przez operatora
Zarządzanie użytkownikami	Podgląd użytkowników i kart skonfigurowanych za pomocą EntraPass Dodawanie i usuwanie użytkowników i kart z poziomu NOVUS MANAGEMENT SYSTEM AC
Obsługa wind	Z wykorzystaniem systemu KANTECH

Rejestracja czasu pracy (RCP)	
Nazwa parametru lub funkcji	**Wartość parametru lub opis funkcji**
Wspierane urządzenia	
Terminale RCP	KDH-TA500CFP-IP-U/M/D, KDH-TA500C-IP-U/M/D
Kontrolery	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, inteligentny kontroler HID®Aero® X1100 IP (kontroler master), kontroler rozszerzeń przejść HID®Aero® X100 RS (SLAVE), kontrolery integrowanego systemu Kantech
Struktura firmy	TAK
Wideoweryfikacja zdarzeń	TAK
Korekty zdarzeń	TAK
Lista obecności	TAK
Automatyczne raporty	TAK
Tryb jednozmianowy	TAK
Tryb wielozmianowy	TAK (od 1 do 4 zmian w ciągu doby)
Harmonogramy czasu pracy	TAK
Kalendarze czasu pracy	TAK
Raporty zdarzeń	Filtrowane, zapis w formacie csv, html (pdf)
Raporty RCP (z terminali lub z czytników KD)	Rozliczanie czasu pracy na podstawie harm.

Telewizja dozorowa VSS	
Nazwa parametru lub funkcji	**Wartość parametru lub opis funkcji**
Wideo	TAK
Wspierane urządzenia	Kamery IP Novus serii 4000/6000/8000, Kamery IP ONVIF/RTSP, Rejestratory IP Novus serii 4000/6000, Rejestratory multistandard Novus serii 4000/6000 Rejestratory IP NOVUS MANAGEMENT SYSTEM VSS / NMS
Ilość obsługiwanych kanałów wideo/audio	Brak ograniczeń programowych
Wspierane protokoły	Novus, ONVIF, RTSP
Wspierane kodeki	H.264, H.264+, H.265, H.265+, MJPEG
Wsparcie obsługi urządzeń jednostrumieniowych	TAK
Wsparcie dla kamer fisheye	TAK
Wyświetlanie	TAK
Obsługa wielu monitorów	TAK, do 6 monitorów
Rozdzielczość maksymalna	6 x 4K UltraHD
Odtwarzanie nagrań	TAK
Odtwarzanie do przodu	TAK
Przyspieszone odtwarzanie	TAK, do x10
Spowolnione odtwarzanie	TAK, do x0.1
Odtwarzanie do tyłu	TAK
Pobieranie nagrań	TAK
Format pobieranych nagrań	AVI, MP4
Dołączanie metadanych do wideo	TAK, nazwa kanału, nazwa urządzenia, znak wodny, znacznik czasu
Harmonogram pobierania nagrań	TAK
Alarmy	TAK
Wejścia/wyjścia alarmowe w kamerach / rejestratorach	TAK, wsparcie wejść/wyjść alarmowych dostępnych w kamerach
Detekcja ruchu	TAK, wsparcie detekcji ruchu dostępnej w kamerach /rejestratorach
Analiza obrazu	TAK, wsparcie funkcji analizy obrazu dostępnych w kamerach / rejestratorach
Rozpoznawanie numerów tablic rejestracyjnych (LPR)	TAK, współpraca z kamerami Novus NVIP-2H-6732M/LPR NVIP-4H-6732M/LPR NVIP-2H-6732M/LPR-II NVIP-4H-6732M/LPR-II
Sterowanie PTZ	TAK
Funkcje PTZ	obrót, uchył, zoom, presety, trasy, patrole, skanowania, focus, iris
Inne	TAK
Możliwość łączenia urządzeń telewizji dozorowej na żądanie	TAK

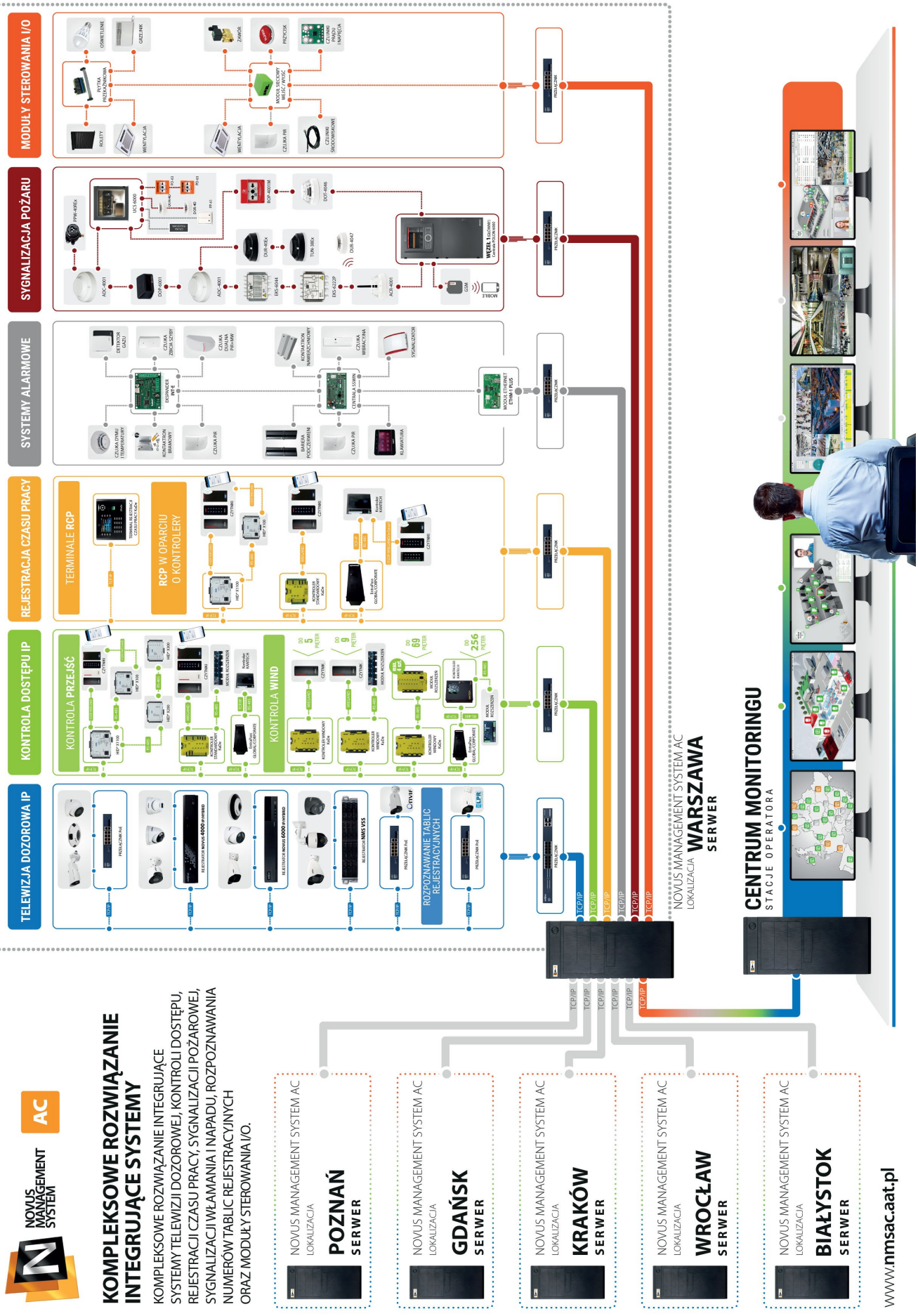
Rozpoznawanie tablic rejestracyjnych (LPR)	
Nazwa parametru lub funkcji	**Wartość parametru lub opis funkcji**
Wspierane urządzenia	Kamery IP Novus NVIP-2H-6732M/LPR, NVIP-4H-6732M/LPR, NVIP-2H-6732M/LPR-II, NVIP-4H-6732M/LPR-II podłączone bezpośrednio lub za pośrednictwem rejestratora IP NOVUS MANAGEMENT SYSTEM VSS, NMS
Ilość obsługiwanych kamer	Brak ograniczeń programowych
Wsparcie drukarek kodów QR	TAK
Stefy parkingowe	TAK
Poziomy dostępu	TAK
Harmonogramy działania	TAK
Wizualizacja ilości pojazdów w strefach	TAK
Baza numerów tablic rejestracyjnych	TAK
Import/eksport numerów tablic rejestracyjnych	TAK
Wyszukiwanie zdarzeń związanych z rozpoznaniem	TAK
Definiowanie reakcji związanych z rozpoznaniem	TAK
Limit pojazdów w strefie parkingowej	TAK
Współpraca ze szlabanami, bramami itp.	TAK
Obsługa przycisków wjazdu	TAK
Alarmy	TAK
Wejścia/wyjścia alarmowe w kamerach / rejestratorach	TAK, wsparcie wejść/wyjść alarmowych dostępnych w kamerach

System sygnalizacji włamania i napadu (SSWiN)	
Nazwa parametru lub funkcji	**Wartość parametru lub opis funkcji**
Wspierane urządzenia	Centrale alarmowe Satel: Integra 24, Integra 32, Integra 64, Integra 64 Plus, Integra 128, Integra 128 Plus, Integra 128-WRL, Integra 256 Plus
Funkcje wykonawcze	Uzbrojenie rozbrojenie partycji, uzbrojenie rozbrojenie wszystkich partycji, uzbrojenie/ rozbrojenie strefy, uzbrojenie/rozbrojenie wszystkich stref, blokowanie czujki, odblokowanie czujki, kasuj alarm partycji, kasuj alarm strefy, kasuj alarm wszystkich stref, kasuj historię pamięci alarmów, wł./wył. wyjście, podgląd aktualnych użytkowników centrali, wprowadź pierwsze hasło, aby uzbroić, wprowadź pierwsze hasło, aby rozbroić, aktualizacja struktury z aktualnej konfiguracji, anuluj pierwsze hasło, ustawienie zegara **Zarządzanie użytkownikami (dodawanie, usuwanie, modyfikacja):** - nazwa użytkownika - hasło - dostęp do stref - uprawnienia
Akcje (zdarzenia przychodzące)	**Alarm:** Włamanie, sabotaż, naruszenie wejścia obwodowego, alarm wejście/wyjście, alarm gazowy, brak wartownika, alarm napadowy, alarm ciśnienia, przerwanie pętli zabezpieczeń, alarm pompy, alarm temperatury, alarm czujnika zaworu, wyciek wody, alarm poziomu wody **Alarm pożarowy:** Przycisk, czujnik płomieni, czujnik dymu, czujnik temperatury, przepływ wody Uszkodzenie z informacją o usterce, awaria akumulatora lub ładowania, uzbrojenie/ rozbrojenie, sabotaż, maskowanie (tylko seria Plus), czujnik zablokowany, wyjście wł./wył., strefa blokowana, błąd połączenia/ połączenie utracono, połączony/rozłączony, podanie pierwszego hasła, nieudane wprowadzenie pierwszego hasła, nieudane anulowanie pierwszego hasła - 3 nieprawidłowe kody dostępu, wygaśnięcie pierwszego hasła

System sygnalizacji pożaru (SSP)	
Nazwa parametru lub funkcji	**Wartość parametru lub opis funkcji**
Wspierane urządzenia	Centrale POLON 6000 (wersja oprogramowania 1.016 lub nowsza)
Akcje (zdarzenia przychodzące)	Potwierdzenie alarmu, Utrata komunikacji, Alarm pożarowy potwierdzony, Alarm pożarowy pierwszego stopnia, Alarm pożarowy drugiego stopnia, Alarm pożarowy wstępny, Alarm pożarowy testowy, Koniec alarmu pożarowego, Koniec alarmu pożarowego testowego, Awaria, Brak awarii, , Koniec awarii, Moduł nie odpowiada, Moduł nie odpowiada w kanale a, Moduł nie odpowiada w kanale b, Błędny status w kanale a, Błędny status w kanale b, Testowanie, Koniec testowania, Blokowanie, Koniec blokowania, Brak lub uszkodzenie zasilania 230V Niskie napięcie akumulatora Brak akumulatora Doziemienie centrali Przekroczona rezystancja wewnętrzna akumulatora Niesprawny tor ładowania Niesprawny tor sterowania Uszkodzenie napięcia 24V Brak zasilania 27V Za niskie napięcie 27V Za wysokie napięcie 27V Przekroczony pobór prądu Restart procesora Linia sygnałowa Is - przerwa, zwarcie Brak lub błąd sondy temperaturowej Przekaźnik pk2 - brak ciągłości linii wyjściowej Podwyższona temperatura otoczenia akumulatora Wyjście sterujące włączone, Wyjście sterujące wyłączone, Wyjście sterujące - brak ciągłości linii sterującej Wyjście sterujące - zwarcie Wyjście sterujące - przerwa w linii Wyjście sterujące - uszkodzenie przekaźnika Wyjście sterujące - moduł zawierający wyjście nie odpowiada Linia dozorowa adresowalna - zwarcie pętli Linia dozorowa adresowalna - zwarcie linii Linia dozorowa adresowalna - przerwa w linii Linia dozorowa adresowalna - zamieniona kolejność elementów na linii Linia dozorowa adresowalna - elementy nie odpowiadają Linia dozorowa adresowalna - elementy niezadeklarowane Linia dozorowa adresowalna - nieprawidłowe parametry r/c Linia dozorowa adresowalna - za dużo elementów w linii Linia dozorowa adresowalna - moduł zawierający linię nie odpowiada Element liniowy nie odpowiada Element liniowy - uszkodzenie pamięci eprom Element liniowy - załączony izolator zwarć Element liniowy - uszkodzenie sprzętowe

Moduły sterowania I/O	
Wspierane urządzenia	Moduł sieciowy wejść/wyjść LANKON-008 marki Tinycontrol
Odbieranie zdarzeń	TAK
Pomiar parametrów środowiskowych	TAK
Pomiar prądu i napięcia	TAK
Sterowanie wyjściami	TAK

1.3 Schemat blokowy systemu - struktura komunikacyjna



Rozdział 2 Instalacja i uruchomienie programu

W niniejszym rozdziale omówione zostaną zagadnienia dotyczące instalacji, pierwszego uruchomienia oraz elementów okna programu NOVUS MANAGEMENT SYSTEM AC.

2.1 Wymagania na PC

Dobór odpowiednich komputerów na serwer i stacje klienckie powinien być ściśle uzależniony od ilości zainstalowanego sprzętu integrowanych systemów, stopnia skomplikowania wykorzystywanej konfiguracji czy architektury systemu. W szczególności dotyczy to systemów telewizji dozorowej VSS z dużą ilością kamer. W przypadku systemów VSS należy również przy doborze komputerów uwzględnić z ilu kamer równocześnie będą wyświetlane strumienie wideo. Liczba skomunikowanych kamer ma w tym przypadku mniejsze znaczenie. Dlatego też ścisłe określenie parametrów komputera przeznaczonego do pracy z oprogramowaniem nie jest możliwe.

Rozdzielczość monitora należy ustawić na Full HD (1920x 1080) lub wyższą. Ustawienie mniejszej rozdzielczości może spowodować niepoprawne wyświetlanie interfejsu graficznego aplikacji jak np. brak wyświetlania części opisów.

Najlepszym rozwiązaniem jest zakup komputera z naszej oferty wraz zainstalowanym oprogramowaniem. Jednostki są przystosowane do pracy ciągłej.

UWAGA!

Kontrolery kontroli dostępu z oprogramowaniem NOVUS MANAGEMENT SYSTEM AC muszą pracować w wydzielonej sieci fizycznej lub logicznej (oddzielna karta sieciowa, przełącznik, VLAN), aby uniknąć wzajemnych zakłóceń z innymi urządzeniami w sieci. Jeżeli program obsługuje systemy KD i VSS to zalecamy wykorzystanie oddzielnych kart sieciowych do komunikacji z urządzeniami systemu KD i VSS.

Poniżej zostały podane **orientacyjne** parametry jednostek komputerowych przeznaczonych dla oprogramowania NOVUS MANAGEMENT SYSTEM AC.

Minimalna konfiguracja komputera PC pracującego jako serwer

1. Procesor CPU **Intel i3 dziesiątej generacji** lub nowszy (istnieje możliwość zastosowania innych procesorów CPU, należy mieć jednak na uwadze, że nie były one testowane z oprogramowaniem).

2. Pamięć operacyjna RAM DDR4 lub nowsza **16 GB**.

3. System operacyjny **Windows 10/11 IoT Enterprise 64 bit.**

4. Karta sieciowa **1 Gb/s** (zalecana dodatkowa karta sieciowa 1Gb/s, system kontroli dostępu powinien pracować w wydzielonej sieci).

5. Karta dźwiękowa

6. Dysk systemowy **SSD 128 GB** lub większy.

7. Karta graficzna - **GeForce GTX 1050** lub nowsza (istnieje możliwość zastosowania innych układów graficznych obsługujących rozdzielczość min. 1920x1080, należy mieć jednak na uwadze, że nie były one testowane z oprogramowaniem).

Zalecana konfiguracja komputera PC pracującego jako serwer

1. Procesor CPU **Intel i7 jedenastej generacji** lub nowszy / **Intel Xeon Silver trzeciej generacji** lub nowszy (istnieje możliwość zastosowania innych procesorów CPU, należy mieć jednak na uwadze, że nie były one testowane z oprogramowaniem).

2. Pamięć operacyjna RAM DDR4 lub nowsza **16GB ECC**.

3. System operacyjny **Windows 10/11 IoT Enterprise 64 bit.**

4. Karta sieciowa **1 Gb/s, 3 sztuki** (system kontroli dostępu powinien pracować w wydzielonej sieci).

5. Karta dźwiękowa

6. Dysk systemowy **SSD 256 GB** lub większy.

7. Karta graficzna - **GeForce GTX 1050** lub nowsza (istnieje możliwość zastosowania innych układów graficznych obsługujących rozdzielczość min. 1920x1080, należy mieć jednak na uwadze, że nie były one testowane z oprogramowaniem).

Minimalna konfiguracja komputera PC pracującego jako klient

1. Procesor CPU **Intel i3 dziesiątej generacji** lub nowszy (istnieje możliwość zastosowania innych procesorów CPU, należy mieć jednak na uwadze, że nie były one testowane z oprogramowaniem).

2. Pamięć operacyjna RAM DDR4 lub nowsza **8 GB**.

3. System operacyjny **Windows 10 Pro 64 bit, Windows 11 Pro 64 bit, Windows 10/11 IoT 64 bit**.

4. Karta sieciowa **1 Gb/s**.

5. Karta dźwiękowa.

6. Dysk systemowy **SSD 64 GB** lub większy.

7. Karta graficzna - **GeForce GTX 1050** lub nowsza (istnieje możliwość zastosowania innych układów graficznych obsługujących rozdzielczość **min. 1920x1080**, należy mieć jednak na uwadze, że nie były one testowane z oprogramowaniem).

Zalecana konfiguracja komputera PC pracującego jako klient

1. Procesor CPU **Intel i7 jedenastej generacji** lub nowszy (istnieje możliwość zastosowania innych procesorów CPU, należy mieć jednak na uwadze, że nie były one testowane z oprogramowaniem).

2. Pamięć operacyjna RAM DDR4 lub nowsza **16 GB**.

3. System operacyjny **Windows 10 Pro 64 bit, Windows 11 Pro 64 bit, Windows 10/11 IoT 64 bit**.

4. Karta sieciowa **1 Gb/s**.

5. Karta dźwiękowa.

6. Dysk systemowy **SSD 128 GB** lub większy.

7. Karta graficzna - **GeForce GTX 1050** lub nowsza, **2 sztuki** (istnieje możliwość zastosowania innych układów graficznych obsługujących rozdzielczość **min. 1920x1080**, należy mieć jednak na uwadze, że nie były one testowane z oprogramowaniem).

Rozdział 2 Instalacja i uruchomienie programu

2.2 Licencje

Korzystanie z programu NOVUS MANAGEMENT SYSTEM ADVANCED CONTROL wymaga rejestracji oraz dokupienia odpowiednich licencji na funkcjonalności/rozszerzenia. Sposób licencjonowania w wersji 6 został stworzony tak, że umożliwia dokładne dopasowanie ilości potrzebnych licencji do charakterystyki poszczególnych obiektów. Dodatkowo do systemu w dowolnym momencie mogą zostać dokupione dodatkowe licencje w celu jego rozbudowy czy zwiększenia funkcjonalności.

Za ilość urządzeń jakie mogą zostać podłączone do serwera NOVUS MANAGEMENT SYSTEM AC odpowiada licencja **NOVUS MANAGEMENT SYSTEM AC PKT LIC v5** na punkty licencyjne. Każde urządzenie dodawane do serwera zużywa określoną liczbę punktów licencyjnych. Sprzedawane są one po **1 punkcie** lub w pakietach po **10 punktów**. Należy zakupić licencję na ilość punktów licencyjnych umożliwiającą podłączenie do serwera wszystkich przewidzianych urządzeń.

Standardowo do serwera NOVUS MANAGEMENT SYSTEM AC w wersji 6 może połączyć się jedna stacja operatora. W celu zwiększenia tej ilości należy dokupić odpowiednią ilość licencji **NOVUS MANAGEMENT SYSTEM AC KL1 v5**.

Włączenie funkcjonalności rejestracji czasu pracy jest realizowane przy użyciu licencji **NOVUS MANAGEMENT SYSTEM AC RCP v5**, licencja ta umożliwia również obsługę 10 użytkowników. W celu zwiększenia ilości użytkowników funkcji rejestracji czasu pracy należy dokupić odpowiednią ilość licencji **NOVUS MANAGEMENT SYSTEM AC URCP v5** lub **NOVUS MANAGEMENT SYSTEM AC URCP 100 v5** lub **NOVUS MANAGEMENT SYSTEM AC URCP 500 v5** lub **NOVUS MANAGEMENT SYSTEM AC URCP 2000 v5** .

Włączenie funkcjonalności rozpoznawania tablic rejestracyjnych jest realizowane przy użyciu licencji **NOVUS MANAGEMENT SYSTEM AC LPR v5**, licencja ta umożliwia również obsługę 10 pojazdów. W celu zwiększenia ilości pojazdów obsługiwanych przez funkcję rozpoznawania tablic rejestracyjnych, należy dokupić odpowiednią ilość licencji **NOVUS MANAGEMENT SYSTEM AC ULPR v5** lub **NOVUS MANAGEMENT SYSTEM AC ULPR 100 v5** lub **NOVUS MANAGEMENT SYSTEM AC ULPR 500 v5** lub **NOVUS MANAGEMENT SYSTEM AC ULPR 5000 v5** lub rozszerzenie **NOVUS MANAGEMENT SYSTEM AC ULPR OP v6** które wyłącza ograniczenie ilości pojazdów.

Dla systemów pracujących w trybie rozporoszonym, należy dokupić licencję **NOVUS MANAGEMENT SYSTEM AC SRV v5** umożliwiającą korzystanie z funkcji muliserwerowości. Umożliwia ona obsługę wielu lokalizacji z poziomu jednego interfejsu programu NOVUS MANAGEMENT SYSTEM AC. Licencję należy dokupić na każdy serwer będący elementem systemu multiserwerowego (rozproszonego). Dostępne są również rozszerzenia **NOVUS MANAGEMENT SYSTEM AC NMS VSS OP**, które powoduje, że system nie pobiera punktów licencyjnych dla dodawanych urządzeń NOVUS MANAGEMENT SYSTEM VSS oraz **NOVUS MANAGEMENT SYSTEM AC KaDe OP v6,** które powoduje, że system nie pobiera punktów licencyjnych dla dodawanych urządzeń kontroli dostępu KaDe.

Aktywacja licencji wymaga wcześniejszego zarejestrowania programu NOVUS MANAGEMENT SYSTEM AC. Rejestracja odbywa się z poziomu programu. Wymagane jest, aby komputer, z którego dokonujemy rejestracji miał dostęp do sieci Internet (rejestracja w trybie on-line). W przypadku braku dostępu do sieci Internet na jednostce komputerowej dla której chcemy dokonać rejestracji możliwe jest wykonanie rejestracji w trybie offline polegającej na wygenerowaniu specjalnego pliku, przeniesieniu go na komputer posiadający dostęp do sieci Internet, zarejestrowaniu go na dedykowanej stronie www, a następnie użyciu pliku wynikowego na jednostce komputerowej dla której chcemy dokonać rejestracji.

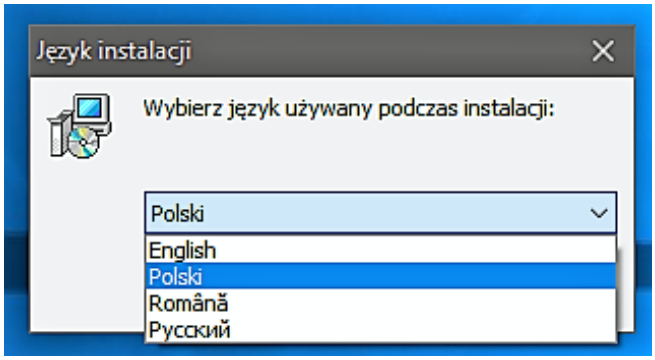
Dostępna jest również licencja testowa programu (**TRIAL**), czas jej trwania wynosi 60 dni. Zawiera ona pełną funkcjonalność oraz limit 500 000 punktów licencyjnych, 500 000 użytkowników RCP, 500 000 pojazdów LPR oraz 100 stacji operatora. W celu uzyskania szczegółowych informacji prosimy o kontakt z działem handlowym AAT SYSTEMY BEZPIECZEŃSTWA sp. z o.o.

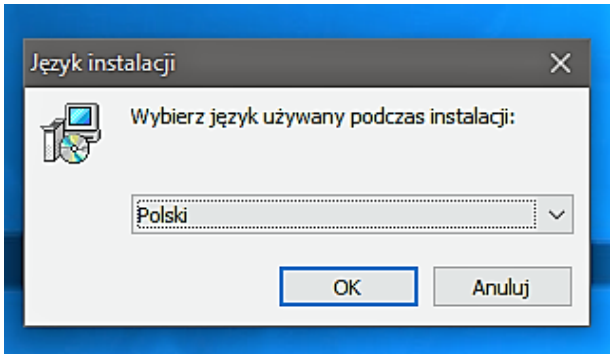
2.3 Instalacja programu

W celu uruchomienia procesu instalacji należy kliknąć na pliku NOVUS MANAGEMENT SYSTEM AC_full_X.XX.XXX.exe lub polecenie *Uruchom* z menu kontekstowego. W celu uzyskania wersji instalacyjnej oprogramowania Novus Management System AC w wersji 6 należy skontaktować się z działem handlowym AAT SYSTEMY BEZPIECZEŃSTWA sp. z o.o. lub zakupić dedykowany nośnik USB (pozycja w cenniku: *NOVUS MANAGEMENT SYSTEM AC USB*).

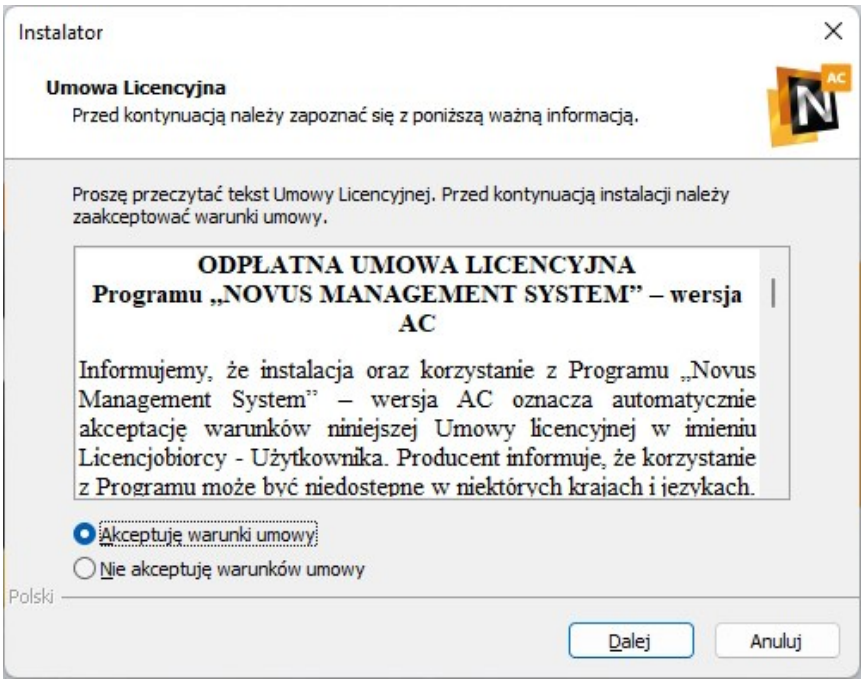
Dodatkowe licencje zwiększające pojemność systemu dostępne są w cenniku i można je zakupić w działach handlowych, a następnie dodać do systemu zgodnie z procedurą opisaną w dalszej części tej instrukcji (zakładka *System*).

Po uruchomieniu instalatora programu NOVUS MANAGEMENT SYSTEM AC na ekranie pojawi się okno widoczne poniżej. Z rozwijanej listy należy wybrać język instalatora i zatwierdzić przyciskiem ***OK***.

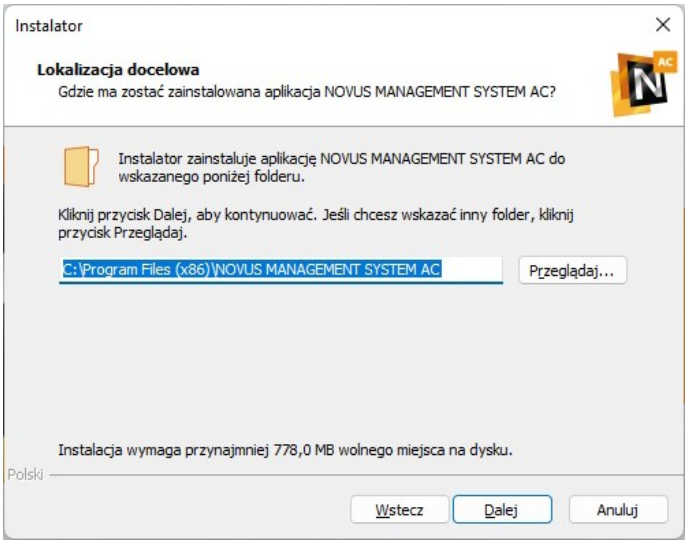


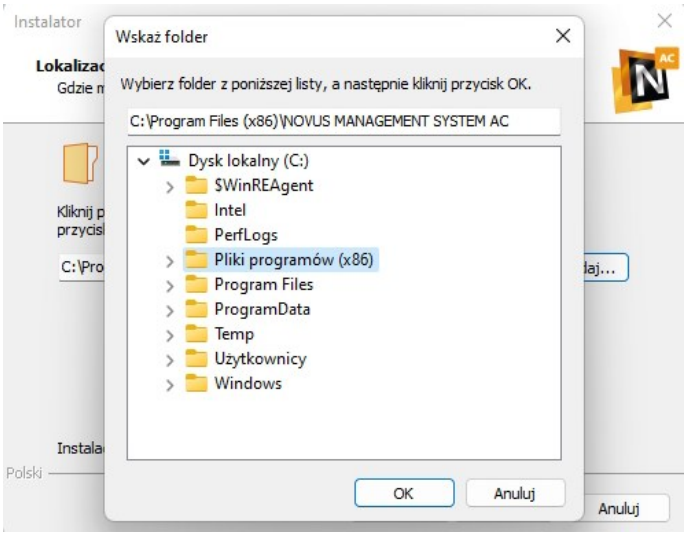


Wyświetlona zostanie Umowa Licencyjna, którą po przeczytaniu należy zaakceptować, aby przejść do kolejnego kroku instalacji. Po zaznaczeniu pola wyboru ***Akceptuję warunki umowy*** należy kliknąć ***Dalej***.



W widocznym na poniższych rysunkach oknie należy wybrać ścieżkę instalacji programu. Domyślną ścieżkę można edytować w polu tekstowym lub wybrać z drzewa katalogów po kliknięciu przycisku ***Przeglądaj…*** i zatwierdzić przyciskiem ***OK***. Po wybraniu ścieżki instalacji NOVUS MANAGEMENT SYSTEM AC należy kliknąć przycisk ***Dalej***, aby przejść do kolejnego kroku instalacji.

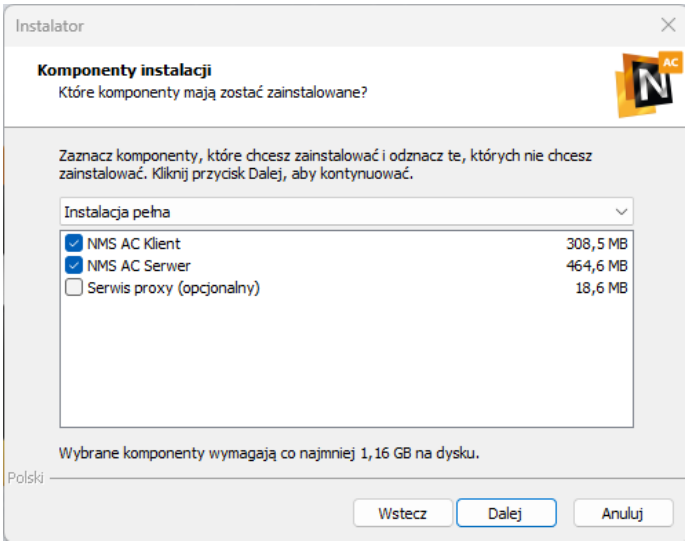


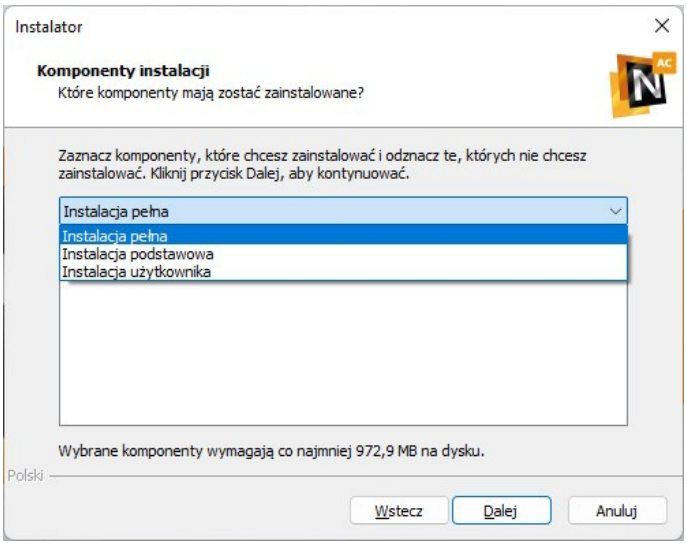


Na tym etapie instalacji oprogramowania należy wybrać jej zakres. Z rozwijanej listy wyboru dostępne są trzy opcje:

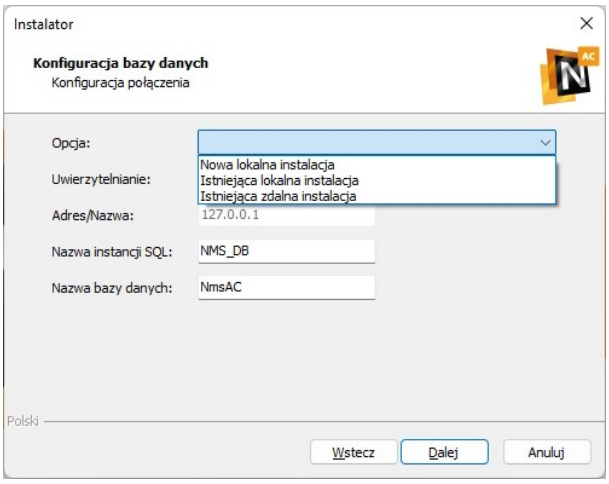
- ***Instalacja pełna*** - instaluje zarówno serwer NOVUS MANAGEMENT SYSTEM AC, jak i aplikację klienta
- ***Instalacja podstawowa*** - instaluje tylko aplikację klienta, którą należy połączyć z serwerem NOVUS MANAGEMENT SYSTEM AC na innym komputerze
- ***Instalacja użytkownika*** - instaluje komponenty wybrane przez użytkownika poprzez zaznaczenie odpowiednich pól wyboru

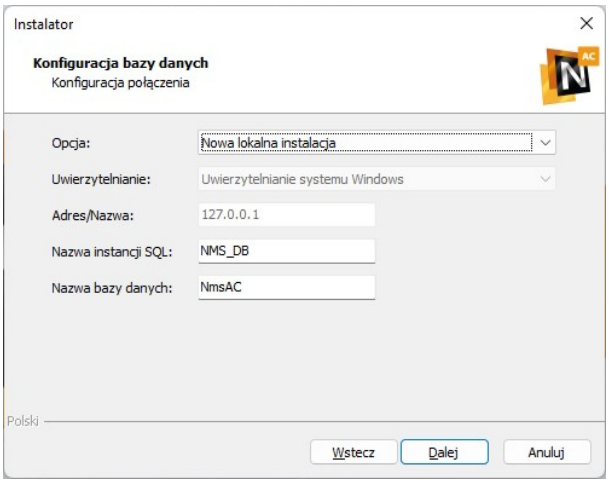
Po wyborze zakresu instalacji należy kliknąć przycisk ***Dalej***.

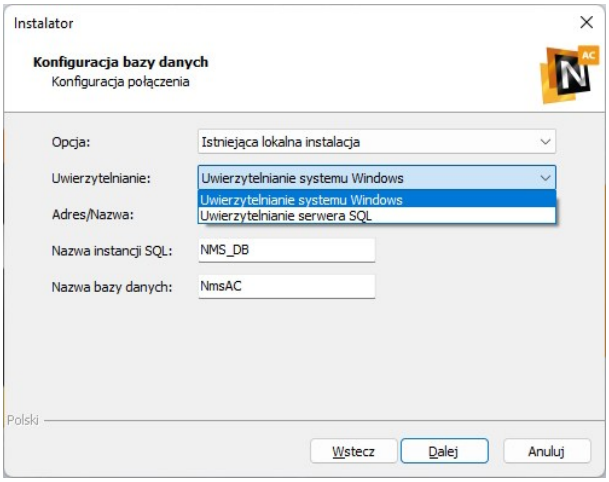


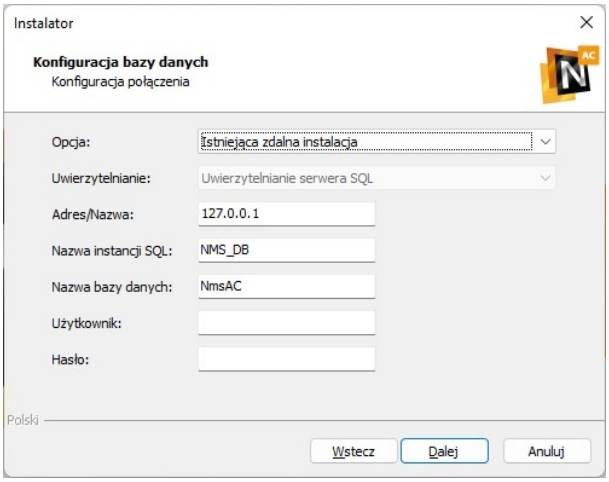


Na etapie konfiguracji bazy danych należy z rozwijanej listy poniżej wybrać jedną z trzech opcji.





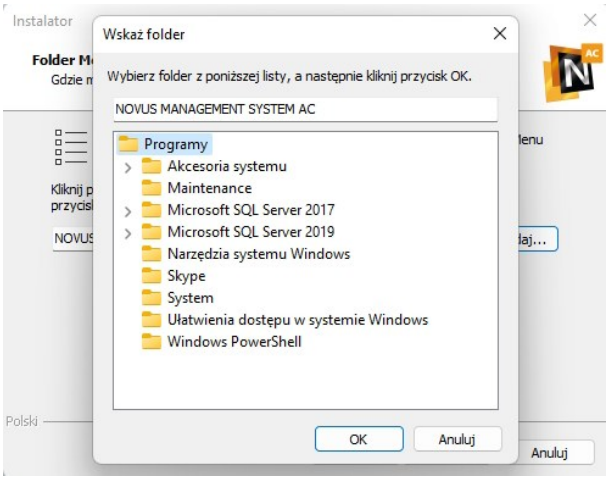




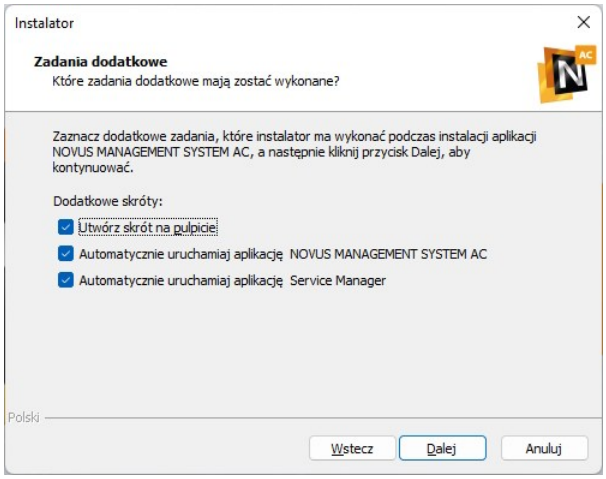
Nowa lokalna instalacja - instaluje na komputerze serwer SQL, tworzy nową instancję SQL oraz bazę danych o nazwach podanych w polach tekstowych.

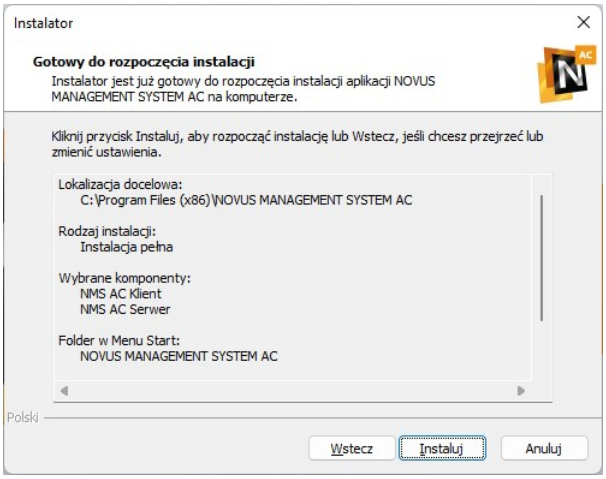
Istniejąca lokalna instalacja - tę opcję można wybrać, jeżeli na komputerze jest już zainstalowany serwer SQL; tworzy nową instancję SQL oraz bazę danych o nazwach podanych w polach tekstowych; w przypadku wyboru autentyfikacji poprzez SQL Serwer należy podać dane logowania używane do potwierdzenia dostępu do serwera SQL.

Istniejąca zdalna instalacja - umożliwia połączenie serwera NOVUS MANAGEMENT SYSTEM AC z serwerem SQL zainstalowanym na innym komputerze w sieci; tworzy nową instancję SQL oraz bazę danych o określonej w polach tekstowych nazwie na serwerze SQL o wskazanym w polu ***Adres/Nazwa*** adresie IP; dla obowiązującej autentyfikacji SQL Serwer należy podać dane logowania używane do potwierdzenia dostępu do zdalnego serwera SQL.



Po skonfigurowaniu bazy danych należy kliknąć przycisk ***OK*** w celu przejścia do kolejnego kroku, w którym należy zdecydować o nazwie folderu skrótów w menu start, a po kliknięciu przycisku ***Dalej***, zdecydować o utworzeniu skrótu na pulpicie oraz automatycznego uruchamiania aplikacji NOVUS MANAGEMENT SYSTEM AC przy starcie systemu poprzez zaznaczenie albo odznaczenie odpowiednich pól wyboru.

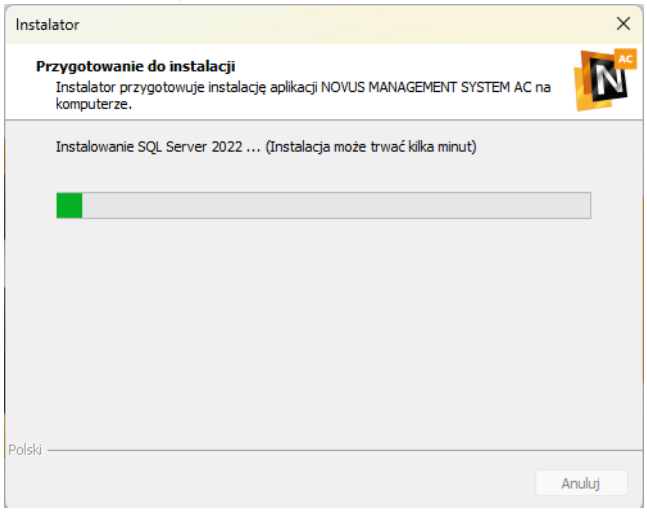


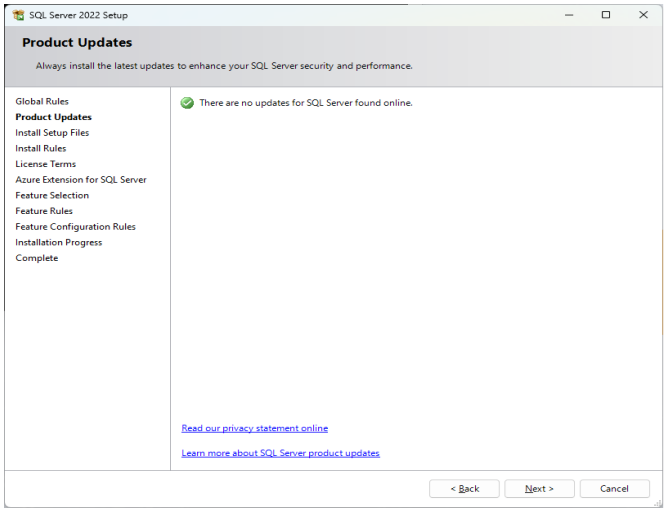


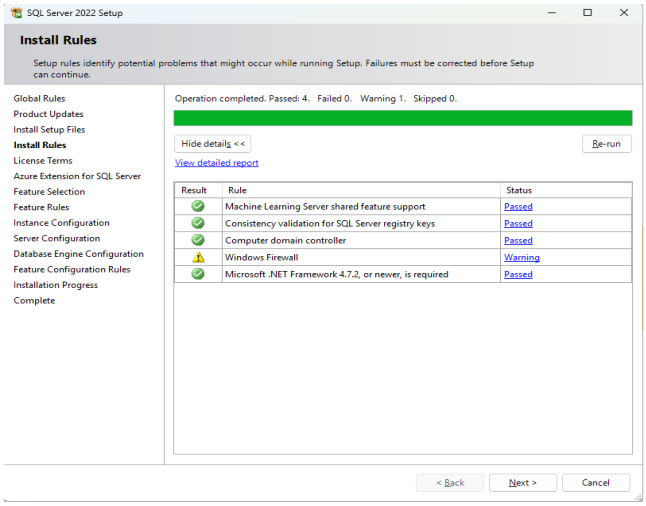
Po naciśnięciu przycisku ***Dalej*** pojawi się widoczne po prawej okno gotowości do instalacji podsumowujące dotychczas wybrane ustawienia. Do tego etapu można swobodnie wracać do poprzednich kroków konfiguracji instalacji przy pomocy przycisku ***Wstecz***. Kiedy ustawienia w podsumowaniu są prawidłowe, należy kliknąć przycisk ***Instaluj***.

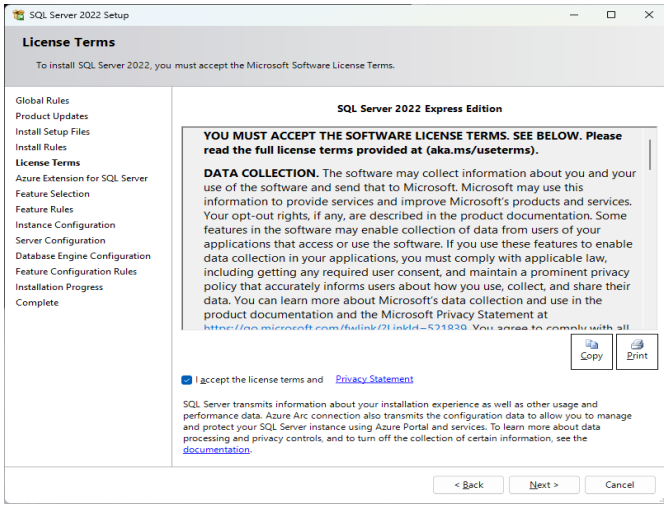
Na tym etapie po wybraniu lokalizacji i nazw rozpoczyna się właściwy proces instalacji oprogramowania.

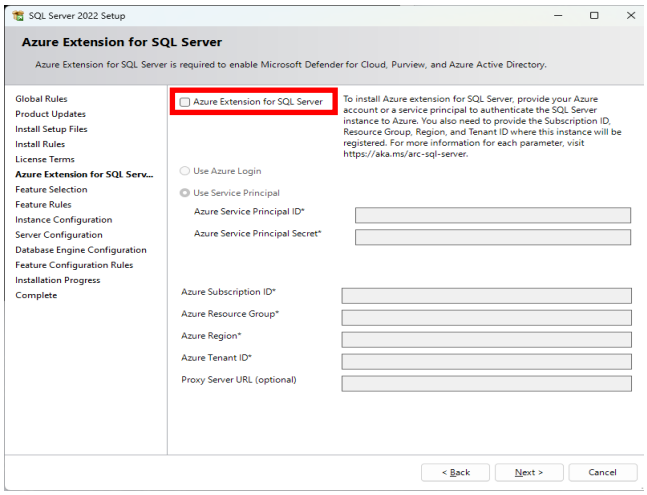
W pierwszej kolejności zostanie zainstalowana baza danych SQL zgodnie z wybrana opcją, a następnie aplikacja NOVUS MANAGEMENT SYSTEM AC. Jeżeli komputer nie jest podłączony do Internetu to w trakcie instalacji bazy SQL może się pojawić monit o braku możliwości sprawdzenia dostępnych aktualizacji - w takim przypadku należy go zignorować i kliknąć ***Dalej***.

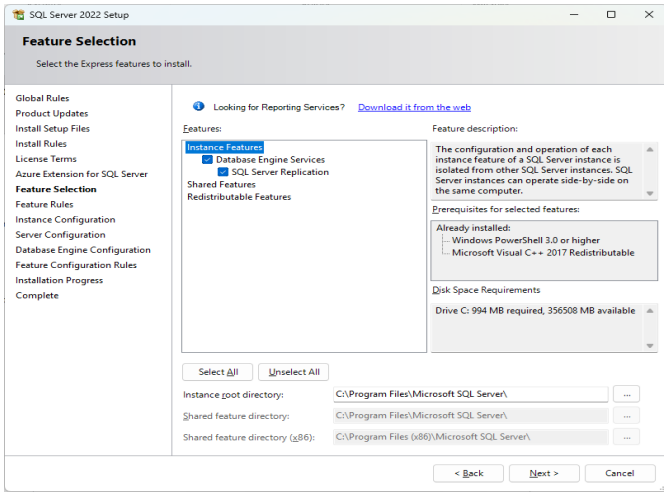




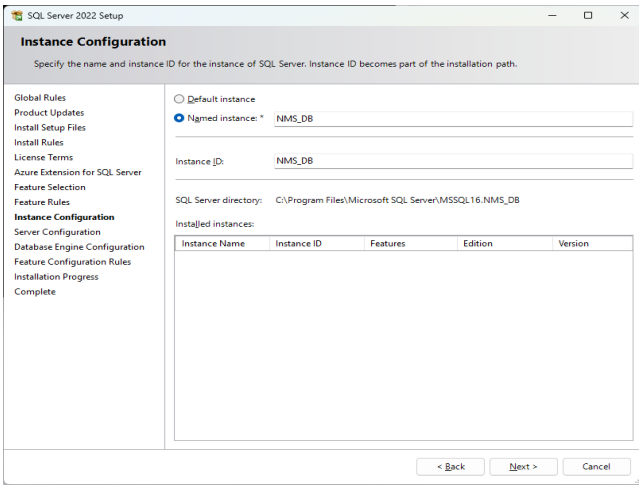


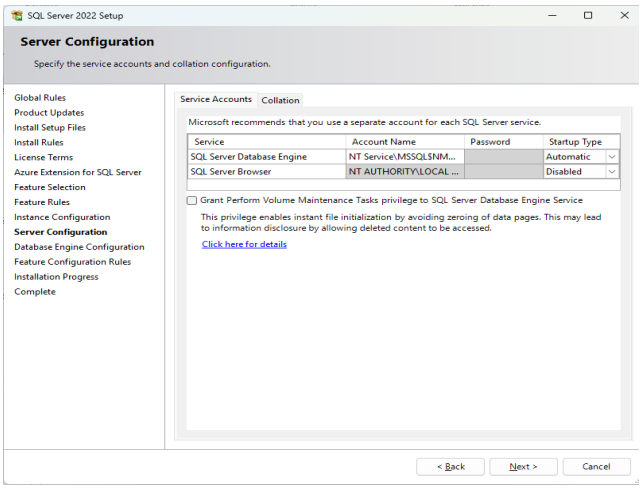


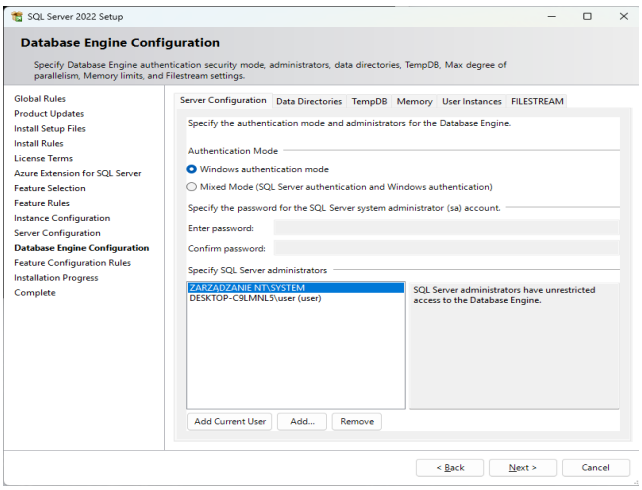


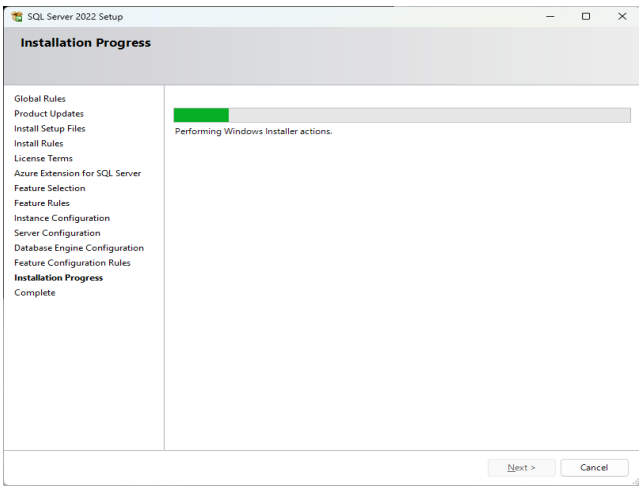


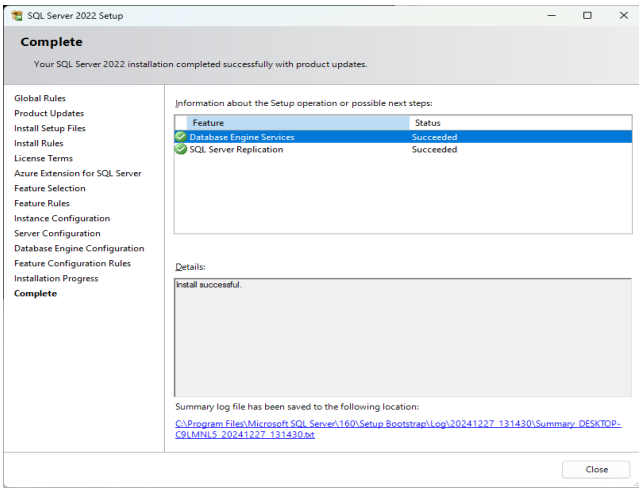
Na tym etapie w kolejnych oknach należy klikać przycisk ***Dalej (Next),*** a w oknie ***License Terms*** zaznaczyć pole akceptacji licencji (I accept the license terms and Privacy Statement). W oknie ***Azure Extension for SQL Server*** należy odznaczyć opcję Azure Extension for SQL Server.







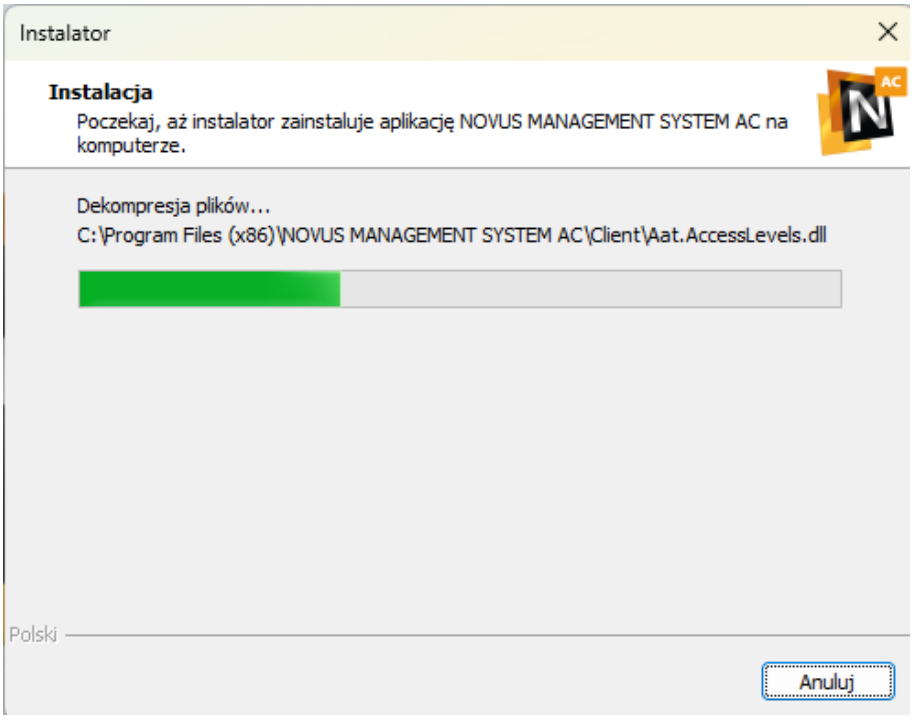




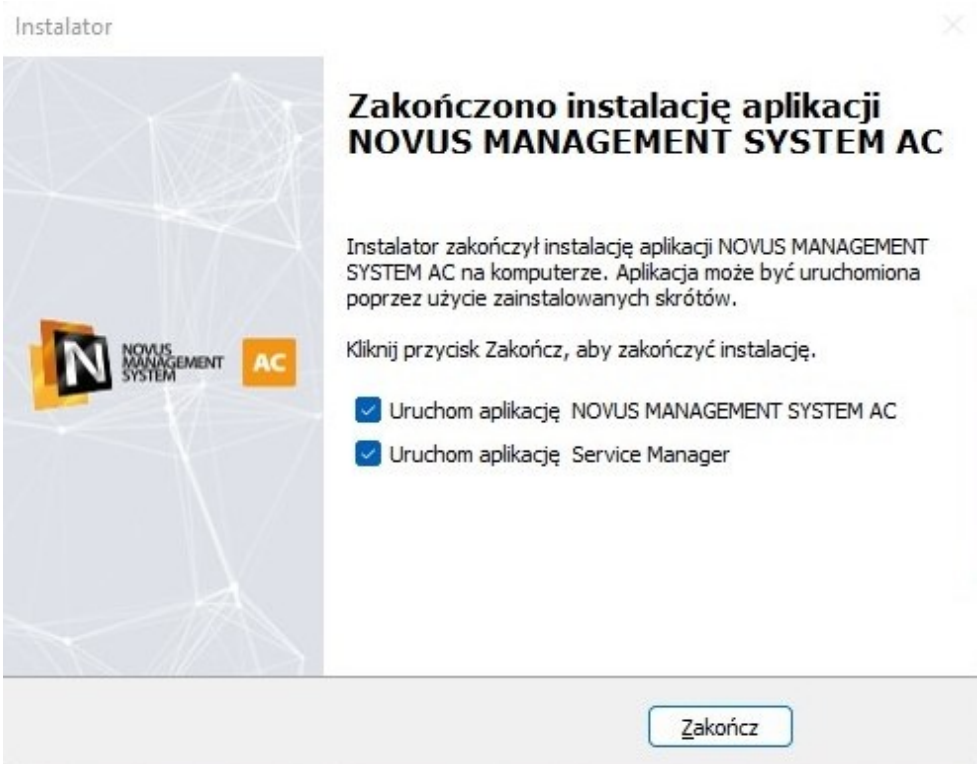
W kolejnych krokach instalacji wykonywane są czynności zgodnie z listą po prawej stronie okna.

Po pomyślnym zakończeniu instalacji bazy SQL w oknie ***Complete*** wyświetlona zostanie informacja o pomyślnym zakończeniu tej części instalacji. Następnie kliknąć ***Close***.

Instalator przeprowadzi następnie proces instalacji odpowiednich komponentów systemu NOVUS MANAGEMENT SYSTEM AC, który trwa kilka chwil.

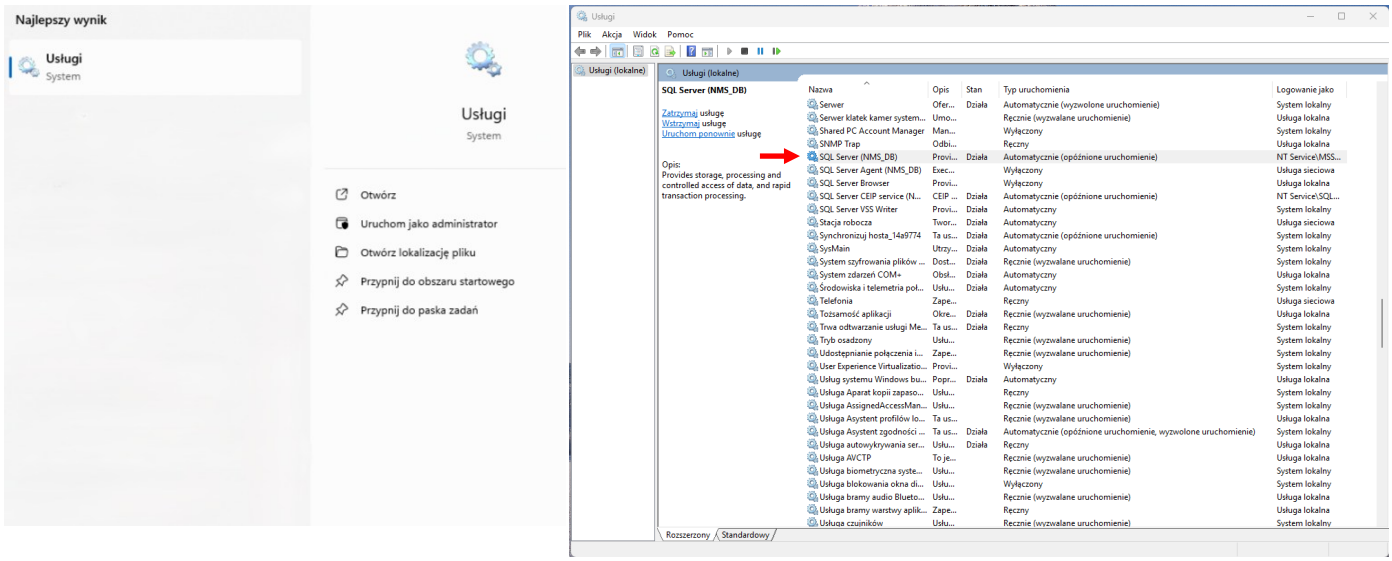


Po zainstalowaniu aplikacji pojawia się okno informacyjne widoczne poniżej. Można od razu uruchomić program NOVUS MANAGEMENT SYSTEM AC klikając przycisk ***Zakończ*** przy jednocześnie zaznaczonym polu wyboru ***Uruchom aplikację NOVUS MANAGEMENT SYSTEM AC***. Odznaczenie tego pola i kliknięcie przycisku skutkuje wyjściem z instalatora bez uruchamiania aplikacji. Zaznaczenie pola ***Uruchom Service Manager*** spowoduje pojawienie się w oknie ***Tray*** w prawym dolnym rogu ekranu ikony umożliwiającej zatrzymanie lub uruchomienie usługi *NOVUS MANAGEMENT SYSTEM AC Service*.

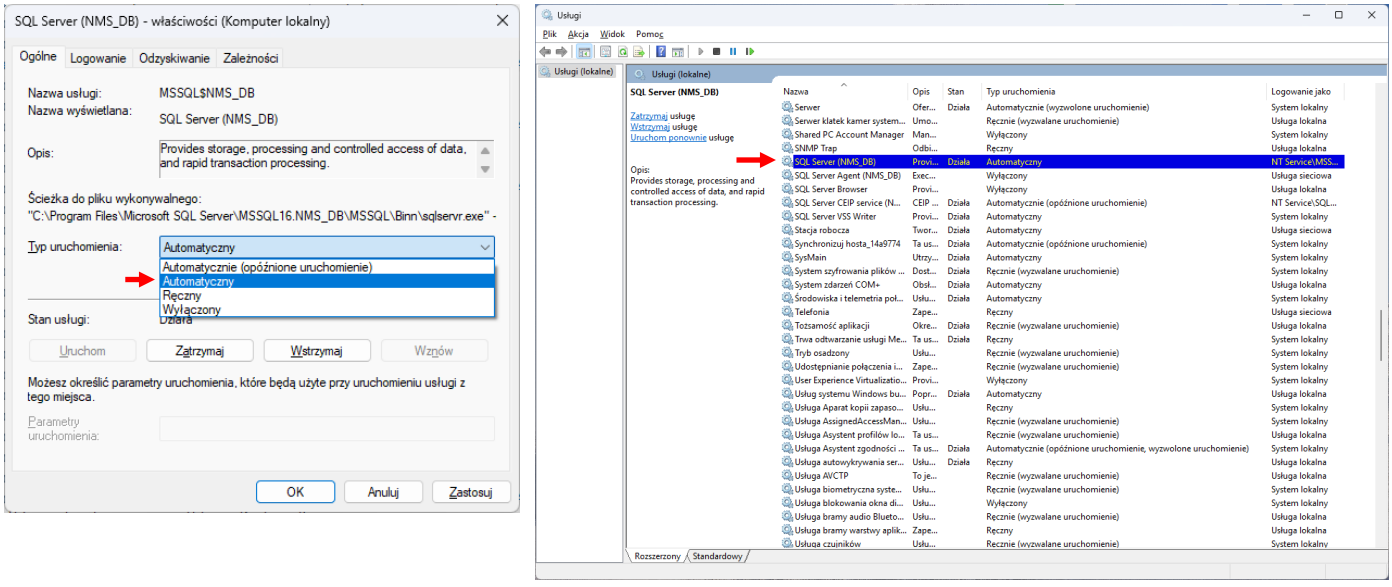


UWAGA!

Po instalacji serwera programu należy zmienić typ uruchomienia serwera SQL. Aby to zrobić należy wyszukać „Usługi” w polu wyszukiwaniu na pasku zadań systemu Windows 10/11.



Wyszukujemy usługę SQL Server (NMS_DB) i zmieniamy typ uruchomienia z Automatyczne (opóźnione uruchomienie) na Automatyczne a następnie potwierdzamy klikając ***OK***.



2.4 Aktualizacja programu

UWAGA!

Bezpośrednia aktualizacja programu MANAGEMENT SYSTEM AC z wersji 4 do wersji 5/6 nie jest możliwa. Wykonanie takiej aktualizacji może spowodować uszkodzenie bazy danych.

W celu aktualizacji wersji 4 do wersji 5/6 należy przeprowadzić aktualizację pośrednią do wersji 4 do wersji 4.03.01 przy użyciu pliku NMS AC_update_4.03.01.exe. W celu uzyskania szczegółowych informacji na temat należy skontaktować się z działem handlowym lub działem wsparcia technicznego KD lub VSS AAT SYSTEMY BEZPIECZEŃSTWA sp. z o.o.

Przed aktualizacją z wersji 6.00.004 do wersji 6.01.039 lub nowszej należy wykonać aktualizację pośrednią do wersji 6.00.012.

Aktualizacja wersji 6.01.039 do nowszej wersji 6 może zostać przeprowadzona bezpośrednio, bez konieczności stosowania aktualizacji pośrednich.

Pliki aktualizujące na wyższe wersje programu mają nazwy:

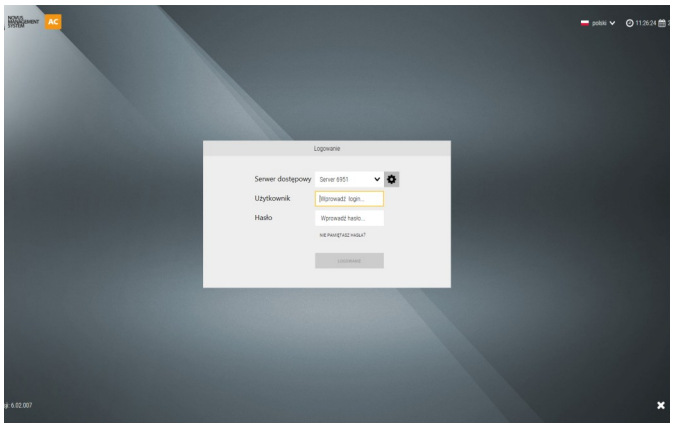
NOVUS MANAGEMENT SYSTEM AC_update_X.XX.XXX.exe.

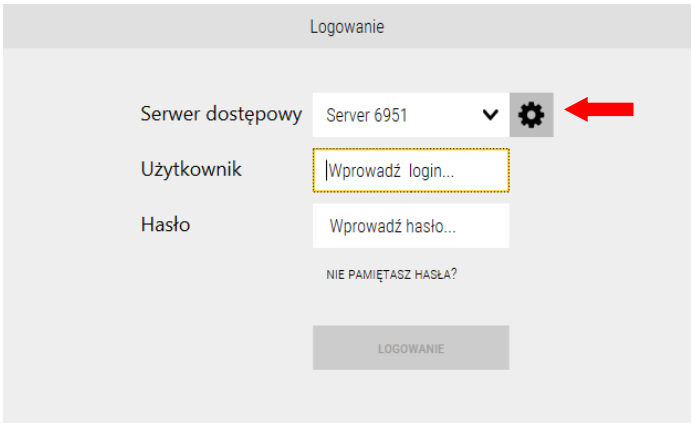
W celu przeprowadzenia aktualizacji należy postępować w analogiczny sposób jak zostało to opisane w rozdziale dotyczącym instalacji programu.

2.5 Uruchomienie programu

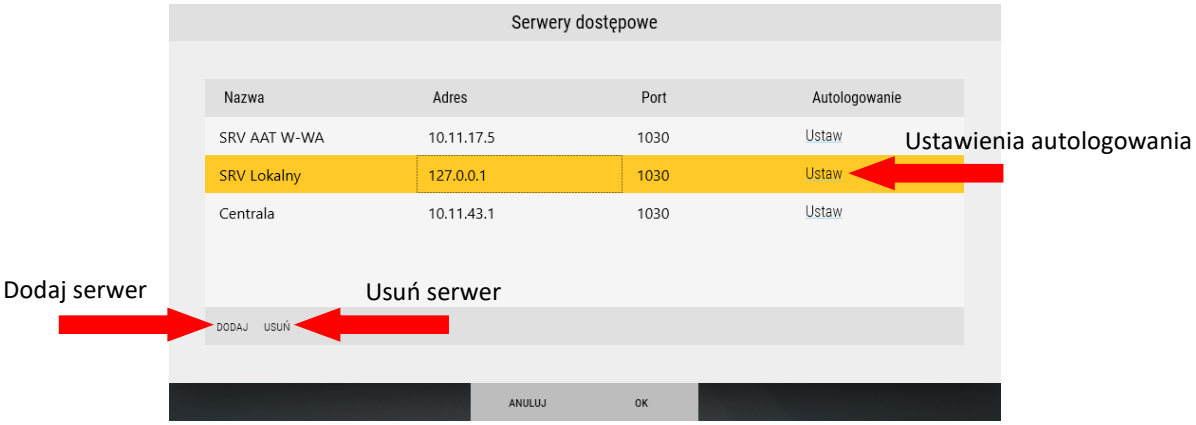
Po zainstalowaniu oprogramowania NOVUS MANAGEMENT SYSTEM AC domyślnie na pulpicie pojawi się ikona widoczna poniżej, a w menu start systemu Windows utworzona zostanie grupa NOVUS MANAGEMENT SYSTEM AC. Za ich pomocą można uruchomić program.

Uruchomienie programu skutkuje pojawieniem się ekranu logowania. W jego centralnej części znajduje się okno logowania. W sekcji ***Serwer*** można wybrać serwer NOVUS MANAGEMENT SYSTEM AC, z którym należy się połączyć. Zainstalowana aplikacja NOVUS MANAGEMENT SYSTEM AC Klient umożliwia połączenie się z jednym dowolnym serwerem. Aplikacja serwer pracuje jako usługa i domyślnie jest uruchamiana wraz ze startem systemu Windows. Dzięki temu można się z nim połączyć i zalogować z dowolnej stacji klienckiej w obrębie sieci. Usługa serwera łączy się z bazą SQL systemu. Ikona obok pola wyboru zaznaczona na poniższym rysunku otwiera ***Listę serwerów***. W pola ***Login*** i ***Hasło*** należy wprowadzić dane logowania operatora. Login domyślnego operatora to **root**, natomiast hasło to **pass**. W celu uniemożliwienia nieautoryzowanego dostępu do systemu zaleca się zmianę tego hasła w trakcie konfiguracji. Czynność ta zostanie opisana w dalszej części instrukcji. Przycisk ***Wyjście*** w prawym dolnym rogu zamyka program.

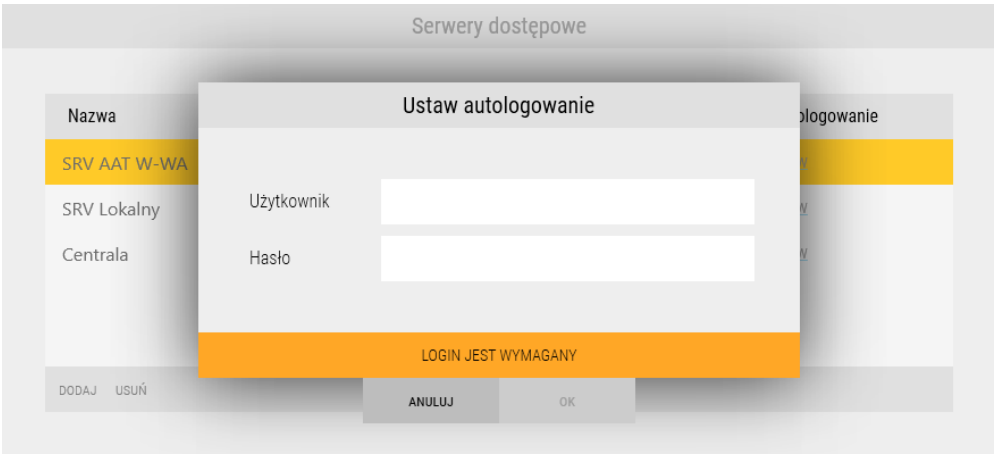




Okno listy serwerów dostępowych umożliwia dodawanie, usuwanie oraz konfigurację serwerów NOVUS MANAGEMENT SYSTEM AC, do których można podłączyć stację operatora. Podczas dodawanie serwera należy podać jego adres IP oraz numer portu (domyślnie 1030). Nazwa serwera zostanie pobrana automatycznie po nawiązaniu połączenia. Dla dodanych serwerów możliwe jest również włączenie funkcji autologowania.

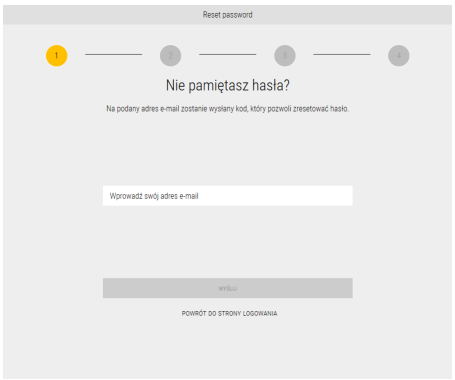


Po kliknięciu przycisku ***Autologowanie/Ustaw*** możliwe jest ustawienie nazwy operatora oraz hasła automatycznego logowania operatora dodanego do systemu bezpośrednio po uruchomieniu programu.

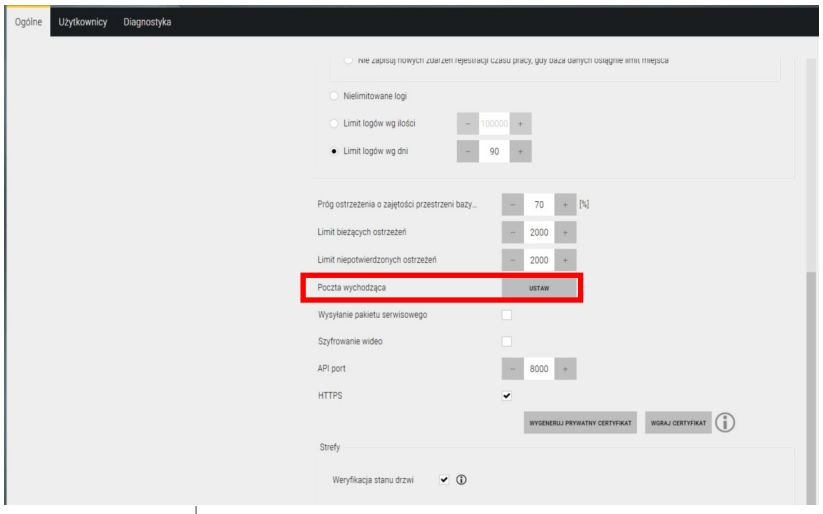


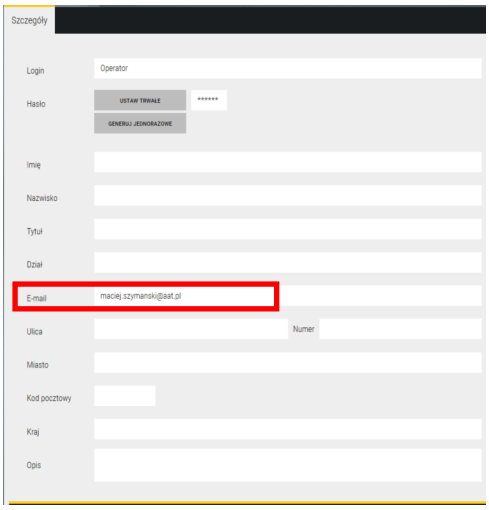
Należy mieć na uwadze, że funkcja autologowania jest dostępna jedynie dla operatorów przypisanych do grup posiadających uprawnienie „Autologowanie dostępne”.

Po kliknięciu przycisku **NIE PAMIĘTASZ HASŁA?** możliwe jest odzyskanie hasła Operatora do systemu (działa po uprzedniej konfiguracji).

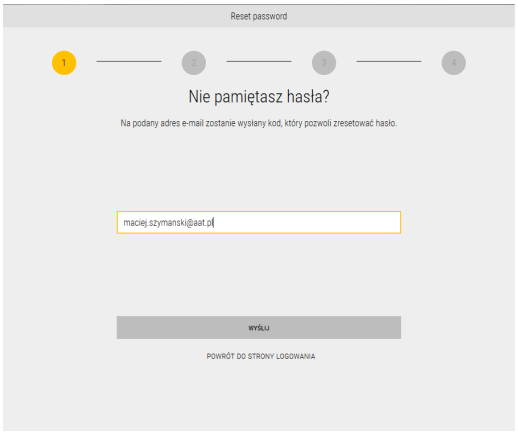


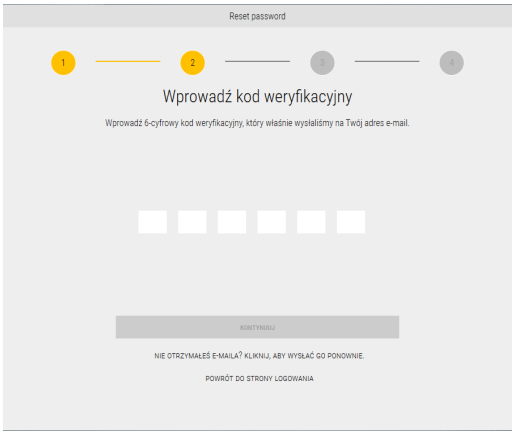
UWAGA! Funkcja działa po ustawieniu poczty wychodzącej w zakładce *System/Ustawienia serwerów* oraz ustawieniu adresu email operatora w zakładce *System/Grupy i operatorzy*

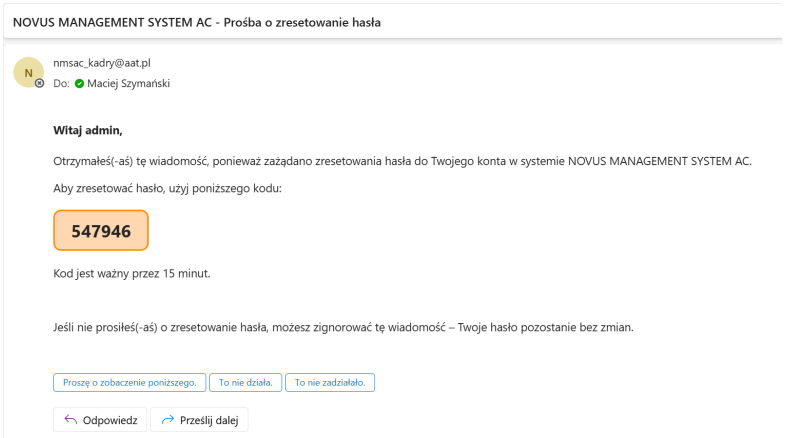


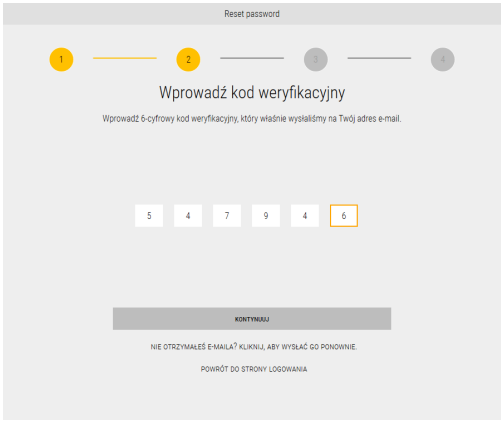


Operator odzyskuje hasło poprzez wpisanie przypisanego mu emaila na który zostanie wysłany sześciocyfrowy kod. Email zostanie wysłany automatycznie po przejściu do okna wpisywania kodu.



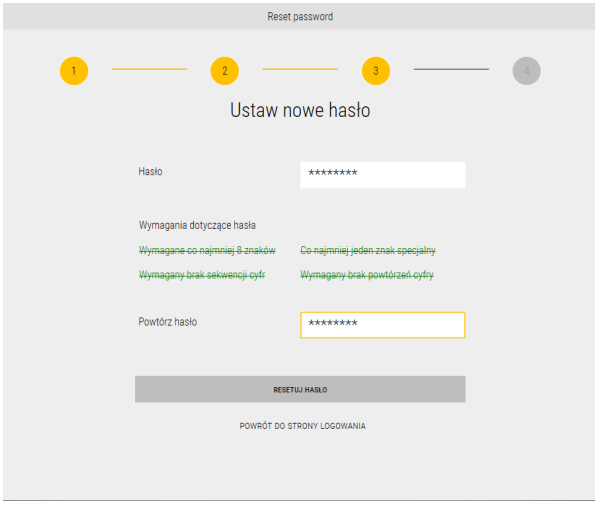


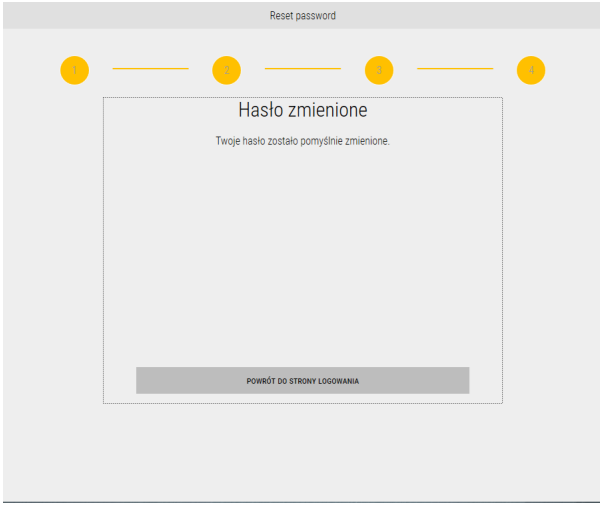




Po poprawnym podaniu sześciocyfrowego kodu operator może zmienić swoje hasło zgodnie z wymaganiami.

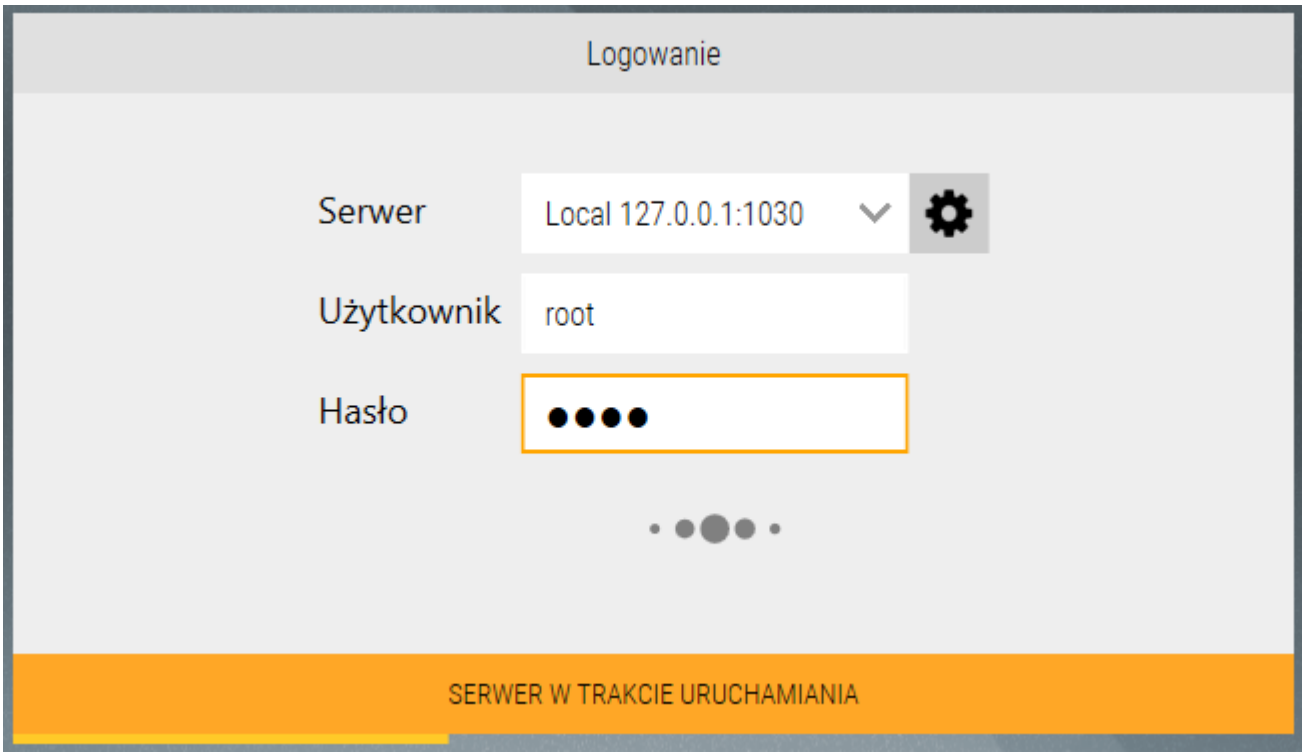
Po potwierdzeniu hasło zostaje zmienione.



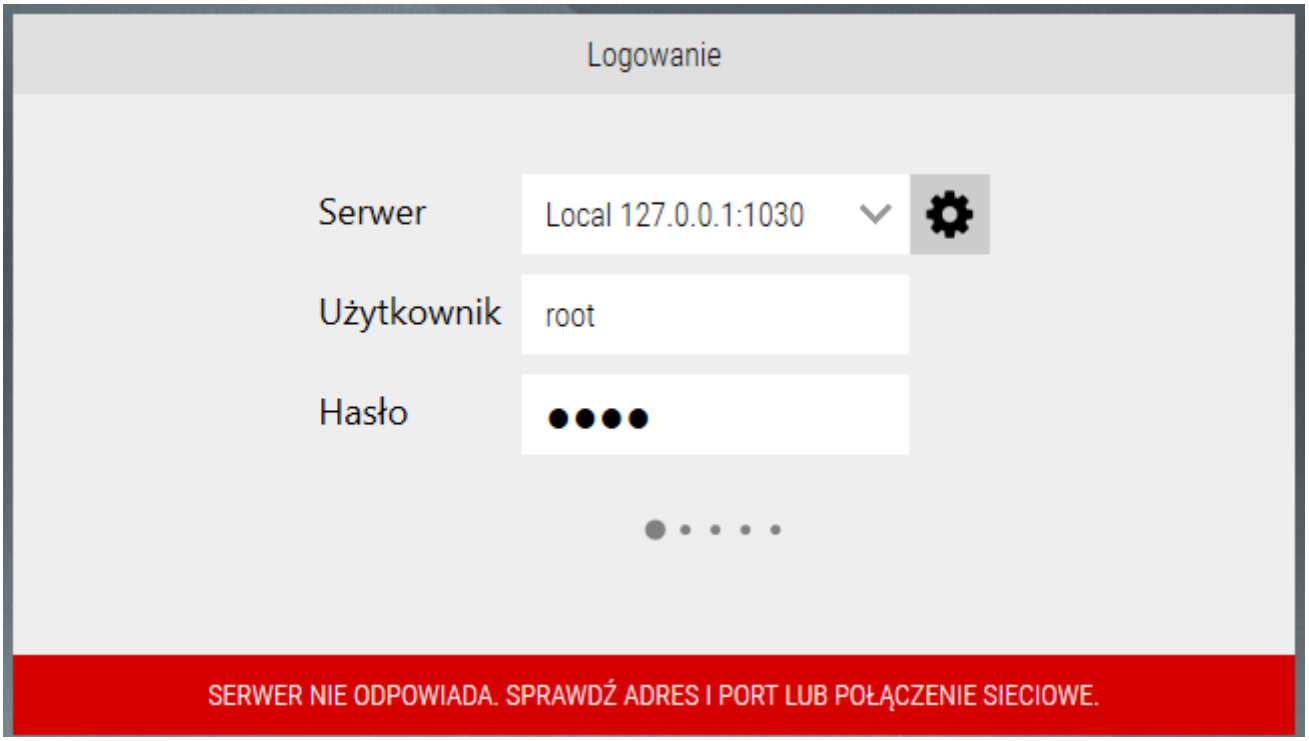


UWAGA! Jeżeli wiadomość email z kodem nie zostanie dostarczona należy kliknąć ***NIE OTRZYMAŁEŚ E-MAILA? KLIKNIJ, ABY WYSŁAĆ GO PONOWNIE*****.** Jeżeli email dalej nie przychodzi należy sprawdzić w skrzynce mailowej folder **SPAM.**

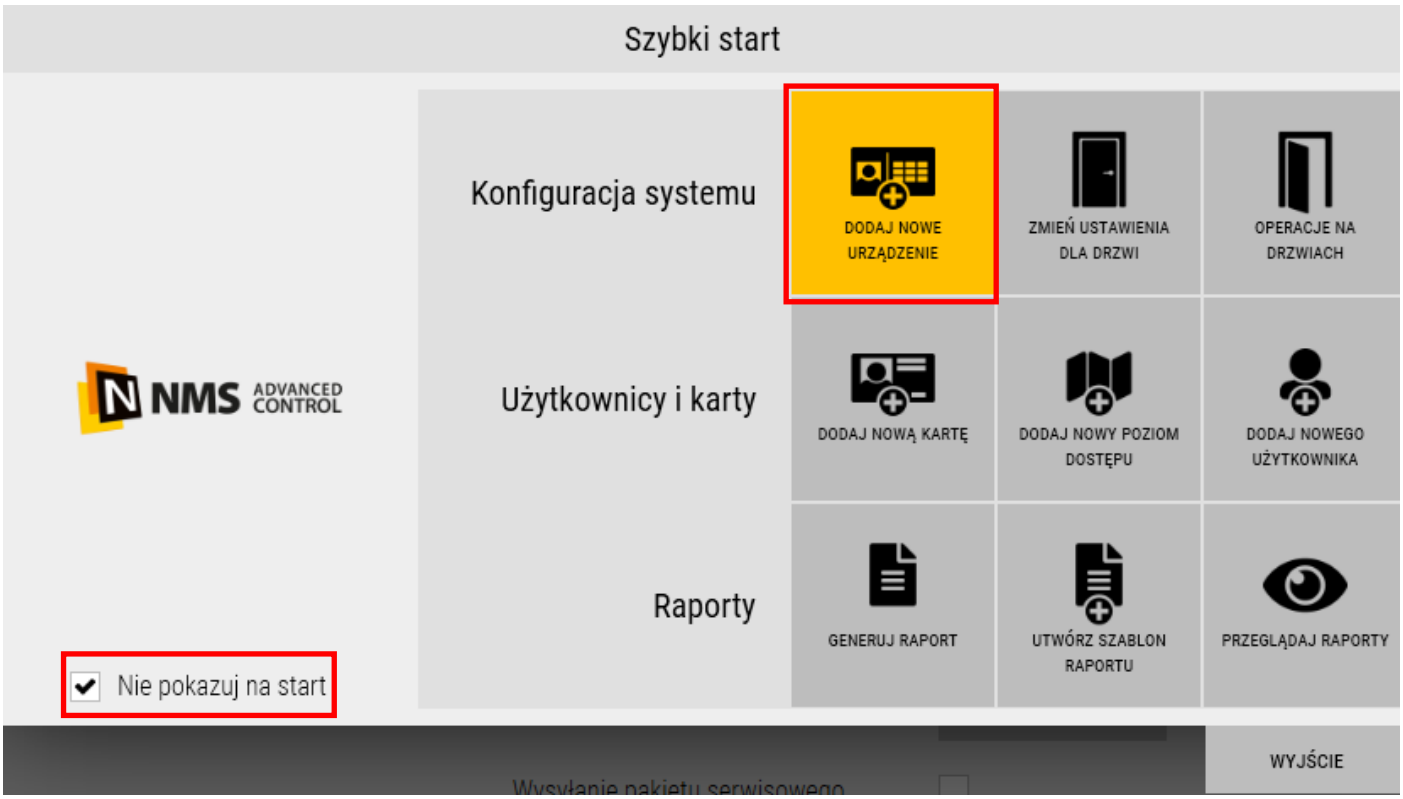
Po wpisaniu nazwy i hasła oraz kliknięciu przycisku ***LOGOWANIE,*** w dolnej części okna może się pojawić komunikat *SERWER W TRAKCIE URUCHAMIANIA.* Oznacza to, że należy poczekać, ponieważ uruchamia się usługa serwera (np. po restarcie).



W analogicznej sytuacji, w dolnej części okna może się pojawić komunikat *SERWER NIE ODPOWIADA.* Oznacza to, że usługa serwera została z jakiegoś powodu zatrzymana. Należy wówczas uruchomić ręcznie usługę korzystając z okna ***Menadżer zadań/Usługi*** w Windows lub uruchamiając skrypt **start.cmd** dostępny w folderze aplikacji.



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



Okno ***Szybki start*** zawiera dziewięć ikon skrótów do najczęściej wykorzystywanych opcji systemu z trzech grup tematycznych:

1. Konfiguracja systemu

- ***Dodaj nowe urządzenie*** - otwiera okno dodawania urządzeń do systemu
- ***Zmień ustawienia drzwi*** - szybko otwiera zakładkę szczegółów ustawień drzwi w dodanych do systemu kontrolerach
- ***Operacje na drzwiach*** - szybko otwiera zakładkę operacji możliwych do wykonania na drzwiach dodanych do systemu

2. Użytkownicy i karty

- ***Dodaj nową kartę*** - otwiera okno dodawania kart do systemu
- ***Dodaj nową grupę dostępu*** - szybko otwiera zakładkę *Grupy dostępu* i dodaje nową grupę dostępu
- ***Dodaj nowego użytkownika*** - szybko otwiera zakładkę *Użytkownicy* i dodaje nowego użytkownika

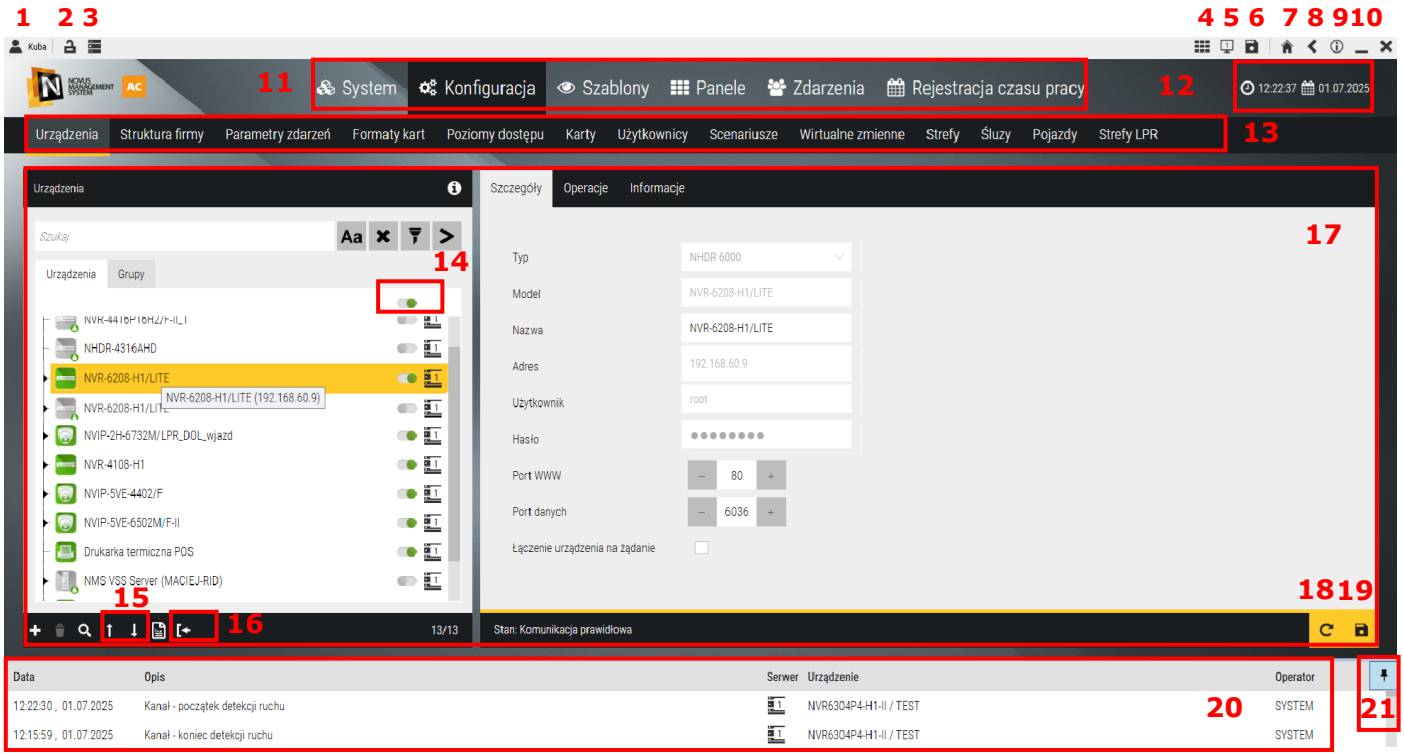
3. Raporty

- ***Generuj raport*** - otwiera okno listy zdarzeń gdzie możemy przejrzeć i wykonać raport ze zdarzeń
- ***Utwórz szablon raportu*** - otwiera okno ***Zdarzenia/Automatyczne raporty***
- ***Przeglądaj raporty*** - otwiera zakładkę *Pliki na serwerze* w sekcji *Zdarzenia*

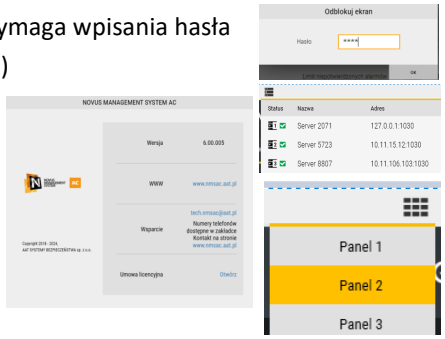
Zaznaczenie przycisku wyboru ***Nie pokazuj na start*** wyszczególnionego na powyższym rysunku powoduje, że okno ***Szybki start*** nie jest automatycznie wyświetlane po uruchomieniu programu NOVUS MANAGEMENT SYSTEM AC. Przycisk ***Wyjście*** zamyka okno ***Szybki start***.

2.6 Pulpit operatora i nawigacja w oknie programu

Pulpit operatora jest graficznym interfejsem użytkownika pozwalającym na interakcję z systemem NOVUS MANAGEMENT SYSTEM AC.

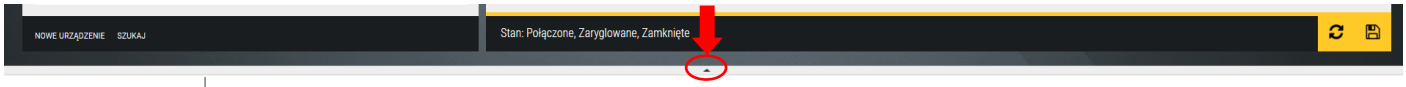


1. Wyświetla okno z dwoma dostępnymi opcjami ***Zmiana operatora*** oraz ***Wyloguj.***
2. Przycisk ***Blokada ekranu*** - blokuje dostęp do menu programu, odblokowanie wymaga wpisania hasła
3. Wyświetla bieżący serwer lub listę serwerów w grupie (jeżeli została utworzona)
4. Wyświetla listę paneli w możliwością otwarcia wybranego z listy
5. Wyświetla numer aktualnego monitora
6. Zapisuje aktualny układ okien wyświetlanych na poszczególnych monitorach
7. Przycisk ***Szybki start*** - otwiera okno ***Szybki start***.
8. Przycisk ***Wstecz*** - wyświetla poprzednie okno
9. Przycisk ***O aplikacji*** - otwiera okno z numerem wersji oprogramowania i link do treści licencji

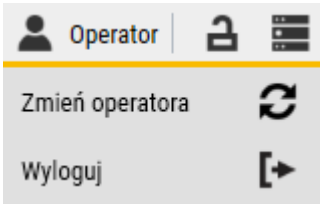


10. Przycisk ***Minimalizuj*** - minimalizuje okno NOVUS MANAGEMENT SYSTEM AC.
11. Pasek wyboru sekcji - kliknięcie na odpowiednią sekcję pozwala na konfigurację lub podgląd opcji.
12. Aktualna godzina i data serwera.
13. Pasek zakładek - umożliwia przechodzenie pomiędzy poszczególnymi zakładkami wybranej sekcji.
14. Przycisk połącz/rozłącz wszystkie urządzenia na liście.
15. Strzałki góra/dół - przesuwanie urządzeń na liście o jedno miejsce w górę/ w dół. Przytrzymanie LP myszki umożliwia ciągłe przeciąganie urządzeń, aż do momentu zwolnienia LP myszki.
16. Przycisk importu listy urządzeń z pliku wyeksportowanego z programu NOVUS MANAGEMENT SYSTEM VSS.
17. Obszar roboczy - właściwości wybranego w lewym oknie elementu
18. Przycisk odświeżania - odświeża wyświetlane dane
19. Przycisk zapisu - zapisuje zmiany wprowadzone w konfiguracji systemu
20. Okno logów systemowych - wyświetla logi dotyczące zmian w konfiguracji systemu oraz innych zdarzeń w systemie.
21. Przycisk przypięcia okna logów (pinezka) - umożliwia zmianę wyświetlania okna logów - jako widoczne na stałe w obszarze ekranu albo mieć postać zwijanej belki w dole ekranu zwiększając w ten sposób obszar roboczy (17). Po kliknięciu na ten przycisk można zwinąć belkę. Aby ją ponownie rozwinąć należy kliknąć na:

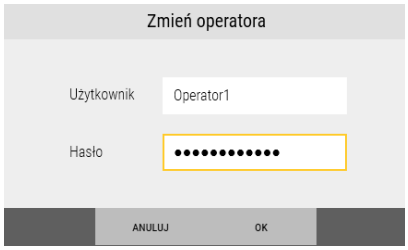
Belka rozwija się automatycznie po pojawieniu się nowych zdarzeń w tym oknie, i zwija po kliknięciu w obszarze roboczym.



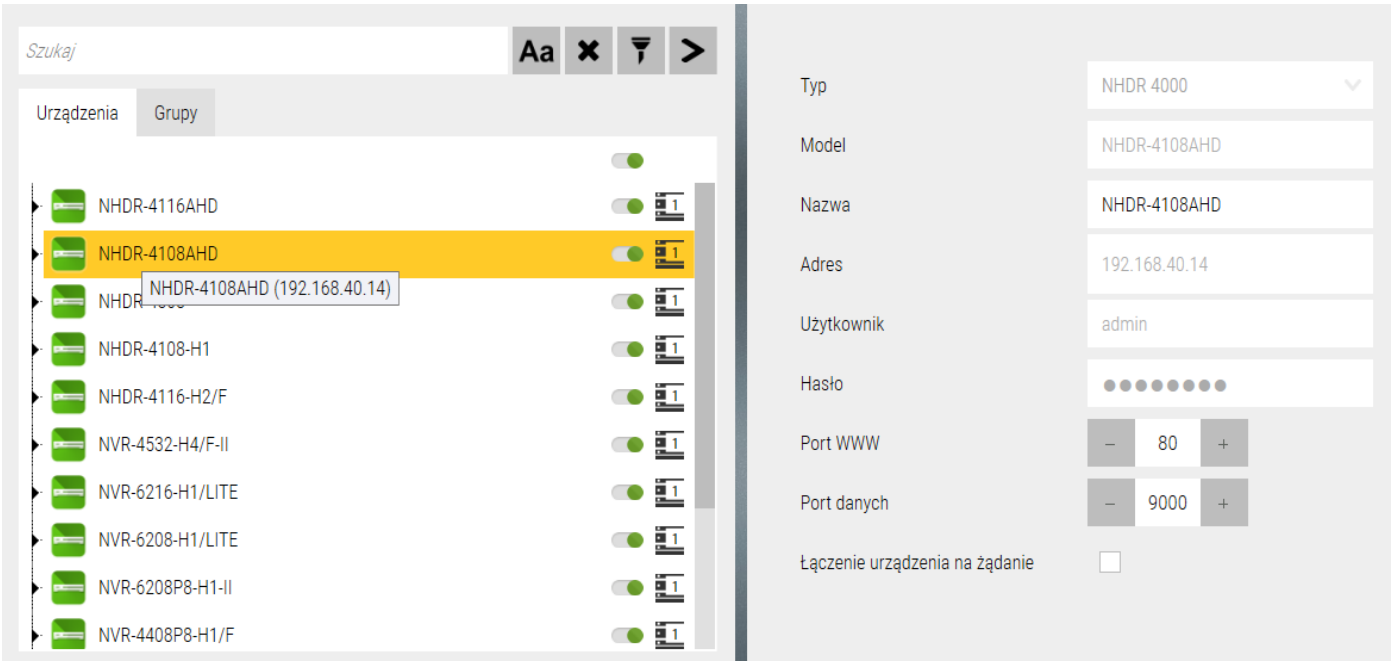
W górnym lewym, górnym rogu ekranu startowego po najechaniu na ikonę pojawia się nowe okno z dwoma opcjami Wyloguj oraz Zmiana operatora.



Opcja *Wyloguj* - wylogowuje aktualnego operatora i otwiera ekran logowania.
Opcja *Zmiana operatora* - po wybraniu tej opcji pojawia się nowe okno z polami do wprowadzenia nowych danych logowania innego operatora.



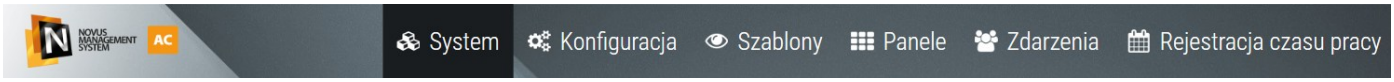
Kolejną opcją jest wyświetlanie adresu IP wraz z nazwą urządzenia po najechaniu kursorem na jego nazwę na liście *Drzewo Urządzeń*. Dzięki temu operator może znacznie szybciej sprawdzić adres IP, bez konieczności otwierania zakładki *Szczegóły danego urządzenia*.



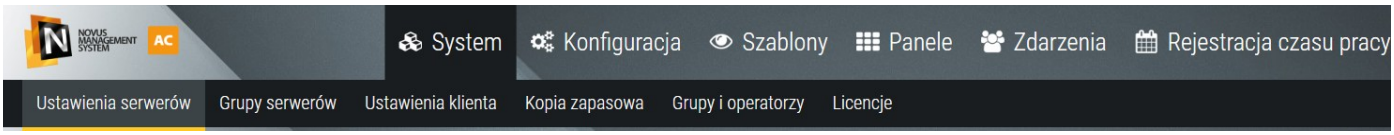
2.7 Menu programu

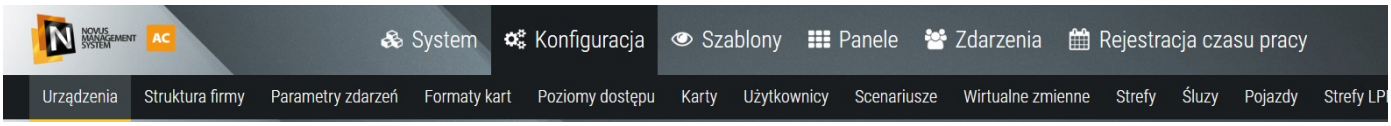
Menu programu zawiera dwa paski.

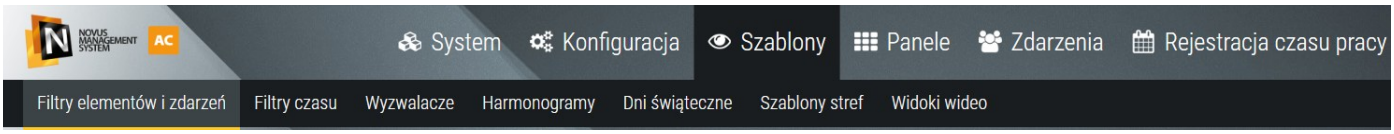
Pasek główny:

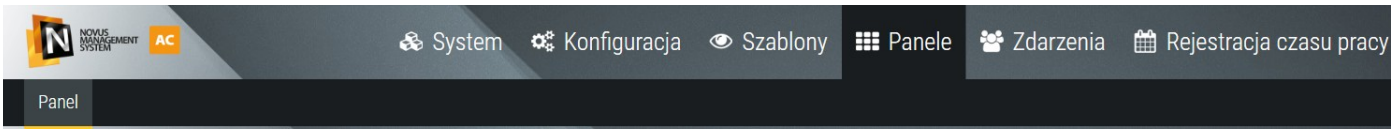


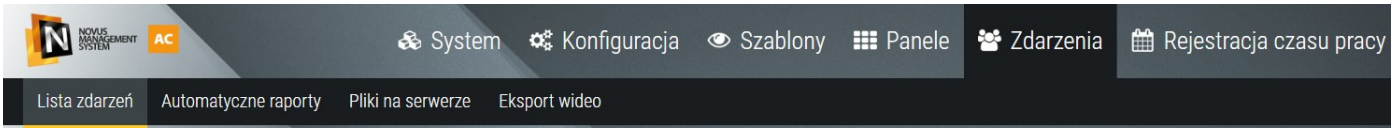
Posiada 6 zakładek, z których każda zawiera następujące pozycje:

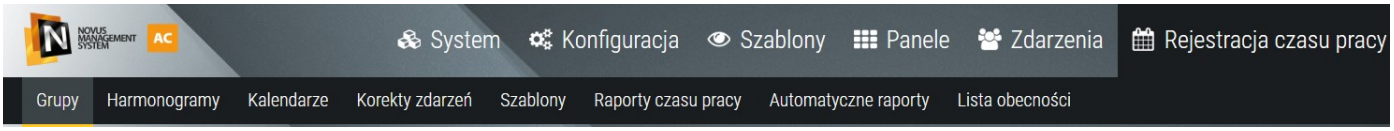




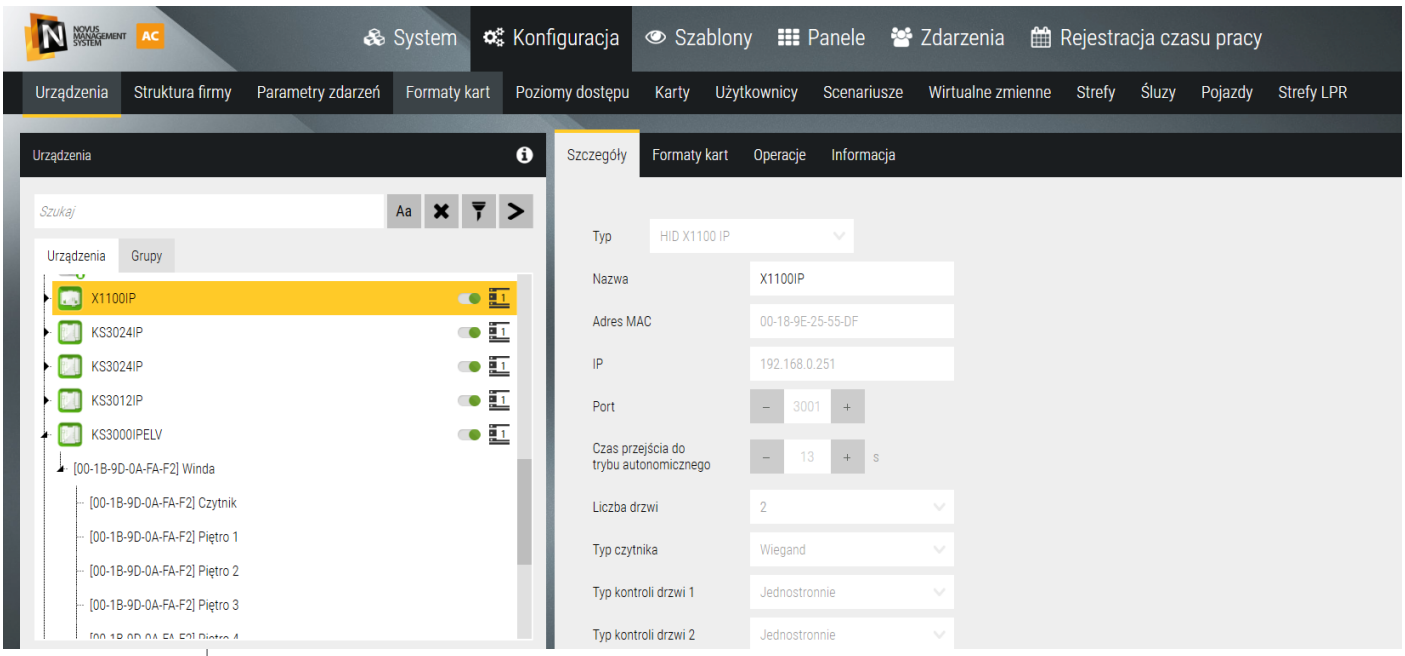








Każda zakładka na drugim pasku zawiera dalsze zakładki oraz dwa okna: lewe z listą elementów i prawe z ustawieniami zaznaczonej w lewym oknie pozycji. Przykładowo w oknie *Konfiguracja / Urządzenia* wygląda to następująco:



2.8 Ikony występujące w oknach programu

Symbol ikony	Opis	Lokalizacja
	Wstecz	Górny pasek
	Opcje	Górny pasek
	Zmiana operatora	Górny pasek
	Wyloguj	Górny pasek
	O aplikacji	Górny pasek
	Szybki start	Górny pasek
	Wybór monitora	Górny pasek
	Minimalizuj	Górny pasek
	Edycja panelu	Górny pasek
	Powrót do	Górny pasek
	Zablokuj ekran	Górny pasek
	Lista serwerów	Górny pasek
	Lista paneli	Górny pasek
	Zapis okien na	Górny pasek
	Szukaj	Górny pasek
	Idź do panelu	Górny pasek
	Data	Górny pasek
	Czas	Górny pasek
	Przypnij konsolę	-
	Numer serwera	-

Symbol ikony	Opis	Lokalizacja
	Uzupełnij setup	-
	Raport w CSV	Zdarzenia
	Raport w HTML	Zdarzenia
	Raport autom.	Zdarzenia
	Kasowanie alarmów	-
	Alarm	-
	Wielkość liter	-
	Błąd / info	-
	Odśwież	Konfiguracja
	Zapisz	Konfiguracja
	Dodaj	Konfiguracja
	Usuń	Konfiguracja
	Importuj listę	Konfiguracja
	Eksportuj listę	Konfiguracja
	Wyszukaj	Konfiguracja
	Klonuj	Konfiguracja
	Resetuj do domyślnych	Konfiguracja
	Ustaw jako domyślne	Konfiguracja
	Przesuń w górę	Konfiguracja
	Przesuń w dół	Konfiguracja

2.9 Skróty oraz kombinacje klawiaturowe

Oprogramowanie NOVUS MANAGEMENT SYSTEM AC udostępnia zestaw skrótów klawiszowych, których sposób działania jest zbliżony do skrótów stosowanych w systemie operacyjnym Windows. Umożliwiają one szybkie poruszanie się po interfejsie, zaznaczanie elementów oraz wykonywanie podstawowych operacji bez użycia myszy. Poniżej znajduje się lista obsługiwanych kombinacji wraz z opisem ich działania.

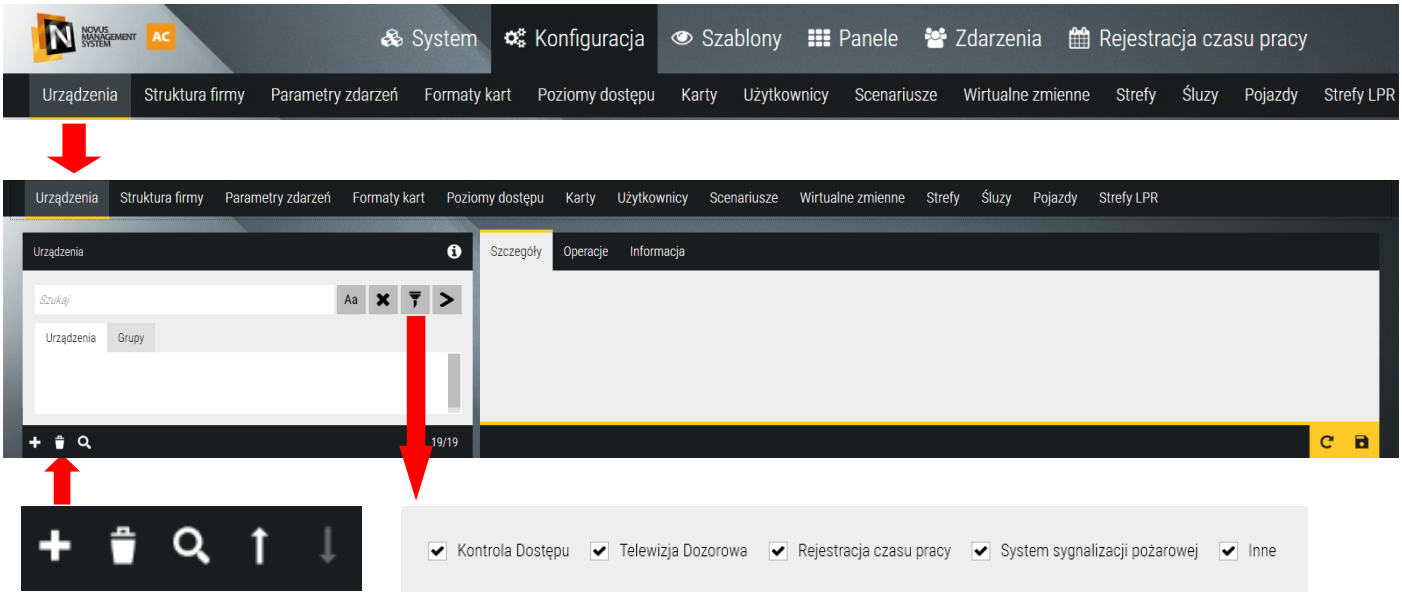
Kombinacja	Sposób użycia	Działanie
CTRL	Przytrzymaj	Pozwala zaznaczyć wiele elementów na liście (oddzielnych)
SHIFT	Przytrzymaj	Pozwala zaznaczyć wiele elementów w ciągłym zakresie
TAB	Naciśnij	Przejście do następnego elementu
TAB + SHIFT	Przytrzymaj SHIFT, naciśnij TAB	Przejście do poprzedniego elementu
CTRL + TAB	Przytrzymaj CTRL, naciśnij TAB	Przełączanie się pomiędzy zakładkami na wyższy poziom (do następnej zakładki)
CTRL + SHIFT + TAB	Przytrzymaj CTRL+SHIFT, naciśnij TAB	Przełączanie pomiędzy zakładkami wyższy poziom (do poprzedniej zakładki)
SPACE	Naciśnij	Zaznaczenie/Odznaczenie elementu
ENTER	Naciśnij	Przejście do następnej linii
ESCAPE	Naciśnij	Anulowanie lub zamknięcie okna
Strzałki ↑ ↓ ← →	Naciśnij	Nawigacja pomiędzy elementami

Rozdział 3. Konfiguracja systemu

W niniejszym rozdziale omówione zostaną zagadnienia dotyczące konfiguracji systemu NOVUS MANAGEMENT SYSTEM AC. Są to czynności wykonywane przez instalatora systemu. Służy do tego zakładka *Konfiguracja.* Zawiera ona szereg okien służących do dodawania urządzeń do systemu, poziomów dostępu, kart i użytkowników, scenariuszy i wirtualnych zmiennych, pojazdów, stref LPR i innych.

3.1 Urządzenia - Kontrola dostępu - Kontrolery

Proces konfiguracji rozpoczynamy od zakładki *Urządzenia*.



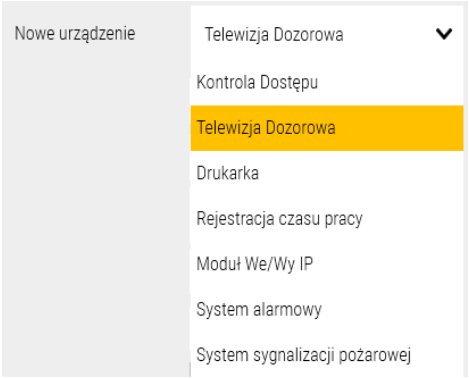
- dodaj nowe urządzenie
- usuń
- wyszukaj
- zmień kolejność urządzeń góra/dół

Filtr typu umożliwia wyświetlanie listy urządzeń zawierającej jeden lub różne rodzaje urządzeń

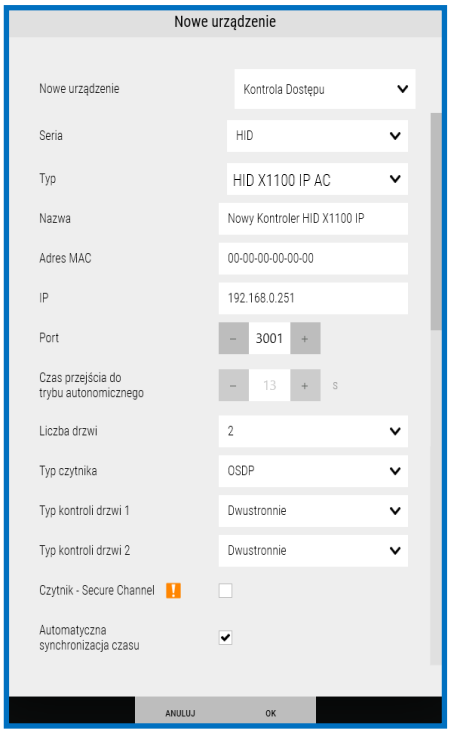
System można skonfigurować w trybie off-line przed podłączeniem do systemu na obiekcie, ale znacznie szybciej proces konfiguracji przebiega w trybie on-line, gdy urządzenia mamy już zainstalowane, podłączone do zasilania i sieci Ethernet. Możemy wówczas skorzystać z wyszukiwarki, która po przeszukaniu sieci wyświetli listę dostępnych urządzeń wraz z parametrami adresowymi. Ta procedura zostanie opisana w następnym punkcie.

Dodaj nowe urządzenie

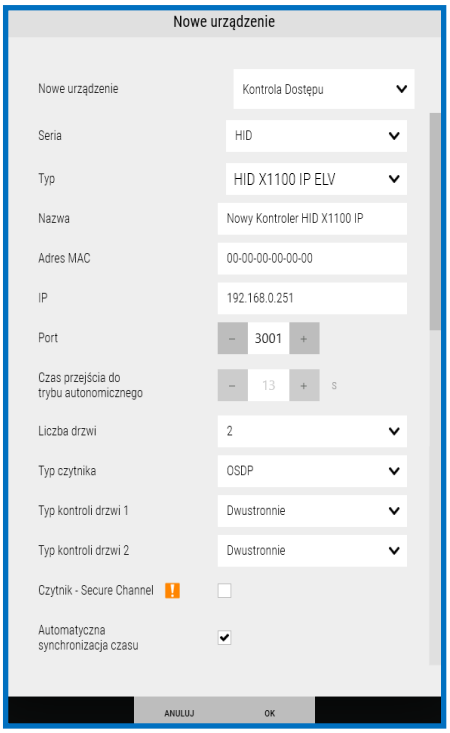
Ta opcja pozwala na dodanie nowego urządzenia w trybie off-line, gdy nie możemy skorzystać z wyszukiwarki. Po kliknięciu na ten przycisk wyświetli się okno jak na następnej stronie, w którym możemy wybrać typ urządzenia jaki chcemy dodać:

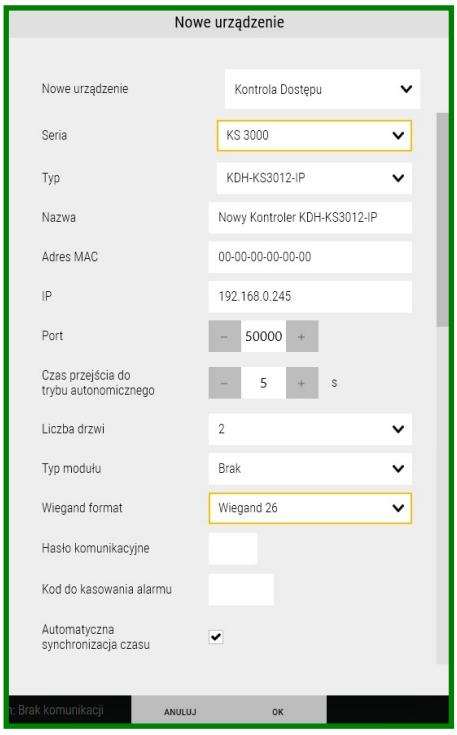


Po wybraniu urządzenia do systemu kontroli dostępu wyświetli się okno jak poniżej:



Seria HID®





Seria 3000

Seria - z rozwijanej listy można wybrać serię dodawanych kontrolerów:

- HID®
- KS 3000

Seria HID®:

Typ - z rozwijanej listy można wybrać model kontrolera:

- HID®X1100 AC
- HID®X1100 ELV
- HID®X100
- HID®X200
- HID®X300

Nazwa - edytowalne pole na wpisanie nazwy kontrolera

MAC - edytowalne pole na wpisanie adresu MAC kontrolera (jest na naklejce na urządzeniu).
Jeżeli na tym etapie nie znamy tego adresu to należy zostawić domyślny.
Po nawiązaniu komunikacji z urządzeniem o adresie IP jak poniżej, pole to zostanie zaktualizowane.

IP - edytowalne pole na wpisanie statycznego adresu IP kontrolera
(domyślny dla HID® 192.168.0.251 - należy zmienić na docelowy)

Port - edytowalne pole na wpisanie nr portu (zaleca się pozostawienie wartości domyślnej)

Konfiguracja przejść, tylko dla **serii HID®**- X1100 i X100:

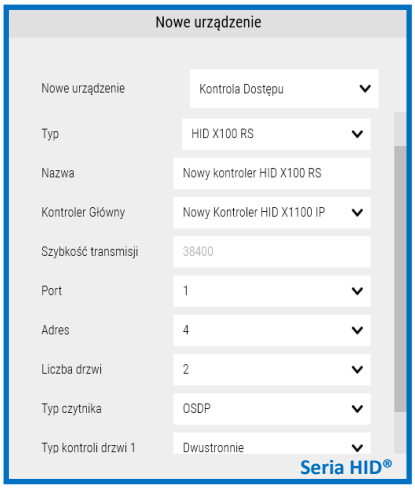
Liczba drzwi - z rozwijanej listy można wybrać 1 lub 2 drzwi w zależności od wymagań instalacji.

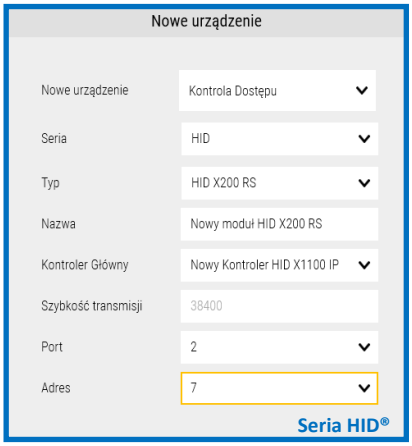
Typ czytnika - OSDP lub Wiegand w zależności od sposobu komunikacji pomiędzy kontrolerem a czytnikami.

Typ kontroli drzwi 1/2 - Dwustronnie lub Jednostronnie kontrolowane, w przypadku kontrolerów HID®Aero® możemy na jednym urządzeniu wykonać instalację mieszaną z przejściami jedno i dwustronnie kontrolowanymi.

Czytnik Secure Channel - Włączenie szyfrowania AES-128 pomiędzy kontrolerem a czytnikami - **tylko dla OSDP!**

Automatyczna synchronizacja czasu - Włączenie automatycznej synchronizacji zegara z serwerem.





Kontroler Główny - wybór kontrolera do którego połączymy moduły (X100, X200 i X300)

Port - Wybór portu 1 lub 2 magistrali RS-485 do którego podłączamy moduły (X100, X200 i X300)

Adres - Adres magistrali RS-485 ustawiany na przełącznikach DIP modułów (X100, X200 i X300) określany w przedziale 0-31

Seria 3000:

Typ - z rozwijanej listy można wybrać model kontrolera:

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

Nazwa - edytowalne pole na wpisanie nazwy kontrolera

MAC - edytowalne pole na wpisanie adresu MAC kontrolera (jest na naklejce na urządzeniu).
Jeżeli na tym etapie nie znamy tego adresu to należy zostawić domyślny.
Po nawiązaniu komunikacji z urządzeniem o adresie IP jak poniżej, pole to zostanie zaktualizowane.

IP - edytowalne pole na wpisanie statycznego adresu IP kontrolera
(domyślny dla KS30xx 192.168.0.245 - należy zmienić na docelowy)

Port - edytowalne pole na wpisanie nr portu (zaleca się pozostawienie wartości domyślnej)

Liczba drzwi - z rozwijanej listy można wybrać 1,2 lub 4 drzwi w zależności od modelu kontrolera

Typ modułu - z rozwijanej listy można wybrać w zależności od modelu kontrolera:
- KDH-MOD3000INOUT (dla kontrolerów KDH-KS3012/24),
- KDH-MOD-30004-ELV i KDH-MOD-30016-ELV (dla kontrolera KDH-KS3000-IP-ELV)

Format Wiegand - z rozwijanej listy można wybrać w zależności od modelu czytnika i kart: 26, 32, 34, 37, 39

Hasło komunikacyjne - edytowalne pole na wpisanie 4 cyfrowego hasła komunikacyjnego (0000 - 9999)

Kod do kasowania alarmu - edytowalne pole na wpisanie 6 cyfrowego kodu kasowania alarmu

Automatyczna synchronizacja czasu - po zaznaczeniu tego pola czas w kontrolerze będzie synchronizowany z serwera co 4 godziny

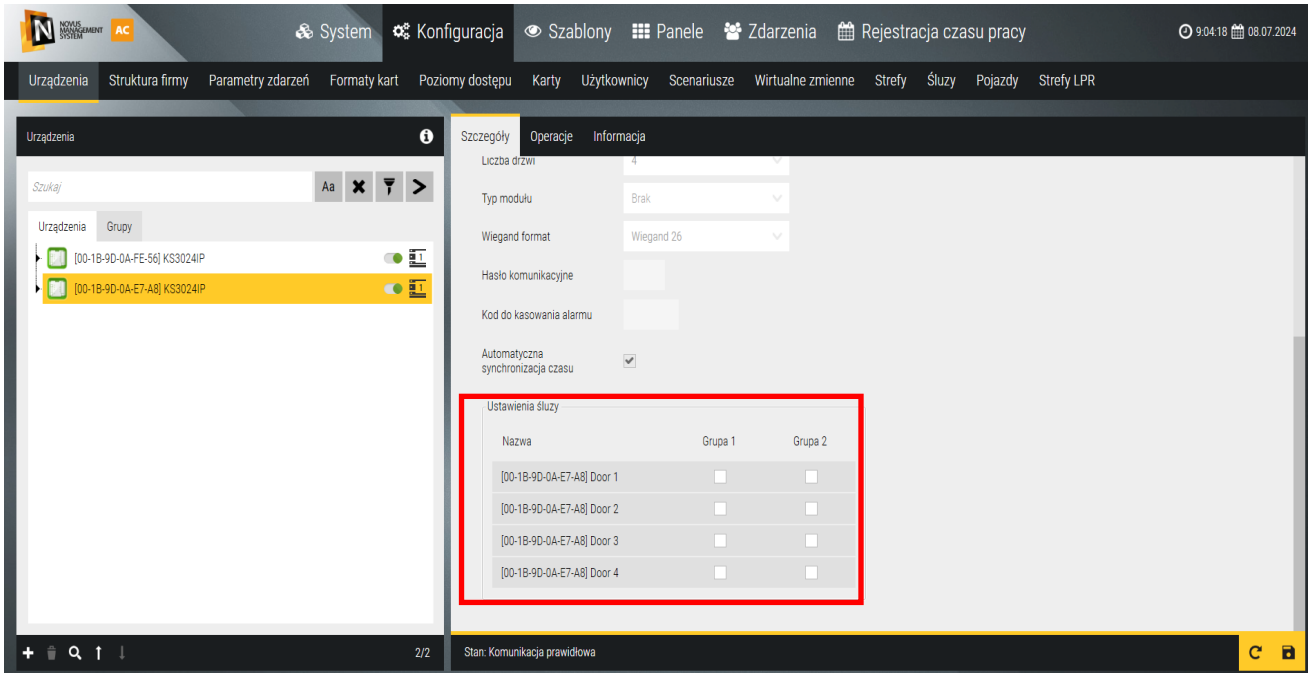
Opcje dla kontrolerów zintegrowanych:

Hasło administratora - wejście w tryb programowania z klawiatury (dotyczy KDH-KZ3000-IP-U lub M)

Alarm sabotażowy - włączenie/wyłączenie alarmu sabotażowego (dotyczy KDH-KZ3000-IP-U lub M)

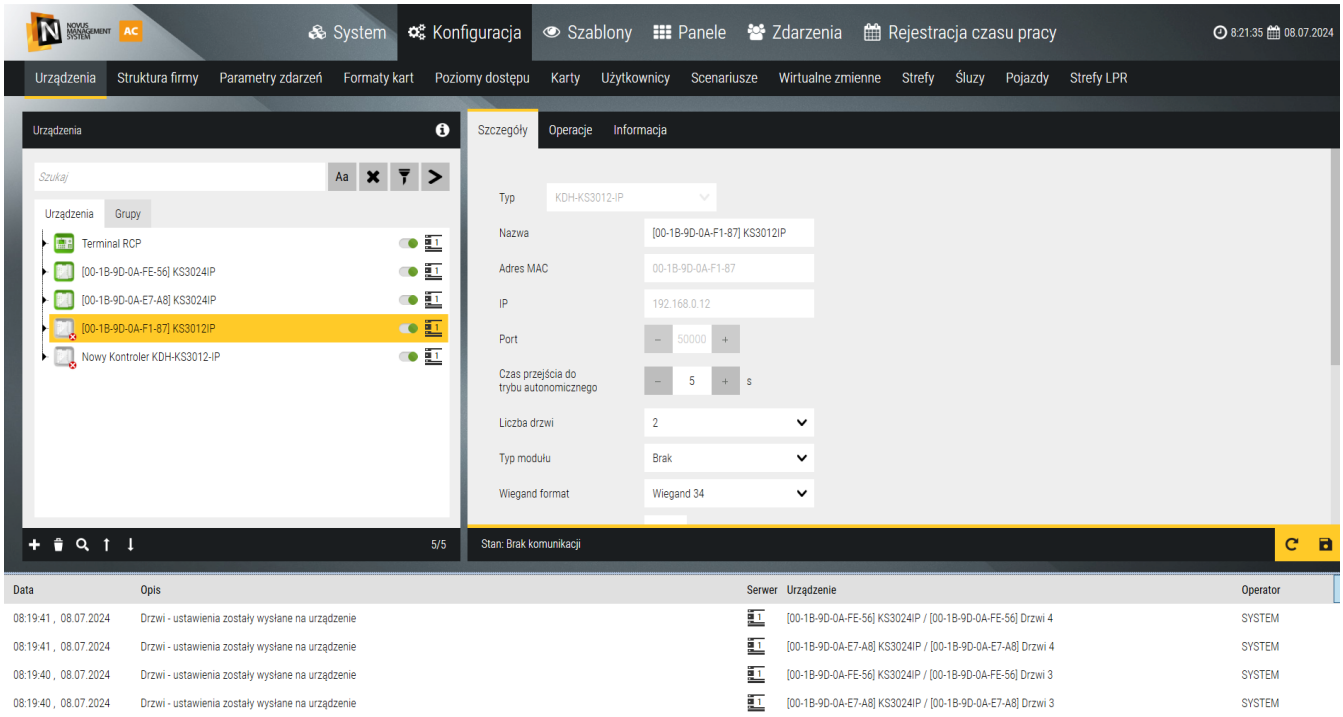
Alarm sforsowania drzwi - włączenie/wyłączenie alarmu sforsowania drzwi (dotyczy KDH-KZ3000-IP-U lub

Po dokonaniu w/w ustawień należy kliknąć ***OK*** - program wróci do głównego okna konfiguracji, a dodane urządzenie pojawi się na liście w prawym oknie.



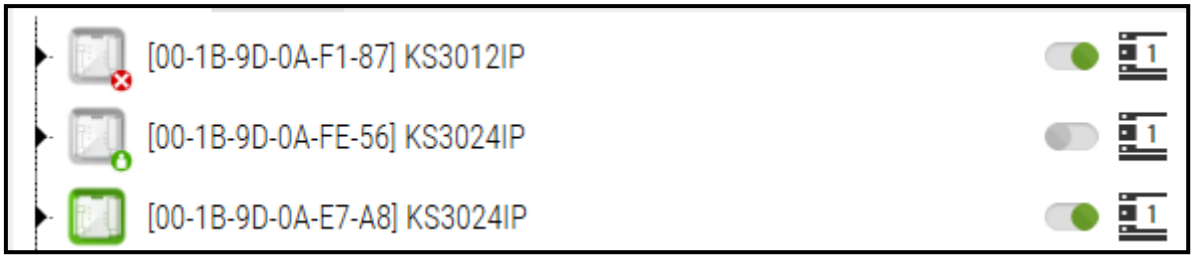
W przypadku kontrolerów KDH-KS3012/24-IP w prawym dolnym oknie pojawiają się dodatkowe pola umożliwiające dodanie drzwi i czytników kontrolera do jednej lub dwóch grup. Dotyczy to funkcji śluzy (czyli wzajemnej kontroli stanu skrzydła drzwi). Pola te nie występują w przypadku kontrolera windowego.

Po dokonaniu wszystkich ustawień należy je zapisać klikając na ikonie ***dyskietki*** w prawym dolnym rogu. W oknie logów systemu pojawi się seria komunikatów dotycząca o tej operacji a ikony ***kontrolerów*** zmienia kolor na zielony. Zapisu można dokonać jednorazowo po dodaniu więcej niż jednego urządzenia.

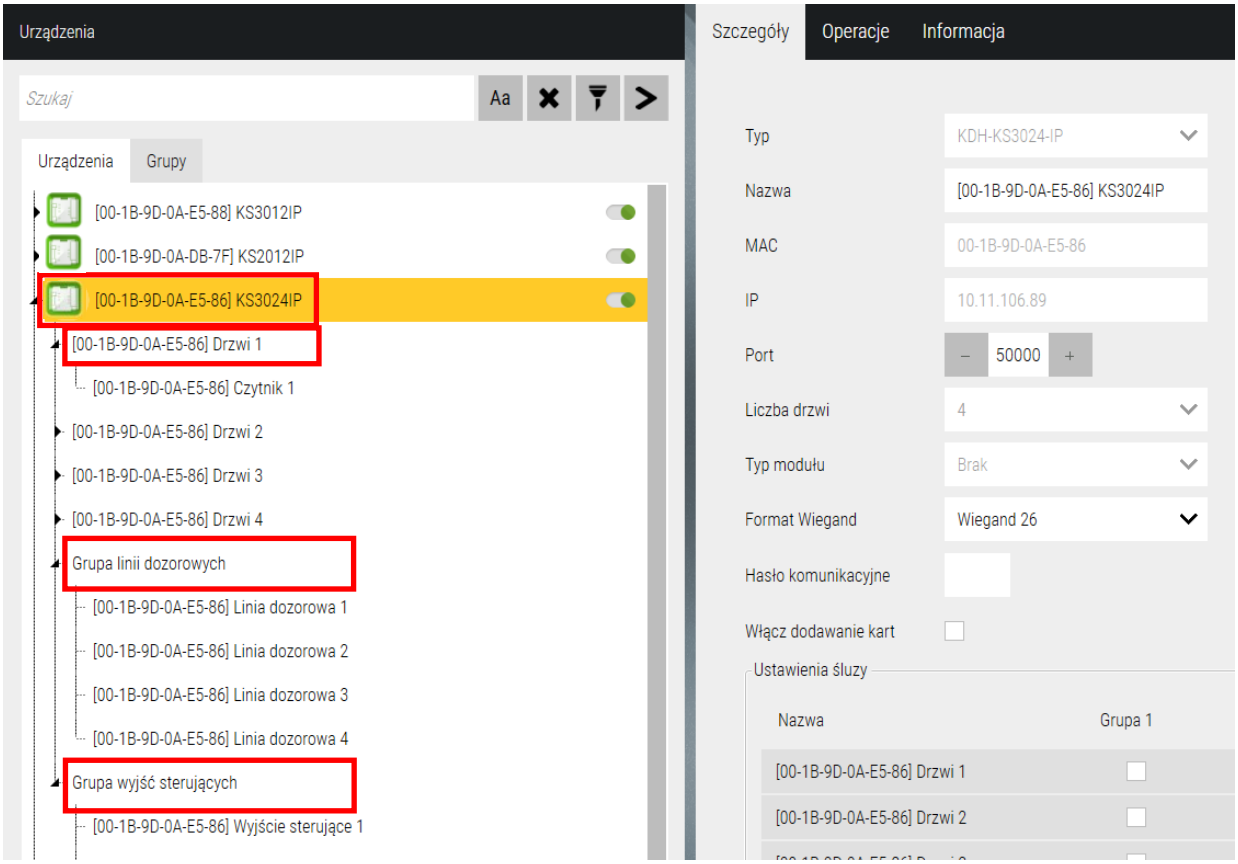


Po zapisaniu ustawień stan ikon może pokazywać jedną z trzech sytuacji:

- Brak komunikacji z urządzeniem - szara ikona z czerwonym polem (należy sprawdzić ustawienia adresu lub podłączenie do sieci oraz zasilanie)
- Urządzenie rozłączone przez operatora - szara ikona z zielonym polem (wyłączenie monitorowania poprzez przesunięcie w lewo suwaka po prawej stronie, w celu edycji ustawień lub wykonania czynności serwisowych)
- Komunikacja prawidłowa - zielona ikona



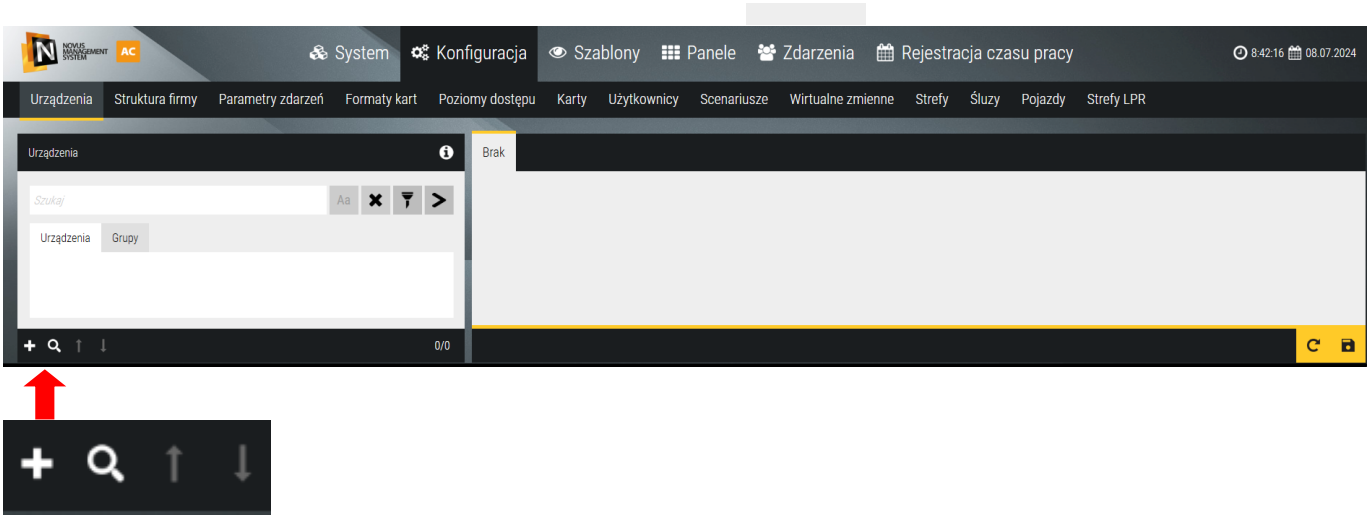
Ikonę ***kontrolera*** można rozwinąć klikając na czarny trójkąt na linii głównego drzewa i wyświetlić elementy współpracujące. Zaznaczając wybrany element na rozwiniętej liście możemy edytować jego ustawienia.



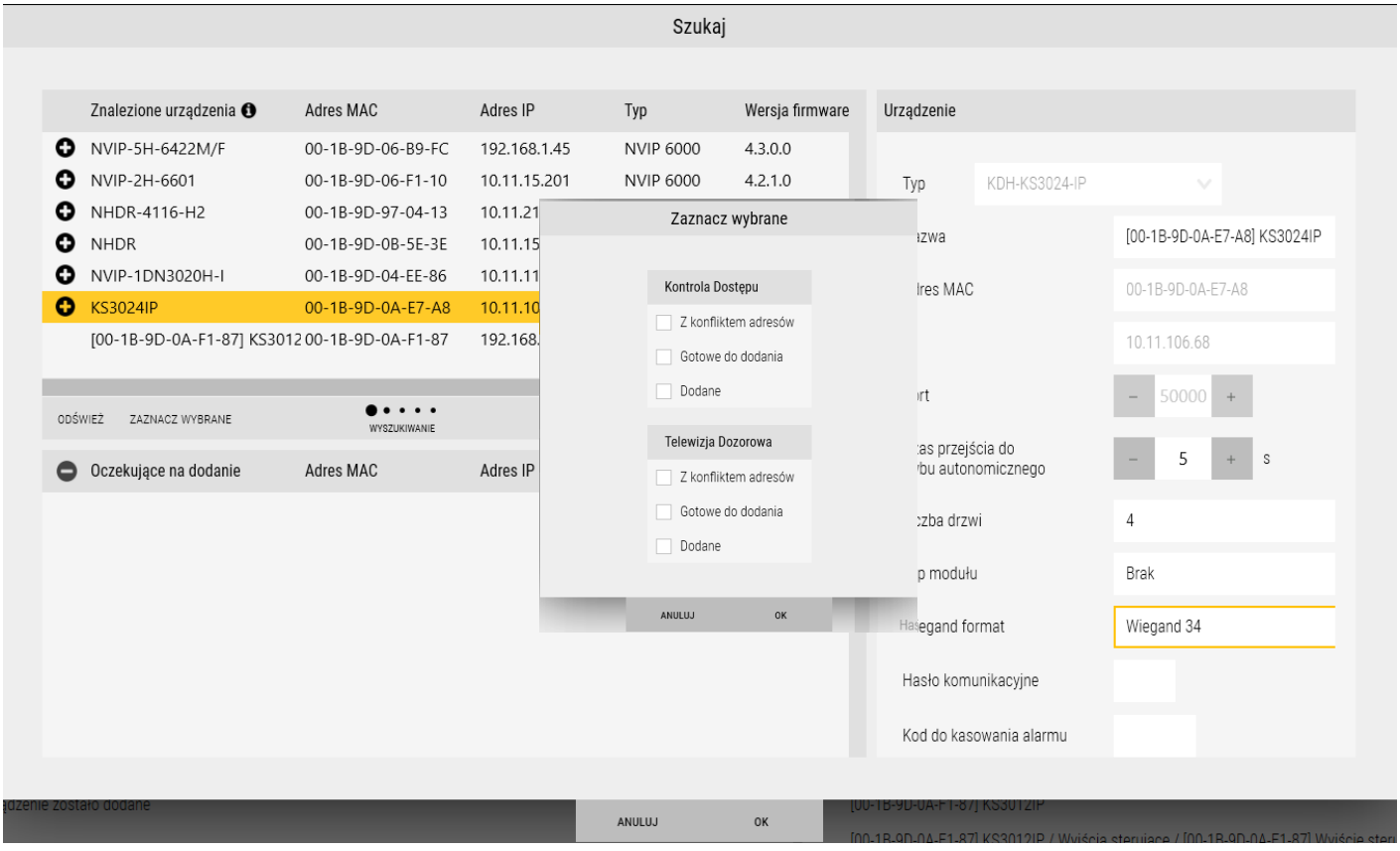
Dotyczy to takich elementów jak: drzwi, czytniki, linie dozorowe i wyjścia sterujące. Po zaznaczeniu wybranego elementu, w prawym oknie wyświetlane są jego ustawienia, które można edytować. Wybrany element podświetlany jest na żółto. Po zmianie ustawień należy je zapisać klikając na dyskietce w prawym dolnym rogu okna konfiguracji. Żeby edytować ustawienia kontrolera należy go rozłączyć przesuwając zielony suwak w lewą stronę. Po zakończeniu edycji należy ponownie przestawić suwak w prawo i kliknąć na dyskietce ***Zapisz***.

Zdefiniowany kontroler można edytować lub usuwać zaznaczając go na liście i klikając na przycisk ***Usuń*** w lewym dolnym rogu okna. Wraz z kontrolerem usuwane są wszystkie elementy współpracujące w całym systemie.

Wyszukiwanie urządzeń kontroli dostępu



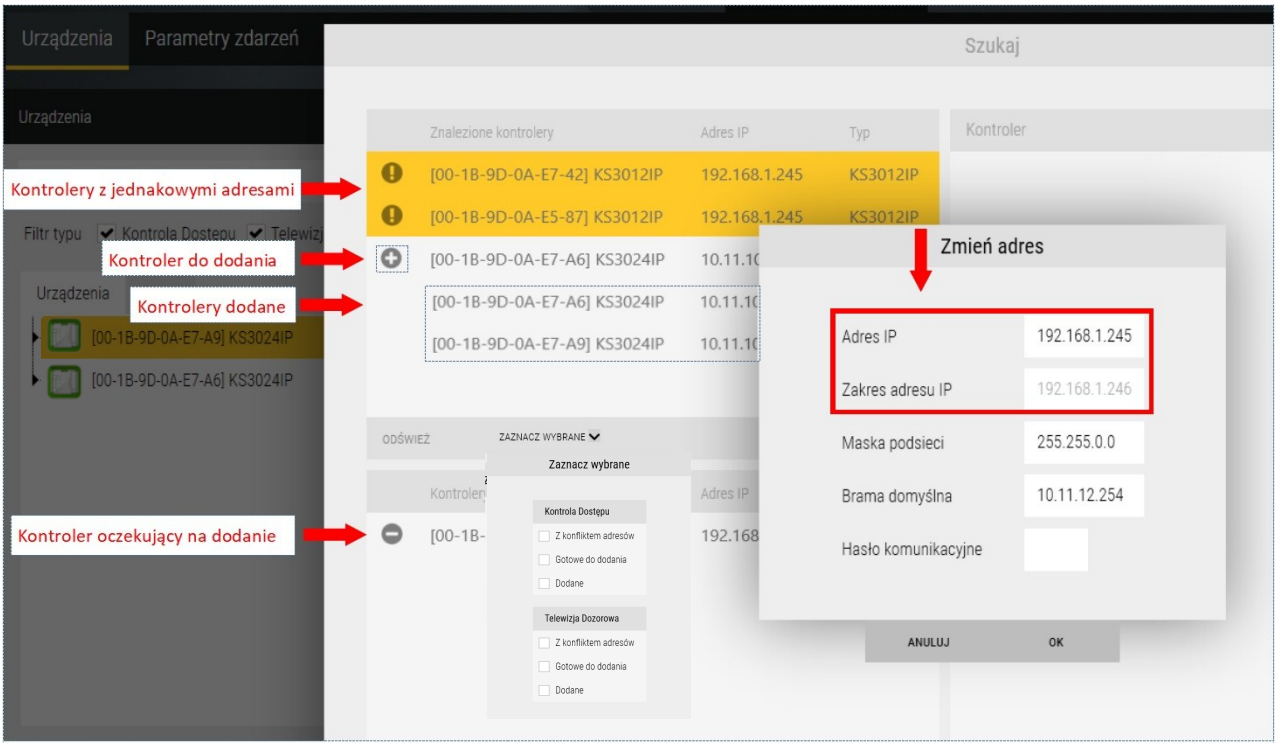
Gdy kontrolery zostały zainstalowane na obiekcie, podłączone do sieci Ethernet i zasilania, to w celu dodania ich do bazy systemu zaleca się skorzystać z dostępnej w programie wyszukiwarki. Przyspiesza to znacznie ten proces. Aby uruchomić wyszukiwarkę należy kliknąć na przycisk ***Szukaj*** na dole okna jak powyżej. Program wyświetli okno, w którym pojawi się lista wyszukanych w sieci kontrolerów.



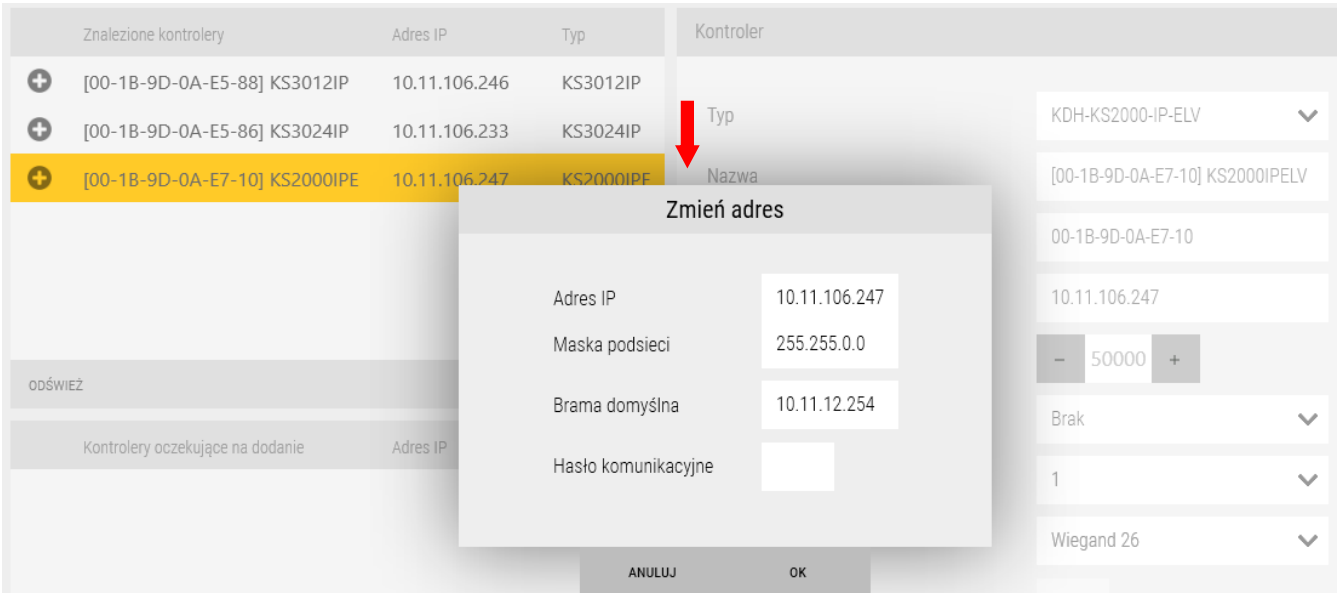
Wyszukane w sieci kontrolery wyświetlane są w lewej górnej części okna z ikonami informującymi o ich statusie:

- - kontrolery z taki samymi adresami IP - wyświetlane są na samym początku listy
- - kontrolery możliwe do dodania do systemu
- - kontrolery przeniesione z listy w górnym oknie i oczekujące na dodanie, można je cofnąć na górną listę
- - kontrolery wyszukane, ale już dodane do systemu - brak ikony przed kontrolerem

Każdy nowy kontroler **serii 3000** posiada ten sam domyślny adres IP - 192.168.0.245. Ta grupa kontrolerów jest wyświetlana na początku listy z ikoną - należy je wszystkie zaznaczyć (z CTRL) i zmienić im grupowo adresację zgodnie z przydzieloną przez administratora pulą adresów na kolejne docelowe klikając na przycisku *Zmień adres.* Po wpisaniu adresu początkowego, adres końcowy zakresu zostanie wygenerowany automatycznie w zależności od ilości zaznaczonych kontrolerów z jednakowym adresem IP. Ikony zmienią się na i można je wtedy dodać do dolnego okna klikając na tych ikonach. Adresy kontrolerów **serii HID®** należy konfigurować z poziomu przeglądarki zgodnie z instrukcją zawartą w opakowaniu, brak możliwości zmiany adresu z poziomu oprogramowania NOVUS MANAGEMENT SYSTEM AC.



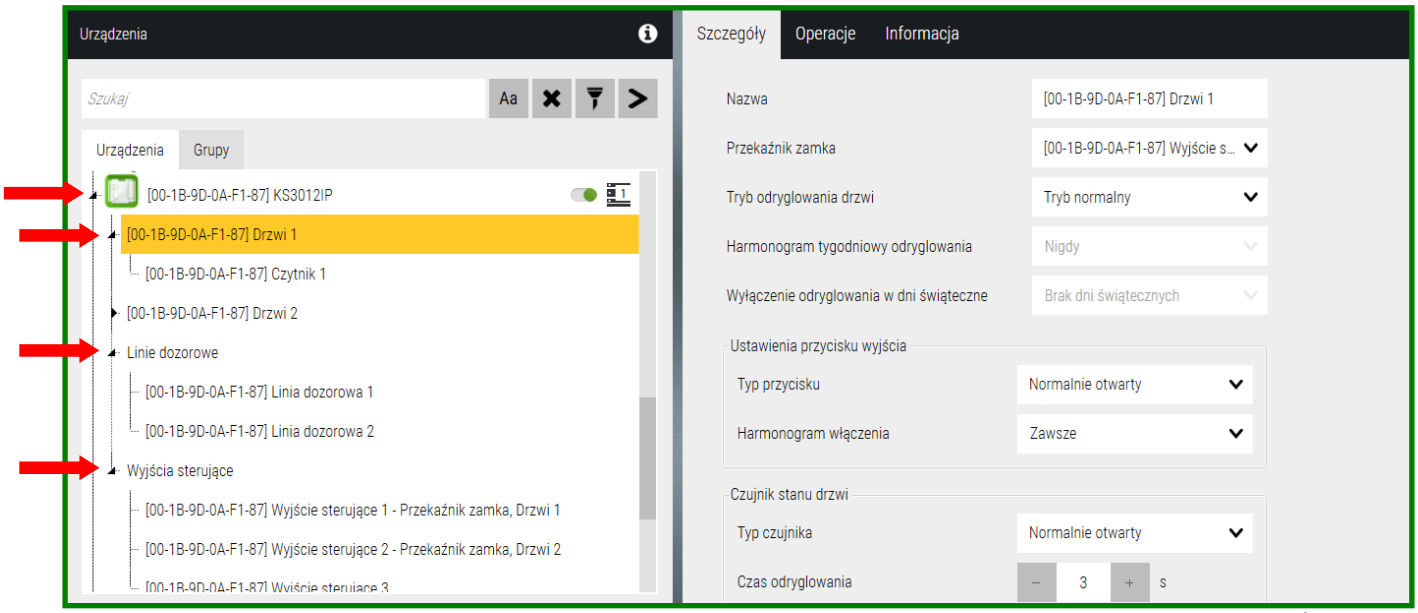
Na rozwijanej liście możemy wybrać, którą grupę kontrolerów chcemy zaznaczyć. W przypadku gdy chcemy zmienić adres jednego wyszukanego kontrolera, zaznaczamy go na liście w górnym oknie i klikamy na przycisku ***Zmień adres***.



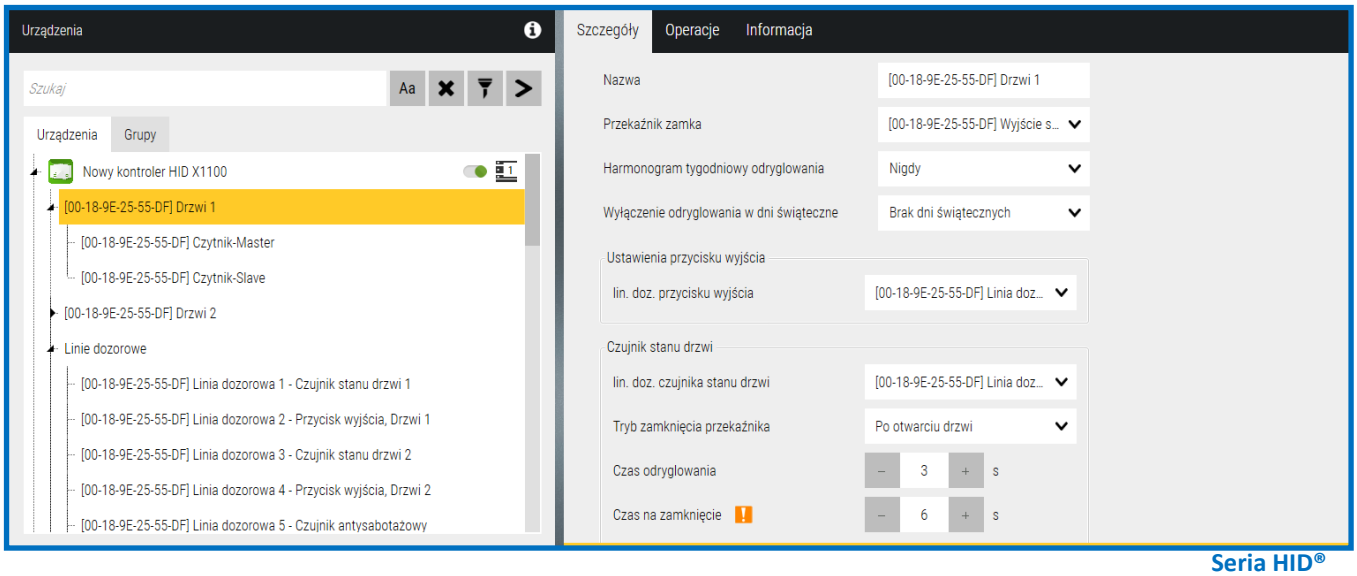
Po ustawieniu adresów i dodaniu wszystkich kontrolerów do listy w dolnym oknie należy kliknąć na przycisk ***OK***. Dodane kontrolery pojawią się w oknie ***Urządzenia***.

3.2 Urządzenia - Kontrola dostępu - Kontroler - Drzwi

W procesie dodawania kontrolerów program automatycznie dodaje elementy współpracujące w ilościach zależnych od typu kontrolera. Dotyczy to drzwi, linii dozorowych, wyjść sterujących i modułów rozszerzeń. Elementy te pojawiają się pod każdym z dodanych kontrolerów i możemy je wyświetlić klikając na czarne trójkąty w poszczególnych gałęziach drzewa urządzeń.



Seria 3000



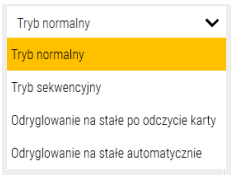
Seria HID®

Ustawienia drzwi

Nazwa - edytowalne pole na wpisanie nazwy drzwi w miejsce nazwy domyślnej.

Przekaźnik zamka - z rozwijanej listy można wybrać wyjście sterujące (przekaźnik), które będzie sterowało zamkiem, domyślnie przypisane są przekaźniki 1-2 lub 1-4, a przekaźnik 3 lub 5 jest przekaźnikiem do podłączenia sygnalizatora alarmu.

Tryb odryglowania drzwi - do wyboru jeden z czterech trybów - tylko w kontrolerach **serii 3000:**



Tryb normalny odryglowuje drzwi na czas ustawiony w polu poniżej.
Tryb sekwencyjny odryglowuje i zaryglowuje drzwi na przemian po kolejnych odczytach karty.
Tryb 3 i 4 wymaga ustawienia terminarza, na początku którego drzwi zostają odryglowane na na stałe po odczycie ważnej karty lub automatycznie.

Harmonogram tygodniowy odryglowania - z rozwijanej listy można wybrać zdefiniowany uprzednio terminarz, zgodnie z którym drzwi zostaną odryglowane na stałe po odczycie ważnej karty (seria 3000) lub automatycznie w zależności od wybranej powyżej opcji.

Wyłączenie odryglowania w dni świąteczne - dotyczy dni świątecznych, jest nadrzędny nad tygodniowym terminarzem odryglowania i blokuje jego działanie jeżeli w ciągu tygodnia występuje dzień świąteczny, w którym drzwi nie powinny się odryglować na stałe.

Ustawienia przycisku wyjścia

Seria 3000:

Typ przycisku - z rozwijanej listy można wybrać typ NO lub NC - zalecany NC.

Harmonogram włączenia - z rozwijanej listy można wybrać zdefiniowany uprzednio terminarz, w okresie jego aktywności drzwi nie będzie można odryglować przez naciśnięcie przycisku.

Seria HID®:

lin.doz.przycisku wyjścia - wybór z listy linii dozorowej przypisanej do przycisku wyjścia.

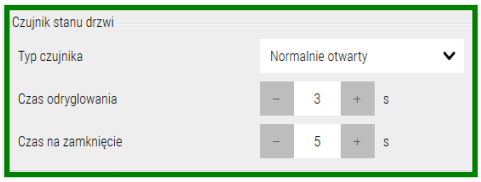
Ustawienia czujnika stanu drzwi

Seria 3000:

Typ czujnika - z rozwijanej listy można wybrać typ NO lub NC

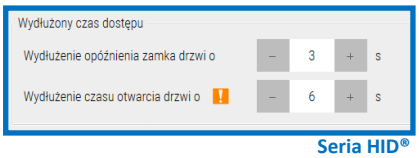
Czas odryglowania - edytowalne pole na wpisanie czasu (s) odryglowania zamka po odczycie ważnej karty lub naciśnięciu przycisku wyjścia. Czas można ustawić również klikając na przyciski **-** lub **+**. Wartość maksymalna - 50 s.

Czas na zamknięcie - edytowalne pole na wpisanie czasu (s) na zamknięcie skrzydła drzwi. Po upływie czasu, który jest sumą czasów na zamknięcie i odryglowanie zostanie wygenerowany alarm *Drzwi przetrzymane* - domyślnie 8 s. (3+5). Czas można ustawić również klikając na przyciski **-** lub **+**. Wartość maksymalna - 50 sekund.



Seria 3000

Seria HID®



Seria HID®

Seria HID®:

Lin. doz. czujnika stanu drzwi - wybór z listy linii dozorowej przypisanej do czujnika stanu drzwi (kontaktronu).

Tryb zamknięcia przekaźnika - Po otwarciu drzwi / Po zamknięciu drzwi

Czas odryglowania - edytowalne pole na wpisanie czasu (s) odryglowania zamka po odczycie ważnej karty lub naciśnięciu przycisku wyjścia. Czas można ustawić również klikając na przyciski **-** lub **+**. Wartość maksymalna - 255 s.

Czas na zamknięcie - edytowalne pole na wpisanie czasu (s) na zamknięcie skrzydła drzwi. Po upływie czasu, który jest sumą czasów na zamknięcie i odryglowanie zostanie wygenerowany alarm *Drzwi przetrzymane ,* konfigurowane tylko w przedziale liczb parzystych od 2 (s) do 512 (s).

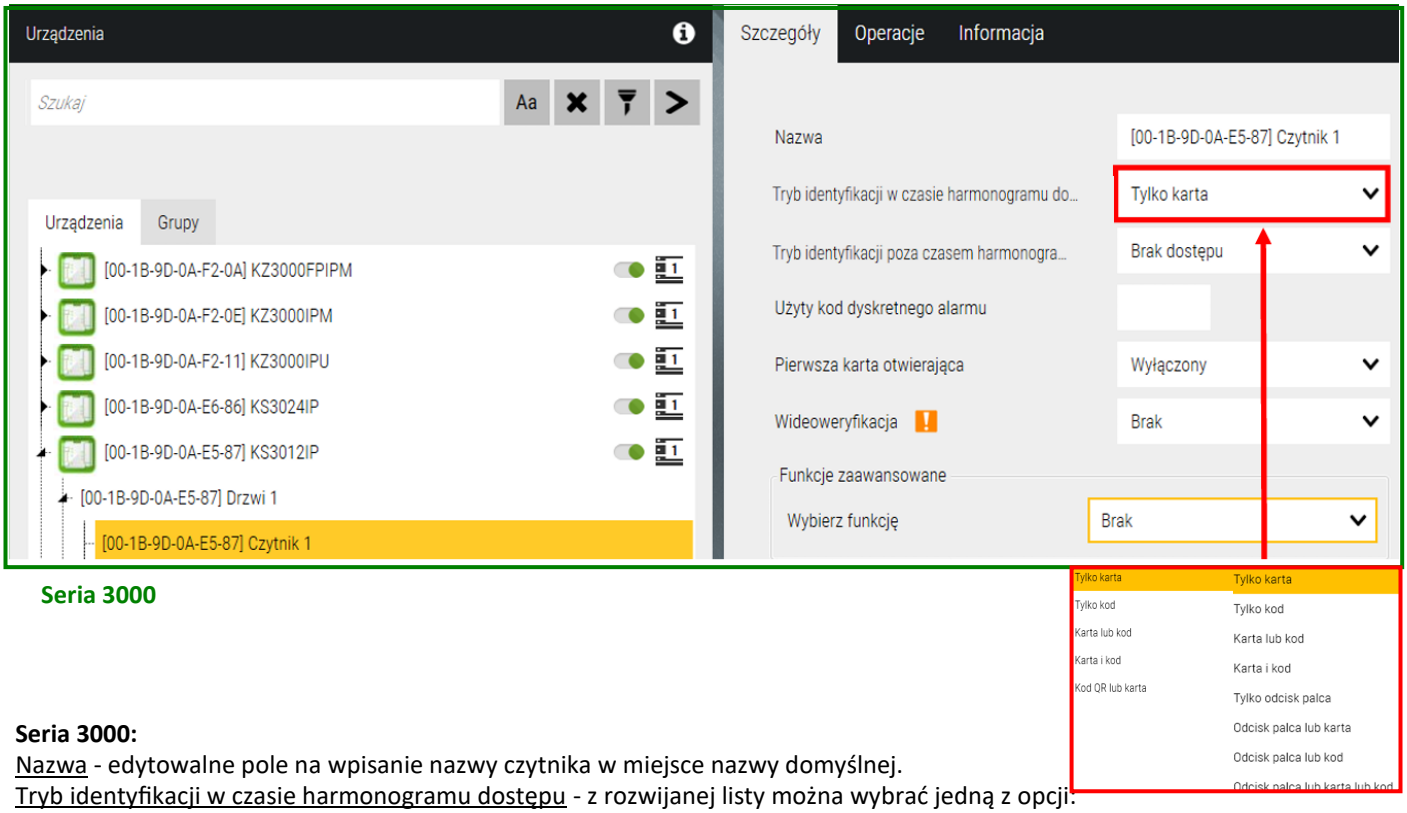
Wydłużony czas na dostęp - pozwala na wydłużenie dostępu do danego przejścia użytkownikom z odpowiednimi uprawnieniami

Wydłużenie opóźnienia zamka o - wydłuża czas odryglowania zamka o ustawiony czas w sekundach

Wydłużenie czasu otwacia drzwi o - wydłuża czas na zamknięcie drzwi o ustawiony czas w sekundach

(tylko parzysty)

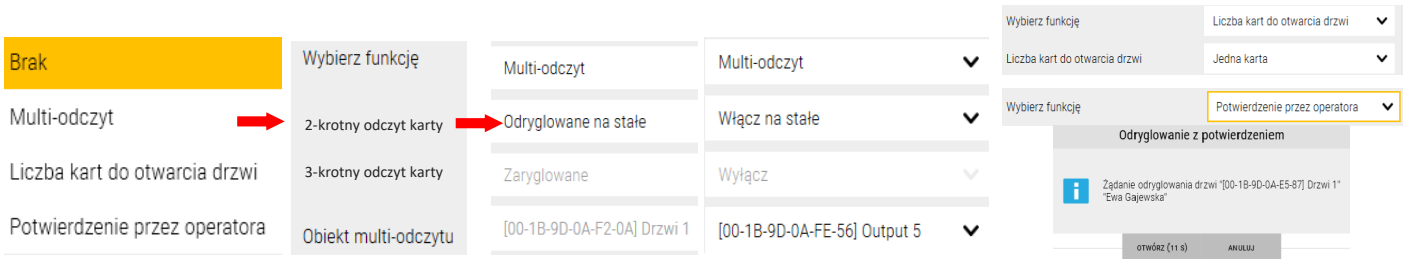
3.3 Urządzenia - Kontrola dostępu - Kontroler - Drzwi - Czytnik

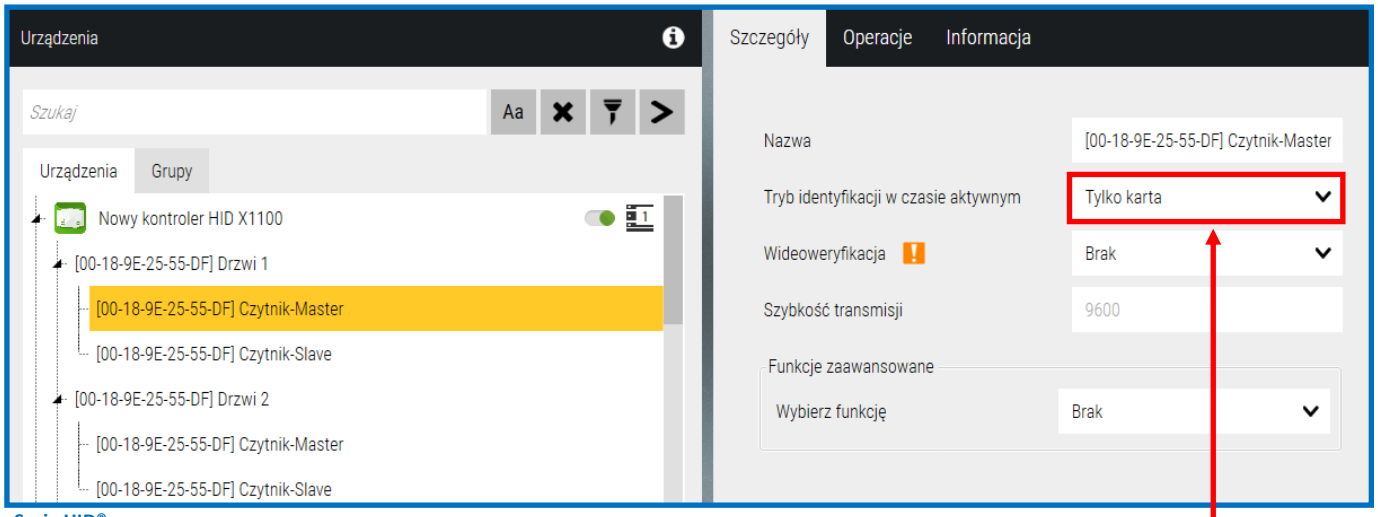


Seria 3000

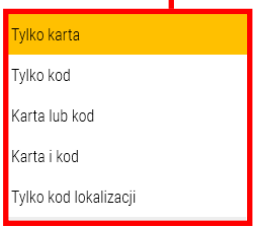
Seria 3000:
Nazwa - edytowalne pole na wpisanie nazwy czytnika w miejsce nazwy domyślnej.
Tryb identyfikacji w czasie harmonogramu dostępu - z rozwijanej listy można wybrać jedną z opcji:
Tryb identyfikacji poza czasem harmonogramu dostępu - z rozwijanej listy można wybrać jedną z opcji:
(ten tryb dotyczy okresu poza godzinami pracy, w weekendy i święta)
Kod dyskretnego alarmu - pole na wpisanie kodu dostępu, którego należy użyć na klawiaturze czytnika w przypadku wejścia pod przymusem. Powoduje on wygenerowanie dyskretnego alarmu na stacji operatora.
Pierwsza karta otwierająca - uzyskanie dostępu wymaga użycia w ciągu każdej doby najpierw karty z ustawioną tą opcją na TAK (jest takie pole w ustawieniach karty).
Wideoweryfikacja - umożliwia przypisanie do czytnika zainstalowanej nad nim (lub wbudowanej) kamery do rejestracji stop-klatki w chwili odczytu karty. Stopklatka jest dołączana do zdarzenia na stosie i w raporcie na ekranie.
Funkcje zaawansowane: - wybór jak w oknie poniżej:

Multi-odczyt - pozwala rozszerzyć funkcję karty. Poprzez 2-lub 3-krotny odczyt uprawnionej karty możliwe jest odryglowanie/ zaryglowanie drzwi na stałe lub włączenie/wyłączenie wyjścia sterującego. Dotyczy wybranych drzwi i uprawnionej karty.
Liczba kart do otwarcia drzwi - uzyskanie dostępu wymaga użycia kolejno od jednej do czterech ważnych kart.
Opcja specjalna do pomieszczeń wymagających większego bezpieczeństwa (tzw. wejście komisyjne).
Potwierdzenie przez operatora - po zaznaczeniu uzyskanie dostępu z tego czytnika będzie wymagało odczytu ważnej karty oraz potwierdzenia przez operatora w specjalnym wyskakującym okienku. Opcję tą należy wybrać tylko, gdy system pracuje w trybie on-line i przy stacji obecny jest operator lub pracownik ochrony.





Seria HID®



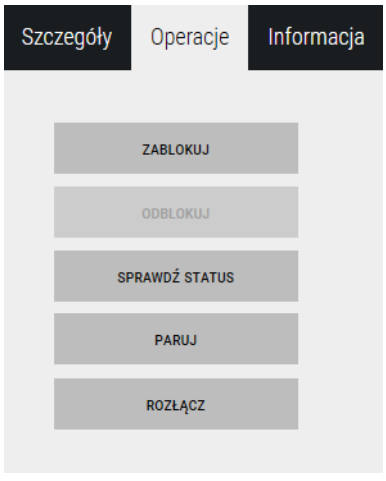
Seria HID®:
Czytnik-Master - Czytnik podłączony poprzez protokół OSDP z adresem 0
Czytnik-Slave - Czytnik podłączony poprzez protokół OSDP z adresem 1
Nazwa - edytowalne pole na wpisanie nazwy czytnika w miejsce nazwy domyślnej.
Tryb identyfikacji w czasie aktywnym - z rozwijanej listy można wybrać jedną z opcji:

Wideoweryfikacja - umożliwia przypisanie do czytnika zainstalowanej nad nim kamery do rejestracji stopklatki w chwili odczytu karty. Stopklatka jest dołączana do zdarzenia na stosie i w raporcie na ekranie.
Szybkość transmisji: Tylko w przypadku czytników podłączonych po OSDP - szybkość Transmisji danych (standardowo 9600) wymaga ustawienia takiej samej konfiguracji w czytniku.

Funkcje zaawansowane: - wybór jak w oknie poniżej:

Potwierdzenie przez operatora - po zaznaczeniu uzyskanie dostępu z tego czytnika będzie wymagało odczytu ważnej karty oraz potwierdzenia przez operatora w specjalnym wyskakującym okienku. Opcję tą należy wybrać tylko, gdy system pracuje w trybie on-line i przy stacji obecny jest operator lub pracownik ochrony.
Liczba kart do otwarcia drzwi - uzyskanie dostępu wymaga użycia kolejno 2 dwóch ważnych kart.
Opcja specjalna do pomieszczeń wymagających większego bezpieczeństwa (tzw. wejście komisyjne).
Multi-odczyt - pozwala rozszerzyć funkcję karty. Poprzez 2-krotny odczyt uprawnionej karty możliwe jest odryglowanie/ zaryglowanie drzwi na stałe lub włączenie/wyłączenie wyjścia sterującego. Dotyczy wybranych drzwi i uprawnionej karty.

Operacje:



Seria HID®

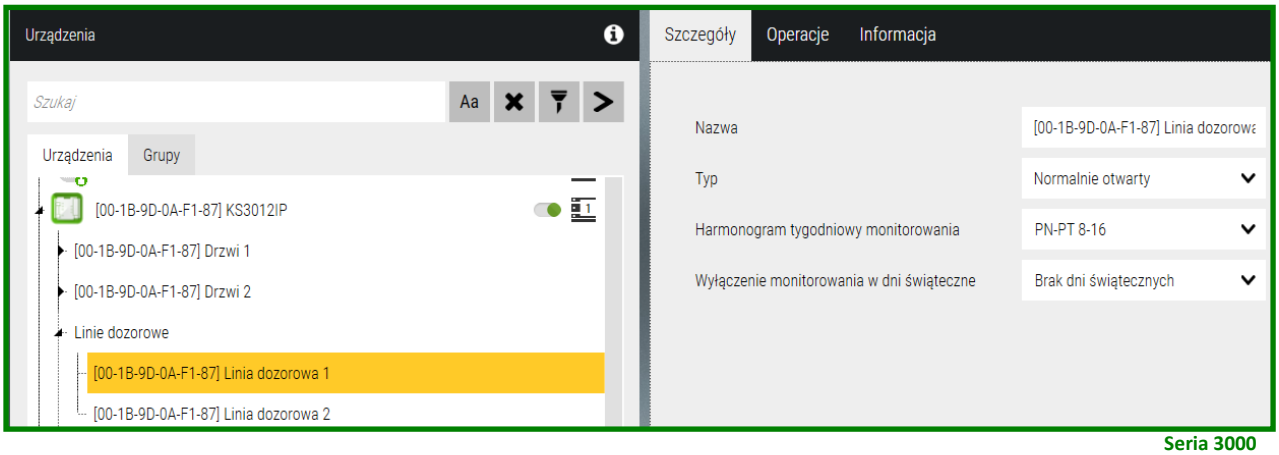
Zablokuj / Odblokuj czytnik - umożliwia zablokowanie czytnika przez operatora

Sprawdź status - wyświetla stan czytnika (tylko dla OSDP) informując o komunikacji ,włączonym lub wyłączonym szyfrowaniu połączenia.

Paruj - służy do sparowania czytników podłączonych po OSDP z włączonym szyfrowaniem (secure channel) - w czytniku HID® należy odpowiednio skonfigurować jego komunikację poprzez włączenie w aplikacji mobilnej *HID® Reader Manager:* **SPEC COMPLIANCE - V2, Install Mode - włączony, Secure Mode - włączony**

Rozłącz - służy do rozłączenia się z czytnikami podłączonymi po OSDP z włączonym szyfrowaniem (secure channel). Po rozłączeniu należy ponownie skonfigurować czytnik w aplikacji *HID® Reader Manager*, resetowi ulega adres czytnika oraz funkcje **Instal Mode i Secure Mode**

3.4 Urządzenia - Kontrola dostępu - Kontroler - Linie dozorowe



Seria 3000

Linie dozorowe zlokalizowane na kontrolerze umożliwiają podłączenie i monitorowanie różnego rodzaju czujek. Żeby włączyć tryb monitorowania należy do linii ustawić terminarz tygodniowy i świąteczny. Jeżeli monitorowanie jest wyłączone to naruszenie linii skutkuje tylko zmianą stanu ikony na panelu. W zależności od modelu kontrolera mamy do dyspozycji 2 lub 4 linie dozorowe i 4 na module rozszerzeń KDH-MOD2000INOUT dla **serii 3000** oraz 7 linii dozorowych dla **serii HID®** X1100 i X100, 19 linii dozorowych dla modułu X200 i 5 linii dla X300.

Seria 3000

Nazwa - edytowalne pole na wpisanie nazwy linii dozorowej w miejsce nazwy domyślnej.

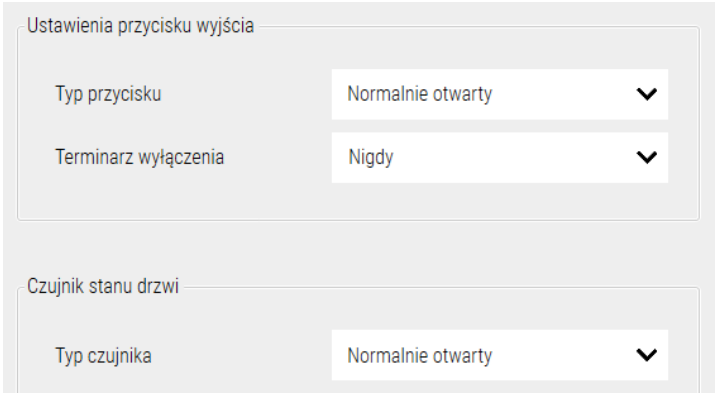
Typ linii dozorowej - z rozwijanej listy można wybrać typ NO lub NC - zalecany NC.

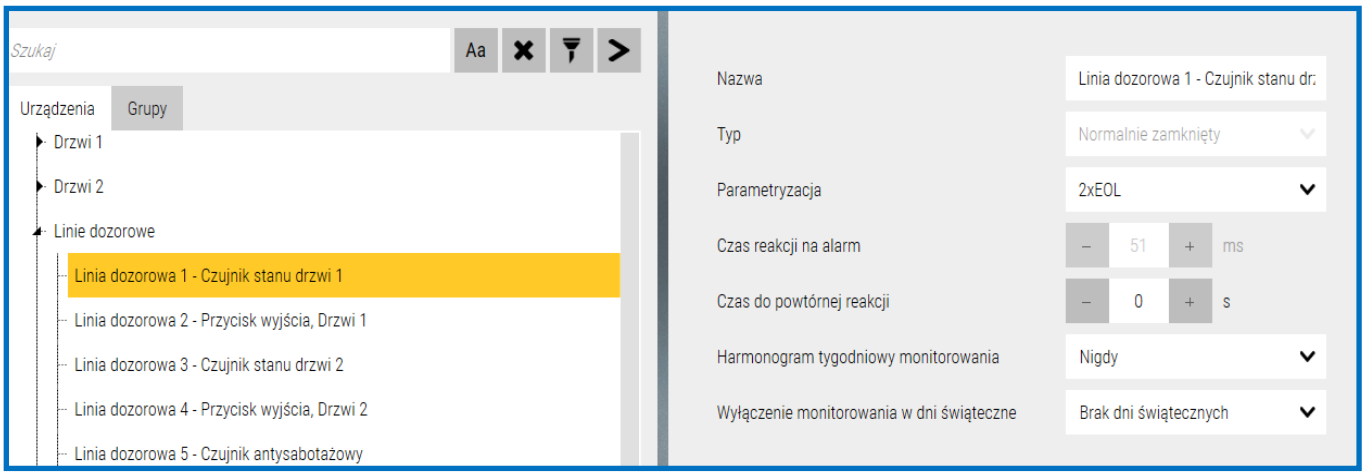
Harmonogram tygodniowy monitorowania - z rozwijanej listy można wybrać zdefiniowany uprzednio terminarz zgodnie, z którym linia będzie monitorowana i wówczas będą generowane alarmy.

Wyłączenie monitorowania w dni świąteczne - dotyczy dni świątecznych, jest nadrzędny nad tygodniowym terminarzem tygodniowym i zmienia jego działanie, jeżeli w ciągu tygodnia występuje dzień świąteczny, w którym linia powinna mieć inny terminarz monitorowania.

Analogicznie wyglądają ustawienia dla linii dozorowych na module rozszerzeń jeżeli został zaimplementowany.

Ustawienia dla linii dozorowych przeznaczonych do czujników stanu drzwi i przycisków wyjścia dostępne są w oknie konfiguracji *Drzwi.*





Seria HID®

Seria HID®

Nazwa - edytowalne pole na wpisanie nazwy linii dozorowej w miejsce nazwy domyślnej.

Typ - z rozwijanej listy można wybrać typ NO lub NC - zalecany NC.

Parametryzacja - Brak/2xEOL - parametryzacja linii dozorowej dwoma rezystorami o wartości 1K, w przypadku wybrania parametryzacji linii dozorowej możemy uzyskać 4 różne stany linii: *stan normalny/alarm/sabotaż/usterka*

Czas reakcji na alarm - ustawienie opóźnienia reakcji linii dozorowej w przedziale 0-255 (ms)

Czas do powtórnej reakcji - ustawienie opóźnienia powtórnej reakcji linii dozorowej w przedziale 0-15 (s)

Harmonogram tygodniowy monitorowania - z rozwijanej listy można wybrać zdefiniowany uprzednio terminarz zgodnie, z którym linia będzie monitorowana i wówczas będą generowane alarmy.

Wyłączenie monitorowania w dni świąteczne - dotyczy dni świątecznych, jest nadrzędny nad tygodniowym terminarzem tygodniowym i zmienia jego działanie, jeżeli w ciągu tygodnia występuje dzień świąteczny, w którym linia powinna mieć inny terminarz monitorowania.

Analogicznie wyglądają ustawienia dla linii dozorowych na modułach rozszerzeń jeżeli został zaimplementowane.

Stany linii dozorowych:

Linia monitorowana przez harmonogram - stan normalny

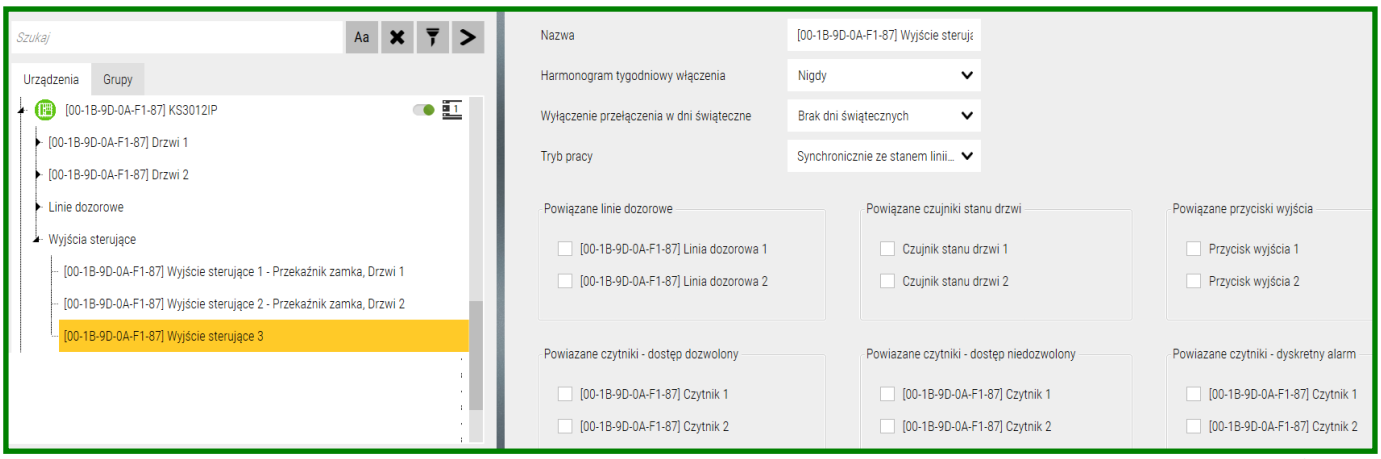
Linia monitorowana przez operatora - stan normalny

Alarm

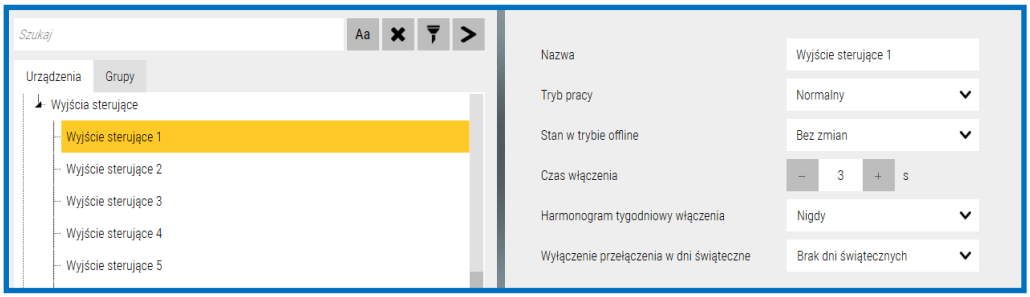
Usterka/zwarcie

Sabotaż

3.5 Urządzenia - Kontrola dostępu - Kontroler - Wyjścia sterujące



Seria 3000



Seria HID®

Wyjścia sterujące zlokalizowane na kontrolerze umożliwiają podłączenie i sterowanie różnego rodzaju urządzeniami. Pod względem funkcjonalności i ustawień dzielą się na dwie grupy:

- Wyjścia przypisane do drzwi i sterujące zamkiem elektrycznym
- Wyjścia sterujące ogólnego przeznaczenia

Seria HID®Aero® - W kontrolerach X1100 i modułach X100 dodatkowe wyjścia sterujące (przekaźniki) są zsynchronizowane z wyjściami sterującymi zamek elektryczny i mogą służyć na przykład do podłączenia sterowania diodami LED na czytnikach. Zalecane w przypadku gdy potrzebny jest impuls sterujący diodą LED podczas wysterowania przejścia z przycisku wyjścia, naciśnięcie przycisku wyjścia nie wyzwala wyjść GREEN LED na kontrolerach!

Wyjścia sterujące zamkiem elektrycznym w ustawieniach mają tylko zmianę nazwy i nie można postawić ich ikony na panelu ponieważ ich stan obrazuje kłódka w ikonie ***drzwi***.

Pozostałe wyjścia mają ustawienia jak na obrazie powyżej. Można do nich przypisać stan elementów systemu zlokalizowanych na tym samym kontrolerze lub wybranych zdarzeń. Zmiana stanu przypisanego elementu lub wystąpienie wybranego zdarzenia powoduje wtedy przełączenie przekaźnika.

W zależności od modelu kontrolera mamy do dyspozycji dla kontrolerów **serii 3000** - 3 lub 5 wyjść sterujących i 4 na module rozszerzeń KDH-MOD2000INOUT. Dla kontrolerów **serii HID®Aero®** - 4 wyjścia sterujące dla X1100 i X100, 2 wyjścia sterujące dla modułu X200 oraz 12 wyjść sterujących dla modułu X300.

Nazwa - edytowalne pole na wpisanie nazwy wyjścia sterującego w miejsce nazwy domyślnej.

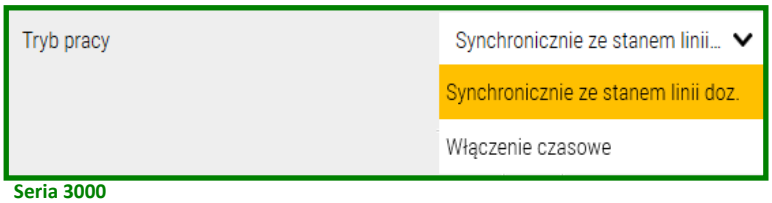
Harmonogram tygodniowy włączenia - z rozwijanej listy można wybrać zdefiniowany uprzednio terminarz zgodnie, z którym wyjcie będzie automatycznie przełączane.

Wyłączenie przełączenia w dni świąteczne - dotyczy dni świątecznych, jest nadrzędny nad tygodniowym terminarzem tygodniowym i zmienia jego działanie jeżeli w ciągu tygodnia występuje dzień świąteczny, w którym wyjście sterujące powinno mieć inny terminarz włączenia.

Analogicznie wyglądają ustawienia dla wyjść sterujących na module rozszerzeń, jeżeli został zaimplementowany

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

Synchronicznie ze stanem linii dozorowej - przełącza się gdy przypisana linia dozorowa wchodzi lub wychodzi ze stanu alarmu



Seria 3000

Do wyboru są:

- Stany trzech elementów: linii dozorowych, czujnika stanu drzwi i przycisku wyjścia
- Zdarzenia dotyczące dostępu zezwolonego, niedozwolonego oraz dyskretnego alarmu z klawiatury

Przypisanie synchronizacji staje się aktywne po zaznaczeniu checkboxa.

Suwaki umożliwiają wyświetlenie pozostałych pól wyboru.

Włączenie czasowe - przełącza się na czas ustawiony w polu poniżej od 0 do 255 (s)

Seria 3000

Stan w trybie offline - Tylko dla kontrolerów **serii HID®,** stan po przejściu kontrolera w tryb offline , do wyboru:

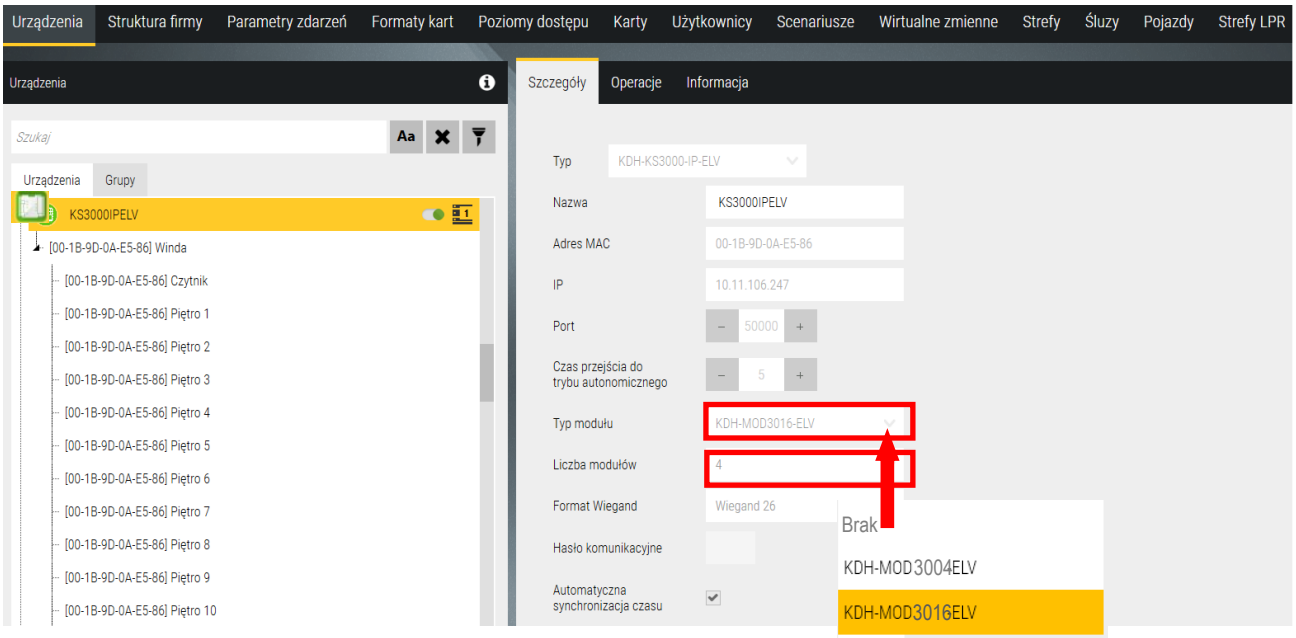
- Bez zmian
- Nieaktywny
- Aktywny

Czas włączenia - przełącza się na czas ustawiony w polu poniżej

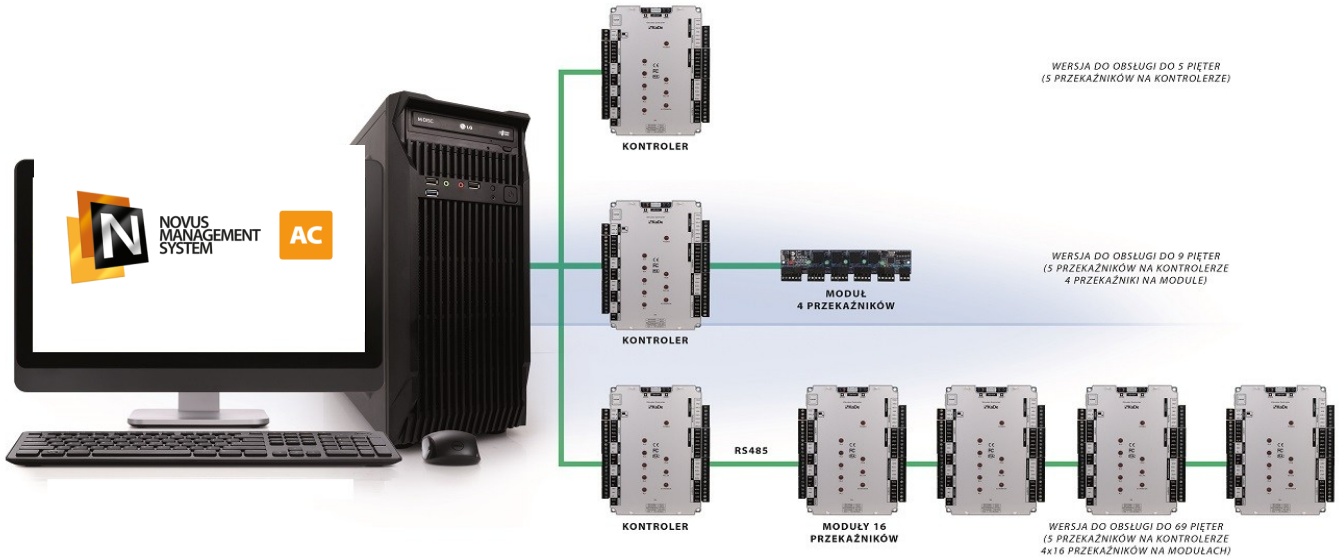
Seria HID®

3.6 Urządzenia - Kontrola dostępu - Kontroler windowy

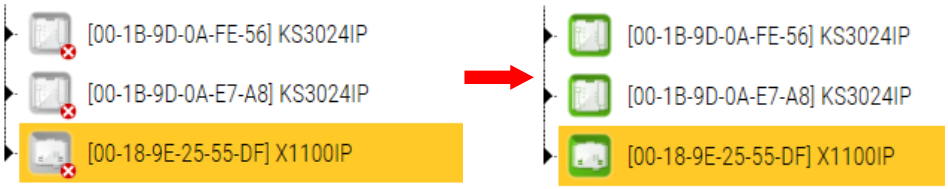
Seria 3000



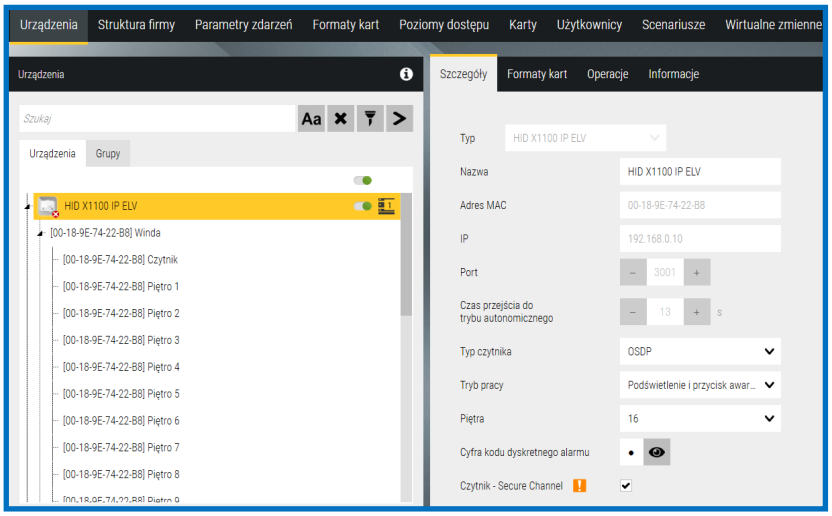
W przypadku kontrolera KDH-KS3000-IP-ELV można również dodać moduły rozszerzające. Do wyboru mamy dwa typy modułów. W zależności od ilości pięter jakie ma obsłużyć winda mamy następujące kombinacje.



Po wykonaniu wszystkich ustawień dla każdego z kontrolerów (analogicznie jak w przypadku dodawania kontrolerów w trybie off-line), należy kliknąć na ikonie ***dyskietki*** w prawym dolnym rogu okna ***Konfiguracja*** w celu dokonania zapisu do bazy. Podczas tego procesu w oknie logów systemowych pojawi się seria komunikatów informujących o pozytywnym zakończeniu zapisu. Ikony ***kontrolerów*** zmienią się na zielone co pokazuje prawidłową komunikację:



Seria HID®Aero®



Nazwa - edytowalne pole na wpisanie nazwy windy w miejsce nazwy domyślnej.

Typ czytnika - OSDP lub Wiegand w zależności od sposobu komunikacji pomiędzy kontrolerem a czytnikami.

Tryb pracy:

- Podświetlenie
- Podświetlenie i przycisk awaryjny
- Podświetlenie z wyborem piętra
- Podświetlenie z wyborem piętra i przyciskiem awaryjnym

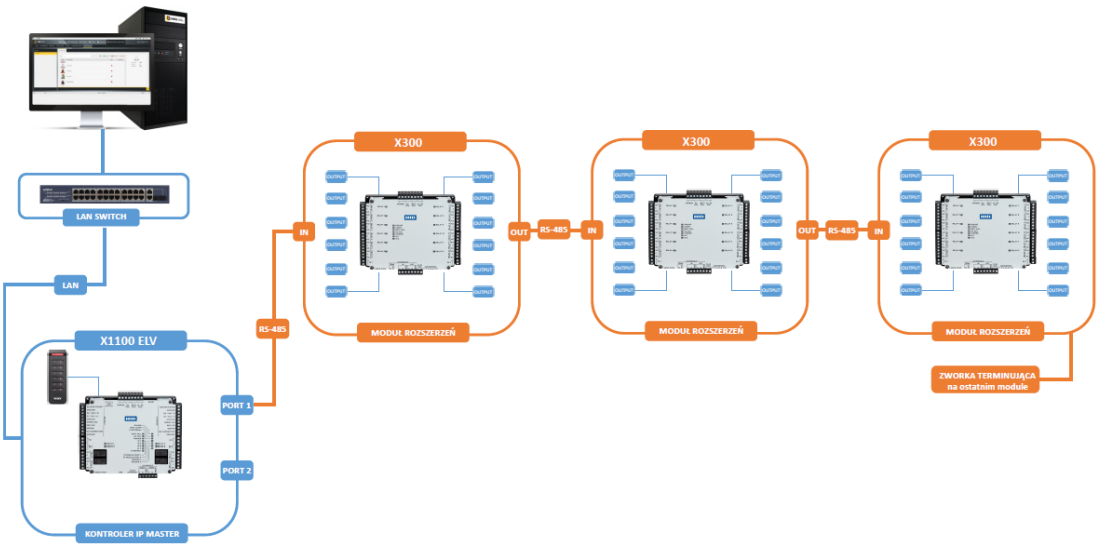
Piętra - wybór od 1 do 128 pięter na jednej magistrali z wykorzystanie modułów rozszerzeń X300 i X200

Po wybraniu odpowiedniej ilości pięter, moduły rozszerzeń zostaną dodane automatycznie z kolejnymi adresami dla RS-485 zaczynając od 0

Cyfra dyskretnego alarmu - wybór od 0 do 9 ustawienia kodu dyskretnego alamu

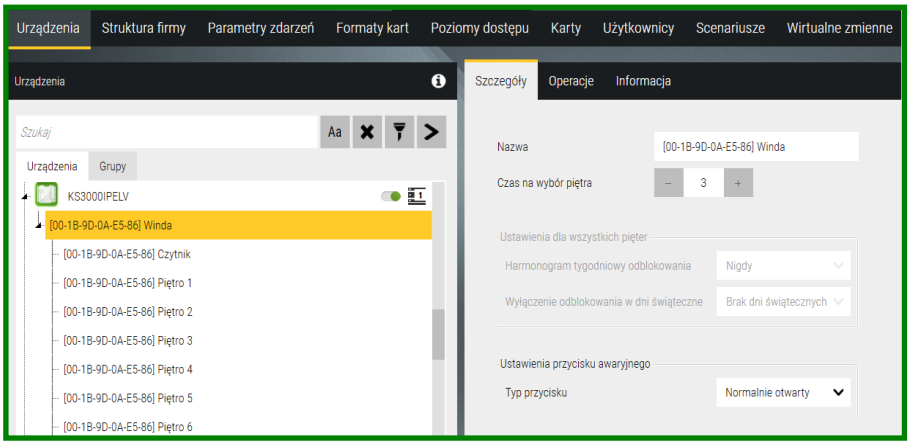
Czytnik Secure Channel - Włączenie szyfrowania AES-128 pomiędzy kontrolerem a czytnikami - **tylko dla OSDP!**

Obsługa do maksymalnie 128 pięter lub szafek przy użyciu kontrolera X1100 i modułów rozszerzeń X300 na jednej magistrali RS-485.



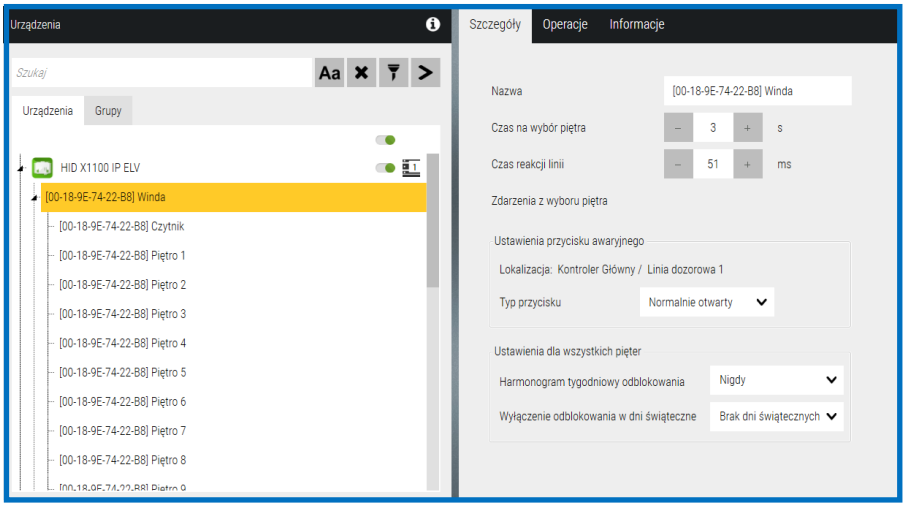
3.7 Urządzenia - Kontrola dostępu - Kontroler windowy - Winda

Seria 3000



Nazwa - edytowalne pole na wpisanie nazwy windy w miejsce nazwy domyślnej.
Czas na wybór piętra - 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***

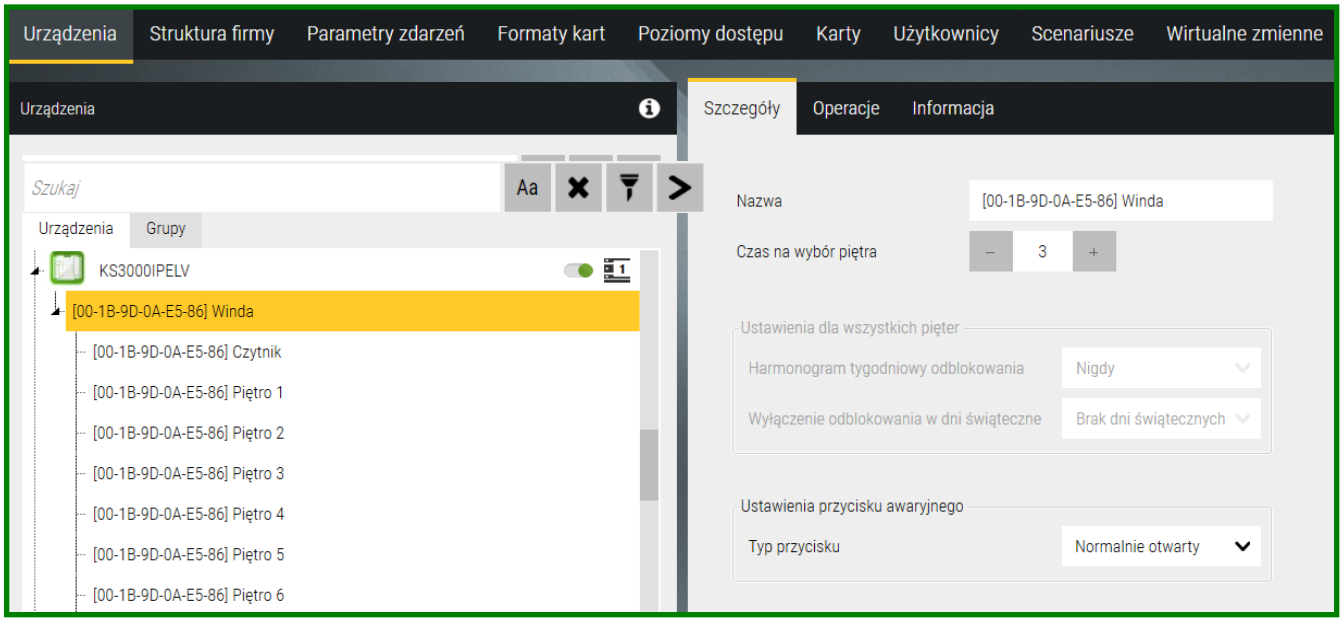
Seria HID®Aero®



Nazwa - edytowalne pole na wpisanie nazwy windy w miejsce nazwy domyślnej
Czas na wybór piętra - ustawienie czasu na wybór piętra po odczycie ważnej karty
Czas reakcji linii - ustawienie dla czasu reakcji przycisku potwierdzenia wyboru piętra 0-255
Typ przycisku - ustawienie trybu pracy przycisku awaryjnego **NO/NC**
Harmonogram tygodniowy odblokowania - pole wyboru harmonogramu automatycznego odblokowania pięter
Wyłączenie odblokowania w dni świąteczne - pole wyboru dni świątecznych wyłączających działanie tygodniowego harmonogramu odblokowania

3.8 Urządzenia - Kontrola dostępu - Kontroler windowy - Winda - Czytnik

Seria 3000



Nazwa - edytowalne pole na wpisanie nazwy czytnika w miejsce nazwy domyślnej.

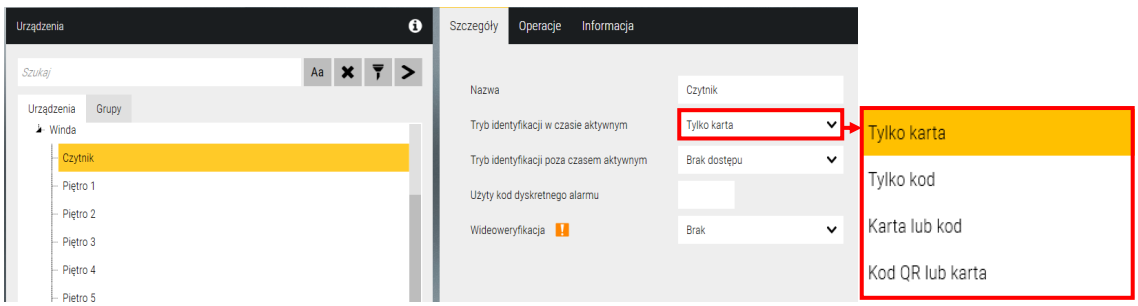
Tryb identyfikacji w czasie aktywnym - z rozwijanej listy można wybrać:

Tryb identyfikacji poza czasem aktywnym - z rozwijanej listy można wybrać:

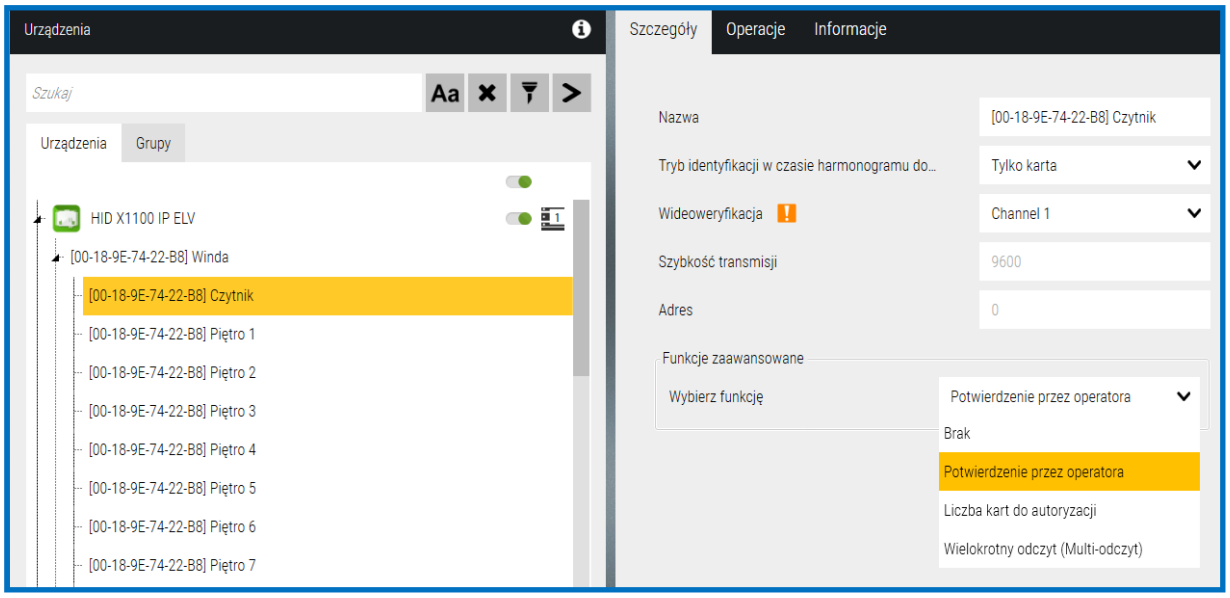
(ten tryb dotyczy okresu poza godzinami pracy, w weekendy i święta)

Użyty kod dyskretnego alarmu - pole na wpisanie kodu dostępu, którego należy użyć na klawiaturze czytnika w przypadku wejścia pod przymusem. Powoduje on wygenerowanie dyskretnego alarmu na stacji operatora.

Wideoweryfikacja - umożliwia przypisanie do czytnika zainstalowanej nad nim kamery do rejestracji stopklatki w chwili odczytu karty



Seria HID®Aero®



Nazwa - edytowalne pole na wpisanie nazwy czytnika w miejsce nazwy domyślnej.

Tryb identyfikacji w czasie harmonogramu dostępu:

- Tylko karta
- Karta i kod
- Tylko kod lokalizacji

Wideoweryfikacja - umożliwia przypisanie do czytnika zainstalowanej nad nim kamery

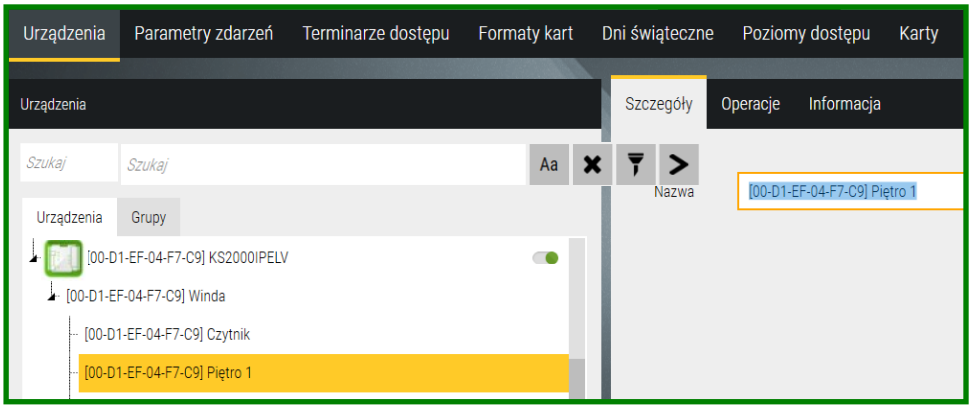
Szybkość transmisji i Adres - Ustawienia wymagane przy konfiguracji czytników - **tylko dla czytników OSDP**

Funkcje zaawansowane:

- Potwierdzenie przez operatora
- Liczba kart do autoryzacji
- Wielokrotny odczyt

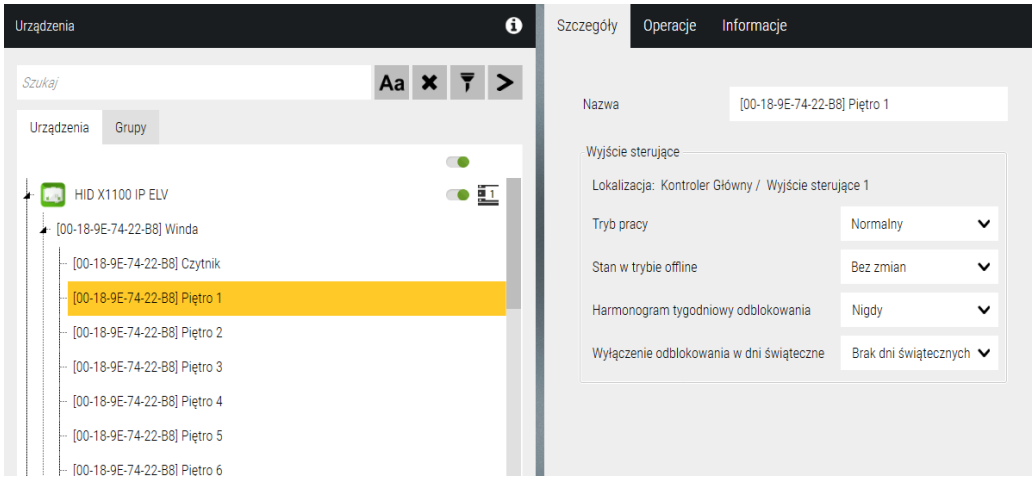
3.9 Urządzenia - Kontrola dostępu - Kontroler windowy - Winda - Piętro

Seria 3000



Nazwa - edytowalne pole na wpisanie nazwy piętra w miejsce nazwy domyślnej.

Seria HID®Aero®



Nazwa - edytowalne pole na wpisanie nazwy piętra w miejsce nazwy domyślnej
Tryb pracy - Tryb pracy przekaźnika Normalny (**NC**) i Odwrócony (**NO**)
Stan w trybie offline*- Bez zmian, Aktywny, Nieaktywny
Harmonogram tygodniowy odblokowania - wybór harmonogramu do automatycznego odblokowania piętra
Wyłączenie odblokowania w dni świąteczne - wybór dni świątecznych dla harmonogramu tygodniowego odblokowania

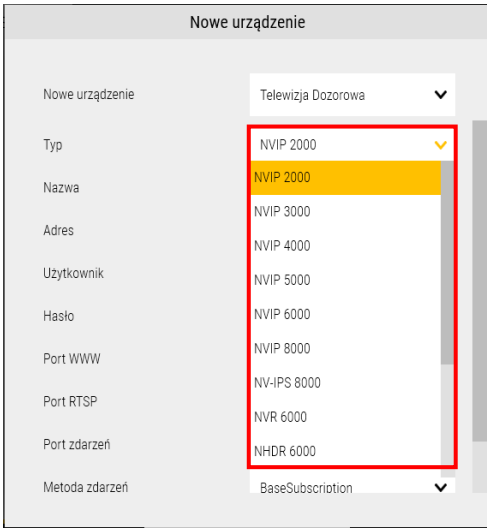
* w przygotowaniu

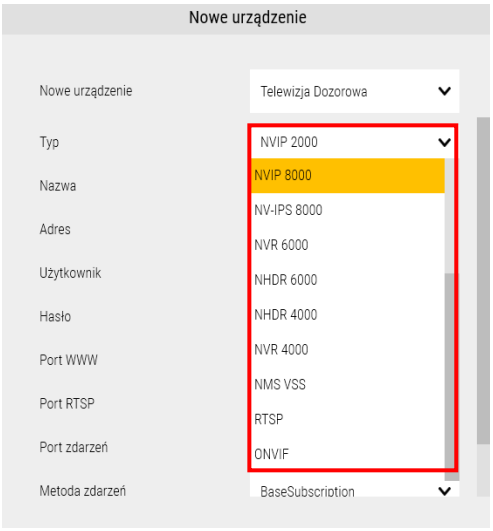
3.10 Urządzenia - Telewizja dozorowa

Program NOVUS MANAGEMENT SYSTEM AC umożliwia integrację z systemem telewizji dozorowej. Na obecnym etapie funkcjonalność ta obejmuje m.in. następujące opcje:

- podgląd obrazu na żywo, odtwarzanie oraz pobieranie nagrań
- definiowanie zaawansowanych widoków wideo
- obsługę do 6 monitorów w rozdzielczości 4K
- wsparcie dla dwustrumieniowości
- wyświetlania obrazu na żywo z wybranej kamery po kliknięciu na ikonie umieszczonej na panelu
- automatycznego wyświetlania takiego obrazu po wystąpieniu określonego zdarzenia (np. sforsowania drzwi, odczytu karty) jako wynik wykonania scenariusza
- przypisanie kamery do czytnika - wideo-weryfikacja
- sterowanie kamerami PTZ
- wsparcie dla kamer fisheye
- odbieranie zdarzeń alarmowych/analizy obrazu
- sterowanie wyjściami alarmowymi
- łączenie urządzeń telewizji dozorowej na żądanie
- możliwość obsługi urządzeń jednostrumieniowych telewizji dozorowej

Lista urządzeń telewizji dozorowej, które można skomunikować z programem NOVUS MANAGEMENT SYSTEM AC:





Główne pozycje na liście to urządzenia marki NOVUS (rejestrator i serie kamer IP), ale możliwa jest również integracja z urządzeniami wykorzystując protokoły RTSP i ONVIF.

Urządzenia telewizji dozorowej można dodawać ręcznie korzystając z opcji *Nowe urządzenie - Telewizja dozorowa,* wyświetli się okno jak na następnej stronie. Można również skorzystać z automatycznej wyszukiwarki, która wyszukuje kontrolery i kamery, sortuje i pozwala przypisać właściwe adresy.

Typ - w pierwszej kolejności należy wybrać typ urządzenia wideo rozwijając listę jak powyżej.

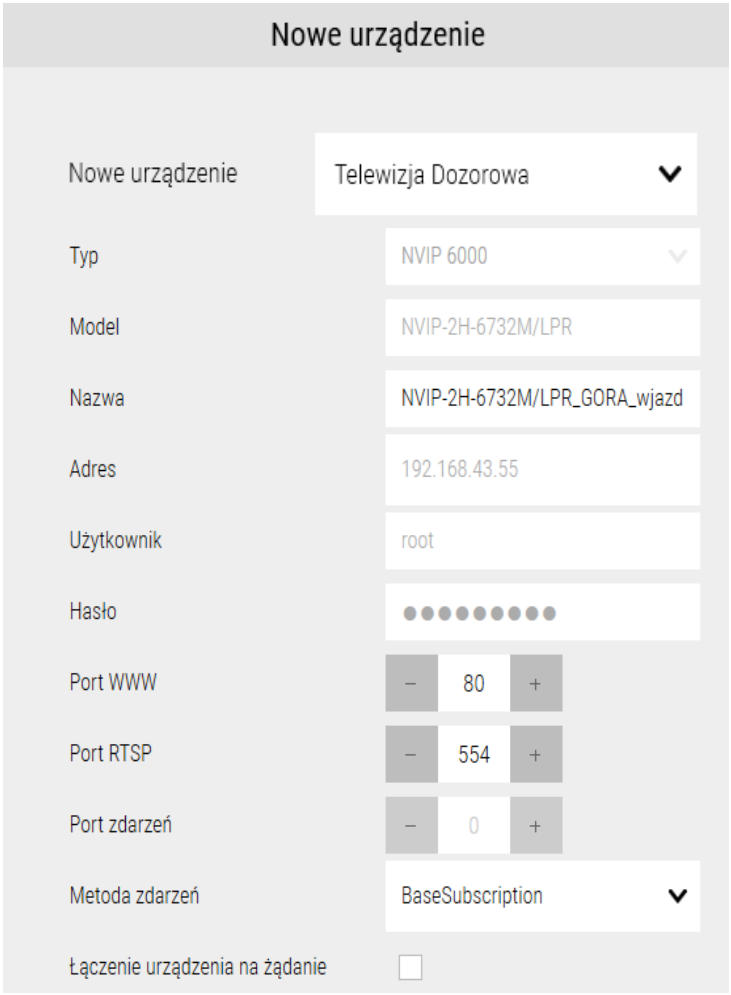
Nazwa - edytowalne pole na wpisanie nazwy urządzenia wideo w miejsce nazwy domyślnej, jeżeli chcemy mieć własną nazwę. Pole to zostanie wypełnione automatycznie po połączeniu z urządzeniem.

Adres IP - pole na wpisanie adresu IP kamery zgodnego z ustawieniami w kamerze

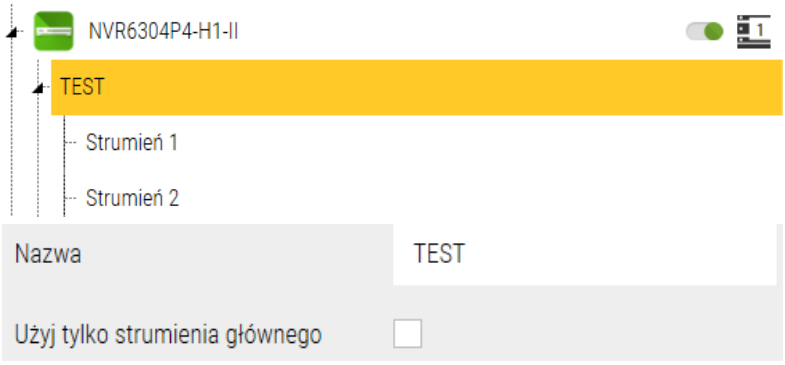
Port www - pole na wpisanie numeru portu zgodnego z ustawieniami w kamerze

Port RTSP - pole na wpisanie numeru portu zgodnego z ustawieniami w urządzeniu wideo

Port zdarzeń - pole na wpisanie numeru portu zgodnego z ustawieniami w urządzeniu wideo

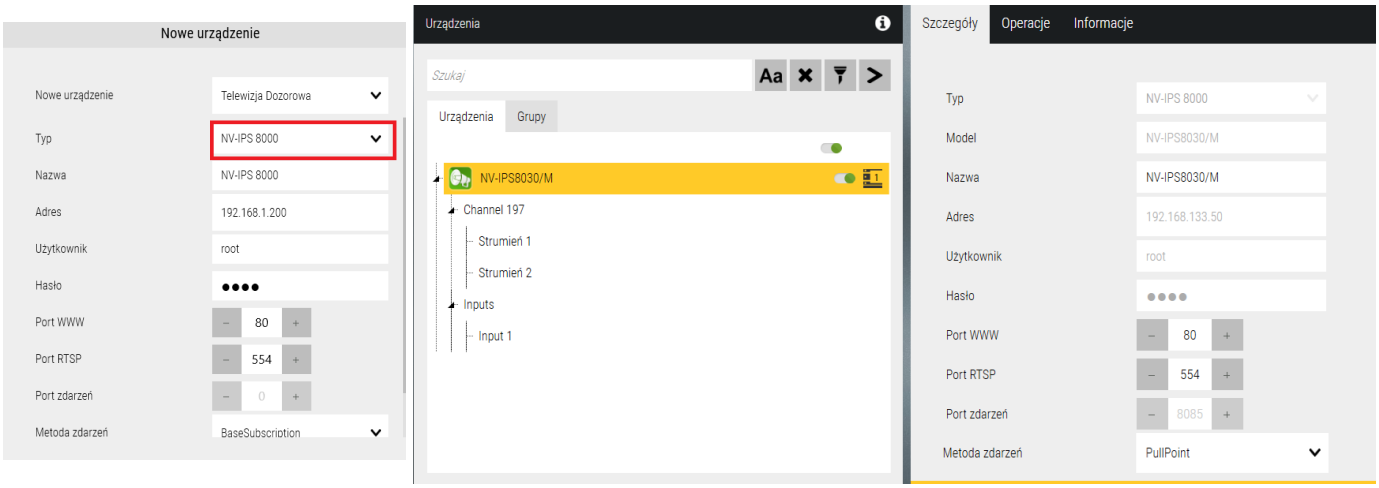


Użytkownik - edytowalne pole na wpisanie nazwy użytkownika zgodnego z ustawieniami w urządzeniu wideo.
Hasło - edytowalne pole na wpisanie hasła użytkownika zgodnego z ustawieniami w urządzeniu wideo.
Łączenie urządzenia na żądanie - opcja umożliwiająca nawiązanie połączenia z urządzeniem podczas wyświetlania obrazu z danego urządzenia, natomiast gdy opcja jest odznaczona użytkownik musi ręcznie nawiązać połączenie z urządzeniem.
Po ustawieniu wymaganych parametrów kliknąć na przycisk ***OK***, a po powrocie do okna ***Urządzenia*** zapisać klikając na dyskietę w prawym dolnym rogu okna ***Konfiguracja***. W oknie logów systemowych pojawi się seria komunikatów informujących o zapisie ustawień do bazy. Następnie po połączeniu z urządzeniem ikona zmieni kolor na zielony.
Do uzyskania funkcjonalności wyświetlenia obrazu po kliknięciu na ikonę na panelu należy wykorzystać kanały urządzenia (domyślna nazwa *Channel X*). Aby skorzystać ze wsparcia tylko dla strumienia głównego, co umożliwia m. in. obsługę funkcji dwukierunkowej komunikacji audio dla głośników Zenitel ELSII-10LHM, zaznacz opcję *Użyj tylko strumienia głównego*.

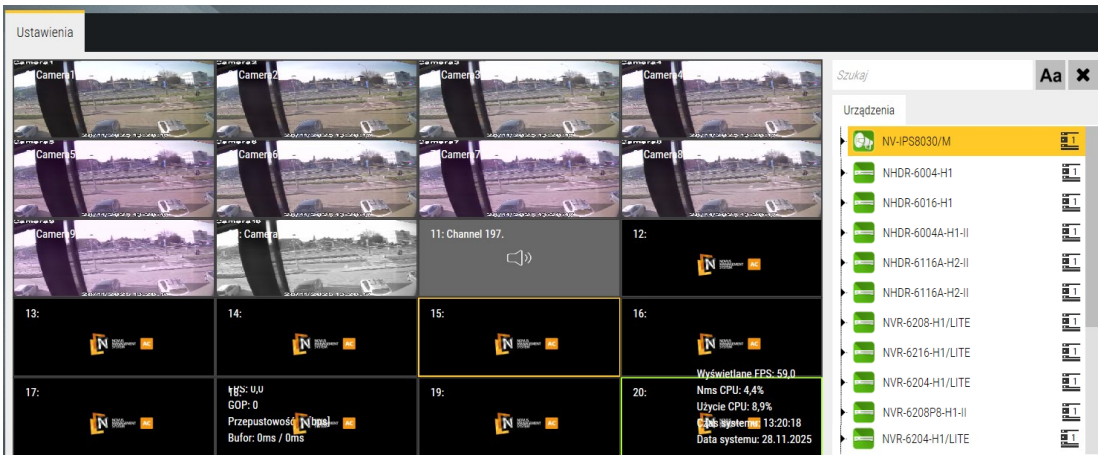


3.11 Urządzenia - Głośniki IP

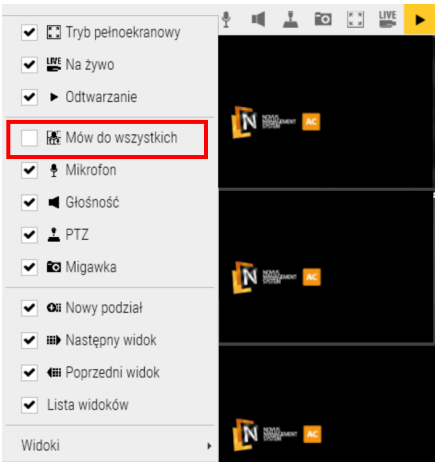
Oprogramowanie NOVUS MANAGEMENT SYSTEM AC umożliwia korzystanie z głośników IP. Głośniki IP zapewniają dwukierunkową komunikację audio oraz odtwarzanie komunikatów głosowych. Wygłoszenie komunikatów można zaplanować poprzez utworzenie odpowiedniego scenariusza.



Na początku należy dodać ręcznie głośnik IP z typem: **NV-IPS 8000.** Następnie należy dodać głośniki do widoku *Wideo* zawierającego kanały kamer lub rejestratorów poprzez przeciągnięcie ikonki głośnika IP w zakładce *Szablony/ Widoki wideo* lub za pomocą narzędzia *Drzewo urządzeń* na panelu.

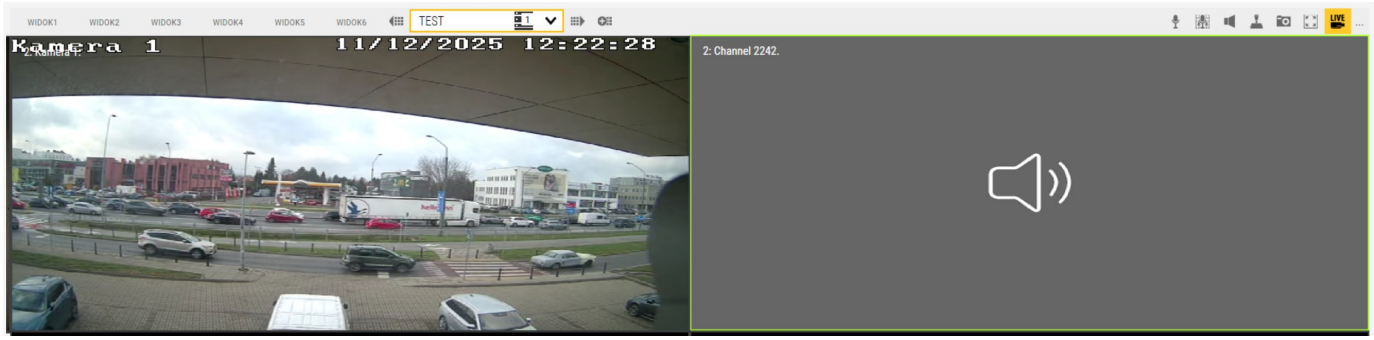


Aby korzystać ze wszystkich funkcji głośnika, należy dodać nową ikonę do narzędzia *Wideo* znajdującego się na panelu. Opcja *Mów do wszystkich* jest domyślnie ukryta. Aby ją włączyć, należy prawym przyciskiem myszy kliknąć górny pasek narzędzi *Wideo*, a następnie zaznaczyć odpowiedni checkbox.



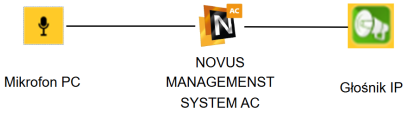
Tryby pracy głośnika

Aby aktywować wybrany tryb pracy należy zaznaczyć odpowiedni kanał z głośnikiem IP dodany do *Widoku Wideo*. Zaznaczony kanał jest oznaczony zielonym obramowaniem.

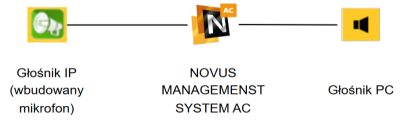


Tryby pracy:

Mikrofon (nadawanie audio) - umożliwia przesyłanie dźwięku z mikrofonu użytkownika (np. podłączonego do komputera) do głośnika IP powiązanego z wybranym kanałem wideo.



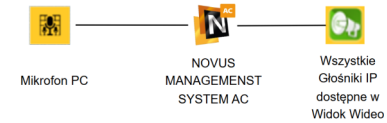
Głośnik (odsłuch audio) - umożliwia odsłuch dźwięku z głośnika IP (nadawanie dźwięku poprzez wbudowany mikrofon) do zewnętrznego głośnika (podłączony do komputera).

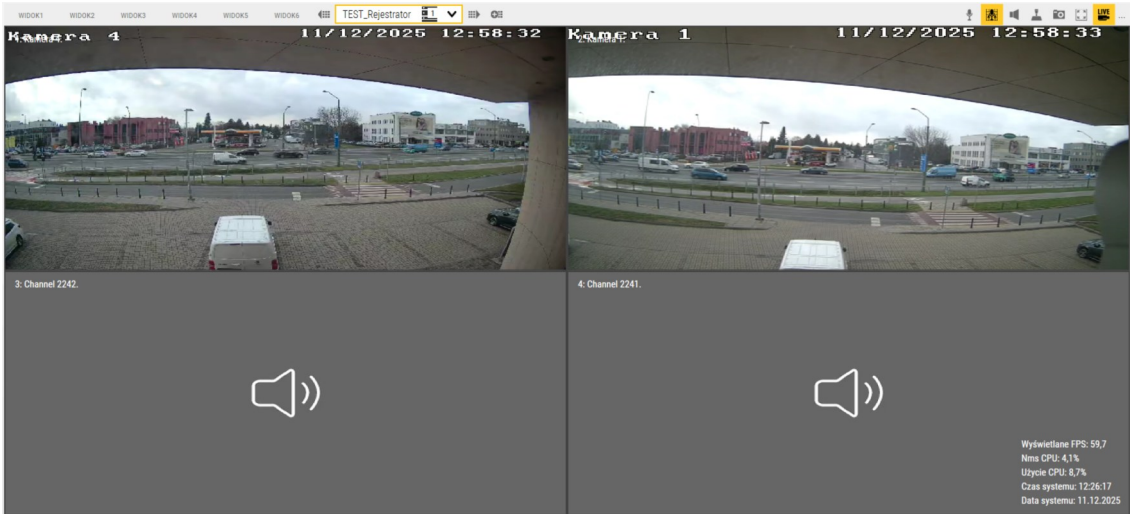


Mikrofon + głośnik (nadawanie i odsłuch audio) - tryb umożliwia dwukierunkową komunikacje audio. Poprzez nadawanie dźwięku z zewnętrznego mikrofonu podłączonego do komputera, na którym działa NOVUS MANAGEMENT SYSTEM AC, pozwala na odsłuch dźwięku z głośnika IP. Umożliwia również nadawanie dźwięku poprzez wbudowany mikrofon w głośniku IP oraz odsłuch tego dźwięku w głośniku podłączonym do komputera.

Mów do wszystkich

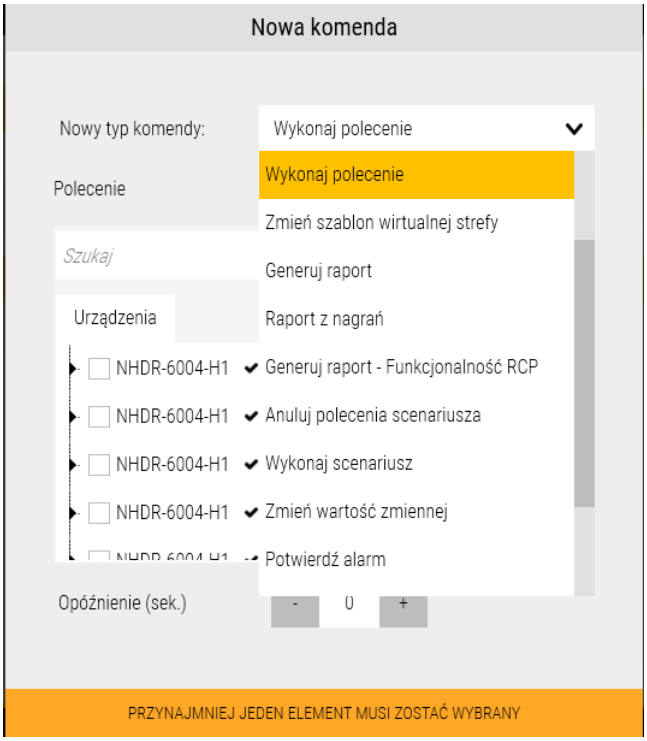
Ta funkcja umożliwia nadawanie dźwięku z mikrofonu użytkownika do wszystkich głośników IP dodanych do tego samego *Widoku Wideo*. Dzięki temu możliwe jest sprawne przekazanie komunikatu do wielu urządzeń jednocześnie.



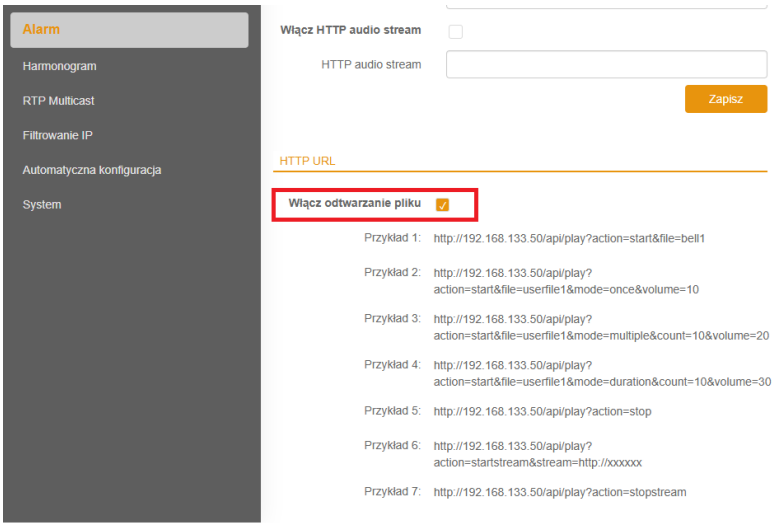


Wygłoszenie komunikatu za pomocą scenariusza

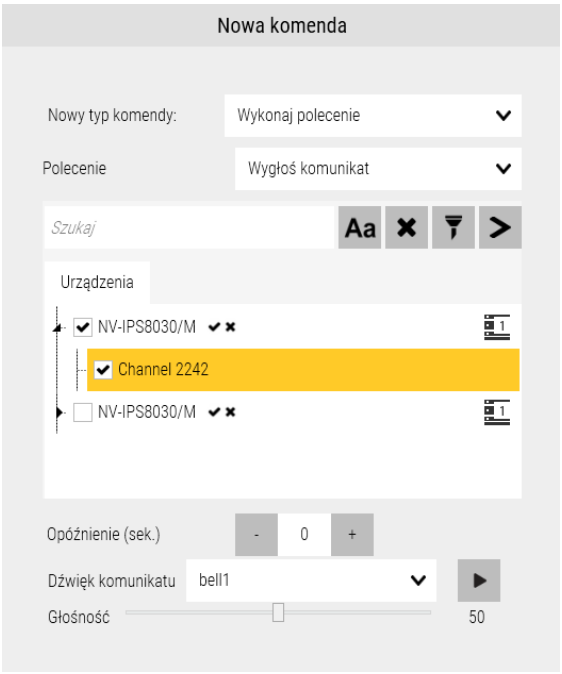
Aby zdefiniować scenariusz polegający na wygłoszeniu komunikatu, należy utworzyć nowy scenariusz. W sekcji *Warunki* należy ustawić odpowiednie parametry, np. naciśnięcie przycisku lub wykrycie zdarzenia z kamery (np. przekroczenie linii), zgodnie z własnymi wymaganiami. Następnie w sekcji *Reakcje* należy wybrać typ komendy *Wykonaj polecenie*, a jako rodzaj polecenia wskazać *Wygłoś komunikat*.



UWAGA! Aby możliwe było sterowanie komunikatami głośnika IP w programie NOVUS MANAGEMENT SYSTEM AC, należy zalogować się do głośnika IP, wpisując jego adres IP w przeglądarce internetowej. Następnie w ustawieniach należy przejść do zakładki *Alarm* oraz zaznaczyć opcję *Włącz odtwarzanie pliku*, która domyślnie jest wyłączona w konfiguracji fabrycznej.



Następnie należy ustawić głośność, opóźnienie komunikatu oraz wybrać odpowiedni dźwięk. Dużą zaletą tej funkcji jest możliwość odtworzenia dźwięku już na etapie konfiguracji scenariusza, co pozwala na sprawdzenie poprawności wybranego komunikatu oraz ustawionego poziomu głośności.



Hierarchia priorytetów zdarzeń (od najwyższego)

1. Alarm
2. Komunikat
3. Nadawanie dźwięku przez użytkownika (np. poprzez mikrofon zewnętrzny)

Zachowanie systemu

- Komunikat ma wyższy priorytet niż nadawanie dźwięku przez użytkownika - podczas jego odtwarzania dźwięk z mikrofonu nie jest słyszalny, a użytkownik nie może go zagłuszyć, niezależnie od momentu rozpoczęcia nadawania.
- Alarm ma najwyższy priorytet w systemie - w chwili jego aktywacji przerywane są zarówno komunikaty, jak i nadawanie użytkownika, a odtwarzany jest wyłącznie dźwięk alarmowy.

3.12 Urządzenia - Terminale do Rejestracji Czasu Pracy

UWAGA!

Zmiany w wersji programu 5.00.071 i nowszych.

Od wersji oprogramowania NOVUS MANAGEMENT SYSTEM AC 5.00.071 sposób komunikacji z terminalami rejestracji czasu pracy uległ modyfikacji w stosunku do wersji 5.00.035. Sposób konfiguracji od wersji 5.00.071 jest następujący:

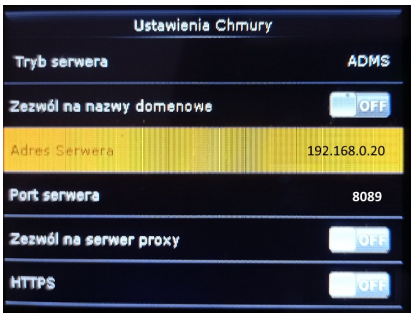
Konfiguracja terminala rejestracji czasu pracy.

Po wejściu do menu opisanym na poprzedniej stronie należy przejść do zakładki *Komunikacja/Ustawienia Chmury.*

Adres serwera - należy ustawić adres IP komputera na którym będzie działać serwer oprogramowania NOVUS MANAGEMENT SYSTEM AC (musi być to adres wybrany w konfiguracji oprogramowania w pozycji *Nasłuchujący adres IP*).

Port serwera - należy ustawić numer portu zgodny z ustawionym numerem portu dla danego terminala na serwerze MANAGEMENT SYSTEM AC. Należy upewnić się, że numer portu nie jest wykorzystywany przez inne urządzenie, oprogramowanie itp.

HTTPS - należy ustawić na *OFF*.



Konfiguracja ustawienia daty/czasu.

Należy wejść do menu *System/Data Czas/Czas letni/zimowy - tryb* i wybrać opcję *Wg daty/godziny*. Następnie należy wejść do menu *System/Data Czas/Czas letni/zimowy - konfig* i zdefiniować datę oraz czas początku oraz końca zmiany czasu. Standardowo jest to ostania niedziela października o godzinie 3:00 oraz ostatnia niedziela marca o godzinie 2:00.

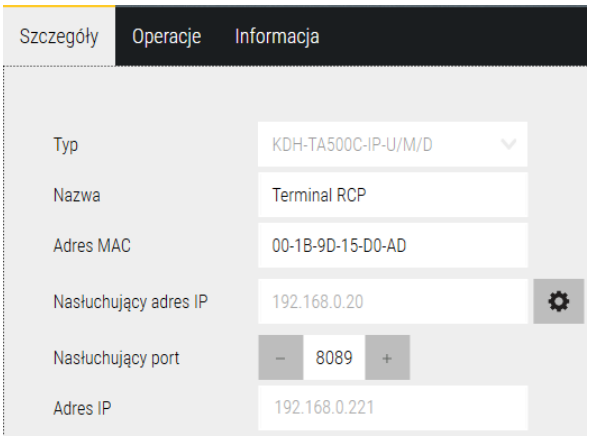
Ustawienia adresu IP terminala

W przypadku wersji 5.00.071 i nowszych korzystanie z trybu DHCP nie jest zalecane.

Konfiguracja oprogramowania NOVUS MANAGEMENT SYSTEM AC.

Nasłuchujący adres IP - po wybraniu opcji ⚙ należy wybrać z listy adres IP komputera, który wykorzystywany będzie do komunikacji z terminalem rejestracji czasu pracy (musi to być ten sam adres, który został zdefiniowany w terminalu w pozycji *Ustawienia Chmury/Adres Serwera*).

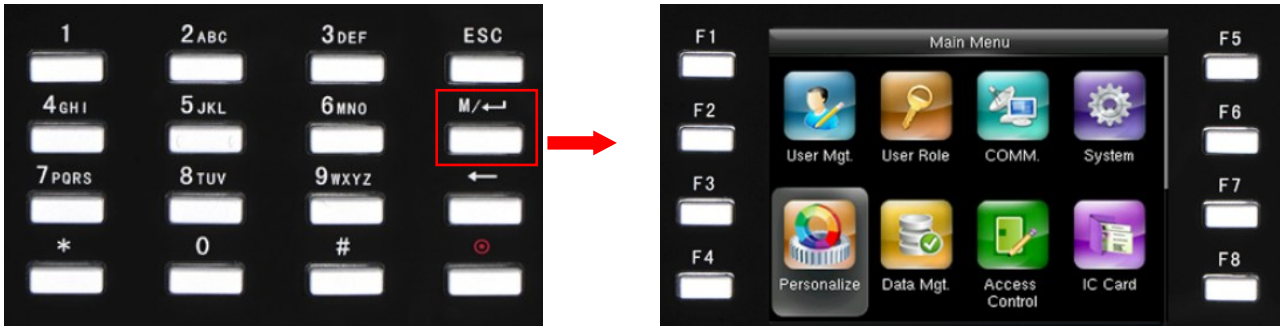
Nasłuchujący port - należy wpisać numer portu, który wykorzystywany będzie do komunikacji z terminalem rejestracji czasu pracy (musi to być ten sam numer portu, który został zdefiniowany w terminalu w pozycji *Ustawienia Chmury/Port Serwera*).



W przypadku aktualizacji z wersji 5.00.035 do wersji 5.00.071 po zakończeniu procesu konfiguracji, **należy wykonać operację inicjalizacji terminala** (w menu *Konfiguracja/Urządzenia* należy wybrać terminal z listy, a następnie z menu *Operacje* opcję *Inicjalizacja*). Należy mieć na uwadze, że spowoduje to usunięcie wszystkich zdarzeń zapisanych w pamięci terminala.

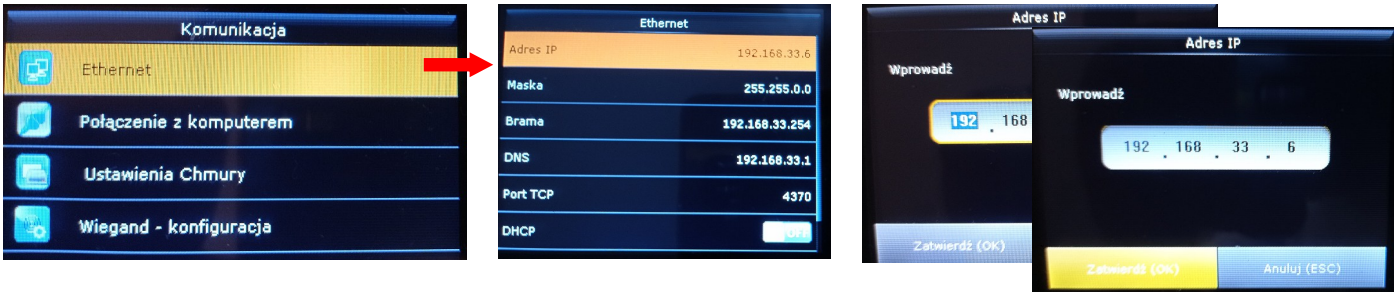
Pozostałe informacje dotyczące konfiguracji terminali rejestracji czasu pracy znajdują się w dalszej części instrukcji.

Program NOVUS MANAGEMENT SYSTEM AC umożliwia integrację z system rejestracji czasu pracy i obecności. Od wersji 4.02.XX i wyższych funkcje te można realizować we współpracy z terminalami RCP typu KDH-TA500C-IP-UMD i KDH-TA500CFP-IP-UMD, które oferują rejestrację różnych rodzajów we/wy (normalne, prywatne , służbowe i na przerwę (płatna licencja, trial 60 dni).
Przed połączeniem programu z terminalem należy w jego menu ustawić adres IP, język oraz format daty.
Wejście do menu poprzez klawisz M na klawiaturze. Na tym etapie nie wymaga to hasła.

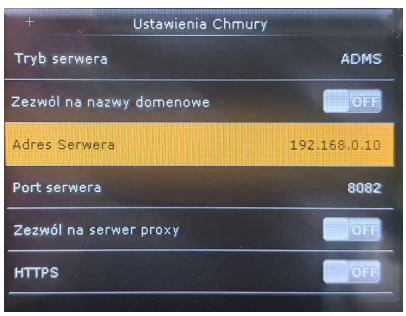


Ustawienie adresu IP

Wybór pozycji kursorami.
(prawy górny róg terminala)

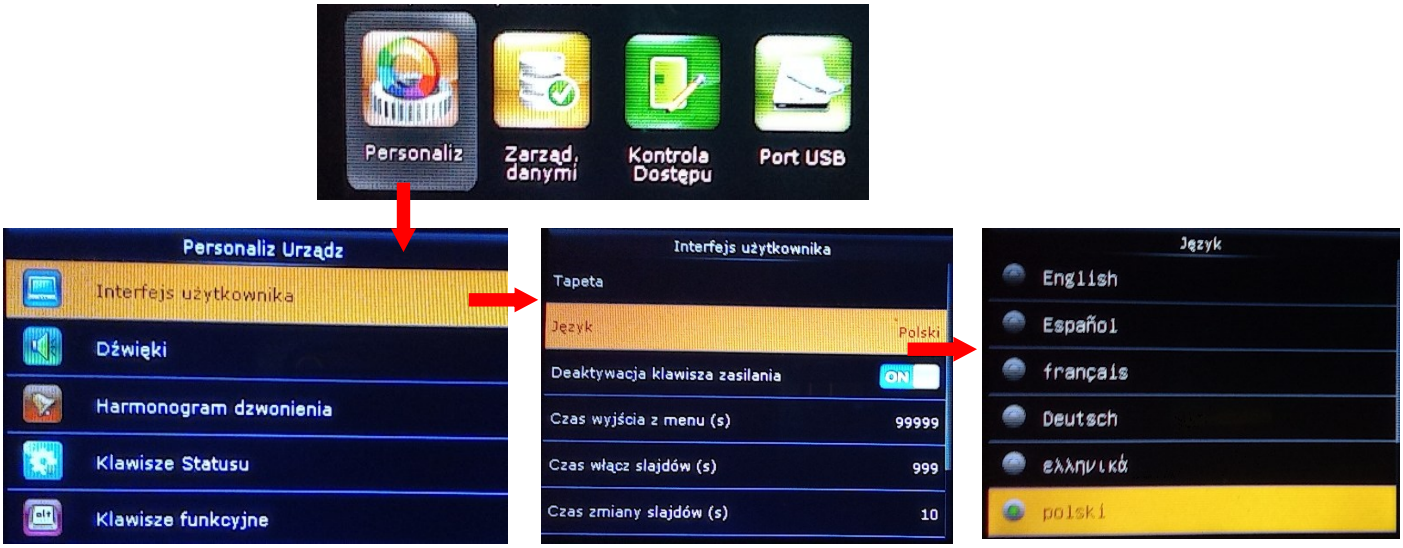


Po kliknięciu na ikonie ***Komunikacja*** należy zaznaczyć poz. *Ethernet* i kliknąć ***OK*** w polu kursorów - prawy górny róg terminala.
Wypełnić pierwsze 4 pola - po wybraniu pola kliknąć ***OK*** i wpisać wartości adresu - port bez zmian.
Jeżeli korzystamy z sieci DHCP to należy tylko wybrać ostatnią pozycję na dole okna i kliknąć ***OK*** (**UWAGA! W przypadku wersji 5.00.071 korzystanie z trybu DHCP nie jest zalecane**). Po restarcie zasilania terminala należy ponownie wejść do tego okna i odczytać przydzielony adres w celu wprowadzenia go w oknie konfiguracji NOVUS MANAGEMENT SYSTEM AC.
Następnie przejść do pozycji *Ustawienia Chmury* i w analogiczny sposób ustawić adres serwera NOVUS MANAGEMENT SYSTEM AC, z którym będzie łączył się terminal. Tylko ta pozycja jest potrzebna do współpracy z NOVUS MANAGEMENT SYSTEM AC.



Przyciskiem ***ESC*** na klawiaturze wychodzimy z menu.

Wybór języka



Po kliknięciu na ikonie ***Personalizacja*** należy zaznaczyć poz. *Interfejs użytkownika,* a w następnym oknie ***Język***.

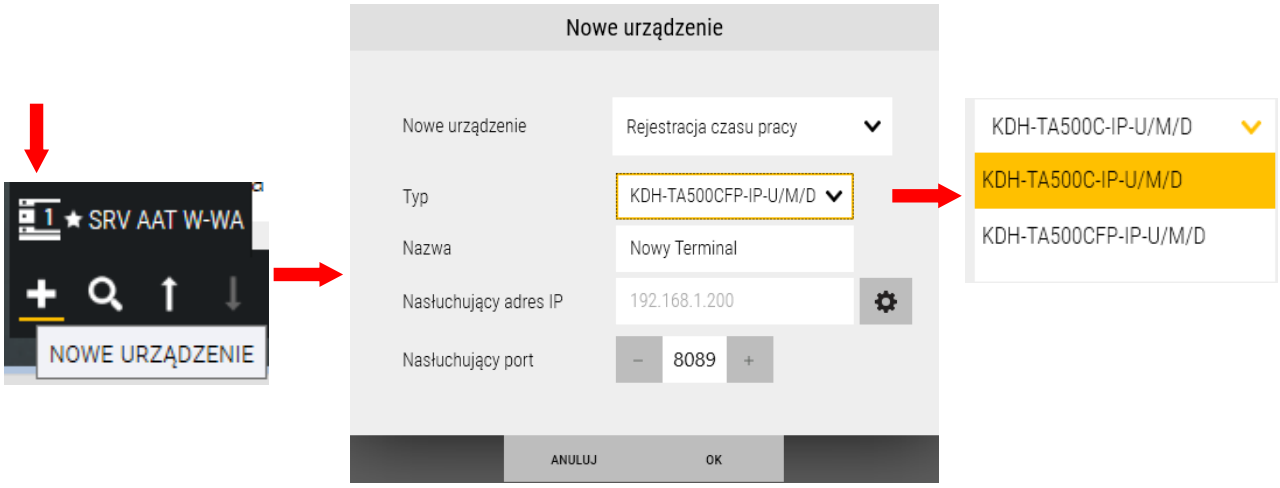
Ustawić język polski i wyjść z menu przyciskiem ***ESC***.

Format daty

Po kliknięciu na ikonie ***System*** należy zaznaczyć poz. *Data Czas,* a w następnym oknie ***Format Daty***.

Ustawić format *DD-MM-RRRR* i wyjść z menu przyciskiem ***ESC***.

Konfiguracja terminala w programie



Terminal należy dodać ręcznie korzystając z opcji *Nowe urządzenie - Rejestracja czasu pracy,* wyświetli się okno jak powyżej.

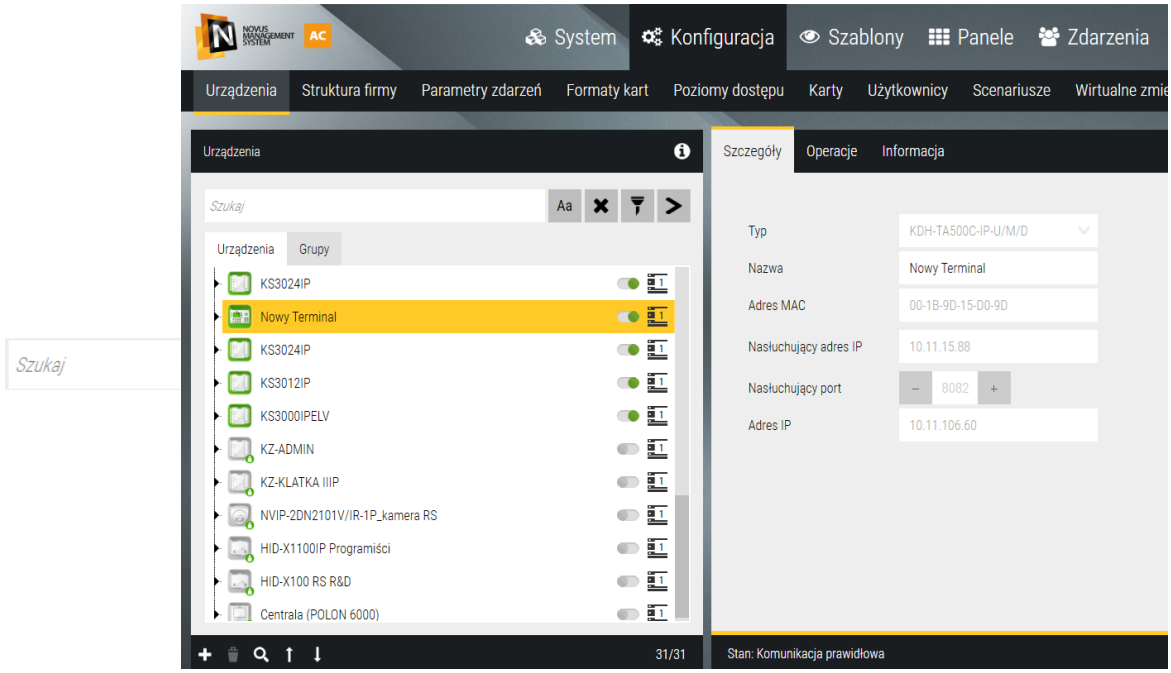
Typ - w pierwszej kolejności należy wybrać typ urządzenia z rozwijanej listę jak powyżej. Do wyboru:
model: KDH-TA500C-IP-UMD lub KDH-TA500CFP-IP-UMD ze skanerem biometrii.

Nazwa - edytowalne pole na wpisanie nazwy urządzenia w miejsce nazwy domyślnej jeżeli chcemy mieć własną nazwę.

Nasłuchujący adres IP - adres serwera ustawiony w terminalu w zakładce *Komunikacja/Ustawienia Chmury*

Nasłuchujący port - numer portu serwera ustawiony w terminalu w zakładce *Komunikacja/Ustawienia Chmury*

Po kliknięciu ***OK*** oraz ***Zapisz*** (w prawym dolnym rogu okna ***Konfiguracji)***, terminal pojawi się na liście urządzeń.



Potwierdzeniem nawiązania komunikacji jest zielony kolor ikony ***terminala*** w lewym oknie.

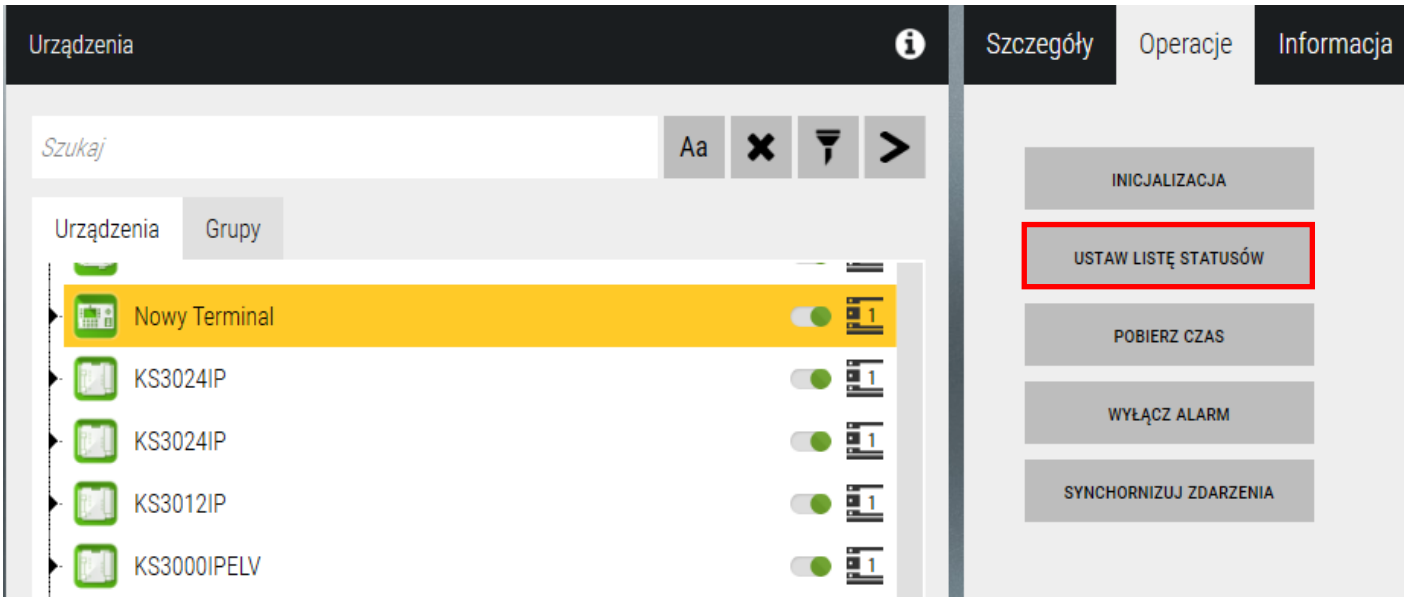
Od tego momentu wejście do menu terminala wymaga użycia hasła administratora.

Domyślny login: Wpisz admin ID - 1 i ***OK***, Weryfikuj hasło: 1 2 3 4 5 6 7 8 i ***OK***

Hasło domyślne należy zmienić po zalogowaniu w menu Zarządz. użytkow. edytując użytkownika Admin.

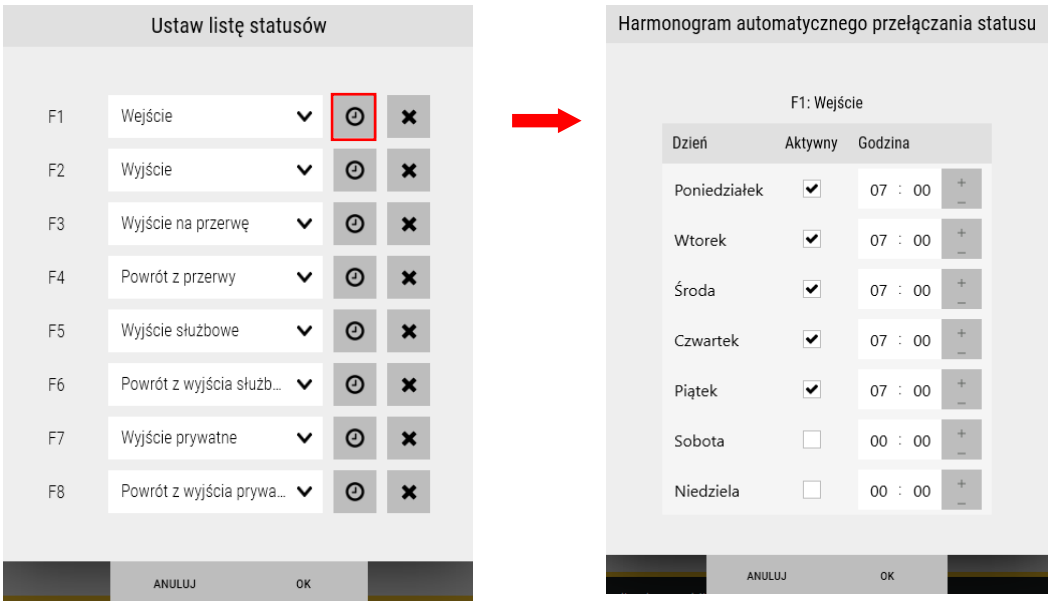
Dodawanie odcisków palców do terminala FP poprzez skaner USB opisane jest w zakładce *Użytkownicy.*

Ustawienie statusów rejestracji we/wy



W zakładce *Operacje* należy kliknąć na przycisku ***Ustaw listę statusów***. Można zostawić ustawienia domyślne lub ustawić własną kolejność wybierając status z rozwijanej listy przy każdym przycisku.

Klikając na ikonie ***zegara*** przy każdym z przycisków można ustawić harmonogram automatycznego przełączania statusu rejestracji dla wybranych dni tygodnia. Po zmianie statusu przez użytkownika na inny domyślny wraca po 5 sek.

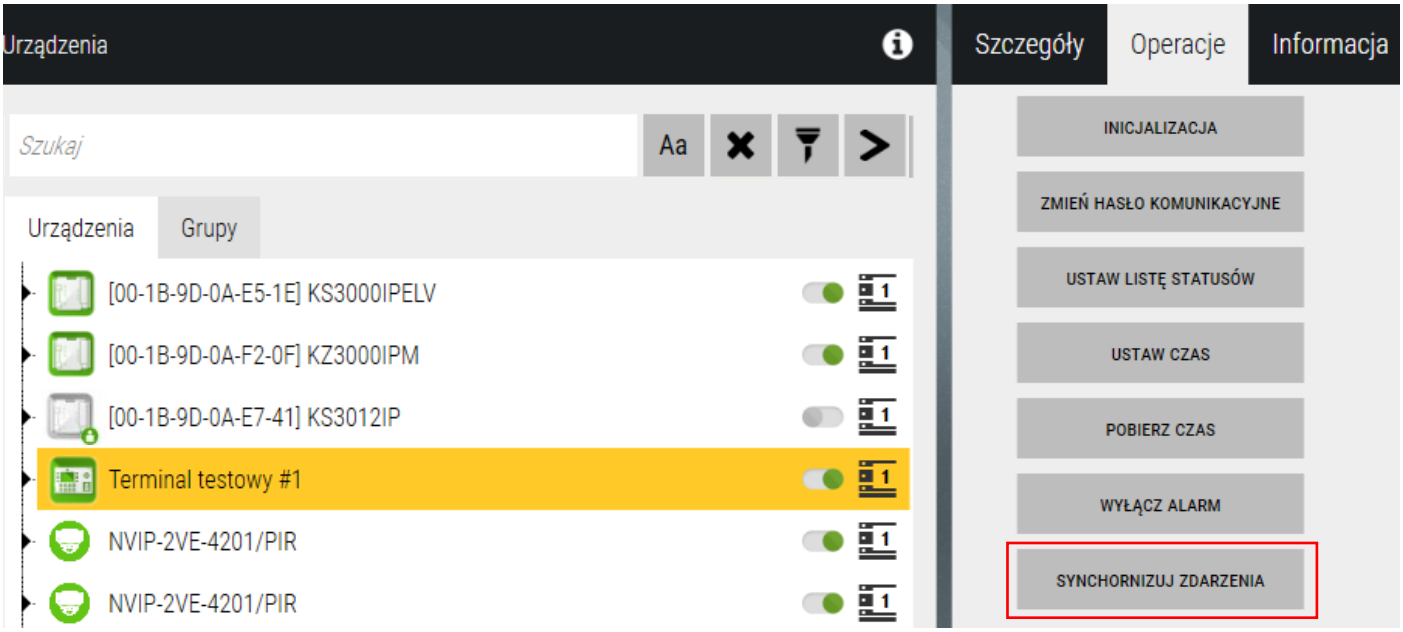


Po wykonaniu ustawień należy potwierdzić ***OK***, a następnie kliknąć przycisk ***Zapisz*** w prawym dolnym rogu okna konfiguracji. Spowoduje to wysłanie prawidłowych opisów statusów rejestracji. Ten proces może trwać do kilku minut. W trakcie tego procesu na wyświetlaczu terminala w polach opisów przycisków pojawi się opis: F1- Przetwarzanie. Dopiero po zakończeniu całego procesu pojawią się wszystkie prawdziwe opisy statusów. Opisy wyświetlane są w języku zalogowanego operatora.

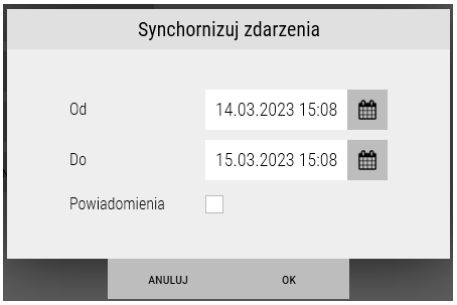
Zakładka *Operacje* udostępnia również inne opcje zgodnie z opisami na przyciskach.
Przycisk ***Wyłącz alarm*** służy do kasowania alarmu wygenerowanego po naruszeniu czujnika antysabotażowego terminala. Kasowanie alarmu możliwe jest również z ikony ***terminala*** na panelu.

Synchronizacja z terminalem

Ta opcja umożliwia pobranie logów z terminala RCP w przypadku gdy z różnych powodów rejestracje we/wy zostały dokonane przez pracowników, ale nie ma ich bazie programu co objawia się brakiem tych zdarzeń w raporcie RCP.



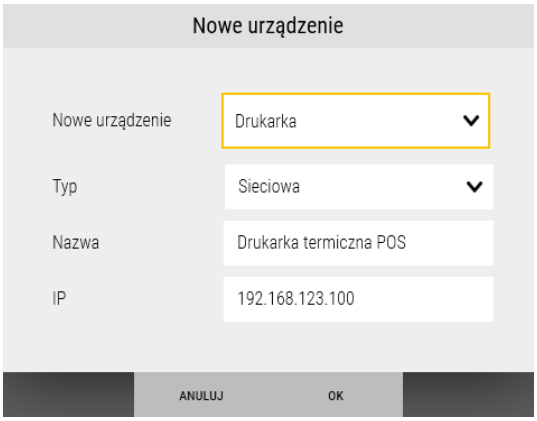
Po kliknięciu na przycisku ***Synchronizuj zdarzenia*** wyświetli się poniższe okno:



Należy wybrać zakres dat i czasu z którego chcemy pobrać zdarzenia. Opcjonalnie można włączyć powiadomienia email, ale jeżeli niepobranych zdarzeń jest dużo to lepiej z tego zrezygnować żeby nie zapełniać skrzynek email pracownikom. Warto je włączyć jeżeli sytuacja dotyczy dnia bieżącego i brak powiadomień z rana. Po kliknięciu ***OK*** na panelu ze stosem zdarzeń pojawi się informacja o ilości pobranych zdarzeń oraz pobrane zdarzenia. W trakcie tej operacji z terminala pobierane są tylko zdarzenia, których brakuje w bazie w podanym okresie czasu.

3.13 Urządzenia - Drukarka biletów

Program NOVUS MANAGEMENT SYSTEM AC umożliwia dodanie drukarki dedykowanej do wydruku biletów z QR-codami dla opcji LPR. Żeby dodać drukarkę należy wybrać jej typ (sieciowa lub lokalna) a następnie odpowiednio wpisać jej adres IP lub wybrać odpowiedni port COM i kliknąć ***Zapisz***.

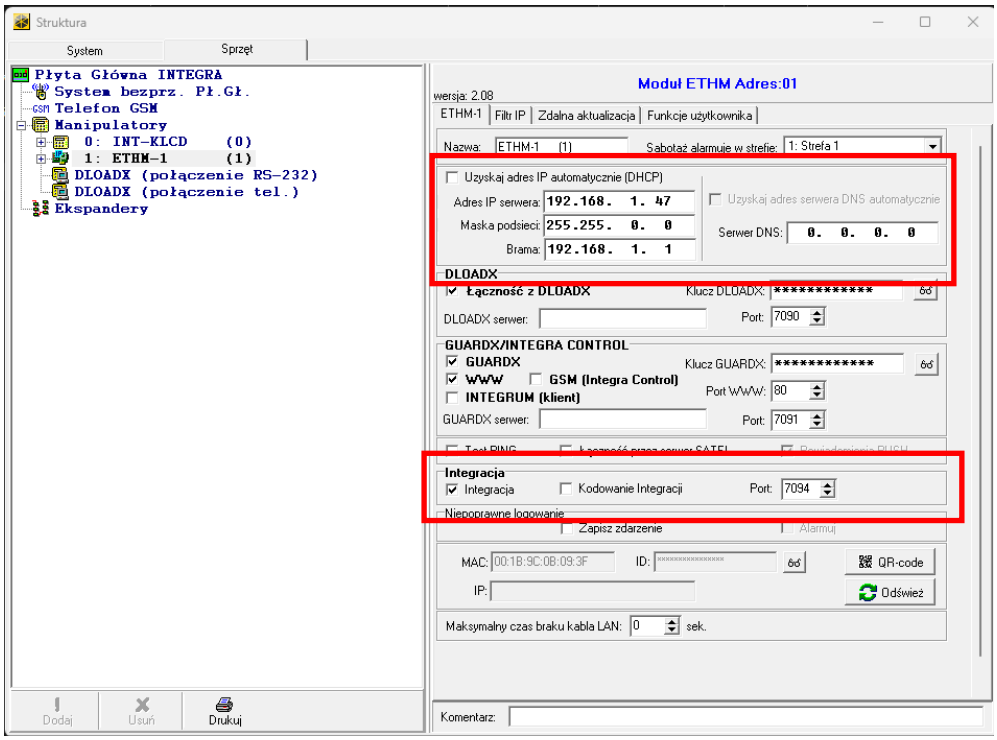


3.14 Urządzenia - System sygnalizacji włamania i napadu

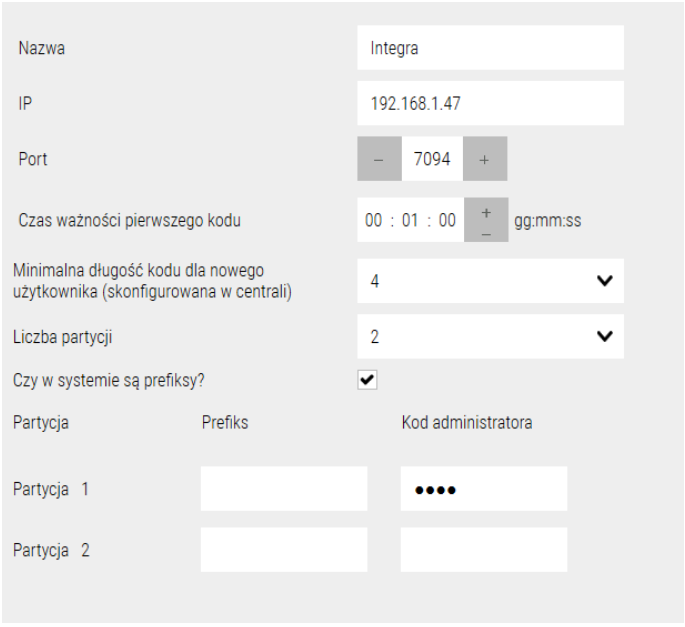
Program NOVUS MANAGEMENT SYSTEM AC w wersji minimum 5, umożliwia integrację z systemem sygnalizacji włamania i napadu.

Z programem NOVUS MANAGEMENT SYSTEM AC można skomunikować centrale alarmowe marki Satel serii Integra poprzez moduł komunikacyjny ETHM-1-PLUS. Aby urządzenia nawiązały prawidłową komunikację centrala alarmowa musi być w wersji minimum 1.19 natomiast moduł ETHM-1-PLUS w wersji minimum 2.07.

Aby nawiązać komunikację z programem NOVUS MANAGEMENT SYSTEM AC należy w ustawieniach modułu ETHM-1-PLUS zaadresować centralę INTEGRA w tym samym segmencie sieci co serwer NOVUS MANAGEMENT SYSTEM AC następnie włączyć opcję *INTEGRACJA* oraz ustawić port integracji zgodnie z instrukcją dla modułu ETHM-1-PLUS. Poniżej przykład z programu DLOADX.



Urządzenia systemów sygnalizacji włamania i napadu można dodawać ręcznie korzystając z opcji *Nowe urządzenie - System alarmowy*. W programie NOVUS MANAGEMENT SYSTEM AC wyświetla się poniższe okno.



Nazwa - edytowalne pole na wpisanie nazwy centrali alarmowej w miejsce nazwy domyślnej.

Adres IP - pole na wpisanie adresu IP centrali alarmowej zgodnego z ustawieniami ETHM-1-PLUS.

Port Integracji - pole na wpisanie numeru portu integracji centrali alarmowej zgodnego z ustawieniami ETHM-1-PLUS.

Czas ważności pierwszego kodu - czas, przez który będzie ważne pierwsze hasło po wprowadzeniu przez NOVUS MANAGEMENT SYSTEM AC. Wprowadzenie drugiego hasła na klawiaturze w tym czasie spowoduje zmianę stanu odpowiednio skonfigurowanej strefy.

Minimalna długość kodu dla nowego użytkownika - minimalna liczba cyfr z których składają się hasła użytkowników zaprogramowana w centrali alarmowej.

Liczba partycji - liczba partycji, którą należy wybrać w celu dodania do NOVUS MANAGEMENT SYSTEM AC. Dla każdej partycji należy podać prefix (o ile występuje) oraz kod administratora partycji.

Czy w systemie są prefiksy? - wybór pola umożliwia wpisanie prefiksu dla każdej partycji jeśli w centrali alarmowej, instalator sprecyzował długość prefiksów następnie zostały one zdefiniowane przez administratora partycji.

Poniżej wymienionych opcji należy wpisać kod administratora oraz prefiks (o ile występuje) dla każdej z zaprogramowanych partycji.

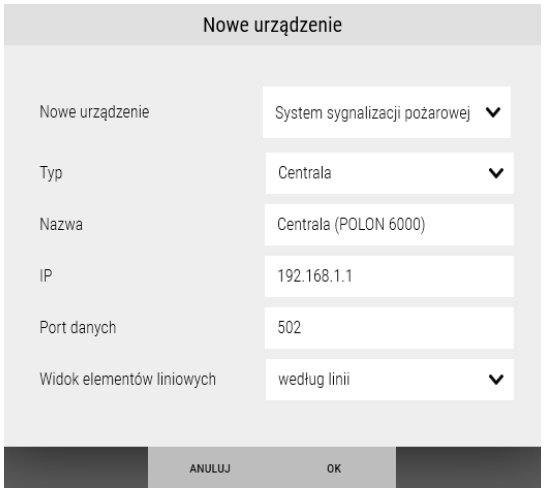
Po ustawieniu wymaganych parametrów kliknąć przycisk ***OK***. Po powrocie do okna ***Urządzenia*** *zapisać ustawienia* klikając na dyskietkę w prawym dolnym rogu okna ***Konfiguracja***. W oknie logów systemowych pojawi się seria komunikatów informujących o zapisie do bazy danych, ikona ***centrali*** zmieni kolor na zielony a program nadzorczy NOVUS MANAGEMENT SYSTEM AC rozpocznie pobieranie konfiguracji centrali alarmowej. Podczas tej czynności zostanie pobrany podział systemu na partycję i strefy oraz lista użytkowników centrali wraz z ich hasłami dostępu.

3.15 Urządzenia - System sygnalizacji pożarowej POLON 6000

Program NOVUS MANAGEMENT SYSTEM AC umożliwia wizualizację z systemu sygnalizacji pożaru Polon 6000 (wymagana wersja oprogramowania **1.016 lub nowsza**). Szczegółowy opis zakresu funkcjonalności został opisany w rozdziale 1.2 niniejszej instrukcji obsługi.

Urządzenia systemu sygnalizacji pożarowej Polon 6000 należy dodawać ręcznie korzystając z opcji *Nowe urządzenie - System sygnalizacji pożarowej,* wyświetli się okno jak powyżej.

Dodawanie centrali Polon 6000



Typ - w pierwszej kolejności należy wybrać typ urządzenia z rozwijanej listy

Nazwa - edytowalne pole na wpisanie nazwy urządzenia w miejsce nazwy domyślnej, jeżeli chcemy mieć własną nazwę

Adres IP - pole na wpisanie adresu IP centrali SSP zgodnego z ustawieniami w centrali SSP

Port danych - pole na wpisanie numeru portu zgodnego z ustawieniami w centrali SSP

Port RTSP - pole na wpisanie numeru portu zgodnego z ustawieniami w urządzeniu wideo

Widok elementów liniowych - z rozwijanej listy należy wybrać sposób wyświetlania elementów liniowych spośród dostępnych *według linii* lub *według stref*

Po skonfigurowaniu w/w elementów kliknąć ***OK***.

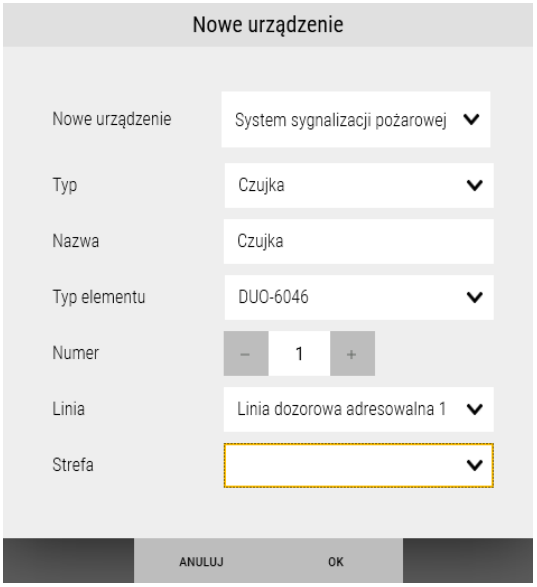
UWAGA! Aby nawiązać połączenie z centralą Polon 6000, należy ją odpowiednio skonfigurować. Opis konfiguracji centrali znajduje się w rozdziale 9.11 niniejszej instrukcji obsługi.

Dodawanie elementów systemu Polon 6000

Istnieją dwa sposoby dodawania elementów systemu Polon 6000:

A) Ręczne dodawanie elementów systemu

Elementy systemu Polon 6000 należy dodawać w sposób analogiczny jak w przypadku dodawania centrali, z tą różnicą, że w pozycji *Typ* należy wybrać odpowiedni typ elementu, który chcemy dodać. Poniżej przedstawiony został sposób dodawania elementu typu *czujka*.



Typ - należy wybrać odpowiedni typ urządzenia, w tym przypadku *czujka*

Nazwa - edytowalne pole na wpisanie nazwy urządzenia w miejsce nazwy domyślnej, jeżeli chcemy mieć własną nazwę

Typ elementu - należy wybrać odpowiedni typ urządzenia, model

Numer - należy wybrać numer elementu na linii

Linia - należy wybrać linię dozorową do której ma zostać przypisany dany element

Strefa - należy wybrać strefę do której ma zostać przypisany dany element

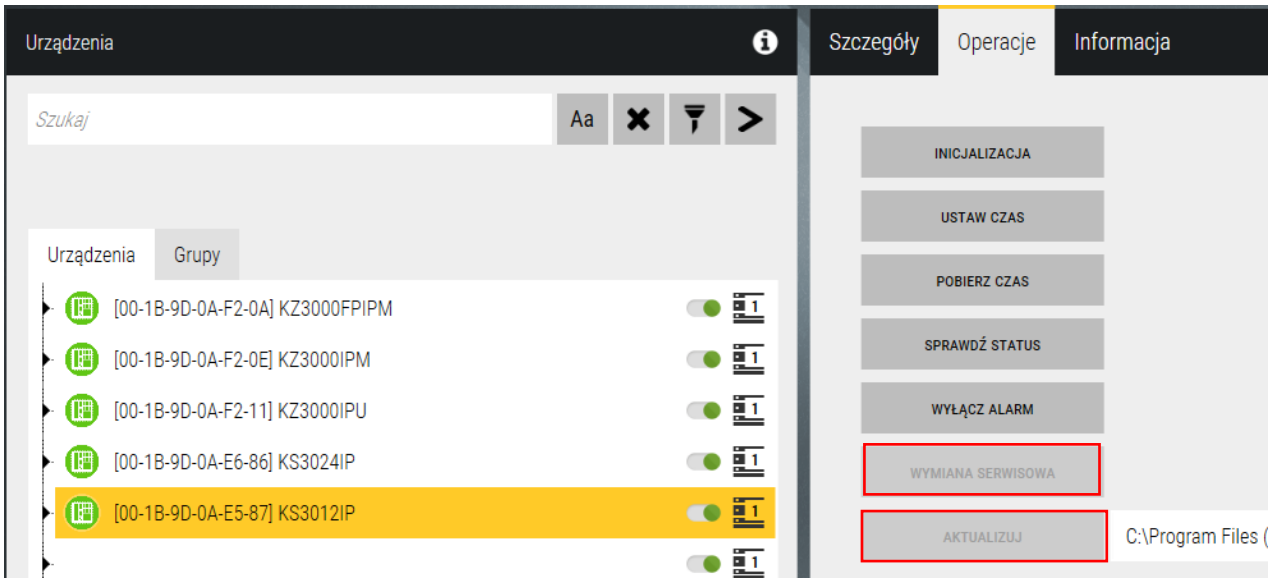
B) Wczytanie konfiguracji wyeksportowanej z centrali

Sposób postępowania został opisany w rozdziale 9.11 niniejszej instrukcji obsługi.

3.16 Urządzenia - Operacje

Pokazane poniżej elementy systemu w zakładce *Operacje* mają komendy dla operatora, które umożliwiają wykonanie określonych operacji jak na listach poniżej.

Kontroler

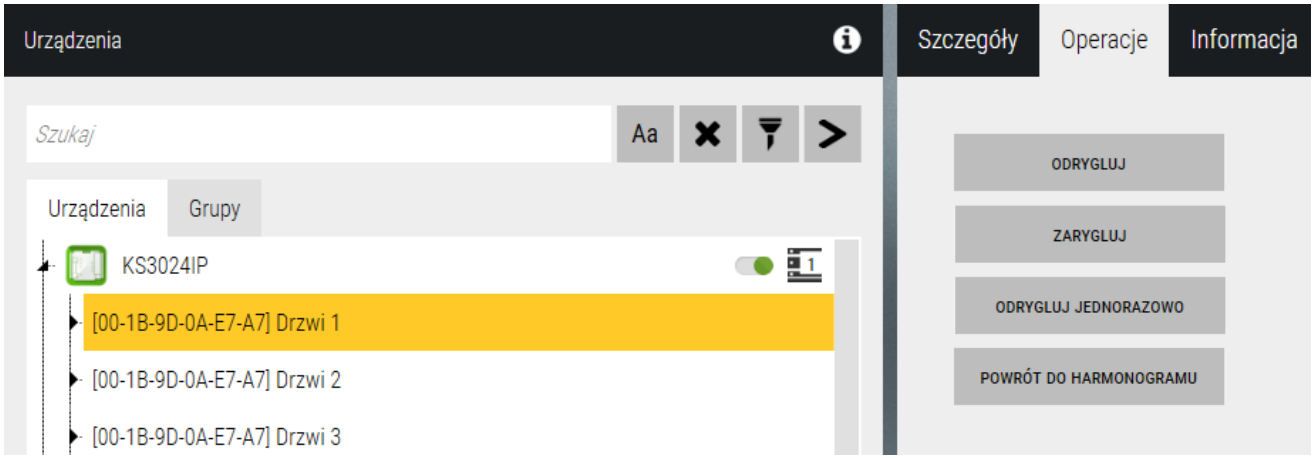


Nowe przyciski:

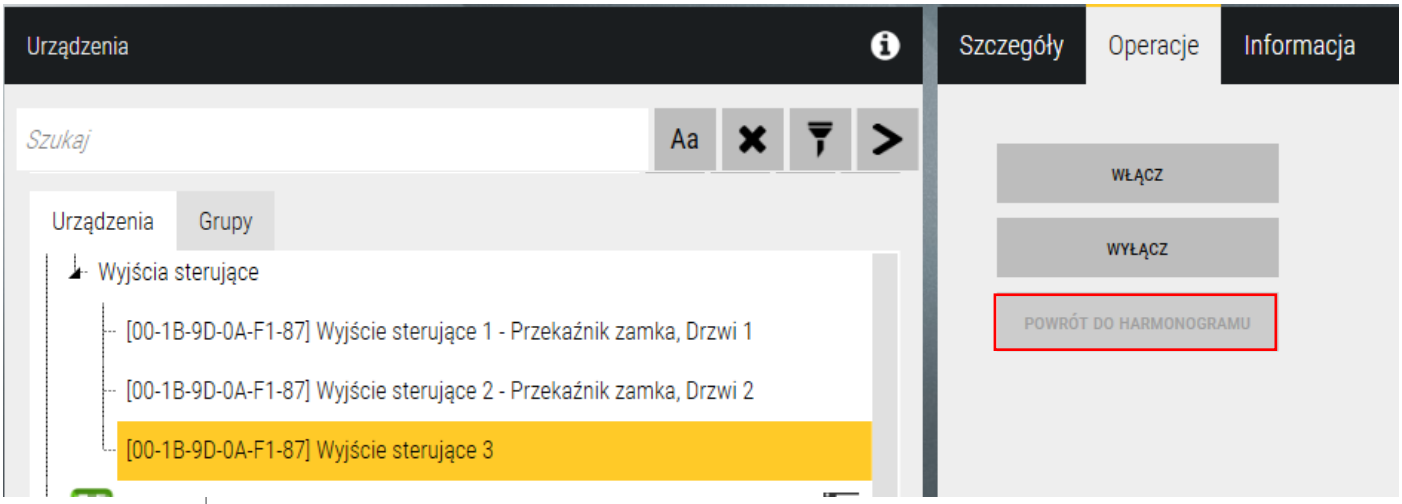
„WYMIANA SERWISOWA” - pozwala wymienić kontroler na nowy, który należy podłączyć z takim samym adresem IP

„AKTUALIZUJ” - pozwala przesłać nowy firmware z programu do kontrolera, jest aktywny przy braku zgodności wersji.

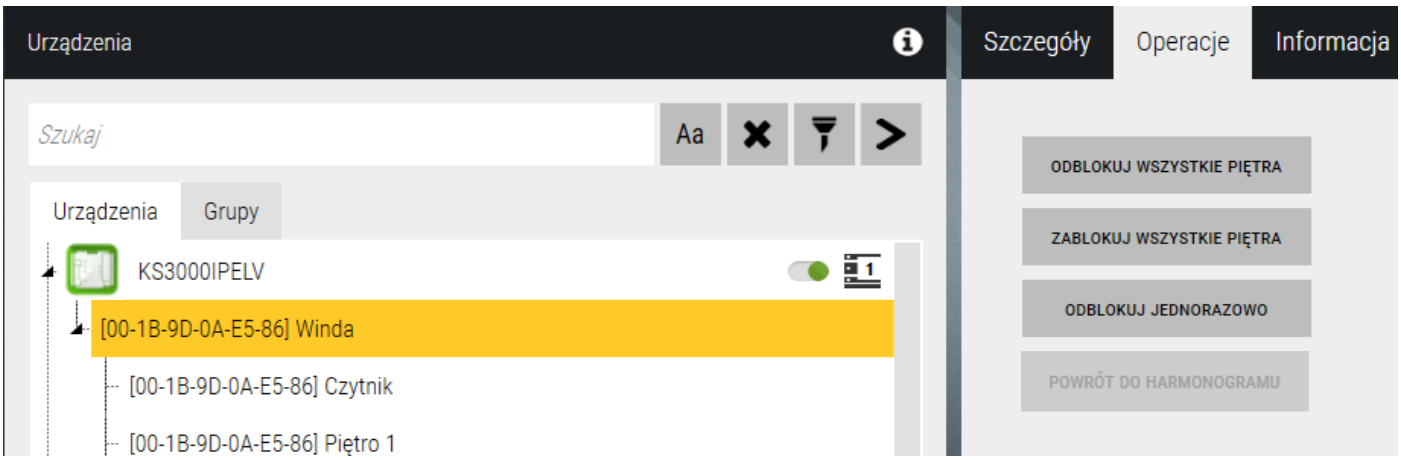
Drzwi



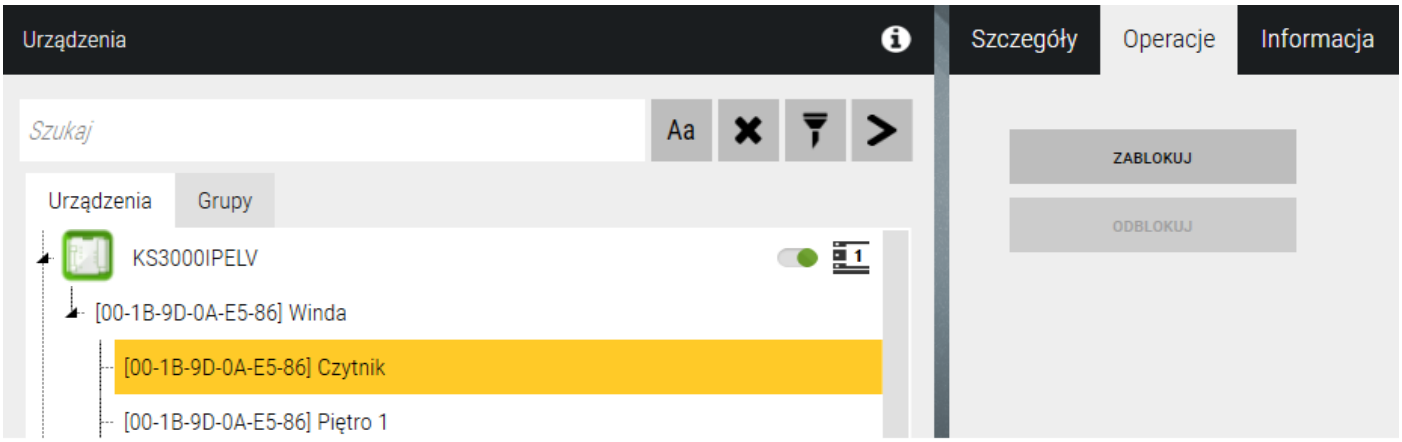
Wyjście sterujące (tylko nie przypisane do zamka) - nowa pozycja - *POWRÓT DO HARMONOGRAMU*



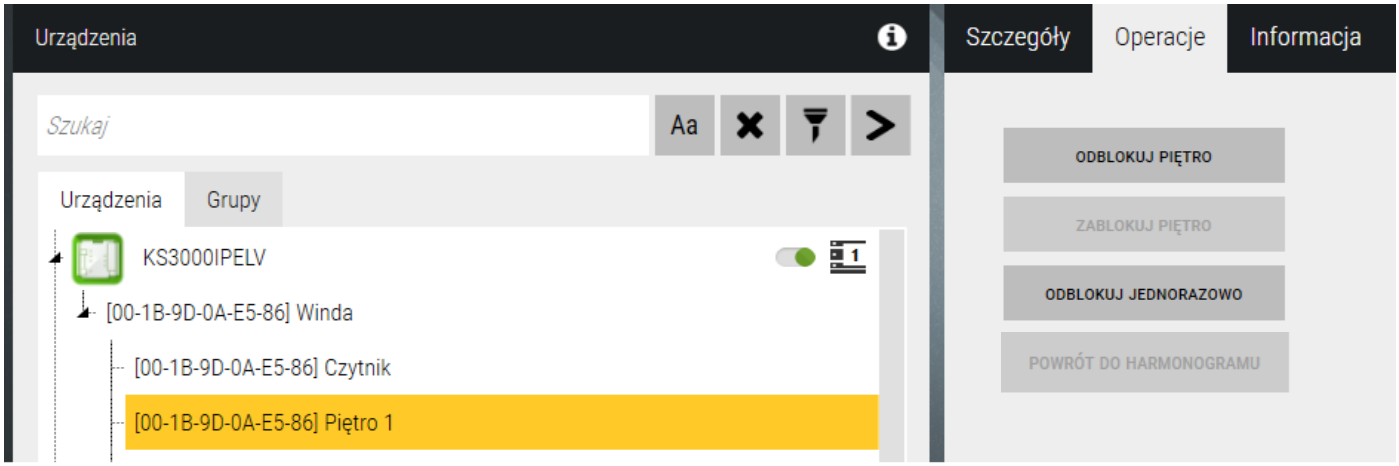
Winda



Czytnik



Piętro



Operacje na centrali alarmowej

Ustaw czas - ustawienie daty oraz godziny w centrali alarmowej zgodnie z czasem komputera, na którym zainstalowany jest program nadzorczy NOVUS MANAGEMENT SYSTEM AC.

Kasuj alarm - jeśli na centrali wystąpił alarm i jest on zapisany w pamięci alarmów to ten przycisk kasuje pamięć alarmów.

Kasuj usterkę - jeśli w pamięci usterek centrali alarmowej znajdują się wyeliminowane usterki ten przycisk kasuje pamięć usterek.

Uzbrój wszystko - przycisk uzbraja wszystkie rozbrojone partycje i strefy w systemie, których status pozwala na włączenie w dozór.

Rozbrój wszystko - przycisk rozbraja wszystkie uzbrojone partycje i strefy w systemie, które nie są w stanie alarmu.

Aktualizuj - pobiera całą konfigurację centrali. Podczas tej czynności program aktualizuje podział systemu na partycję i strefy oraz listę użytkowników wraz z ich kodami.

Użytkownicy - w tym oknie można sprawdzić wszystkich użytkowników centrali, zarówno dodanych przez NOVUS MANAGEMENT SYSTEM AC jak i klawiaturę/DLOADX.

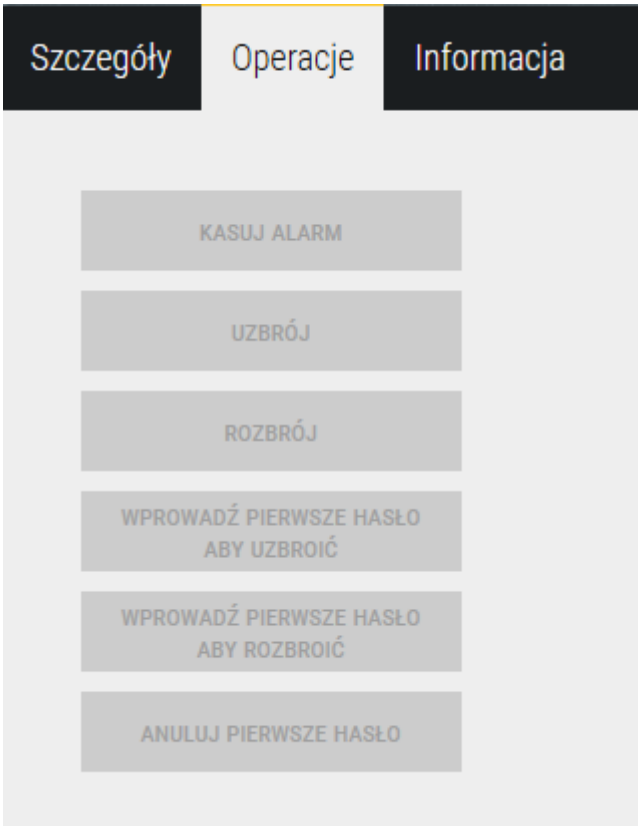
Operacje na partycjach

Kasuj alarm - jeśli w partycji wystąpił alarm i jest on zapisany w pamięci alarmów to ten przycisk kasuje pamięć alarmów.

Uzbrój wszystko - przycisk uzbraja wszystkie rozbrojone strefy w partycji, których status pozwala na włączenie w dozór.

Rozbrój wszystko - przycisk rozbraja wszystkie uzbrojone strefy w partycji, które nie są w stanie alarmu.

Operacje na strefach



Kasuj alarm - jeśli w strefie wystąpił alarm i jest on zapisany w pamięci alarmów to ten przycisk kasuje pamięć alarmów.

Uzbrój - przycisk uzbraja wybraną strefę, jeśli jej status pozwala na włączenie w dozór.

Rozbrój - przycisk rozbraja wybraną strefę, jeśli nie jest w stanie alarmu.

Wprowadź pierwsze hasło aby uzbroić - przycisk wprowadza pierwsze hasło aby uzbroić dla odpowiednio skonfigurowanej strefy. Czas ważności pierwszego hasła ustawiany jest przy dodaniu centrali.

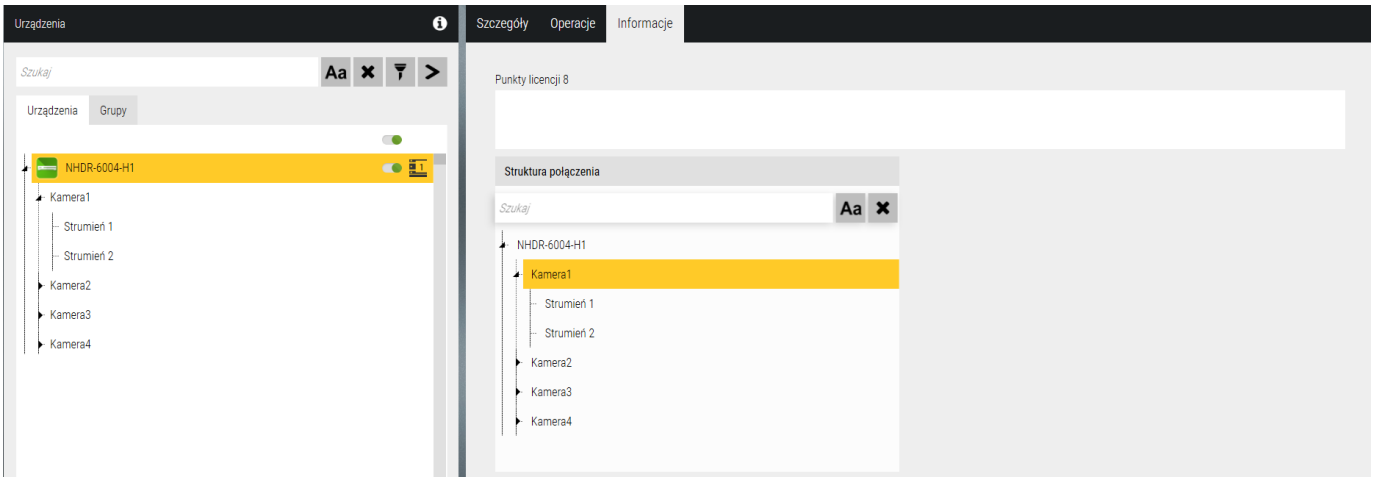
Wprowadź pierwsze hasło aby rozbroić - przycisk wprowadza pierwsze hasło aby rozbroić dla odpowiednio skonfigurowanej strefy. Czas ważności pierwszego hasła ustawiany jest przy dodaniu centrali.

Anuluj pierwsze hasło - przycisk anuluje wprowadzenie pierwszego hasła.

3.17 Urządzenia - Informacje

Każde z urządzeń posiada zakładkę *Informacje,* w której znajdują się następujące dane:

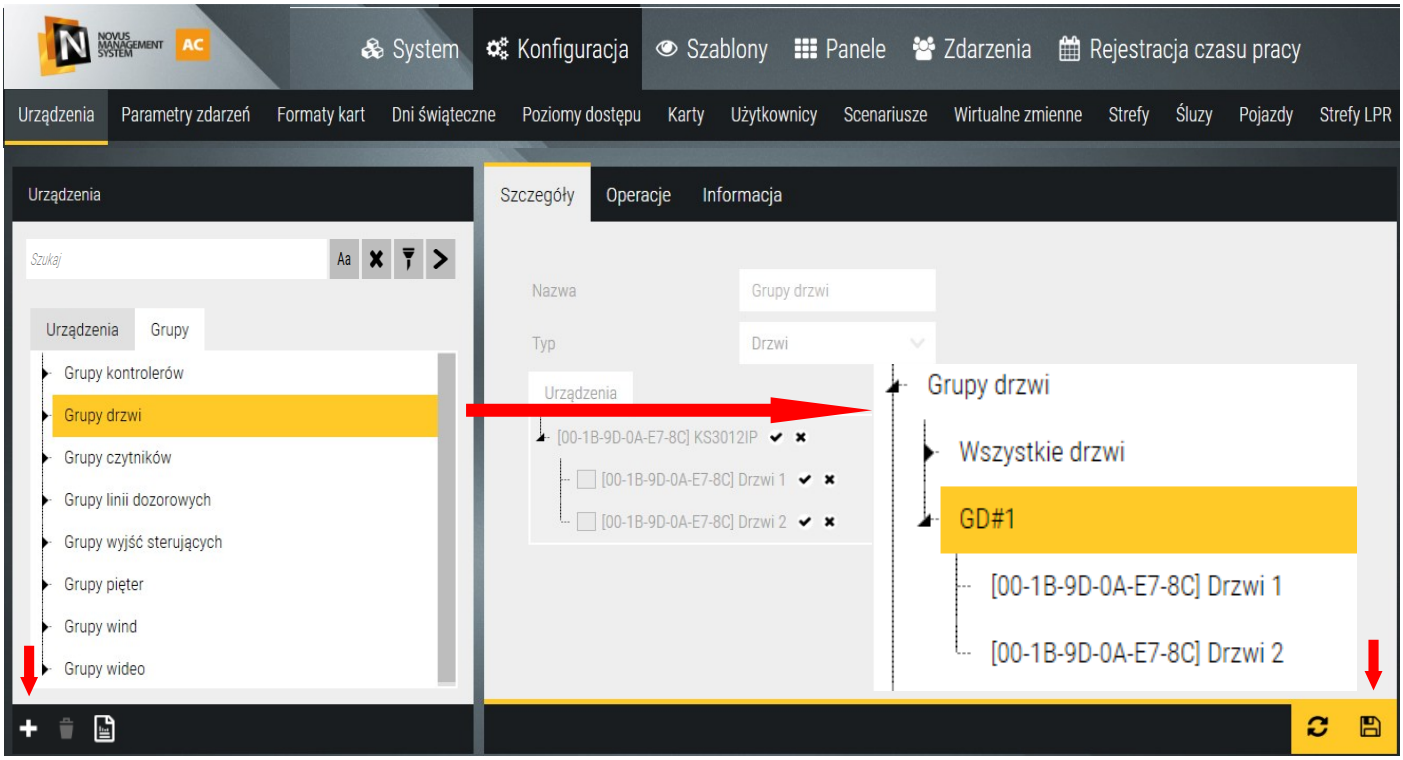
- Liczba punktów licencji pobieranych przez dany element.
- Struktura połączenia urządzenia przedstawiona w formie rozgałęzionej listy.
- Pole opisu, w którym można umieścić dowolne, dodatkowe informacje czy komentarze.



3.18 Urządzenia - Grupy

Zakładka *Grupy* umożliwia zdefiniowanie grup elementów systemu. Lista głównych grup domyślnych wyświetlana jest w lewym oknie. Każda z grup domyślnych ma zdefiniowaną grupę, która zawiera wszystkie elementy danego typu (patrz *Grupy drzwi)* i jest automatycznie aktualizowana po dodaniu nowego elementu danego typu.

Grupy służą do wykonywania zbiorowych operacji na elementach systemu np. odryglowanie grupy drzwi, co znacznie przyspiesza ten proces przy dużej liczbie drzwi. Operacje na grupach można wykonać z poziomu menu kontekstowego czarnej ikony ***grupy*** na panelu lub przechodząc do zakładki *Operacje* w tym oknie.



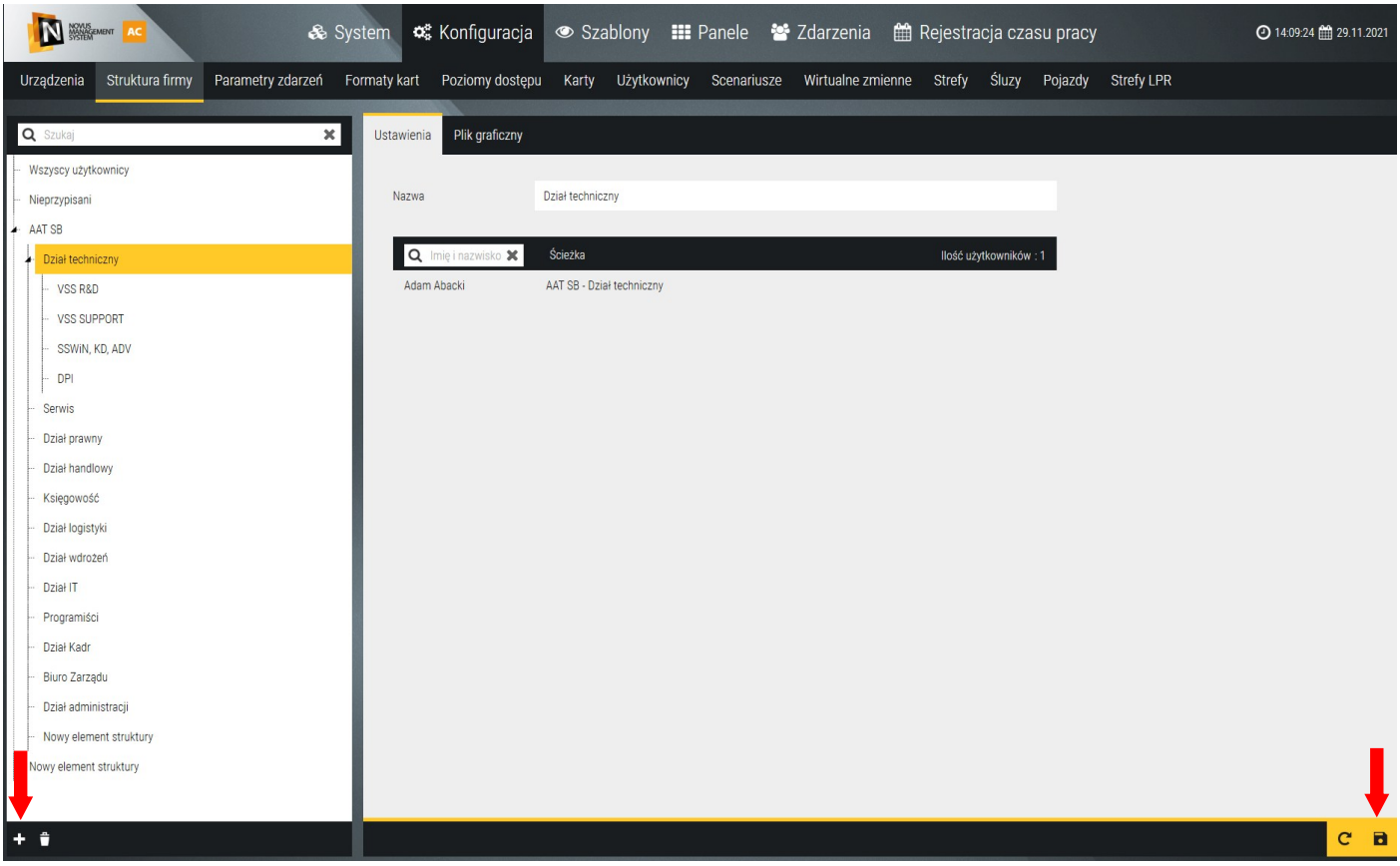
Oprócz grup domyślnych zawierających wszystkie elementy danego typu możemy definiować podgrupy, które zawierają tylko wybrane elementy danego typu. W tym celu należy zaznaczyć grupę domyślną danego typu i kliknąć przycisk ***„+”*** na dole okna. W drzewie grup pojawi się nowa podgrupa, a w prawym oknie lista wszystkich elementów danego rodzaju. Należy zaznaczyć pozycje, które mają należeć do nowej grupy.

Aby dodać nową grupę w drzewie głównym nie może być zaznaczona żadna z grup. Jeżeli jest takie zaznaczenie (żółty pasek) to należy kliknąć na nim trzymając równocześnie naciśnięty przycisk ***CTRL***. Grupa dodana w drzewie głównym może zawierać elementy różnych typów. Można to wykorzystać do tworzenia struktury systemu w wielu lokalizacjach.

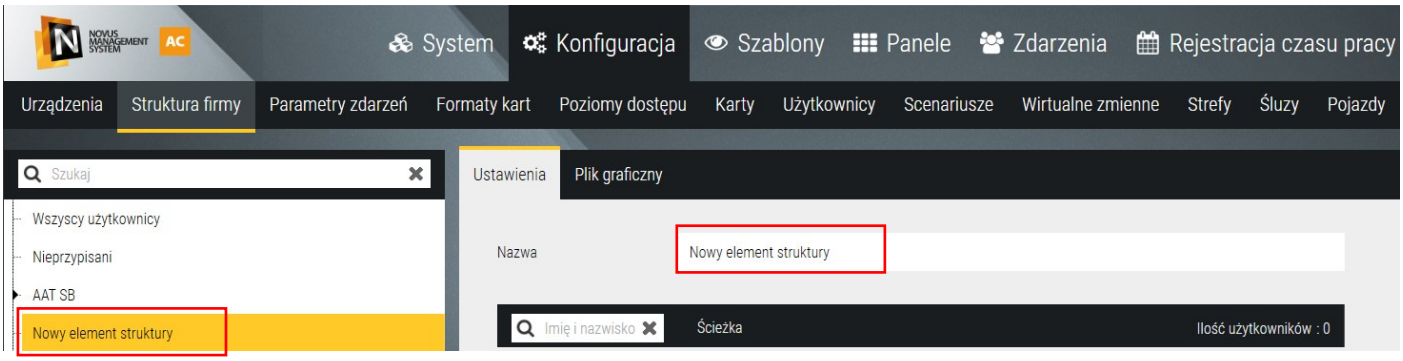
Zdefiniowaną grupę można edytować lub usuwać zaznaczając ją na liście i klikając na przycisk ***kosza*** w lewym dolnym rogu okna.

3.19 Konfiguracja - Struktura firmy

Zakładka umożliwia zdefiniowanie struktury organizacyjnej firmy, a następnie przypisanie do niej pracowników. Pozwala to na generowanie raportów zdarzeń i raportów RCP dla wybranego działu.
Domyślnie w lewym oknie są dwie pozycje:

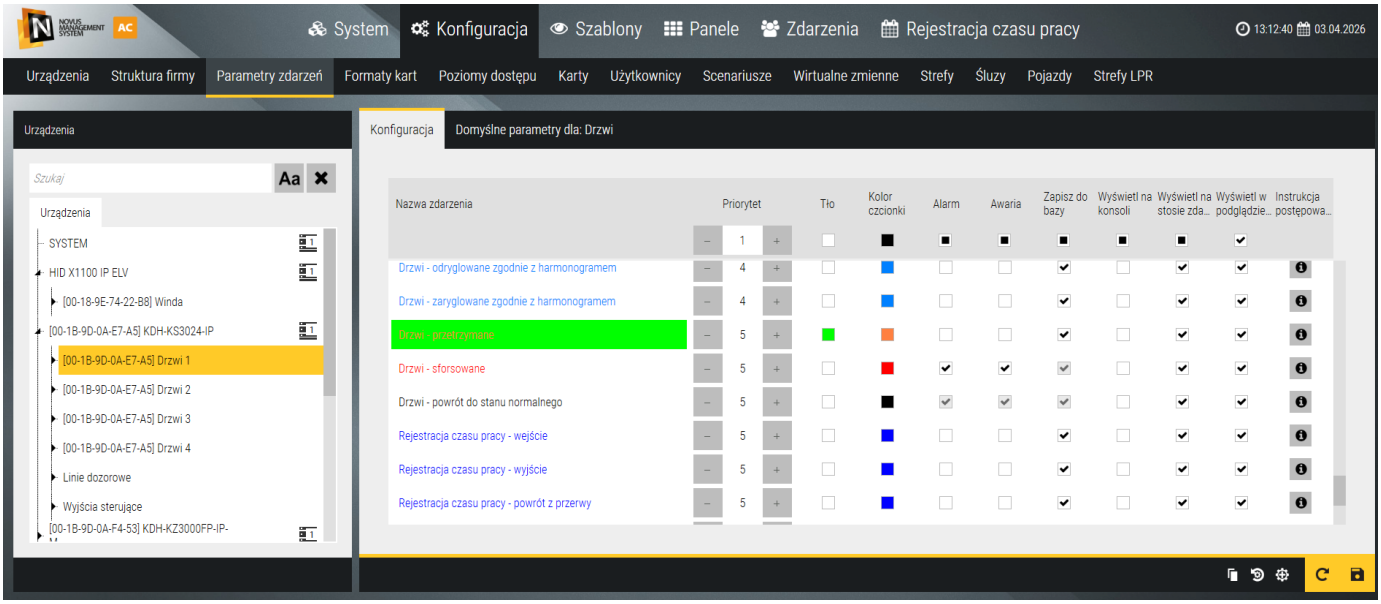


Wszyscy - wyświetla w prawym oknie listę wszystkich użytkowników dodanych do bazy
Nieprzypisani - wyświetla w prawym oknie listę użytkowników nieprzypisanych do struktury
Po dodaniu użytkowników (ręcznie lub poprzez import) obie listy są takie same.
Aby dodać strukturę firmy należy kliknąć na przycisku ***Dodaj*** w lewym dolnym rogu.
W drzewie pojawi się nowa pozycja. Żeby dodać nową pozycje w drzewie głównym, nie może być zaznaczona żadna pozycja (żeby odznaczyć kliknij na zaznaczonej prawym przyciskiem myszy). Jeżeli jest zaznaczona pozycja w drzewie głównym to można dodać do niej kolejne. W ten sposób można stworzyć wielopoziomową strukturę firmy - departament, wydział dział itd.



W prawym oknie można edytować nazwę poz. Po zdefiniowaniu struktury kliknąć na przycisku ***Zapisz*** w prawym dolnym rogu. Przypisanie pracownika do struktury należy wykonać w oknie definiowania użytkownika.

3.20 Konfiguracja - Parametry zdarzeń



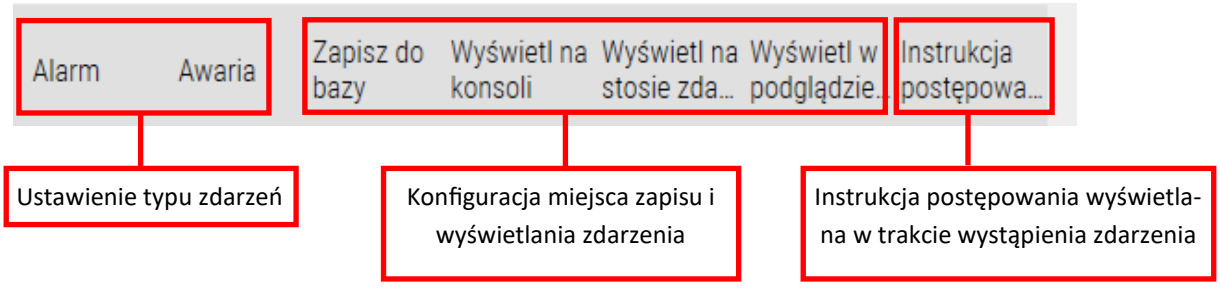
Zakładka *Parametry zdarzeń* służy do konfiguracji i wyboru zdarzeń wszystkich urządzeń i ich elementów, oraz określenia w jakich miejscach w systemie mają się pojawiać.

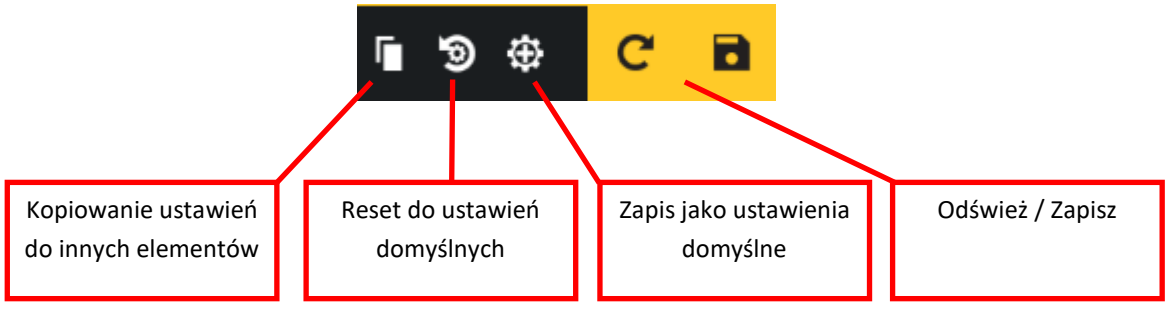
Nazwa zdarzenia - nazwy występujących zdarzeń, to pole nie podlega edycji.

Priorytet - określenie wartości priorytetu od 1 do 5 (5 - najwyższy priorytet zdarzenia)

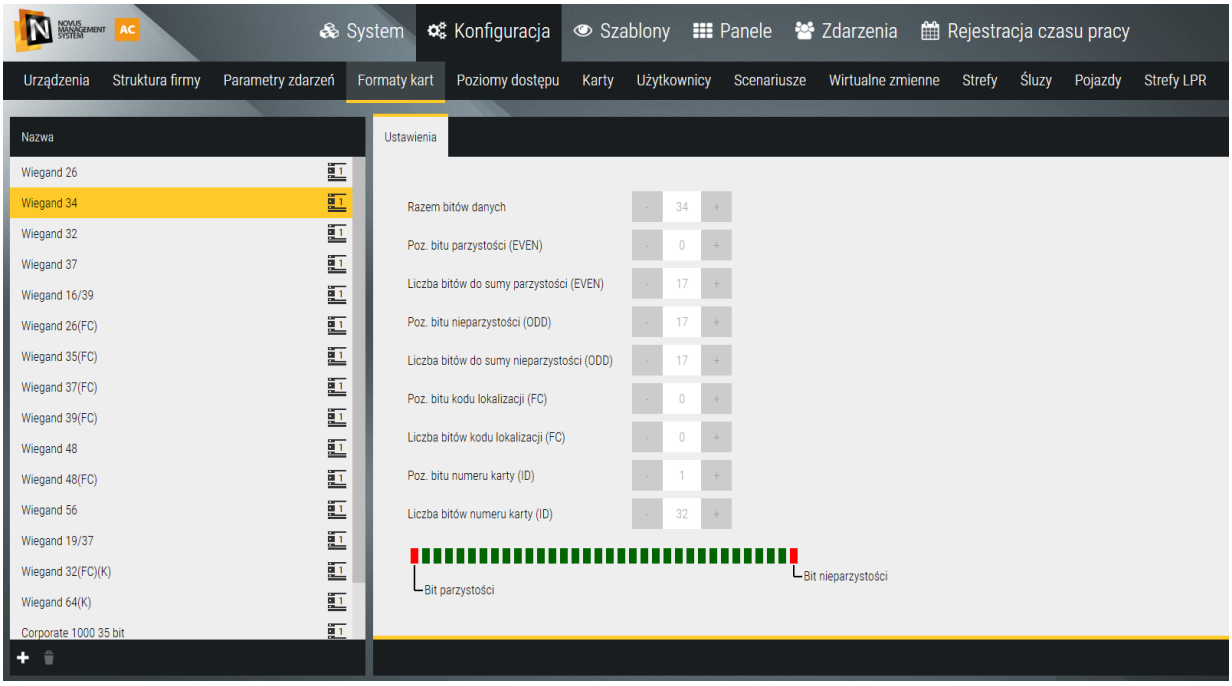
Tło - kolor tła wyświetlanych logów zdarzeń

Kolor czcionki - kolor czcionki wyświetlanych logów zdarzeń



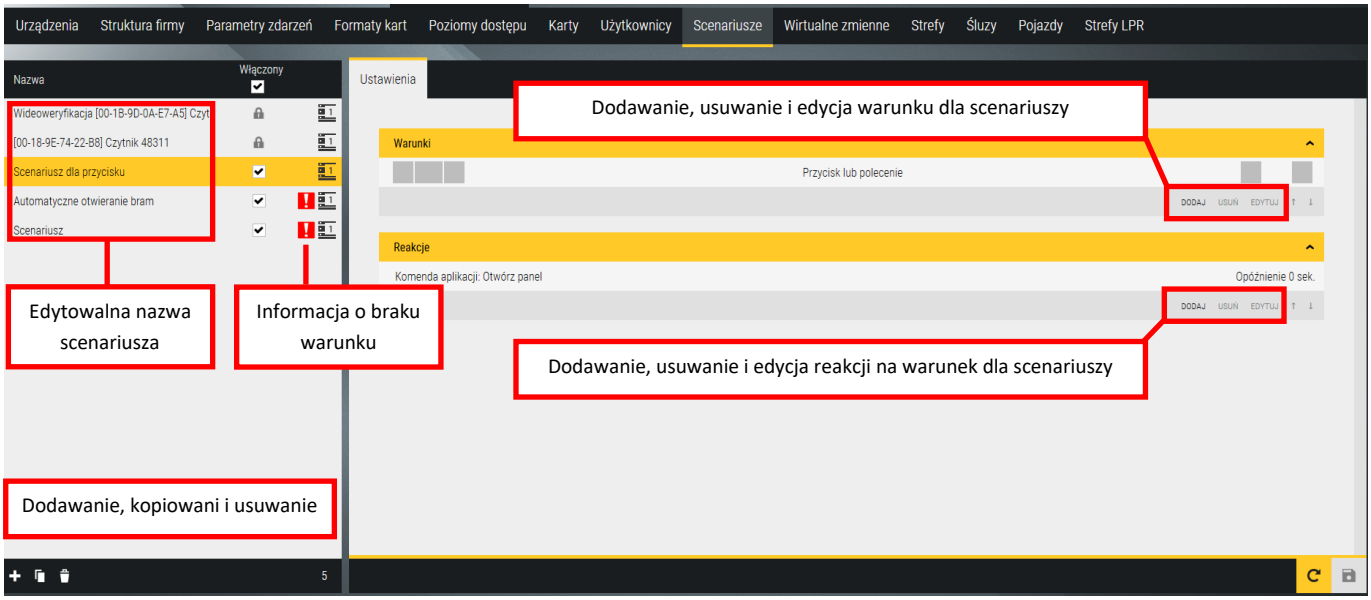


3.21 Konfiguracja - Formaty kart



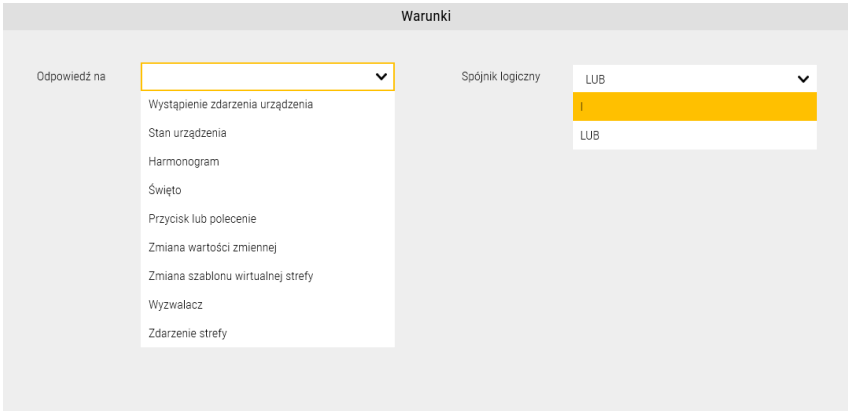
Zakładka *Formaty kart* wyświetla gotowe formaty odczytu kart w systemie kontroli dostępu, a także umożliwia tworzenie własnych formatów po wybraniu ikony „+” na samym dole. Możliwość tworzenia formatów ograniczona jest do możliwości wspieranych kontrolerów KD do maksymalnie 66 bitów.

3.22 Konfiguracja - Scenariusze

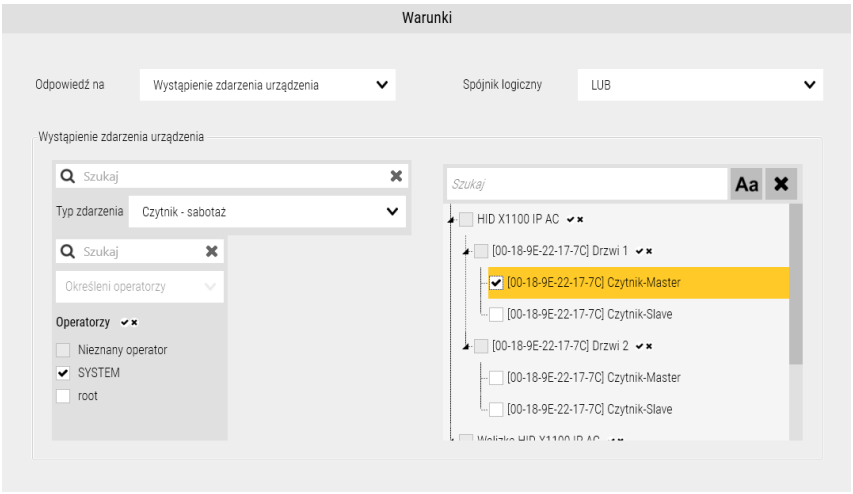


Scenariusze pozwalają na niemal nieograniczone tworzenie wszelkich zależności wykonywanych przez oprogramowanie, pomiędzy większością elementów, zdarzeń, harmonogramów, przycisków itp. a szeregiem reakcji i komend.

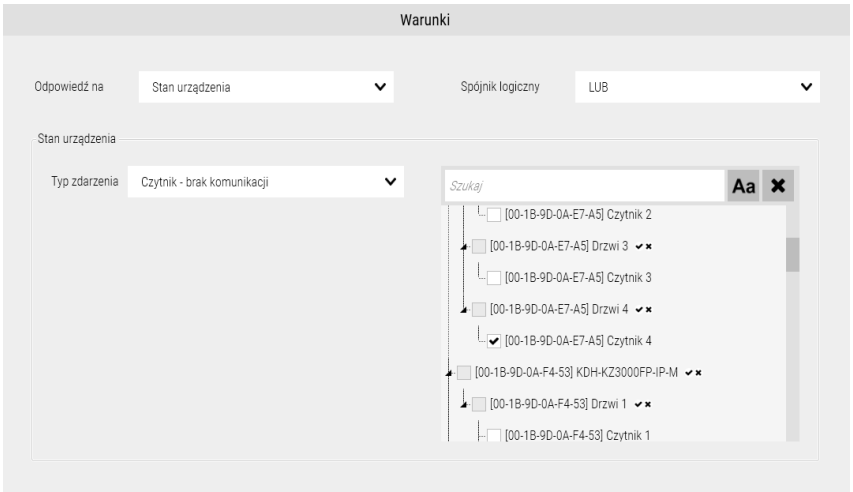
Pozwala to na tworzenie bardzo zaawansowanych scenariuszy zdarzeń, które z ciągłym rozwojem oprogramowania będą rozbudowywane o kolejne funkcje.



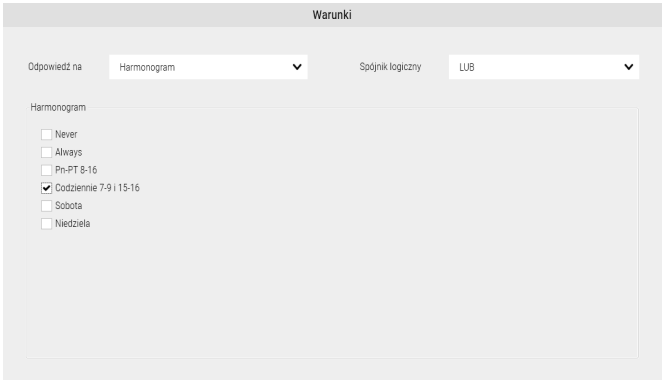
Warunki - Ustawienia warunków, które muszą zostać spełnione aby wykonać reakcję scenariusza, można zastosować kilka warunków ze spójnikiem logicznym „i" oraz „lub" w zależności czy ma być spełnionych kilka warunków czy tylko jeden z nich.

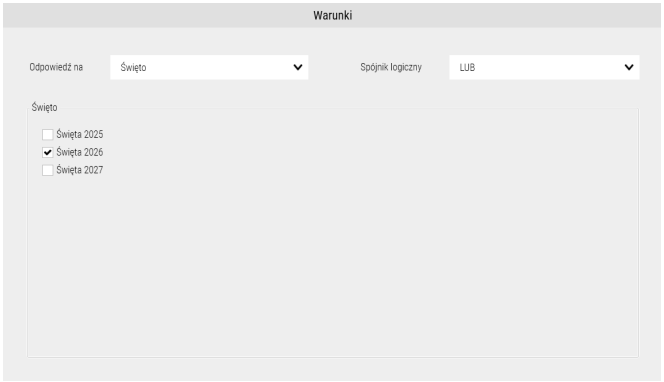


Wystąpienie zdarzenia urządzenia - określamy konkretny rodzaj zdarzenia i element urządzenia którego zdarzenie dotyczy, możemy też zaznaczyć których operatorów dotyczy wykonany warunek.

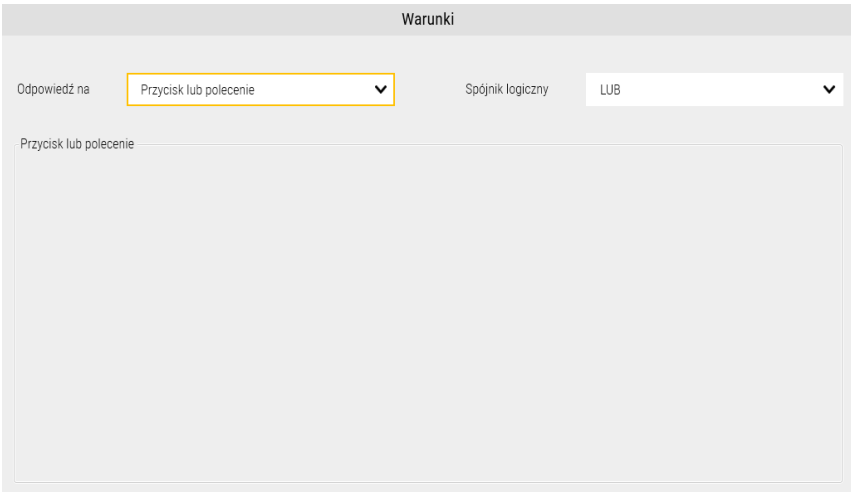


Stan urządzenia - określamy konkretny rodzaj zdarzenia dotyczący stanu i element urządzenia którego zdarzenie dotyczy.

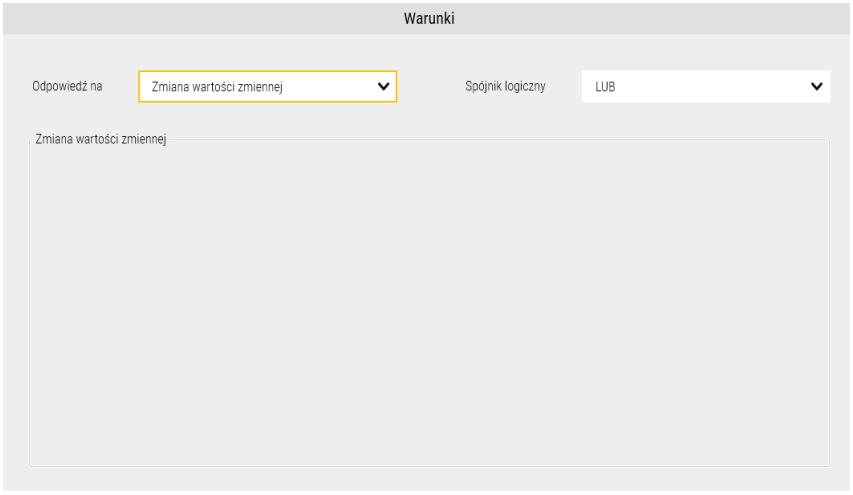




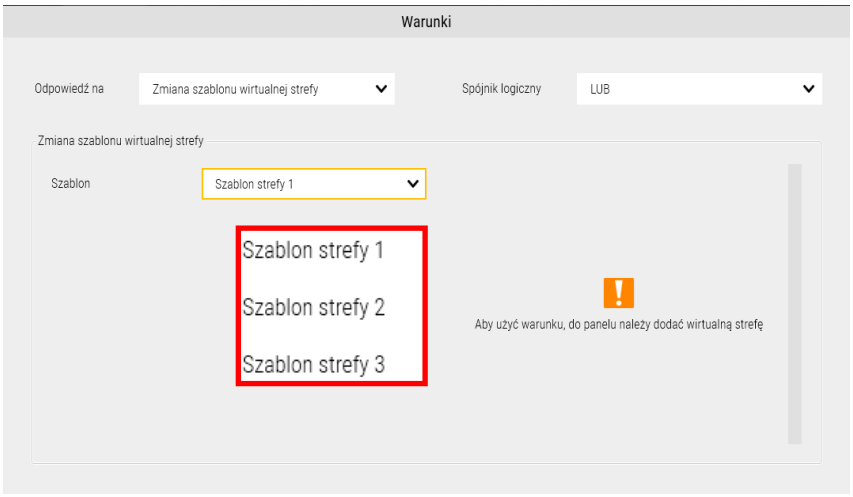
Harmonogram- Ustawienia warunków według skonfigurowanych harmonogramów czasowych.
Święta - Ustawienie warunków według skonfigurowanych dni świątecznych.



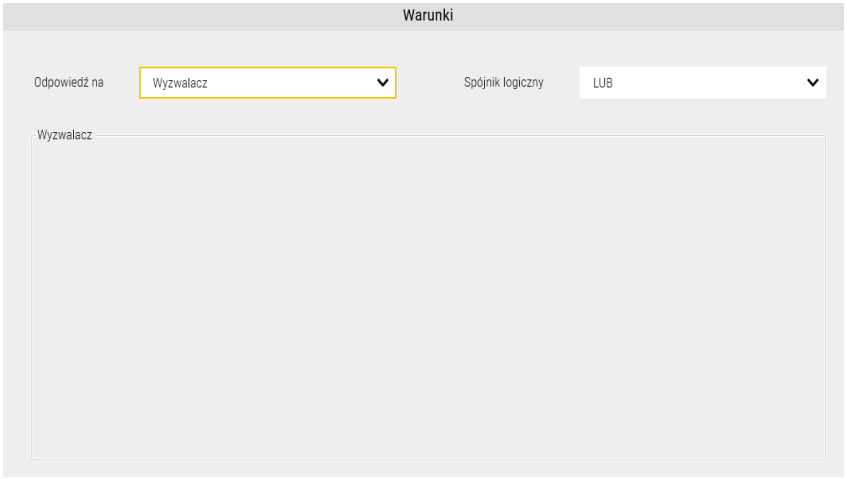
Przycisk lub polecenie - Ustawienie warunku przypisanego do przycisku lub polecenia z aplikacji.



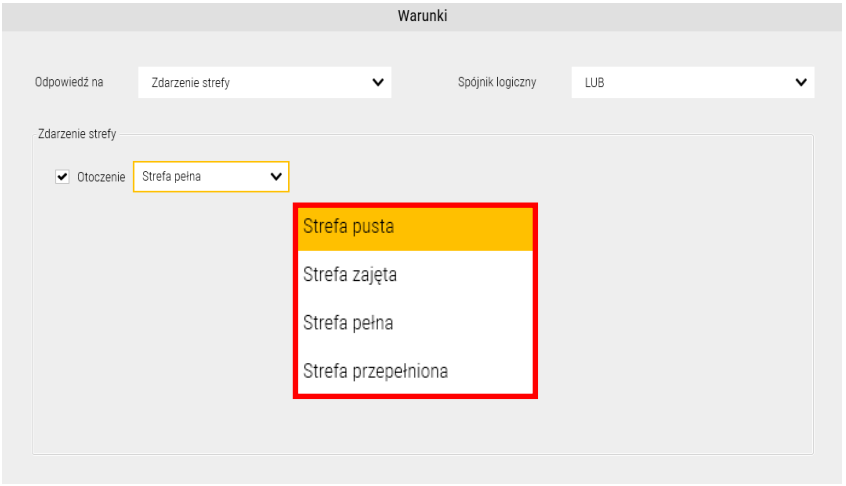
Zmiana wartości zmiennej - Ustawienie warunku na zmianę wartości zmiennej.



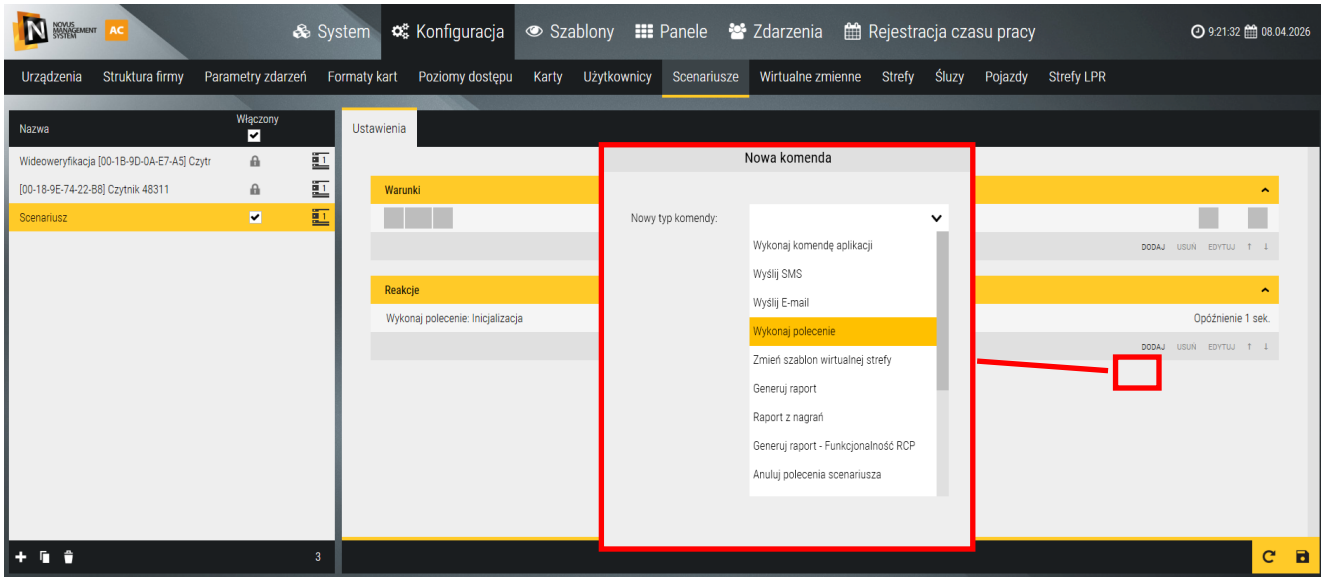
Zmiana szablonu wirtualnej strefy - Ustawienie warunku dotyczącego zmiany szablonu wirtualnej strefy, wymaga wcześniejszego skonfigurowania wirtualnej strefy.



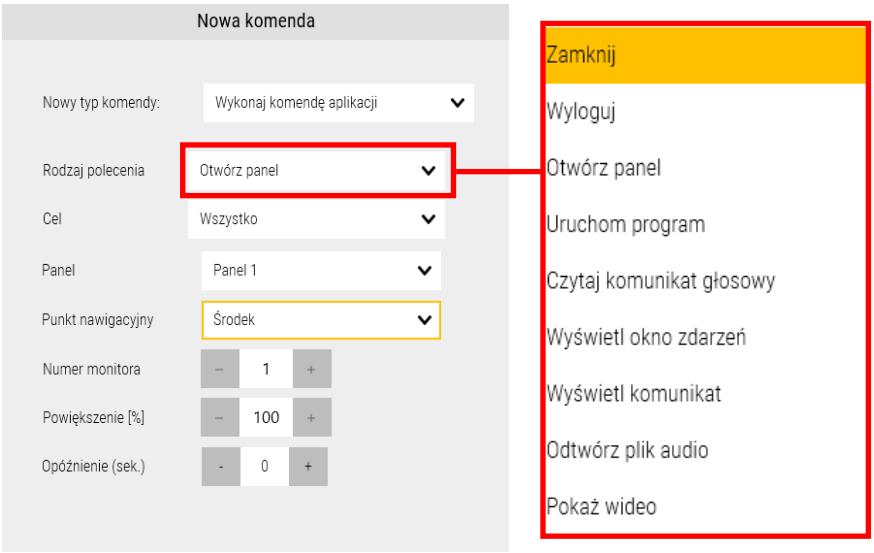
Wyzwalacz - Ustawiamy warunek dotyczący wyzwalacza.



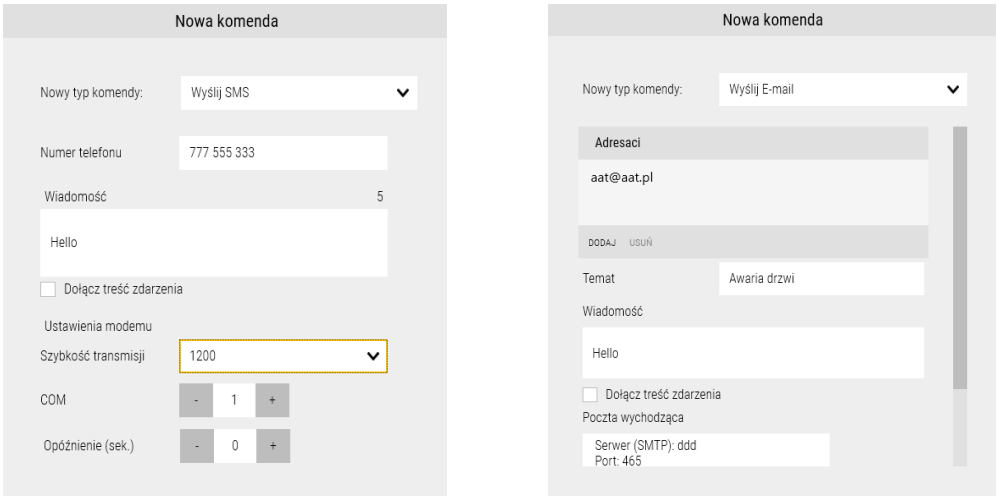
Zdarzenie strefy - Określamy warunek dla wystąpienia konkretnego zdarzenia dotyczącego strefy Strefa pusta, Strefa zajęta, Strefa pełna lub Strefa przepełniona.



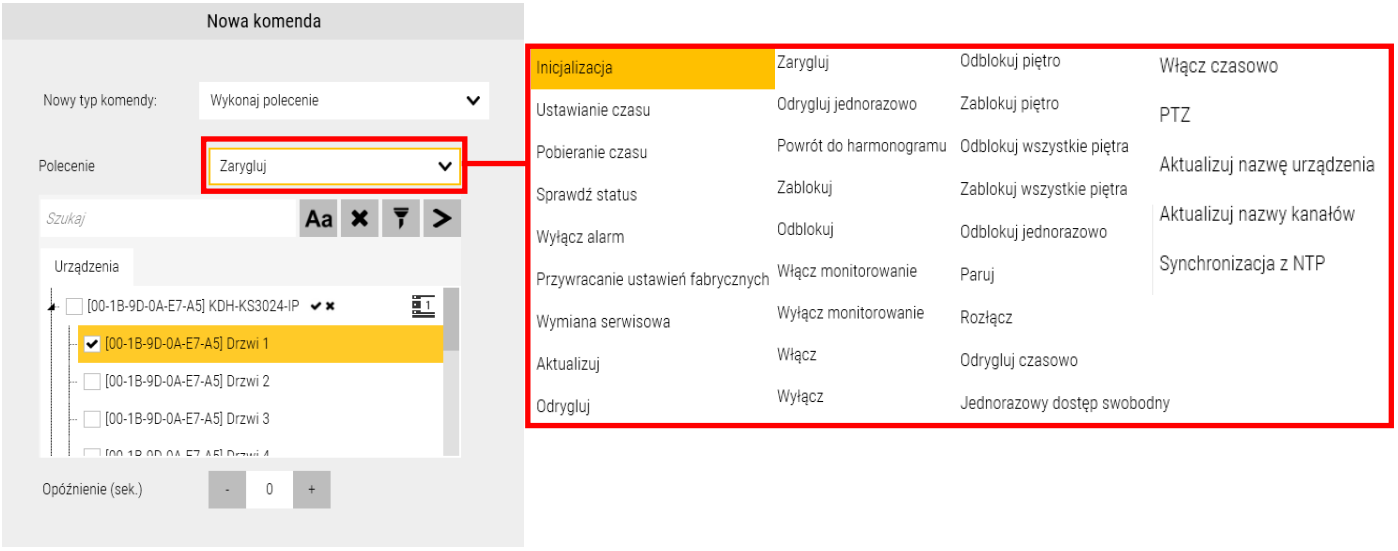
Reakcje - Ustawienie reakcji dla skonfigurowanego wcześniej warunku scenariusza.



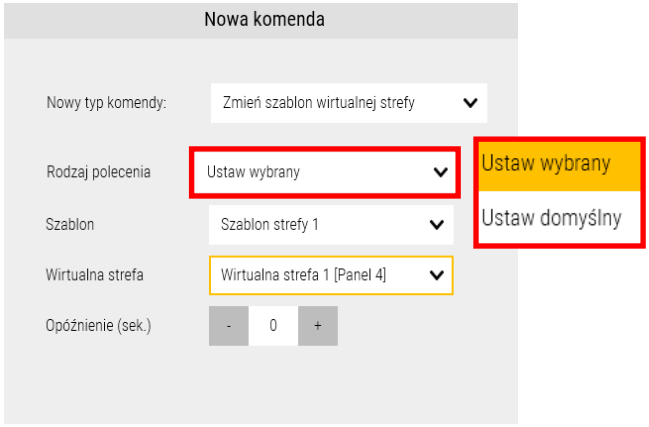
Wykonaj komendę aplikacji - Konfigurujemy rodzaj polecenia aplikacji z dostępnej listy.



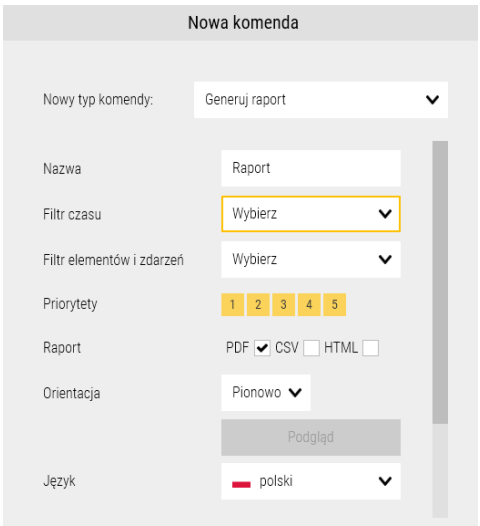
Wyślij SMS, Wyślij E-mail - Konfiguracja polecenia wysłania wiadomości tekstowej SMS lub e-mail.



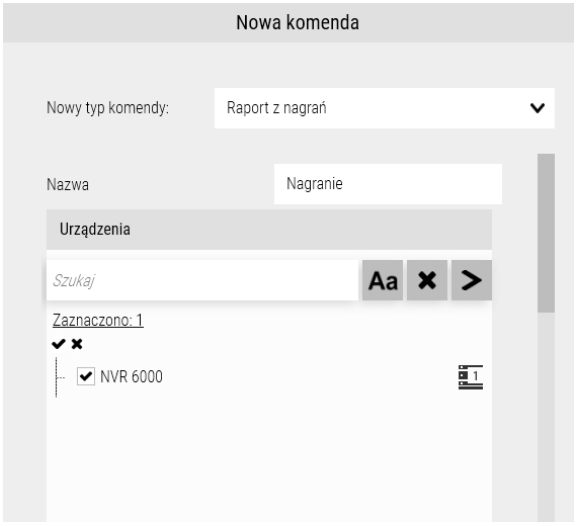
Wykonanie polecenia - Ustawienie reakcji polecenia do wyboru z rozwijanej listy, oraz wybór urządzenia lub konkretnego z elementów urządzeń, którego polecenia ma dotyczyć.



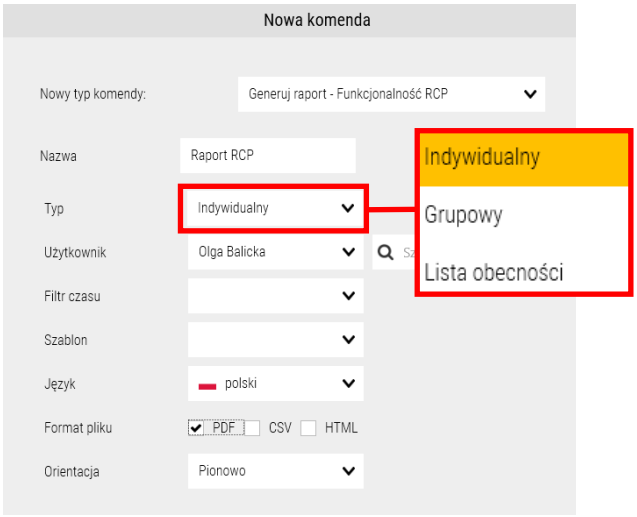
Zmień szablon wirtualnej strefy - Ustawienie reakcji dla zmiany szablonu wirtualnej strefy na domyślny lub wybrany z listy szablonów.



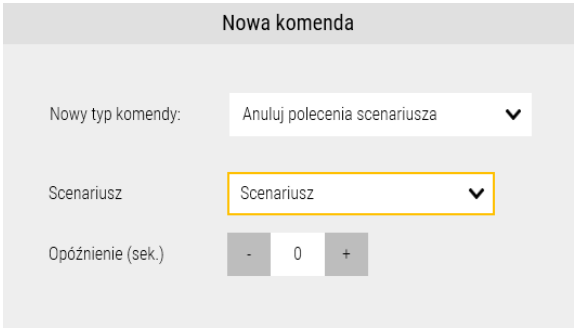
Generuj raport - Ustawienie dla reakcji generowania raportu, z konfiguracją filtra czasu, elementów oraz formatu raportów i wysłaniem raportu w wiadomości e-mail.



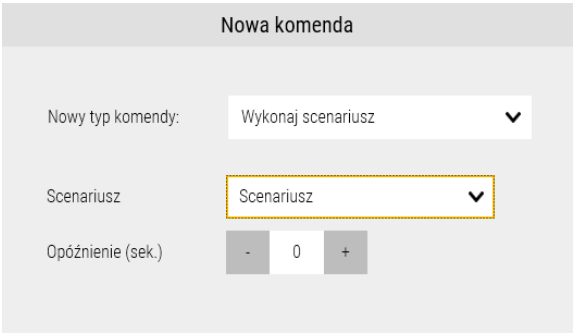
Raport z nagrań - Ustawienie reakcji generowania raportu z nagrań z wyborem rejestratorów z listy.



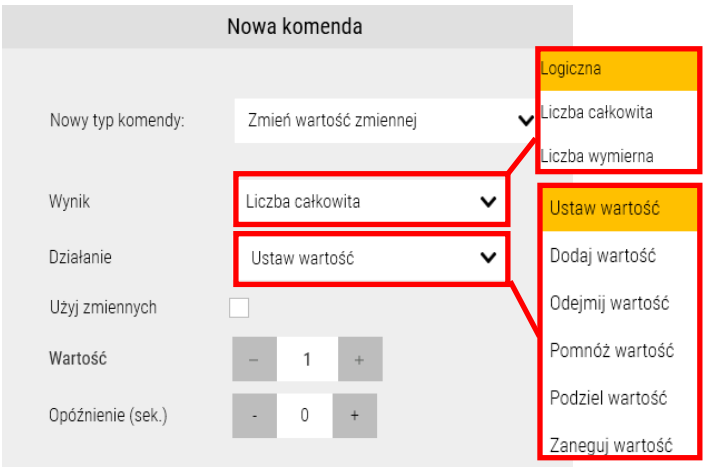
Generuj raport - Funkcjonalność RCP- Ustawienie reakcji do wykonania raportów RCP, Indywidualnych, Grupowych lub z listy obecności, z wyborem zakresu czasu, rodzaju szablonu i formatu pliku raportu.



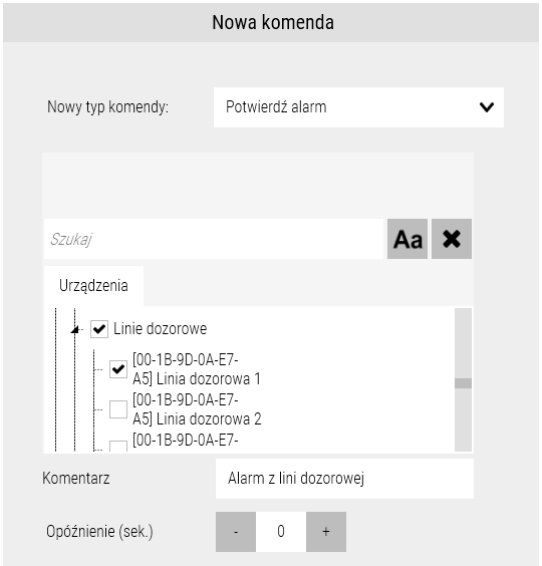
Anuluj polecenie scenariusza - Ustawienie reakcji anulowania innego działającego scenariusza.



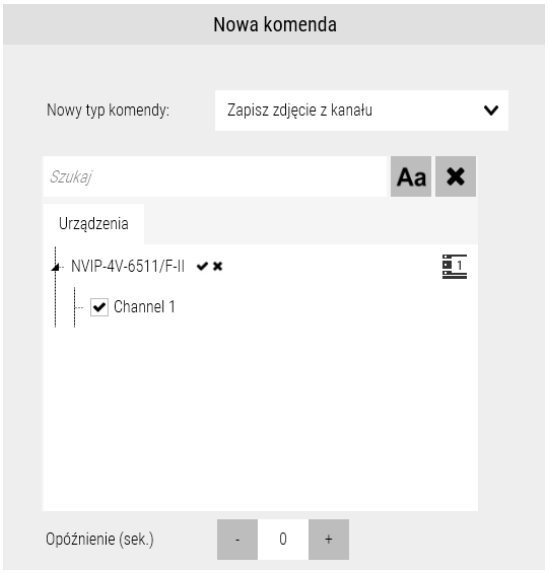
Wykonaj scenariusz - Ustawienie reakcji dla wykonania innego skonfigurowanego scenariusza.



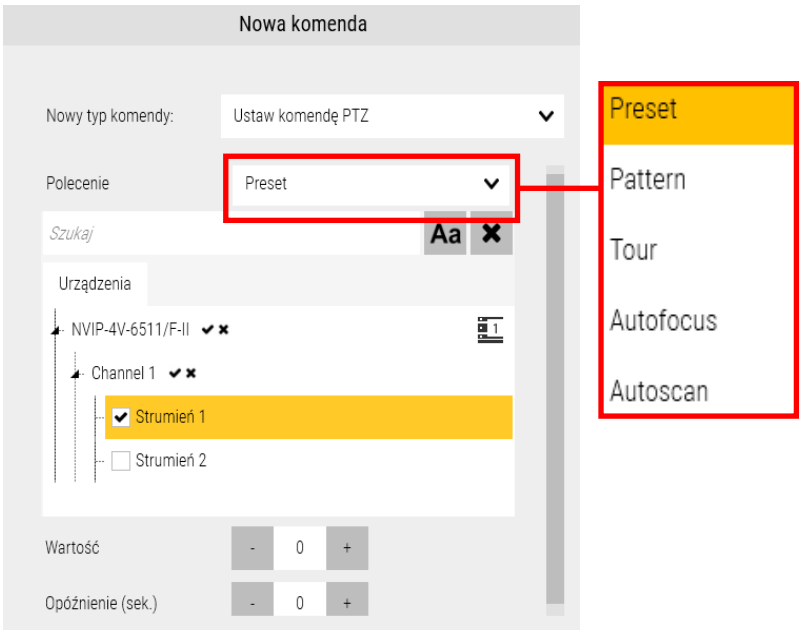
Zmień wartość zmiennej- Ustawienie reakcji dla zmiany wartości zmiennej, konfiguracja zmiennych w zakładce *Konfiguracja/Wirtualne zmienne.*



Potwierdź alarm - Ustawienie reakcji potwierdzenia alarmu z wybranej linii, urządzenia lub elementu.

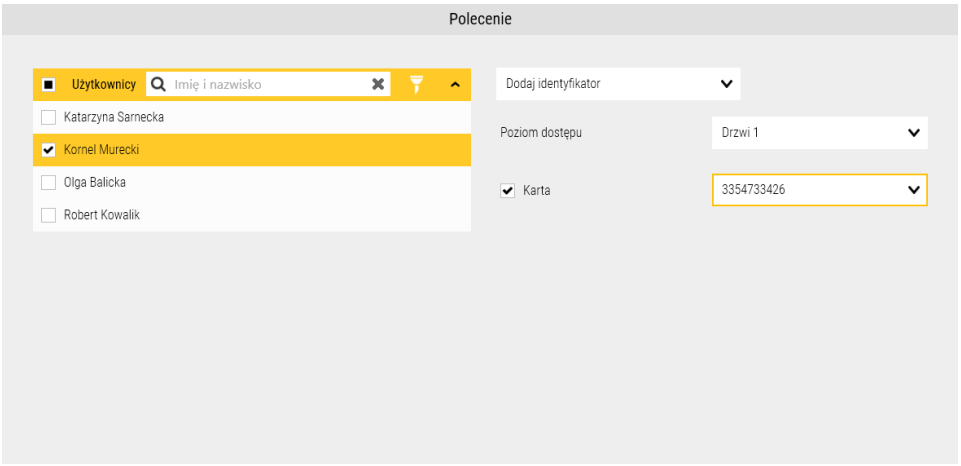


Zapisz zdjęcie z kanału - Ustawienie reakcji dla zapisu zdjęcia z wybranego kanału kamery.

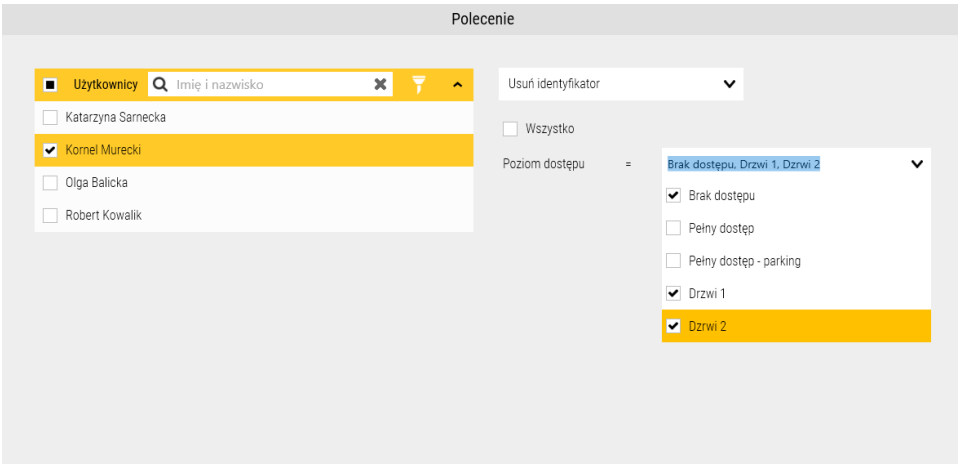


Ustaw komendę PTZ - Ustawienie reakcji dla komend PTZ dla wybranych kanałów w zakresie możliwych poleceń do wyboru z listy.

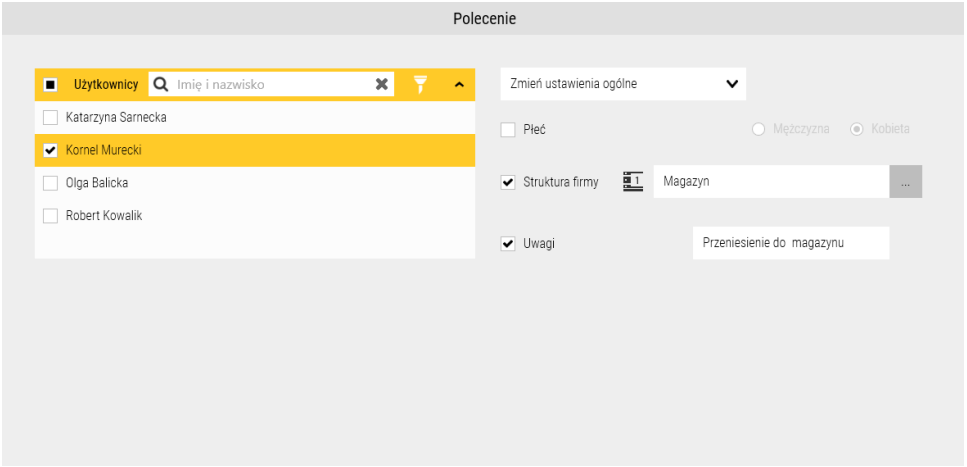
Reakcje dotyczące użytkowników* - funkcjonalność dostępna od wersji 6.06.xxx.



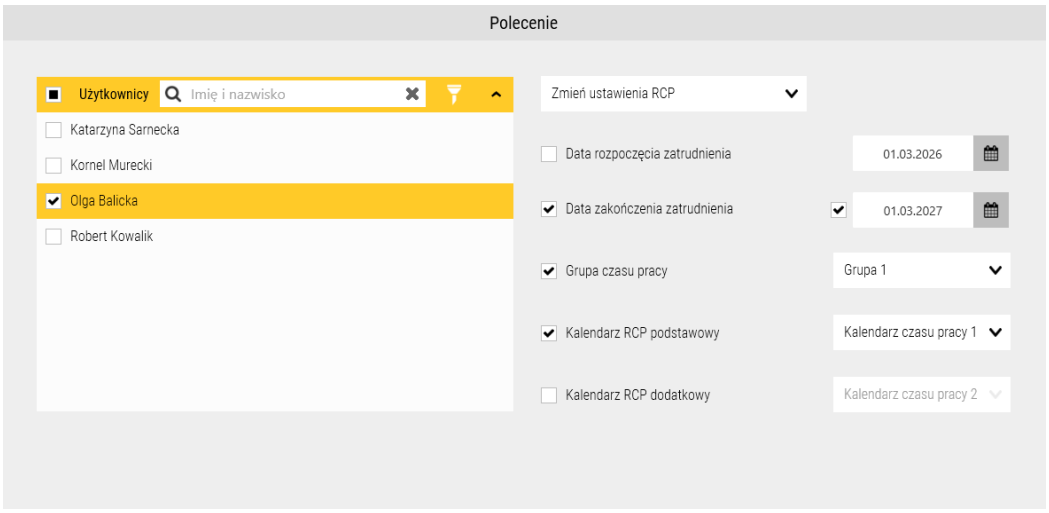
Dodaj identyfikator – Reakcja umożliwia dodanie identyfikatora z konkretnym poziomem dostępu wybranym użytkownikom.



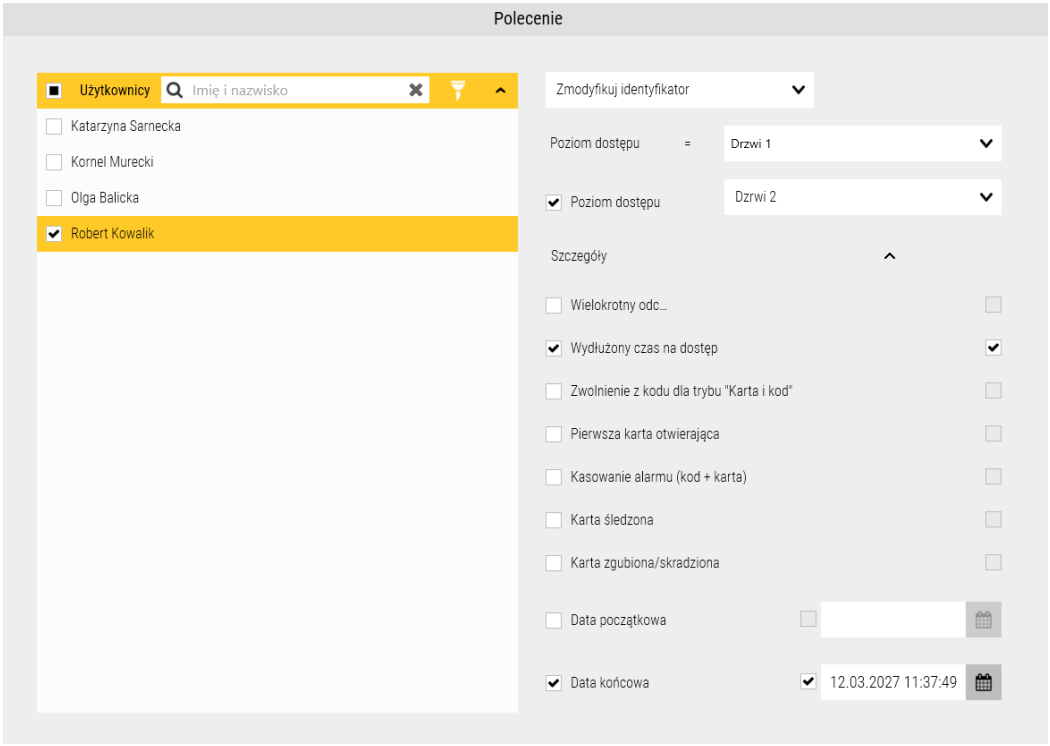
Usuń identyfikator - Ustawienie reakcji usuwania wybranego identyfikatora użytkownika z konkretnym poziomem dostępu.



Zmień ustawienia ogólne - Ustawienie reakcji zmiany wybranych funkcji dotyczących użytkownika.



Zmień ustawienia RCP - Reakcja umożliwia zmianę konfiguracji dotyczącej rejestracji czasu pracy RCP wybranych użytkowników, zmiana daty rozpoczęcia i zakończenia zatrudnienia, zmiana grupy czasu pracy, kalendarze podstawowego i dodatkowego RCP.



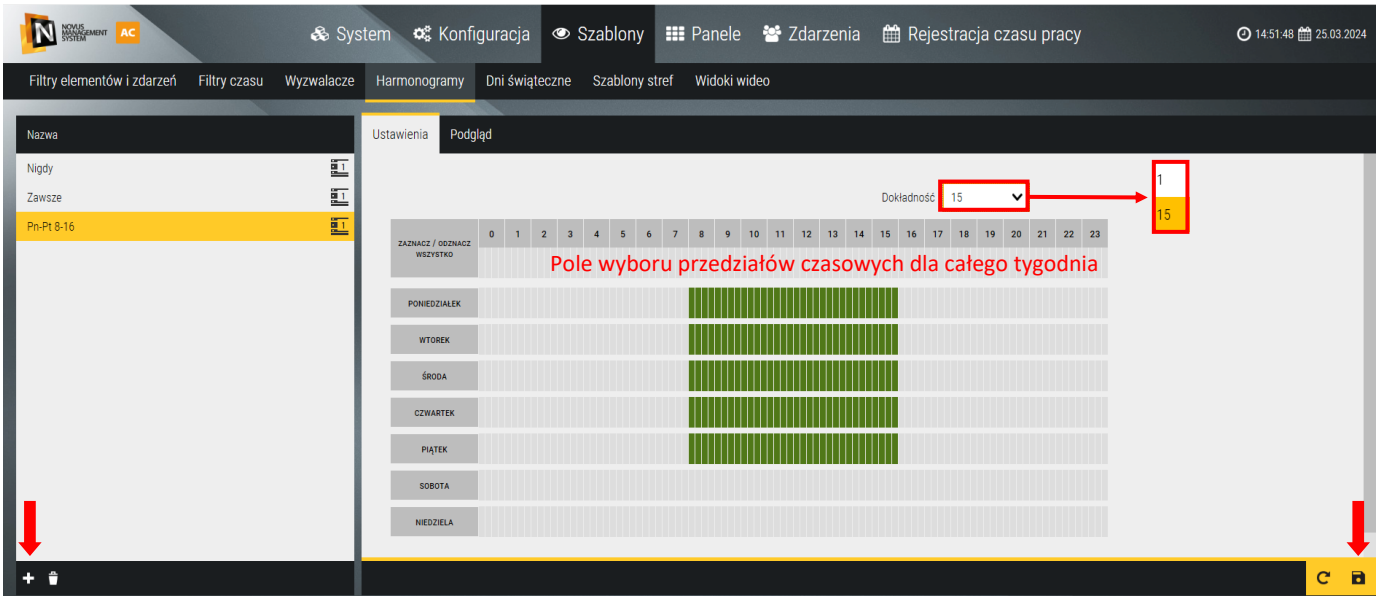
Zmodyfikuj identyfikator - Ustawienie reakcji związanej z modyfikacją identyfikatorów wybranych użytkowników:

- Zmiana poziomu dostępu
- Zmiana szczegółów dotyczących identyfikatorów
- Zmiana daty początkowej ważności identyfikatora
- Zmiana daty końcowej ważności identyfikatora

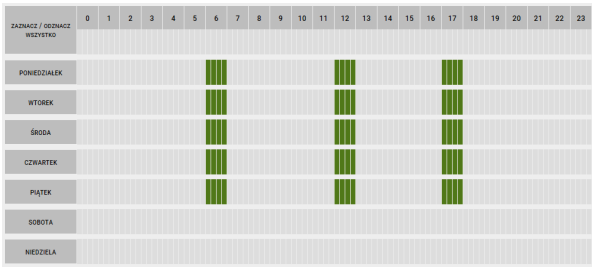
Rozdział 4. Użytkownicy, karty i uprawnienia

4.1 Harmonogramy

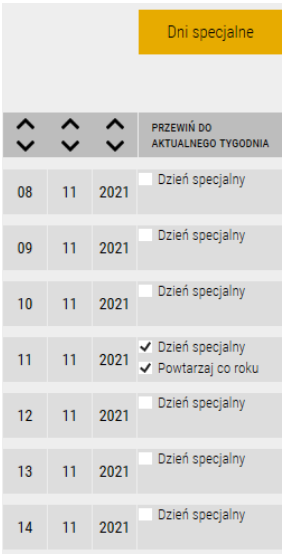
Zakładka *Szablony / Harmonogramy* umożliwia zdefiniowanie harmonogramów przeznaczonych w systemie KD do poziomów dostępu, automatycznego odryglowania drzwi, monitorowania linii dozorowych w określonych przedziałach czasowych oraz włączania wyjść sterujących i scenariuszy.



Domyślnie zdefiniowane są dwa harmonogramy *Nigdy* i *Zawsze,* których nie można usnąć lub edytować.
Żeby dodać nowy harmonogram należy kliknąć na przycisku ***Dodaj*** w lewy dolnym rogu ekranu. Domyślną nazwę na żółtym polu można zmienić na własną.
Klikając lub przesuwając w polu wyboru przedziałów czasowych prawym przyciskiem myszy możemy zaznaczyć na zielono aktywny przedział czasowy dla całego tygodnia. Następnie lewym przyciskiem myszy można wykasować aktywny terminarz w wybrany dzień tygodnia klikając na nazwie dnia z lewej strony (np. sobota, niedziela) lub bezpośrednio na zielonym polu usuwać przedziały 15 minutowe. W harmonogramie przeznaczonym dla kontrolerów serii KS3000 można zdefiniować do 3 przedziałów czasowych w ciągu doby - przykład obok.



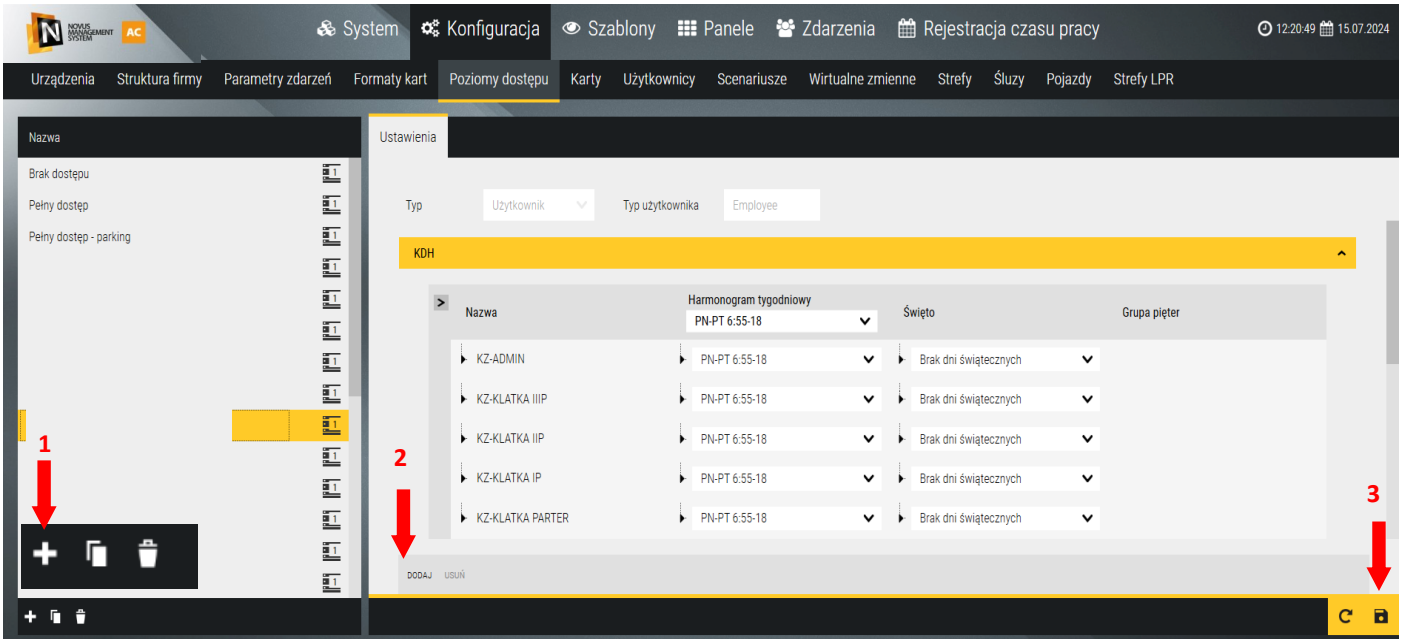
Do działania scenariuszy można zdefiniować dni specjalne (święta) klikając na przycisku po prawej stronie okna. W polach daty ustawiamy kursorami datę święta w kolejności: rok, miesiąc dzień. Następnie zaznaczamy checkbox *Dzień specjalny.* Jeżeli święto jest rekurencyjne zaznaczamy checkobox *Powtarzaj co roku.* Jeżeli święto zawiera więcej niż jeden dzień to zaznaczamy kolejne checkboxy. W dni świąteczne pola aktywności terminarza zostają lekko wyszarzone. Dla każdego terminarza można przypisać te same lub inne dni specjalne.



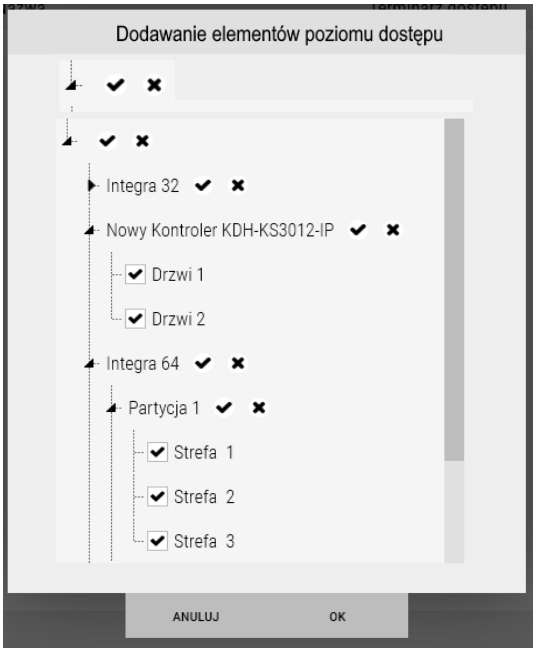
Do kontrolerów KD dni świąteczne definiowane są w zakładce *Konfiguracja / Dni świąteczne.*
W zakładce *Podgląd* możemy wyświetlić wygląd zdefiniowanego terminarza w formie tabeli

Zdefiniowany harmonogram można edytować lub usuwać zaznaczając go na liście i klikając na przycisk ***Usuń*** w lewym dolnym rogu okna.

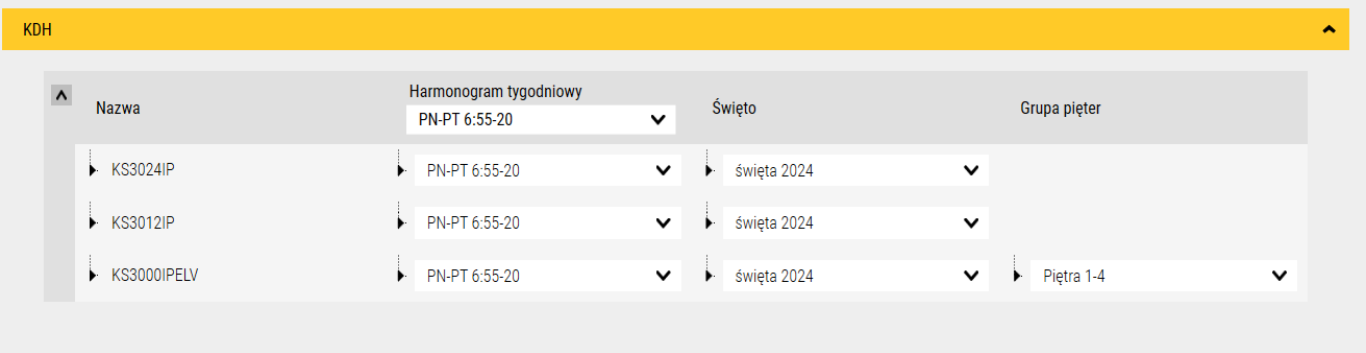
4.2 Poziomy dostępu



Zakładka *Poziomy dostępu* umożliwia zdefiniowanie poziomów dostępu przeznaczonych dla użytkowników kart oraz uprawnień decydujących o tym, do których partycji/stref centrali alarmowej użytkownik będzie miał dostęp. Poziom dostępu do systemu KD to zestaw uprawnień decydujący o tym, do których przejść i w jakim przedziale czasu użytkownik będzie miał dostęp. Szczegółowe uprawnienia do operacji na centrali alarmowej ustawiane są w oknie definiowania użytkownika - zakładka *Identyfikatory/System alarmowy.* W przypadku wind poziom dostępu określa dostęp do wybranych pięter.
Domyślnie zdefiniowane są dwa poziomy dostępu: *Brak dostępu* i *Pełny dostęp,* których nie można usnąć lub edytować.
Żeby dodać nowy poziom dostępu należy kliknąć na przycisku ***Dodaj*** w lewy dolnym rogu ekranu. Domyślną nazwę na żółtym polu można zmienić na własną. Następnie należy kliknąć na przycisk ***Dodaj*** w prawym oknie. Wyświetli się okno zawierające listę wszystkich dodanych uprzednio drzwi oraz wind i central. Należy zaznaczyć drzwi oraz windy (jako czytniki w kabinie), do których dany użytkownik będzie posiadał uprawnienia dostępu w określonym przedziale czasu i potwierdzić przyciskiem ***OK***.
Checkboxy nad listą umożliwiają szybkie odznaczanie i zaznaczanie wszystkich pozycji.



W prawym oknie zostanie wyświetlona tabela jak poniżej, zawierająca wybrany w poprzednim oknie drzwi i windy.



W drugiej kolumnie (*Harmonogram tygodniowy)* z rozwijanej listy należy wybrać harmonogram zgodnie z oczekiwanymi uprawnieniami dostępu.

W trzeciej kolumnie (*Święto)* z rozwijanej listy należy wybrać dzień świąteczny zgodnie z oczekiwanymi uprawnieniami dostępu.

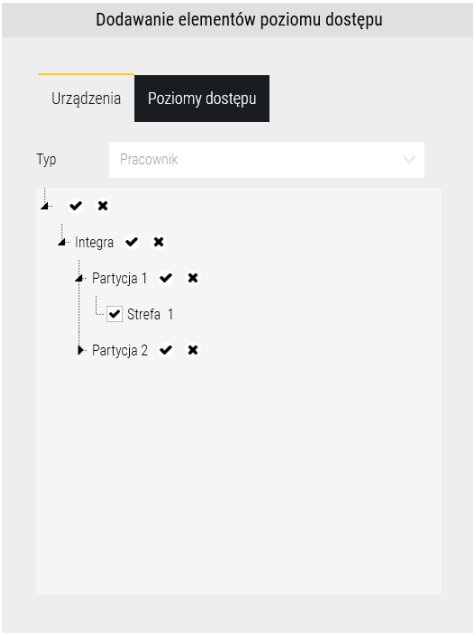
W czwartej kolumnie (*Grupa pięter)* z rozwijanej listy należy wybrać grupę pięter zgodnie z oczekiwanymi uprawnieniami dostępu.

Zapisać ustawienia klikając na ikonie ***dyskietki*** w prawym dolnym rogu okna konfiguracji.

Tak zdefiniowane poziomy dostępu będzie można przypisać jednemu lub większej liczbie użytkowników.

Ikona na dole lewego okna służy do kasowania całego poziomu dostępu, a w prawym do kasowania jednego wiersza, czyli wybranych drzwi. Natomiast ikona do kopiowania stworzonych już poziomów w celu ich edycji.

4.2.1 Poziomy dostępu - Systemy sygnalizacji włamania i napadu



Zakładka *Poziomy dostępu* umożliwia zdefiniowanie poziomów dostępu przeznaczonych dla użytkowników. Poziom dostępu to zestaw uprawnień decydujących o tym, do których partycji/stref użytkownik będzie miał dostęp.

Żeby dodać nowy poziom dostępu należy kliknąć na przycisku + w lewy dolnym rogu ekranu. Domyślną nazwę na żółtym polu można zmienić na własną.

Następnie należy kliknąć na przycisk ***Dodaj*** w prawym oknie.

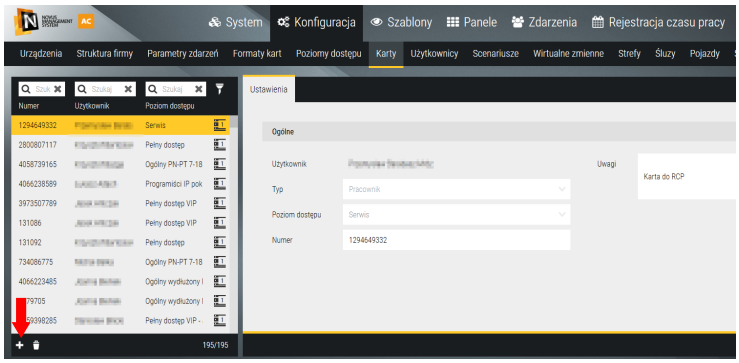
Wyświetli się okno zawierające listę wszystkich dodanych uprzednio urządzeń.

Należy zaznaczyć partycje oraz strefy, do których dany poziom będzie posiadał uprawnienia dotyczące dostępu i potwierdzić przyciskiem ***OK***.

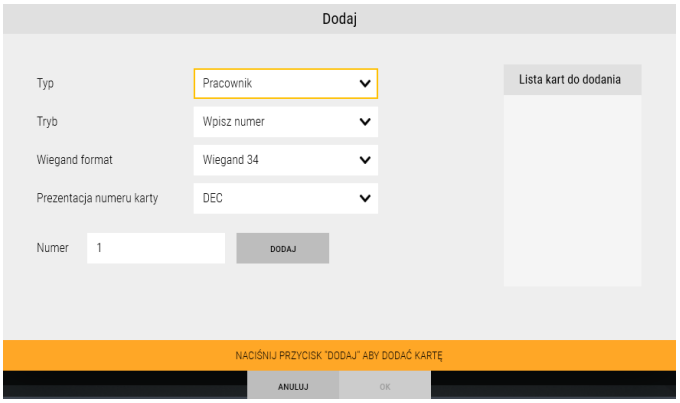
Checkboxy ✔ ✖ umożliwiają szybkie odznaczanie i zaznaczanie wszystkich pozycji.

4.3 Karty

Ta zakładka umożliwia utworzenie listy kart z numerami w celu ich późniejszego i szybszego przypisania dla dowolnego użytkownika.



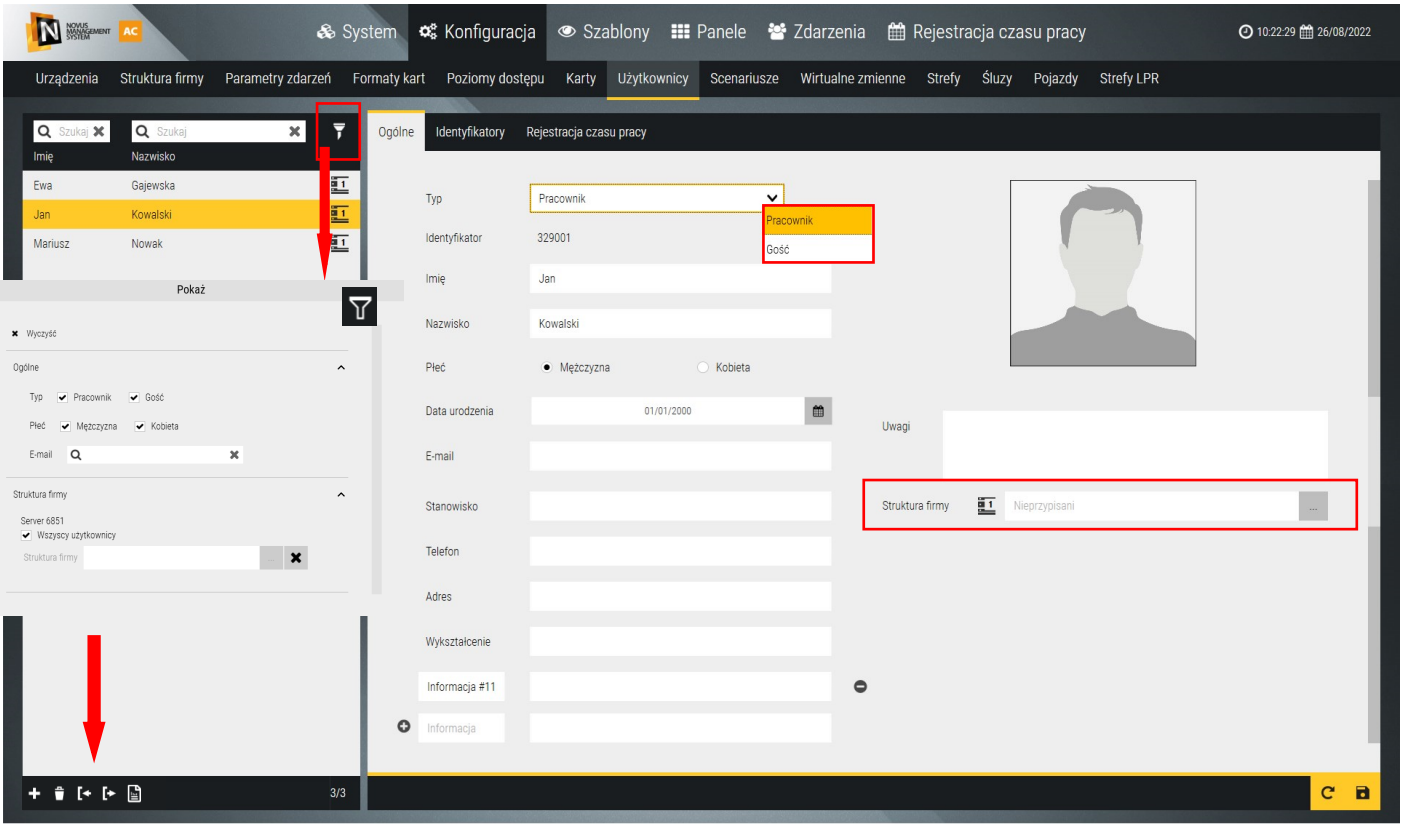
Po kliknięciu na przycisku ***Dodaj*** wyświetlane jest okno jak poniżej:



Szczegółowy opis tej procedury jest opisany jest w punkcie **4.4 Użytkownicy/Karty**. W tym oknie dodając karty przypisujemy je od razu dla danego użytkownika.

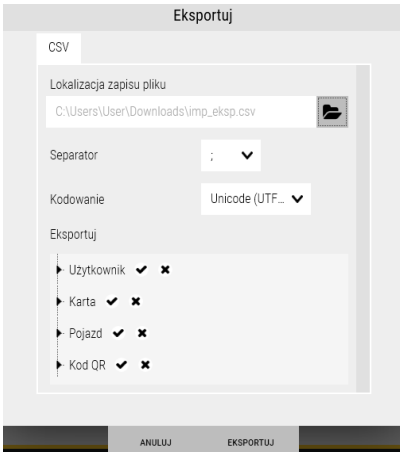
4.4 Użytkownicy

Ta zakładka umożliwia dodawanie do bazy systemu nowych użytkowników oraz przypisanie im danych osobowych, zdjęć oraz identyfikatorów (karta, PIN, odcisk palca). Możliwe jest przypisanie użytkownika do grupy RCP, co pozwala rejestrować i rozliczać jego czas pracy w oparciu o zdefiniowane harmonogramy i kalendarze (płatna licencja). Można też włączyć filtrację listy według typu. Nowa pozycja to przypisanie użytkownika do zdefiniowanej struktury firmy, co umożliwia generowanie raportów zdarzeń i RCP dla wybranych działów.



Użytkowników można dodać ręcznie lub importując dane z pliku. **Procedura importu** pliku znacznie przyspiesza ten proces w przypadku dużej liczby kart lub numerów tablic rejestracyjnych.

W celu wyeksportowania pliku zawierającego dane użytkowników należy wybrać opcję 
Pojawi się okno jak po prawej.
Domyślnie w oknie ***Eksportuj*** zaznaczone są wszystkie opcje możliwe do wyeksportowania. Należy wybrać te opcje, których **eksport ma dotyczyć (np. opcje *Użytkownik, Karta*)**, wybrać odpowiedni separator (domyślnie ;) oraz kodowanie (domyślnie Unicode UTF-8).

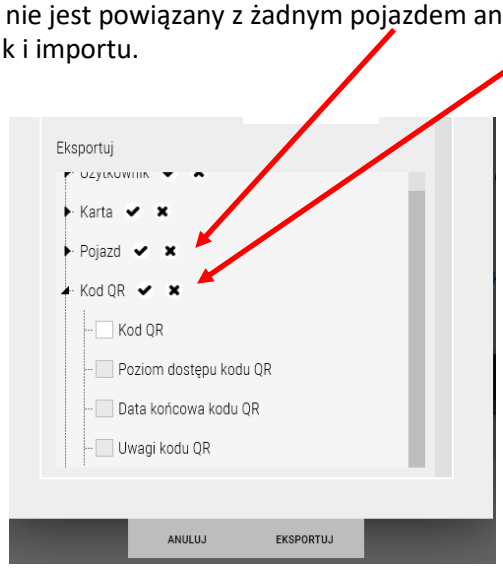


Przykład wyeksportowanego pliku z wybraną częścią opcji dostępnych dla pozycji *Użytkownik* oraz *Karta*:

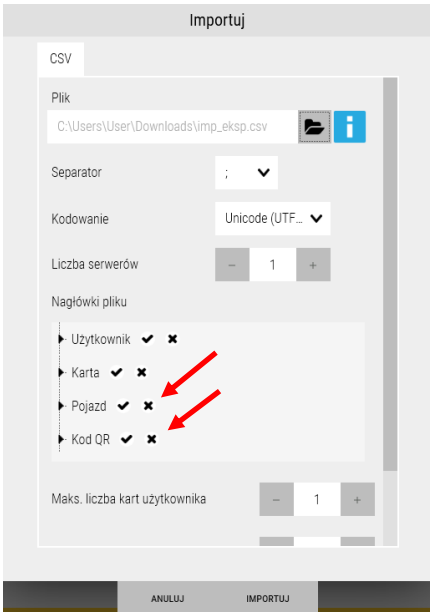
	A	B	C	D	E	F	G	H	I
1	Identyfikator	Typ użytkownika	Nazwa serwera	Imię	Nazwisko	Mężczyzna	Numer karty	Poziom dostę	Data końcowa karty
2	17014006	Pracownik	SRV Lokalny	Jan	Kowalski	Nie	11111	Pełny dostęp	

W celu wykonania importu danych wskazać plik z którego dane mają zostać zaimportowane, wybrać odpowiedni separator, kodowanie oraz określić maksymalną ilość kart, pojazdów oraz kodów QR znajdujących się w importowanym pliku. W pozycji *Nagłówki pliku* należy wybrać **koniecznie tylko** te dane które zawiera plik. W przypadku niepoprawnej konfiguracji import zakończy się niepowodzeniem. **Dla nowych użytkowników kolumna *Identyfikator* powinna być pusta.** Dla wcześniej dodanych będzie zawierała ID przypisane przez program i nie należy go zmieniać. Nazwa serwera musi być zgodna ze zdefiniowaną nazwą serwera na który dane mają zostać zaimportowane.

Przykład. W sytuacji, gdy użytkownik nie jest powiązany z żadnym pojazdem ani kodem QR, obie opcje należy odznaczyć zarówno podczas eksportu jak i importu.



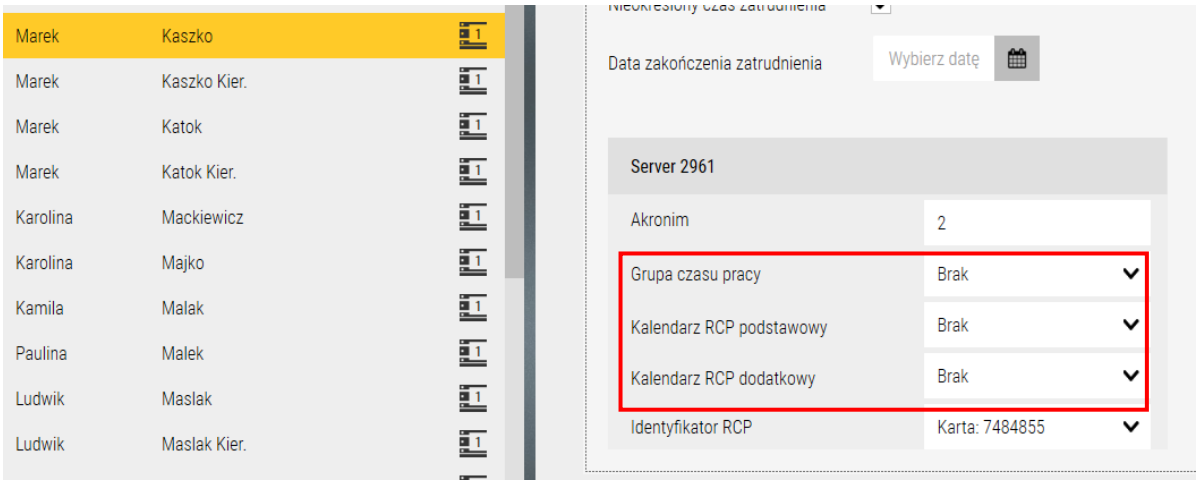
Aby zaimportować plik zawierający dane użytkowników należy wybrać opcję
Pojawi się okno jak po poniżej.



Fragment zaimportowanego pliku bez opcji *Pojazd* oraz *Kod QR*:

AA	AB	AC	AD	AE	AF	AG	AH	AI
Imię	Nazwisko	Mężczyzna	E-mail	Uwagi	Numer karty	Poziom dostępu karty	Data końcowa karty	Pierwsza karta otwierająca
Marek	Kaszko Kier.	Tak						
Luiza	Ponatko	Nie						
Paulina	Tasak Kier.	Nie						
Paulina	Tasak	Nie						
Karolina	Mackiewicz	Nie						
Paulina	Malek	Nie						
Agata	Tomczak	Nie						
Radosław	Utkasz	Tak						
Tadeusz	Retka	Tak						
Marek	Kaszko	Tak			7484855	Pracownicy Terminal RCP		Nie
Marek	Citko	Tak						

UWAGA! W zakładce *Użytkownicy/RCP - Ustawienia* nie ma możliwości eksportu danych dotyczących RCP.



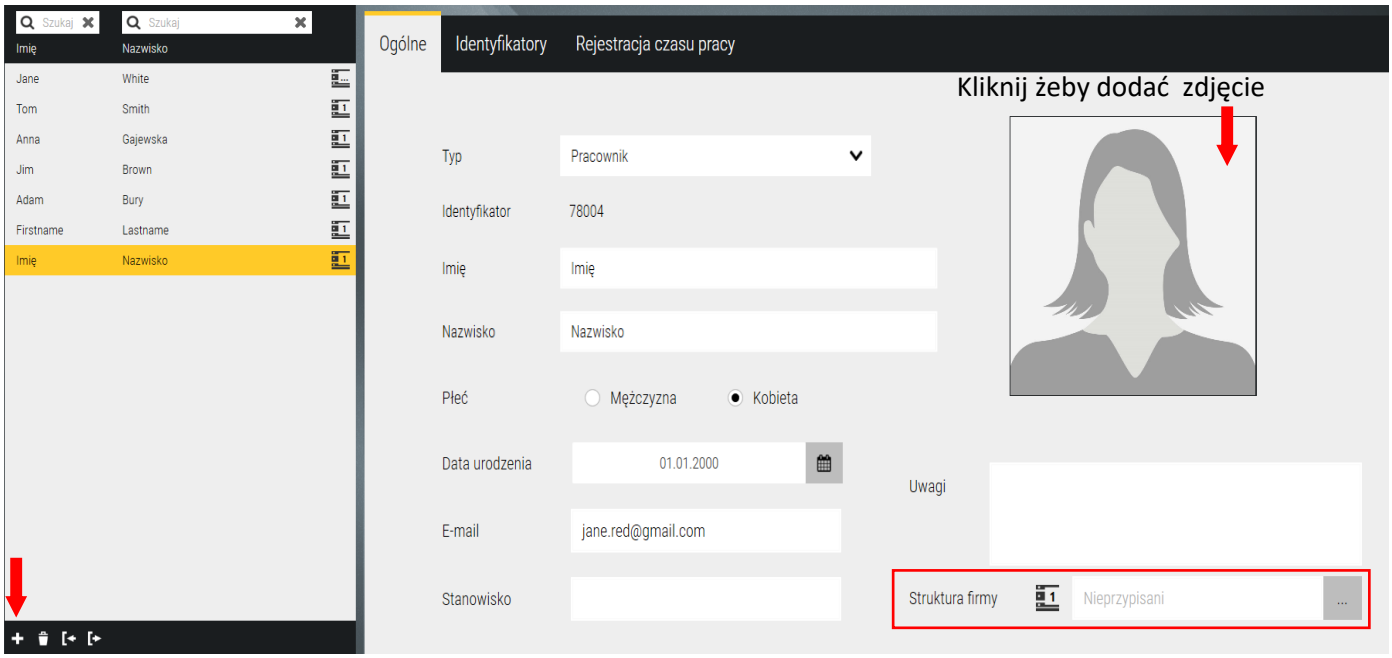
Jeżeli mają zostać zaimportowane dane związane z terminalem czasu pracy w kolumnach: *Grupa czasu pracy, Kalendarz czasu pracy, Kalendarz RCP dodatkowy,* to te pozycje należy najpierw zdefiniować w programie, a potem ich nazwy skopiować i wkleić w odpowiednie kolumny. Jeżeli po pierwszym imporcie chcemy dalej pracować na takim pliku (czyli zmieniać parametry dodanych wcześniej użytkowników lub dodawać nowych) to należy zawsze najpierw wykonać eksport aktualnej bazy danych i na takim pliku pracować.

Widok wyeksportowanego pliku CSV:

A	B	C	D	E	F	G	H	I
Identyfikator	Typ użytkownika	Nazwa serwera	Struktura firmy	Akronim	Grupa czasu pracy	Kalendarz czasu pracy	Kalendarz RCP dodatkowy	Data rozpoczęcia zatrudnienia
59008	Pracownik	Server 2961	Kierowcy	18				27.06.2025 00:00
11168	Pracownik	Server 2961	Kierowcy	14				18.06.2025 00:00
11166	Pracownik	Server 2961	Kierowcy	13				18.06.2025 00:00
65012	Gość	Server 2961	Kierowcy	28				27.06.2025 00:00

UWAGA! Podczas importu danych nie należy mieć otwartego pliku, z którego następuje import (np. w Excelu lub innym programie). W przeciwnym razie może pojawić się błąd:

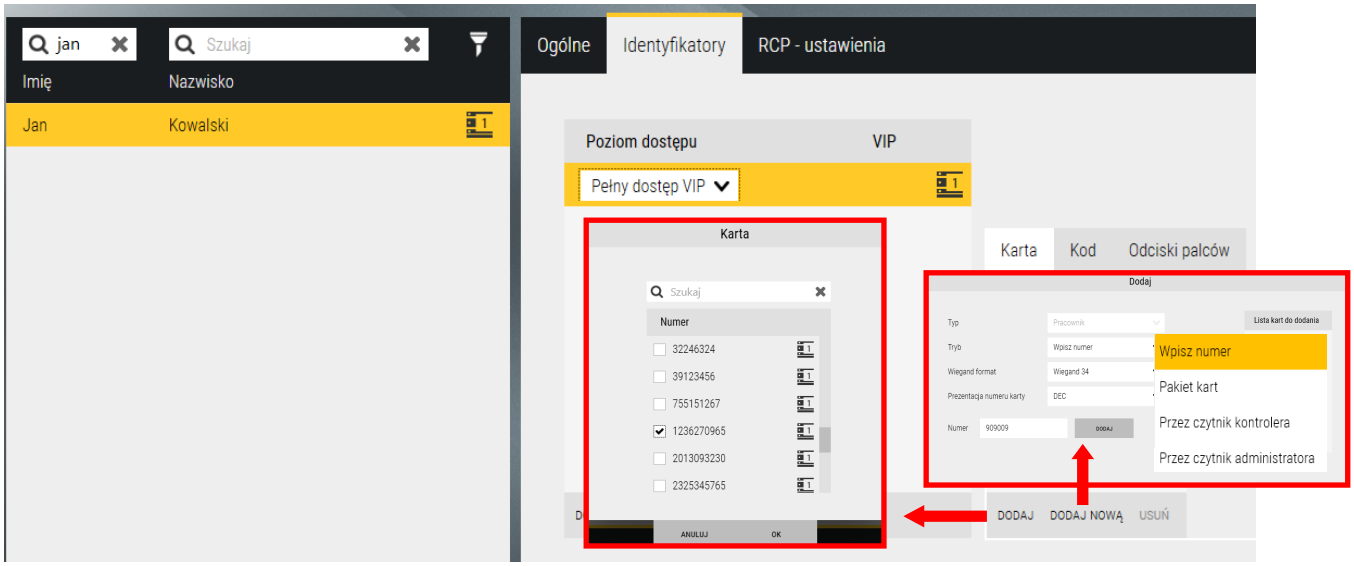
Dodawanie nowego użytkownika - kliknąć na przycisku ***Dodaj*** *(+)* w lewym dolnym rogu okna (żeby usunąć należy zaznaczyć i kliknąć ***Usuń*** *).* Następnie należy wypełnić pola formularza w prawym oknie. Oprócz pola z imieniem i nazwiskiem pozostałe pola nie są obowiązkowe. Można również dodać zdjęcie użytkownika z pliku klikając na przeznaczonym do tego polu z awatarem. W lewym oknie wyświetlana jest lista dodanych użytkowników.



Klikając na ikonę **„+”** można dodać kolejne pole informacyjne z edytowalną nazwą

Klikając na ikonę **„-”** można je usunąć

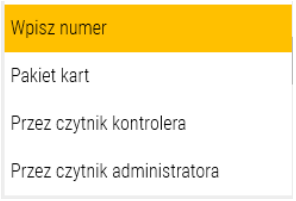
Dodawanie numeru identyfikatora - należy przejść do zakładki *Identyfikatory.* Program wyświetli okno jak poniżej:



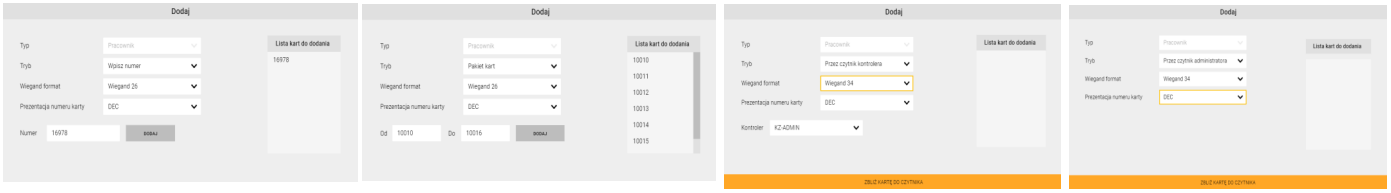
W oknie na poprzedniej stronie mamy dwa sposoby na przypisanie nowej karty użytkownikowi. Użytkownik może mieć więcej niż jedną kartę.

Po kliknięciu na przycisku ***Dodaj*** wyskakuje okienko jak po lewej stronie z listą kart dodanych wcześniej poprzez zakładkę *Karty.* Należy zaznaczyć numery kart, które chcemy przypisać użytkownikowi.

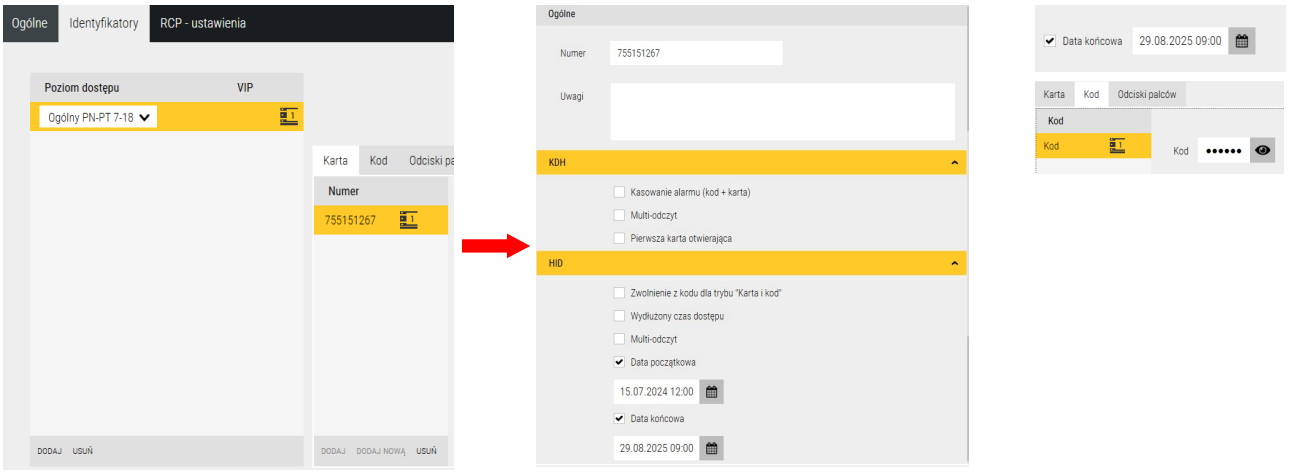
Po kliknięciu na przycisku ***Dodaj nową*** wyskakuje okienko jak po prawej. W oknie tym możemy wybrać jedną z czterech opcji wprowadzania numeru karty na listę:



- Ręczne wpisanie numeru w edytowalne pole (gdy znamy numer karty)
  Wpisany numer podlega weryfikacji, jeżeli już istnieje w bazie systemu to jest podświetlany na czerwono i nie można go dodać.
- Ręczne wpisanie pierwszego numeru z pakietu kart (pakiet z kolejnymi numerami) oraz końcowego
- Odczytanie karty na czytniku jednego z kontrolerów
- Przez czytnik USB administratora



Po dodaniu numerów kart i odcisków palca do listy wracamy do zakładki *Użytkownicy /Identyfikatory:*



Każda z kart ma oddzielne menu po prawej stronie okna, które jest wyświetlane po zaznaczeniu karty na liście.

Usunięcie karty z tej listy nie usuwa jej z systemu. Żeby usunąć kartę z bazy systemu należy przejść do zakładki *Karty.*

Poziom dostępu - należy wybrać z rozwijanej listy

Numer - wyświetlany w systemie unikatowy numer identyfikatora

Uwagi - pole tekstowe umożliwiające wprowadzenie dodatkowego opisu

KDH - Ustawienia funkcji identyfikatora dla kontrolerów serii 3000:

Kasowanie alarmu (kod + karta) - umożliwia wyłączenie aktywnego alarmu na kontrolerze gdzie dołączony jest czytnik, poprzez wpisanie kodu do kasowania alarmu (inny niż PIN, definiowany w ustawieniach kontrolera) i odczyt karty

Multi-odczyt - (2,3-krotny), uprawnia do odryglowania/zaryglowania drzwi na stałe lub włączenia/wyłączenia wyjścia ster.

Pierwsza karta otwierająca - opcja wymagana, gdy użytkownik ma posiadać uprawnienia do odblokowania dostępu na kartę dla innych użytkowników bez tego uprawnienia. Aktywna na czytnikach z włączona tą opcją.

Data końcowa - po zaznaczeniu w polu poniżej należy ustawić wymaganą datę, wpisać lub wybrać z kalendarza

HID®Aero® - Ustawienia funkcji identyfikatora dla kontrolerów serii HID®Aero®:

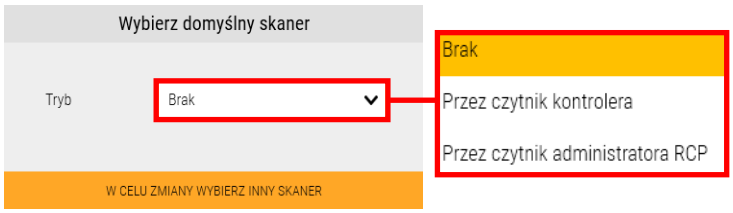
Zwolnienie z kodu dla trybu „Karta i kod" - Można ustawić wybranym użytkownikom, przejścia ustawione w trybie „karta i kod" nie będą wymagały wpisania kodu PIN.

Wydłużony czas na dostęp - czas odryglowania i otwarcia drzwi będzie taki jak w ustawieniach *Drzwi/Wydłużony czas na dostęp*

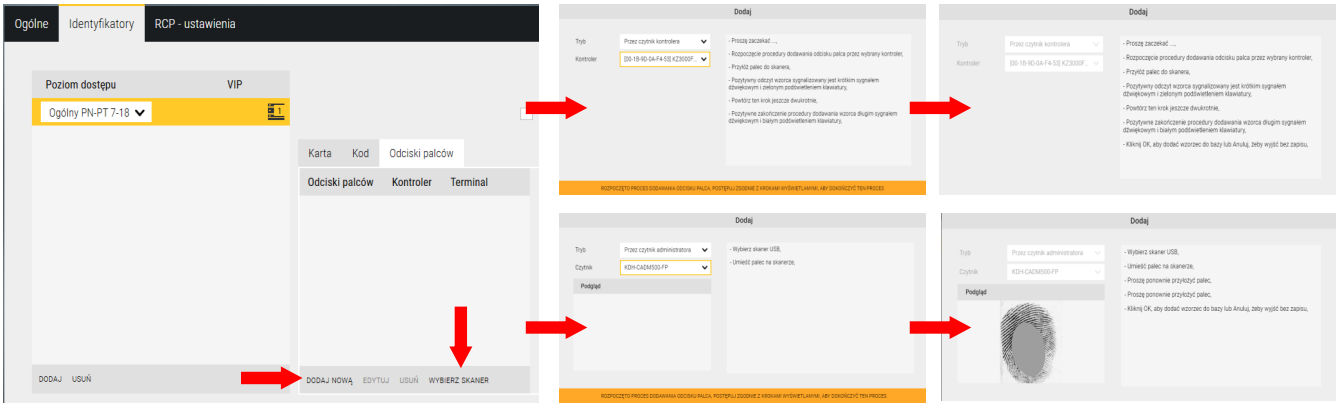
Multi-odczyt - (2-krotny), uprawnia do odryglowania/zaryglowania przejścia na stałe lub wł/wył wyjścia sterującego.

Data początkowa i końcowa - pozwala na wprowadzenie daty początku i końca aktywności identyfikatora.

Dodawanie odcisków palców - dotyczy **KDH-KS3000FP-IP-U_M i KDH-TA500CFP-IP-UMD**.
Żeby rozpocząć procedurę dodawania odcisków palców należy kliknąć na przycisku ***Wybierz skaner*** w sekcji *Odciski palców.*
Dla modeli KDH-KS3000FP-IP-U_M dodawanie przez wybór kontrolera z listy - ***Przez czytnik kontrolera***
Dla KDH-TA500CFP-IP-UMD dodawanie przez skaner **USB - KDH-CADM500-FP** - ***Przez czytnik administratora RCP***



Po wybraniu skanera należy kliknąć na przycisku ***Dodaj nowy***



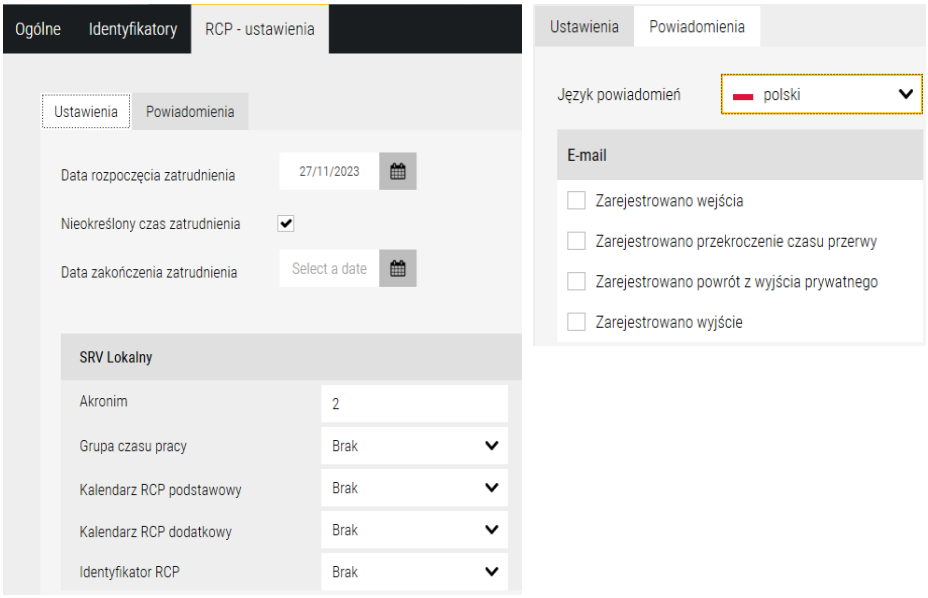
Dodawanie odcisków palców odbywa się poprzez skaner w wybranym kontrolerze biometrycznym. Można dodać do 3 odcisków. Po otwarciu okna jak powyżej i wybraniu kontrolera w prawym oknie wyświetli się instrukcja postępowania.

Po zakończeniu procedury (3 przyłożenia palca) należy kliknąć ***OK***, a po zamknięciu okna można w analogiczny sposób dodać odciski z kolejnych palców. Następnie kliknąć ***Zapisz*** w celu zapisania danych użytkownika do bazy i wysłania ich do kontrolerów.

Po dodaniu odcisków przy każdym z nich pojawi się informacja do czego może być wykorzystywany: Kontroler lub Terminal

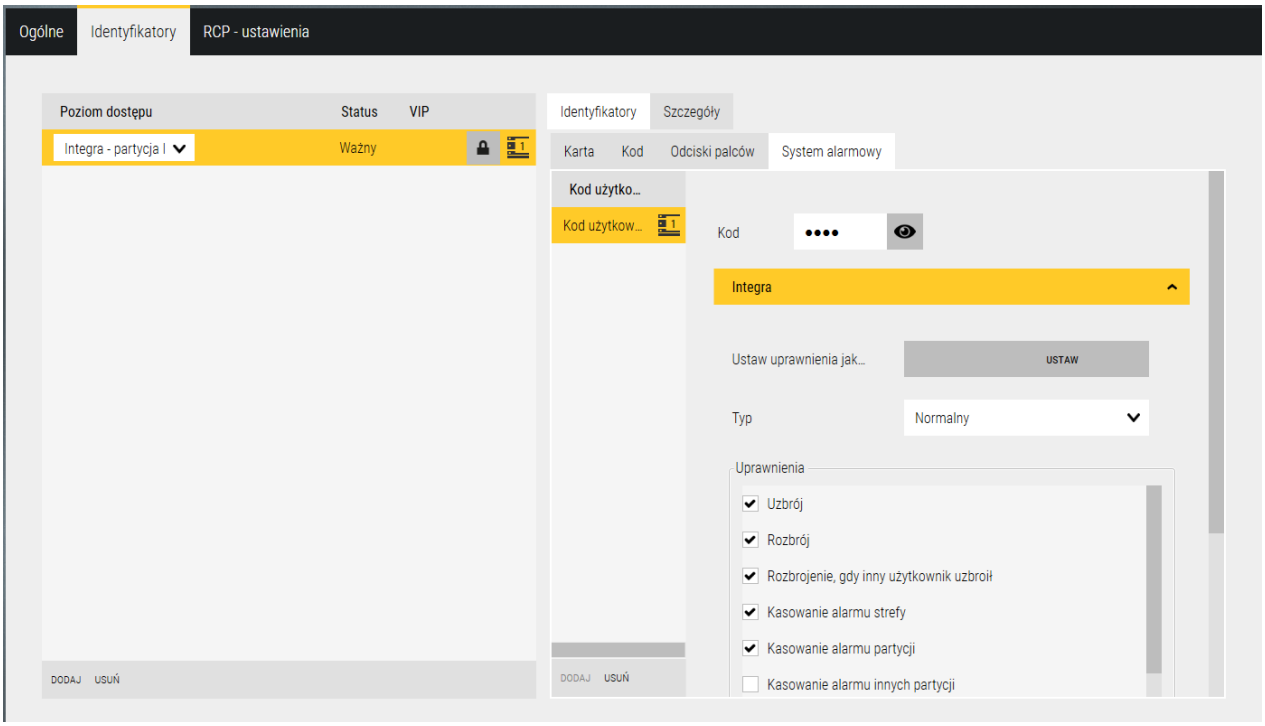
RCP ustawienia - w tej zakładce można zdefiniować użytkownikowi datę rozpoczęcia oraz zakończenia zatrudnienia, przypisać grupę i kalendarze czasu pracy oraz wybrać identyfikator dla rejestracji czasu pracy. Można również zdefiniować Akronim będący numerem identyfikacyjnym użytkownika. To umożliwia rejestrację we/wy na terminalu lub wybranych czytnikach oraz generowanie raportów czasu pracy.

W zakładce powiadomienia można zaznaczyć zdarzenia RCP po wystąpieniu, których zostanie wysłany email do pracownika z podaniem aktualnego czasu dla przepracowania dobowej normy czasu pracy.
Funkcjonalność rejestracji czasu pracy objęta jest płatną licencją.



4.4.1 Użytkownicy - Systemy sygnalizacji włamania i napadu

Dodawanie hasła użytkownika - po dodaniu identyfikatora zawierającego poziom dostępu z centralą alarmową przejść do zakładki *System alarmowy*.

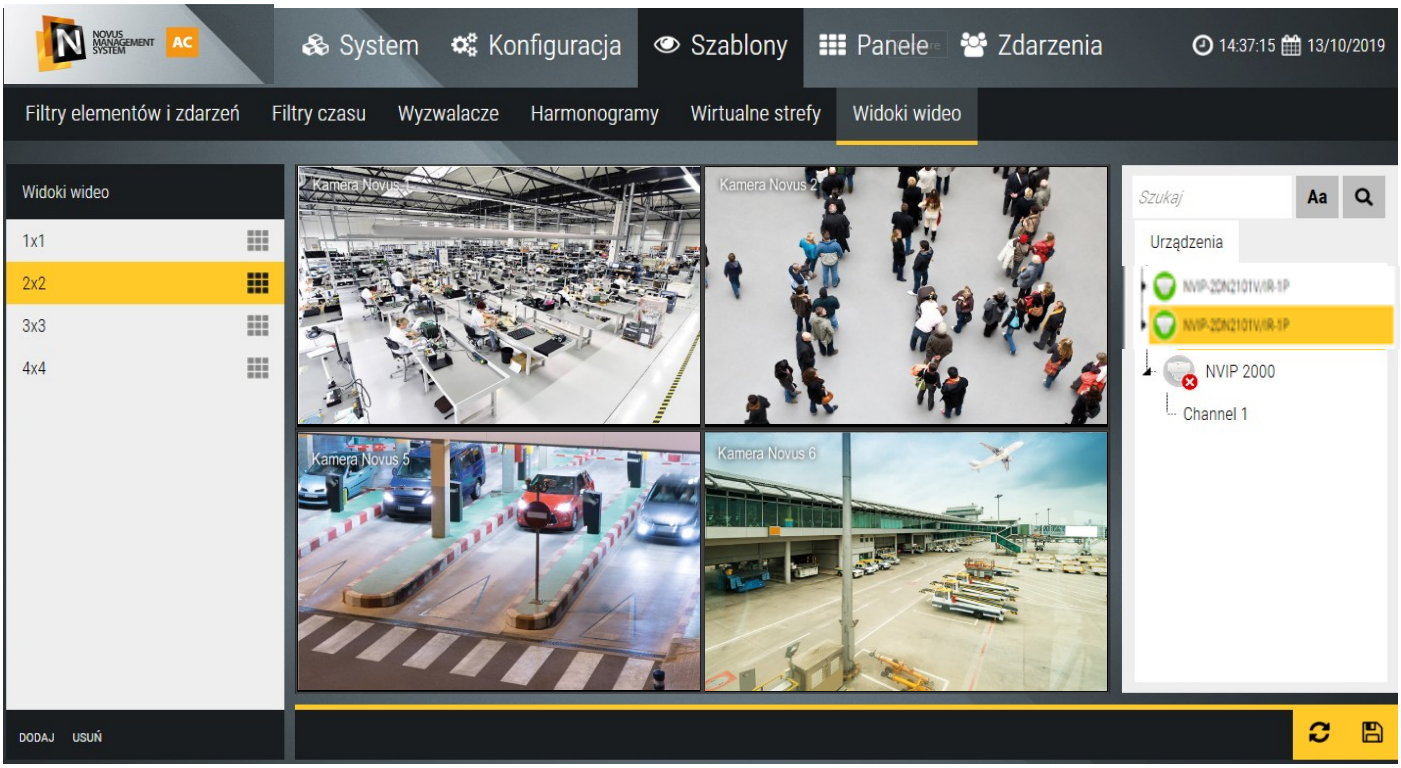


Po kliknięciu przycisku ***Dodaj*** należy zdefiniować hasło użytkownika oraz jego uprawnienia (lub skopiować od innego użytkownika). Minimalną długość hasła określamy przy dodawaniu centrali.

Rozdział 5. Szablony

5.1 Widoki wideo

W zakładce *Widoki wideo* możemy zdefiniować zestawy widoków wideo, które służą do wizualizacji i monitorowania stanu systemu oraz wyświetlania strumieni wideo z kamer lub rejestratorów dodanych do systemu. Lista zdefiniowanych widoków wideo jest wyświetlana w lewym oknie. Domyślnie zdefiniowane są cztery widoki z różnymi podziałami. Po kliknięciu przycisku ***Dodaj*** możemy dodać nowy widok, zmienić mu nazwę, przypisać mu podział klikając na ikonę w polu nazwy widoku. W celu przypisania kanałów wideo do widoku należy przeciągnąć je myszą z listy po prawej stronie w wybrane okno widoku. Widok wideo możemy wyświetlić klikając na jego nazwę w lewym oknie.



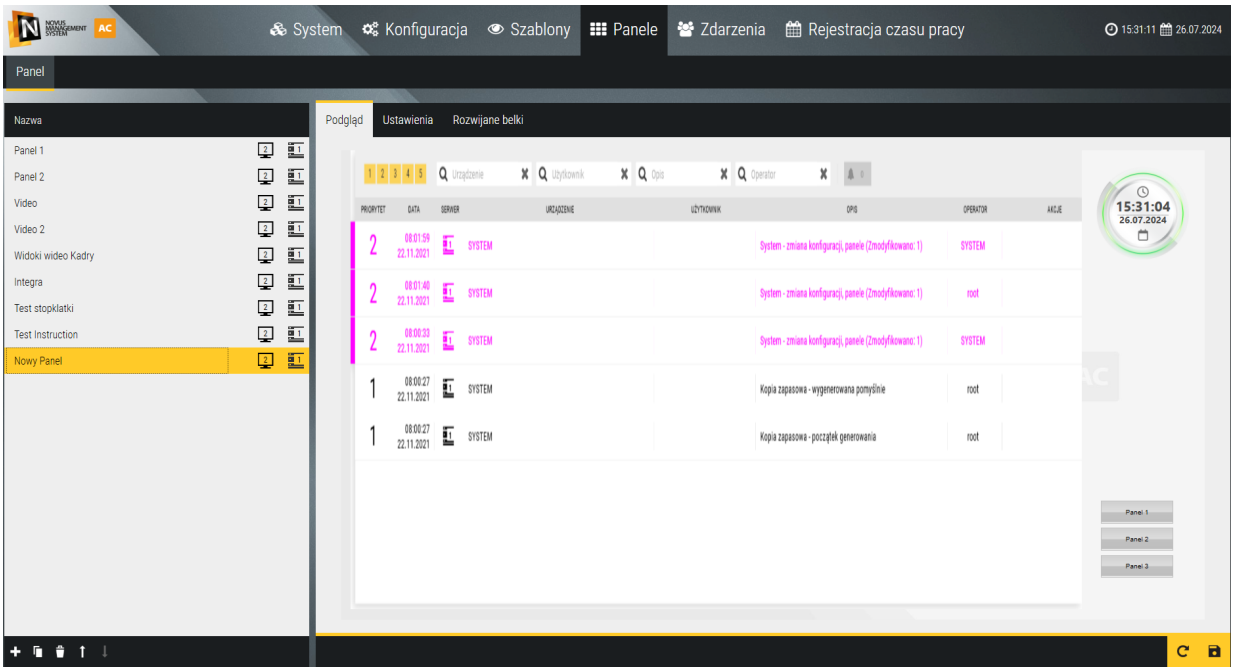
Zdefiniowanie domyślnie widoki można edytować i zmieniać według własnych potrzeb.

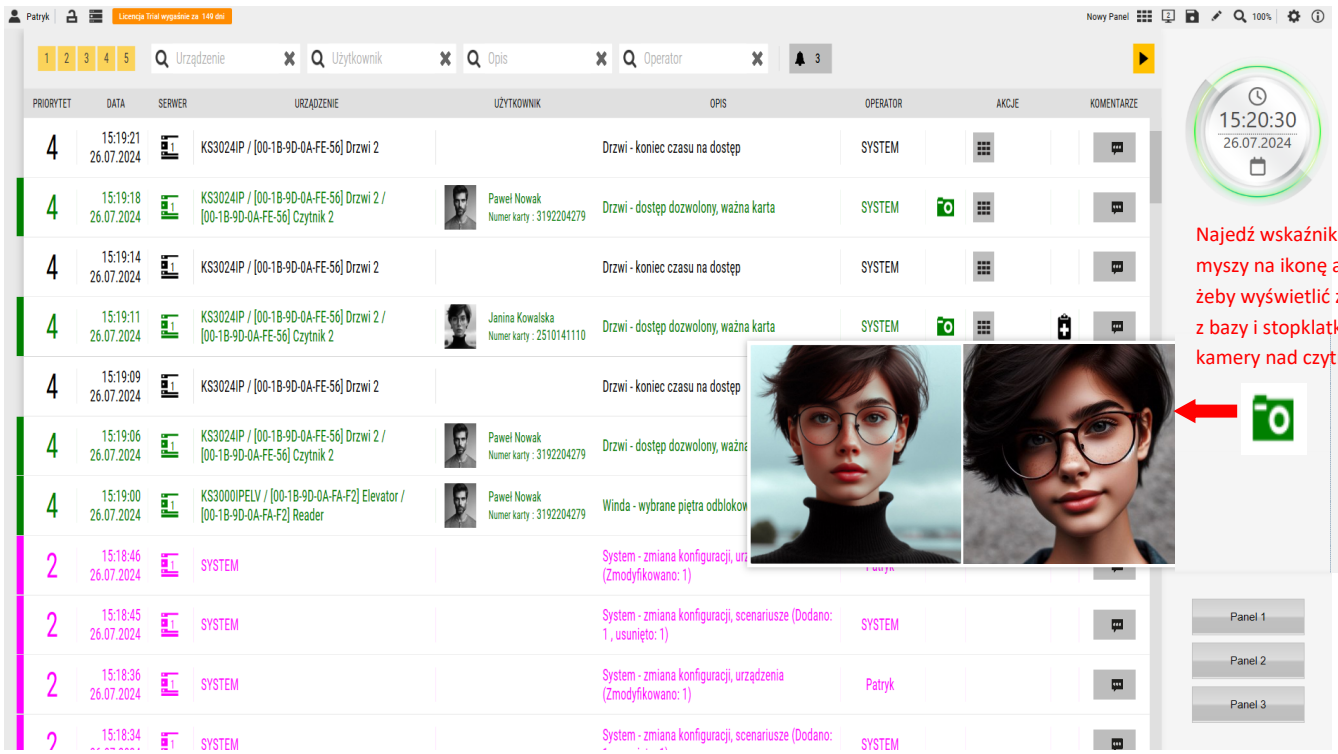
Klikając prawym przyciskiem na jednym z ekranów podziału, można go ustawić jako monitor ***HOTSPOT***. To pole podziału nie będzie miało na stałe przypisanej kamery. Będzie się na nim wyświetlała kamera kliknięta na oknie widoku przez użytkownika za pomocą **rolki** myszki (środkowy przycisk).

Po zdefiniowaniu widoków wideo kliknąć na przycisku ***Zapisz*** w prawym dolnym rogu.
Zdefiniowane *Widoki wideo* można wyświetlać na panelach w oknach wideo. Zdefiniowany domyślnie Panel 3 zawiera takie okno widoków.

Rozdział 6. Panele

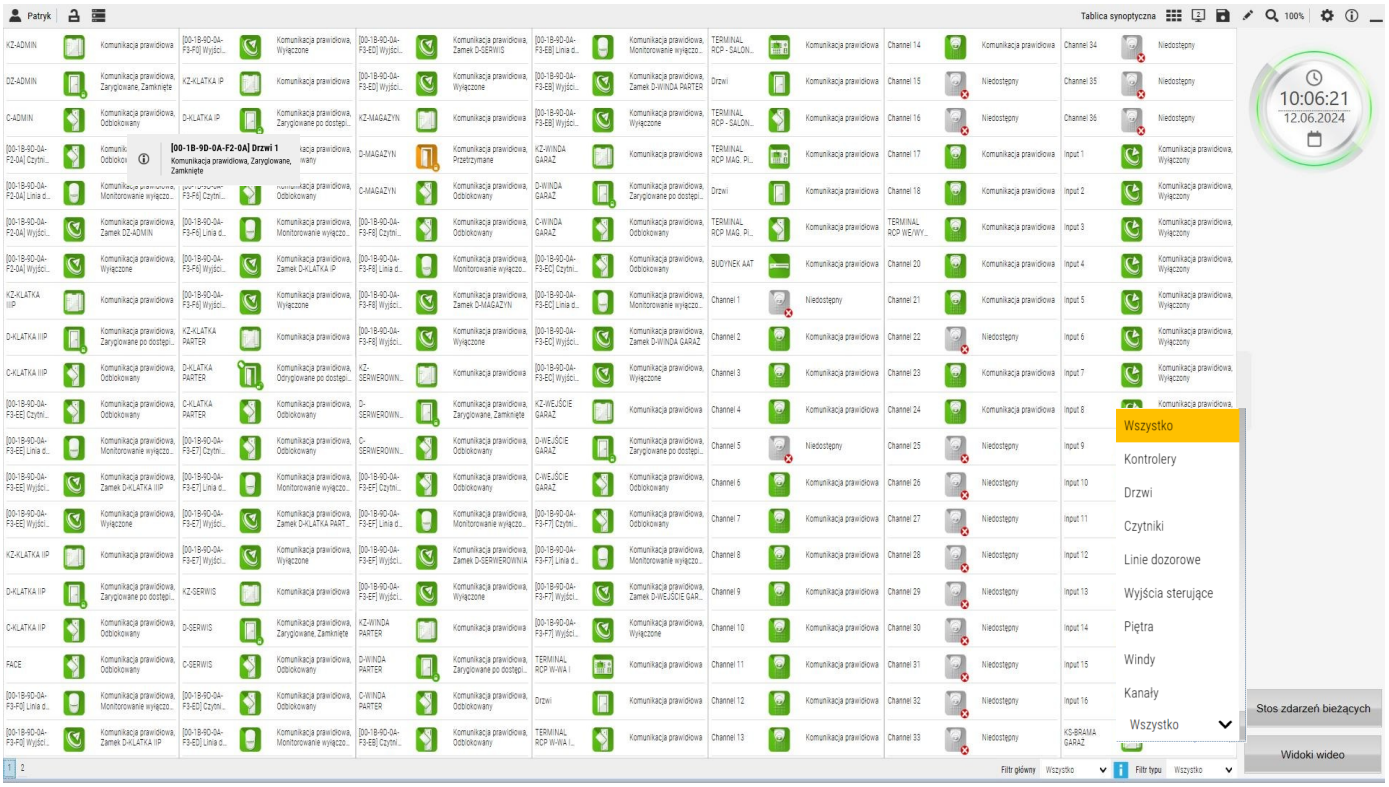
W zakładce *Panele* możemy zdefiniować panele, które służą do wizualizacji i monitorowania stanu różnych elementów systemu oraz wyświetlania zdarzeń i innych dodatkowych informacji. Panel możemy wyświetlić klikając na jego nazwę w lewym oknie.
Domyślny *Panel 1* zawiera: stos zdarzeń, zegar oraz przycisk z linkiem do *Panelu 2 i 3*.





Opis ikon na górnej belce znajduje się w tabeli na stronie 30.
Na *Stosie zdarzeń* wyświetlane są zdarzenia zgodnie z domyślnymi ustawieniami w zakładce *Parametry zdarzeń.*
Można je filtrować poprzez wpisanie słowa kluczowego w oknach z lupą, lub odznaczając wybrane żółte pola priorytetu.

Domyślny *Panel 2* zawiera: tablicę synoptyczną, zegar oraz przyciski z linkami do pozostałych paneli.



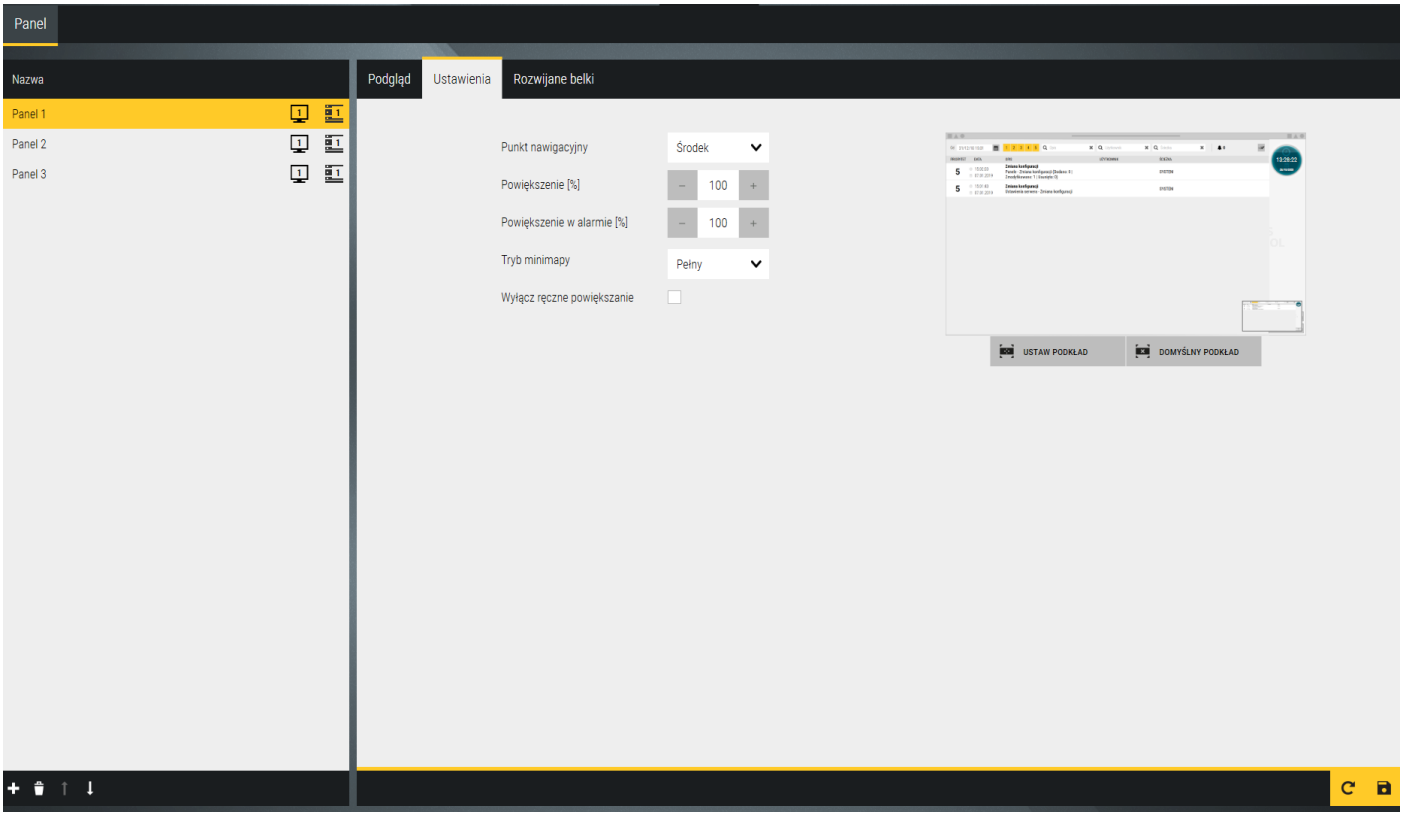
Panel 2 zawiera tablicę synoptyczną, do której dopisywane są automatycznie kolejne dodawane kontrolery wraz z elementami współpracującymi (drzwi, linie dozorowe, wyjścia sterujące, windy, piętra) oraz urządzenia telewizji dozorowej w postaci ikon przedstawiających ich aktualny stan. Stan ikon jest aktualizowany w czasie rzeczywistym (gdy jest prawidłowa komunikacja z urządzeniami). Ikony posiadają menu kontekstowe (lewy przycisk myszy).

W prawym dolnym rogu tablicy synoptycznej znajdują się dwa filtry umożliwiające wyświetlenie w tylko wybranych elementów :

- Filtr główny - zdefiniowany w zakładce *Szablony/Filtr elementów i zdarzeń* i ustawiony w trybie edycji panelu
- Filtr typu - umożliwia wyświetlanie elementów tylko jednego typu spośród dostępnych aktualnie na tablicy. Wybór z rozwijanej listy.

Domyślny *Panel 3* zawiera okno widoków wideo. Widoki wideo należy zdefiniować w zakładce *Szablony/Widoki wideo* jeżeli mamy w systemie dodane urządzenia telewizji dozorowej.

Żeby zdefiniować nowy panel należy kliknąć na przycisku ***Dodaj*** w lewym dolnym rogu okna ***Panele***.



Dodany panel pojawia się na liście w lewym oknie. W prawym wyświetlany jest podgląd tła panelu.

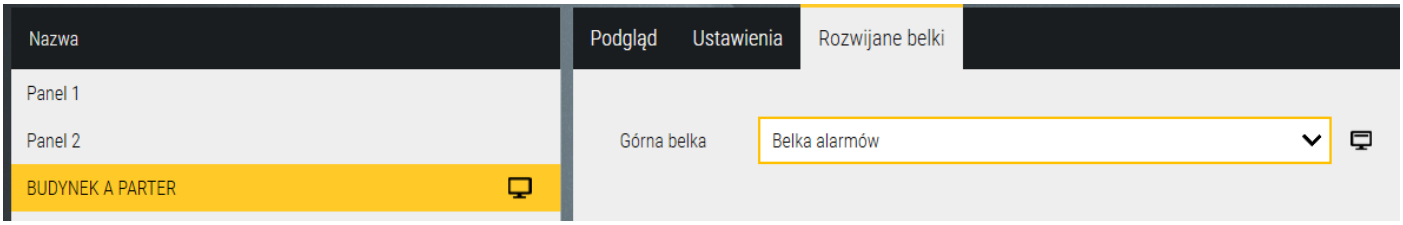
Zakładka *Ustawienia*

Nazwa - edytowalne pole na wpisanie nazwy panelu

Punkt nawigacyjny - punkt na panelu, do którego odnosi się proces , domyślnie ***Środek,*** inne pozycje pojawią się na tej liście po zdefiniowaniu dodatkowych punktów nawigacji na panelu

Powiększenie [%] - pozwala ustawić wartość powiększenia na panelu

Powiększenie w alarmie [%] - pozwala ustawić wartość powiększenia dla zdarzeniu alarmowego na panelu



Włącz ręczne powiększanie - pozwala ustawić powiększenia na panelu kółkiem myszy

Tryb mini mapy - do wyboru z rozwijanej listy tryb wyświetlania miniatury mapy: pełny, tylko tło, przezroczysty lub brak mini mapy.

Ustaw podkład - pozwala wybrać ze wskazanego folderu tło panelu w formacie bmp, jpg, png lub podkład domyślny

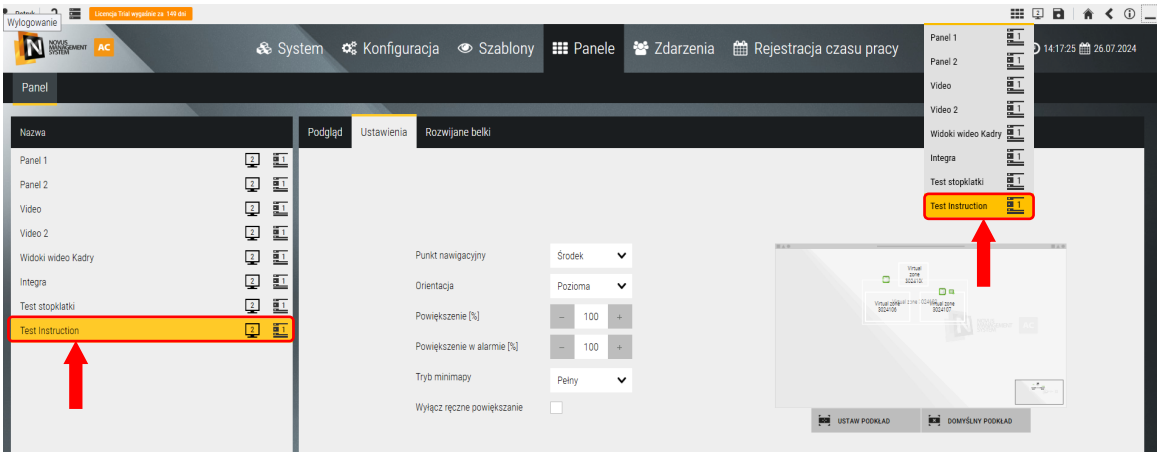
Zakładka *Rozwijane belki*

Górna belka - do wyboru z rozwijanej listy: belka alarmów lub brak

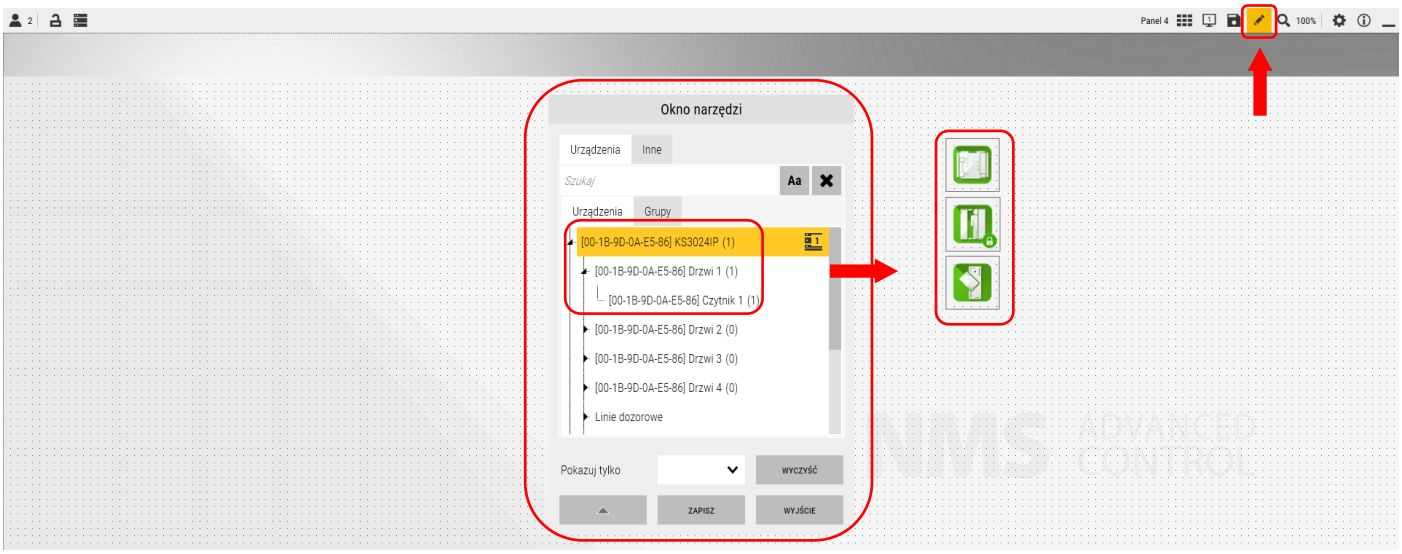
Po zdefiniowaniu zapisać ustawienia dla nowego panelu klikając na ikonie ***dyskietki*** w prawym dolnym rogu.

Klikając na nazwie panelu w lewym oknie możemy przejść do trybu wyświetlania i zweryfikować ustawienia.

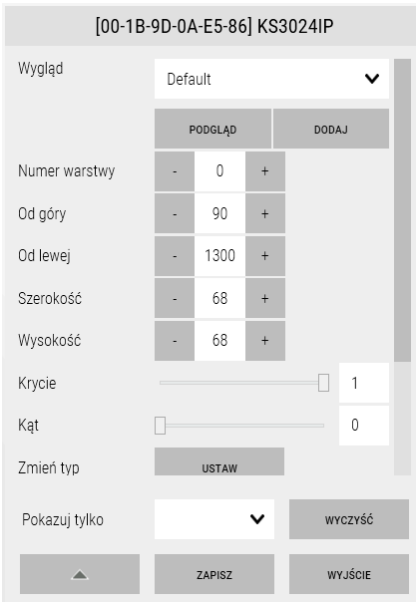
Konfiguracja zdefiniowanego panelu

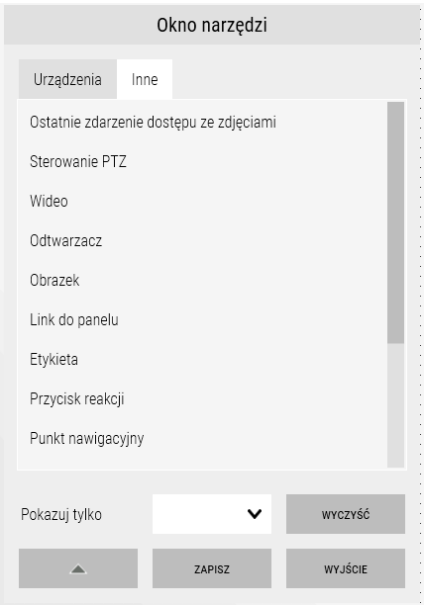


Po kliknięciu na liście w lewym oknie lub w prawym górnym rogu na wybranym monitorze wyświetli się okno jak poniżej.



Kliknięcie na ikonie ***Edycja*** w prawym górnym rogu otwiera ***Okno narzędzi***. W zakładce *Urządzenia* wyświetlana jest lista dodanych do bazy systemu urządzeń, które można przeciągać myszą do okna panelu. Po kliknięciu na ustawionym na panelu elemencie wyświetla się okno jego właściwości - jest różne dla różnych elementów. Oprócz urządzeń na panelu można również postawić ikony ***grup elementów*** oraz pozostałe elementy z zakładki *Inne*.

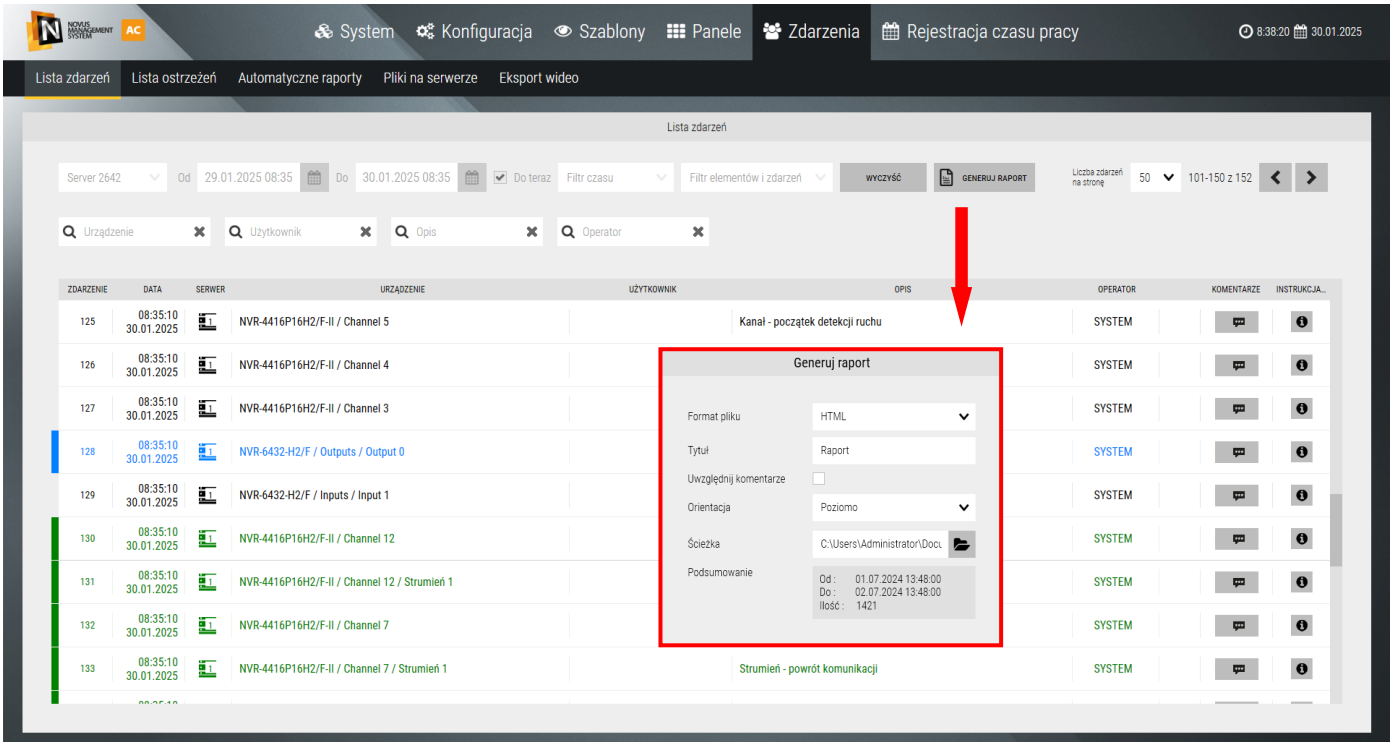




Rozdział 7. Zdarzenia i raporty

7.1 Lista zdarzeń

W zakładce *Lista zdarzeń* możemy wygenerować filtrowany raport. Wygenerowany raport jest wyświetlany na ekranie i może zostać zapisany jako plik na dysku (przyciski w prawym górnym rogu okna) w formacie *.CSV lub *.HTML (z możliwością eksportu do pdf).



Każda linia raportu zawiera znacznik daty i czasu, opis zdarzenia oraz powiązania z operatorem lub użytkownikiem karty oraz fizycznym elementem systemu, dotyczy zdarzenie.

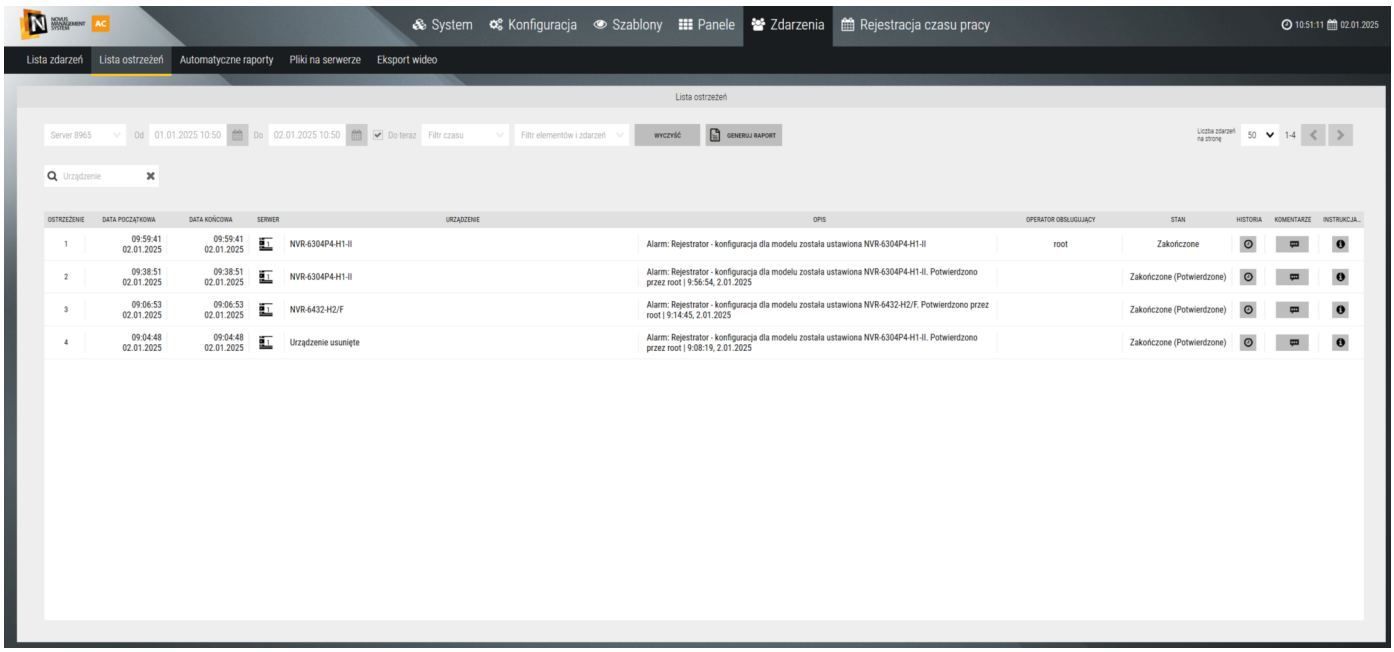
Na górze okna znajdują się okna filtrów dotyczących daty, przedziału czasowego (domyślnie ostatnie 24 godziny wstecz), oraz elementów i zdarzeń. Dzięki temu możliwa jest łatwiejsza analiza wydarzeń na obiekcie.

Po ustawieniu filtrów kliknąć na przycisku ***Szukaj***. W oknie zostanie wyświetlony raport.

W prawym dolnym rogu okna jest wyświetlana informacja o ilości zdarzeń w wygenerowanym raporcie. Maksymalna liczba zdarzeń wynosić 10 000. Jeżeli według ustawień filtrów ta wartość zostanie przekroczona wyświetlana jest taka informacja. Należy wówczas zmienić ustawienia filtrów.

7.2 Lista ostrzeżeń

W zakładce *Lista ostrzeżeń* możemy wygenerować filtrowany raport .Wygenerowany raport jest wyświetlany na ekranie i może zostać zapisany jako plik na dysku (przyciski w prawym górnym rogu okna) w formacie *.CSV lub *.HTML (z możliwością eksportu do pdf).



Każda linia raportu zawiera znacznik daty i czasu, opis zdarzenia oraz powiązania z operatorem lub użytkownikiem karty oraz fizycznym elementem systemu którego dotyczy ostrzeżenie.

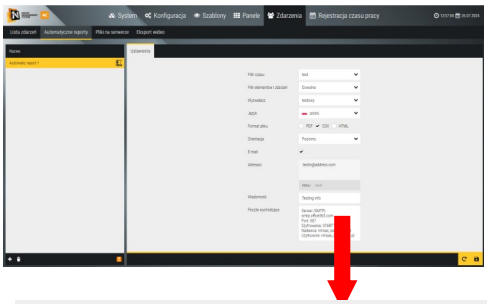
Na górze okna znajdują się okna filtrów dotyczących daty, przedziału czasowego (domyślnie ostatnie 24 godziny wstecz), oraz elementów i zdarzeń. Dzięki temu możliwa jest łatwiejsza analiza wydarzeń na obiekcie.

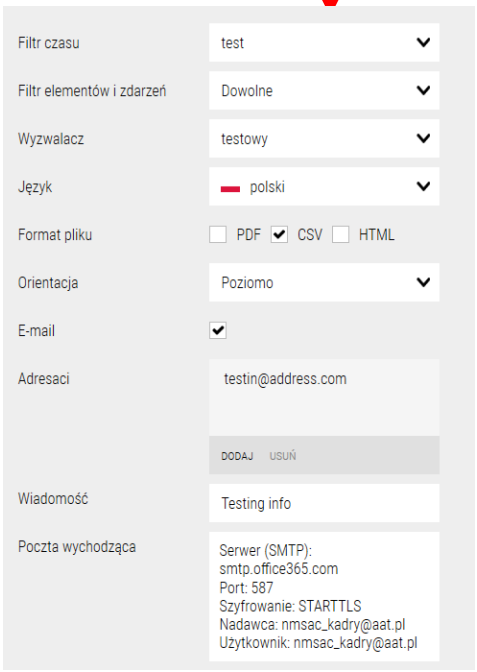
Po ustawieniu filtrów kliknąć na przycisku ***Szukaj***. W oknie zostanie wyświetlony raport.

W prawym dolnym rogu okna jest wyświetlana informacja o ilości ostrzeżeń w wygenerowanym raporcie. Maksymalna liczba zdarzeń wynosić 10 000. Jeżeli według ustawień filtrów ta wartość zostanie przekroczona wyświetlana jest taka informacja. Należy wówczas zmienić ustawienia filtrów.

7.3 Automatyczne raporty

W zakładce *Automatyczne raporty* możemy ustawić parametry nowego szablonu raportu generowanego automatycznie zgodnie z wybranym wyzwalaczem. Generowanie raportów automatycznych jest realizowane poprzez scenariusze. Dla ułatwienia w oknie tym został zaimplementowany prosty w obsłudze kreator takich scenariuszy. Analogicznie jak w przypadku raportów generowanych ręcznie mamy tutaj zestaw filtrów. Klikamy *Dodaj* i konfigurujemy nowy szablon automatycznego raportu.





Nazwa - edytowalne pole na wpisanie nazwy szablonu raportu

Filtr czasu - do wyboru z rozwijanej listy zdefiniowany uprzednio w oknie

Szablony/Filtry czasu

Filtr elementów i zdarzeń - do wyboru z rozwijanej listy zdefiniowany w oknie

Szablony/Filtry elementów i zdarzeń

Wyzwalacz - do wyboru z rozwijanej listy zdefiniowany uprzednio w oknie

Szablony/Wyzwalacze

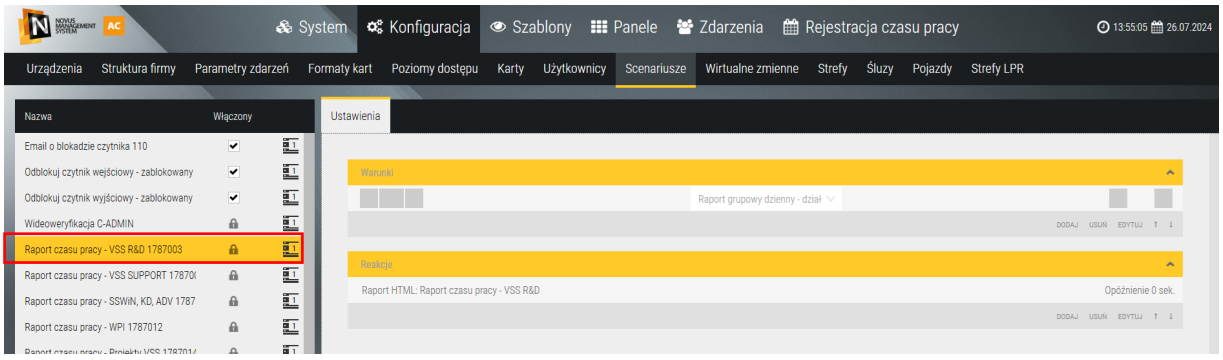
UWAGA! *Każda z trzech powyższych opcji po rozwinięciu zawiera pozycję „Dodaj", która otwiera okno do zdefiniowania nowego filtru lub wyzwalacza*

Język - do wyboru z rozwijanej listy: polski, angielski, rosyjski, azerski. Następne języki w trakcie tłumaczenia.

Format pliku - do wyboru jedne z formatów zapisu pliku: csv lub html

Orientacja - do wyboru pozioma lub pionowa orientacja strony do podglądu lub wydruku. Zalecana orientacja pozioma ze względu na ilość kolumn w raporcie i długie opisy.

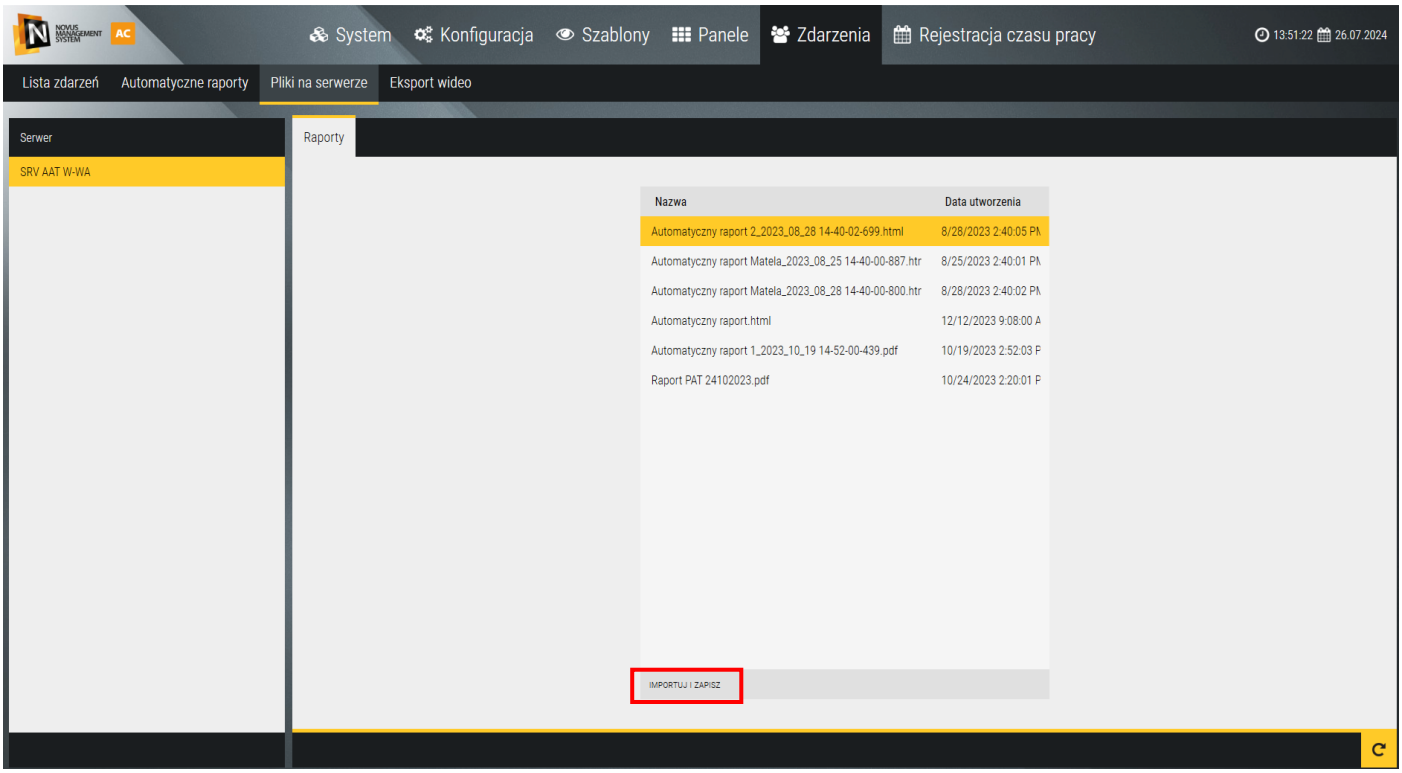
Email - pole do zaznaczenie jeżeli raport ma zostać wysłany jako email. Po zaznaczeniu poniżej wyświetlane są pola na wpisanie adresatów i tematu emaila. Żeby dodać adresata należy kliknąć na przycisku dodaj na dole tego pola i wpisać adres email w wyświetlonym okienku.



Po dokonaniu ustawień i kliknięciu ***OK*** w tle tworzony jest odpowiedni scenariusz, który możemy wyświetlić w zakładce *Konfiguracja / Scenariusze.*

7.4 Pliki na serwerze

Raporty generowane automatycznie zgodnie z przypisanym w szablonie wyzwalaczem zapisywane są w archiwum raportów na komputerze na którym jest zainstalowana usługa serwera NOVUS MANAGEMENT SYSTEM AC. Można zmienić tą ścieżkę w zakładce *System.*



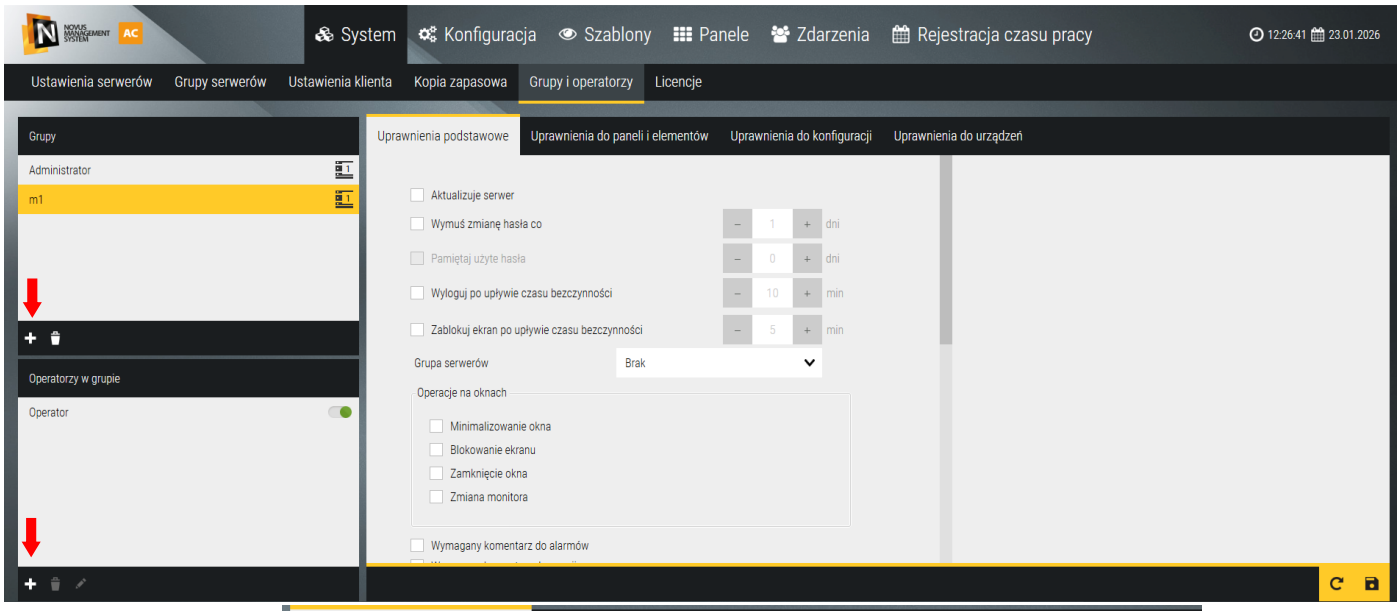
Na stacji klienta, która jest skomunikowana z serwerem widzimy w oknie jak powyżej (zakładka *Pliki na serwerze*) listę wygenerowanych automatycznie raportów. Po zaznaczeniu raportu na liście można go skopiować na stację klienta do wskazanego folderu.

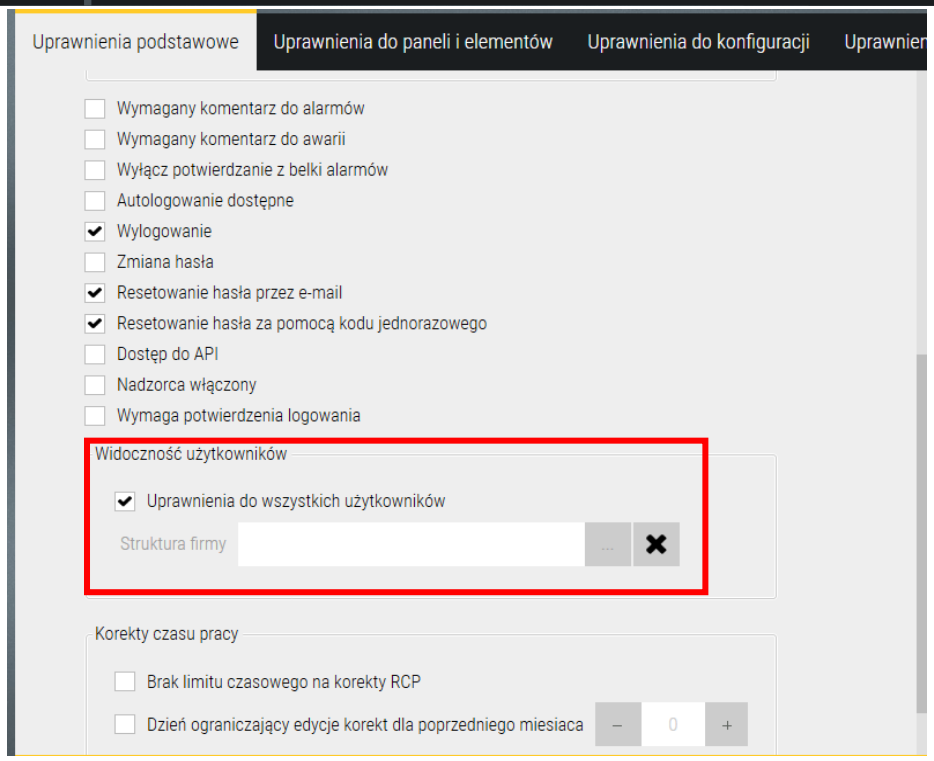
Rozdział 8. Ustawienia systemowe

W zakładce *System* możemy między innymi dodać nowych operatorów wraz z uprawnieniami dotyczącymi dostępu do programu, ustawić język dla operatora, wykonać kopię systemu lub ją przywrócić oraz rozszerzyć licencje.

8.1 Grupy i operatorzy

Domyślnie zdefiniowana jest jedna grupa operatorów o nazwie *Administrator* z pełnymi uprawnieniami do programu i systemu. Klikając na przycisku ***Dodaj*** w lewym górnym oknie możemy dodawać następne grupy z ograniczonymi uprawnieniami. Po zaznaczeniu grupy w górnym oknie można do niej dodawać operatorów. Domyślnie w grupie *Administrator* zdefiniowany jest jeden operator *root* z pełnymi uprawnieniami. Uprawnienia definiuje się dla grupy (nie dla poszczególnych operatorów), dla nowej grupy operatorów należy ustawić je w kolejnych zakładkach.
W zakładce *Uprawnienia podstawowe* znajduje się szereg checkboxów, które należy zaznaczyć, żeby przypisać wybrane opcje.

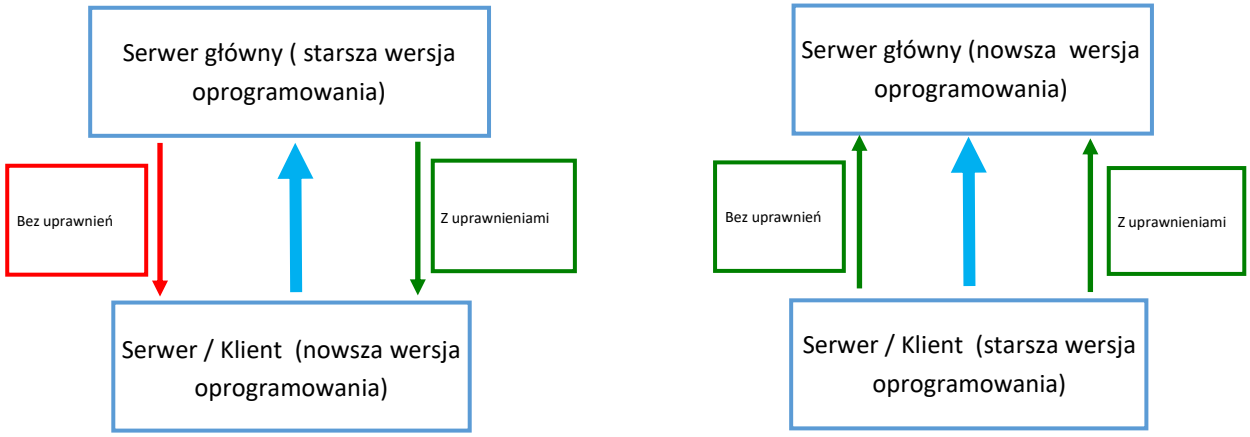




Uprawnienia podstawowe

Aktualizuje serwer - uprawnienie umożliwiające operatorowi przeprowadzenie aktualizacji serwera oraz klienta oprogramowania NOVUS MANAGEMENT SYSTEM AC w trakcie logowania pomiędzy komputerami z różnymi wersjami oprogramowania.
W przypadku logowania ze starszej wersji oprogramowania do nowszej, aktualizacja klienta lub serwera wykonywana jest niezależnie od posiadania tego uprawnienia.
Natomiast przy logowaniu z nowszej wersji oprogramowania do starszej, przeprowadzenie aktualizacji jest możliwe wyłącznie wtedy, gdy operator posiada włączone uprawnienie *Aktualizuje serwer* - w przeciwnym wypadku aktualizacja nie zostanie wykonana.

UWAGA! Aby aktualizacja w kierunku nowsza wersja → starsza wersja była możliwa, operator musi posiadać włączone uprawnienie *Aktualizuje serwer* na koncie, na które następuje logowanie. Na koncie root uprawnienie to jest włączone domyślnie.



Opis schematu:

- Zielone strzałki oznaczają możliwość aktualizacji serwera/klienta oprogramowania.
- Czerwona strzałka oznacza brak możliwości aktualizacji serwera/klienta oprogramowania.

Wymuś zmianę hasła co - wymusza cykliczną zmianę hasła operatora po określonej liczbie dni.
Pamiętaj użyte hasła - uniemożliwia ponowne użycie ostatniego hasła w ramach bieżącego cyklu wymuszonej zmiany hasła. Ta opcja jest dostępna wyłącznie po włączeniu opcji *Wymuś zmianę hasła co*.
Wyloguj po upływie czasu bezczynności - automatycznie wylogowuje operatora po wskazanym czasie braku aktywności.
Zablokuj ekran po upływie czasu bezczynności - blokuje aplikację po określonym czasie bezczynności (bez wylogowania).
Grupa serwerów - określa, do jakiej grupy serwerów operator ma przypisany dostęp.

Minimalizowanie okna - umożliwia minimalizowanie okna aplikacji.
Blokowanie ekranu - pozwala ręcznie zablokować ekranu aplikacji.
Zamknięcie okna - umożliwia zamknięcia okna aplikacji.
Zmiana monitora - umożliwia zmianę monitora, na którym wyświetlane jest okno aplikacji.

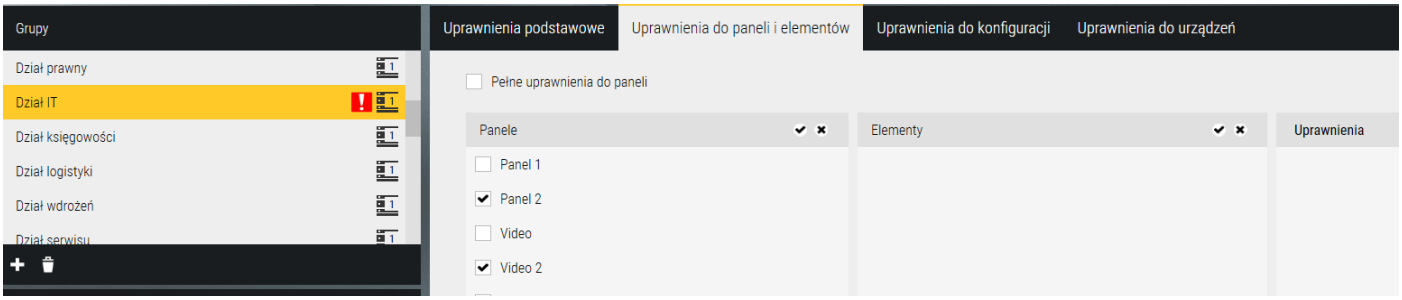
Wymagany komentarz do alarmów - wymusza dodanie komentarza przy obsłudze alarmu.
Wymagany komentarz do awarii - wymusza dodanie komentarza przy obsłudze awarii systemu.
Włącz potwierdzanie z belki alarmów - umożliwia potwierdzanie alarmów bezpośrednio z belki alarmowej.

Autologowanie dostępne - pozwala na automatyczne logowanie operatora do aplikacji bez ponownego podawania danych logowania.
Wylogowanie - umożliwia ręczne wylogowanie operatora z aplikacji.
Zmiana hasła - pozwala operatorowi samodzielnie zmienić swoje hasło.
Resetowanie hasła przez e-mail - umożliwia reset hasła przy użyciu linku wysyłanego na adres e-mail.
Resetowanie hasła za pomocą kodu jednorazowego - umożliwia reset hasła z użyciem jednorazowego kodu autoryzacyjnego.

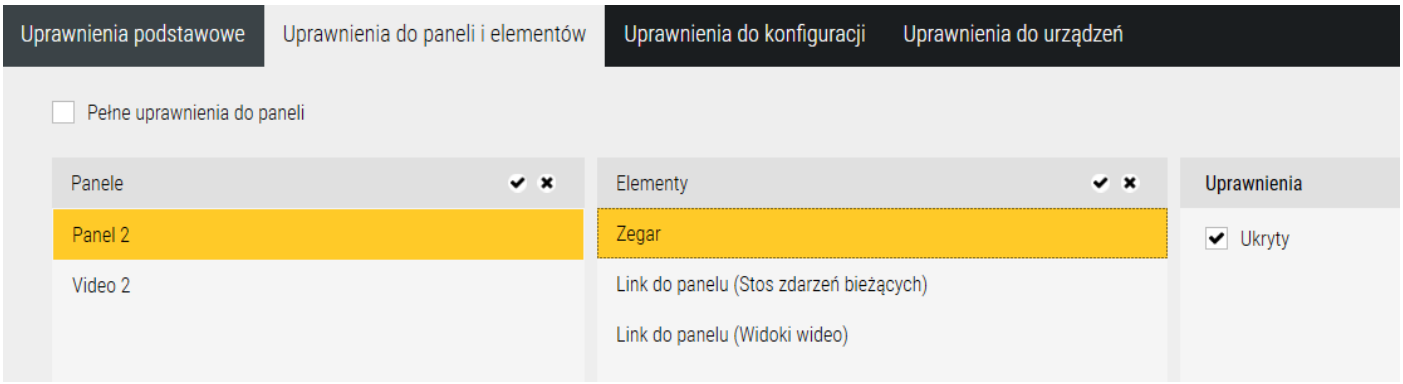
Dostęp do API - pozwala na korzystanie z interfejsu API systemu NOVUS MANAGEMENT SYSTEM AC.
Nadzorca włączony - nadaje operatorowi uprawnienia nadzorcy (rozszerzone uprawnienia administracyjne).
UWAGA! Funkcja Nadzorca realizuje kontrolę pracowników służb ochrony obiektu monitorujących system przy stacjach operatorskich w losowych przedziałach czasu. Gdy jest aktywna wymaga potwierdzania w wyświetlanym oknie i jest to rejestrowane.
Wymaga potwierdzenia logowania - wymusza dodatkowe potwierdzenie podczas logowania poprzez zatwierdzenie logowania przez innego operatora.

Uprawnienia do wszystkich użytkowników - umożliwia podgląd i zarządzanie wszystkimi użytkownikami w systemie.
Struktura firmy - ogranicza lub definiuje widoczność użytkowników zgodnie ze strukturą organizacyjną.
UWAGA! Domyślnie dla nowo utworzonej grupy nie są przypisani żadni użytkownicy. Aby to zmienić należy zaznaczyć opcję *Wszyscy użytkownicy* lub wybrać użytkowników zgodnie ze strukturą firmy.
Brak limitu czasowego na korekty RCP - użytkownik może edytować i korygować wpisy czasu pracy bez ograniczenia czasowego.
Dzień ograniczający edycję korekt dla poprzedniego miesiąca - określa do którego dnia bieżącego miesiąca można jeszcze edytować korekty czasu pracy za poprzedni miesiąc.

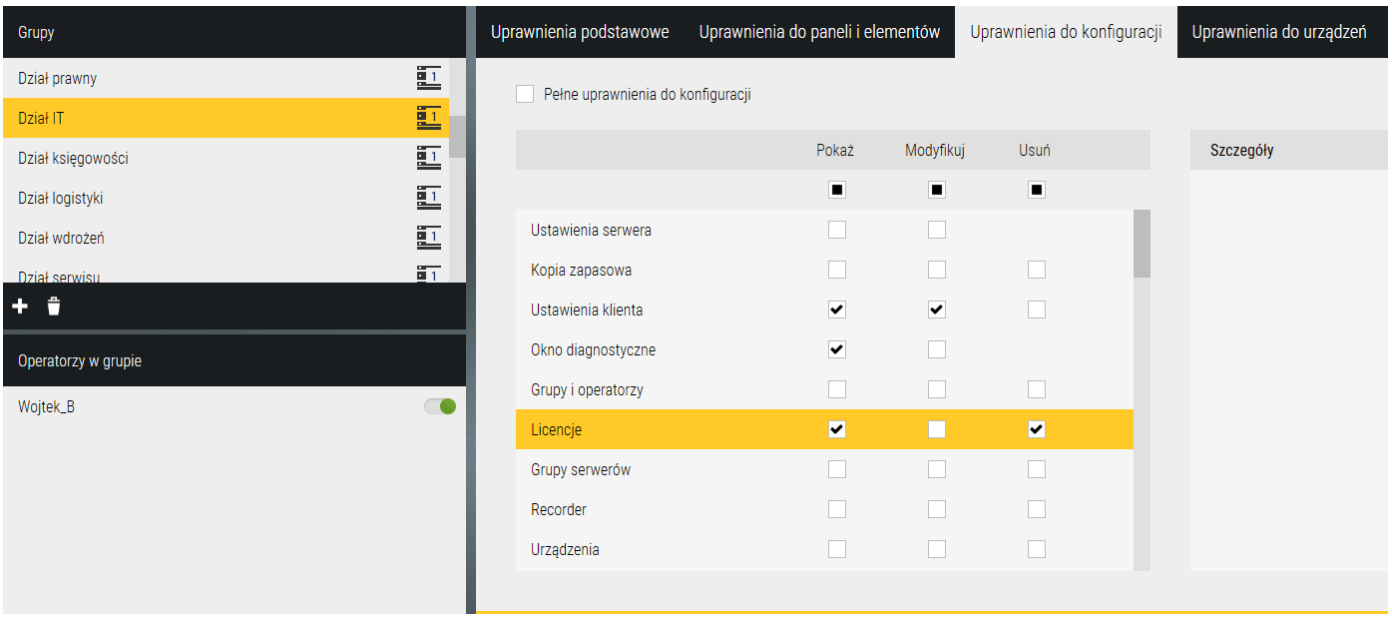
Uprawnienia do paneli i elementów



Po kliknięciu na przycisku na dole okna w pierwszej kolumnie wyświetlana jest lista dostępnych paneli - należy zaznaczyć te do których operatorzy z tej grupy mają mieć dostęp i ***OK***.
W drugiej kolumnie (*Elementy)* wyświetlana jest lista elementów osadzonych na tym panelu. Po zaznaczeniu wybranego elementu na tej liście w trzeciej kolumnie (*Uprawnienia*) możemy wybrać opcję ukrycia tego elementu na panelu.

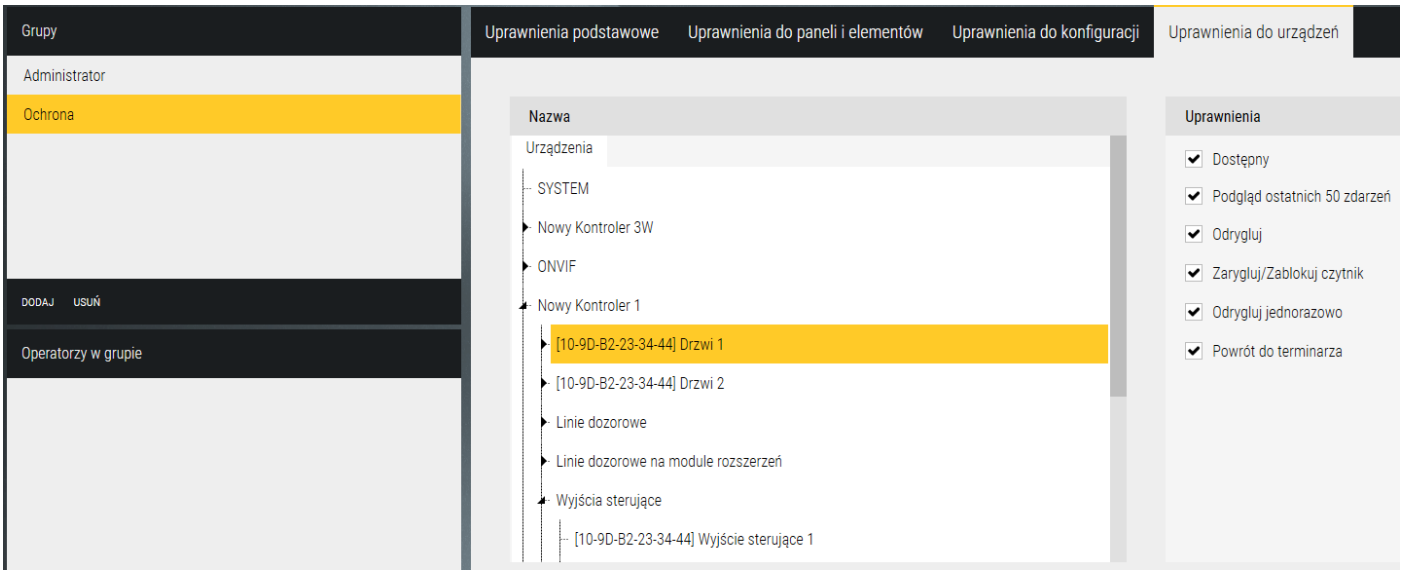


Uprawnienia do konfiguracji



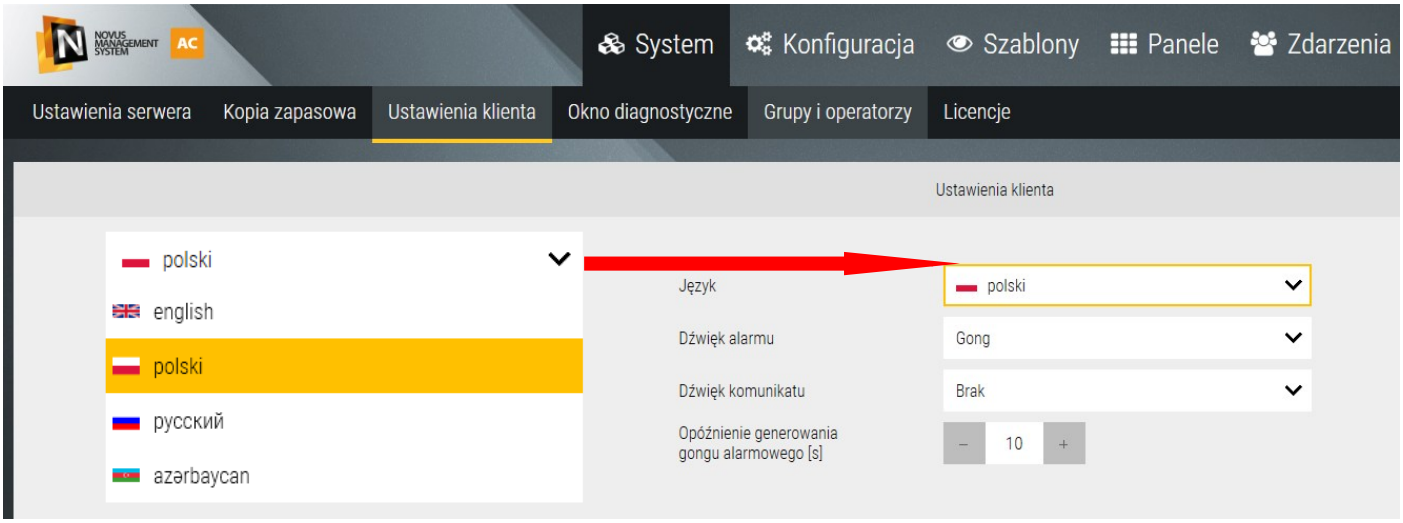
W tej zakładce należy ustawić, do których pozycji z menu programu będą mieli dostęp operatorzy z tej grupy. Administrator ma pełny dostęp w zakresie odczytu, modyfikacji i usuwania. Dla grupy *Ochrona* najczęściej zostawia się tylko wybrane pozycje menu z atrybutem *Odczyt*.

Uprawnienia do urządzeń



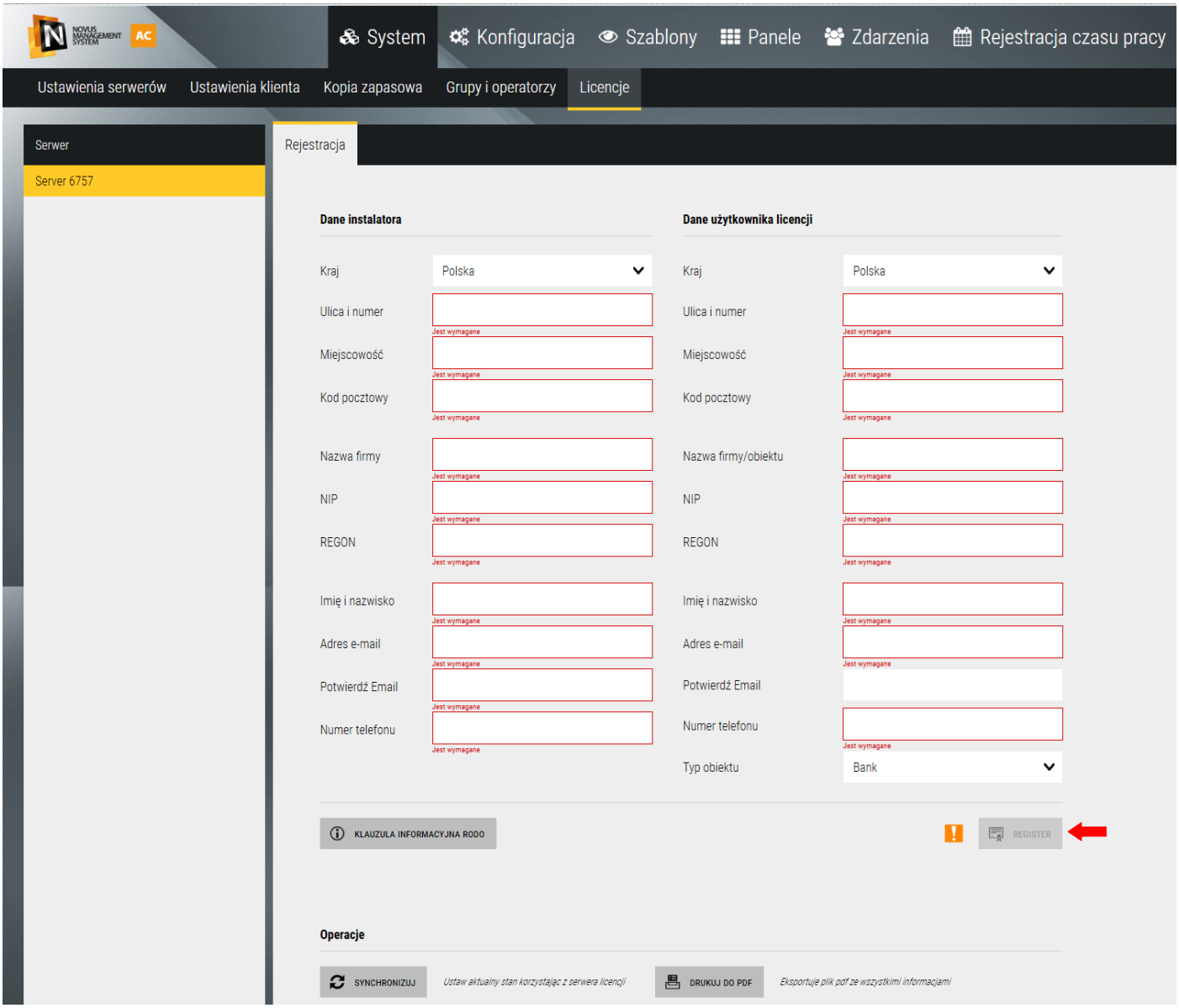
W tej zakładce należy ustawić, do których urządzeń systemu będą mieli dostęp operatorzy z tej grupy w zakresie wykonywania na nich określonych operacji. Administrator ma pełny dostęp do wszystkich operacji. Dla grupy *Ochrona* najczęściej zostawia się tylko wybrane pozycje związane z podstawowymi operacjami np. *Odryglowanie/ zaryglowanie drzwi.*

8.2 Ustawienia klienta (stacji operatora)



W tej zakładce można ustawić język menu programu dla operatora. Do wyboru aktualnie jeden z czterech języków: angielski, polski, rosyjski lub azerbejdżański. Pozostałe opcje służą do ustawień związanych z sygnalizacją alarmów.

8.3 Licencje

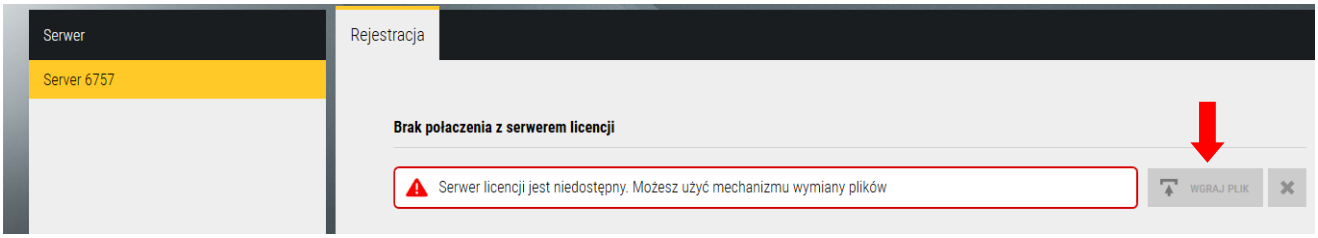


Korzystanie z programu NOVUS MANAGEMENT SYSTEM AC wymaga jego zarejestrowania oraz aktywowania odpowiednich licencji. Aktywacja licencji jest możliwa dopiero po zarejestrowaniu programu.
W celu dokonania rejestracji programu należy wypełnić wszystkie wymagane pola przedstawione na obrazie powyżej.

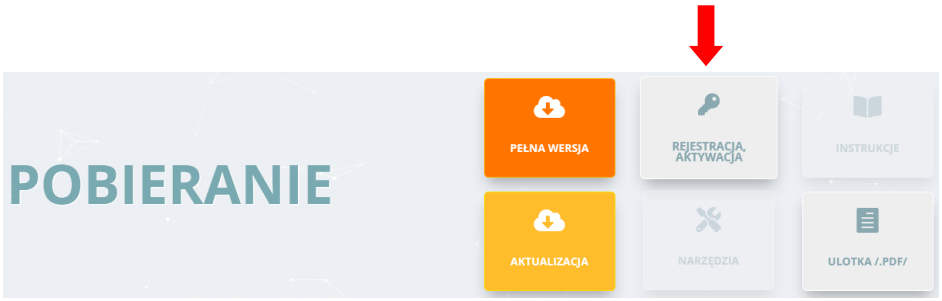
UWAGA!
Po zakończeniu procesu rejestracji edycja danych w sekcji Dane użytkownika licencji nie będzie możliwa. W celu modyfikacji tych danych należy skontaktować się z AAT SYSTEMY BEZPIECZEŃSTWA sp. z o.o. za pośrednictwem adresu e-mail: kontakt@aat.pl.

Gdy komputer na którym dokonujemy rejestracji ma dostęp do sieci Internet w celu zakończenia procesu rejestracji należy wybrać przycisk ***REGISTER***.

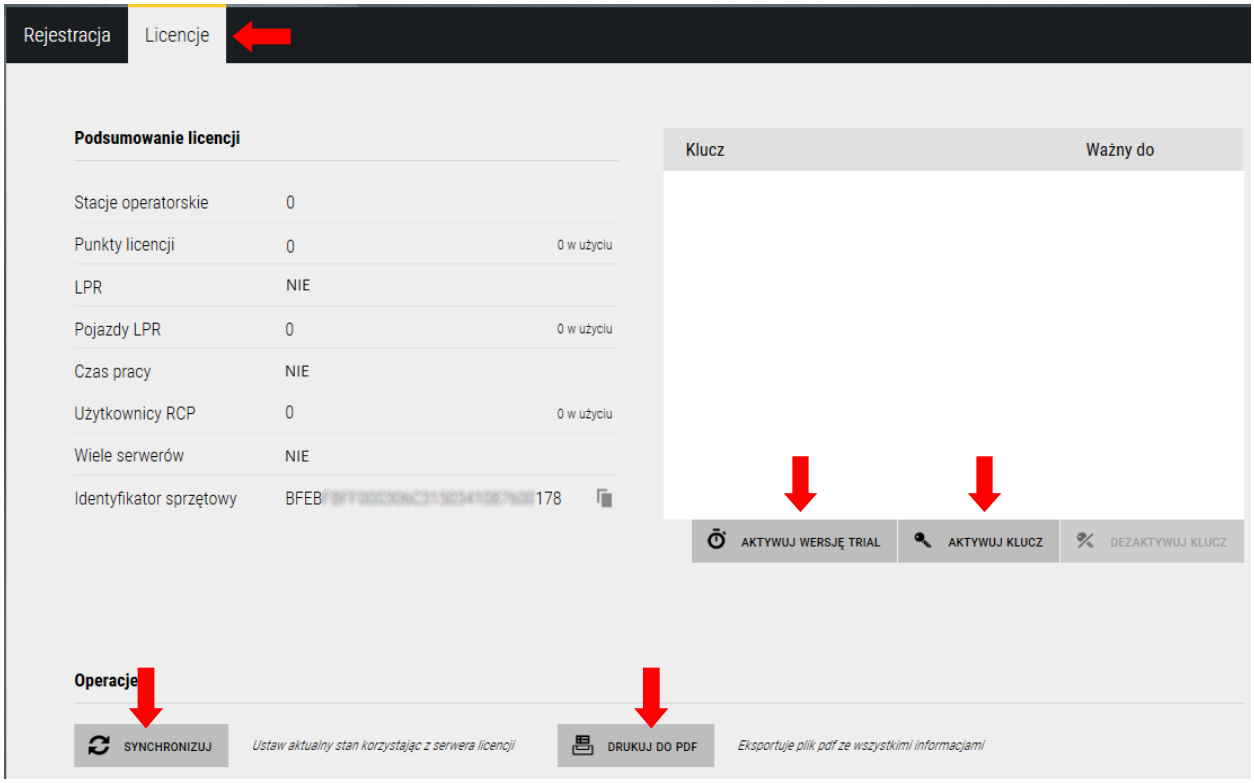
W przypadku rejestracji z komputera nie posiadającego dostępu do sieci Internet w oknie ***Rejestracja*** pojawi się następująca opcja.



W celu dokonania rejestracji bez dostępu do sieci Internet (rejestracja off-line), należy wypełnić wszystkie wymagane pola, a następnie wybrać przycisk ***REGISTER***. Zostanie wygenerowany plik *request.nlic*. Plik należy przenieść na komputer posiadający dostęp do sieci Internet i otworzyć stronę internetową https://nmsac.aat.pl/pl, następnie w sekcji *POBIERANIE* wybrać opcję *REJESTRACJA, AKTYWACJA* i wgrać plik *request.nlic* zgodnie z instrukcjami podanymi na stronie.



Gdy proces przebiegnie poprawnie w odpowiedzi wygenerowany zostanie plik *response.nlic,* który należy przenieść na komputer na który dokonujemy rejestracji i wgrać po wybraniu opcji *WGRAJ PLIK.* Po wykonaniu tych czynności proces rejestracji jest zakończony. W menu *System/Licencje* pojawi się zakładka *Licencje* zawierająca informacje o licencjach danej jednostki komputerowej.



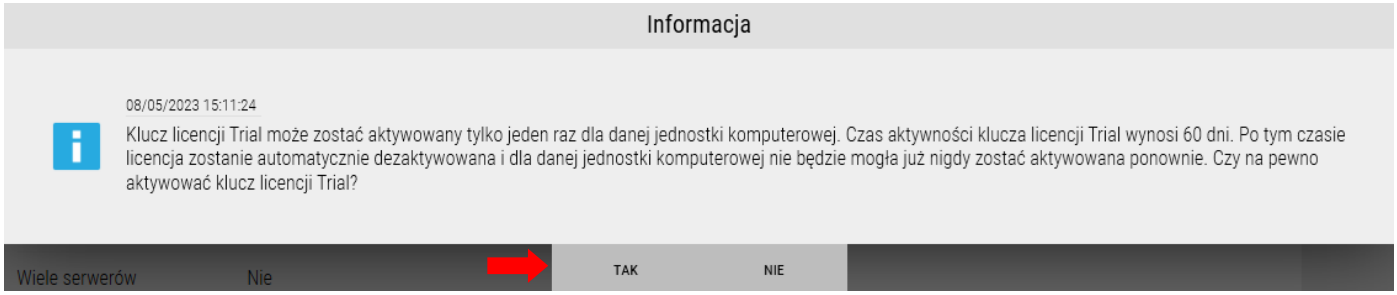
Licencje oparte są na ciągach znaków i nie wymagają kluczy sprzętowych.

Wybranie opcji *SYNCHRONIZUJ* powoduje pobranie z serwera licencji informacji dotyczących danej jednostki komputerowej (jeśli komputer na którym dokonujemy synchronizacji ma dostęp do sieci Internet. W przeciwnym wypadku zostanie wygenerowany plik *request.nlic.* W celu dokończenia procesu synchronizacji, należy postępować analogicznie jak zostało to opisane dla procesu rejestracji bez dostępu do sieci Internet (rejestracja off-line). Jeśli była ona już w przeszłości rejestrowana, była dla niej aktywowana licencja TRIAL lub są aktywne płatne licencje to informacje te zostaną pobrane do programu. Np. w przypadku, gdy oprogramowanie NOVUS MANAGEMENT SYSTEM AC został odinstalowane i zainstalowane ponownie użycie przycisku ***SYNCHRONIZUJ*** spowoduje zaczytanie wszystkich informacji dotyczących rejestracji i licencji.

Opcja *DRUKUJ DO PDF* pozwala na wygenerowanie pliku PDF zawierającego informacje o licencjach dla danej jednostki komputerowej.

Aktywacja licencji TRIAL

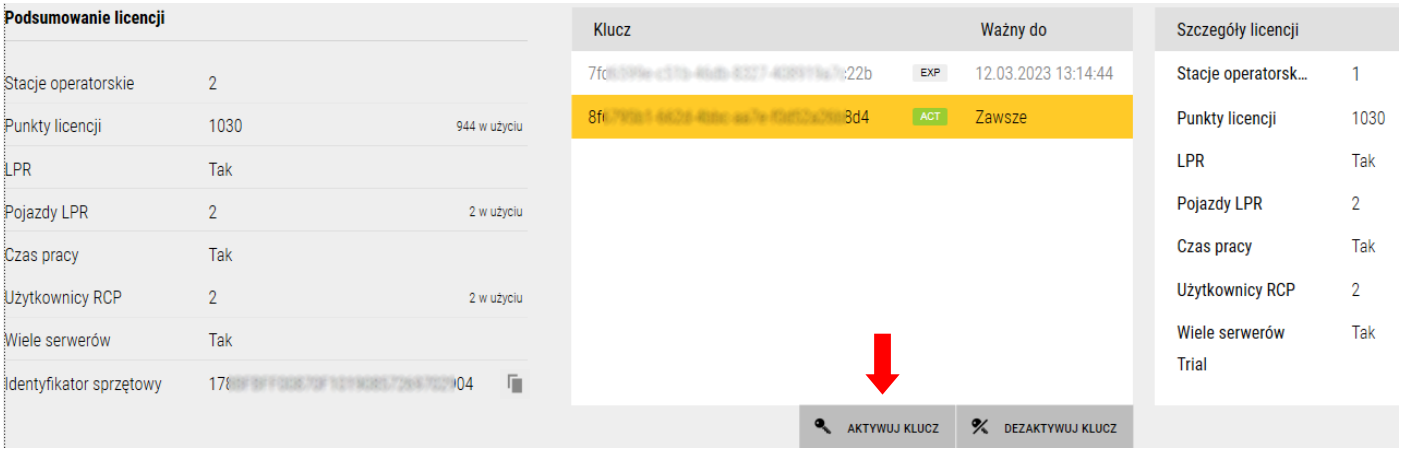
W celu przetestowania funkcji programu dostępna jest licencja testowa TRIAL. Czas jest trwania wynosi 60 dni. W celu aktywacji licencji TRIAL należy wybrać opcję *AKTYWUJ WERSJĘ TRIAL* wskazaną na rysunku na poprzedniej stronie. Pojawi się poniższy komunikat, w celu kontynuowania należy wybrać ***TAK***.



Jeśli komputer ma aktualnie dostęp do sieci Internet licencja TRIAL zostanie aktywowana. W przeciwnym wypadku zostanie wygenerowany plik *request.nlic.* W celu dokończenia procesu aktywacji licencji należy postępować analogicznie jak zostało to opisane dla procesu rejestracji bez dostępu do sieci Internet (rejestracja off-line) na poprzedniej stronie.
W przypadku, gdy nie zostały aktywowane licencje płatne, po upływie czasu trwania licencji TRIAL wszystkie urządzenia dodane do systemu zostaną rozłączone, ale konfiguracja systemu nie ulegnie zmianie. Po wykupieniu i aktywowaniu odpowiednich licencji płatnych możliwość nawiązania komunikacji z urządzeniami zostanie przywrócona. Informacja o czasie jaki pozostał do wygaśnięcia licencji TRIAL wyświetlana jest w lewym górnym rogu interfejsu programu.

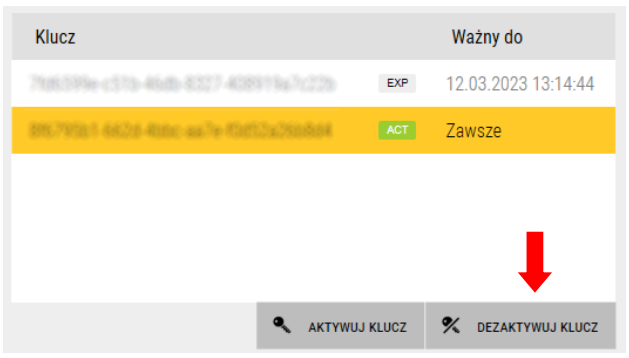
Aktywacja klucza licencji płatnej

Licencje oparte są na ciągach znaków i nie wymagają kluczy sprzętowych.
Po otrzymaniu klucza płatnej licencji w celu jego aktywacji, należy wybrać opcję *AKTYWUJ KLUCZ* wskazaną na rysunku poniżej. Pojawi się okno jak poniżej, w którym należy wpisać/wkleić skopiowany klucz licencji płatnej i wybrać opcję ***OK***. Jeśli komputer na którym dokonujemy aktywacji ma dostęp do sieci Internet klucz licencji zostanie aktywowany. W przeciwnym wypadku zostanie wygenerowany plik *request.nlic.* W celu dokończenia procesu aktywacji licencji należy postępować analogicznie jak zostało to opisane dla procesu rejestracji bez dostępu do sieci Internet (rejestracja off-line) na poprzedniej stronie.
Licencja płatna może zostać aktywowana tylko na jednym komputerze.
Informacje na temat kluczy licencji przypisanych do danego komputera znajdują się w oknie przedstawionym poniżej. Po wybraniu klucza licencji z listy, w oknie po prawej stronie zostaną wyświetlone szczegółowe informacje. Po lewej stronie znajduje się podsumowanie dotyczące aktywnych licencji, ich wykorzystania w systemie oraz identyfikator sprzętowy.

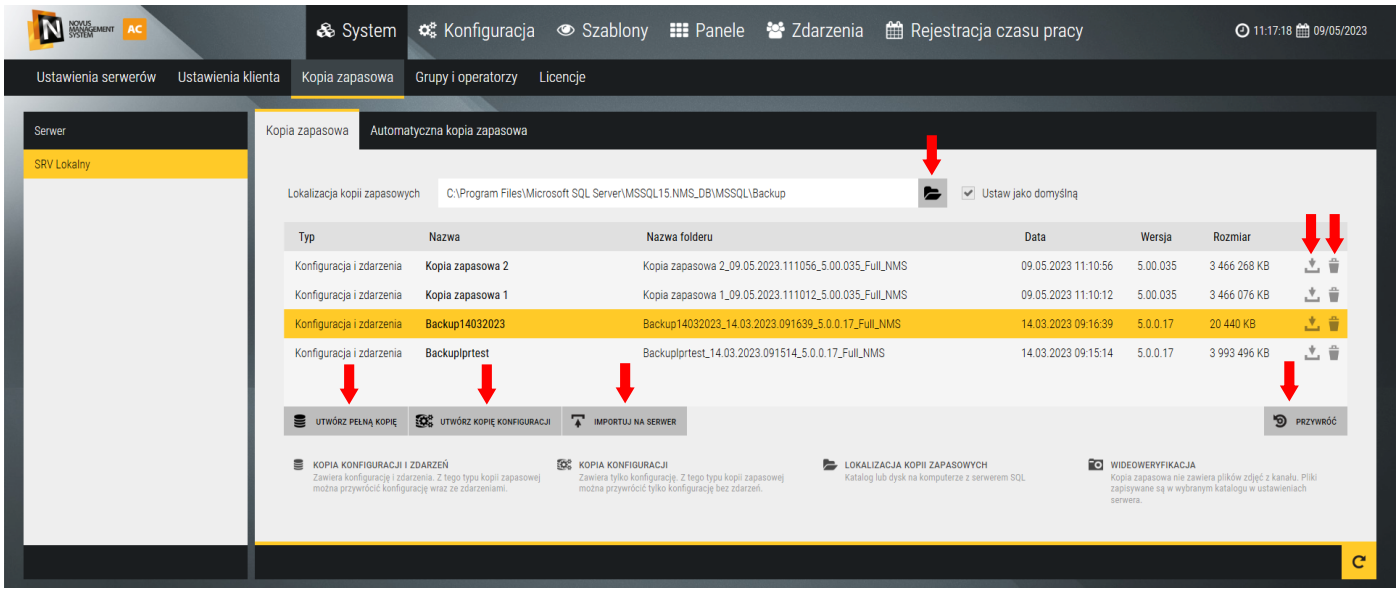


Dezaktywacja klucza licencji płatnej

System NOVUS MANAGEMENT SYSTEM AC umożliwia dezaktywację klucza licencji płatnej z poziomu komputera na którym jest aktualnie aktywowany i jej ponowną aktywację na innym komputerze. W celu dokonania dezaktywacji klucza licencji płatnej należy w menu System/*Licencje/Licencje* wybrać klucz z listy, a następnie opcję *DEZAKTYWUJ KLUCZ.* Jeśli komputer na którym dokonujemy aktywacji ma dostęp do sieci Internet klucz licencji zostanie dezaktywowany. W przeciwnym wypadku zostanie wygenerowany plik *request.nlic.* W celu dokończenia procesu dezaktywacji klucza licencji należy postępować analogicznie jak zostało to opisane dla procesu rejestracji bez dostępu do sieci Internet (rejestracja off-line). Po zakończeniu procesu dezaktywacji klucz licencji może zostać aktywowany na innym komputerze.



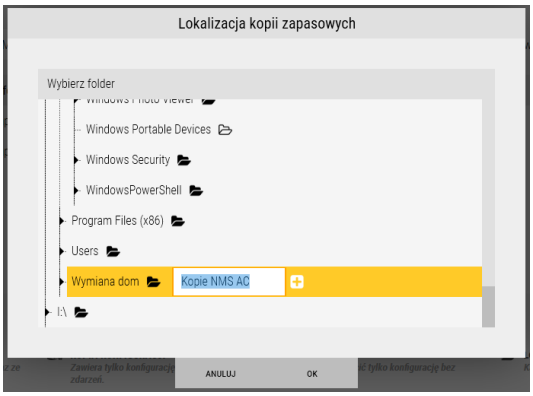
8.4 Kopia zapasowa



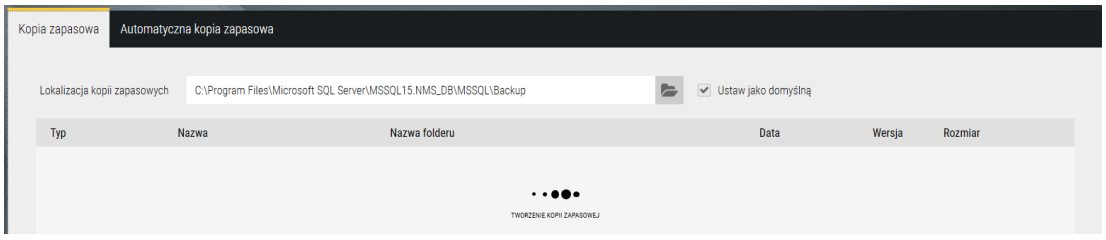
W tej zakładce można wykonać lub przywrócić kopię systemu.

<u>Tworzenie kopii zapasowej</u>

Na górze okna wyświetla się pole lokalizacji kopii zapasowych systemu. Domyślną ścieżkę możemy zmienić klikając na ikonie ***folderów***.



Można wskazać wybrany folder na bieżącym dysku, pendrivie lub zmapowanym dysku innego komputera i wybrać ją jako lokalizację domyślną. Można wykonać kopię zdarzeń i konfiguracji lub tylko konfiguracji klikając na jeden z przycisków na dole okna. Początek nazwy kopii można zmienić. Domyślna nazwa kopii zawiera znacznik daty i godziny jej wygenerowania oraz typ kopii.



Po wykonaniu kopii pojawia się ona na liście. Po prawej stronie znajduje się ikona umożliwiająca jej usunięcie oraz ikona umożliwiająca pobranie kopii z lokalizacji w której się znajduje.

Opcja *IMPORTUJ NA SERWER* umożliwia zaimportowanie pliku kopii zapasowej w celu jej przywrócenia.

Przywracanie kopii zapasowej

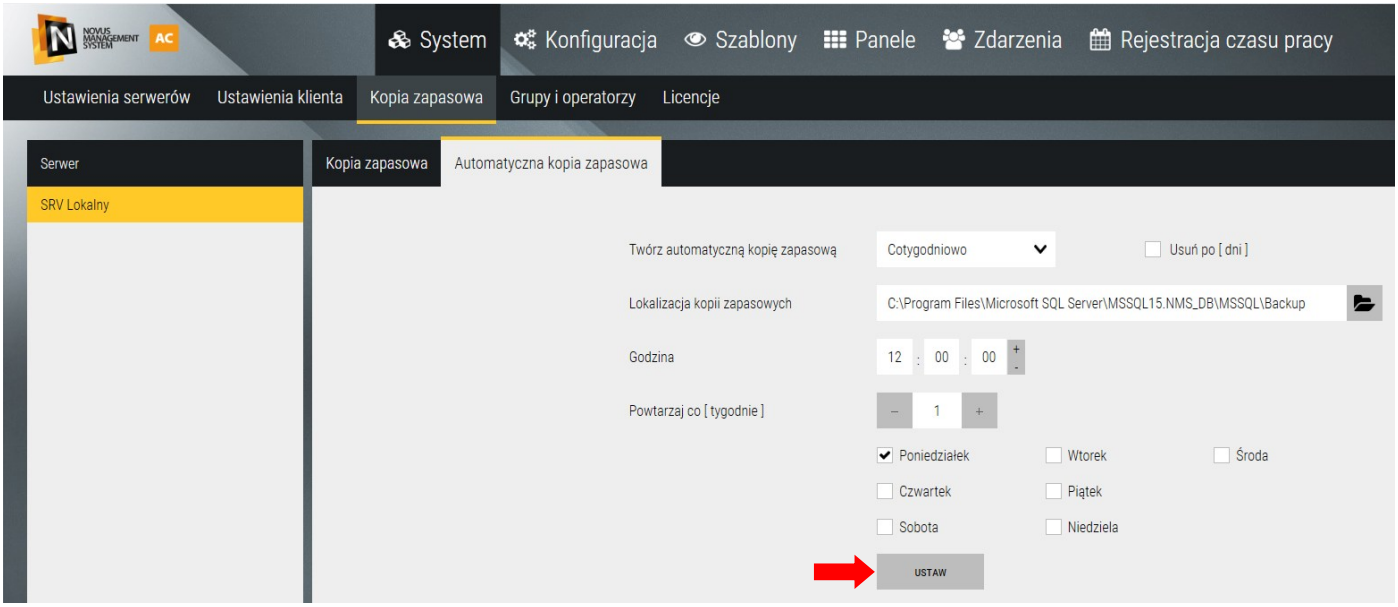
Aby odtworzyć kopię systemu należy wybrać ją z listy (jeśli pliku kopii nie ma na liście należy użyć opcji IMPORTUJ *NA SERWER*), a następnie wybrać przycisk ***PRZYWRÓĆ***.

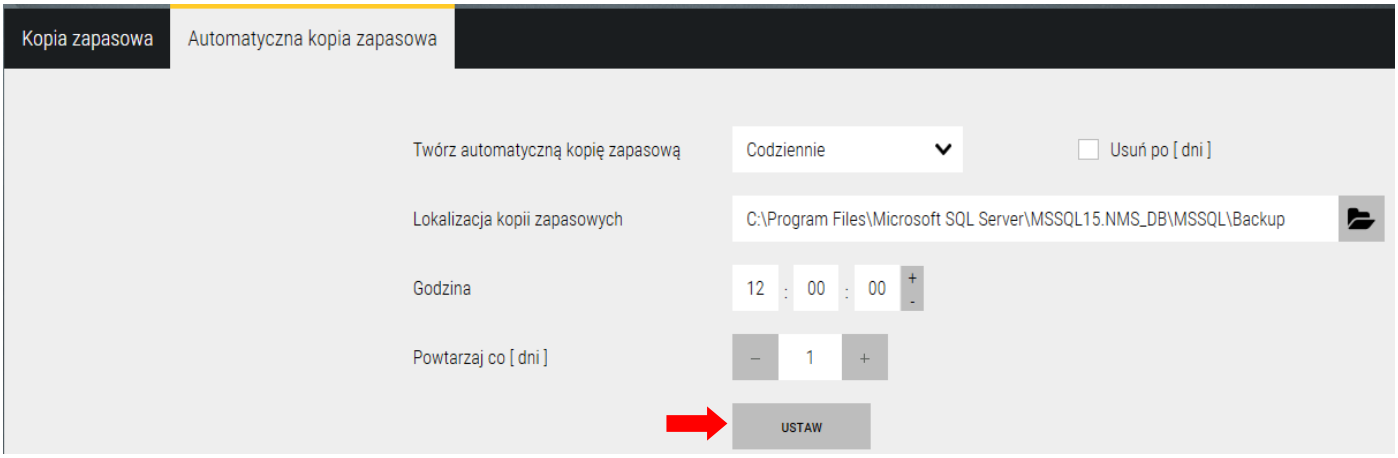
Możliwe jest również przywrócenie stanu początkowego systemu (wyczyszczenie bazy danych) - np. po testach systemu. W tym celu należy przywrócić kopię zapasową pod nazwą *Ustawienia domyślne,* która jest generowana automatycznie po zainstalowaniu systemu.

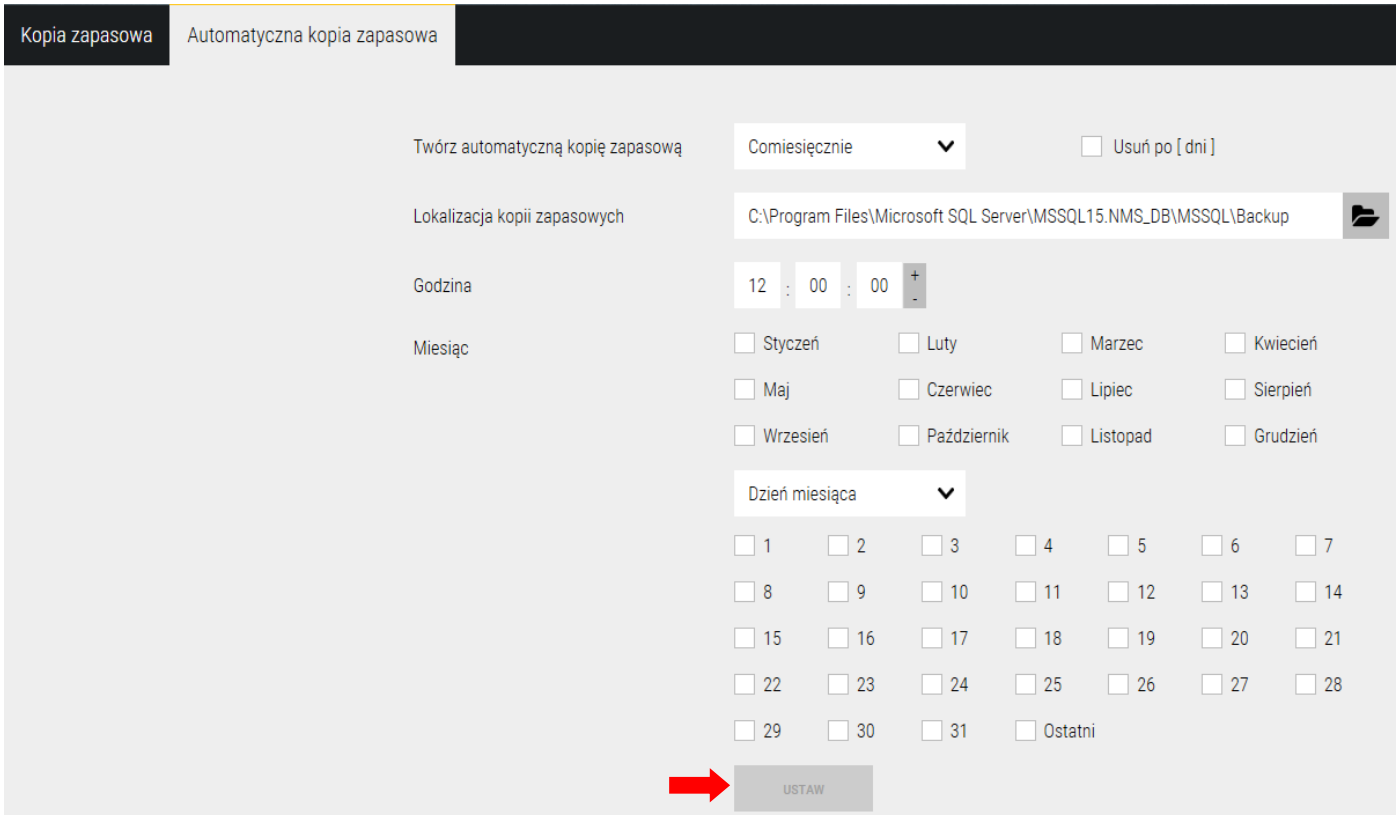
Automatyczna kopia zapasowa

Okno, w którym możemy ustawić parametry automatycznej kopii zapasowej.

Automatyczna kopia zapasowa może zostać utworzona i zapisana codziennie, co tydzień lub co miesiąc.







Rozdział 9. Funkcje zaawansowane

9.1 Grupy serwerów

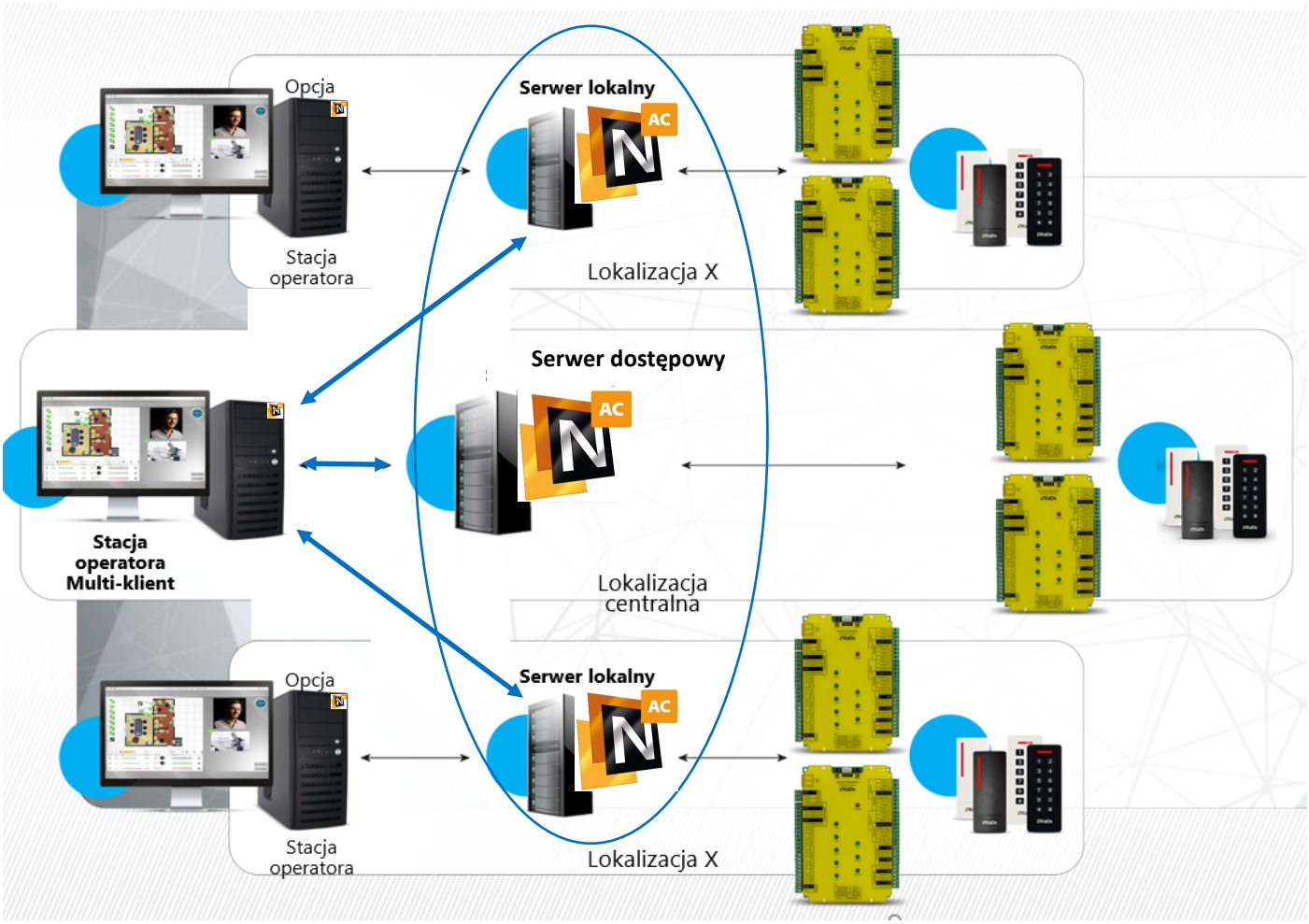
Ta opcja dostępna jest po aktywacji dodatkowej płatnej licencji (NOVUS MANAGEMENT SYSTEM AC SRV v5). Przeznaczona jest głównie dla obsługi systemów w wielu lokalizacjach, ale może być również użyta do obsługi dużego systemu w jednej lokalizacji zwłaszcza w przypadku, gdy zainstalowana jest duża liczba urządzeń VSS.

Serwery NOVUS MANAGEMENT SYSTEM AC zainstalowane w każdej z lokalizacji obsługują lokalne systemy oraz komunikują się z lokalnymi stacjami klienckimi tak jak w systemie bez multiserwerowości. Ta opcja pozwala połączyć wybrane serwery z grupę w celu równoczesnej konfiguracji i monitorowania tych podsystemów z jednej lub kilku stacji klienckich (multi-klient). To powoduje, że utrata komunikacji z daną lokalizacją nie wpływa na pracę, konfigurację i monitorowanie lokalnego systemu. Nie jest to możliwe w przypadku systemu z jednym centralnym serwerem. Definicje użyte na schemacie i opisach poniżej:

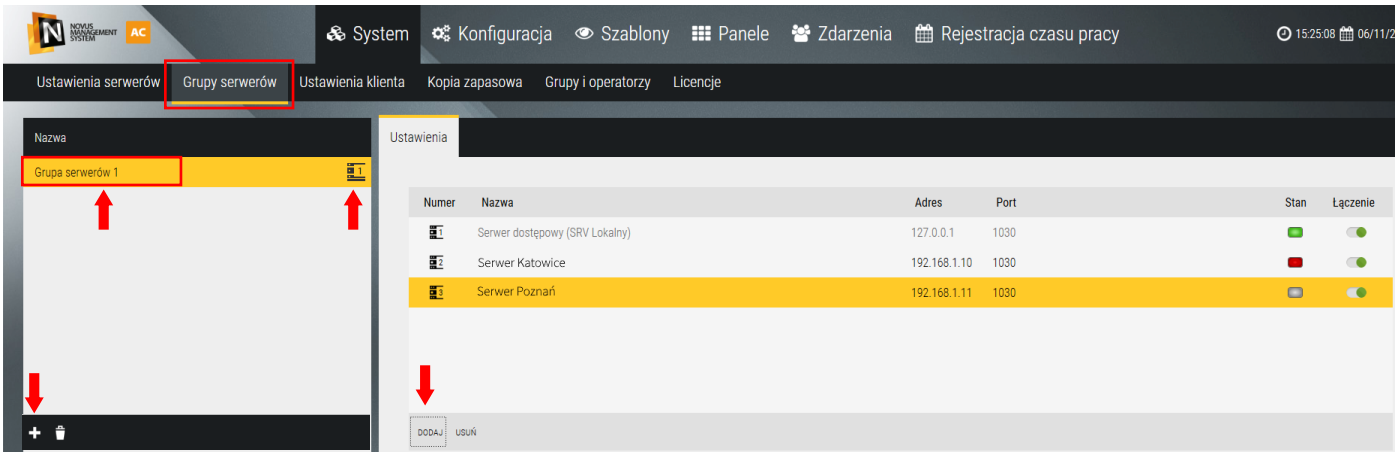
Serwer dostępowy - jeden serwer w systemie z dodaną licencją na multi-serwerowość, na którym została utworzona grupa z serwerów lokalnych (każdy z nich musi mieć dodaną licencję na multi-serwerowość). W systemie, a nawet w ramach jednej grupy może być więcej niż jeden serwer dostępowy.

Multi-klient - stacja operatora (NOVUS MANAGEMENT SYSTEM AC Client) zalogowana do serwera dostępowego przez operatora posiadającego login wspólny dla wszystkich serwerów z grupy.

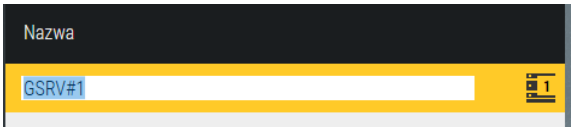
NOVUS MANAGEMENT SYSTEM AC - system z wieloma serwerami



Jeżeli chcemy utworzyć grupę serwerów to na każdy z nich wymagany jest zakup dodatkowej licencji NOVUS MANAGEMENT SYSTEM AC SRV v5 . Po dodaniu zakupionej licencji do serwera NOVUS MANAGEMENT SYSTEM AC w zakładce *SYSTEM* pojawi się nowa zakładka - *Grupy serwerów* oraz nowe ikony w oknach konfiguracji z numerem serwera do którego należy dany element .



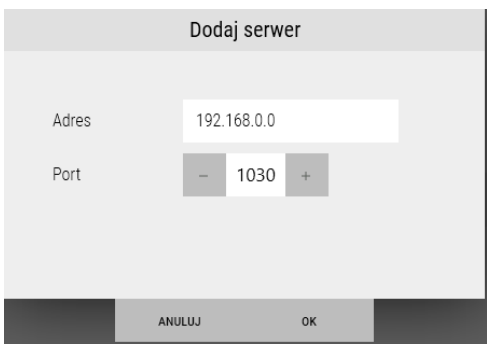
Dodaj - aby utworzyć grupę serwerów należy kliknąć na przycisku **+** (***Dodaj***) lewym dolnym rogu okna. Następnie w polu nazwy należy wpisać nazwę definiowanej grupy serwerów.

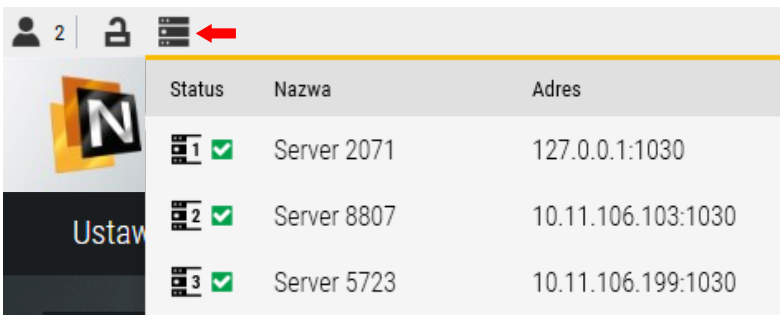


Po zdefiniowaniu grupy można do niej dodawać serwery, do których zostały dodane licencje na multiserwerowość.

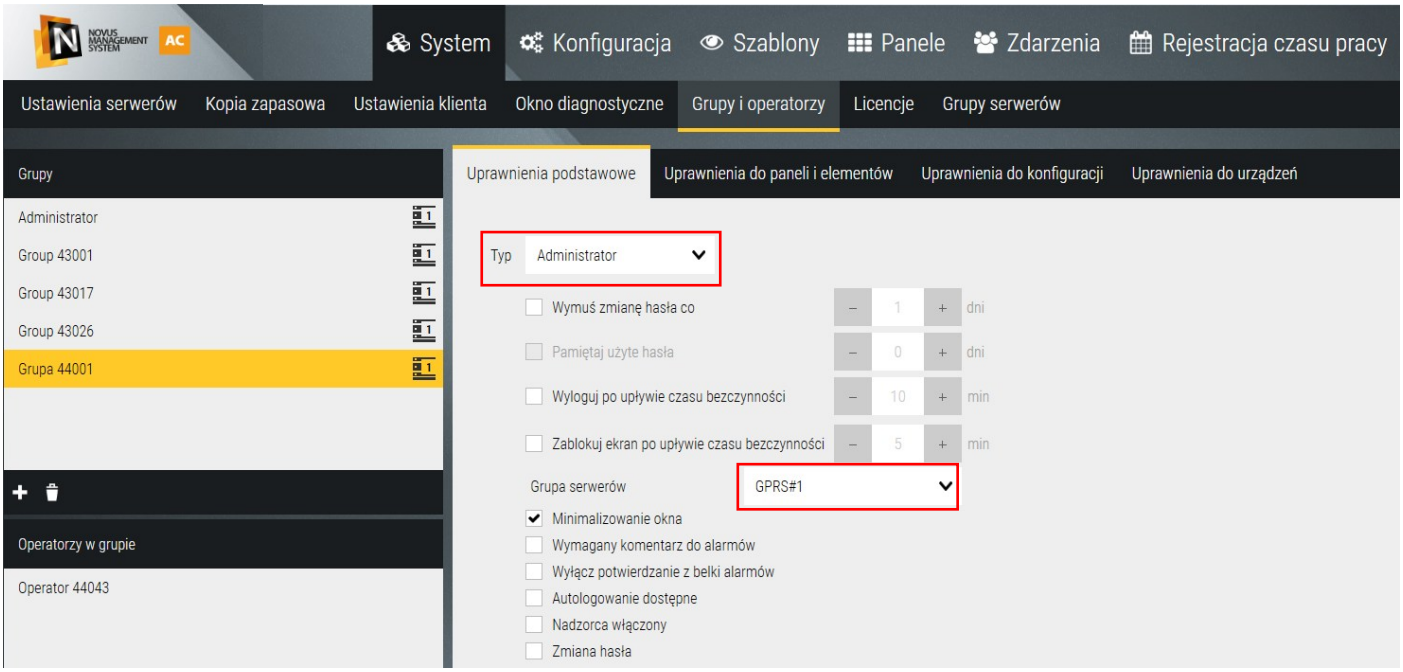
W tym celu należy kliknąć na przycisku ***Dodaj*** w prawym oknie:

Po wpisaniu adresu i kliknięciu ***OK*** serwer pojawi się na liście. Jeżeli jest uruchomiony w dostępnej dla tej grupy sieci to ikona po lewej strony nazwy zapali się na zielono. Pojawi się też na liście na górnym pasku z lewej strony po wskazaniu myszą ikony z listą serwerów. Można zdefiniować więcej niż jedną grupę serwerów.

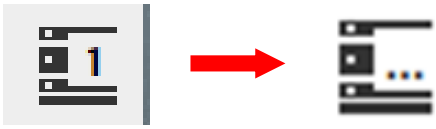




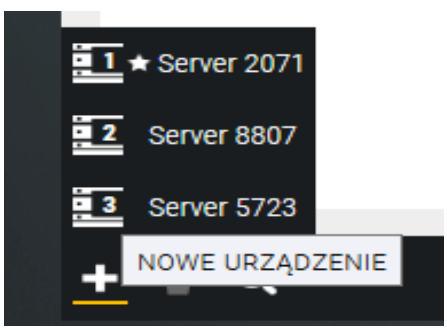
Po utworzeniu grupy serwerów należy zdefiniować na każdym z nich operatora przypisanego do tej grupy. To pozwoli uzyskać dostęp do podsystemów w obrębie grupy po zalogowaniu na jednej ze stacji klienckich w ramach tej grupy. Po dodaniu licencji na multi-serwerowość w zakładce definiowania operatorów pojawia się nowa opcja - *Grupa serwerów.*

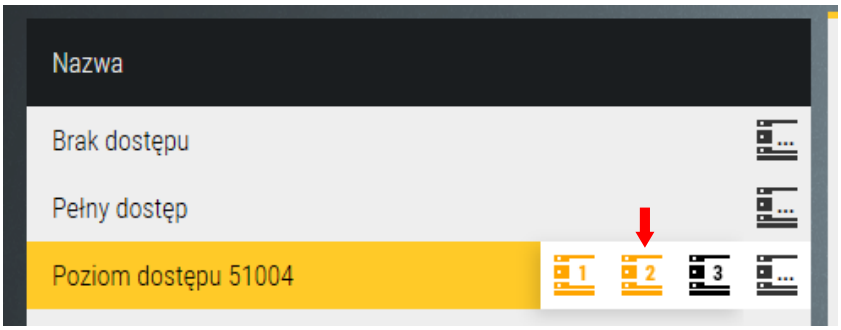


Z rozwijanej listy należy wybrać grupę serwerów do której dany operator będzie miał uprawnienia. Po zalogowaniu operator w zależności od przypisanych uprawnień będzie mógł dodawać, edytować i usuwać elementy przypisane do serwerów oraz na nich określone operacje (np. *Odrygluj drzwi* - w dowolnej lokalizacji). Przy dodawaniu nowych elementów operator ma możliwość wyboru serwera do którego dodaje nowy element. Gwiazdką oznaczony jest serwer dostępowy na którym pracujemy lokalnie. Dodany do jednego serwera nowy element logiczny (np.. Poziom dostępu) można przypisać do pozostałych serwerów w grupie po najechaniu i kliknięciu wskaźnikiem myszy na ikony z numerami serwerów. Przypisane serwery są wyświetlane w kolorze pomarańczowym a ikona na końcu listy zmienia wygląd na:



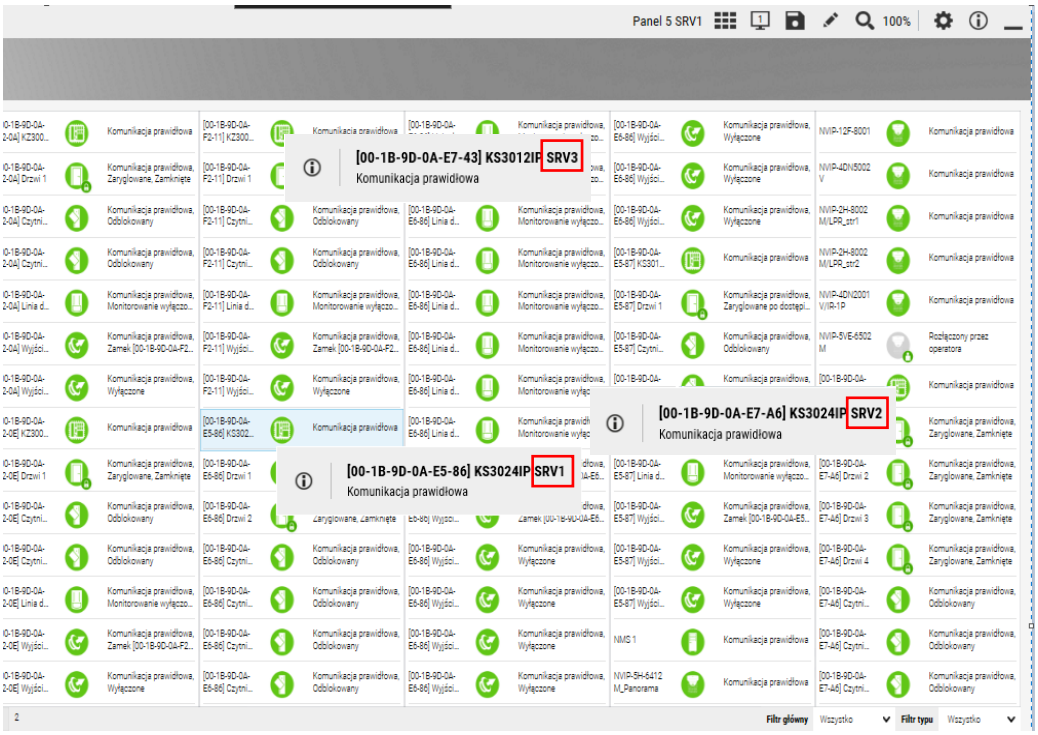
Wybrane domyślne elementy systemu, które są takie same na serwerach są na listach w lewym oknie tylko jeden raz bez względu na liczbę serwerów w grupie. Dotyczy to np. terminarzy, poziomów dostępu, świąt.





Jeżeli nowo dodany np. panel ma zawierać elementy skomunikowane z różnymi serwerami lokalnymi (kontrolery, drzwi itp.) to po dodaniu go do listy należy go przypisać do pozostałych serwerów w grupie, zapisać nowy panel i dopiero przejść do trybu edycji panelu.

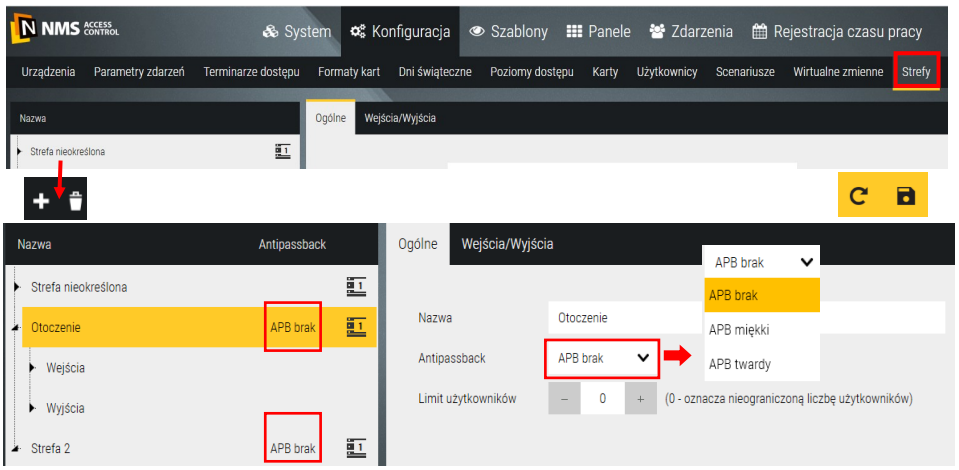
Podobnie ma to miejsce z przypadku tablicy synoptycznej.



Podobna zasada dotyczy stosu zdarzeń bieżących na którym mogą być wyświetlane równocześnie zdarzenia ze wszystkich serwerów w grupie.

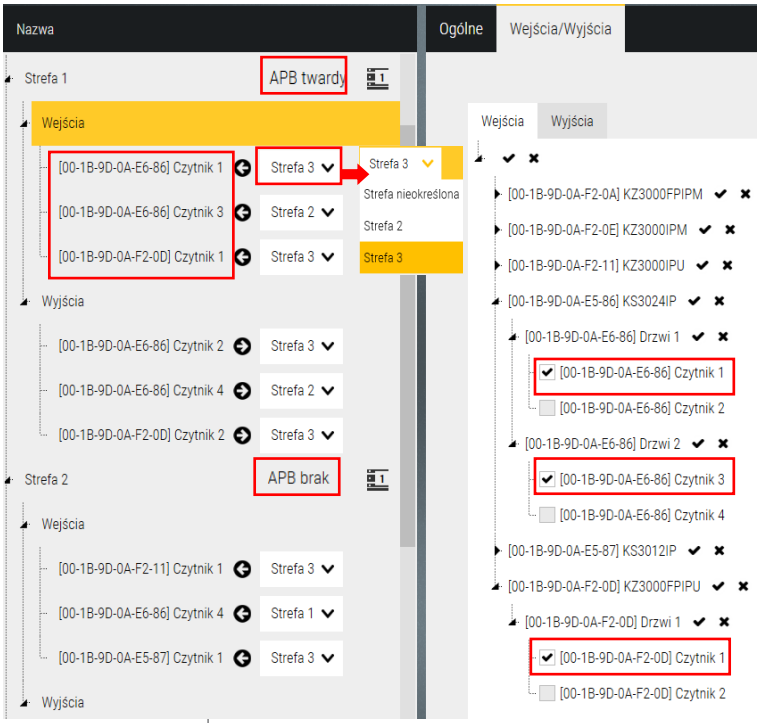
9.2 Strefy globalne

Ta opcja przeznaczona jest do kontroli stanu osób i pojazdów w obszarach objętych dwustronną kontrolą dostępu. Strefa globalna może obejmować czytniki z wielu kontrolerów, obsługuje funkcję antipassbacku zarówno twardego, miękkiego i czasowego. Funkcja działa tylko w trybie on-line gdy serwer NOVUS MANAGEMENT SYSTEM AC ma komunikację z kontrolerami.



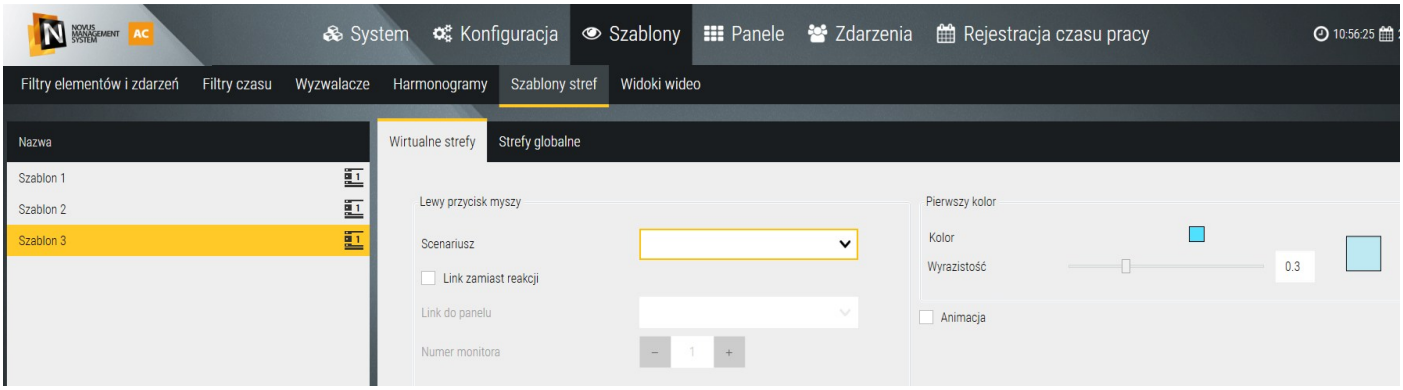
W strefie można ustawić limit użytkowników, którego przekroczenie jest sygnalizowane kolorem obrzeża na panelu oraz odpowiednią reakcją (np. blokada wejścia). Można również wybrać typ funkcji APB - antipassback.
Na liście wyświetlana jest domyślna *Strefa nieokreślona,* która zawiera listę nowych użytkowników, którzy jeszcze nie poruszali się po obiekcie. Przed uruchomieniem tej funkcjonalności znajdują się w niej wszyscy użytkownicy dodani do bazy systemu. Po każdym odczycie karty na czytniku przypisanym do jednej ze stref i otwarciu skrzydła drzwi (naruszenie czujnika stanu drzwi) karta (użytkownik) przepisywana jest do nowej strefy.
Do wybranych stref, które zostały zdefiniowane można przypisać kontrolę APB: *Miękki, Twardy lub Czasow.* APB twardy wymusza odczyt karty w czytniku wejścia i wyjścia. APB miękki generuje tylko komunikat o niewłaściwej lokalizacji użytkownika. APB czasowy ogranicza wstęp do wejścia lub wyjścia ze strefy na określony czas.

Przed przystąpieniem do definiowania stref zaleca się wykonanie szkicu na planie obiektu lub terenu z zaznaczeniem obrzeży stref i lokalizacji czytników we/wy.
Po kliknięciu na przycisku ***Dodaj*** na liście w lewym oknie pojawia się nowa pozycja *Strefa X* - możemy do niej przypisać czytniki wejścia i wyjścia w prawym oknie. Po przypisaniu czytników wejściowych i wyjściowych należy przejść do lewego okna i do każdego czytnika przypisać z rozwijanej listy strefę w której znajduje się ten czytnik. To pozwala stworzyć strukturę wzajemnej lokalizacji stref i przejść pomiędzy nimi. Po zdefiniowaniu stref i zapisie do bazy do zakładki *Panele* i na nowym panelu przystąpić do wizualizacji zdefiniowanych stref.

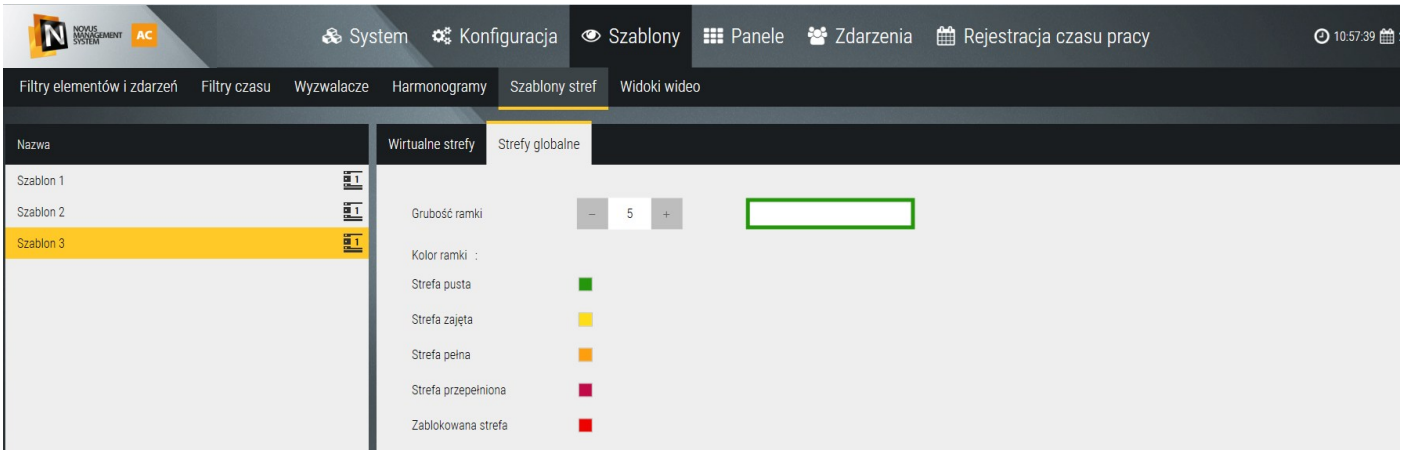


Wizualizacja stref globalnych na panelach

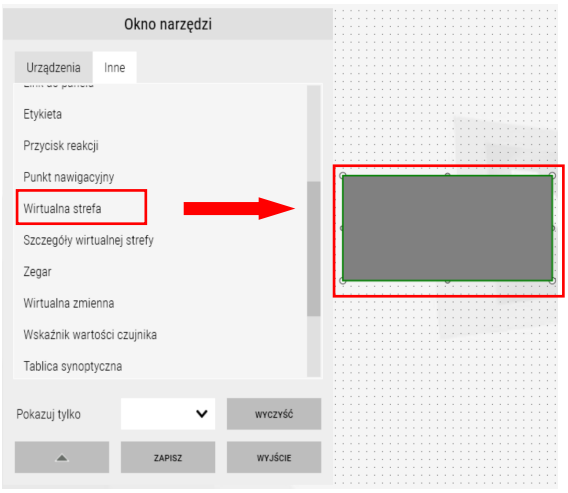
Strefy globalne można na panelach w celu monitorowania ich stanu oraz przepisywania użytkowników na listach w strefach jeżeli zachodzi potrzeba uporządkowania ich statusu. Na panelach strefy globalne są połączone z szablonami stref wirtualnych. Dlatego w pierwszej kolejności należy zdefiniować szablony stref wirtualnych do których na panelach zostaną przypisane strefy globalne.

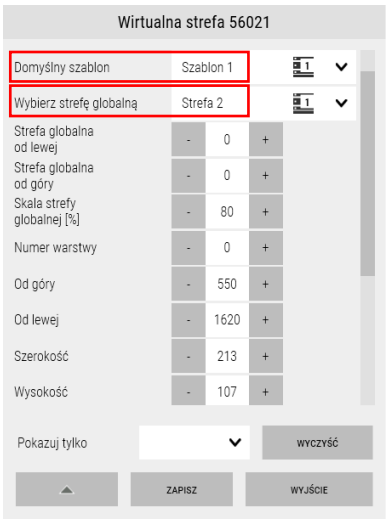


Parametry stref wirtualnych pokazane są powyżej. W przypadku użycia ich do wizualizacji stref globalnych należy dobrać zróżnicowaną kolorystykę tła. Następnie należy przejść do zakładki *Strefy globalne* i ustalić grubość ramki na obrzeżu strefy wirtualnej, której kolor sygnalizuje status strefy zgodnie z legendą.

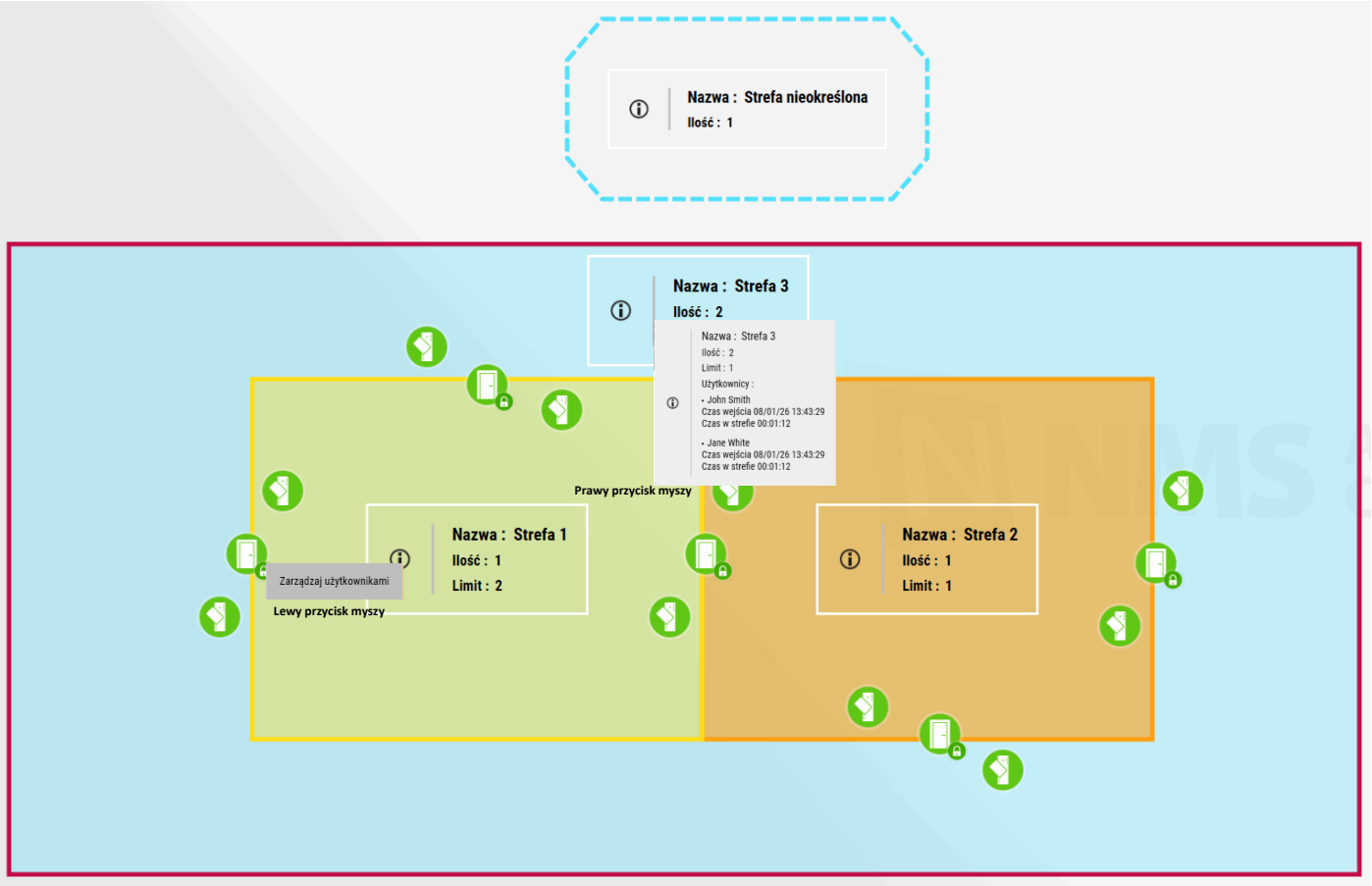


Po przejściu na panel należy wejść w tryb edycji i dodać wirtualną strefę, przypisać jej szablon oraz strefę globalną. Następnie należy zmodyfikować parametry strefy wirtualnej oraz globalnej (położenie, wielkość, skala) i zapisać.

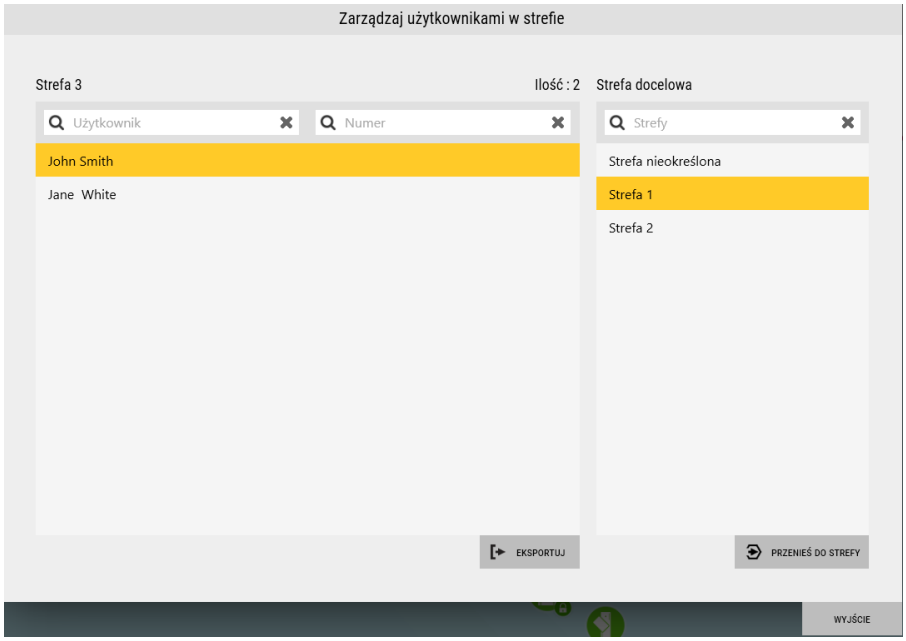




Przykładowy widok po skonfigurowaniu trzech stref i naniesieniu na nich elementów poniżej.



Po kliknięciu lewym przyciskiem myszy na ikonie strefy globalnej wyświetli się okno jak poniżej:



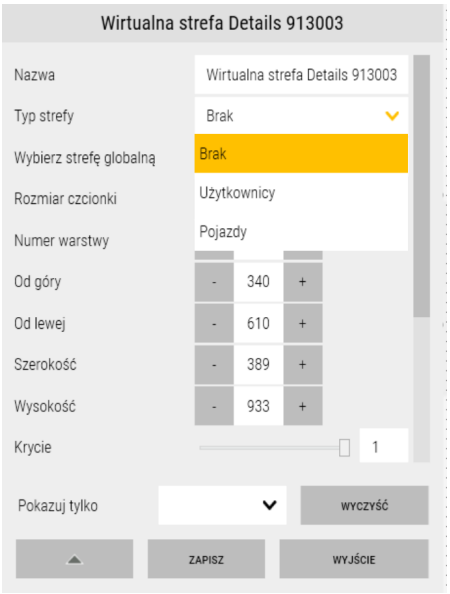
W oknie wyświetlana jest lista zarejestrowanych osób w danej strefie. Po zaznaczeniu jednej lub więcej pozycji na liście (z CTRL) i strefy w prawym oknie można je przepisać do tego obszaru. Można również wyeksportować listę użytkowników do pliku (*.CSV) i wydrukować.

Narzędzie Szczegóły wirtualnej strefy

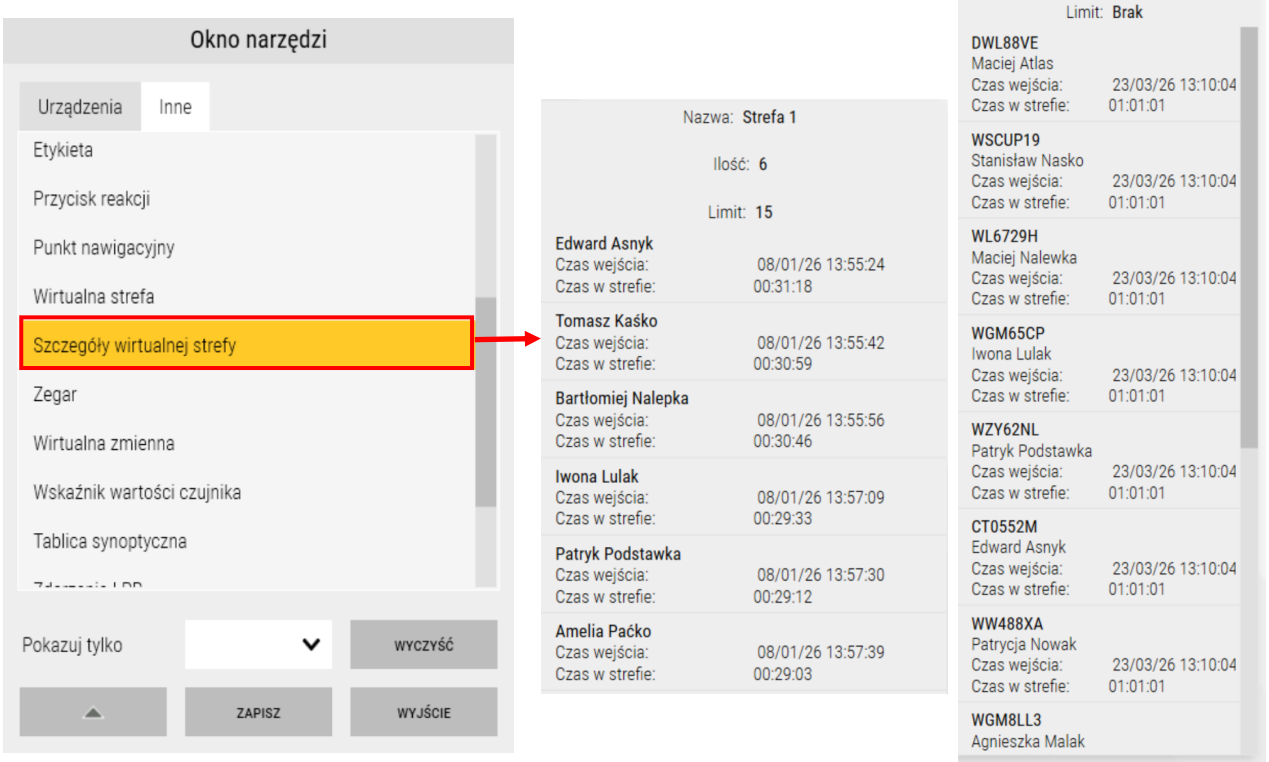
Narzędzie *Szczegóły wirtualnej strefy* umożliwia wyświetlenie szczegółowych informacji dotyczących użytkowników lub pojazdów znajdujących się w danej strefie. Pozwala ono na monitorowanie aktywności użytkowników czy pojazdów w bardziej przejrzysty sposób. Narzędzie przedstawia informacje takie jak:

- Nazwa strefy,
- Ilość - aktualna liczba użytkowników lub pojazdów w strefie,
- Limit - maksymalna dopuszczalna liczba użytkowników lub pojazdów w strefie,
- Czas wejścia - dokładny czas, kiedy użytkownik lub pojazd pojawił się w strefie,
- Czas w strefie - czas przebywania w strefie użytkownika lub pojazdu.

Podobnie jak dla narzędzia *Wirtualna strefa*, możliwe jest przypisanie kontrolki zawierającej szczegóły dotyczące strefy do strefy z użytkownikami lub do strefy LPR z pojazdami.



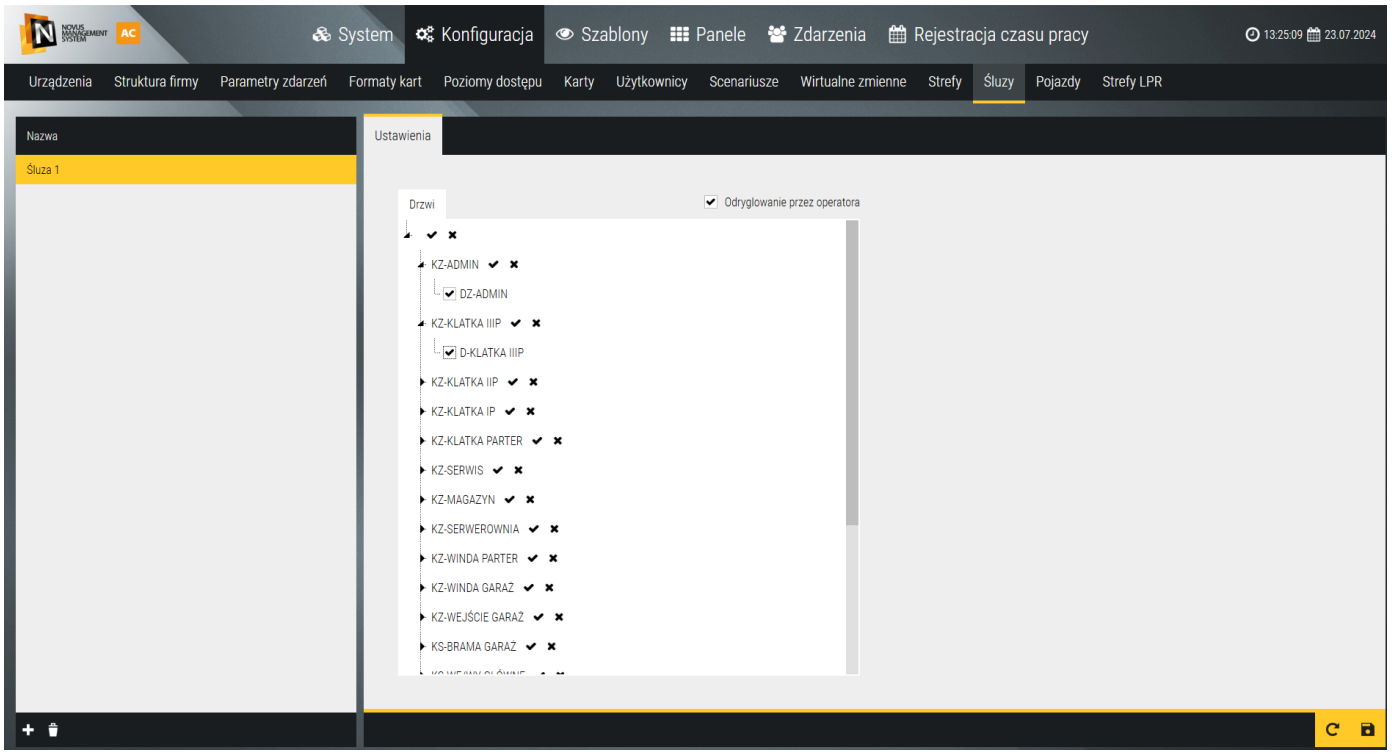
Poniżej widok narzędzia *Szczegóły wirtualnej strefy*.



9.3 Śluzy globalne

Opcja ta przeznaczona jest do kontroli stanu zamknięcia i zaryglowania grupy drzwi. Drzwi mogą być kontrolowane przez różne kontrolery. Funkcja działa tylko w trybie on-line gdy serwer NOVUS MANAGEMENT SYSTEM AC ma komunikację z kontrolerami.

Aby zdefiniować grupę drzwi dla danej śluzy należy kliknąć na ikonie **+** w lewym dolnym rogu okna.



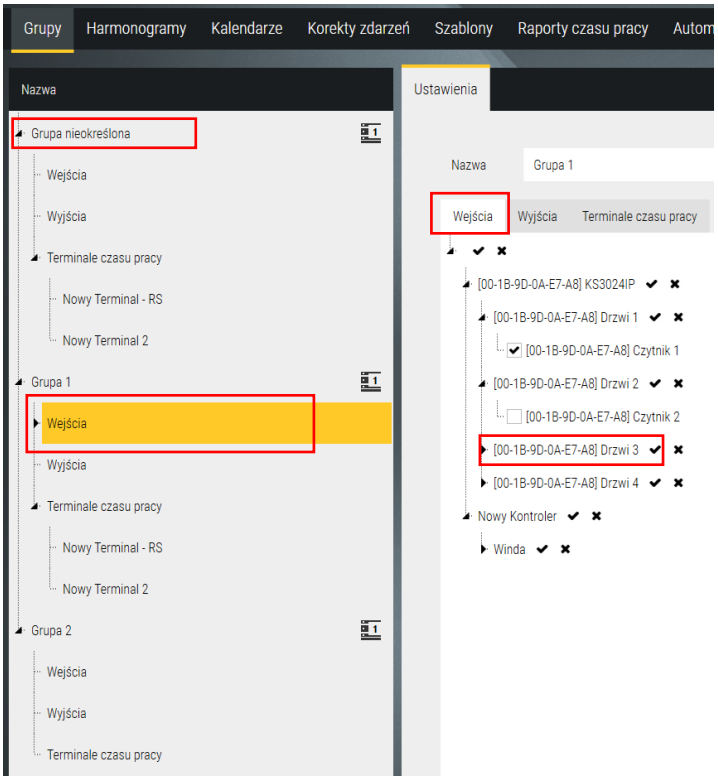
Odryglowanie przez operatora - zaznaczenie tego pola umożliwia operatorowi odryglowanie dowolnych drzwi z grupy śluzy nawet gdy inne z tej grupy są otwarte lub odryglowane

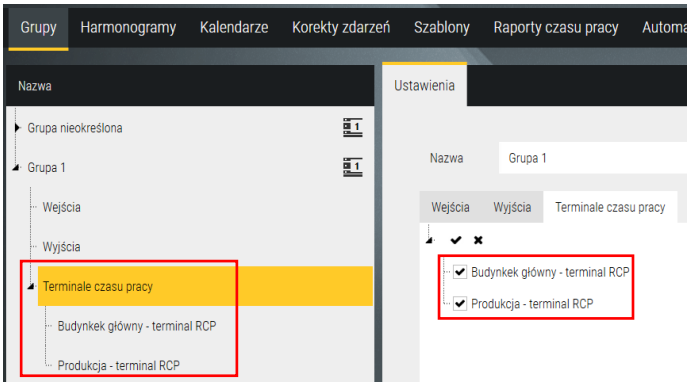
9.4 Rejestracja czasu pracy

Ta opcja dostępna jest w postaci płatnej licencji (dostępny Trial 60 dni). Przeznaczona jest do rejestracji i rozliczania czasu pracy w oparciu o zdarzenia z terminali RCP i czytników systemu KD przypisanych do grup RCP (terminale RCP są dostępne od wersji 4.02). Żeby skorzystać z tej funkcjonalności wymagany jest zakup odpowiednich licencji na samą funkcjonalność (NOVUS MANAGEMENT SYSTEM AC RCP v5), określoną ilość użytkowników RCP (NOVUS MANAGEMENT SYSTEM AC URCP v5) oraz dodanie urządzeń rejestracji czasu pracy do systemu (NOVUS MANAGEMENT SYSTEM AC PKT LIC v5). Po dodaniu zakupionej licencji do serwera NOVUS MANAGEMENT SYSTEM AC w zakładce *Rejestracja czasu pracy* odblokowana zostaje możliwość definiowania grup RCP w zakresie przypisania do każdej z nich terminali i czytników wejściowych i wyjściowych. Liczba tak zdefiniowanych grup nie jest limitowana. Grupa RCP może obejmować czytniki z wielu terminali i kontrolerów. Do rozliczania czasu pracy brane są zdarzenia tylko z czytników przypisanych do grup RCP.
Terminal RCP umożliwia rejestracje dodatkowych we/wy w czasie pracy: na przerwę, służbowe, prywatne.
Rejestracja tych dodatkowych we/wy w czasie pracy możliwa jest też na czytnikach KD - jeden czytnik do jednego rodzaju we/wy.

Grupy

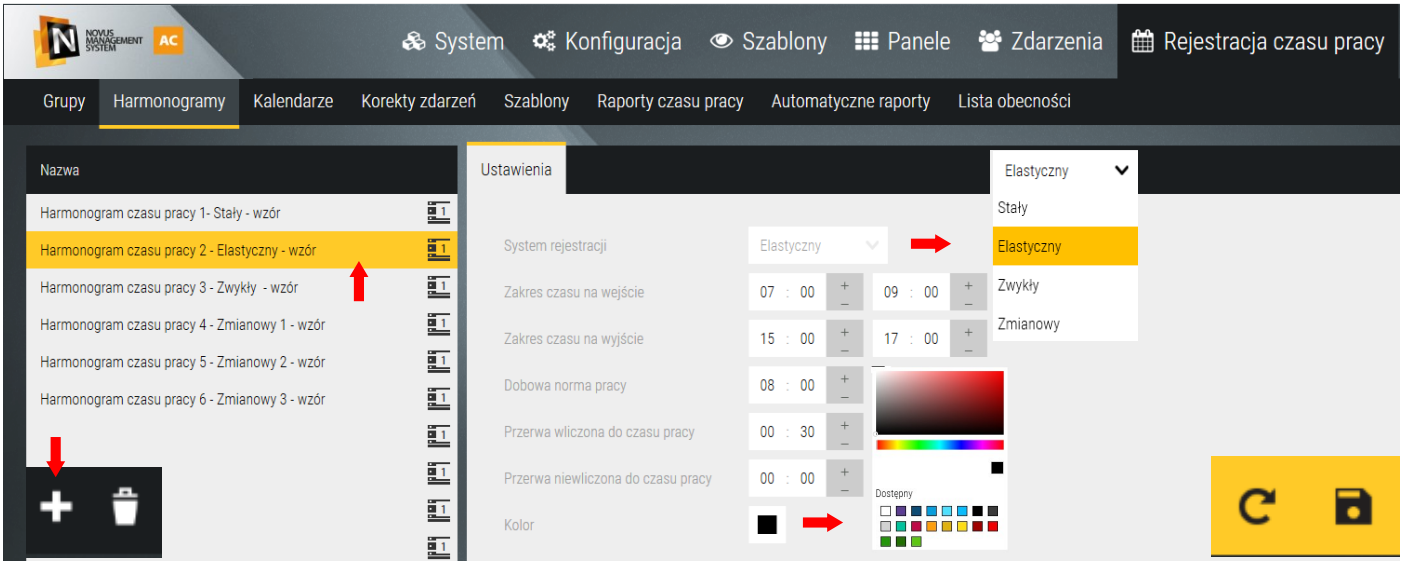
Na liście wyświetlana jest domyślna *Grupa nieokreślona,* która zawiera listę wszystkich czytników przypisanych do grup RCP wraz z informacją do której grupy należą. Po kliknięciu na przycisku ***Dodaj*** na liście w lewym oknie pojawia się nowa pozycja *Grupa X* - możemy do niej przypisać terminale i czytniki wejścia i wyjścia w prawym oknie. Po przypisaniu terminali i czytników wejściowych i wyjściowych są one wyświetlane w strukturze w lewym oknie. Zdefiniowane w ten sposób grupy RCP przypisujemy użytkownikom w zakładce *Konfiguracja/Użytkownicy/Rejestracja czasu pracy.*
Terminale należy dodawać korzystając z zakładki *Terminale czasu pracy.*

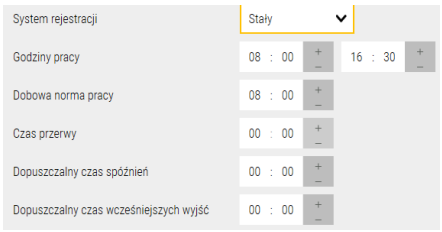


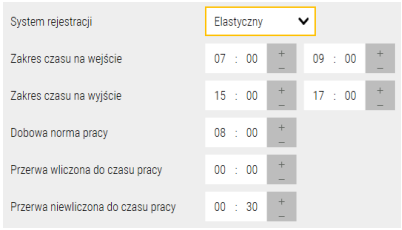


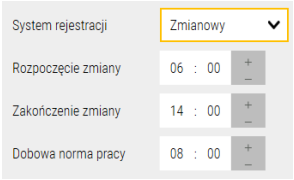
Harmonogramy

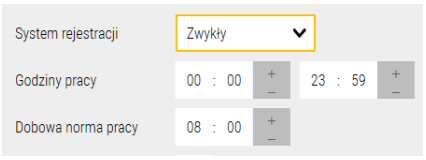
Harmonogramy RCP są potrzebne do rozliczenia czasu pracy w wybranym okresie zgodnie z ustaloną dobową normą. Po kliknięciu na przycisk **+** w lewym oknie pojawia się nowy harmonogram z domyślną nazwą, którą można edytować.











Definiowanie harmonogramu zależy od wyboru systemu rejestracji:
Stały - oznacza, że pracownik ma stały czas pracy w ustalonych godzinach z przerwą.
Dobowa norma pracy - dobowa norma czasu pracy.
Czas przerwy - czas odliczany od zarejestrowanego casu pracy w procesie generowania raportu.
Dopuszczalny czas spóźnień i wcześniejszych wyjść - oznacza, ze pracodawca dopuszcza spóźnienia i wcześniejsze wyjścia

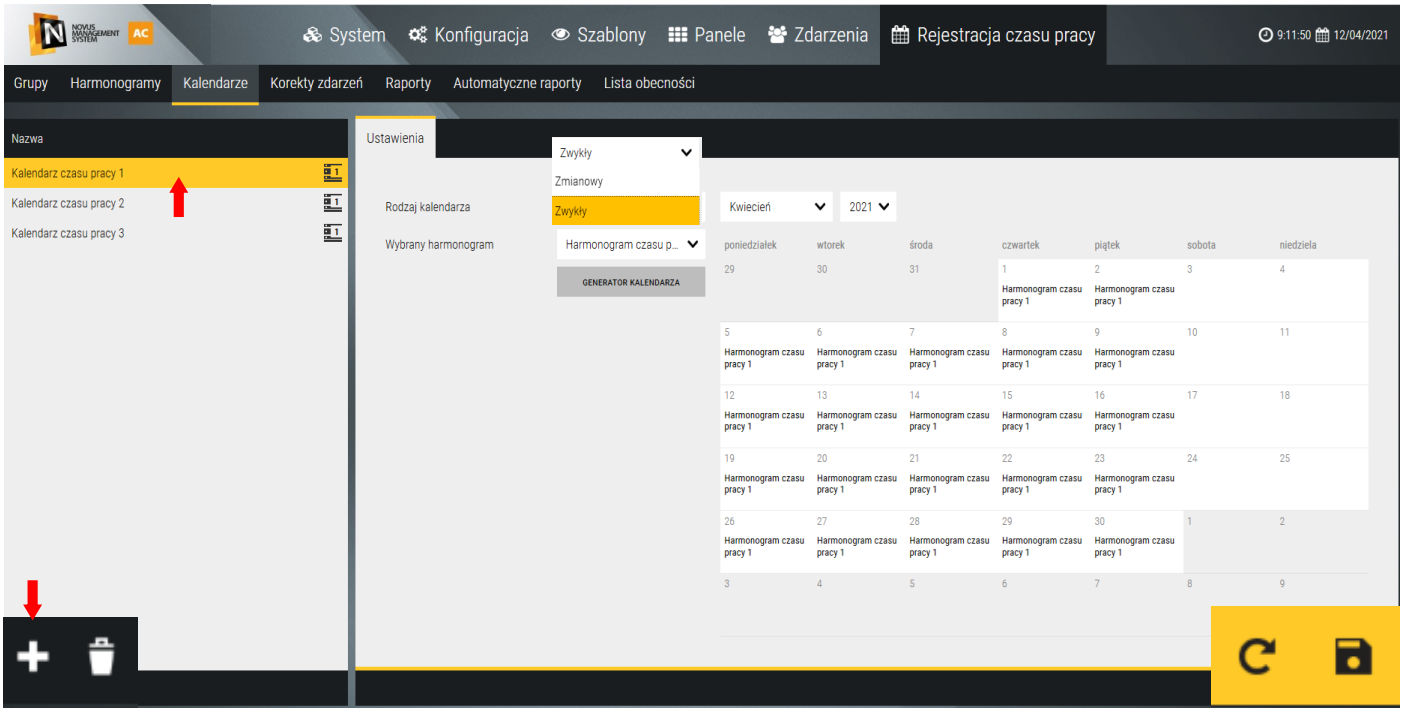
Elastyczny - oznacza, że pracownik będzie miał ustaloną dzienną normę czasu pracy w celu wyliczenia normy miesięcznej (po przemnożeniu przez liczbę dni do przepracowania w danym miesiącu zgodnie z kalendarzem).
Zakres czasu na wejście - należy ustalić przedział czasu, w którym pracownik powinien rejestrować rozpoczęcie pracy. Tylko rejestracje z tego zakresu czasu będą uwzględniane w rozliczeniu. Wcześniejsza rejestracja przed zakresem czasu na wejście będzie skutkowała naliczeniem od początku czasu na wejście, późniejsza (po końcu czasu na wejście) jako nieobecność.
Zakres czasu na wyjście - należy ustalić przedział czasu, w którym pracownik powinien rejestrować zakończenie pracy. Tylko rejestracje z tego zakresu czasu będą uwzględniane w rozliczeniu. Późniejsza rejestracja (po końcu czasu na wyjście) będzie skutkowała naliczeniem na koniec czasu na wyjście, wcześniejsza (przed początkiem czasu na wyjście) jako nieobecność.
Dobowa norma pracy - służy do wyliczenia normy miesięcznej na podstawie kalendarza, która jest wyświetlana w raporcie
Czas przerwy (wliczanej i niewliczanej) - czas odliczany (lub nie) od zarejestrow. czasu pracy w procesie generowania raportu.

Zmianowy (do 4 zmian, konfiguracja) - oznacza, że pracownik będzie miał ustaloną dobową normę czasu pracy. Konfiguracja czasu pracy dla systemu zmianowego odbywa się w zakładce *Kalendarze.* Przykładowe wzorce harmonogramów dla systemu z trzema zmianami pokazują poz. 4, 5 i 6.
Kolor - kolor opisu harmonogramu jaki będzie wyświetlany w kalendarzu, ważne dla systemu zmianowego.

Zwykły - oznacza, że pracownik może pracować w dowolnych godzinach i rozliczany jest miesięcznie. W ciągu każdej doby może pracować przez różną liczbę godzin. Przepracowane w ciągu poszczególnych dni godziny są sumowane i odnoszone do normy za dany okres na podstawie kalendarza.

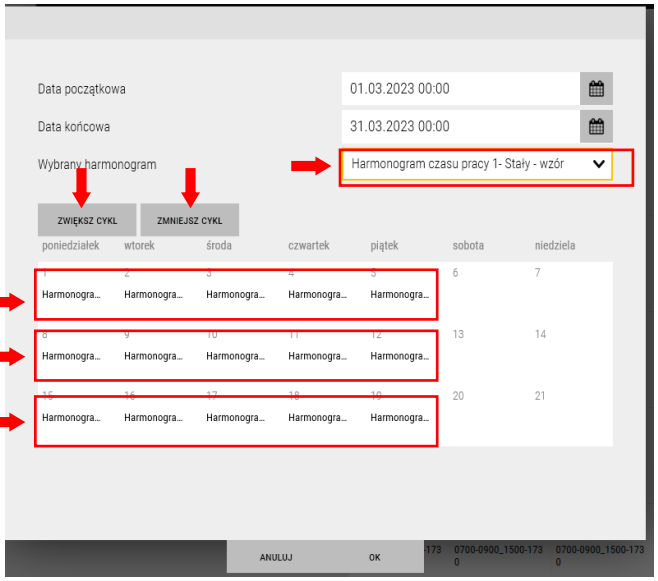
Kalendarze

Kalendarze są potrzebne do rozliczenia czasu pracy w zadanym okresie zgodnie z normą. W trakcie ich definiowanie należy przypisać do każdego roboczego dnia tygodnia wybrany harmonogram. Kalendarz przypisuje się potem użytkownikowi. Po kliknięciu na przycisk **+** w lewym oknie pojawia się nowy kalendarz z domyślną nazwą, którą można edytować.



Ustawienia

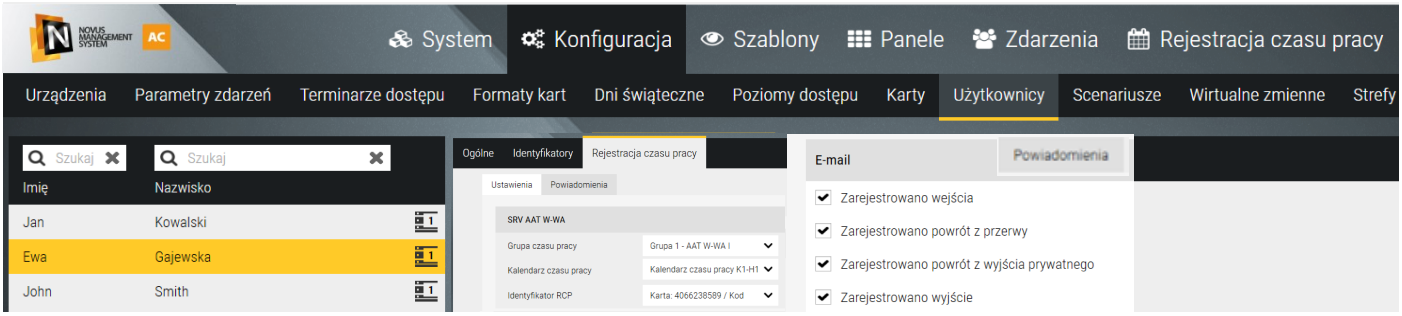
Rodzaj kalendarza - Zmianowy lub *Zwykły* - po wybraniu *Zmianowy* w pozycji *Wybrany harmonogram* mamy do wyboru zdefiniowane harmonogramy typu *Zmianowego, po wybraniu Zwykłego* harmonogramy typu *Stały, Elastyczny* i *Zwykły* . W polu obok należy wybrać miesiąc dla którego będziemy generować kalendarz z harmonogramami pracy, a na końcu rok. W oknie wyświetlane są również kafelki symbolizujące poszczególne dni danego miesiąca.
Harmonogramy do poszczególnych dni możemy przypisywać ręcznie lub korzystając z generatora raportów.
Tryb ręczny - żeby przypisać wybrany harmonogram ręcznie należy kliknąć na danym dniu lewym przyciskiem myszy, prawym - żeby usunąć.
Tryb automatyczny - kliknąć na przycisku ***Generator kalendarza***.



- ustawić datę początkową i końcową kalendarza
- wybrać harmonogram z rozwijanej listy
- klikając lewym przyciskiem myszy na dniach
- tygodnia dodać wybrany harmonogram

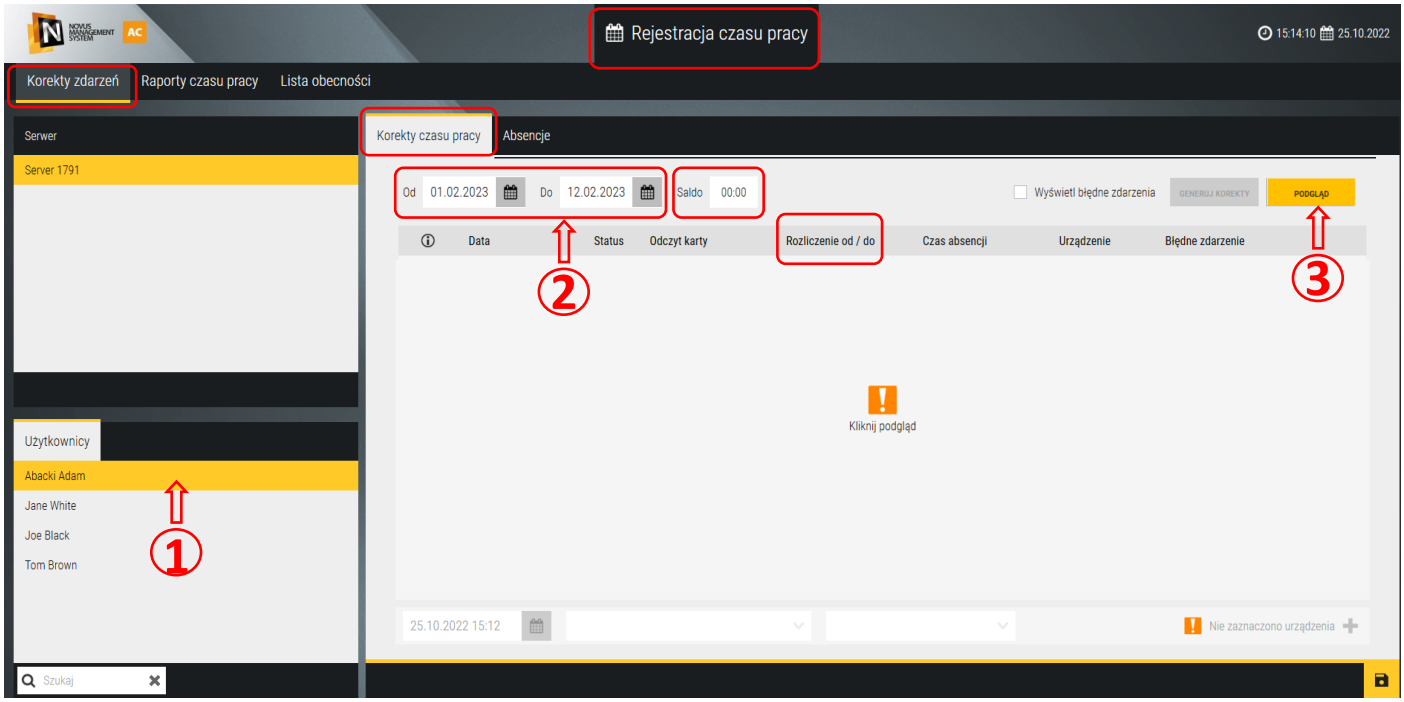
Dla trybu zmianowego należy ustawić cykl w zależności od ilości zmian klikając na przyciski ***Zwiększ/Zmniejsz cykl***. Przykład obok pokazuje cykl dla systemu z trzema zmianami w ciągu doby. W pierwszym tygodniu należy ustawić harmonogram dla pierwszej zmiany, w drugim dla drugiej itd. Po kliknięciu ***OK*** harmonogramy zostaną automatycznie przypisane w kalendarzu za cały ustawiony okres. Zaleca się wybór różnych kolorów opisów przy definiowaniu harmonogramów dla systemu zmianowego. Zakładka *Harmonogramy* zawiera przykładowe wzory dla trzech zmian.

Użytkownicy - RCP



W tej zakładce można przypisać użytkownikowi grupę i kalendarz czasu pracy oraz powiadomienia. To umożliwia rejestrację we/wy na terminalu lub wybranych czytnikach oraz generowanie raportów czasu pracy.
W zakładce powiadomienia można zaznaczyć zdarzenia RCP po wystąpieniu, których zostanie wysłany email do pracownika z podaniem aktualnego czasu dla przepracowania dobowej normy czasu pracy.
Ta funkcjonalność objęta jest płatną licencją.

Korekty zdarzeń

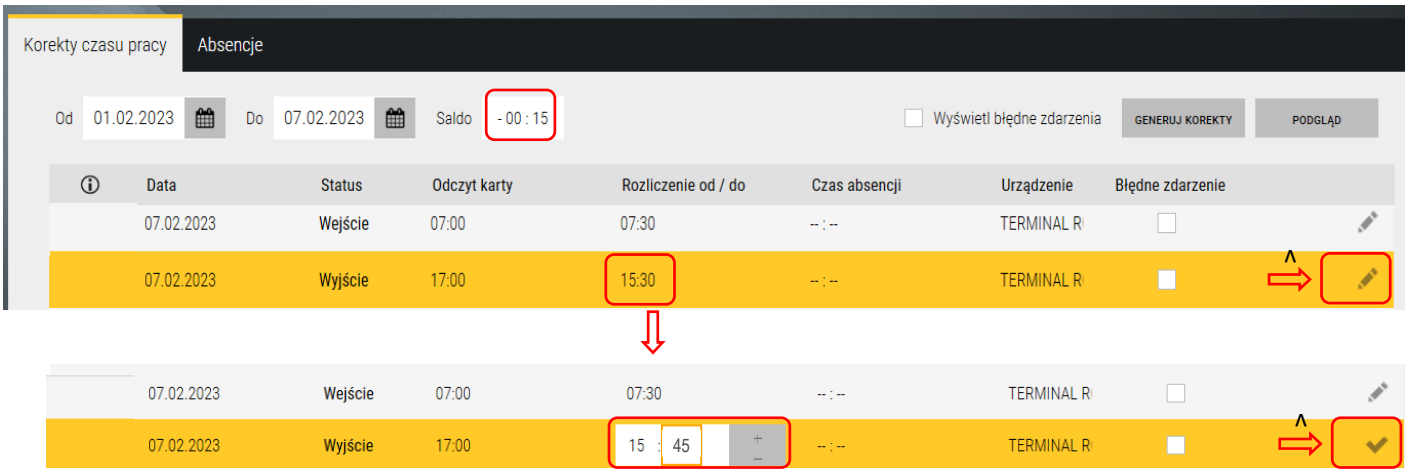


By dokonać zmian w czasie pracy danego pracownika, w podzakładce *Korekty czasu pracy* należy kolejno:

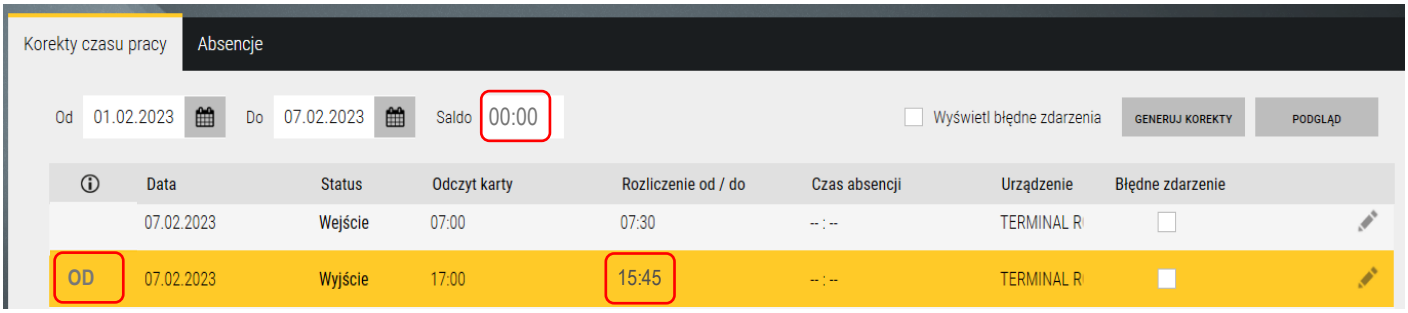
1) po lewej stronie zaznaczyć odpowiedniego pracownika
2) W górnej części okna wyświetlany jest zakres dni obejmujący domyślny okres rozliczeniowy (od początku miesiąca do końca dnia poprzedniego) oraz **saldo wyliczone za ten okres**. Można ustawić inny zakres dat.
3) kliknąć ***Podgląd*** w prawym górnym rogu

Spowoduje to wygenerowanie listy wszystkich zdarzeń dokonanych przez pracownika w ustawionym okresie w kolejności chronologicznej. Każda doba musi zaczynać się od wejścia i kończyć wyjściem. Podobnie każde wyjście w ciągu dnia pracy musi mieć powrót. Tylko w tedy saldo oraz wygenerowany w następnej podzakładce raport będzie poprawny. Brakujące rejestracje należy uzupełnić w sposób opisany poniżej, a błędne zdarzenia zaznaczyć w kolumnie *Błędne zdarzenia* i zapisać, żeby nie były wyświetlane i brane pod uwagę przy rozliczaniu czasu pracy. Dlatego po wygenerowaniu podglądu należy przejrzeć listę pod kątem prawidłowych sekwencji we/wy.

Od wersji 5 programu w oknie tym oprócz pola „Saldo" jest również nowa kolumna *Rozliczenie od/do*, która służy do korekty czasu pracy, gdy pojawia się saldo ujemne i pracownik go odpracował. Tylko to pole jest edytowalne i pozwala ustawić godzinę początku lub końca czasu pracy. To w efekcie powoduje przeliczenie na nowo salda czasu pracy za podany okres. Godziny rejestracji we/wy pozostają cały czas niezmienione co pozwala na łatwą analizę poprawności rozliczenia. Edycja pola początku/końca czasu pracy odbywa się poprzez kliknięcie na ikonie edycji na końcu wiersza. Po ustawieniu nowej godziny zatwierdzamy operację klikając na ikonie ***Zatwierdź*** na końcu linii. Po każdej takiej operacji należy kliknąć ***Zapisz*** w prawym dolnym rogu okna i sprawdzić skorygowane saldo.
Ustawiona w tej kolumnie godzina końca pracy nie może być późniejsza niż godzina *WY* w kolumnie *Odczyt karty* oraz nie może wychodzić poza zakres godzin pracy ustalonych dla danego działu.
Jeżeli po korekcie saldo jest w dalszym ciągu ujemne, należy wyszukać innego dnia w którym można dokonać takiej korekty lub poprosić pracownika o odpracowanie w następnych dniach. Po akceptacji korekty i zapisie na początku wiersza pojawia się znak **OD** - odpracowanie.
Przykład korekty:
Saldo i godzina końca pracy przed korektą odpracowania.



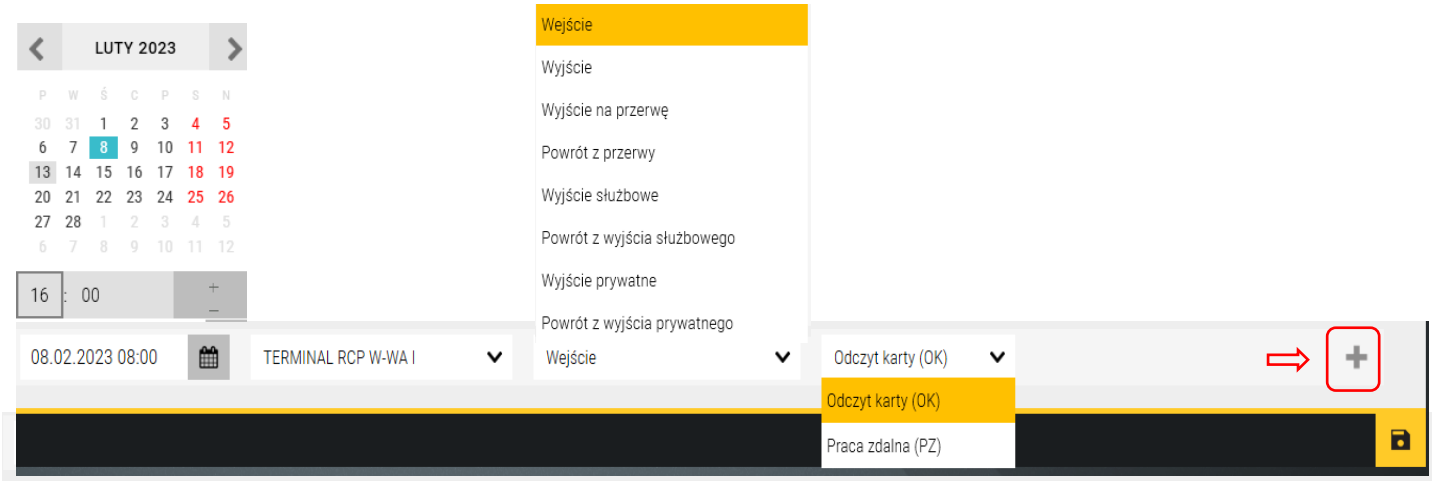
„Rezerwa" czasowa na wyjściu wynosi 01:30 godziny w dniu 07.02.2023.
Saldo i godzina końca pracy po korekcie odpracowania.



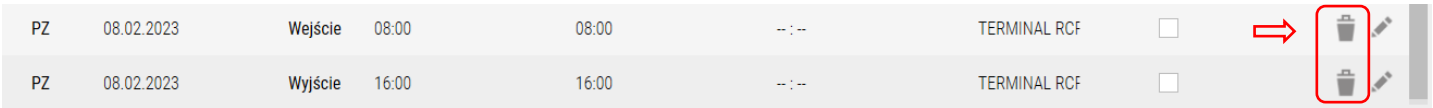
Z „rezerwy" zostało wykorzystane 00:15 minut, co wystarcza do wyzerowania ujemnego salda.
Okienko salda ułatwia i przyspiesza wykonywanie korekt ponieważ nie ma potrzeby odczytywania go z raportu.
Czas w kolumnie *Rozliczenie od/do* można użyć tylko dla rejestracji we/wy normalnego ponieważ dotyczy to początku i końca czasu pracy dla wypracowania normy.
W przypadku we/wy w ciągu dnia pracy, jeżeli wystąpią jakieś pomyłki (np. podwójny odczyt) lub braki rejestracji to wówczas należy wykorzystać opcję związaną z kolumną *Błędne zdarzenie* i dodać poprawną rejestrację ręcznie w sposób opisany w dalszej niniejszej instrukcji.

Można dokonać modyfikacji zarówno w ramach zarejestrowanego zdarzenia w sposób opisany na poprzedniej stronie jak również dodać całkiem nowe zdarzenie (np. w przypadku braku odczytu karty przez pracownika w związku z pracą wykonywaną zdalnie - PZ).
W tym przypadku, należy wykonać następujące czynności w wierszu na dole okna:

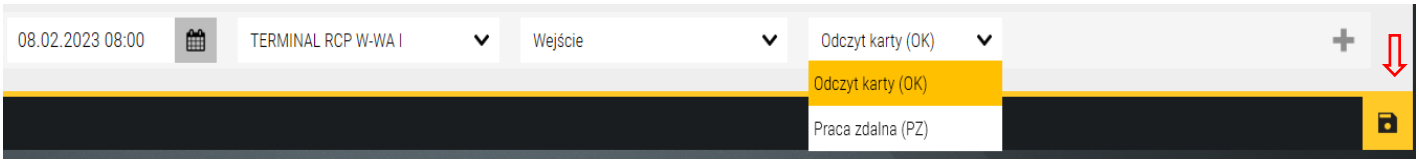
1) klikając w ikonę ***Kalendarza*** - ustawić datę oraz godzinę wprowadzanego zdarzenia
2) zaznaczyć odpowiedni dla danego pracownika/lokalizacji terminal
3) określić rodzaj wprowadzanego zdarzenia
4) kliknąć ikonę **„+”** znajdującą się na końcu wiersza



Wprowadzona modyfikacja pojawi się na liście zdarzeń pracownika w kolejności chronologicznej z symbolem ***OK*** *lub* ***PZ*** oraz symbolem ***Kosza***. Kliknięcie na ikonie ***Kosz*** usuwa nieprawidłowy wpis z listy przed zapisem.

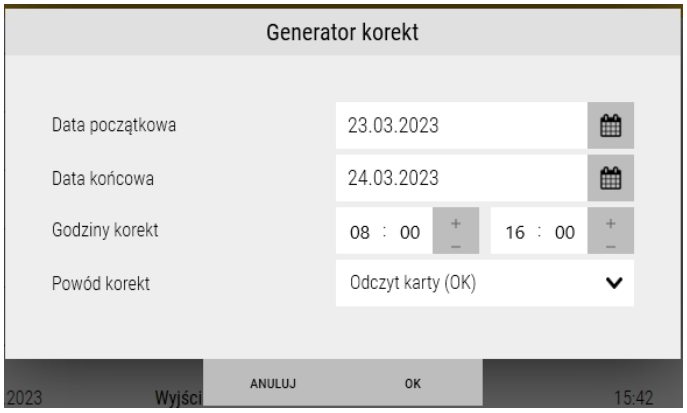


Jeśli wszystkie parametry zostały ustawione poprawnie, wprowadzone zmiany należy zapisać, korzystając z symbolu ***Dyskietki***. Po zapisie ikona ***Kosza*** znika.



Po dodaniu i zapisie wejścia w analogiczny sposób dodać wyjście.
Jeśli brak we/wy obejmuje kilka kolejnych dni, warto skorzystać z generatora korekt W tym celu :

1) klikamy przycisk ***Generuj korekty***
2) ustawiamy datę początkową i końcową
3) wybieramy typ nieobecności z rozwijanej listy
4) klikamy ***OK***.



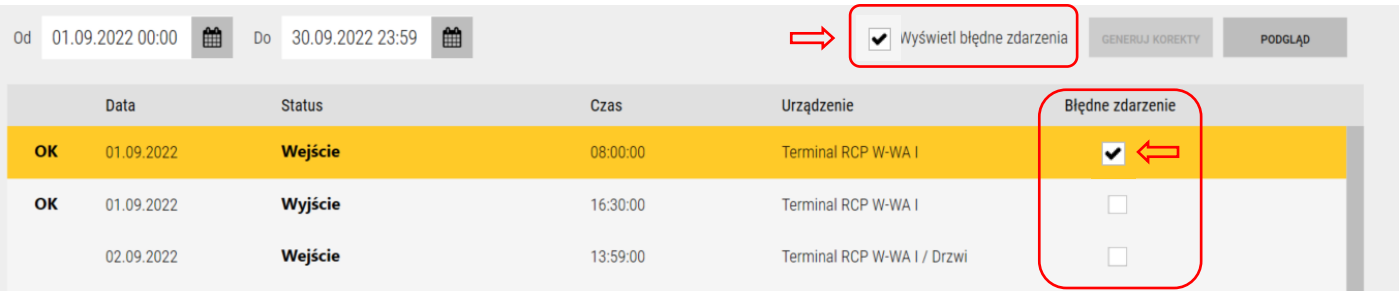
Dodane we/wy pojawią się na liście, a po zapisaniu i kliknięciu *Podgląd* również na karcie *Korekty czasu pracy* po wybraniu odpowiedniego zakresu dat. Można ją usunąć klikając na ikonie ***Kosza***. Dodana korekta wymaga zapisu (***Dyskietka***).

UWAGA!

Nieprawidłowe odczyty z terminala lub błędnie zapisane korekty ręczne *OK* / PZ można ukryć zaznaczając pole w kolumnie *Błędne zdarzenie*.

W tym celu należy:

1) zaznaczyć checkbox dla danego zdarzenia w kolumnie *Błędne zdarzenie*



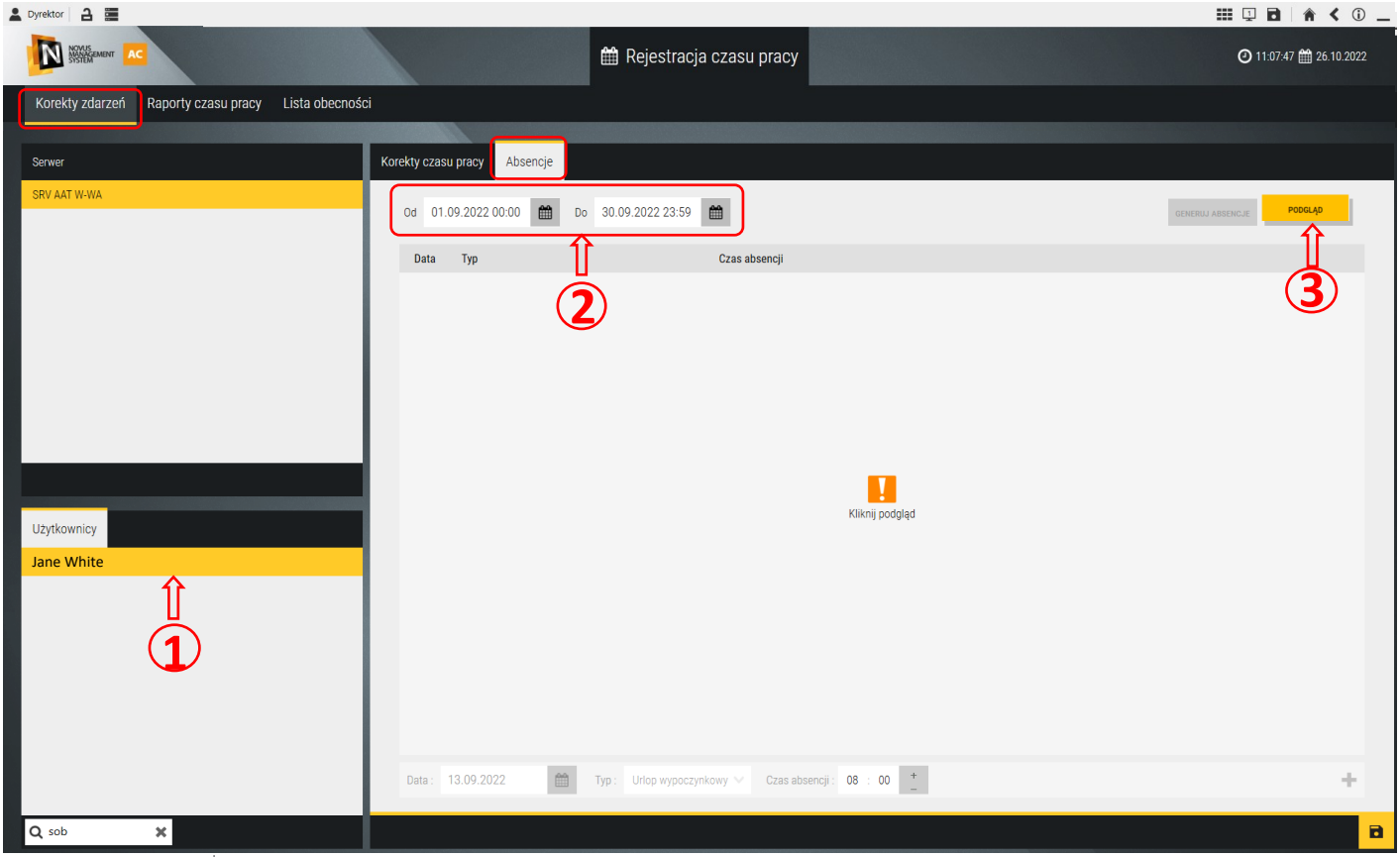
2) kliknąć zapisz (***Dyskietka***).

Tak wykonana operacja spowoduje, że zaznaczony wiersz zniknie z listy zdarzeń danego pracownika i nie będzie brany pod uwagę przy kalkulacji i w raporcie. Można je przywrócić zaznaczając pole ***Wyświetl błędne zdarzenia*** i ***Podgląd***, a następnie odznaczyć pole i zapisać.

Podzakładka *Absencje*

By dodać lub usunąć absencję danego użytkownika, w podzakładce *Absencje* należy kolejno:

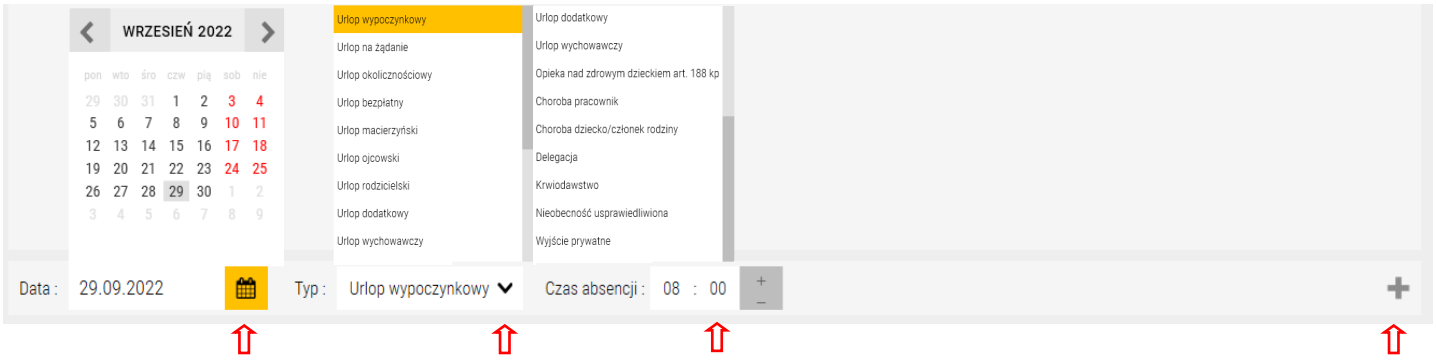
1) po lewej stronie zaznaczyć odpowiedniego pracownika
2) zaznaczyć okres, w ramach którego chcemy dokonać modyfikacji
3) kliknąć ***Podgląd*** w prawym górnym rogu.



Wykonane powyżej operacje wygenerują listę wszystkich absencji pracownika w zaznaczonym okresie w kolejności chronologicznej. W przypadku ich braku - okno pozostanie puste.

W celu dodania absencji, należy wykonać następujące czynności w wierszu na dole okna:

1) klikając w ikonę ***Kalendarza*** - ustawić datę wprowadzanego zdarzenia
2) wybrać typ absencji z rozwijanej listy
3) ustawić czas absencji - dzienna norma czasu pracy z harmonogramu lub czas np.. Urlopu opiekuńczego nad dzieckiem
4) kliknąć ikonę **„+”** znajdującą się na końcu wiersza.

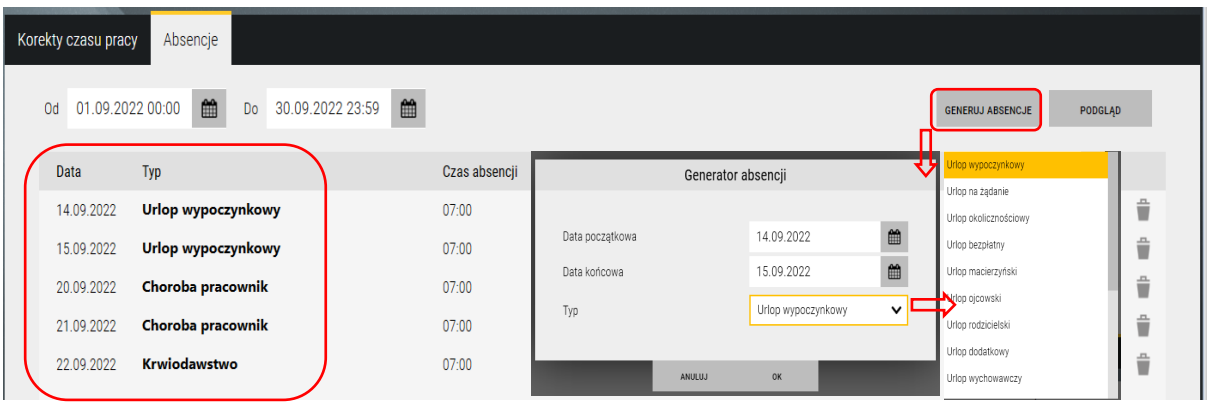


Wprowadzona modyfikacja pojawi się na liście absencji pracownika w kolejności chronologicznej z symbolem ***Kosza***. Kliknięcie na ikonie ***Kosz*** przed zapisem usuwa wpis z listy. Dodana absencja wymaga zapisu (***Dyskietka***).

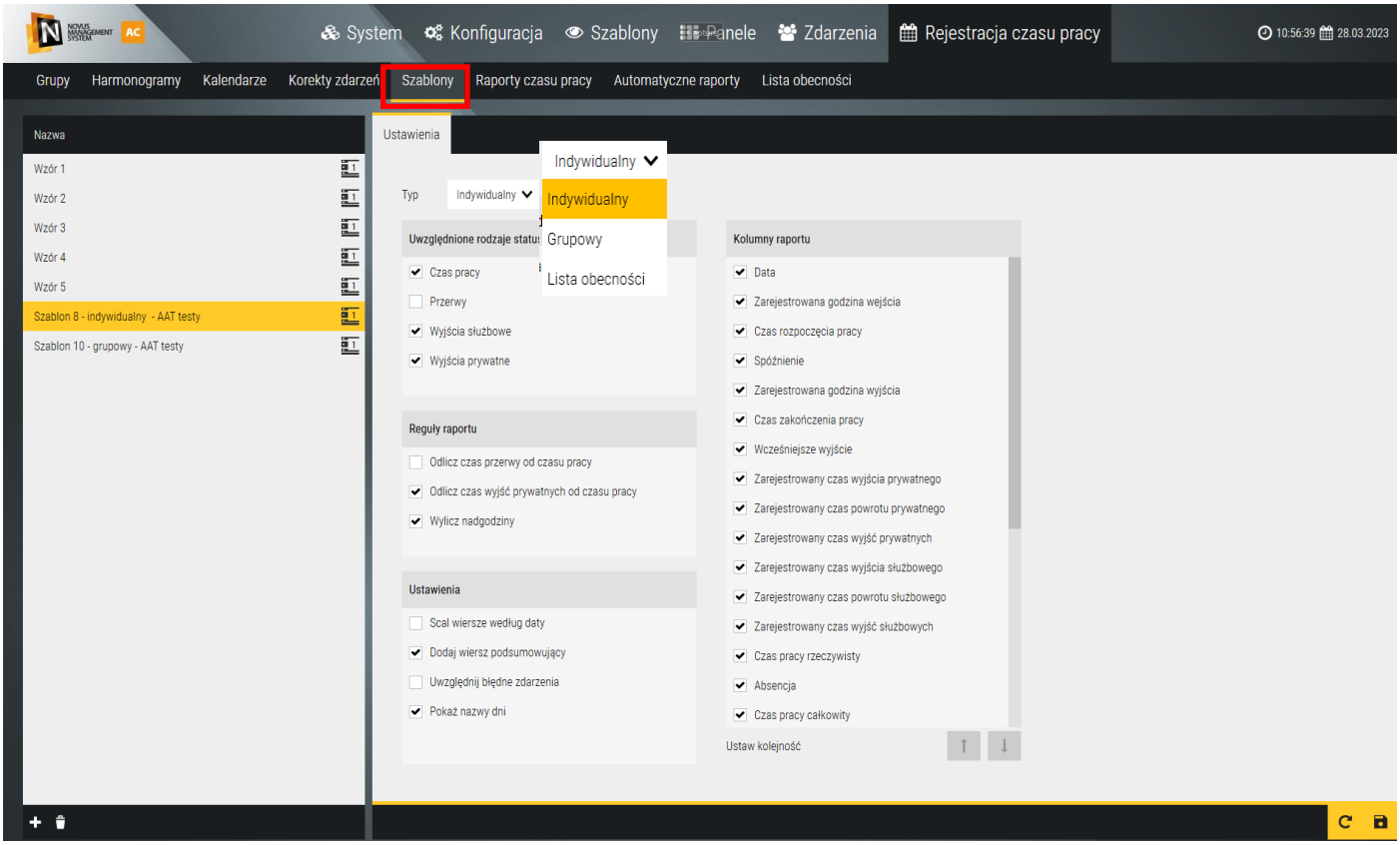
Wskazówka:
Jeśli absencja obejmuje kilka kolejnych dni, warto skorzystać z generatora absencji. W tym celu na karcie *Absencje*:

1) klikamy przycisk ***Generuj Absencje***
2) ustawiamy czas trwania absencji - datę początkową i końcową
3) wybieramy typ absencji z rozwijanej listy
4) klikamy ***OK***.

Dodane absencje pojawią się na liście, a po zapisaniu i kliknięciu ***Podgląd*** również na karcie *Korekty czasu pracy* po wybraniu odpowiedniego zakresu dat. Można ją usunąć klikając na ikonie ***Kosza***. Dodana absencja wymaga zapisu (***Dyskietka***).



Szablony



Ta zakładka umożliwia zdefiniowanie szablonów niezbędnych do generowania raportów RCP.
Do wyboru mamy trzy typy szablonów do raportów indywidualnych, grupowych i z listy obecności.
Każdy z typów oferuje inny zestaw kolumn do wyboru.
Lewe okno zawiera pięć zdefiniowanych domyślnie wzorów do raportów indywidulanych, grupowych i generowanych z listy obecności. Tych szablonów nie można edytować - można je wykorzystać do generowania raportów lub jako przykłady do zdefiniowania własnych raportów.
Aby zdefiniować nowy raport należy kliknąć znak plus w lewym dolnym rogu okna, a następnie zaznaczyć wybrane pola w prawym oknie.
Listy w sekcjach w prawym oknie pozwalają wybrać następujące parametry szablonu.

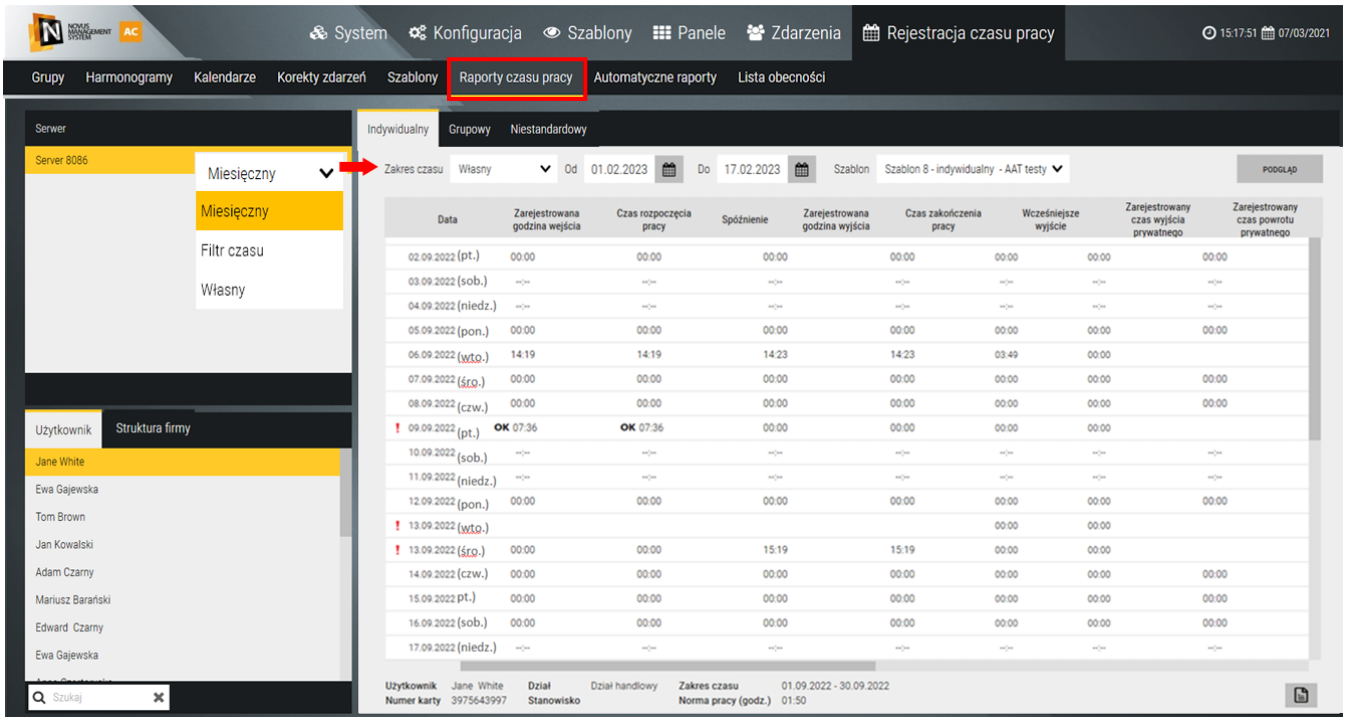
Uwzględnione rodzaje statusu - należy zaznaczyć, które rodzaje statusu pracy mają być uwzględnione w raporcie. Te ustawienia mają wpływ na wygląd i sposób naliczania czasu pracy.

Reguły raportu - definiują czy w kalkulacji raportu maja być uwzględnione wyjścia na przerwę oraz prywatne.

Ustawienia - pozwalają określić wygląd formularza raportu.

Kolumny raportu - checkboxy pozwalają określić, które kolumny będą wyświetlane w raporcie. Pozwala to uniknąć wyświetlania lub drukowania zbędnych kolumn. Pozycje zaznaczone ustawiane są na początku listy. W zależności od potrzeby ten sam raport można wygenerować z wykorzystaniem różnych szablonów, żeby otrzymać wynik w interesującej nas formie. Kolejność kolumn w szablonie, które zostały zaznaczone (czyli również w raporcie) można zmieniać za pomocą strzałek na dole lewego okna. Po zaznaczeniu wybranej pozycji na liście można ja przesunąć w górę lub w dół.

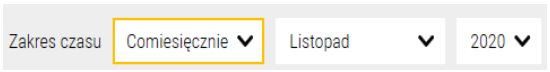
Raporty



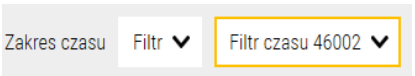
Raport indywidualny rozliczający czas pracy pracownika generowany jest na podstawie zdarzeń z czytników wejścia/wyjścia przypisanych do grup RCP. Na górnym pasku mamy filtry pozwalające ustawić parametry raportu:

W zakresie czasu mamy wyboru trzy opcje:

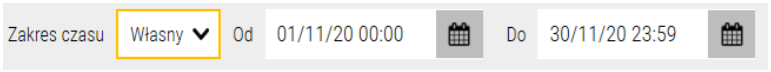
1. Z całego miesiąca (domyślnie poprzedniego)



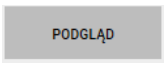
2. Z zakresu czasu ustawionego w wybranym filtrze czasu



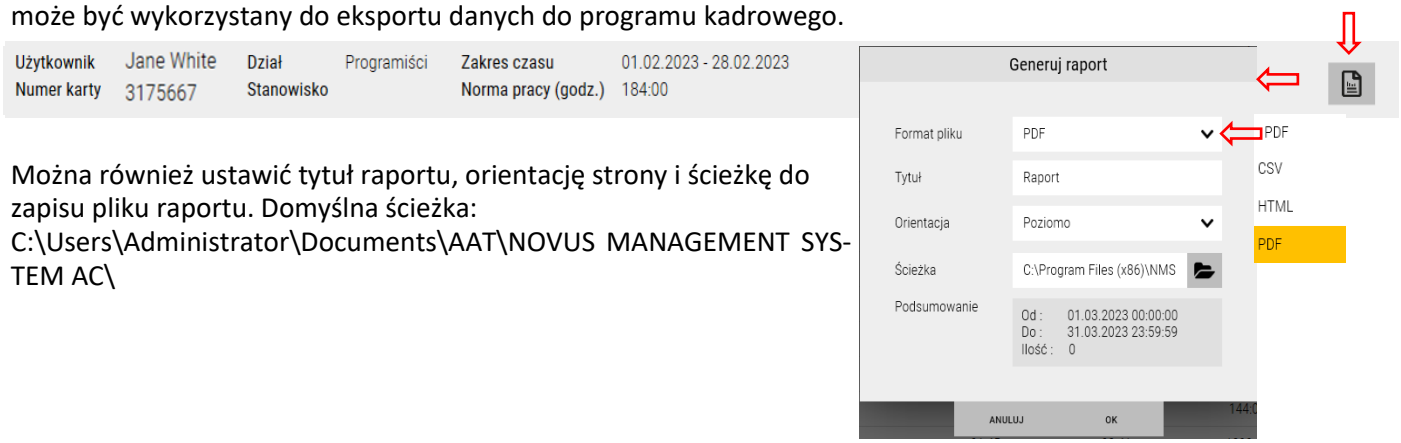
3. Z zakresu zdefiniowanego według kalendarza



W systemie z wieloma serwerami należy wybrać serwer (domyślnie jest lokalny) a następnie dział.
Do wyszukania nazwy działu można użyć pola ***Szukaj***.
Z rozwijanej listy wybrać *Szablon* raportu. Po ustawieniu filtrów należy kliknąć na przycisku ***Podgląd***.

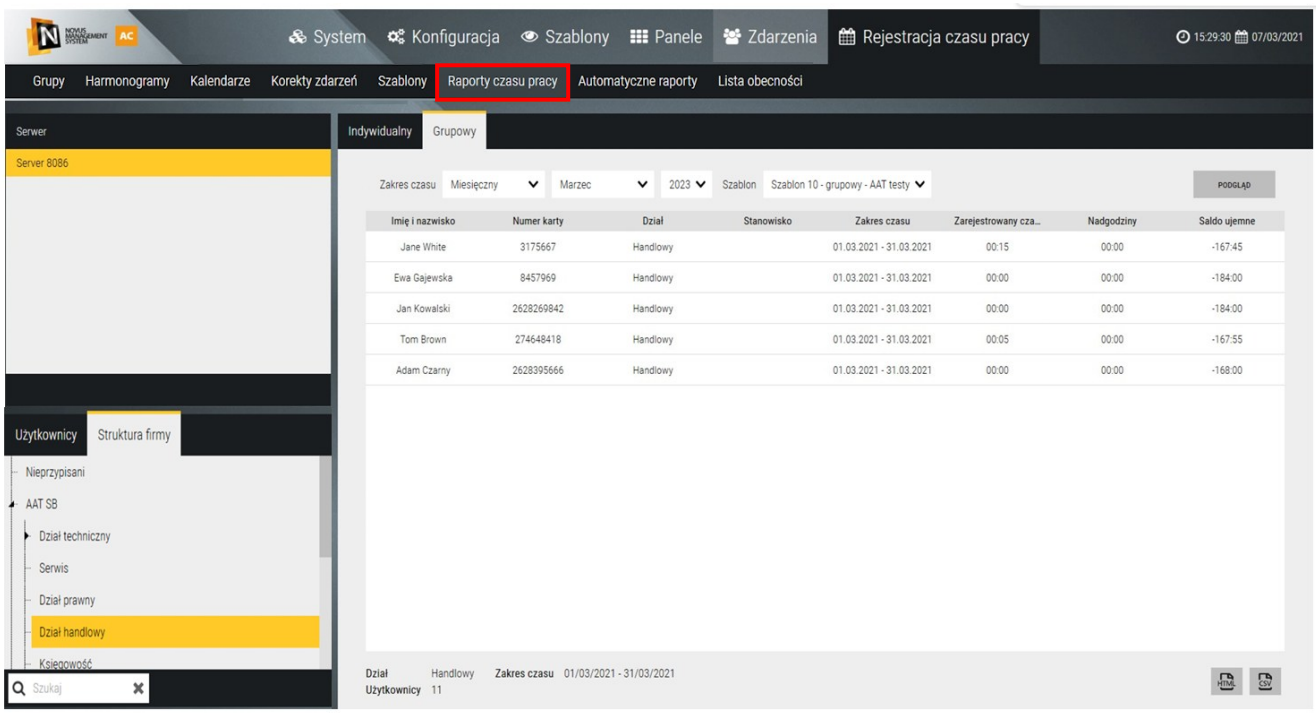


Raport zostanie wyświetlony na ekranie. Na dole raportu wyświetlone jest podsumowanie.
Wyświetlony raport zawiera w każdej linii zestawienie przepracowanych godzin w jednym dniu, obejmuje wybrany zakres dat i można go zapisać do pliku w formacie HTML, PDF lub jako plik edytowalny w formacie CSV. Ten ostatni może być wykorzystany do eksportu danych do programu kadrowego.



Można również ustawić tytuł raportu, orientację strony i ścieżkę do zapisu pliku raportu. Domyślna ścieżka: C:\Users\Administrator\Documents\AAT\NOVUS MANAGEMENT SYSTEM AC\

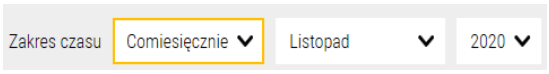
Raport grupowy



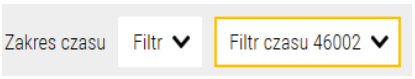
Raport grupowy rozliczający czas pracy wybranego działu generowany jest na podstawie zdarzeń z czytników wejścia/wyjścia przypisanych do grup RCP. Na górnym pasku mamy filtry pozwalające ustawić parametry raportu:

W zakresie czasu mamy wyboru trzy opcje:

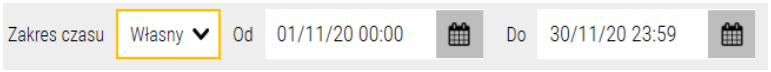
1. Z całego miesiąca (domyślnie poprzedniego).



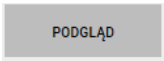
2. Z zakresu czasu ustawionego w wybranym filtrze czasu



3. Z zakresu zdefiniowanego według kalendarza

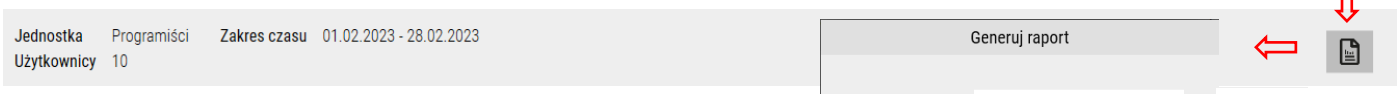


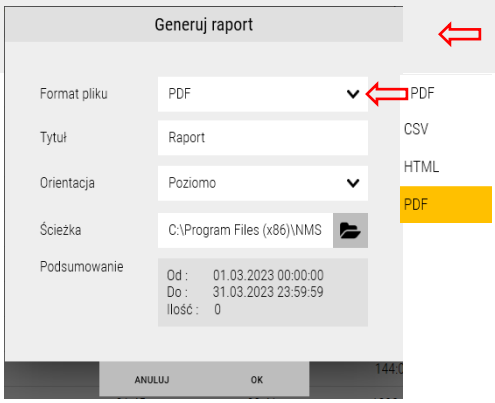
W systemie z wieloma serwerami należy wybrać serwer (domyślnie jest lokalny) a następnie dział.
Do wyszukania nazwy działu można użyć pola ***Szukaj***.
Z rozwijanej listy wybrać *Szablon* raportu. Po ustawieniu filtrów należy kliknąć na przycisku ***Podgląd***.



Raport zostanie wyświetlony na ekranie. Na dole raportu wyświetlone jest podsumowanie.
Wyświetlony raport zawiera w każdej linii podsumowanie przepracowanych godzin dla jednego pracownika i można go zapisać do pliku w formacie HTML, PDF lub jako plik edytowalny w formacie CSV. Ten ostatni może być wykorzystany do eksportu danych do programu kadrowego.

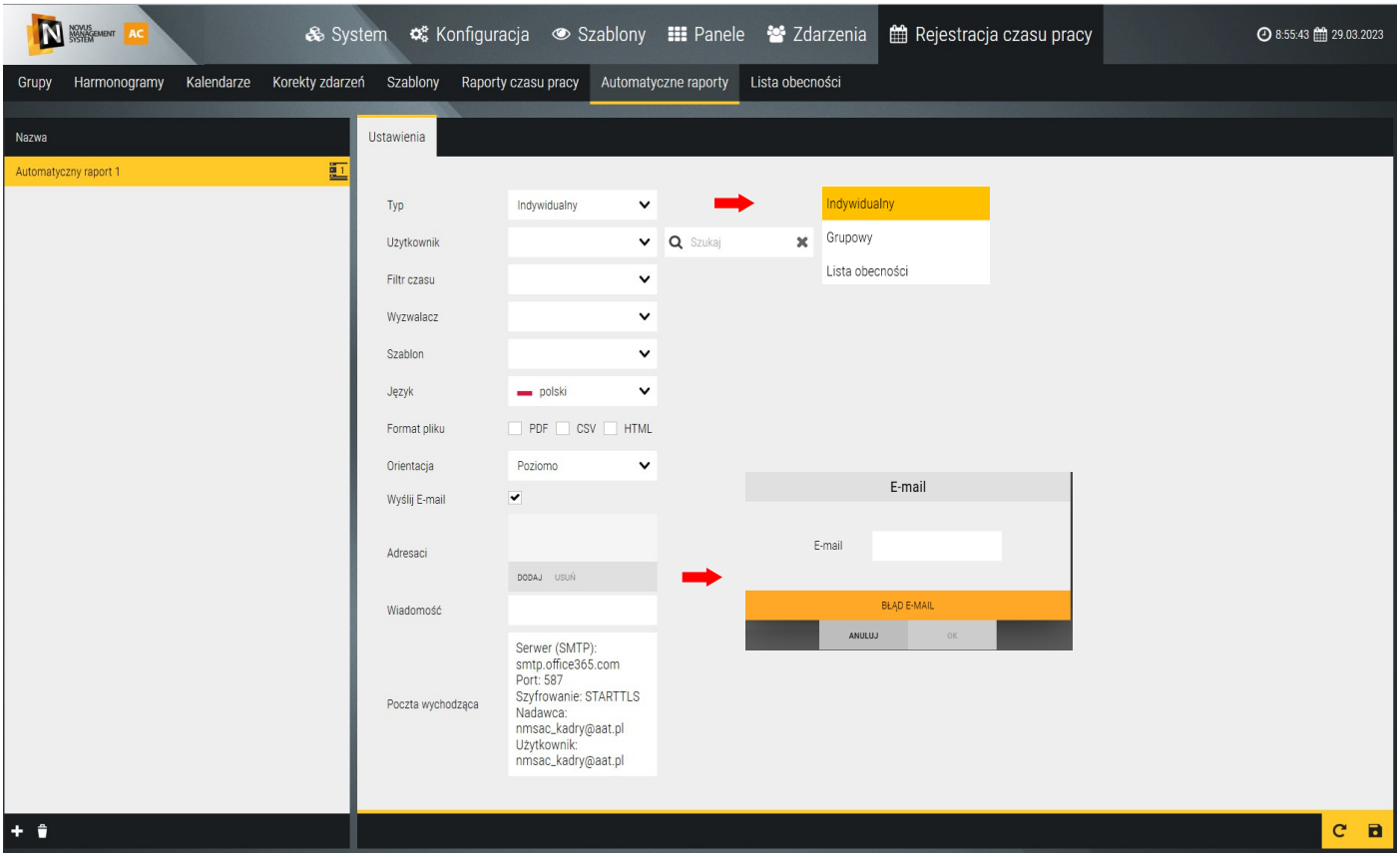
Zapisz plik





Można również ustawić tytuł raportu, orientację strony i ścieżkę do zapisu pliku raportu. Domyślna ścieżka:
C:\Program Files (x86)\NOVUS MANAGEMENT SYSTEM AC\Client\Reports

Raporty automatyczne



Raport rozliczający czas pracy może być generowany ręcznie przez operatora w sposób opisany w poprzednim punkcie lub w sposób automatyczny zgodnie z ustalonym kalendarzem. Po kliknięciu na przycisk **+** w lewym oknie pojawia się nowy szablon raportu z domyślną nazwą, którą można edytować.

Następnie w prawym oknie należy ustawić parametry filtrów.

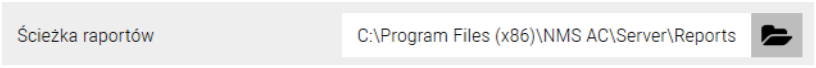
Filtr czasu, Wyzwalacz i Szablon trzeba wcześniej zdefiniować w zakładce Szablony.

Filtr czasu pozwala określić przedział/przedziały czasowe, które obejmie raport.

Wyzwalacz pozwala ustawić godzinę, dzień oraz cykl w jakim ma być powtarzane generowanie raportów.

Można wybrać również język raportu, format pliku i orientację.

Domyślny folder do zapisywania raportów:



Można go zmienić w zakładce *System / Ustawienia serwerów.*

Wygenerowany raport można wysłać na email po zaznaczeniu checkboxa oraz ustawieniu adresata.

Poprawne działanie tej opcji wymaga ustawienia parametrów poczty wychodzącej w zakładce: *System / Ustawienia serwerów/ Poczta wychodząca.*

Przykładowe raporty

PDF:

Szablon 4 - Grupowy standardowy
Serwis
01.07.2024 00:00 - 31.07.2024 23:59

Imię i nazwisko	Numer karty	Dział	Zakres czasu	Czas pracy rzeczywisty
[redacted]	[redacted]	Serwis	01.07.2024 - 31.07.2024	32:00
[redacted]	[redacted]	Serwis	01.07.2024 - 31.07.2024	72:00
[redacted]	[redacted]	Serwis	01.07.2024 - 31.07.2024	72:00
[redacted]	[redacted]	Serwis	01.07.2024 - 31.07.2024	72:00
[redacted]	[redacted]	Serwis	01.07.2024 - 31.07.2024	72:00
[redacted]	[redacted]	Serwis	01.07.2024 - 31.07.2024	72:00
[redacted]				392:00

CSV:

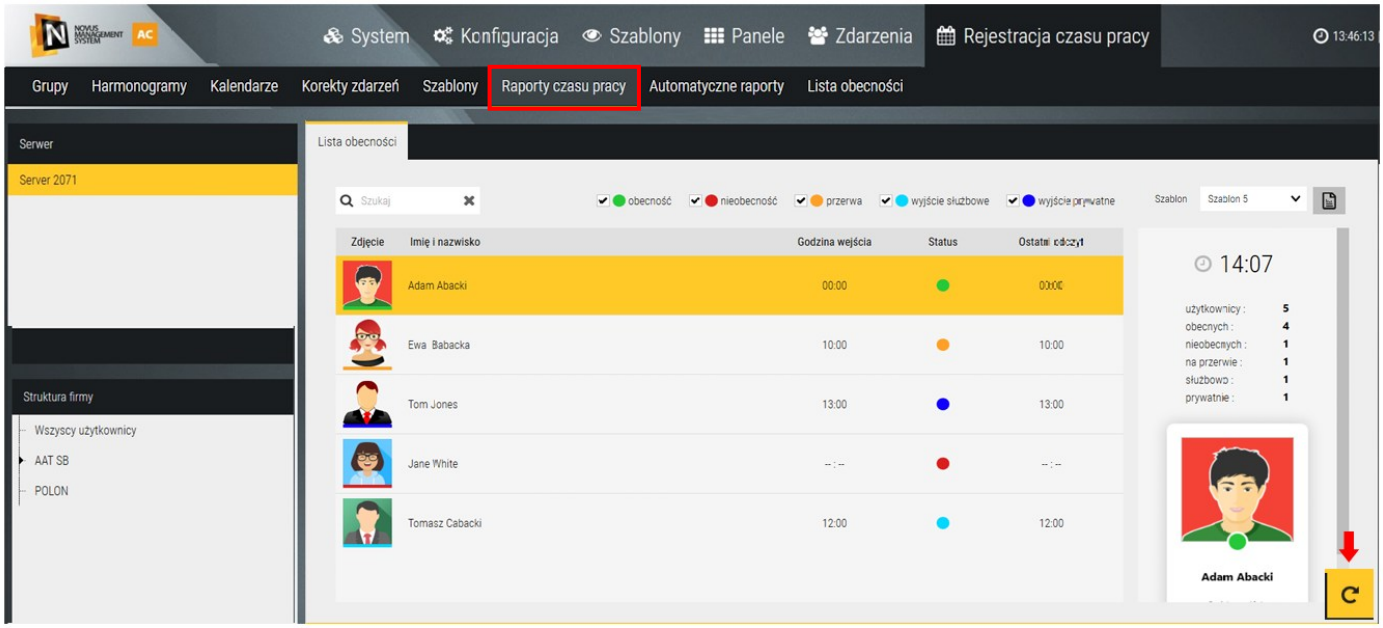
	A	B	C	D	E	F
1	Adam Nowak					
2	Raport czasu pracy dla działu					
3	01.07.2024 00:00 - 12.07.2024 23:59					
4	Data	Spóźnienie	Czas przekroczenia przerwy	Zarejestrowana godzina wyjścia	Czas pracy całkowity	
5	01-07-2024 (pon)	00:00	00:00	08:58		
6	15:30	08:00				
7	02-07-2024 (wt)	00:00	00:00	16:31	08:00	
8	03-07-2024 (śr)	00:00	00:00	15:33	08:00	
9	04-07-2024 (czw)	00:00	00:00	15:32	08:00	
10	05-07-2024 (pt)	00:00	00:00	15:41	08:00	
11	06-07-2024 (sob)	--:--	--:--	--:--	--:--	
12	07-07-2024 (niedz)	--:--	--:--	--:--	--:--	
13	08-07-2024 (pon)	00:00	00:00	15:39	08:00	
14	09-07-2024 (wt)	00:07	00:00	16:37	08:00	
15	10-07-2024 (śr)	00:00	00:00	15:30	08:00	
16	11-07-2024 (czw)	00:00	00:00	15:31	08:00	
17	12-07-2024 (pt)	00:00	00:00	00:00	00:00	
18	Podsumowanie	00:07	00:00		72:00:00	
19						
20						
21						

HTML:

Szablon 3 - Indywidualny pełny
[redacted]
01.07.2024 00:00 - 31.07.2024 23:59

Data	We-Wy normalne	Zarejestrowana godzina wejścia	Czas rozpoczęcia pracy	Zarejestrowana godzina wyjścia	Czas zakończenia pracy	Spóźnienie	Wcześniejsze wyjście	We-Wy przerwa	Zarejestrowany czas wyjścia na przerwę	Zarejestrowany czas powrotu z przerwy	Czas przerwy wg harmonogramu
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

Lista obecności

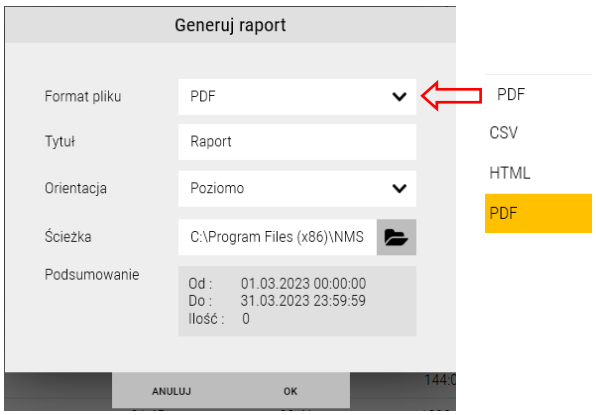


Lista obecności pozwala bardzo szybko zweryfikować aktualny stan obecności pracowników. Po otwarciu okna wyświetlana jest w nim lista pracowników ze zdjęciami oraz status obecności i godzina zarejestrowanego wejścia do firmy. Status zgodnie z legendą pokazuje jeden z pięciu stanów: obecność, nieobecność oraz wyjścia w czasie pracy.

Listę można sortować klikając na nagłówki kolumn: *Godzina wejścia*, *Status* i *Ostatni odczyt*.

Z prawej strony okna wyświetlana jest godzina - po otwarciu okna jest to czas aktualny i status obecności na tą chwilę. Odświeżanie statusu po przez kliknięcie na przycisku ***Odśwież.***

Ikona  w prawym górnym rogu umożliwia wygenerowanie i zapisanie raportu z listy obecności na daną chwilę.

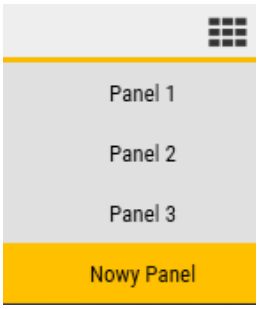


Generowanie raportu z listy obecności możliwe jest również w trybie automatycznym.

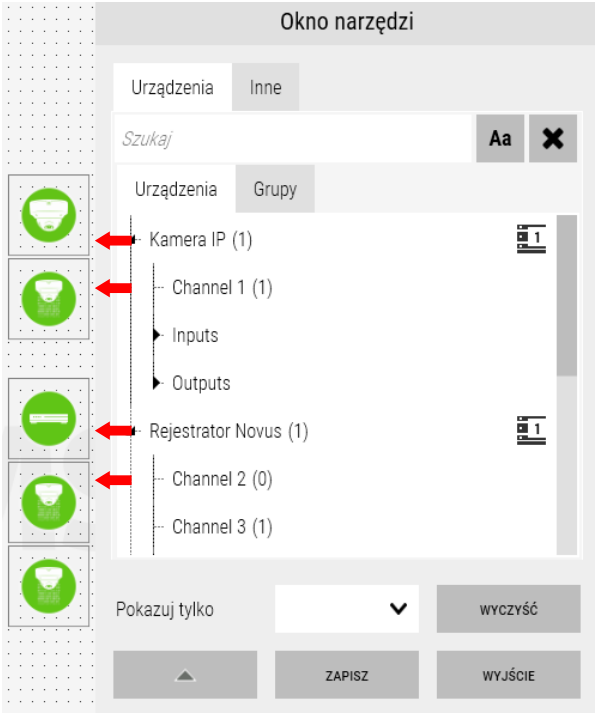
9.5 Integracja z urządzeniami VSS

Program NOVUS MANAGEMENT SYSTEM AC umożliwia integrację z systemem telewizji dozorowej. Dodawanie urządzeń tego typu zostało opisane w rozdziale **3.10 Urządzenia - Telewizja dozorowa**.

Podłączone urządzenia można obsługiwać z poziomu *Paneli* opisanych w rozdziale **6. Panele**. Domyślny *Panel 3* zawiera okno widoków wideo. Można go zmodyfikować lub stworzyć nowe panele, aby w pełni wykorzystać możliwości integracji z urządzeniami VSS. W tym celu należy wejść w dany panel za pomocą przycisku znajdującego się w głównej belce programu i wyboru odpowiedniego panelu.



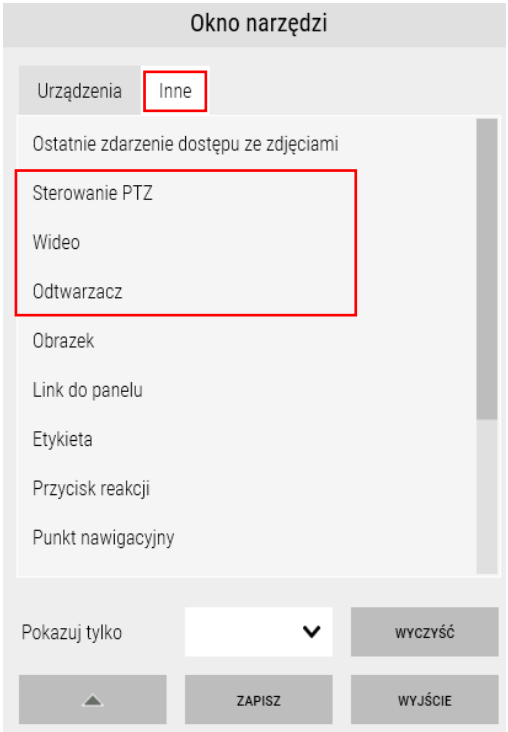
Po wyborze panelu można przejść do jego edycji za pomocą ikony ***ołówka*** . Pojawia się wtedy ***Okno narzędzi***, w którym znajdują się wszystkie elementy do konfiguracji panelu. W zakładce *Urządzenia* możemy znaleźć dodane wcześniej urządzenia VSS. Można je przenieść na panel przeciągając samo urządzenie lub strumienie wideo. Po wyjściu z trybu edycji kliknięcie myszką na ikonę ***urządzenia*** pozwala wyświetlić jego listę zdarzeń. Kliknięcie na ikonę ***strumienia wideo*** pokazuje obraz z kamery w wyskakującym okienku.



Zakładka *Inne* w ***Oknie narzędzi*** pokazuje pozostałe elementy do konfiguracji panelu. Do integracji urządzeń VSS istotne są narzędzia *Wideo*, *Odtwarzacz* oraz *Sterowanie PTZ* .

Warto zwrócić uwagę na opcje pojawiające się po kliknięciu na ikonę ***strumienia*** w trybie edycji:

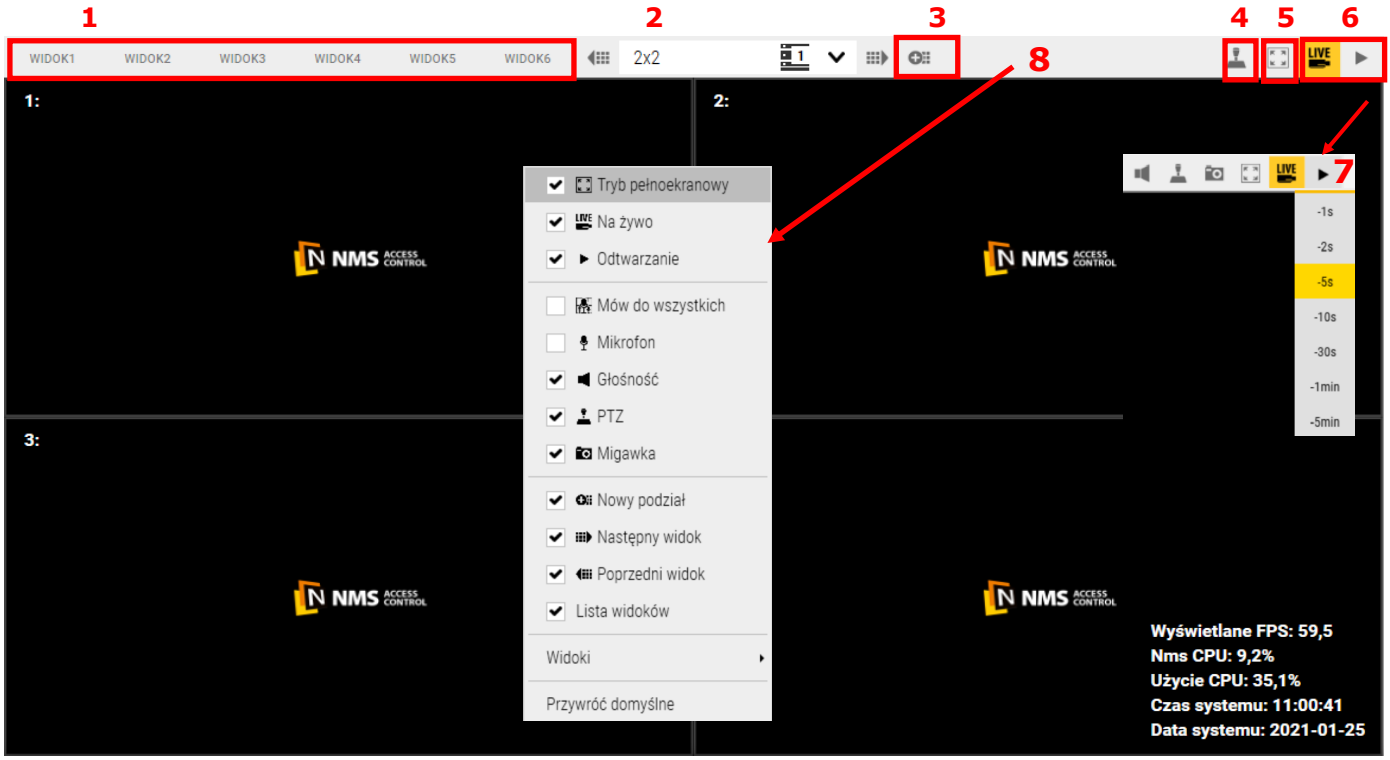
- Włącz OSD - checkbox włączający wyświetlanie w obrazie parametrów strumienia wideo.
- Zostaw podgląd otwarty - po zaznaczeniu tego checkboxa strumień wideo będzie się wyświetlał dopóki użytkownik nie zamknie go za pomocą czerwonego krzyżyka znajdującego się w prawym górnym rogu okienka. Przy wyłączonej opcji obraz znika przy pierwszym kliknięciu w inny obiekt.
- Rozmiar podglądu - pole wyboru pozwalające zdefiniować wielkość wyskakującego okna wideo.



Kolejną funkcją jest dwukrotne kliknięcie w wyskakujące okienko wideo powodujące wyświetlenie strumienia na pełnym ekranie. Z kolei zaznaczenie fragmentu na obrazie uruchamia cyfrowy zoom, który można regulować za pomocą rolki myszy. Wyjście z tej funkcji następuje za pomocą prawego przycisku myszy.

9.5.1 Narzędzia do integracji VSS - Wideo

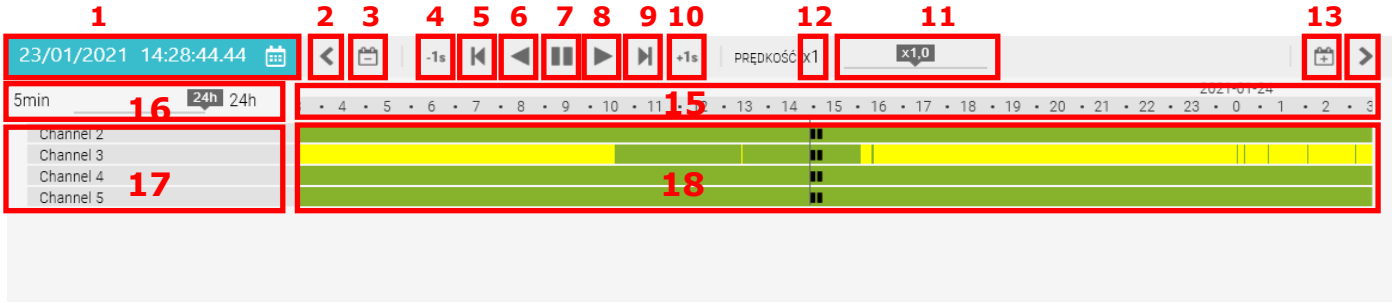
Okno ***Wideo*** służy do wyświetlania strumieni wideo. Wyświetla kamery zdefiniowane wcześniej w *Szablonach*, zakładka *Widoki wideo*. (opisane w rozdziale **5.1 Widoki wideo**). W górnej belce tego okna znajdują się ikony do zarządzania oknem.



1. Przyciski widoków - skróty wyświetlania zdefiniowanych *Widoków wideo*. Początkowo przyciski nie mają zdefiniowanych widoków. Aby je przypisać należy nacisnąć dany skrót prawym przyciskiem myszy. Można wtedy dodać *Widok wideo* lub zmienić nazwę przycisku skrótu. Do zdefiniowanego przycisku można podpiąć wiele widoków. W takiej sytuacji po jego naciśnięciu pojawi się liska przypisanych widoków. Jeśli tylko jeden widok jest podpięty pod przycisk, jego naciśnięcie wyświetli widok od razu.
2. Przyciski pozwalające przełączać widoki na następny, poprzedni lub wybrać z listy zdefiniowanych widoków.
3. Przycisk pozwalający dodać kolejny *Widok wideo*. Po jego naciśnięciu pojawia się okno z różnymi podziałami. Po wyborze podziału, zdefiniowaniu wyświetlanych kamer przez przeciągnięcie ikon ***strumieni*** (patrz poprzednia strona) można zapisać *Widok wideo* za pomocą ikony dyskietki, która pojawia się po wybraniu podziału. Należy wtedy podać nazwę dla zapisanego *Widoku wideo*.
4. Ikona ***joysticka*** - włącza/wyłącza możliwość sterowania kamerami PTZ. Po jej naciśnięciu i najechaniu kursorem na obraz z danej kamery wskaźnik strzałki zmienia się w strzałkę sterowania, pozwala ona sterować kamerą obrotową bezpośrednio na obrazie wideo. Zmiany krotności zoomu dokonuje się za pomocą rolki na myszce.
5. Ikona ***pełnego ekranu*** - po jej naciśnięciu *Panel* wyświetlany jest na pełnym ekranie. Widoczna jest jeszcze górna belka, którą można usunąć klikając prawym przyciskiem na dowolny obraz wideo i wybierając „Ukryj belkę menu”.
6. Ikony ***widoku na żywo i odtwarzania***. Podświetlone zamiennie informują jaki tryb jest aktualnie wyświetlany. W celu sterowania odtwarzanym materiałem konieczne jest narzędzie *Odtwarzacz*.
7. Kliknięcie prawym przyciskiem myszy na ikonę ***odtwarzania*** powoduje wyświetlanie listy dostępnych opóźnień względem obrazu na żywo. Po wyborze jednej z opcji system automatycznie przełączy się tryb w Playback z wybranym przesunięciem czasowym.
8. Klikając prawym przyciskiem na górną belkę pojawia się okienko, w którym można dodać/usunąć wybrane ikony ***górnej belki***.

9.5.2 Narzędzia do integracji VSS - Odtwarzacz

Narzędzie odtwarzacza jest niezbędne do przeglądania nagrań z rejestratorów VSS. W czasie oglądania obrazów na żywo jest puste i wyszarzone. W momencie przełączenia któregokolwiek widoku wideo w tryb odtwarzania wypełnia się listą kanałów danego okna i obrazuje na grafie ilość nagrań.

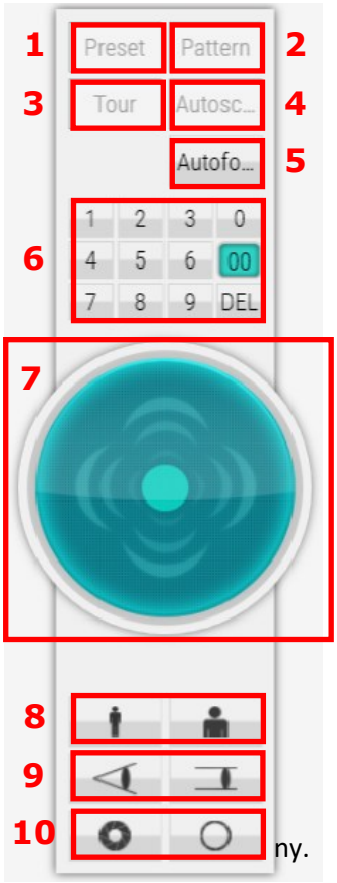


1. Data i czas aktualnie odtwarzanego materiału wideo. Po naciśnięciu przycisku kalendarza można zmienić datę i godzinę odtwarzanego materiału.
2. Przycisk przesuwania wstecz osi czasu panelu odtwarzania.
3. Przycisk przesuwania osi czasu panelu odtwarzania o całą dobę.
4. Przycisk przesunięcia odtwarzanych nagrań o jedną sekundę do tyłu.
5. Przycisk przesunięcia odtwarzanych nagrań o jedną klatkę do tyłu.
6. Przycisk odtwarzania do tyłu.
7. Przycisk pauzy, zatrzymania odtwarzania.
8. Przycisk normalnego odtwarzania.
9. Przycisk przesunięcia odtwarzanych nagrań o jedną klatkę do przodu.
10. Przycisk przesunięcia odtwarzanych nagrań o jedną sekundę do przodu.
11. Suwak prędkości odtwarzania. Umożliwia spowolnione lub przyspieszone odtwarzanie nagrań (od **x0,1** do **x10**).
12. Przycisk ***„x1”*** ustawiający domyślną prędkość odtwarzania (**x1**).
13. Przycisk przesuwania osi czasu panelu odtwarzania do przodu o całą dobę.
14. Przycisk przesuwania osi czasu panelu odtwarzania do przodu.
15. Oś czasu. Domyślnie pokazuje 24 godziny, można ją zoomować do 5 minut. Naciskając na oś lewym przyciskiem myszy można ją płynnie przesuwać.
16. Skala osi czasu, pozwala zrobić zoom na osi czasu (od 5 minut do 24 godzin).
17. Lista odtwarzanych kanałów. Na liście są wszystkie kamery, które w widokach wideo zostały przełączone w tryb odtwarzania.
18. Nagrania przedstawione w postaci grafu i różnych kolorów. Klikając w odpowiednie miejsce grafu można szybko zmienić godzinę odtwarzanego materiału.

9.5.3 Narzędzia do integracji VSS - Sterowanie PTZ

Sterowanie kamerami PTZ możliwe jest bezpośrednio na obrazie kamery po naciśnięciu ikony ***joysticka*** w górnej belce okna ***Wideo***. Do pełnej kontroli służy narzędzie *Sterowanie PTZ*.

Należy pamiętać, że aby narzędzie *PTZ* działało, ikona ***joysticka*** musi być aktywna oraz musi zostać wskazana kamera do obsługi.

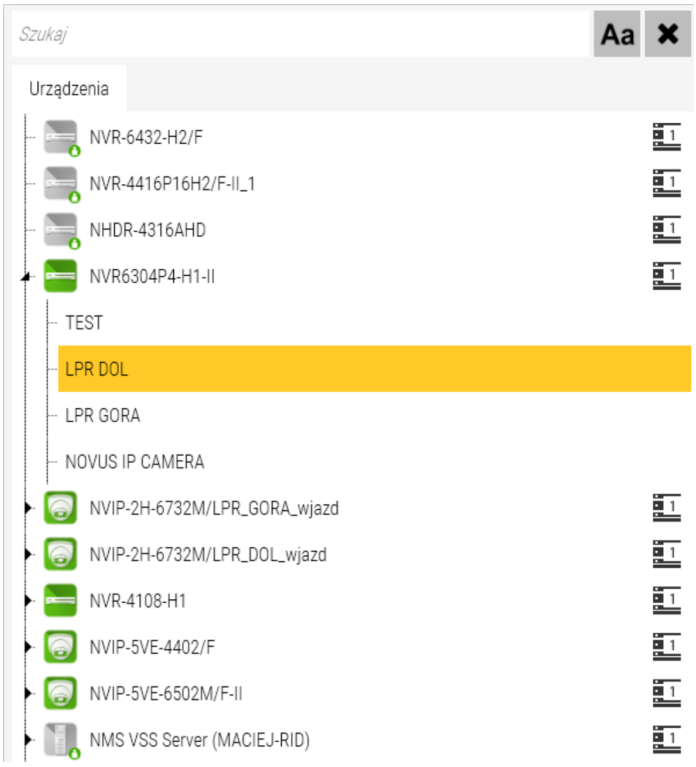


1. Przycisk ***Preset*** - służy do wywoływania presetu. Domyślnie jest wyszarzona, uaktywnia się po wybraniu numeru w niższej części narzędzia.
2. Przycisk ***Pattern*** - służy do wywoływania trasy obserwacji. Domyślnie jest wyszarzona, uaktywnia się po wybraniu numeru w niższej części narzędzia.
3. Przycisk ***Tour*** - służy do wywoływania patrolu. Domyślnie jest wyszarzona, uaktywnia się po wybraniu numeru w niższej części narzędzia.
4. Przycisk ***Autoscan*** - służy do wywoływania trasy automatycznego skanowania. Domyślnie jest wyszarzona, uaktywnia się po wybraniu numeru w niższej części narzędzia.
5. Przycisk ***Autofocus*** - powoduje automatyczne ustawienie ostrości.
6. Klawiatura numeryczna - pozwala wybrać numer wywoływanego presetu, trasy itd. Podświetlony element wskazuje wybraną liczbę.
7. Obszar sterowania PT - pozwala poruszać kamerami obrotowymi, używać różnych prędkości obrotu.
8. Przyciski zoom - pozwalają oddalić i przybliżyć obraz w kamerze z obiektywem motorzoom.
9. Przyciski ostrości - pozwalają ręcznie wyostrzyć obraz.
10. Przyciski przesłony - pozwalają ręcznie zmniejszyć lub zwiększyć otwarcie przesłony.

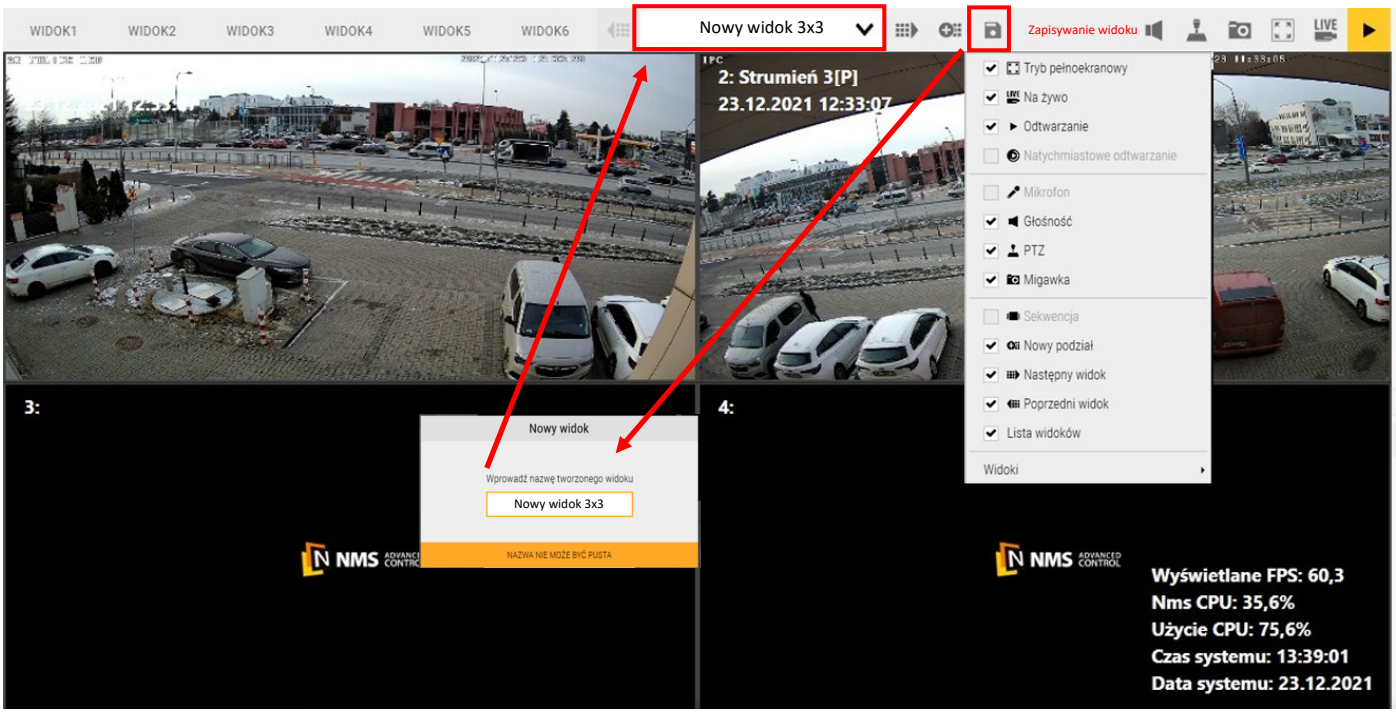
UWAGA! Dostępność poszczególnych funkcji zależy od funkcjonalności danego modelu kamery.

9.5.4 Narzędzia do integracji VSS - Drzewo urządzeń

Narzędzie *Drzewo urządzeń* pełni funkcję przeglądarki struktury systemu CCTV, prezentując w formie listy wszystkie urządzenia telewizji dozorowej dodane do systemu - zarówno pojedyncze kamery, jak i rejestratory z przypisanymi kanałami wideo.

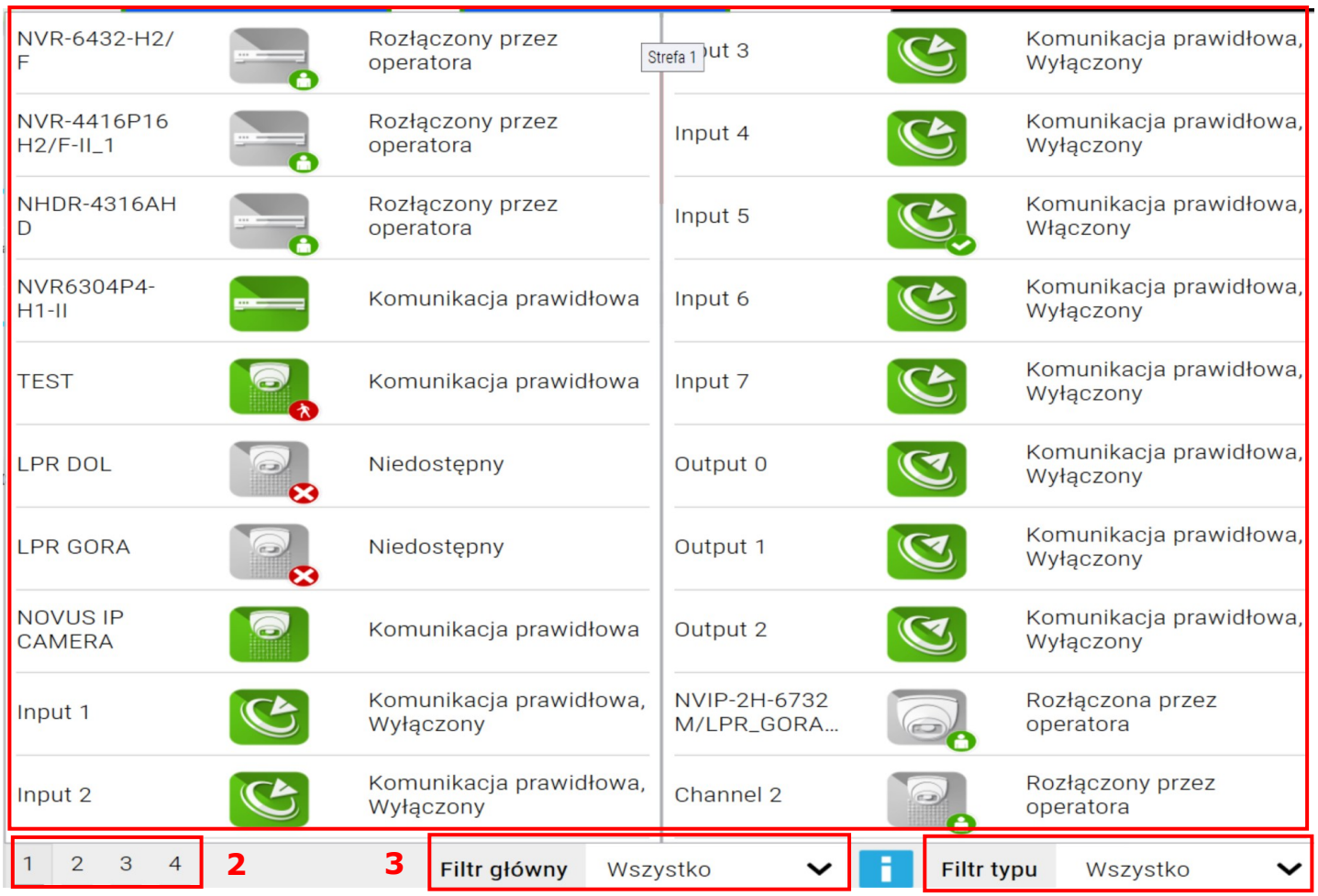


Aby utworzyć tymczasowy widok w narzędziu *Wideo* oraz opcjonalnie go zapisać, należy przeciągnąć urządzenie lub kanał z listy na wybrany widok w narzędziu *Wideo*, przytrzymując kursor na danym elemencie.



9.5.5 Narzędzia do integracji VSS - Tablica synoptyczna

Narzędzie *Tablica synoptyczna* to narzędzie służące do wyświetlenia urządzeń oraz monitorowania ich stanów. Użytkownik może w czasie rzeczywistym obserwować statusy urządzeń, takie jak np. *Komunikacja prawidłowa*, *Wykrycie zdarzenia*, *Niedostępny* czy *Rozłączenie przez operatora*.



1. **Okno urządzeń** - wyświetla wszystkie urządzenia, kanały, wejścia i wyjścia dostępne w systemie.
2. **Wybór strony** - umożliwia przełączanie między stronami z listą urządzeń i elementów systemu.
3. **Filtr główny** - opcja pozwalająca na wybór filtrów zdefiniowanych wcześniej w zakładce *Filtry elementów i zdarzeń*
4. **Filtr typu** - umożliwia zawężenie listy do wybranych kategorii, m.in.:
   - *Wszystko*
   - *Kontrolery*
   - *Kamery*
   - *Czytniki*
   - *Linie dozorowe*

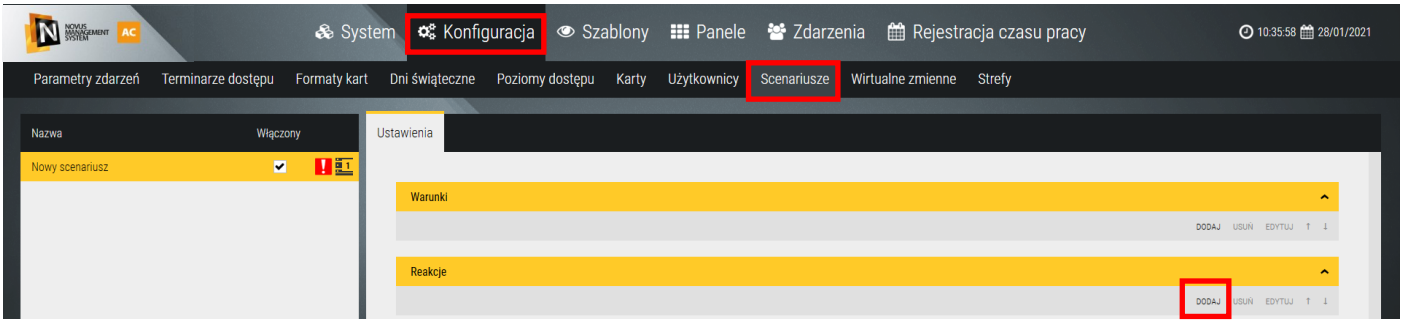
Aby zobaczyć obraz z danego urządzenia, należy przytrzymać kursor na ikonie ***kanału*** i przeciągnąć go na wybrany widok w narzędziu *Wideo*.

UWAGA! Funkcja działa tylko na ikonach ***kanałów***, nie na całych urządzeniach.

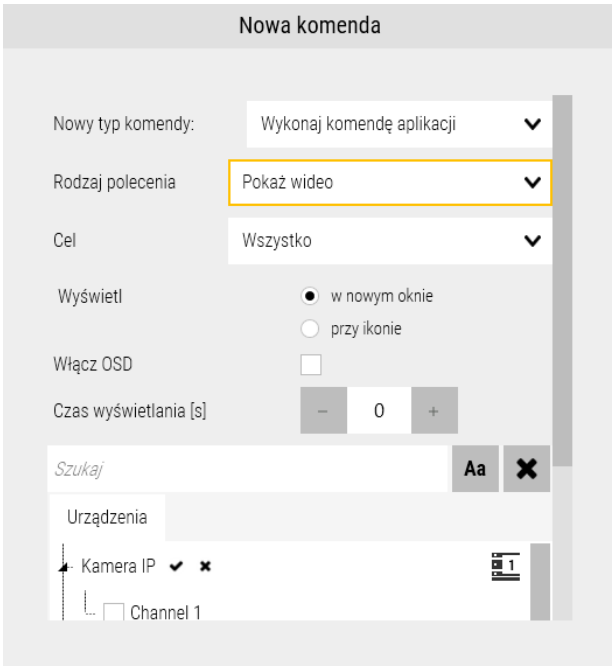
9.5.6 Wyświetlanie strumieni wideo w reakcji scenariusza

Integracja oprogramowania NOVUS MANAGEMENT SYSTEM AC z urządzeniami VSS dotyczy również wyświetlania strumieni wideo jako reakcję na dowolne zdarzenia dostępne w systemie. Ustawienia reakcji dokonuje się w menu *Konfiguracja*, zakładka *Scenariusze*.

Po stworzeniu nowego scenariusza oraz warunków jego uruchomienia należy w części *Reakcje* kliknąć przycisk ***Dodaj***. W pojawiającym się okienku ***Nowa komenda*** należy wybrać typ komendy ***Wykonaj komendę aplikacji***. Pojawią się dalsze opcje, jako rodzaj polecenia należy ustawić ***Pokaż wideo***.



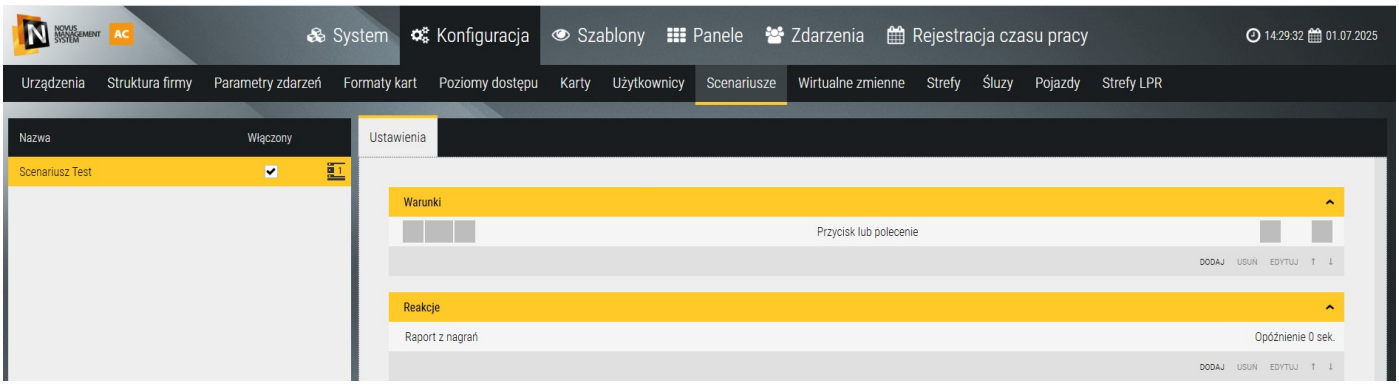
Pojawiają się dodatkowe opcje dotyczące wyświetlania:



- Cel - wyświetlanie wideo można ustawić dla konkretnego operatora lub grupy operatorów.
- Wyświetl - wyświetlanie można ustawić w nowym oknie lub w okienku podglądu przy ikonie ***strumienia wideo***. W pierwszym przypadku pojedyncza kamera będzie zajmowała całe okno. Zwiększając ilość strumieni nastąpi automatyczny podział na 4, 9 lub 16 strumieni. W przypadku ilości strumieni większej niż 16, strumienie wyświetlane najwcześniej znikają.
- Włącz OSD - wyświetlając wideo w nowym oknie można włączyć w nim OSD
- Czas wyświetlania - wartość domyślna *0* oznacza, że strumień po wywołaniu będzie się wyświetlał dopóki operator go nie wyłączy. Podając inną wartość sprawiamy, że w przypadku wyświetlania kolejnych strumieni, wskazane w tym scenariuszu strumienie znikną po danej ilości sekund.
- Urządzenia - lista dodanych urządzeń wideo, można wybrać dowolne strumienie z kamer i rejestratorów.
- Opóźnienie - czas opóźnienia reakcji.

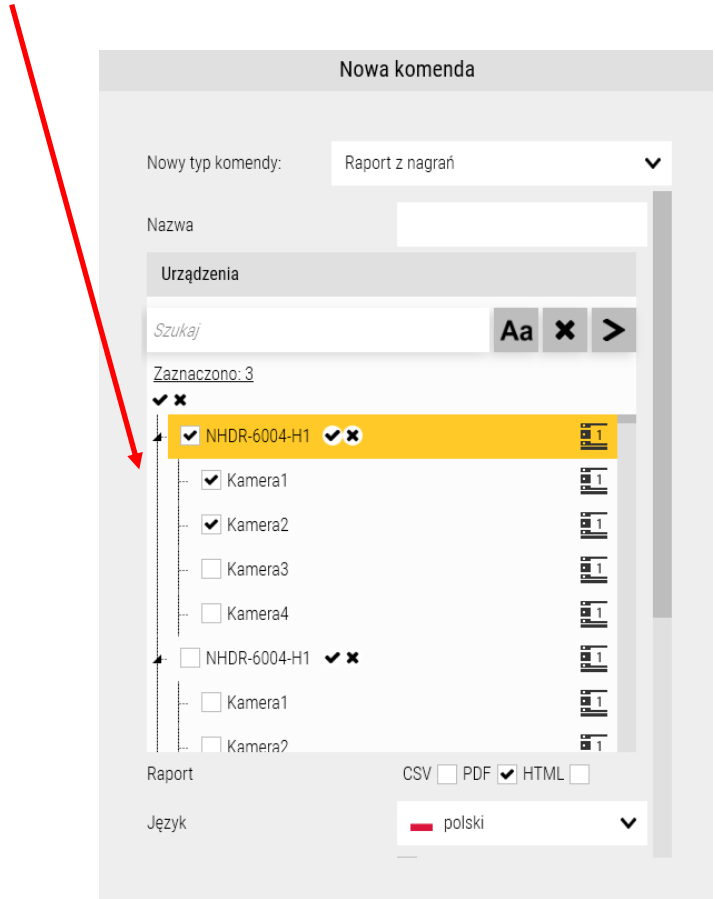
9.5.7 Generowanie raportów nagrań w reakcji scenariusza

Dodano funkcję umożliwiającą generowanie raportów poprzez zdefiniowanie scenariusza. Wygenerowany raport zawiera kluczowe informacje o stanie rejestratorów, takie jak: adres IP, adres MAC urządzenia, numer portu, stan dysku, stan komunikacji, całkowity czas nagrań, zakres czasowy nagrań, różnica czasu między rejestratorem a serwerem. Ponadto zawiera numer wersji oprogramowania lub programu, nazwę modelu urządzenia, informację o włączeniu mechanizmu DST czy protokołu NTP.

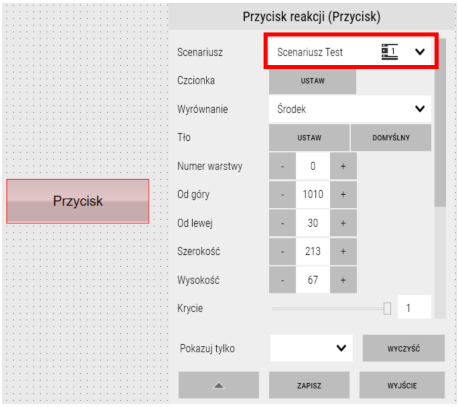


W celu wygenerowania raportu nagrań należy stworzyć nowy scenariusz w którym określane są warunki działania. W tym przypadku wybieramy polecenie typu ***Przycisk lub Polecenie***, które będzie inicjować generowanie raportu.

Następnie w zakładce *Reakcje* należy wybrać typ komendy **Raport z nagrań**. Komenda umożliwia wygenerowanie raportu nagrań z wybranych rejestratorów oraz wybranych kanałów.



W oknie edycji narzędzia ***Przycisk reakcji*** należy wybrać nowo utworzony scenariusz, który będzie uruchamiał generowanie raportu.



Po uruchomieniu scenariusza, raport jest zapisywany automatycznie przy użyciu przycisku dostępnego na panelu. Plik trafia do lokalizacji określonej wcześniej w konfiguracji systemu - w zakładce *System/Ogólne*, gdzie podaje się ścieżkę zapisu.

Poprawne zaimplementowanie procesu generowania raportu powoduje wygenerowanie wpisu w oknie logów, potwierdzającego wykonanie operacji. Dla kanałów, które nie były nagrywane, nagrania są niedostępne.

Data	Opis	Serwer	Urządzenie	Operator
08:55:27 , 02.07.2025	Scenariusz - wykonany Scenariusz Test		SYSTEM	Kuba

Tworzone raporty obejmują szczegółowe informacje dotyczące nagrań, w tym: nazwę urządzenia, nazwę kanału, adres IP, adres MAC, maskę podsieci, bramę domyślną, port, stan strumienia, stan dysku, całkowity czas nagrania, pola „Nagrania od” oraz „Nagrania do”, różnicę czasu na urządzeniu, ustawienia DST i NTP, a także model urządzenia i wersję firmware.
Dane sieciowe, takie jak adres IP, adres MAC, maska podsieci oraz brama domyślna, prezentowane są dla wszystkich interfejsów sieciowych danego urządzenia.

EXCEL:

Nazwa urządzenia	Nazwa kanału	IP	Port	Maska podsieci	Brama domyślna	MAC	Stan	Stan dysku	Całkowity czas nagrania	Nagrania od	Nagrania do	Różnica czasu na urządzeniu	DST	NTP	Model	Firmware
		LAN1: 192.168.60.10 LAN2: 10.11.70.1		LAN1: 255.255.0.0 LAN2:	LAN1: 192.168.1.254 LAN2:	LAN1: 00:1B:9D:12:89:81 LAN2: 00:1B:9D:										
NVR-6208P8-H1-II_pierwszy			6036	255.255.0.0		12:89:81	Komunikacja prawidłowa	OK				0d 00:03:35	Włączony	Wyłączony	NVR-6208P8-H1-II	1.4.13.85508B260127.N3V.U1(8B118)
NVR-6208P8-H1-II_pierwszy	Kamera 1 Główny						Komunikacja prawidłowa, Strumieniowanie	OK	20d 03:41:50	31.03.2026 04:28	20.04.2026 08:10					
NVR-6208P8-H1-II_pierwszy	Kamera 1 Do podziału						Komunikacja prawidłowa, Strumieniowanie	OK	20d 03:41:50	31.03.2026 04:28	20.04.2026 08:10					
NVR-6208P8-H1-II_pierwszy	Kamera 2 Główny						Komunikacja prawidłowa, Strumieniowanie	OK	20d 03:41:50	31.03.2026 04:28	20.04.2026 08:10					
NVR-6208P8-H1-II_pierwszy	Kamera 2 Do podziału						Komunikacja prawidłowa, Strumieniowanie	OK	20d 03:41:51	31.03.2026 04:28	20.04.2026 08:10					
NVR-6208P8-H1-II_pierwszy	Kamera 3 Główny						Komunikacja prawidłowa, Strumieniowanie	OK	20d 03:41:51	31.03.2026 04:28	20.04.2026 08:10					
NVR-6208P8-H1-II_pierwszy	Kamera 3 Do podziału						Komunikacja prawidłowa, Strumieniowanie	OK	20d 03:41:51	31.03.2026 04:28	20.04.2026 08:10					
NVR-6208P8-H1-II_pierwszy	Kamera 4 Główny						Komunikacja prawidłowa, Strumieniowanie	OK	20d 03:41:51	31.03.2026 04:28	20.04.2026 08:10					
NVR-6208P8-H1-II_pierwszy	Kamera 4 Do podziału						Komunikacja prawidłowa, Strumieniowanie	OK	20d 03:41:51	31.03.2026 04:28	20.04.2026 08:10					
NVR-6208P8-H1-II_pierwszy	Kamera 5 Główny						Komunikacja prawidłowa, Strumieniowanie	OK	20d 03:41:51	31.03.2026 04:28	20.04.2026 08:10					
NVR-6208P8-H1-II_pierwszy	Kamera 5 Do podziału						Komunikacja prawidłowa, Strumieniowanie	OK	20d 03:41:52	31.03.2026 04:28	20.04.2026 08:10					
NVR-6208P8-H1-II_pierwszy	Kamera 6 Główny						Komunikacja prawidłowa, Strumieniowanie	OK	20d 03:41:52	31.03.2026 04:28	20.04.2026 08:10					
NVR-6208P8-H1-II_pierwszy	Kamera 6 Do podziału						Komunikacja prawidłowa, Strumieniowanie	OK	20d 03:41:52	31.03.2026 04:28	20.04.2026 08:10					
NVR-6208P8-H1-II_pierwszy	Kamera 7 Główny						Komunikacja prawidłowa, Strumieniowanie	OK	20d 03:41:52	31.03.2026 04:28	20.04.2026 08:10					
NVR-6208P8-H1-II_pierwszy	Kamera 7 Do podziału						Komunikacja prawidłowa, Strumieniowanie	OK	20d 03:41:53	31.03.2026 04:28	20.04.2026 08:10					
NVR-6208P8-H1-II_pierwszy	Kamera 8 Główny						Komunikacja prawidłowa, Strumieniowanie	OK	20d 03:41:53	31.03.2026 04:28	20.04.2026 08:10					
NVR-6208P8-H1-II_pierwszy	Kamera 8 Do podziału						Komunikacja prawidłowa, Strumieniowanie	OK	20d 03:41:53	31.03.2026 04:28	20.04.2026 08:10					

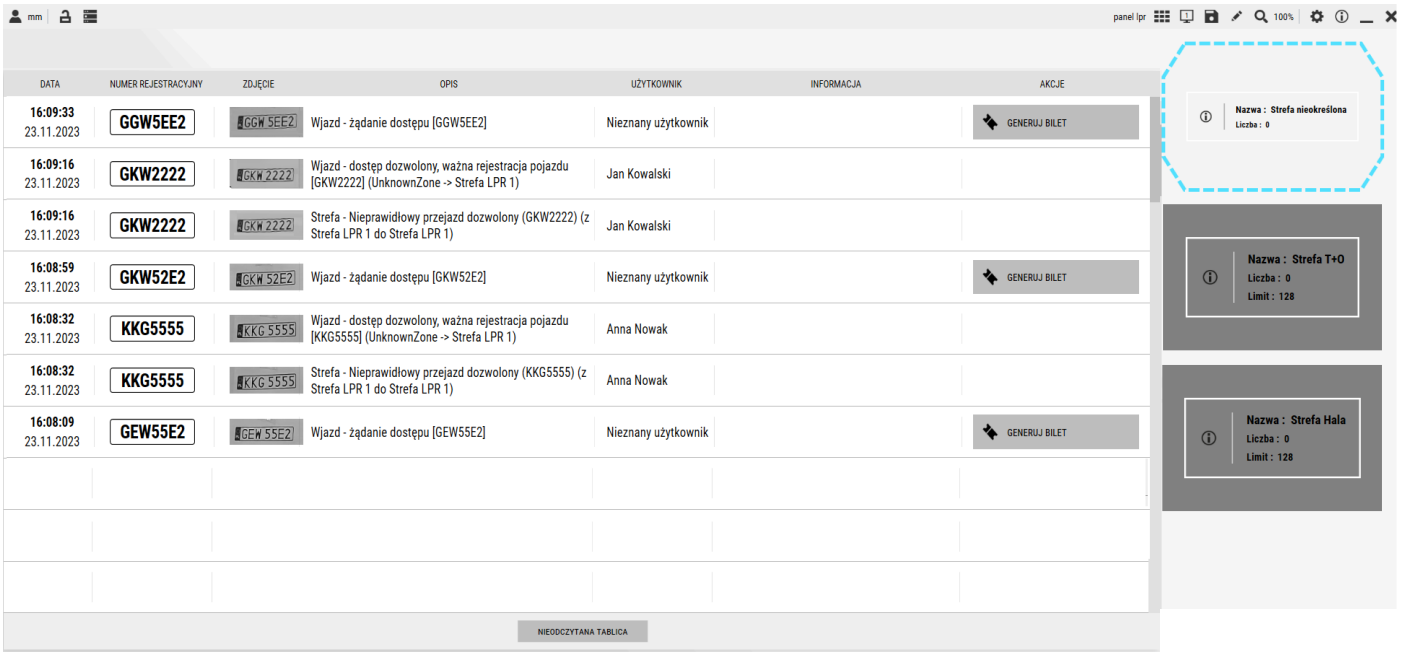
HTML:

Nazwa urządzenia	Nazwa kanału	IP	Port	Maska podsieci	Brama domyślna	MAC	Stan	Stan dysku	Całkowity czas nagrania	Nagrania od	Nagrania do	Różnica czasu na urządzeniu	DST	NTP	Model	Firmware
NVR-6208P8-H1-II		LAN1: 192.168.60.10 LAN2: 10.11.70.1	6036	LAN1: 255.255.0.0 LAN2: 255.255.0.0	LAN1: 192.168.1.254 LAN2:	LAN1: 00:1B:9D:12:89:81 LAN2: 00:1B:9D:12:89:81	Komunikacja prawidłowa	OK				0d 00:00:11	Włączony	Wyłączony	NVR-6208P8-H1-II	1.4.13.85508B260127.N3VU1(8B118)
NVR-6208P8-H1-II	Kamera 1 (Główny)						Komunikacja prawidłowa	OK	0d 00:15:44	27.04.2026 11:42:58	27.04.2026 11:58:42					
NVR-6208P8-H1-II	Kamera 1 (Do podziału)						Komunikacja prawidłowa	OK	0d 00:15:44	27.04.2026 11:42:58	27.04.2026 11:58:42					
NVR-6208P8-H1-II	Kamera 2 (Główny)						Komunikacja prawidłowa	OK	0d 00:15:44	27.04.2026 11:42:58	27.04.2026 11:58:42					
NVR-6208P8-H1-II	Kamera 2 (Do podziału)						Komunikacja prawidłowa	OK	0d 00:15:44	27.04.2026 11:42:58	27.04.2026 11:58:42					
NVR-6208P8-H1-II	Kamera 3 (Główny)						Komunikacja prawidłowa	OK	0d 00:15:44	27.04.2026 11:42:58	27.04.2026 11:58:42					
NVR-6208P8-H1-II	Kamera 3 (Do podziału)						Komunikacja prawidłowa	OK	0d 00:15:44	27.04.2026 11:42:58	27.04.2026 11:58:42					
NVR-6208P8-H1-II	Kamera 4 (Główny)						Komunikacja prawidłowa	OK	0d 00:15:44	27.04.2026 11:42:58	27.04.2026 11:58:42					
NVR-6208P8-H1-II	Kamera 4 (Do podziału)						Komunikacja prawidłowa	OK	0d 00:15:44	27.04.2026 11:42:58	27.04.2026 11:58:42					
NVR-6208P8-H1-II	Kamera 5 (Główny)						Komunikacja prawidłowa	OK	0d 00:15:44	27.04.2026 11:42:58	27.04.2026 11:58:42					
NVR-6208P8-H1-II	Kamera 5 (Do podziału)						Komunikacja prawidłowa	OK	0d 00:15:44	27.04.2026 11:42:58	27.04.2026 11:58:42					
NVR-6208P8-H1-II	Kamera 6 (Główny)						Komunikacja prawidłowa	OK	0d 00:15:44	27.04.2026 11:42:58	27.04.2026 11:58:42					
NVR-6208P8-H1-II	Kamera 6 (Do podziału)						Komunikacja prawidłowa	OK	0d 00:15:44	27.04.2026 11:42:58	27.04.2026 11:58:42					
NVR-6208P8-H1-II	Kamera 7 (Główny)						Komunikacja prawidłowa	OK	0d 00:15:44	27.04.2026 11:42:58	27.04.2026 11:58:42					
NVR-6208P8-H1-II	Kamera 7 (Do podziału)						Komunikacja prawidłowa	OK	0d 00:15:44	27.04.2026 11:42:58	27.04.2026 11:58:42					
NVR-6208P8-H1-II	Kamera 8 (Główny)						Komunikacja prawidłowa	OK	0d 00:15:44	27.04.2026 11:42:58	27.04.2026 11:58:42					
NVR-6208P8-H1-II	Kamera 8 (Do podziału)						Komunikacja prawidłowa	OK	0d 00:15:44	27.04.2026 11:42:58	27.04.2026 11:58:42					

9.6 Rozpoznawanie tablic rejestracyjnych LPR

Ogólny opis funkcjonalność systemu parkingowego realizowanego przy wykorzystaniu funkcji rozpoznawania numerów tablic rejestracyjnych LPR:

- współpraca z kamerami z funkcją LPR marki Novus połączonymi z NOVUS MANAGEMENT SYSTEM AC bezpośrednio lub za pośrednictwem oprogramowania NMS
- kontrola dostępu pojazdów do zdefiniowanych stref zgodnie z określonymi harmonogramami
- możliwość definiowania stref parkingowych oraz przypisywania im różnych poziomów dostępu
- definiowanie limitów ilości pojazdów przebywających w zdefiniowanych strefach
- wizualizacja pojazdów przebywających w zdefiniowanych strefach
- przypisywanie numerów tablic rejestracyjnych jako identyfikatory użytkowników
- definiowanie bazy numerów tablic rejestracyjnych pojazdów wraz z dodatkowymi informacjami o pojeździe, właścicielu pojazdu oraz dacie ważności
- zapis historii rozpoznanych numerów tablic rejestracyjnych wraz z możliwością późniejszego eksportu
- możliwość współpracy z drukarkami termotransferowymi w celu drukowania biletów zawierających takie informacje jak m.in. rozpoznany numer tablicy rejestracyjnej, dozwolony czas przebywania w strefie, data oraz godzina wydrukowania biletu i inne



9.6.1 LPR - rozpoznawanie tablic rejestracyjnych

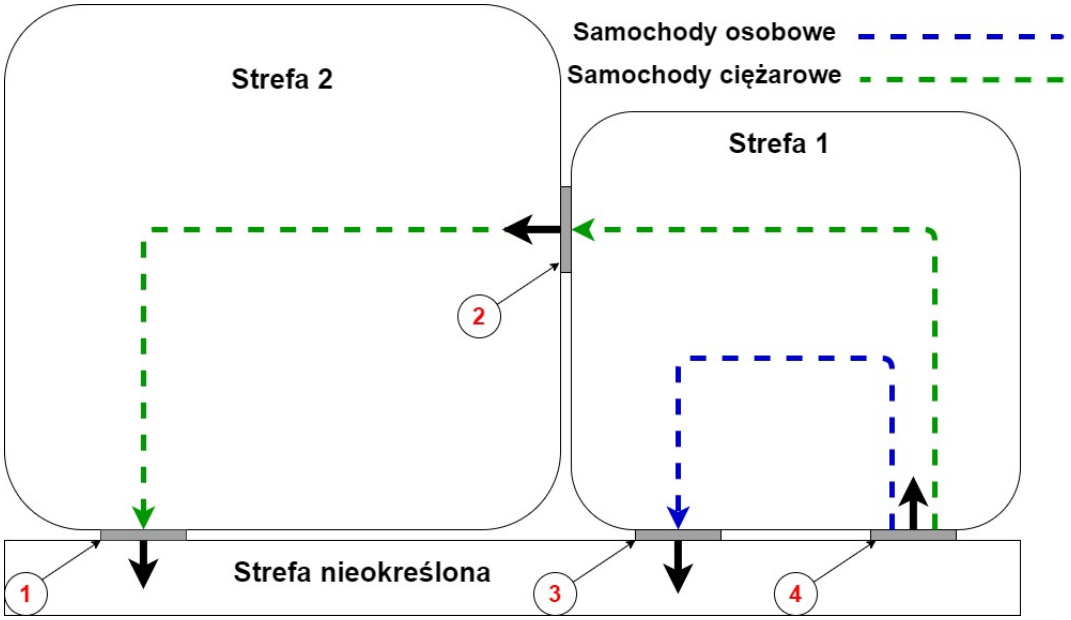
Oprogramowanie NOVUS MANAGEMENT SYSTEM AC zintegrowane z kamerami IP wyposażonymi w funkcje LPR pozwala na kontrolę dostępu pojazdów do zdefiniowanych wcześniej stref.

Przy założeniu, że:

Użytkownik chce mieć kontrole nad dwoma wydzielonymi strefami tak jak na rysunku poniżej.

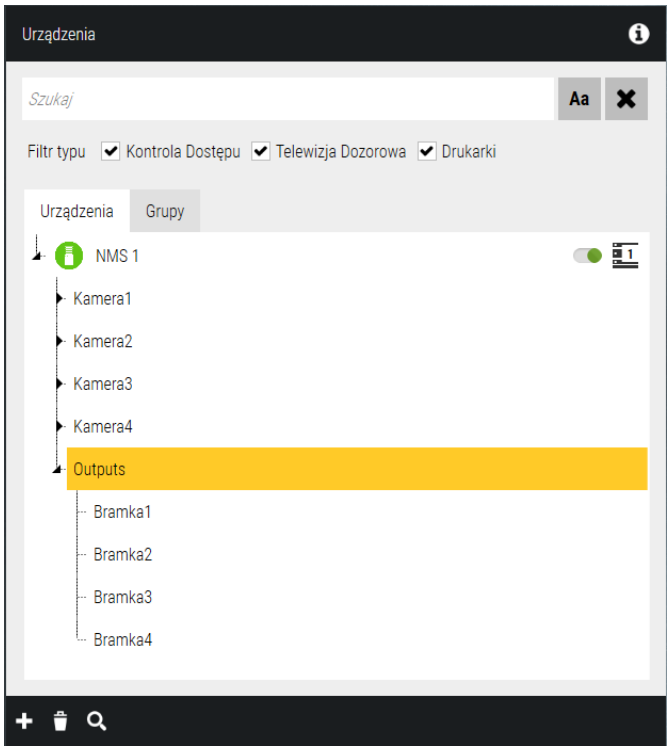
Do **Strefy 1** dostęp może mieć grupa: **„Samochody osobowe”** i grupa **„Samochody ciężarowe”**.

Do **Strefy 2** dostęp może mieć grupa **„Samochody ciężarowe”**.



Cyfry 1-4 oznaczają zarówno numery zamontowanych kamer jak i przekaźników sterujących urządzeniami takimi jak np. szlabany czy bramy.

Konfiguracja programu powinna przebiegać w następujący sposób:



9.6.2 Dodawanie urządzeń

W celu zapewnienia kontroli nad pojazdami wjeżdżającymi jak i wyjeżdżającymi z określonych stref, należy przy wjeździe/wyjeździe ze strefy zamontować kamery wyposażone w funkcje rozpoznawania tablic rejestracyjnych, a następnie dodać je do programu NOVUS MANAGEMENT SYSTEM AC.

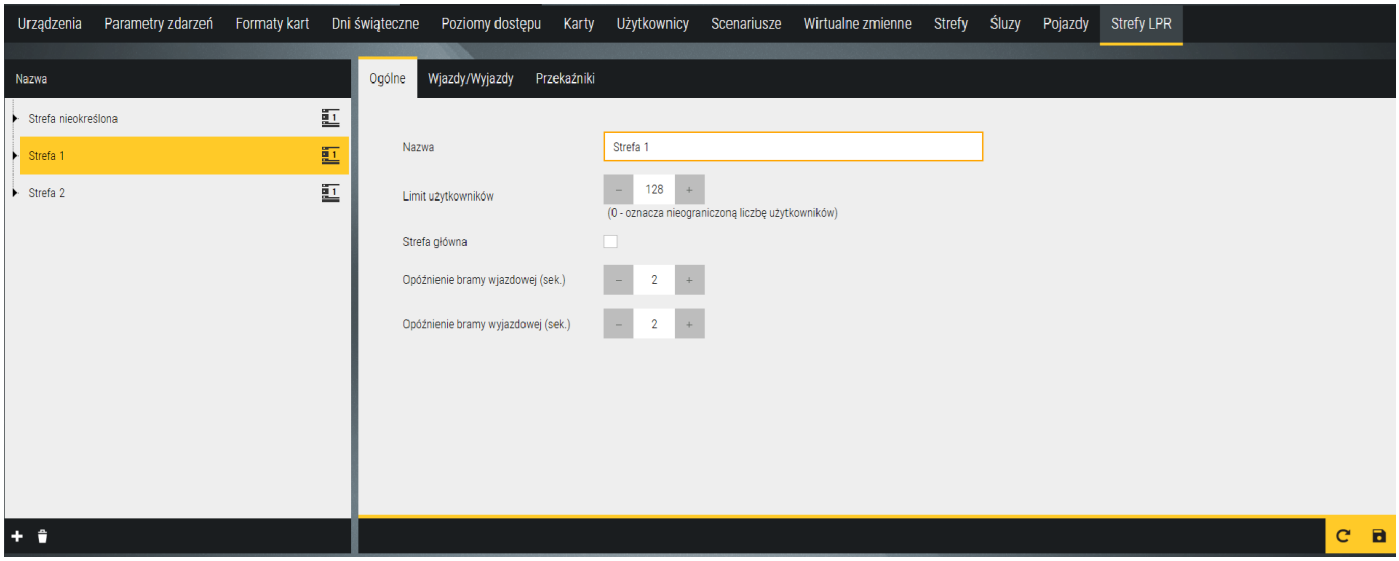
Proces dodawania urządzeń telewizji dozorowej został opisany w rozdziale **3.10 Telewizja dozorowa**. W powyższym przykładzie, dodane do systemu kamery, zostały nazwane zgodnie z rysunkiem obok.

UWAGA! Aby kamera LPR działała prawidłowo, w zakładce *Urządzenia/Szczegóły* wybranej kamery LPR należy w polu ***Metoda zdarzeń*** wybrać opcję *LongPolling*. Ustawienie to należy zastosować indywidualnie dla każdej kamery.

9.6.3 Strefy LPR

9.6.3.1 Konfiguracja stref

Po dodaniu urządzeń do NOVUS MANAGEMENT SYSTEM AC, należy utworzyć w programie wirtualne strefy. W tym celu należy przejść do zakładki *Konfiguracja/Strefy LPR* i klikając ikonę z symbolem ***plusa*** , dodać wymaganą ilość stref.



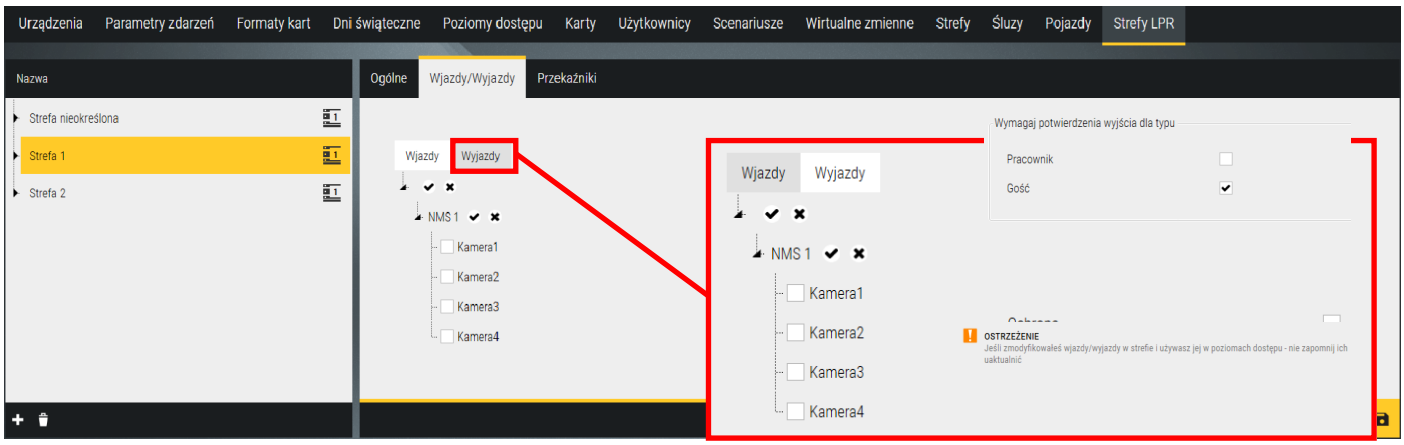
Po kliknięciu na wybraną strefę, w zakładce *Ogólne* znajdują się pola:

Nazwa - umożliwia nazwanie strefy

Limit użytkowników - określa maksymalną liczbę pojazdów mogących znajdować się w strefie w tym samym czasie

Strefa główna **-** po wyjechaniu ze strefy głównej do strefy nieokreślonej bilet traci ważność

Opóźnienie bramy wjazdowej/wyjazdowej - to czas opóźnienia zadziałania wyjścia przekaźnikowego sterującego bramą wjazdową/wyjazdową.

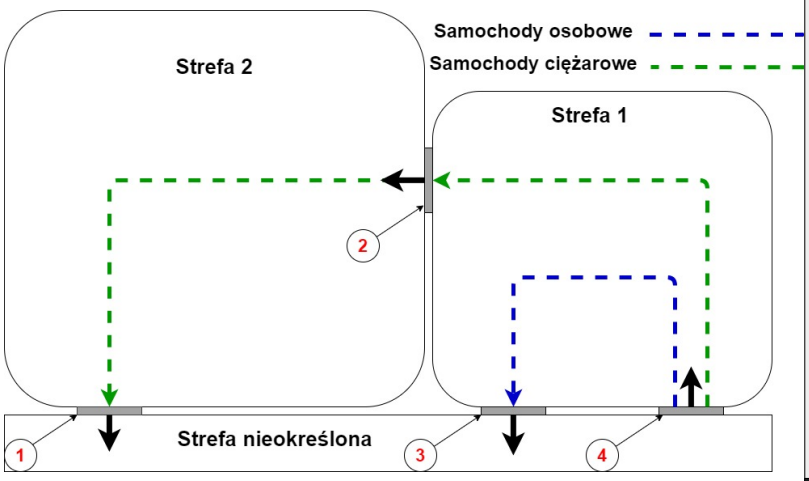


W zakładce *Wjazdy/Wyjazdy* można przyporządkować poszczególne kamery odpowiednio do wjazdów i wyjazdów z zaznaczonej żółtym kolorem strefy.

Przyciski ✔ ✖ służą do zaznaczania i odznaczania wielu kanałów jednocześnie.

Przycisk 🗑 służy do usuwania poszczególnych stref po ich zaznaczeniu.

Po kliknięciu *Wyjazdy***,** poza możliwością przypisania do wyjazdów odpowiednich kamer, można również zdefiniować dla której z 2 specjalnych grup (Pracownik, Gość) wyjazd do strefy nieokreślonej będzie wymagał potwierdzenia przez operatora (żądanie wyjazdu).



Wjazdy/Wyjazdy

Zgodnie z rysunkiem:

- Na wjeździe do **Strefy 1** jest kamera **4.**
- Na dwóch wyjazdach ze **Strefy 1** są kamery **2 i 3.**

W związku z tym wjazdy i wyjazdy dla **Strefy 1** powinny być ustawione tak jak na rysunku**(1).**

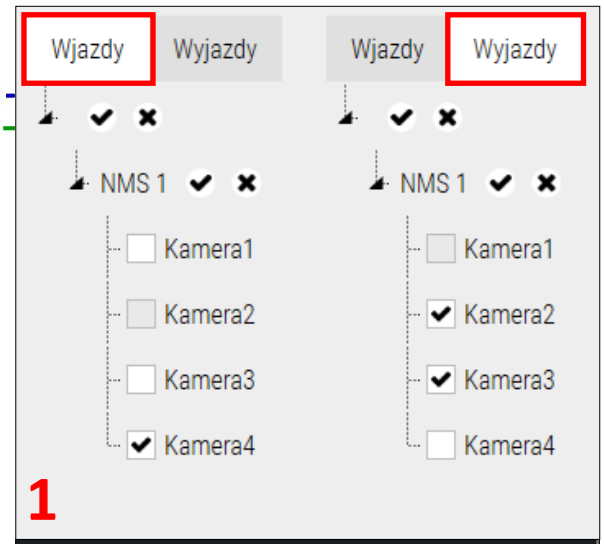
Wjazd do **Strefy 1:**

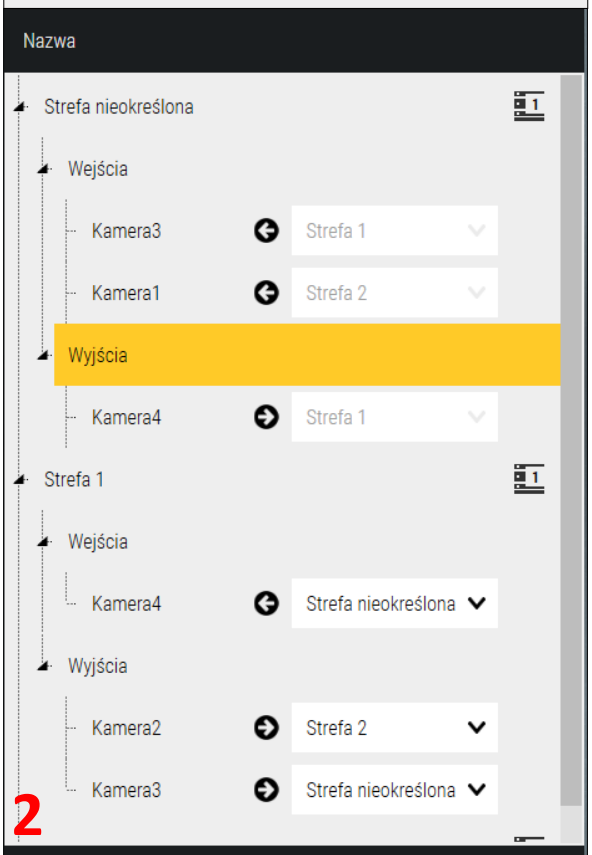
- Ze „Strefy nieokreślonej" monitoruje **kamera 4**

Wyjazd ze **Strefy 1:**

- Do „Strefy nieokreślonej" monitoruje **kamera 3**
- Do „Strefy 2" monitoruje **kamera 2**

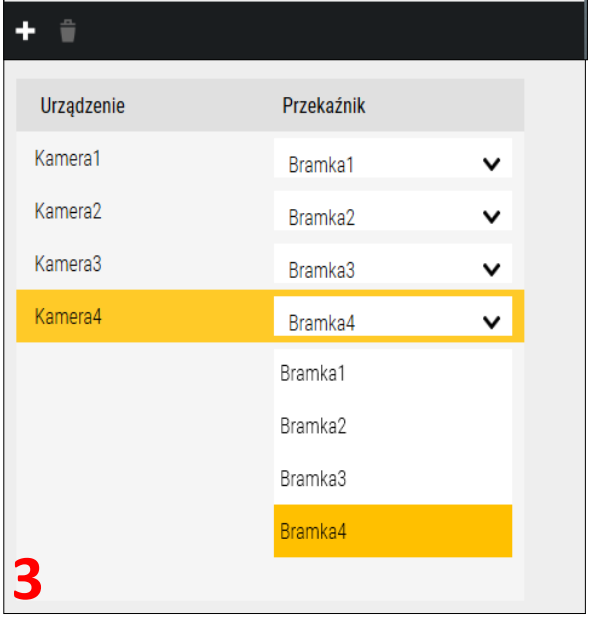
A zatem menu rozwijane po lewej stronie panelu powinno być skonfigurowane tak jak na rysunku **(2).**





Przekaźniki

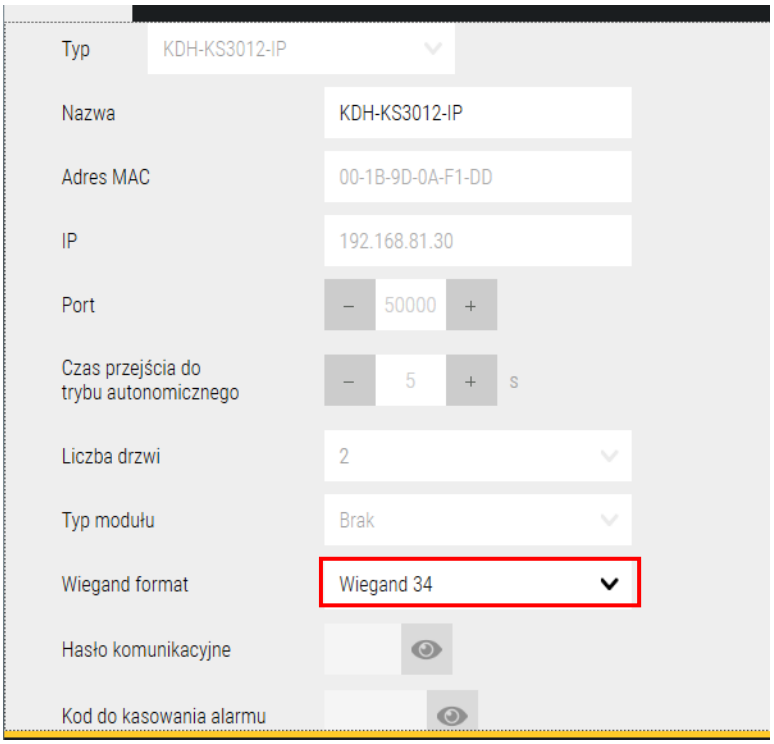
Etap konfiguracji Stref LPR można zakończyć przypisaniem przekaźników do odpowiednich urządzeń. Nazwy urządzeń i przekaźników, zostały uprzednio zdefiniowane podczas dodawania urządzeń w punkcie **9.5.1.** Ze względu na to, że w przyjętym projekcie, każda kamera ma sterować bramką przy której jest umieszczona, przekaźniki powinny być skonfigurowane w taki sposób jak na rysunku **(3).** Dodatkowo w tej sekcji do kamer mogą zostać przypisane wejścia sterujące oraz drukarki kodów QR w przypadku, gdy zezwolenie na wjazd ma być udzielane automatycznie np. po naciśnięciu przycisku i uzyskaniu biletu z kodem QR.

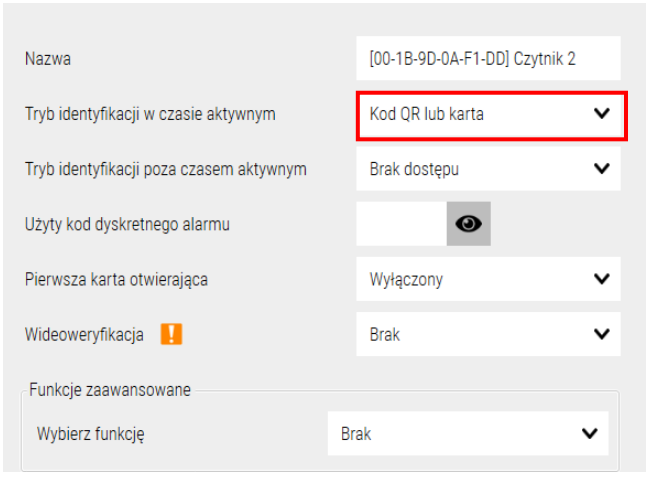


9.6.3.2 Obsługa wyjazdu gościa z użyciem kontrolera z czytnikiem, drukarki QR i kamery LPR

W celu wyjazdu ze strefy LPR gość musi zeskanować wydany bilet przy czytniku, co powoduje automatyczne otwarcie szlabanu i zapis zdarzenia w systemie. Kamera LPR rejestruje numer tablicy rejestracyjnej, który zostaje powiązany z wydanym biletem, co umożliwia późniejszą weryfikację i kontrolę wyjazdu.

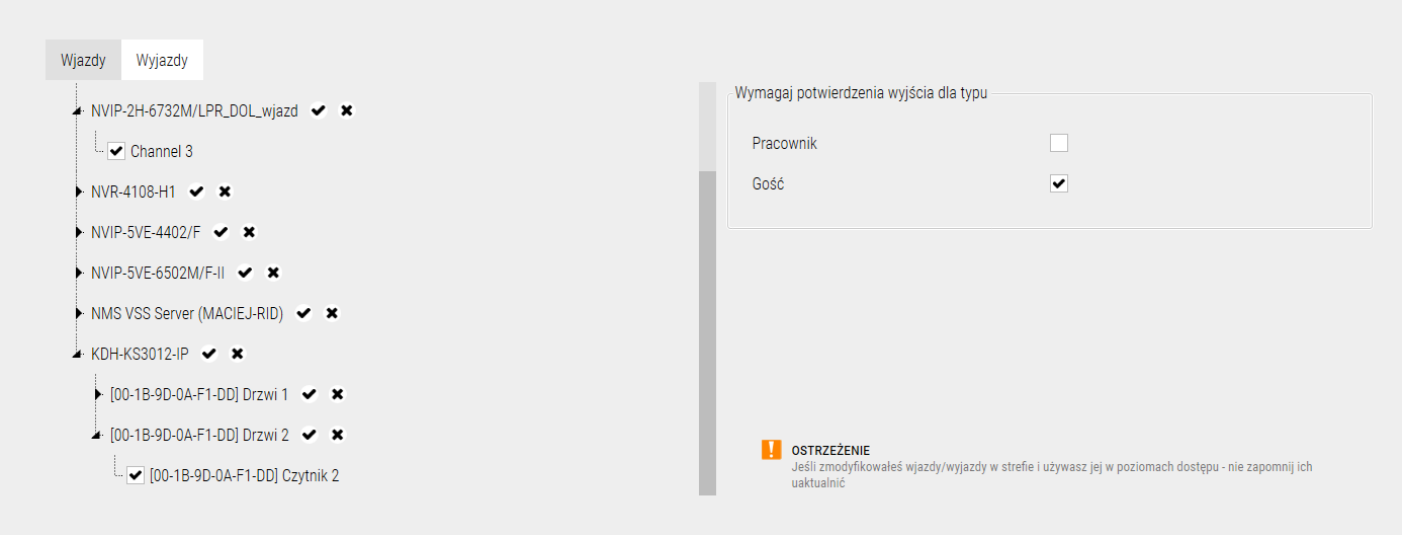
Przykładem konfiguracji czytnika wybranego urządzenia *Kontroli Dostępu*, tutaj dla KDH **Seria 3000** jest ta przedstawiona na poniższych zdjęciach:



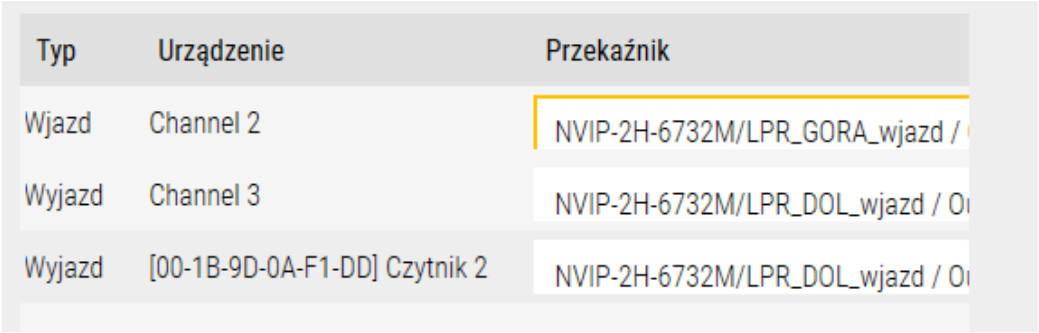


UWAGA! Aby czytnik mógł prawidłowo odczytywać kody QR z biletów, należy w konfiguracji urządzenia *Kontroli Dostępu* ustawić *format Wiegand* na **Wiegand 34**, a w zakładce *Szczegóły* wybranego *Czytnika*, w polu ***Tryb identyfikacji w czasie aktywnym***, wybrać opcję *Kod QR lub karta*.

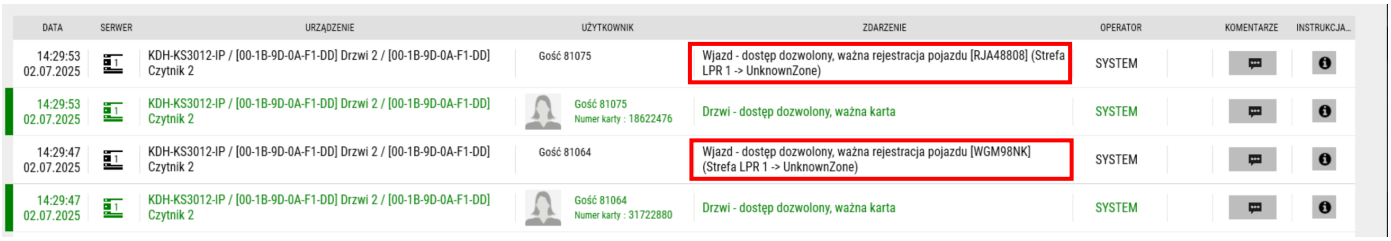
Ponadto należy wybrać w zakładce *Strefy LPR* kolejne urządzenie jako wyjazd - oprócz wybranej kamery LPR również dodać *Czytnik*, wraz z zaznaczeniem opcji wymogu potwierdzenia wyjścia dla typu *Gość*.



Natomiast w zakładce *Przekaźniki* należy przypisać nowo utworzone wyjścia do wcześniej skonfigurowanego wyjścia, odpowiedzialnego np. za podnoszenie szlabanu podczas wyjazdu ze strefy - analogicznie jak w przypadku kamery LPR przypisanej do wyjazdu.



W rezultacie, po przyłożeniu biletu QR do czytnika, w logach powinny pojawić się wpisy potwierdzające prawidłowy wyjazd ze strefy LPR z ważnym biletem.

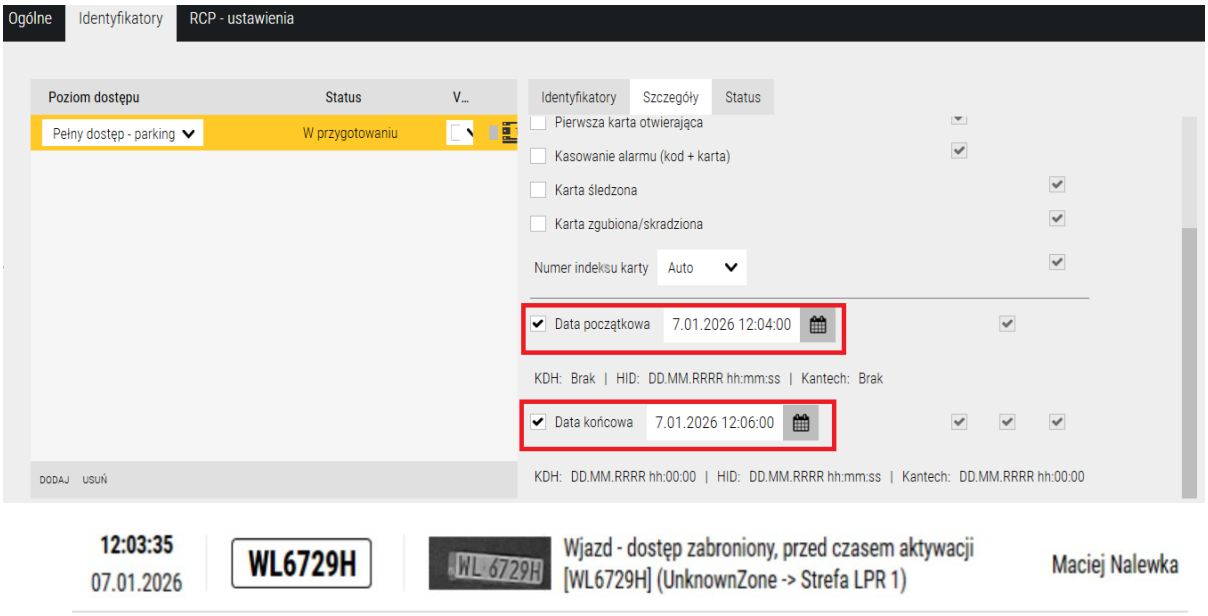


9.6.3.3 Awizacja gościa w strefie LPR

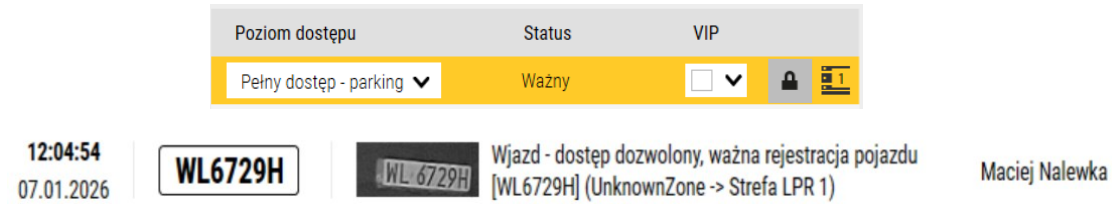
Ta funkcja polega na przypisaniu do danego gościa daty początkowej oraz daty końcowej określającej czas jego aktywności w strefie. W tym czasie gość nie musi generować biletu z kodem QR - wystarczy standardowy wjazd do strefy LPR poprzez zeskanowanie tablicy rejestracyjnej pojazdu.

W tym celu należy przejść do zakładki *Konfiguracja/Użytkownicy*, następnie wybrać konkretnego użytkownika i przejść do zakładki *Identyfikatory/Szczegóły,* gdzie należy zaznaczyć datę początkową oraz końcową okresu awizacji.

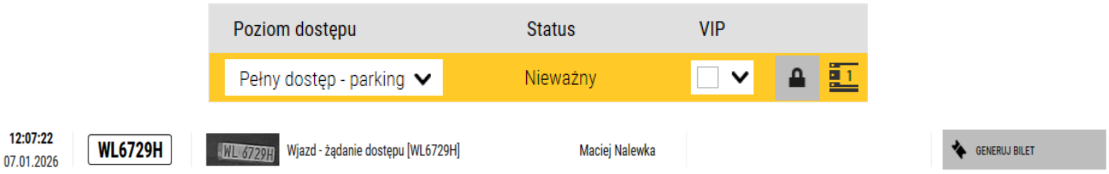
Wjazd gościa do strefy LPR przed rozpoczęciem okresu awizacji, status **W przygotowaniu**.



Wjazd podczas okresu awizacji do strefy LPR, status **Ważny**.

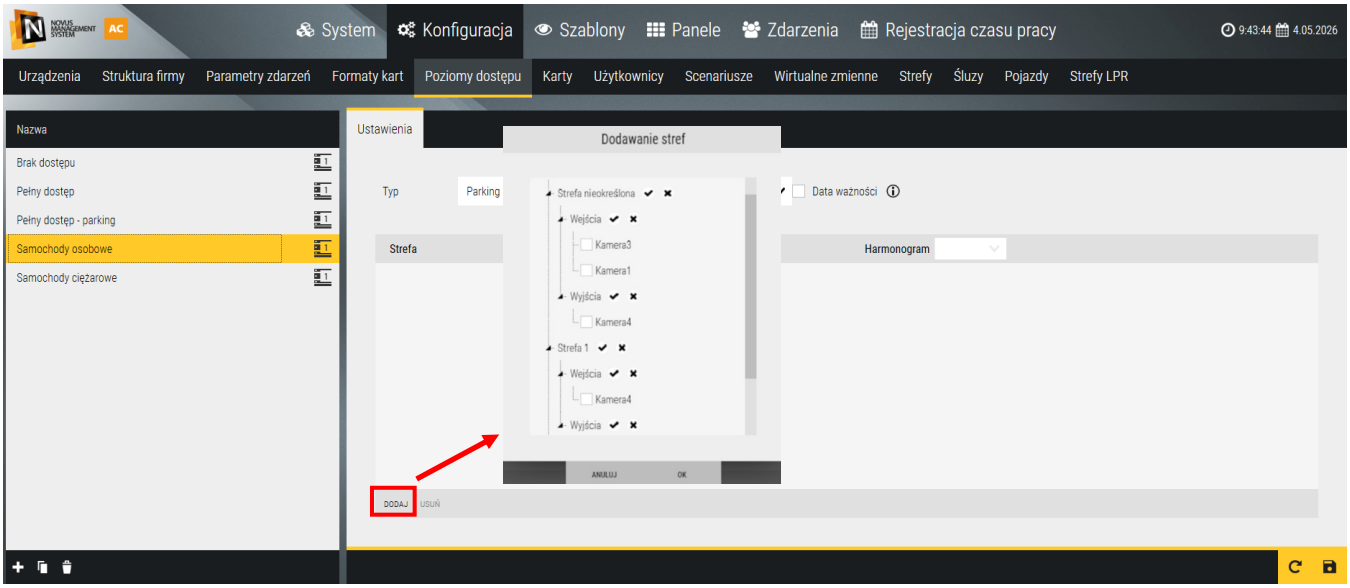


Po upłynięciu terminu ważności awizacji -> zmiana statusu na **Nieważny**, przy kolejnym wjeździe do strefy konieczne będzie ponowne wygenerowanie biletu.



9.6.4 Poziomy dostępu - parking

Menu poziomy dostępu zostało opisane w rozdziale **4.2 Poziomy dostępu**, na przykładzie definiowania dostępu do drzwi i wind. W przypadku LPR zamiast drzwi i wind, użytkownik ma do czynienia ze strefami, do których dostęp jest kontrolowany m.in. przez kamery LPR.

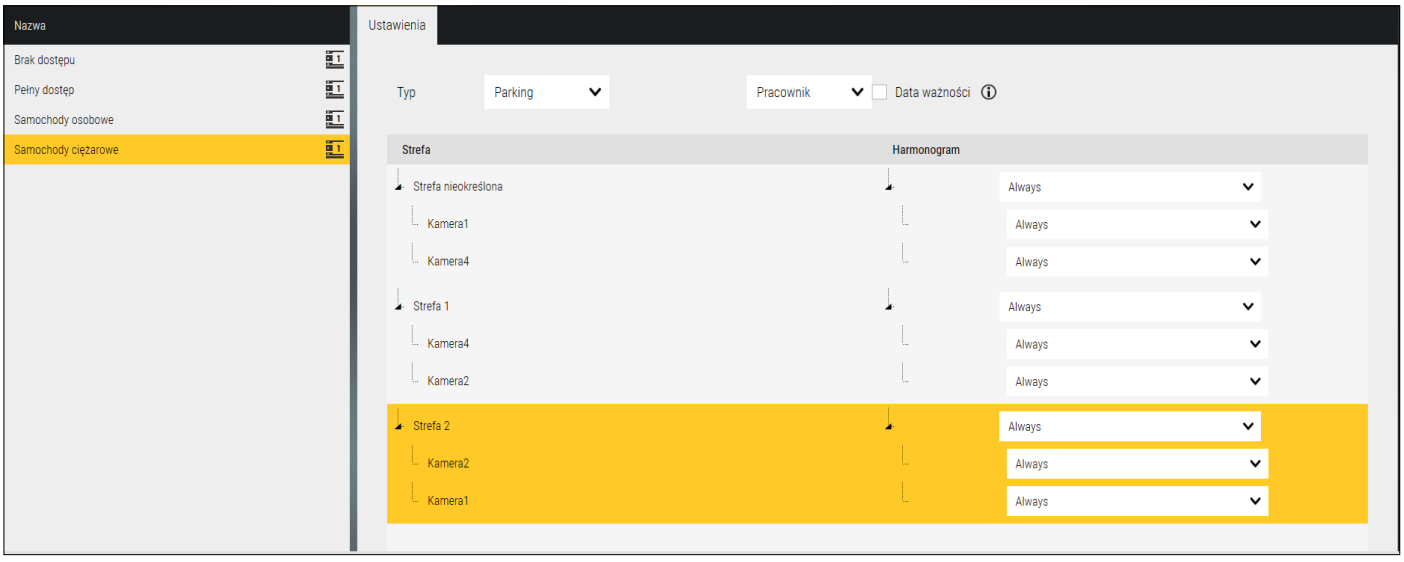


W przykładowym projekcie należy stworzyć dwa poziomy dostępu:

Samochody osobowe - które będą miały dostęp do **Strefy 1** i będą miały możliwość przejazdu przez bramki **3** i **4.**

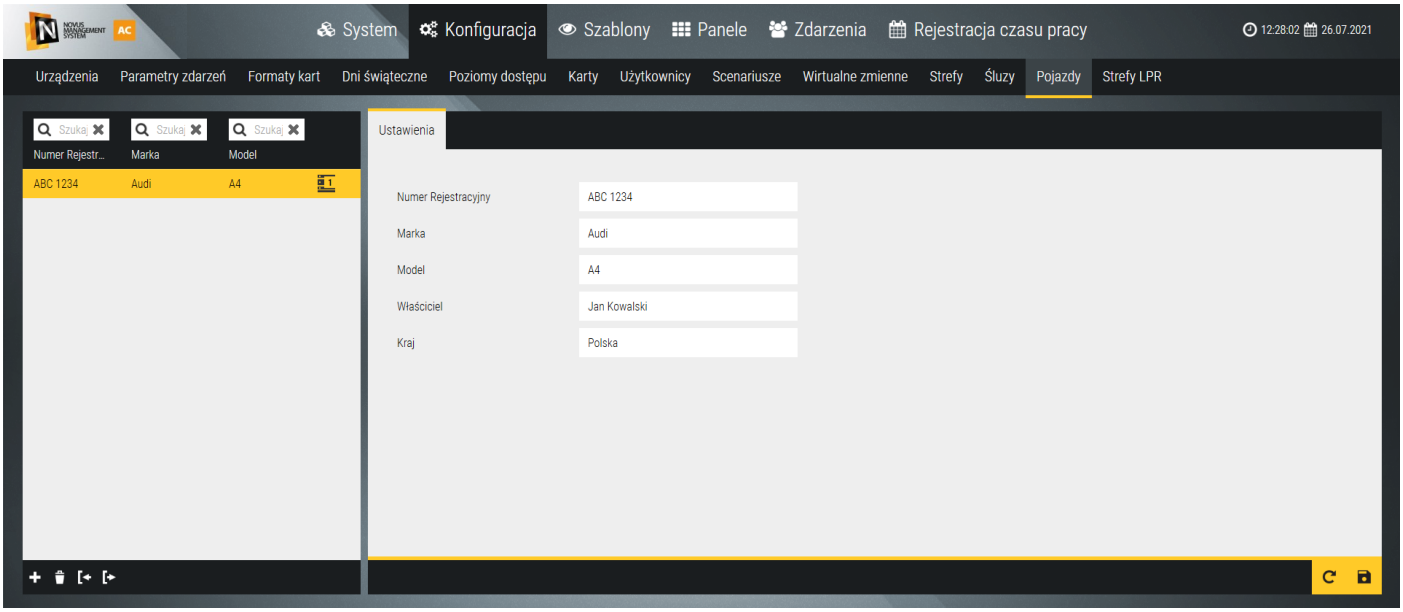
Samochody ciężarowe - które będą miały dostęp do **Strefy 1** i **Strefy 2** i będą miały możliwość przejazdu przez bramki **1,2,4.**

Aby to zrobić należy kliknąć ikonę  i dodać dwa powyższe poziomy dostępu. Aby zmienić nazwę nowo utworzonych poziomów dostępu należy na nią podwójnie kliknąć. Po nazwaniu i kliknięciu na nowo utworzony poziom, podświetli się on na żółto, w karcie **Ustawienia** należy zmienić typ na **Parking**. Następnie klikając przycisk ***Dodaj***, dla każdego z poziomów z osobna będzie można zdefiniować dostęp do poszczególnych wjazdów i wyjazdów. Zgodnie z założeniami projektu ze strony 85, dostęp do stref przez samochody ciężarowe powinien być skonfigurowany tak jak na rysunku poniżej. Na końcu, w kolumnie harmonogram należy zmienić **Never** na **Always** dla każdej ze stref.



9.6.5 Pojazdy

Zakładka *Pojazdy* służy do tworzenia bazy pojazdów. Przechowywane są tam informacje takie jak: numer rejestracyjny, marka, model, właściciel i kraj. Program umożliwia również zdefiniowanie czasu po którym pojazd będzie usunięty z bazy. Aby dodać pojazd do bazy należy kliknąć ikonę , następnie w celu uzupełnienia informacji o pojeździe należy kliknąć na nowo utworzone pole i w zakładce *Ustawienia* uzupełnić odpowiednie informacje.

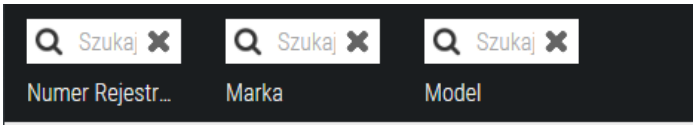


Przyciski:

- służy do importowania bazy pojazdów w formacie .csv,

- służy do eksportowania bazy pojazdów w formacie .csv,

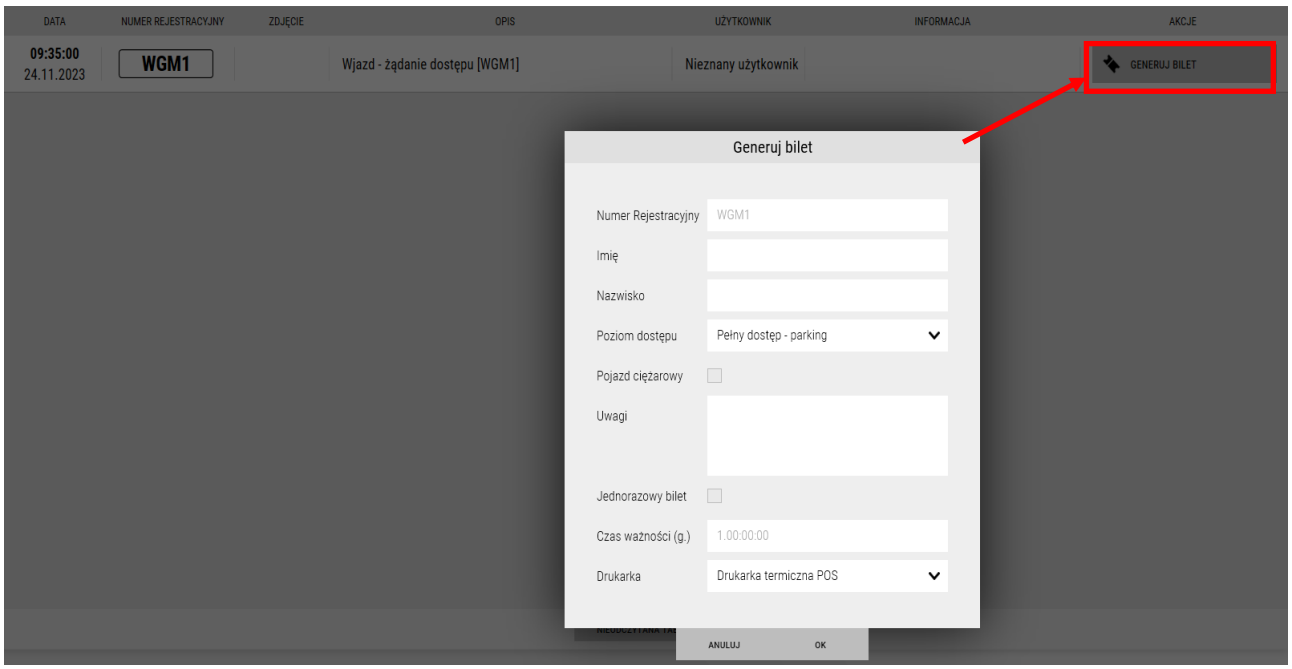
Nad listą dodanych tablic rejestracyjnych znajduje się wyszukiwarka, umożliwiająca zawężanie listy tablic rejestracyjnych według numeru rejestracyjnego, marki oraz modelu samochodu.



9.6.6 Narzędzia w panelu LPR

Aby mieć wgląd w pracę systemu rozpoznawania numerów tablic rejestracyjnych pojazdów, oprogramowanie NOVUS MANAGEMENT SYSTEM AC umożliwia tworzenie paneli dopasowanych do potrzeb użytkownika. Proces dodawania paneli wraz z ich konfiguracją został szerzej opisany w rozdziale **6. Panele.** W celu prawidłowej obsługi systemu kontroli dostępu pojazdów, najlepiej jest używać co najmniej dwóch narzędzi.

Najważniejszym narzędziem jest okno ***Zdarzenia LPR***. Służy do wyświetlania zdarzeń związanych z rozpoznawaniem numerów tablic rejestracyjnych oraz do manualnego zarządzania wjazdami i wyjazdami samochodów z poszczególnych stref. Po wykryciu tablicy rejestracyjnej system wyświetla w oknie czas zdarzenia, zdjęcie tablicy, numer rejestracyjny i opis zdarzenia. Opis może zawierać między innym: informacje na temat przemieszania się pojazdów między strefami; informacje na temat udzielenia, bądź nie udzielenia pojazdom dostępu do stref; informacje na temat ważności biletów; żądania dostępu.



Szczególnym zdarzeniem jest **żądanie dostępu**, które wyświetla się gdy nieznany pojazd chce wjechać ze strefy nieokreślonej do stref objętych kontrolą dostępu. Osoba nadzorująca działanie systemu może kliknąć przycisk ***Generuj Bilet***, wyświetli się wtedy okno w którym należy podać informacje związane z wjeżdżającym pojazdem. Osoba generująca bilet może przydzielić pojazdowi odpowiedni poziom dostępu i zdefiniować czas ważności biletu. Na wypadek gdyby wydruk biletu się nie powiódł, po wygenerowaniu biletu pojawia się przycisk ***Ponów wydruk***.

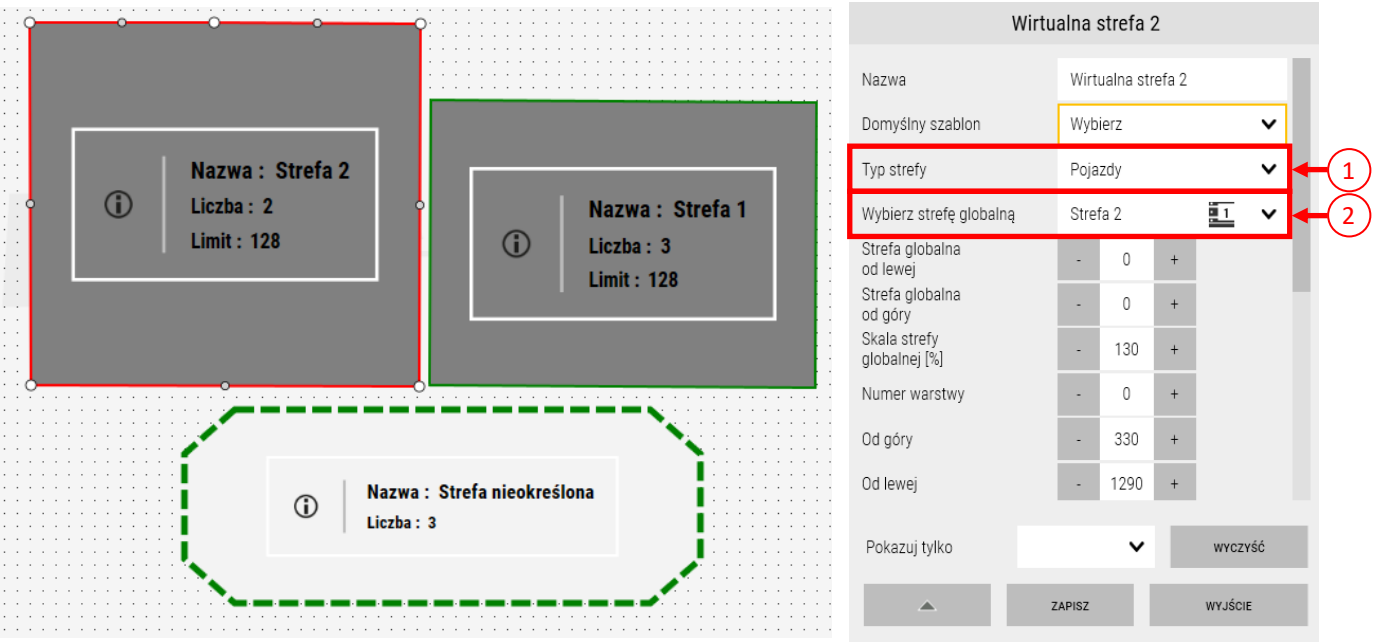
Aby wydrukować bilet, do systemu powinna zostać uprzednio dodana przeznaczona do tego drukarka. Można to zrobić w zakładce *Konfiguracja/ Urządzenia*. Więcej informacji na temat dodawania urządzeń do NOVUS MANAGEMENT SYSTEM AC znajduje się w rozdziale **3.Konfiguracja systemu.**

Przykładowy bilet dla pojazdu z rejestracją „ABC 1234” jest pokazany na rysunku obok. Bilet poza informacjami uzupełnionymi przy jego generowaniu posiada unikalny kod QR (możliwość wykorzystania funkcjonalności kodu QR będzie dostępna w przyszłości).

Wirtualna strefa

Kolejnym narzędziem wykorzystywanym w panelu LPR jest **wirtualna strefa**.

Proces dodawania stref do panelu został już opisany w niniejszej instrukcji w rozdziale **9.2 Strefy globalne**.



Specjalnym rodzajem jest **Strefa nieokreślona**, reprezentuje ona obszar poza strefami objętymi kontrolą dostępu (np. ulica z której wjeżdża się do obiektu objętego systemem kontroli dostępu). Do pozostałych stref dodanych do panelu można przypisać wcześniej utworzone (roz. 9.5.2) Strefy LPR. Aby to zrobić należy w trybie edycji kliknąć lewym przyciskiem myszy na nowo utworzoną strefę i w oknie edycji wybrać **Typ strefy (1) : Pojazdy** oraz w polu **Wybierz strefę globalną (2)** wybrać strefę LPR lub strefę nieokreśloną. Pozostałe ustawienia dotyczą wyglądu i położenia strefy w panelu.

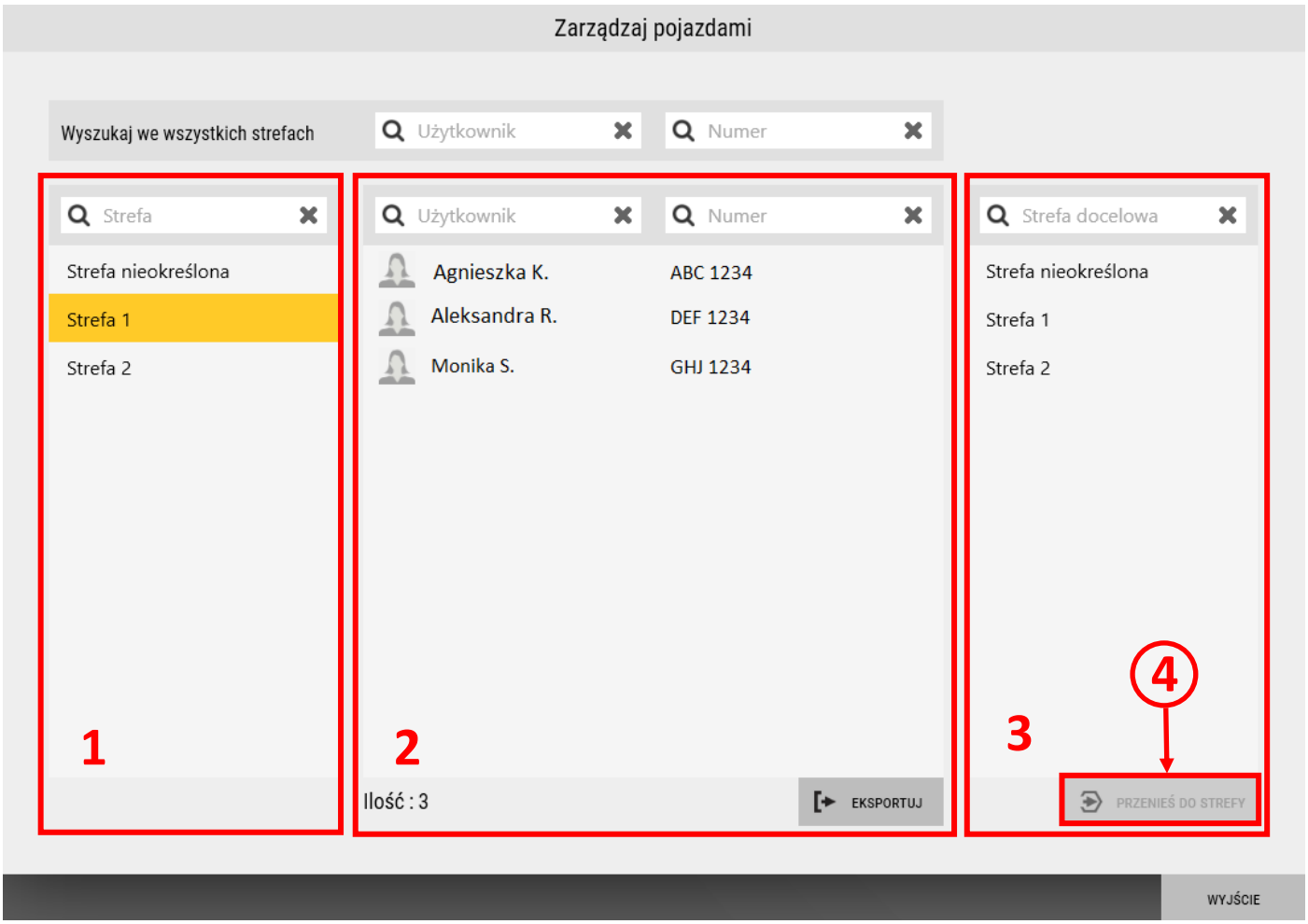
Po skonfigurowaniu nowo utworzonej strefy, w jej obrębie wyświetlą się informacje takie jak:

- nazwa,
- liczba pojazdów znajdujących się aktualnie w strefie
- limit osób mogących jednocześnie znajdować się w strefie.

Po kliknięciu prawym przyciskiem myszy na wirtualną strefę, obok wyświetli się lista z numerami rejestracyjnymi pojazdów znajdujących się w strefie i nazwy ich użytkowników.

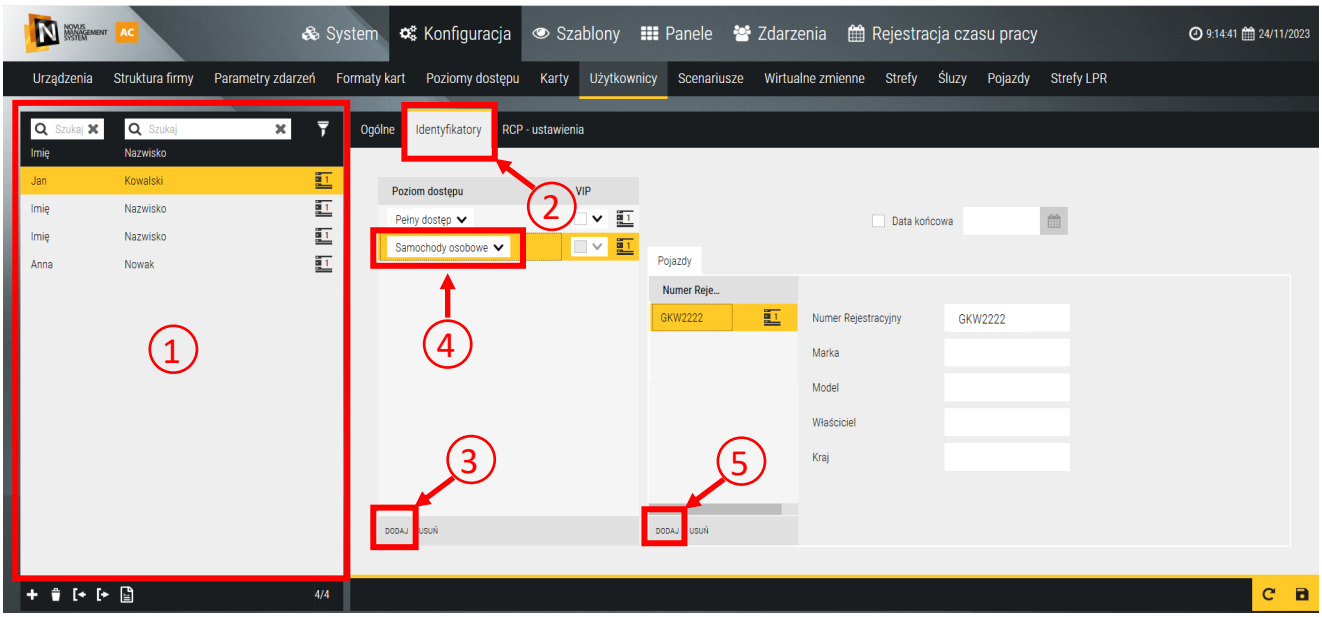
Zarządzanie pojazdami znajdującymi się w strefach

Po kliknięciu lewym przyciskiem myszy na dowolną strefę, użytkownik ma możliwość przejścia do okna zarządzania pojazdami. Pole **(1)** służy do zaznaczania strefy z której podgląd wyświetla się w środkowym polu **(2).** Pole **(2)** służy do podglądu, którzy użytkownicy znajdują się aktualnie w danej strefie. Na wypadek niezgodności informacji na temat pojazdów znajdujących się w strefie ze stanem faktycznym, użytkownik ma możliwość przeniesienia pojazdów z owej strefy do strefy docelowej **(3).** Aby to zrobić należy zaznaczyć wybranego użytkownika oraz strefę docelową i kliknąć przycisk ***Przenieś do strefy*** **(4).**



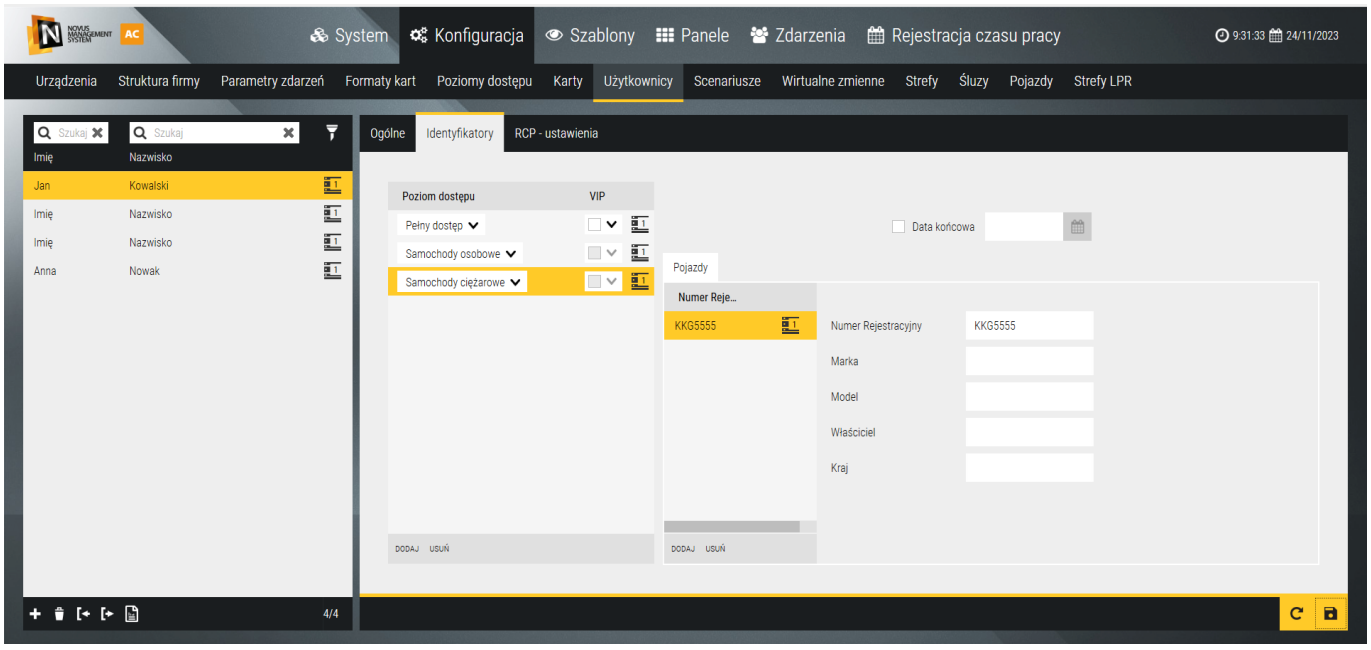
9.6.7 Użytkownicy - Identyfikatory

Nadawanie użytkownikom uprawnień wjazdu do określonych stref realizowane jest przy pomocy zakładki *Użytkownicy/Identyfikatory***.** Polega to na przypisaniu do użytkownika pojazdu (z wcześniej utworzonej bazy pojazdów) oraz nadaniu mu określonego poziomu dostępu. Pełny opis zakładki *Użytkownicy* dostępny jest w niniejszej instrukcji w rozdziale **4.4 Użytkownicy.**



Zakładając, że użytkownik ma mieć dostęp do strefy *„Samochody Osobowe”* samochodem z rejestracją GKW 2222, a do strefy *„Samochody Ciężarowe*” - samochodem z rejestracją KKG 5555, należy w pierwszej kolejności wybrać go z menu po lewej stronie **(1)** i przejść do zakładki *Identyfikatory* **(2).** W polu ***Poziomy dostępu*** należy kliknąć przycisk ***Dodaj*** **(3),** pojawi się wtedy domyślnie ustawiony poziom *„Brak dostępu”,* w polu **(4)** należy zmienić go na *„Samochody osobowe”.* Następnie po kliknięciu ***Dodaj*** **(5)** wyświetli się lista przypisanych do tego użytkownika pojazdów (zdefiniowanych wcześniej w zakładce *Pojazdy*), należy dodać pojazd z rejestracją GKW 2222. Powyższym sposobem została skonfigurowana zakładka na rysunku powyżej.

W przypadku dostępu do drugiej strefy, należy dodać poziom dostępu *„Samochody ciężarowe”* i czynność powtórzyć, z tą różnicą, że w polu **(5)** należy dodać pojazd z rejestracją KKG 5555, tak jak na rysunku poniżej.

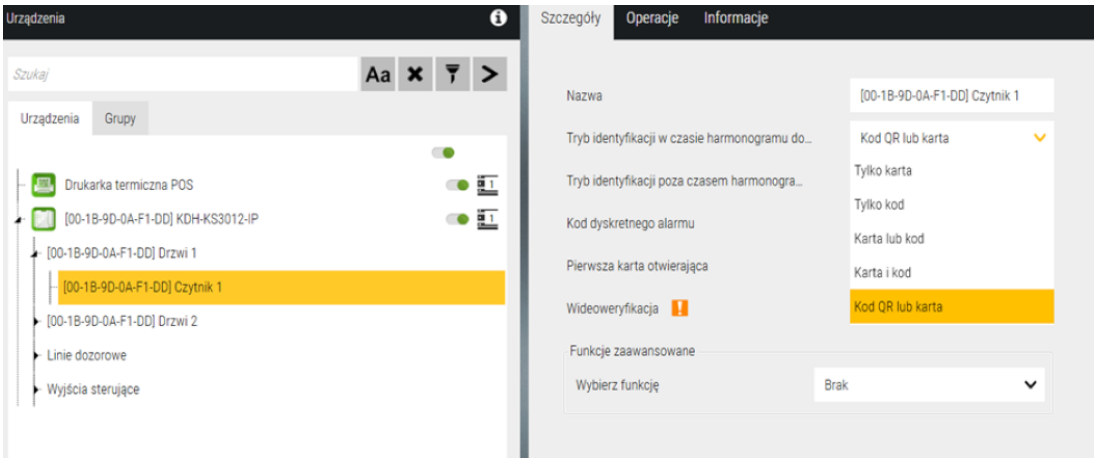


9.6.8 Przypisanie wygenerowanego kodu QR do użytkownika typu Gość

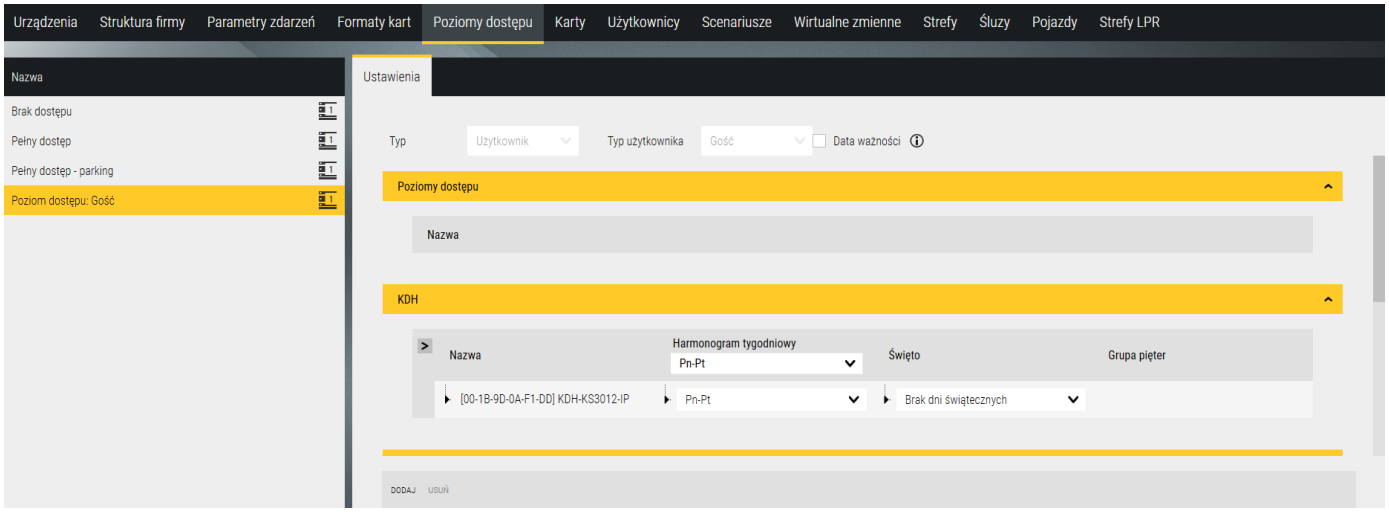
Kolejną funkcją oprogramowania NOVUS MANAGEMENT SYSTEM AC jest możliwość przypisania wygenerowanego kodu QR do użytkownika typu **Gość** oraz wysłania go poprzez e-mail. Funkcja ta pozwala utworzyć jednorazowy lub czasowy kod QR, który umożliwia użytkownikowi wejście i wyjście bez konieczności używania karty.

W tym celu należy dodać kontroler z serii KDH, w tym przykładzie model KDH-KS3012-IP wyposażony w czytnik kodu QR.

Następnie w zakładce *Szczegóły* po wybraniu czytnika należy zaznaczyć w trybie identyfikacji w czasie harmonogramu dostępu: *Kod QR lub karta*.

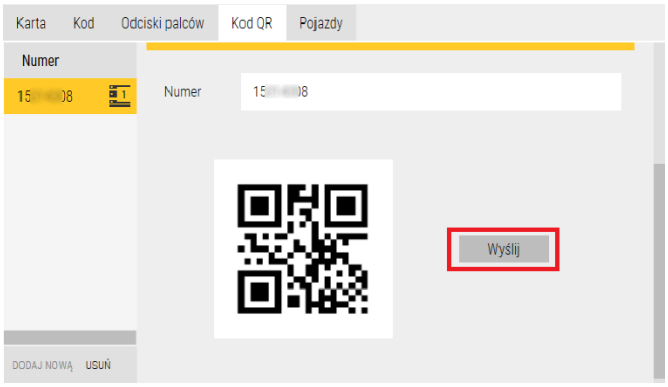


Konieczne jest również utworzenie lub wykorzystanie wcześniej zdefiniowanego poziomu dostępu przeznaczonego dla typu ***Użytkownik/Gość*** oraz przypisanie do niego kontrolera KDH.



UWAGA! Aby można było dodać kontroler KDH do poziomu dostępu dla typu **Użytkownik/Gość**, przedtem należy prawidłowo ustawić tryb identyfikacji na przypisanym do niego czytniku.

Kolejnym krokiem jest wygenerowanie kodu QR dla użytkownika typu **Gość**. W tym celu należy przejść do zakładki *Konfiguracja/Użytkownicy* i wybrać konkretnego użytkownika typu Gość. Następnie w podzakładce *Identyfikatory/ Kod QR* należy użyć opcji ***Dodaj nową***, aby wygenerować nowy kod QR. Na końcu należy kliknąć przycisk ***Wyślij***, aby przesłać kod QR do użytkownika poprzez e-mail.



UWAGA! Funkcja działa po ustawieniu poczty wychodzącej w zakładce *System/Ustawienia*, co zostało opisane w **2.5 Uruchomienie programu** oraz ustawieniu adresu email w polu *E-mail* w zakładce *System/Użytkownicy/Ogólne* dla konkretnego użytkownika, do którego ma zostać wysłany kod QR.

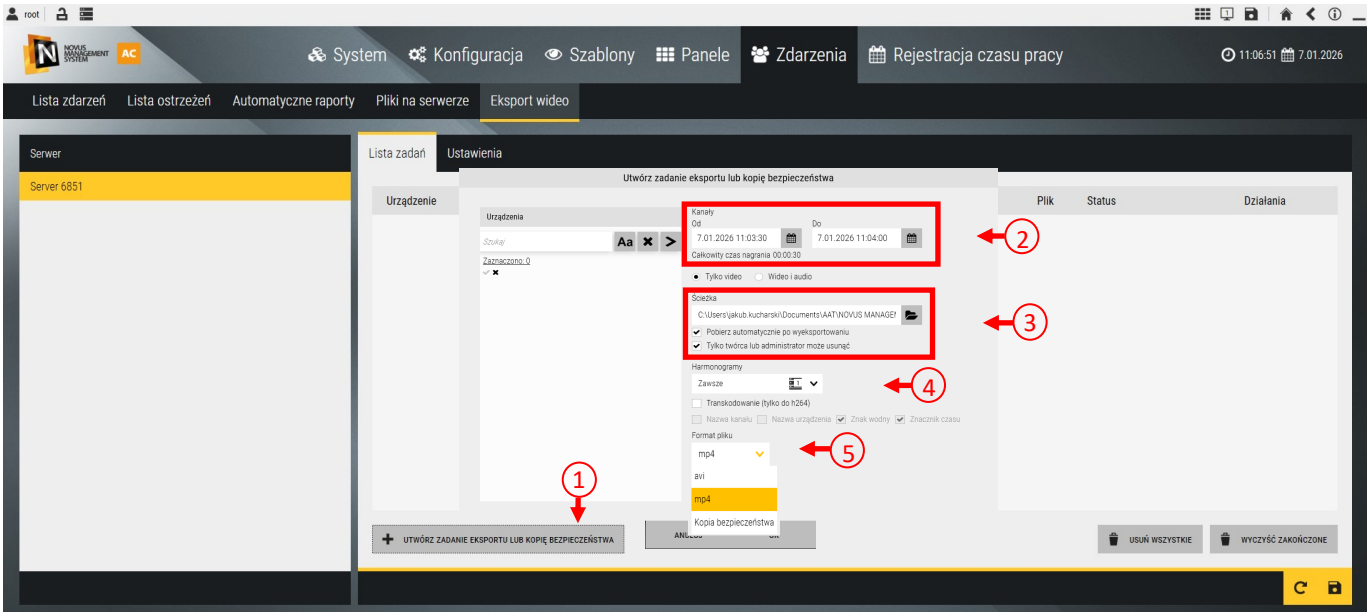
Rezultatem poprawnego skonfigurowania poczty wychodzącej oraz danych użytkownika na skrzynkę pocztową z podanym adresem e-mail powinna pojawić się wiadomość z kodem QR.

W rezultacie prawidłowej konfiguracji, a następnie po zeskanowaniu kodu QR przez czytnik, w logach kontrolera powinny pojawić się wpisy potwierdzające poprawne odczytanie i przetworzenie kodu QR, podobne do tych przedstawionych poniżej.

9.7 Eksport nagrań

9.7.1 Eksport nagrań z poziomu menu głównego

W celu wyeksportowania nagrań zgromadzonych na rejestratorach sieciowych podłączonych do systemu (NMS, NVR, NHDR NOVUS itp.), należy przejść do karty **Zdarzenia**, a następnie **Eksport wideo** i kliknąć przycisk **Utwórz *zadanie eksportu* (1).** Wyświetli się wtedy okno w którym w pierwszej kolejności trzeba wybrać kamery których ma dotyczyć eksport nagrań, można to zrobić w lewej części okna zaznaczając poszczególne kanały wideo.



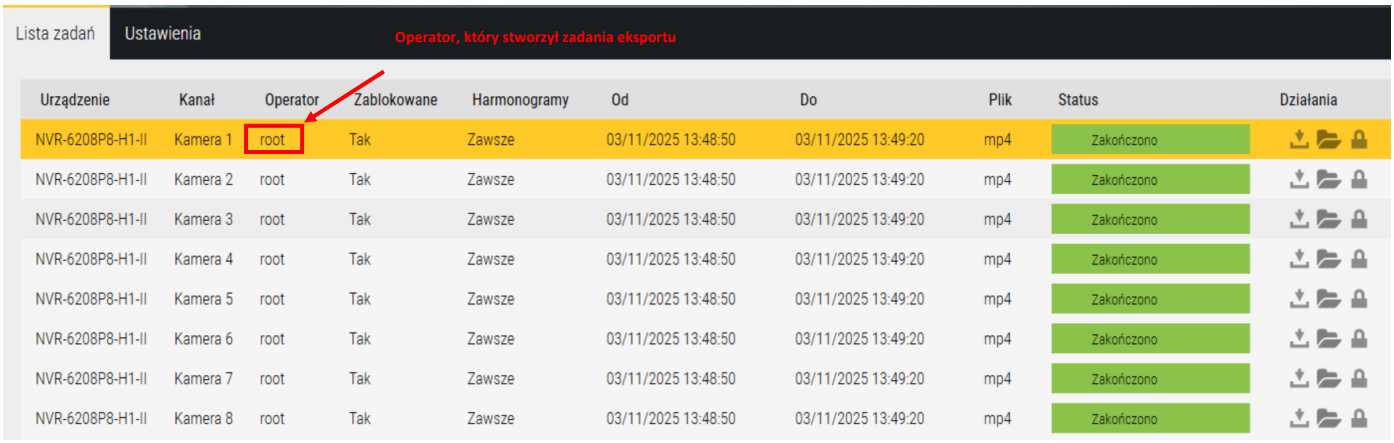
W polu **(2)** klikając w ikonę ***kalendarza*** można wybrać przedział czasu z którego ma być wyeksportowane nagranie natomiast poniżej w istnieje możliwość wyboru czy nagranie ma mieć obraz i/lub dźwięk (funkcja dostępna w przyszłości). Warto nadmienić, że nagrania są eksportowane z urządzeń nagrywających do serwera NOVUS MANAGEMENT SYSTEM AC. Aby nagrania od razu po wyeksportowaniu zostały pobrane i zapisane pod wybraną ścieżką na jednostce na której znajduje się klient NOVUS MANAGEMENT SYSTEM AC, w polu **(3)** należy zaznaczyć checkbox „**Pobierz automatycznie po wyeksportowaniu**” w przeciwnym wypadku zostaną one wyeksportowane do serwera NOVUS MANAGEMENT SYSTEM AC i będą gotowe do pobrania poprzez kliknięcie przycisku znajdującego się obok niebieskiego paska ze statusem „Gotowy do pobrania”. Zaznaczenie checkboxa „**Tylko twórca lub administrator może usunąć**” powoduje, że utworzony plik może zostać usunięty wyłącznie przez administratora (root) lub operatora, który utworzył zadanie eksportu, opcja domyślnie jest zaznaczona. Funkcja Harmonogramy **(4)** służy do okresowego eksportu nagrań i będzie dostępna w przyszłości. Istnieje również możliwość wybrania formatu w jakim mają być wyeksportowane nagrania **(5),** dostępne formaty to: AVI i mp4.

Po kliknięciu przycisku ***OK*** ustawienia zostaną zapisane, natomiast aby nagrania zostały wyeksportowane i pobrane należy kliknąć ikonę ***dyskietki*** znajdującą się w prawym dolnym rogu okna. Po pomyślnym pobraniu nagrań wyświetli się status **Zakończono**.

Ikona służy do otwarcia folderu w którym zostały zapisane pobrane nagrania, natomiast ikona służy do usunięcia wybranej pozycji z listy. Ikona oznacza zablokowanie usunięcia nagrania znajdującego się na liście zadań eksportu.

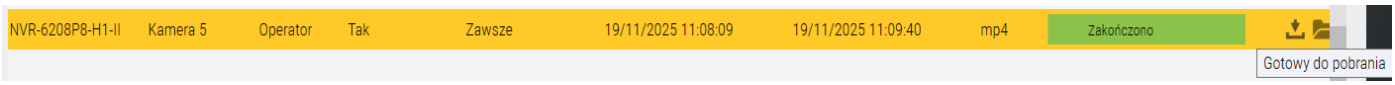
Lista zadań

Poniżej przedstawiono listę zadań eksportu wideo. Zadania zostały zrealizowane przy zaznaczonej opcji *Tylko twórca lub administrator może usunąć* na koncie operatora root. Obecnie zalogowane konto Operator1 nie ma możliwości usunięcia tych nagrań - co symbolizuje ikona ***zamkniętej kłódki***. Ta opcja zabezpiecza przed przypadkowym usunięciem nagrań.

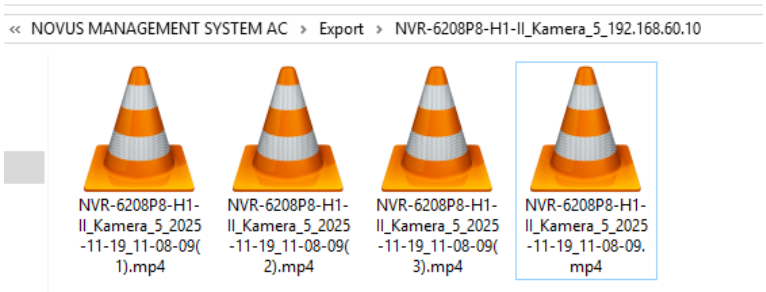


Urządzenie	Kanał	Operator	Zablokowane	Harmonogramy	Od	Do	Plik	Status	Działania
NVR-6208P8-H1-II	Kamera 1	root	Tak	Zawsze	03/11/2025 13:48:50	03/11/2025 13:49:20	mp4	Zakończono	
NVR-6208P8-H1-II	Kamera 2	root	Tak	Zawsze	03/11/2025 13:48:50	03/11/2025 13:49:20	mp4	Zakończono	
NVR-6208P8-H1-II	Kamera 3	root	Tak	Zawsze	03/11/2025 13:48:50	03/11/2025 13:49:20	mp4	Zakończono	
NVR-6208P8-H1-II	Kamera 4	root	Tak	Zawsze	03/11/2025 13:48:50	03/11/2025 13:49:20	mp4	Zakończono	
NVR-6208P8-H1-II	Kamera 5	root	Tak	Zawsze	03/11/2025 13:48:50	03/11/2025 13:49:20	mp4	Zakończono	
NVR-6208P8-H1-II	Kamera 6	root	Tak	Zawsze	03/11/2025 13:48:50	03/11/2025 13:49:20	mp4	Zakończono	
NVR-6208P8-H1-II	Kamera 7	root	Tak	Zawsze	03/11/2025 13:48:50	03/11/2025 13:49:20	mp4	Zakończono	
NVR-6208P8-H1-II	Kamera 8	root	Tak	Zawsze	03/11/2025 13:48:50	03/11/2025 13:49:20	mp4	Zakończono	

Wyeksportowane nagranie można pobrać na komputer klienta NOVUS MANAGEMENT SYSTEM AC wiele razy. Po każdym pobraniu status pozostaje **Zakończono**, a ikona ***pobierania*** jest nadal aktywna, co umożliwia ponowne pobranie pliku.

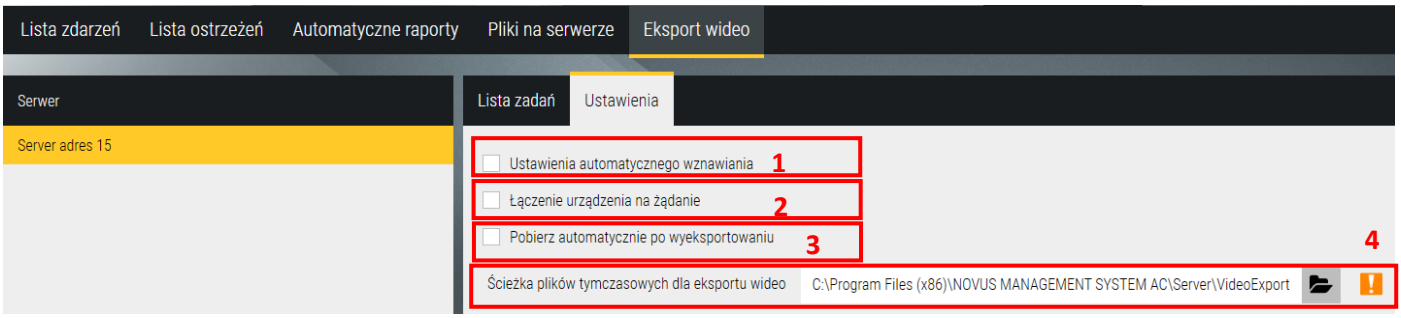


Poniżej przedstawiono folder ze ścieżką przypisaną do plików nagrań, w którym znajdują się trzy kopie pliku, pobranego kilkukrotnie.



Ustawienia globalne eksportu wideo

Dodatkowo w zakładce *Eksport wideo/Ustawienia* dodano możliwość zaznaczenia opcji *Ustawienia automatycznego* wznawiania z urządzeniami, *Łączenie urządzenia na żądanie* czy *Pobierz automatycznie po wyeksportowaniu* pliku. Funkcje te działają globalnie dla wszystkich zadań eksportu i pozwalają na optymalizację pracy systemu, szczególnie w środowiskach z dużą liczbą kamer i rejestratorów.



1. **Automatyczne wznawianie** - system samodzielnie próbuje ponownie pobrać nagrania w przypadku chwilowej utraty łączności lub wystąpienia innych problemów technicznych.
2. **Łączenie na żądanie** - opcja umożliwiająca automatyczne nawiązanie połączenia z urządzeniem w przypadku żądania eksportu wideo z danego urządzenia. Jeśli opcja jest odznaczona użytkownik musi ręcznie nawiązać połączenie z urządzeniem.
3. **Pobierz automatycznie po wyeksportowaniu** - po zakończeniu eksportu nagrania system automatycznie pobiera go na urządzenie klienta aplikacji. Opcja jest domyślnie zaznaczona.
4. **Ścieżka plików tymczasowych dla eksportu wideo** - system wykorzystuje lokalną ścieżkę tymczasową do przechowywania plików przed ich finalnym zapisaniem lub pobraniem.

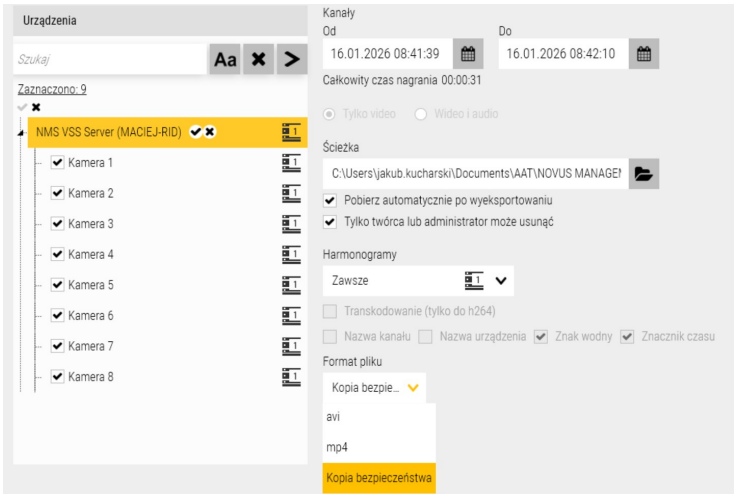
Dzięki tym opcjom możliwe jest zmniejszenie obciążenia sieci i serwera, przy jednoczesnym zachowaniu pełnej funkcjonalności systemu.

Kopia bezpieczeństwa w NOVUS MANAGEMENT SYSTEM AC

Oprócz standardowego eksportu nagrań w formatach .avi oraz .mp4, dostępnych w oprogramowaniu NOVUS MANAGEMENT SYSTEM AC, system umożliwia również wykonanie kopii bezpieczeństwa nagrań w formacie .pak, przy czym funkcja tworzenia kopii bezpieczeństwa jest dostępna wyłącznie dla kanałów dodanych do NOVUS MANAGEMENT SYSTEM VSS.

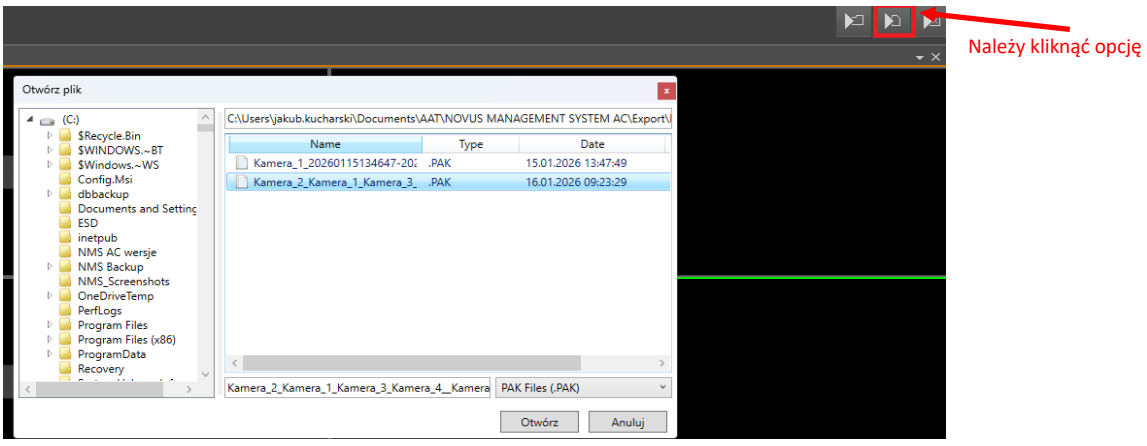
Format .pak jest specjalnym formatem tworzenia kopii bezpieczeństwa materiału wideo bez wprowadzania jakichkolwiek modyfikacji w stosunku do materiału źródłowego. Dodatkowo format .pak pozwala na łączenie nagrań z kilku kanałów w jeden plik, w przeciwieństwie do formatów .avi i .mp4.

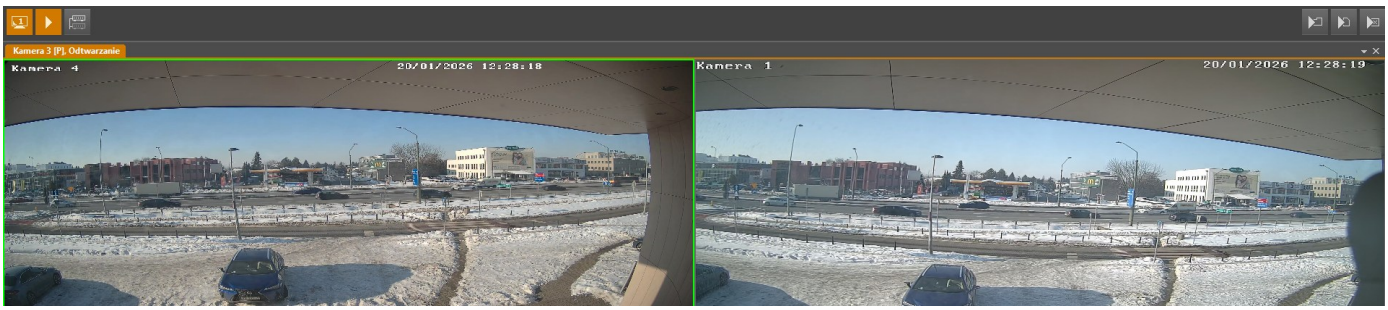
W tym celu, podczas procesu eksportu nagrań, należy jako format pliku wybrać opcję *Kopia bezpieczeństwa*, a następnie wskazać kanały z połączonego NOVUS MANAGEMENT SYSTEM VSS, z których mają zostać wyeksportowane nagrania.



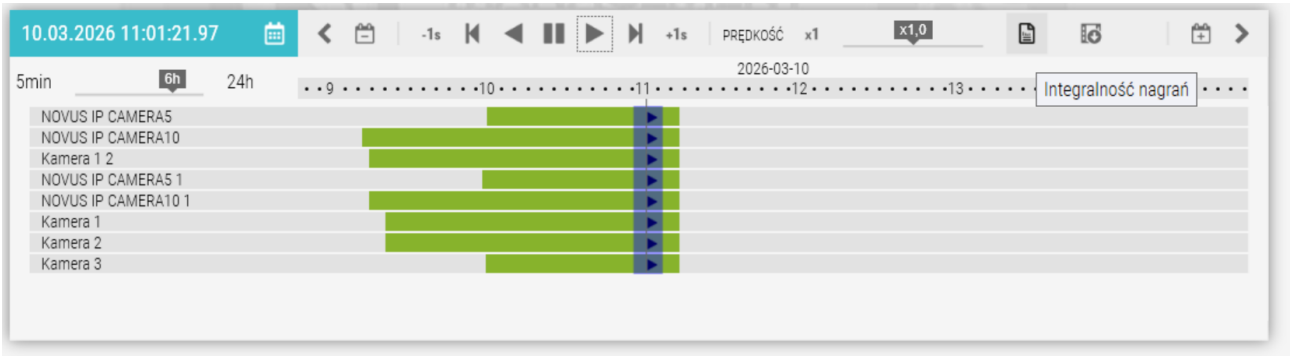
UWAGA! Aby wykonać kopię bezpieczeństwa, należy dodać serwer NMS VSS i nawiązać z nim połączenie.

Po udanym wykonaniu kopii w celu jej odtworzenia należy odtworzyć nowo powstały plik w programie NMS VSS Player, wybierając opcję *Plik*. Następnie zostanie wyświetlone okno z nagraniami.

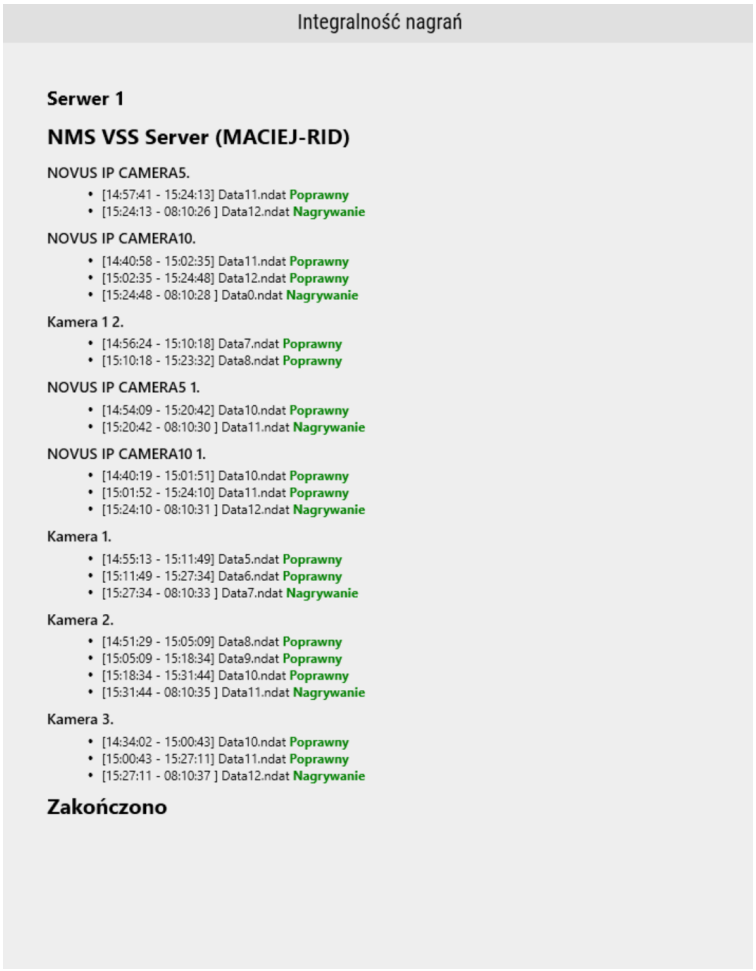




Aby sprawdzić integralność nagrań, należy w narzędziu *Wideo* w NMS VSS wybrać odpowiedni widok wideo, a następnie zaznaczyć wybrany przedział czasu na dolnym grafie odtwarzania. Kolejnym krokiem jest kliknięcie przycisku *Integralność nagrań*.



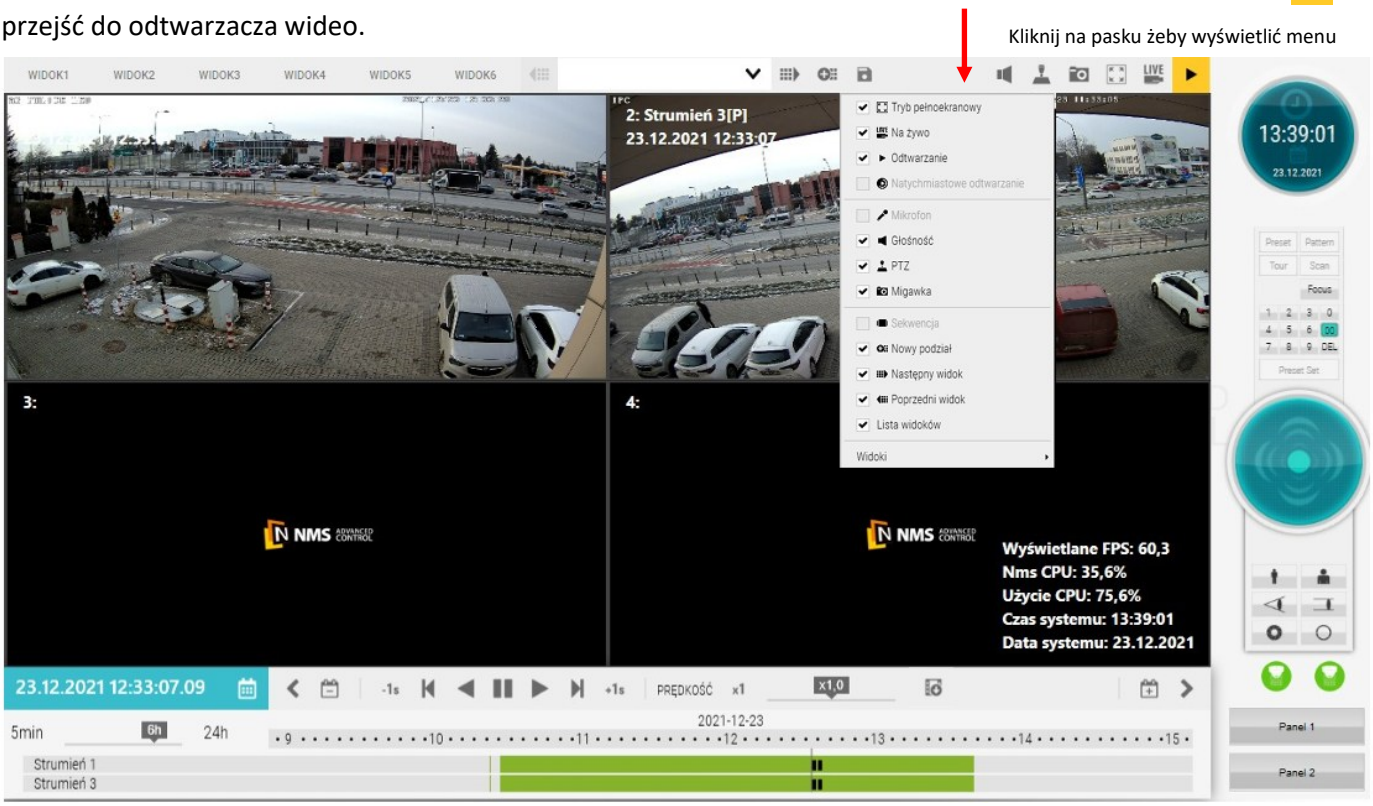
Jeżeli konfiguracja systemu jest prawidłowa, status integralności powinien być wyświetlany jako *Poprawny* lub *Nagrywanie*.



W zakładce *Rejestrator*, dla każdego kanału, należy włączyć nagrywanie obu strumieni, zaznaczając opcję *Utwórz przestrzeń do nagrywania dla strumieni pomocniczych*.

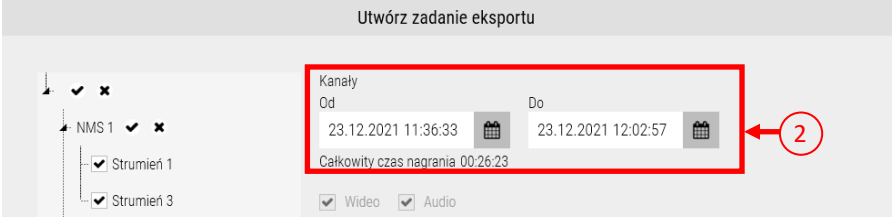
9.7.2 Eksport nagrań z poziomu odtwarzacza wideo

Drugi sposób na eksport nagrań z serwera NMS polega na przejściu do panelu w którym umieszczony jest odtwarzacz oraz okno wideo. Można to wykonać przechodząc do zdefiniowanego domyślnie panelu 3. Aby to zrobić należy kliknąć na ikonę znajdującą się po prawej części górnego paska interfejsu. Następnie w oknie ***Wideo*** należy wybrać widok z kamer, z których mają zostać wyeksportowane nagrania po czym kliknąć przycisk aby przejść do odtwarzacza wideo.



Istnieją dwa sposoby na zdefiniowanie przedziału czasu z którego mają zostać wyeksportowane nagrania, jeden z nich został wymieniony na poprzedniej stronie. Drugim sposobem jest przeciągnięcie kursora myszy po osi czasu, trzymając wciśnięty prawy przycisk myszy.

Po zaznaczeniu wybranego obszaru na osi czasu należy kliknąć ikonę ***eksportu*** oznaczoną numerem **(1),** wyświetlone zostanie wtedy okno ***Utwórz zadanie eksportu*** w którym pole **(2)** będzie automatycznie wypełnione dla każdego zaznaczonego kanału, zgodnie z zaznaczeniem na osi czasu.

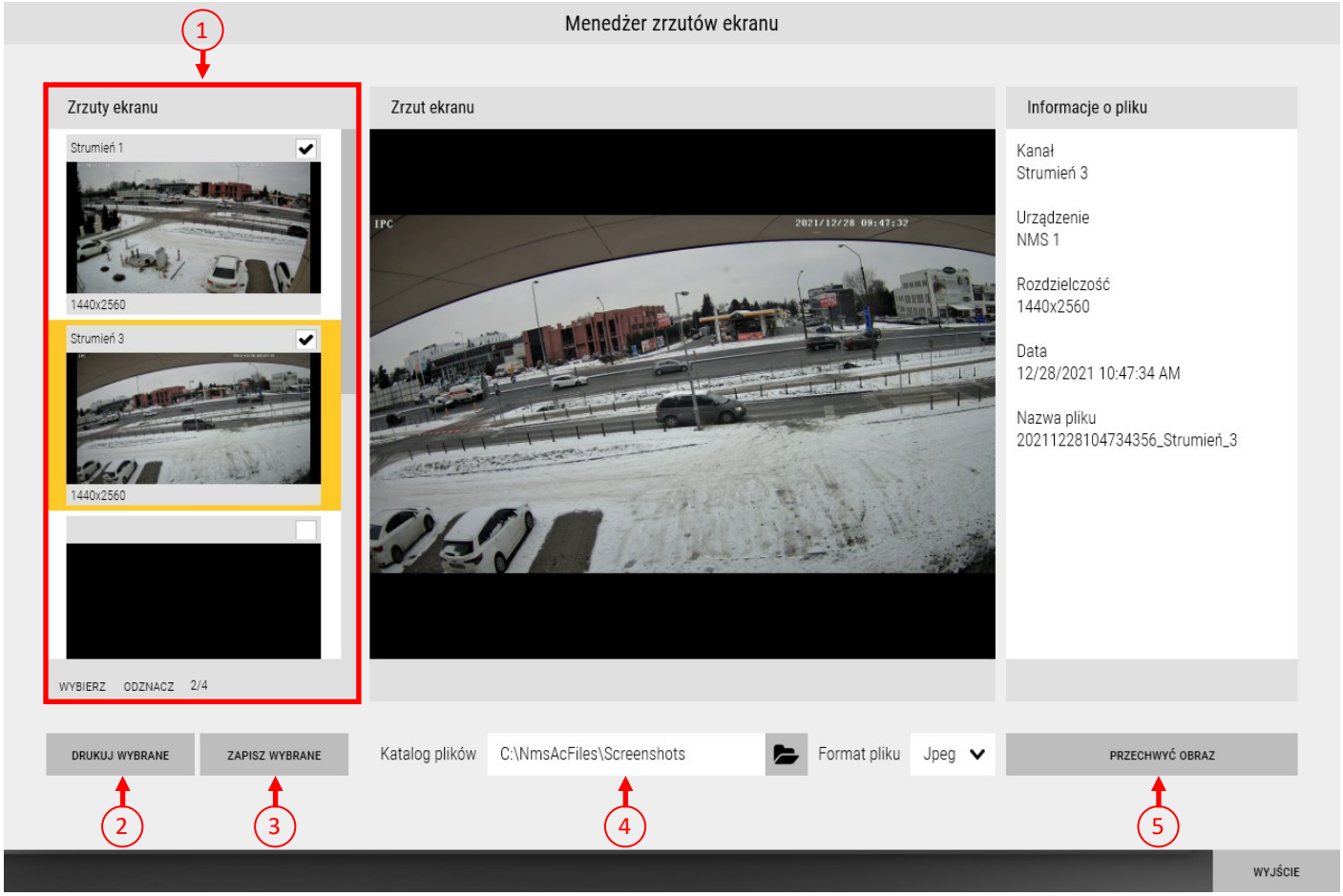


Aby wyeksportować i pobrać nagranie należy postępować analogicznie jak jest to opisane w rozdziale **Eksport nagrań z poziomu menu głównego** z poprzedniej strony.

9.8 Pobieranie zrzutów ekranu

W celu wykonania zrzutów ekranu należy przejść do panelu w którym znajduje się okno wideo, można to zrobić przechodząc do zdefiniowanego domyślnie panelu 3. Aby to zrobić należy kliknąć ikonę znajdującą się po prawej części górnego paska interfejsu. Następnie w oknie wideo należy wybrać widok z kamer, z których ma zostać wykonany zrzut ekranu. W zależności od tego czy zrzut ekranu ma zostać wykonany z nagrania „live" czy nagrania z odtwarzacza wideo, należy kliknąć odpowiednią ikonę w prawym górnym rogu okna wideo .

Aby przejść do menadżera zrzutów ekranu należy kliknąć ikonę ***aparatu*** .



W menadżerze zrzutów ekranu w polu **(1)** istnieje możliwość wybrania kanałów z których mają zostać przechwycone obrazy. Za pomocą przycisku ***Przechwyć Obraz*** **(5)** można przechwycić aktualnie wyświetlany w odtwarzaczu obraz, jeżeli odtwarzacz jest ustawiony w tryb „live" to przechwytywany jest aktualny widok z kamery. Ścieżkę do folderu w którym zapisywane są przechwycone obrazy można wpisać w polu **(4)** lub wskazać ręcznie po kliknięciu ikony , obok znajduje się pole ***Format pliku*** gdzie z listy rozwijanej można wybrać format w jakim ma zostać zapisany obraz (Jpeg, Png lub Bmp). Kliknięcie przycisku ***Drukuj Wybrane*** **(2)** służy do bezpośredniego wydrukowania zdjęć bez ich zapisywania na komputerze, natomiast przycisk ***Zapisz wybrane*** **(3)** powoduje zapisanie zdjęć w wyznaczonym katalogu plików.

9.9 Integracja z Systemami sygnalizacji włamania i napadu

Program NOVUS MANAGEMENT SYSTEM AC umożliwia integrację z systemem sygnalizacji włamania i napadu. Dodawanie urządzeń zostało opisane w rozdziale **3.14 Urządzenia - System Sygnalizacji włamania i napadu.**

Podłączone urządzenia można obsługiwać z poziomu Paneli opisanych w rozdziale **6. Panele.**

Modyfikacje lub utworzenie nowych paneli pozwala w pełni wykorzystać możliwości integracji z systemem sygnalizacji włamania i napadu. W tym celu należy wejść w dany panel za pomocą przycisku znajdującego się w głównej belce programu następnie wybrać odpowiedni panel.

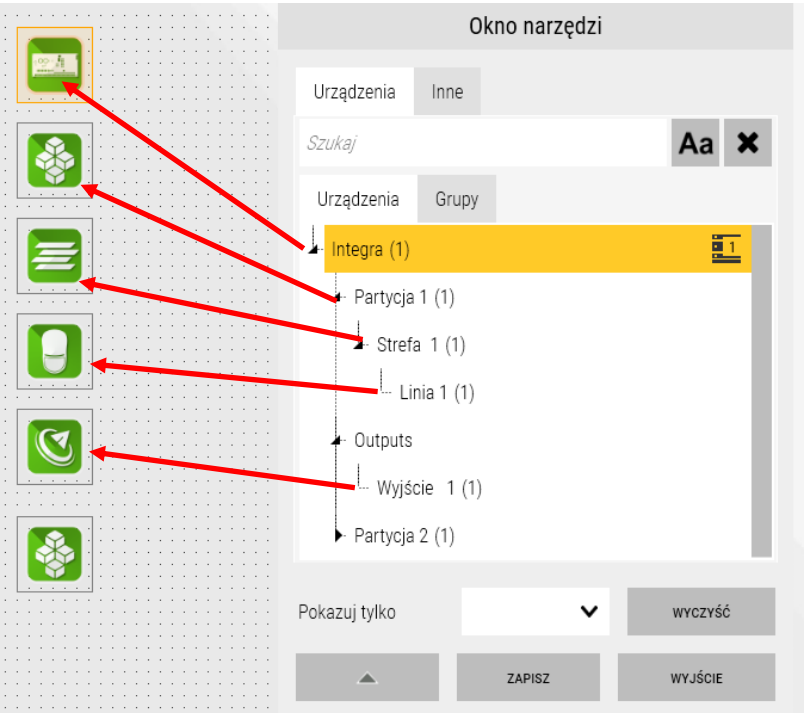
Po wyborze panelu można przejść do jego edycji za pomocą ikony ***ołówka*** .

Pojawia się wtedy ***Okno narzędzi***, w którym znajdują się wszystkie elementy do konfiguracji panelu.

W zakładce *Urządzenia* możemy znaleźć dodane wcześniej urządzenia SSWiN. Można je przenieść na panel przeciągając samo urządzenie, partycje, strefę lub wejście.

Po wyjściu z trybu edycji kliknięcie myszką na ikonę ***urządzenia*** pozwala wyświetlić jego listę zdarzeń.

Lista zdarzeń dla centrali, partycji czy strefy odpowiada operacją z rozdziału **3.16 Urządzenia - Systemy sygnalizacji włamania i napadu - Operacje.**



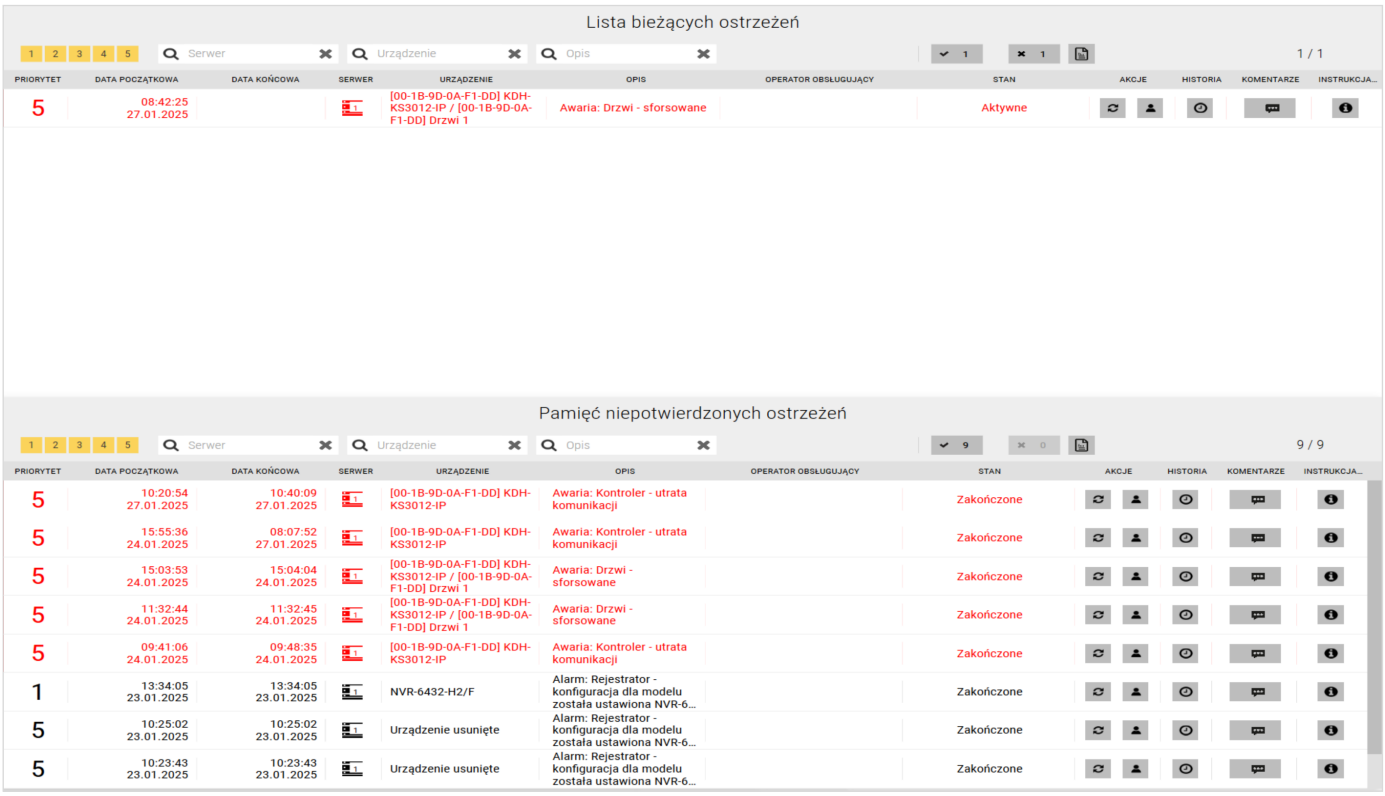
Czynności które można również wykonać to blokowanie/odblokowywanie wejść oraz sterowanie włączeniem i wyłączeniem wyjść. Sterować można wyłącznie wyjściami, które posiadają zaprogramowany odpowiedni typ.

Niedostępne funkcje są wyszarzone.

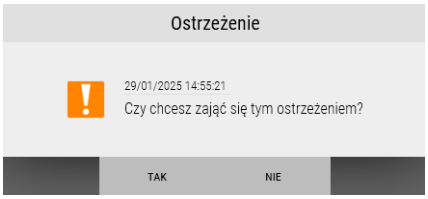
9.10 Narzędzie obsługi ostrzeżeń: wizualizacja i raportowanie

Ostrzeżenia - jest to narzędzie obrazujące stan elementów systemów działających na obiekcie pod kątem ewentualnych awarii i alarmów (ostrzeżeń). Po włączeniu opcji wymagania komentarzy, każde zdarzenie zdefiniowane jako alarm lub awaria musi zostać skomentowane przez operatora systemu. Możliwe jest generowania raportów obrazujących aktualny stan alarmów/awarii (ostrzeżeń) na obiekcie oraz historię ich przebiegu wraz z komentarzami.

Narzędzie dzieli się na listę bieżących ostrzeżeń (aktualnie występujących) jak również pamięć niepotwierdzonych ostrzeżeń (aktualnie niewystępujących).

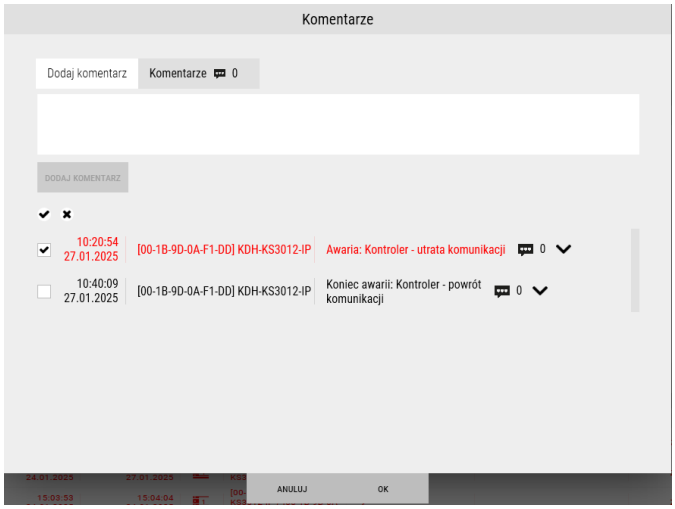


W kolumnie *AKCJE* dostępne są opcje pozwalające zmienić stan ostrzeżenia na potwierdzony lub je zakończyć (dotyczy ostrzeżenia bieżącego), a także przejąć obsługę nad danym ostrzeżeniem.

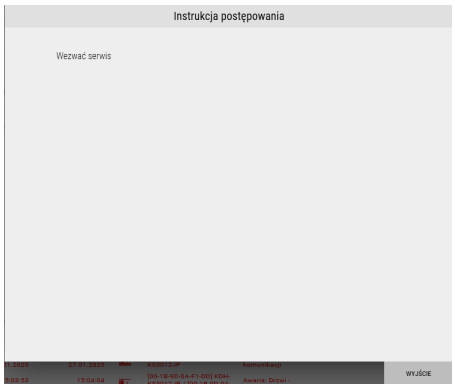


Kolumna *HISTORIA* pozwala zobaczyć historię zdarzeń związaną z ostrzeżeniem.

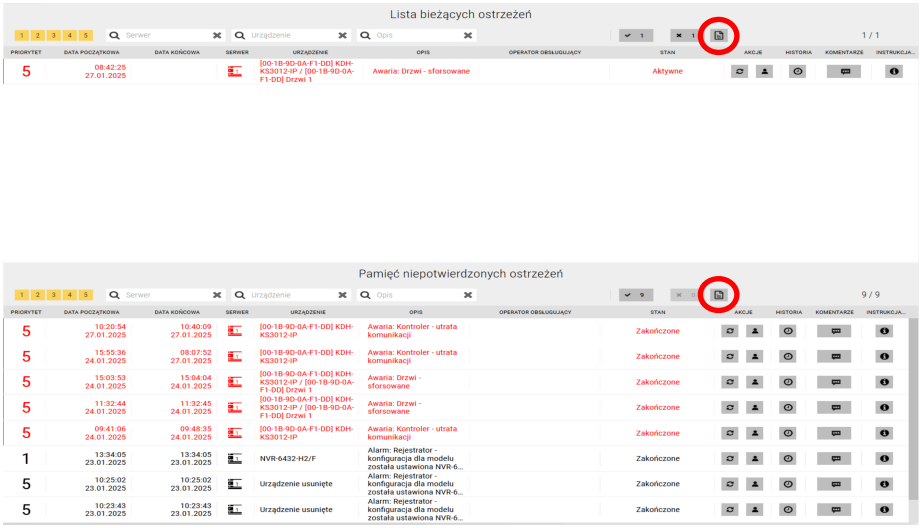
Kolumna *KOMENTARZE* pozwala dodać lub odczytać komentarz do ostrzeżenia oraz końca ostrzeżenia.

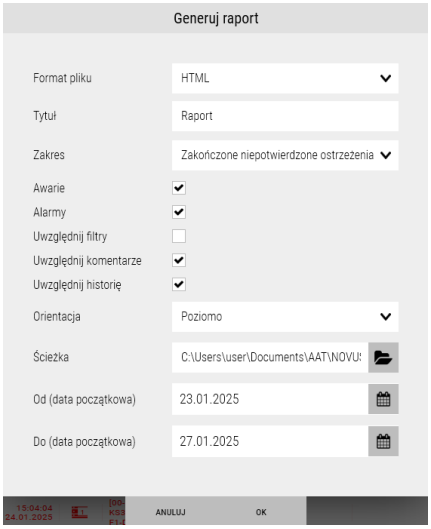


Kolumna *INSTRUKCJA POSTĘPOWANIA* pozwala podejrzeć instrukcję przygotowaną przez instalatora w przypadku pojawienia się danego ostrzeżenia (instrukcję dodajemy w menu *Konfiguracja/Parametry zdarzeń*).



Możliwe jest również wygenerowanie raportów z bieżących jak i niepotwierdzonych ostrzeżeń.





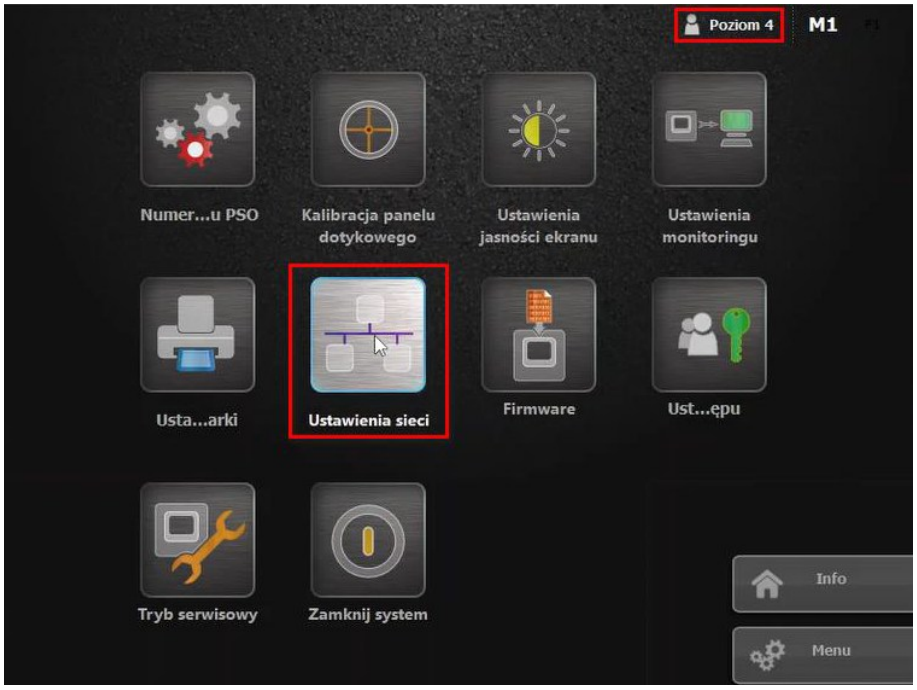
9.11 - Integracja (wizualizacja) z systemami sygnalizacji pożaru Polon 6000

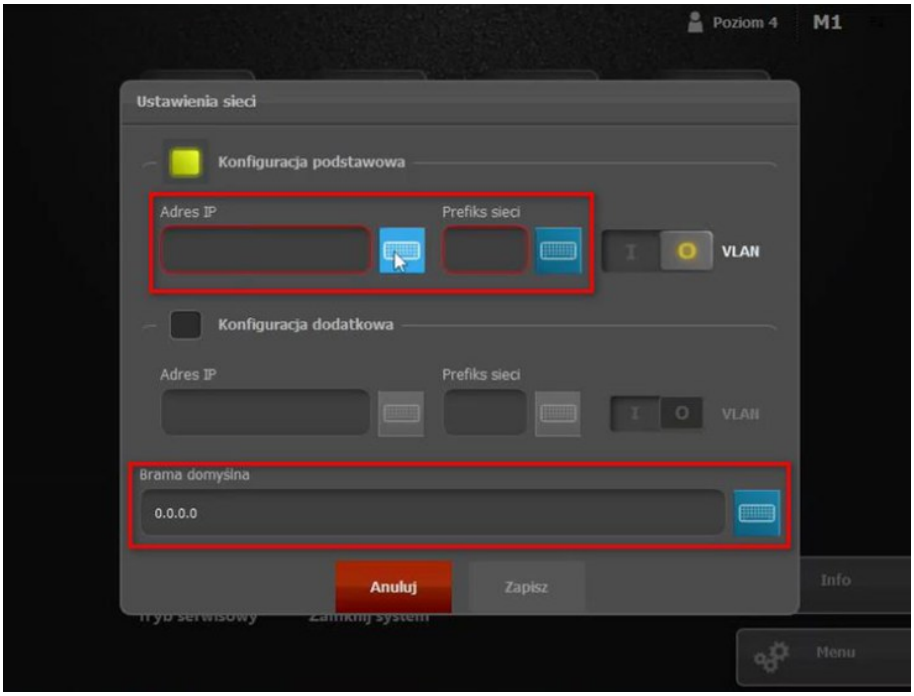
Konfiguracja centrali Polon 6000 pod kątem współpracy z oprogramowaniem NOVUS MANAGEMENT SYSTEM AC

W celu skonfigurowania centrali Polon 6000 do komunikacji z oprogramowaniem NOVUS MANAGEMENT SYSTEM AC należy:

- Zalogować się w centrali na poziomie P4 (domyślne hasło P4)
- Ustawić odpowiedni adres IP oraz pozostałe parametry sieciowe centrali wybierając:

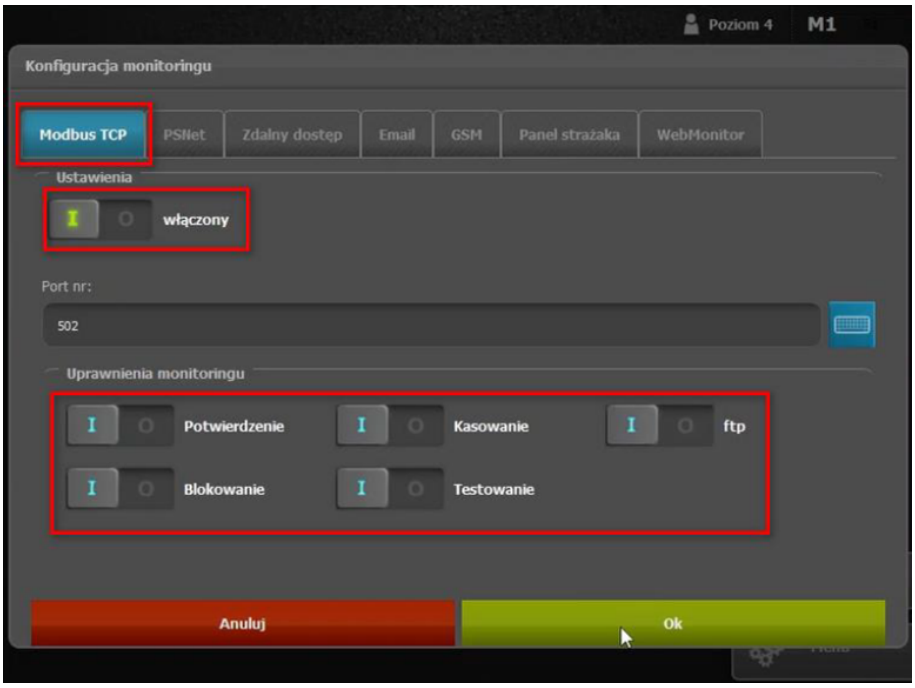
  Menu -> Konfiguracja PSO -> Ustawienia sieć





- Przejść do

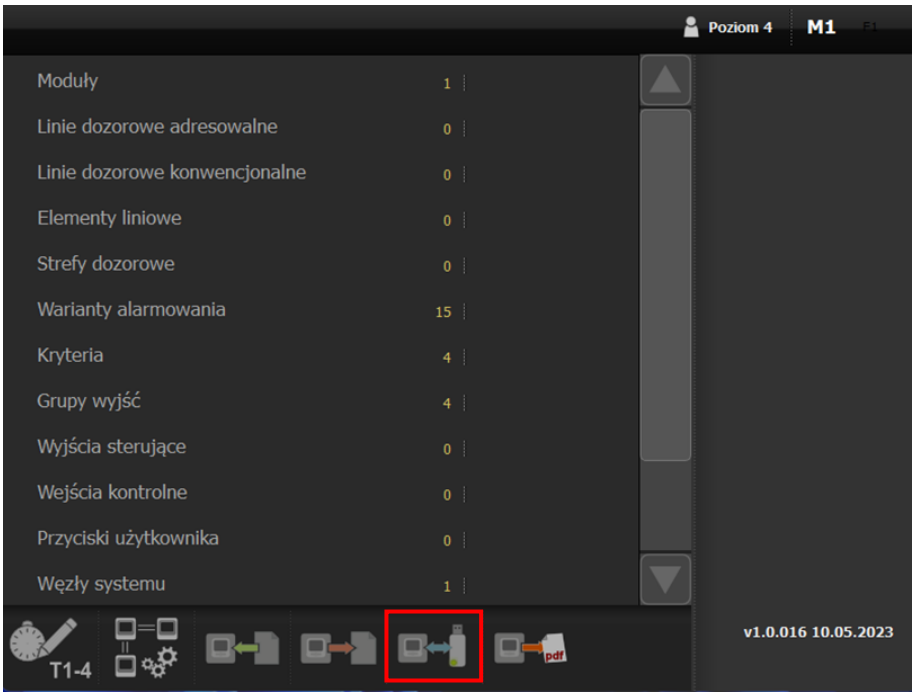
  Menu -> Konfiguracja PSO -> Ustawienia monitoringu
  MODBUS TCP -> włączony



UWAGA! Po włączeniu funkcji Modbus należy wykonać restart modułu PSO

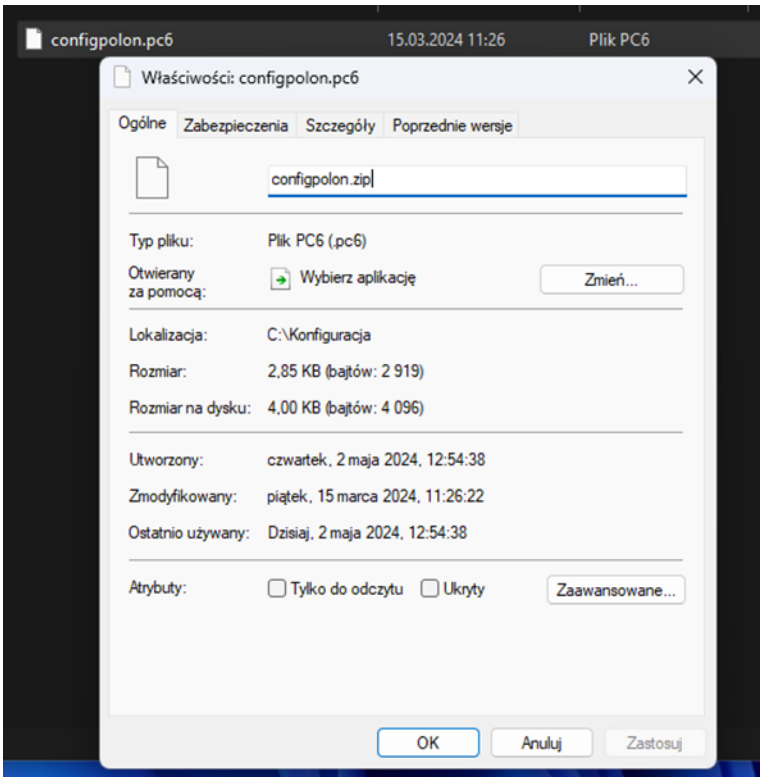
Eksport konfiguracji z centrali Polon 6000 oraz jej import do oprogramowania NOVUS MANAGEMENT SYSTEM AC

- Po zalogowaniu się do centrali przechodzimy do konfiguracji systemu (kopiowanie konfiguracji)

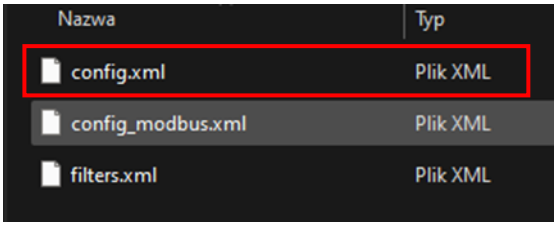


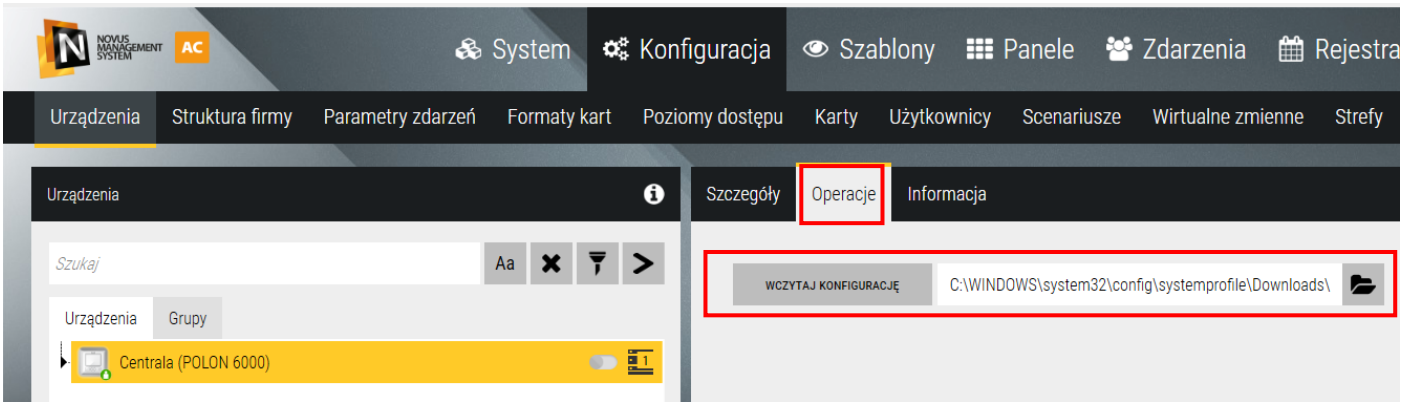
- Eksportujemy konfigurację na Pendrive.

- Po wyeksportowaniu konfiguracji otrzymujemy plik *.pc6, należy zmienić jego rozszerzenie na *.zip a następnie wypakować jego zawartość.



- Otrzymujemy plik config.xml, który należy zaimportować w oprogramowaniu NOVUS MANAGEMENT SYSTEM AC dla wybranej centrali Polon 6000



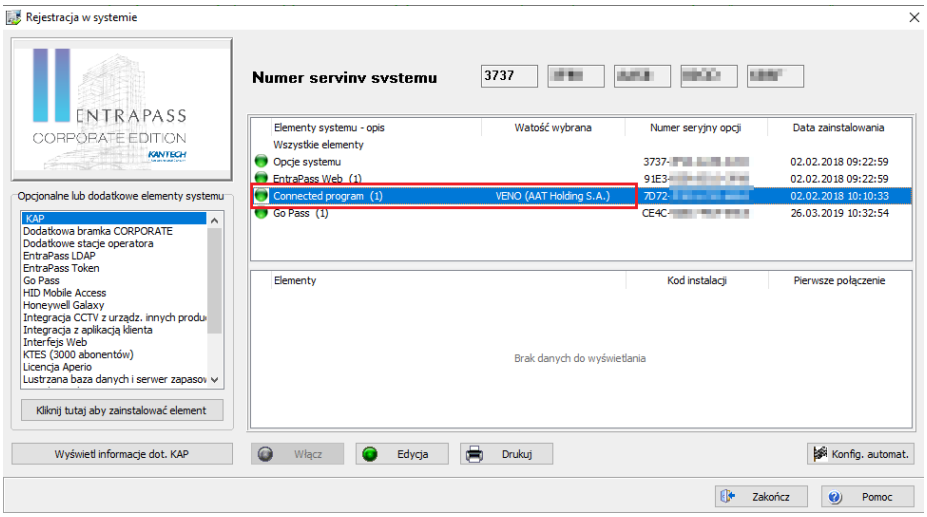


9.12 Integracja (wizualizacja) z systemem kontroli dostępu KANTECH

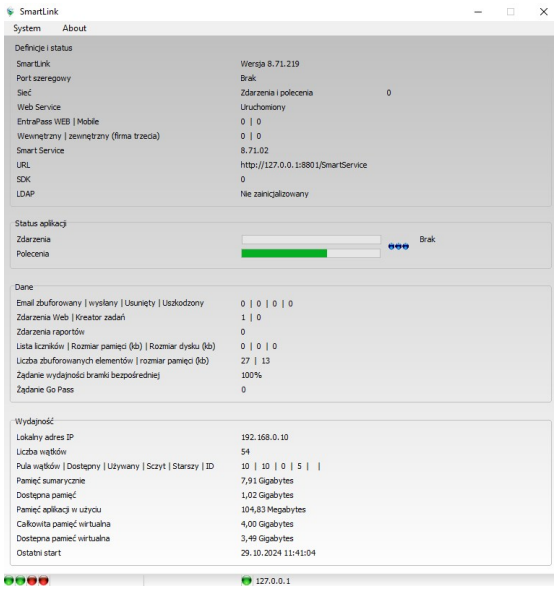
Konfiguracja oprogramowania EntraPass pod kątem współpracy z oprogramowaniem NOVUS MANAGEMENT SYSTEM AC

W celu skonfigurowania oprogramowania EntraPass firmy Kantech do programu NOVUS MANAGEMENT SYSTEM AC należy upewnić się że:

Oprogramowanie EntraPass jest w wersji ***Corporate*** lub ***Global*** i posiada aktywną licencję CONNECT dla integracji z aplikacją klienta:



Aplikacja SmartLink jest zainstalowana i aktywna, oraz ma połączenie z serwerem EntraPass:

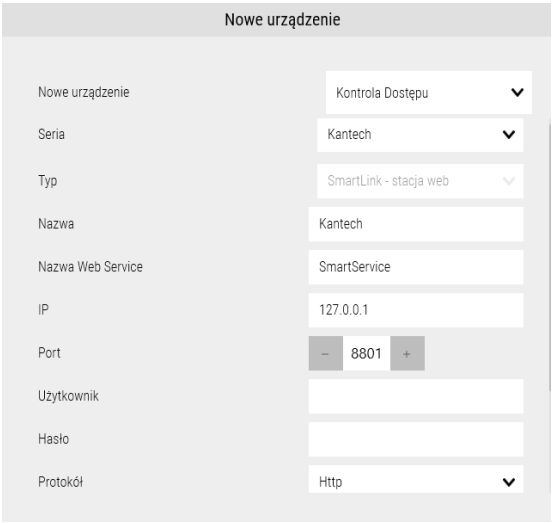


Konfiguracja oprogramowania NOVUS MANAGEMENT SYSTEM AC pod kątem współpracy z programem EntraPass marki Kantech:

- Należy upewnić się że oprogramowanie NOVUS MANAGEMENT SYSTEM AC jest w odpowiedniej wersji obsługującej integrację - minimum 6.01.XX
- Jest wystarczająca ilość punktów licencyjnych (zakładka *System/Licencje/Licencje*) - minimum 60 pkt

Dodawanie kontrolerów KATECH do oprogramowania NOVUS MANAGEMENT SYSTEM AC:

W zakładce *Konfiguracja* dodajemy ikoną **„+”** nowe urządzenie i wybieramy *Kontrola Dostępu - Seria - Kantech*



Nazwa - edytowalne pole tekstowe opisujące połączenie z kontrolerami marki KANTECH

Nazwa Web Service - edytowalne pole tekstowe, należy uzupełnić tak jak skonfigurowana jest nazwa dla aplikacji SmartLink w zakładce *Smartlink Web i API* w oprogramowaniu EntraPass

IP - pole adresu IP aplikacji SmartLink

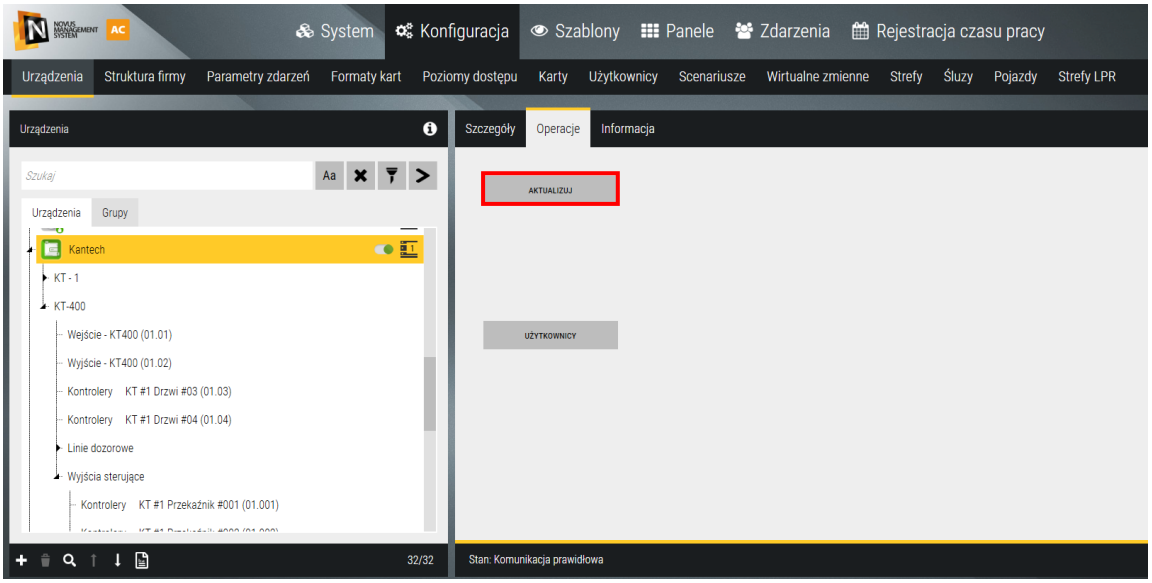
Port - Port aplikacji SmartLink konfigurowany w zakładce *Smartlink Web i API* w oprogramowaniu EntraPass - Port Web Service

Użytkownik - nazwa użytkownika/operatora dla systemu Entrapass

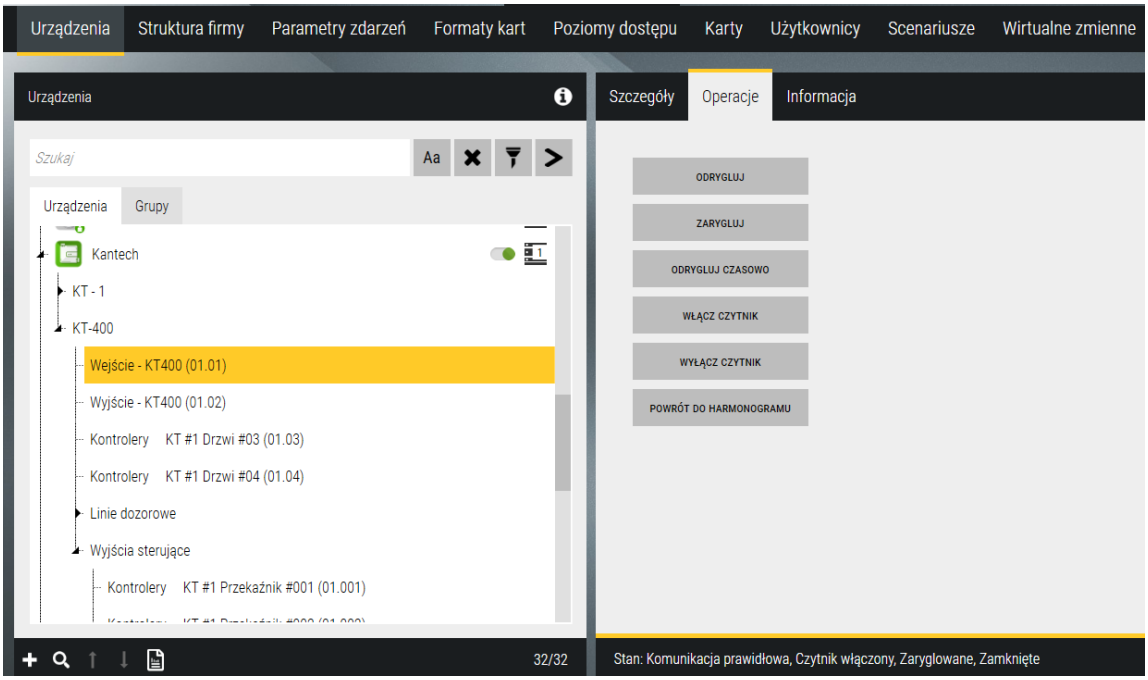
Hasło - hasło użytkownika/operatora dla systemu Entrapass

Protokół - protokół komunikacji konfigurowany w zakładce *Smartlink Web i API* w oprogramowaniu EntraPass - wybrać *http* lub *https*

Po zapisaniu i prawidłowej konfiguracji ikona ***połączenia*** powinna wyświetlać się na zielono, stan powinien zmienić status na - Komunikacja prawidłowa.



Aktualizuj - pobiera informację o wszystkich kontrolerach, drzwiach, liniach dozorowych oraz wyjściach sterujących znajdujących się w oprogramowaniu EntraPass i wyświetla ich listę i stan w postaci drzewa w zakładce *Urządzenia*.



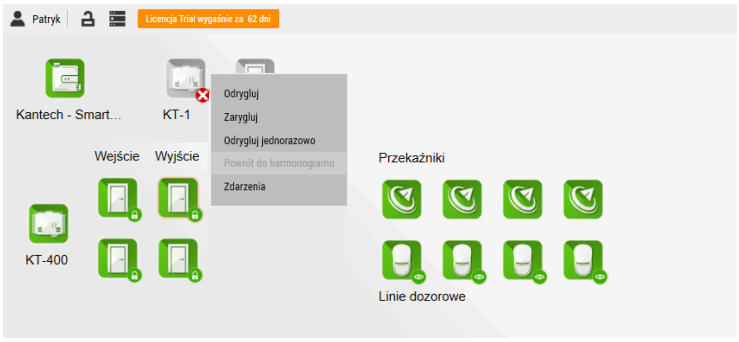
W zakładce *Operacje* możemy wykonywać polecenia dotyczące dodanych urządzeń, wejść i wyjść:

Drzwi - odrygluj/zarygluj/odrygluj czasowo/włącz czytnik/wyłącz czytnik/powrót do harmonogramu

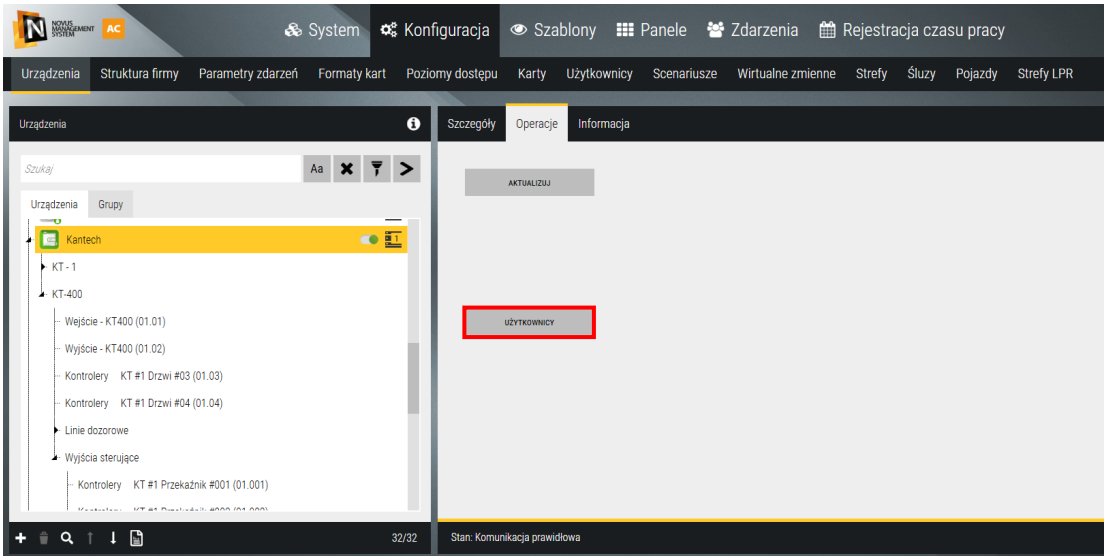
Wyjścia sterujące - włącz/wyłącz/włącz czasowo/powrót do harmonogramu

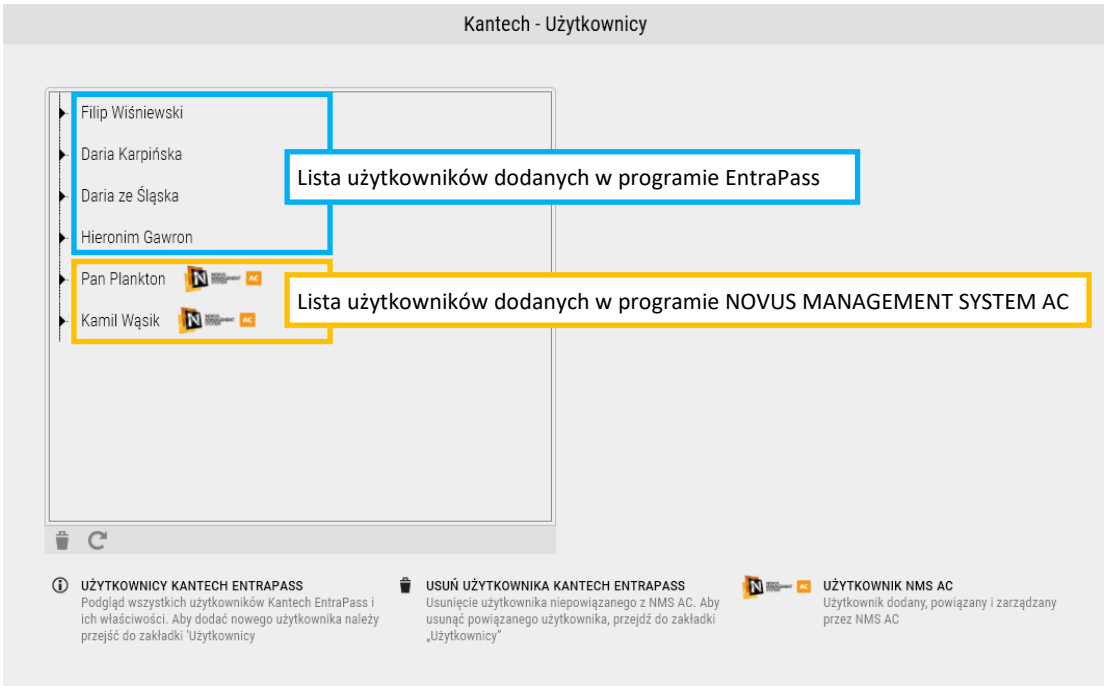
Linie dozorowe - włącz monitorowanie/wyłącz monitorowanie/powrót do harmonogramu

Wszystkie z wyświetlanych w urządzeniach elementów możemy umieszczać na panelach i sterować nimi z pozycji operatora.

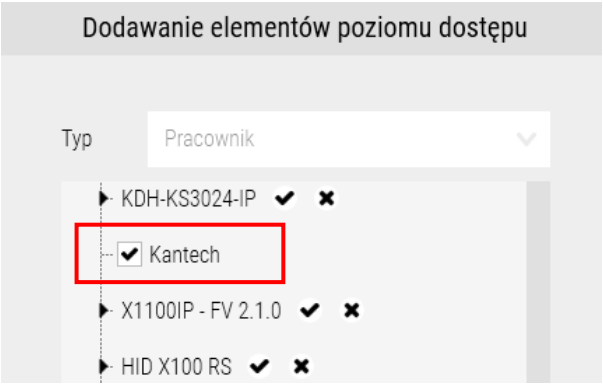


Użytkownicy - wyświetla listę użytkowników przypisanych do oprogramowania EntraPass

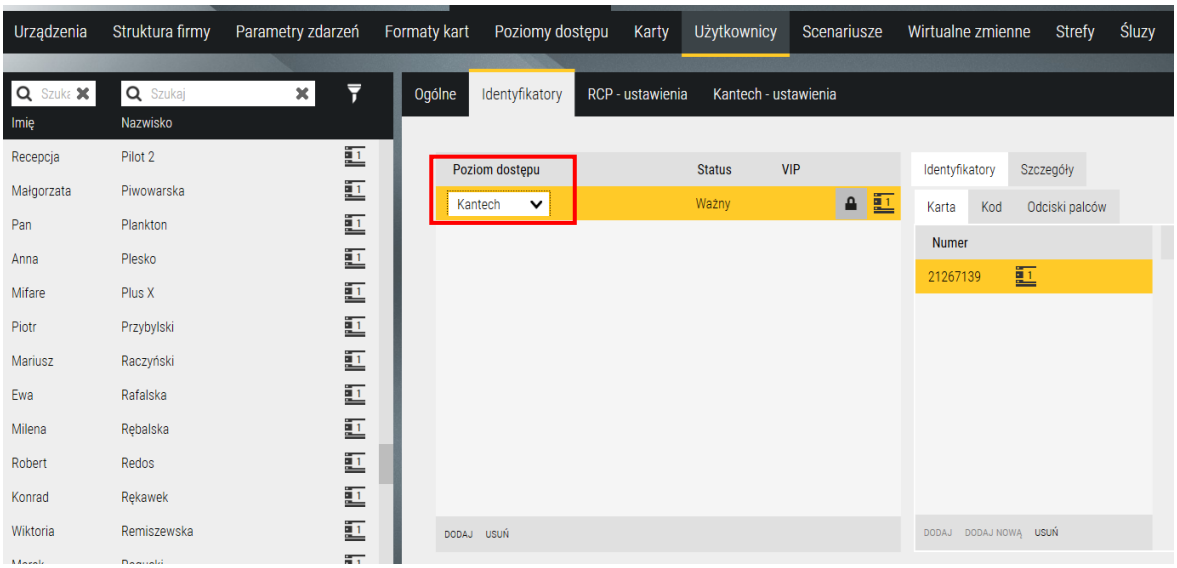




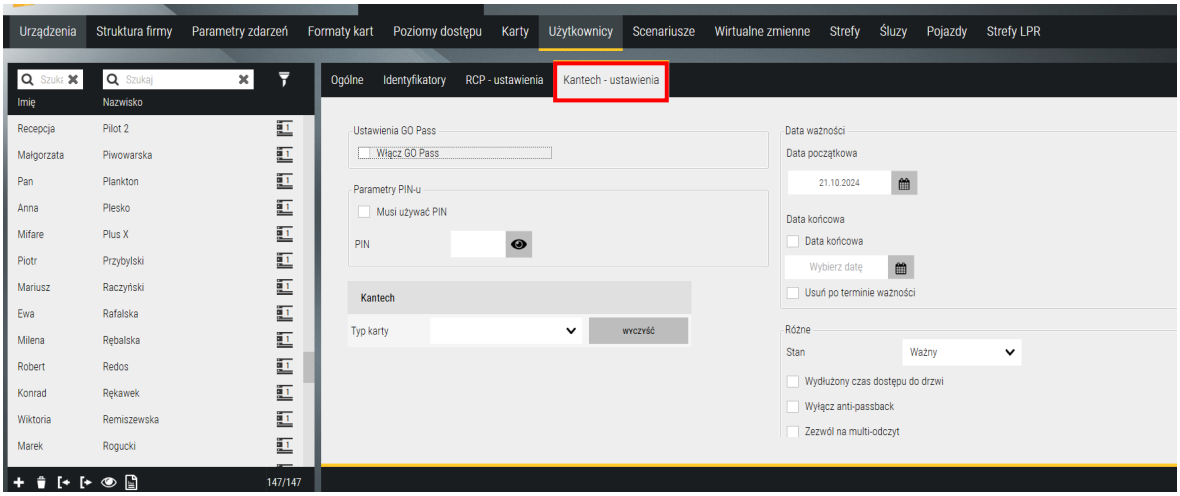
Dodawanie użytkowników - W celu dodania nowego użytkownika dla systemu Kantech EntraPass musimy najpierw stworzyć poziom dostępu dla dodanego systemu z pozycji *Konfiguracja/Poziomy Dostępu*



Następnie dodajemy użytkownika analogicznie jak w przypadku innych użytkowników systemu, poprzez zakładkę *Konfiguracja/Użytkownicy*. W pozycji *Poziom dostępu* wybieramy stworzony wcześniej poziom dla systemu Kantech.



Po zapisaniu użytkownika wraz z wybranym poziomem dostępu dla Kantech w oknie po prawej stronie pojawi się nowa zakładka: *Kantech-ustawienia*



Kantech - ustawienia - W oknie tym możemy skonfigurować parametry identyfikatora dla systemu Kantech

Ustawienie GO Pass - włączenie funkcjonalności dla aplikacji GO Pass (kart wirtualnych systemu Kantech)

Parametry PIN-u - wymuszenie używania PIN przez użytkownika, ustawienie kodu PIN

Typ karty - w tej pozycji możemy wybrać typ karty ustawiony w oprogramowaniu EntraPass, typ karty zawiera przypisany do siebie poziom dostępu do wybranych przejść dla kontrolerów Kantech. Typ karty musi być skonfigurowany od strony oprogramowania EntraPass.

Data ważności - ustawienie daty początkowej i końcowej dla identyfikatora, istnieje też możliwość usunięcia z systemu karty której termin ważności się skończył.

Stan - informacja o statusie identyfikatora *Ważny/Nieważny/Skradziona zgubiona/Po terminie ważności*

Włączenie dodatkowych funkcjonalności dla identyfikatora: Wydłużony czas na dostęp, Wyłączenie z anti-passbacku, zezwolenie na multi-odczyt

Wykaz funkcjonalności w integracji **NOVUS MANAGEMENT SYSTEM AC** z oprogramowaniem **Kantech EntraPass**

Komendy	Zdarzenia	Zarządzanie użytkownikami
Aktualizuj	Alarm	Podgląd użytkowników i kart skonfigurowanych za pomocą EntraPass
Zarygluj / odrygluj drzwi	Uszkodzenie kontrolera	
Odrygluj drzwi czasowo	Drzwi zaryglowane / odryglowane	Dodawanie i usuwanie użytkowników i kart z poziomu NMS AC
Powrót do terminarza	Drzwi przetrzymane	
Włącz / wyłącz czytnik	Drzwi w stanie normalnym	
Włącz / wyłącz przekaźnik	Drzwi sforsowane	
Włącz przekaźnik czasowo	Czytnik aktywny / nieaktywny	
Włącz / wyłącz monitorowanie linii dozorowych	Dostęp zezwolony / zabroniony	
	Monitorowanie linii dozorowej włączone / wyłączone	
	Przekaźnik włączony / wyłączony	
	Utrata komunikacji	
	Powrót komunikacji	
	Rozłączony przez operatora	

9.13 Integracja z oprogramowaniem NOVUS MANAGEMENT SYSTEM AC przy użyciu API

Konfiguracja w NOVUS MANAGEMENT SYSTEM AC

Ogólne informacje

API jest to zestaw komend HTTP/HTTPS. Założenie jest takie, że niemalże wszystko, co jest możliwe do skonfigurowania oraz niemalże wszystkie informacje, które są możliwe do pobrania z serwera NOVUS MANAGEMENT SYSTEM AC z poziomu interfejsu aplikacji klienckiej teoretycznie będzie również możliwe do skonfigurowania, pobrania z poziomu API. Zestaw komend dostępnych w API będzie rozwijany w zależności od potrzeb integracji zgłaszanych przez klientów, będzie to kwestia indywidualnego podejścia. Na chwilę obecną obsługiwany jest szereg komend związanych z systemami LPR oraz użytkownikami kontroli dostępu.

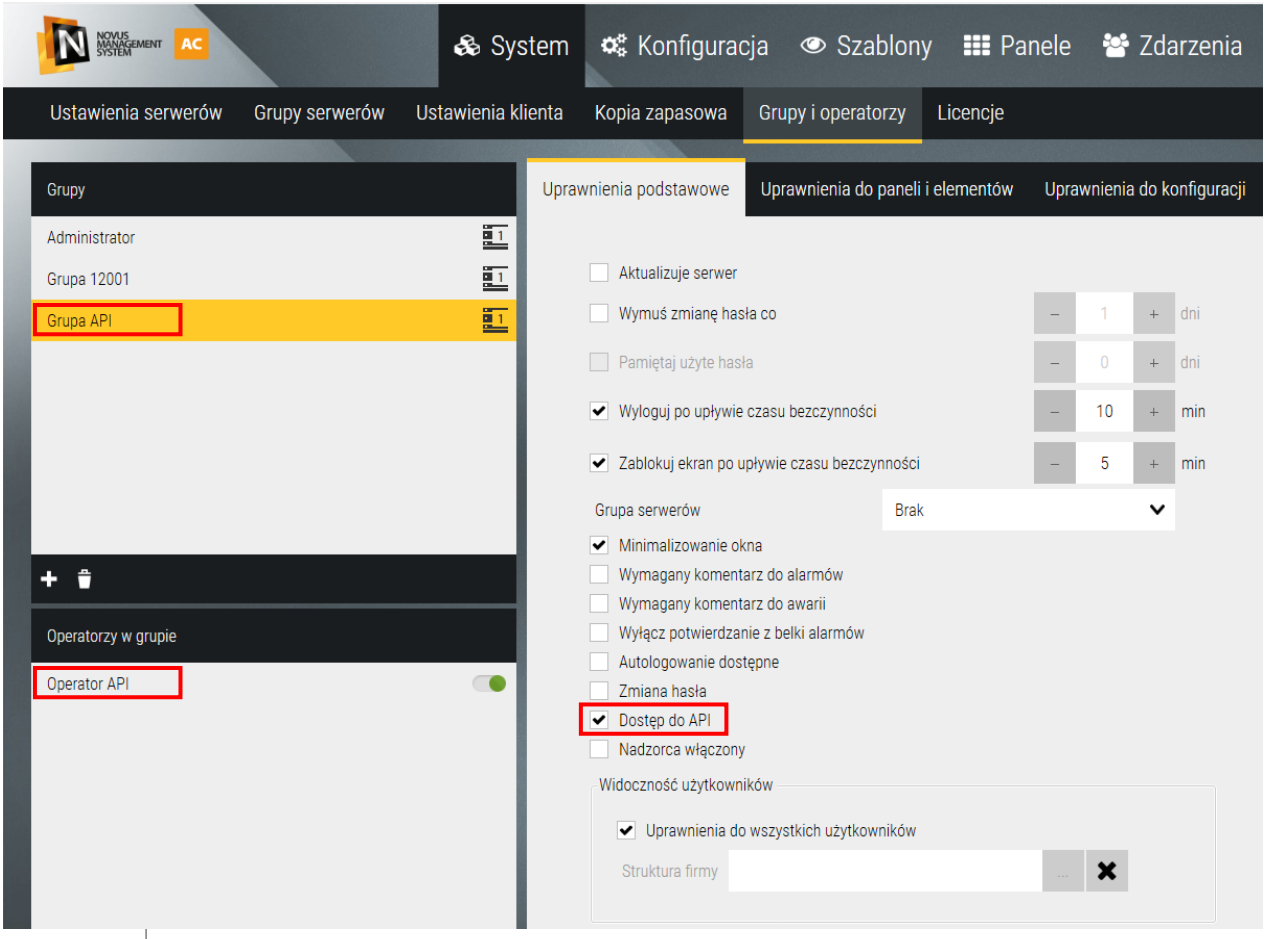
Aby korzystać z funkcjonalności API konieczne jest wykupienie dedykowanej licencji na serwer NOVUS MANAGEMENT SYSTEM AC (NOVUS MANAGEMENT SYSTEM AC API v5).

Dla przykładu chcąc stworzyć dostęp umożliwiający otwieranie drzwi należy utworzyć kartę, którą będą one otwierane, oraz użytkownika, z którym ta karta zostanie powiązana. Następnie stworzyć należy identyfikator, w którym przekazujemy Id użytkownika, id karty oraz Id poziomu dostępu określającego, gdzie użytkownik będzie miał dostęp. Tak stworzone powiązanie (identyfikator) umożliwi używanie karty i otwieranie drzwi.

Podobnie ma się sprawa dla pojazdów w przypadku otwierania wjazdu z tym, że identyfikatorem będzie nie karta a numer rejestracyjny pojazdu. W przypadku pojazdów należy również użyć odpowiedniego poziomu dostępu skonfigurowanego dla pojazdów.

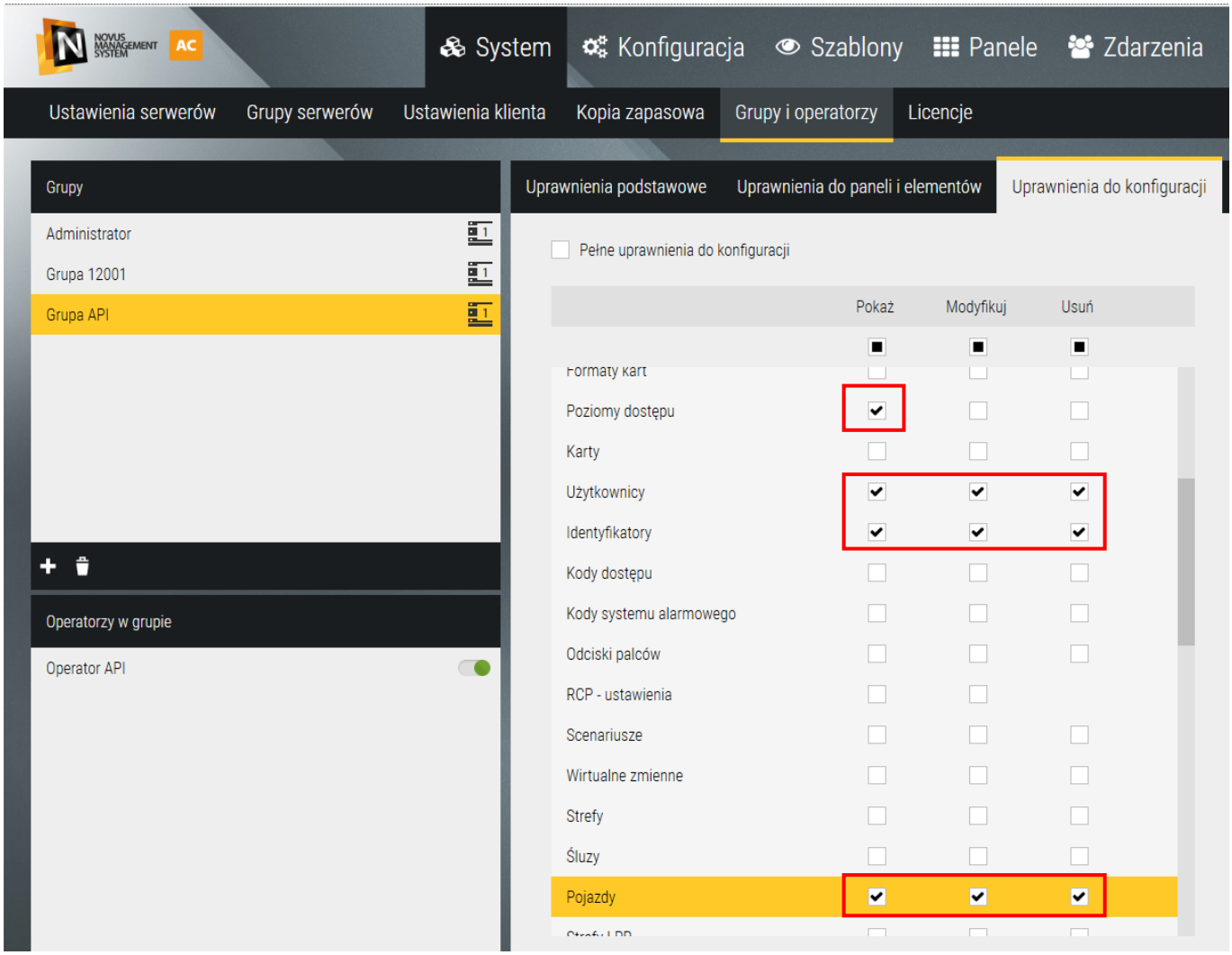
Wstępna konfiguracja

Po zalogowaniu do programu w zakładce *System/Grupy i operatorzy* należy dodać nową grupę i dać jej dostęp do API oraz stworzyć konto operatora z hasłem.

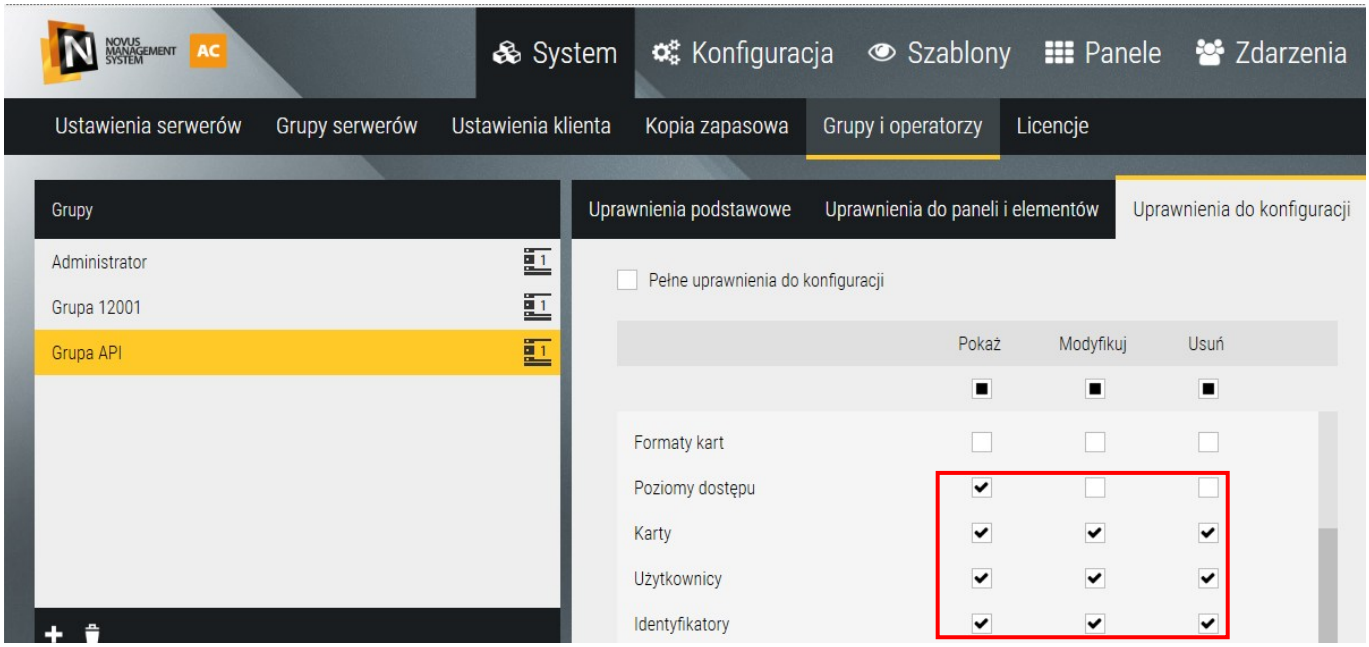


Dodatkowo należy tej grupie nadać odpowiednie uprawnienia do zasobów które będą modyfikowane.

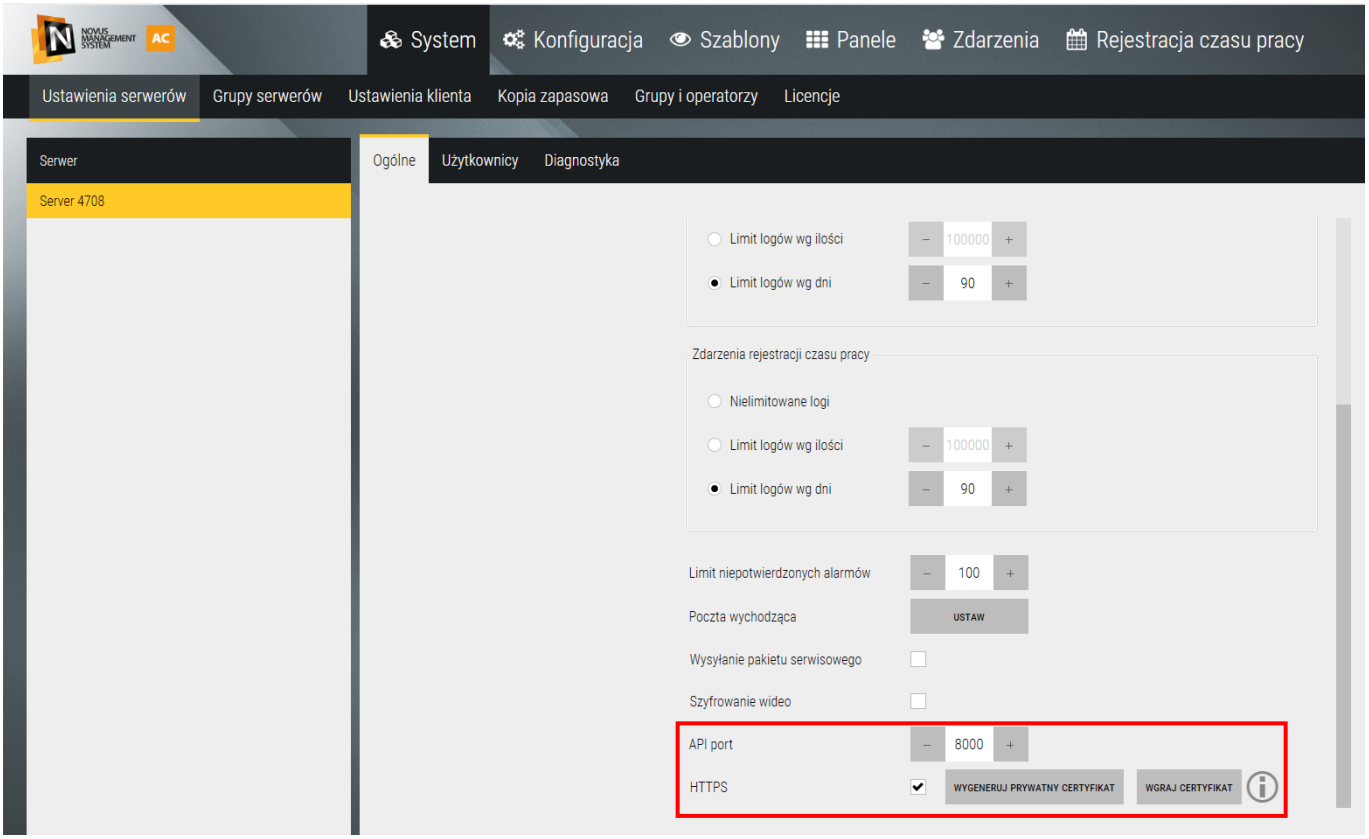
W przypadku pojazdów:



W przypadku kart:



Należy również sprawdzić port API w zakładce *System/Ustawienia serwerów* oraz ustawienia HTTP/HTTPS . Domyślnie port jest ustawiony na 8000 i zaznaczona jest opcja *HTTPS*.



Strona dokumentacji API znajduje się pod adresem:

https://localhost:8000/api/docs

Aby korzystać z API należy pobrać token GET https://localhost:8000/api/auth

Autoryzacja: Basic Auth i użyć loginu i hasła operatora który ma dostęp do API .

Token należy dołączać do każdego kolejnego zapytania. Gdy token straci ważność należy wygenerować nowy token.

W przypadku używania protokołu HTTPS i problemów z połączeniem do API z powodu certyfikatu, należy wygenerować nowy prywatny certyfikat z poziomu konfiguracji programu wprowadzając adres IP serwera NOVUS MANAGEMENT SYSTEM AC. W katalogu głównym aplikacji utworzy się plik certyfikatu, który należy dodać na komputerze klienckim do zaufanych certyfikatów.

Przykładowym programem do wysyłania zapytań HTTP/HTTPS (GET, POST) oraz do generowania i przechowywania tokenów jest aplikacja Postman.

Przykłady:

Dodanie nowego pojazdu

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

JSON BODY

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

W odpowiedzi szczegóły pojazdu z nadanym ID pojazdu

Dodanie nowej karty

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

JSON BODY

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

W odpowiedzi szczegóły utworzonej karty z nadanym ID

Dodanie nowego użytkownika

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

JSON BODY


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


W odpowiedzi szczegóły użytkownika z nadanym ID użytkownika

Wylistowanie poziomów dostępu

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

W odpowiedzi lista poziomów dostępu wraz z ich ID

Powiązanie użytkownika z elementem identyfikacyjnym i poziomem dostępu

W przypadku pojazdów w liście „vehicles” dodać Id pojazdu:

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]
}
```

Natomiast w przypadku wiązania kart w liście „cards” dodać id karty

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": []
}
```

Usuwanie dostępu

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

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

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

lub

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

Zdarzenia aplikacji

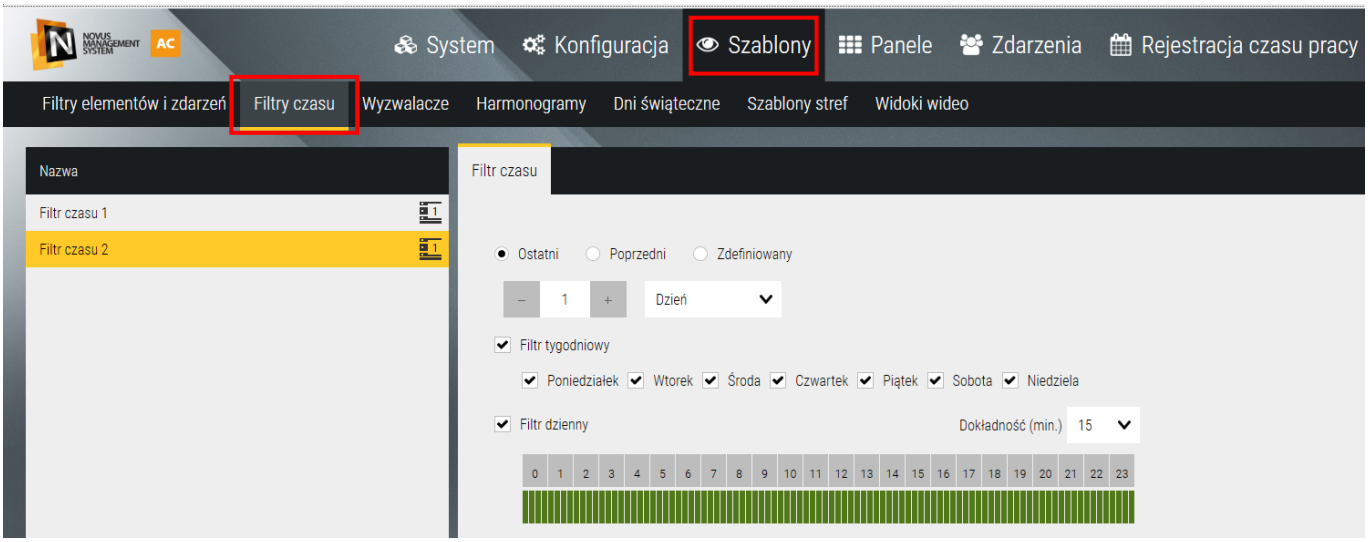
Pobranie zdarzeń

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

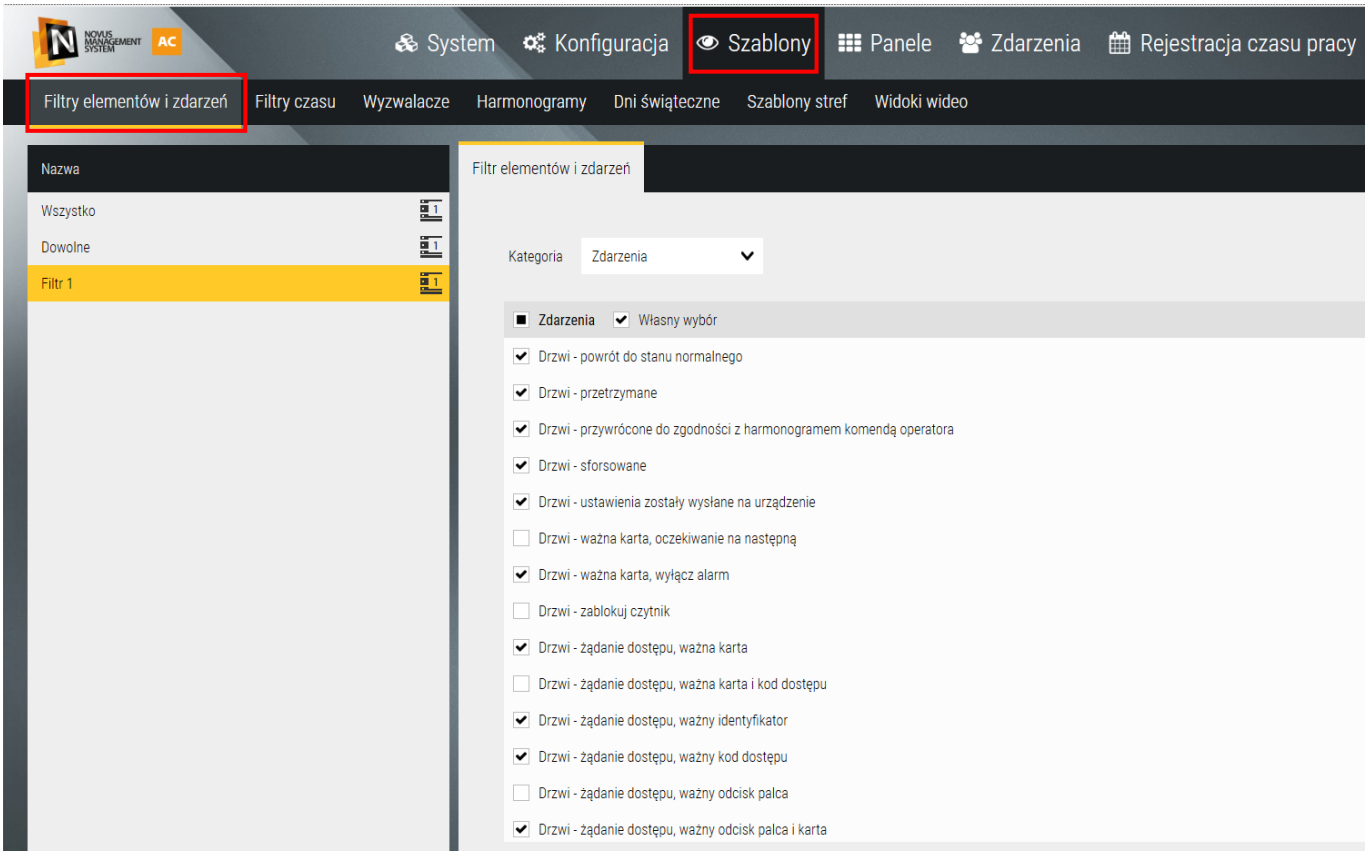
Parametry wykorzystywane do pobierania zdarzeń

- Zakres czasowy od - do
- Opcjonalnie można wykorzystać filtry czasu zdefiniowane w programie

- Opcjonalnie można wykorzystać filtry czasu zdefiniowane w programie

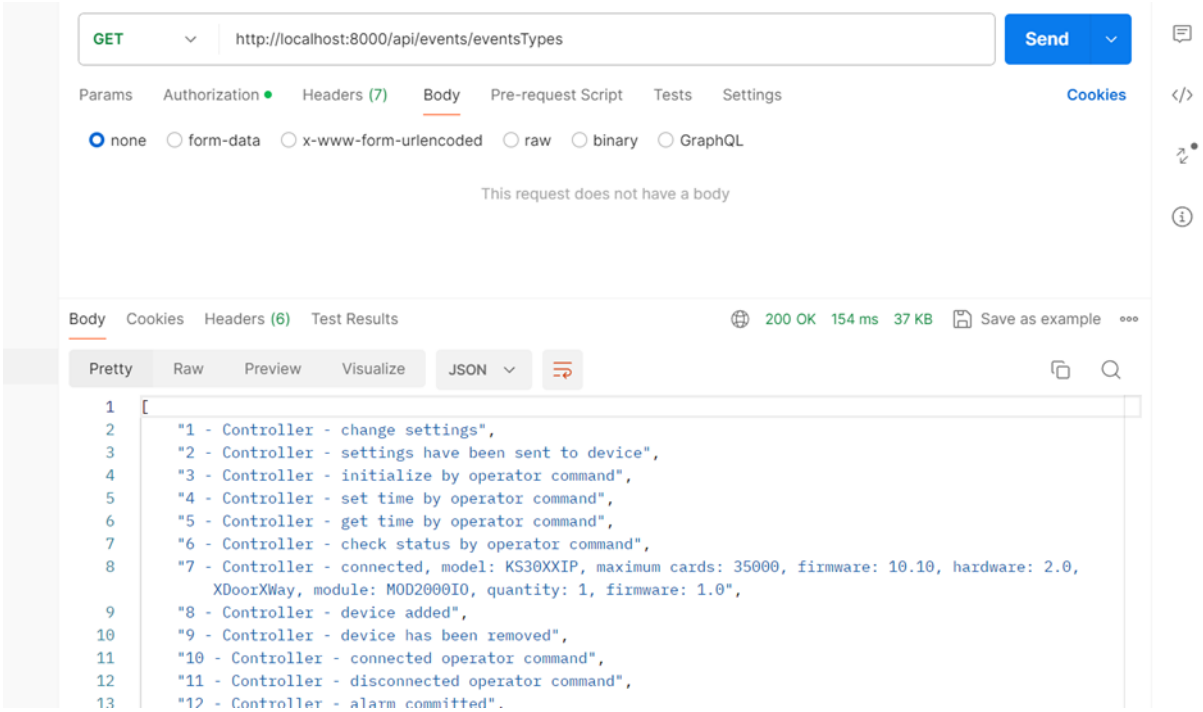


- Opcjonalnie można wykorzystać filtry elementów i zdarzeń zdefiniowane w programie



W/w elementy mogą zostać wylistowane poprzez użycie:
https://localhost:8000/api/itemsAndEventsfilters

Listę wszystkich możliwych identyfikatorów zdarzeń (EventTypeID) wraz z ich opisami (Details) można wylistować za pomocą:
https://localhost:8000/api/events/eventsTypes



Eksport nagrań za pomocą API

Alternatywną możliwością na wykonanie eksportu nagrań jest wykorzystanie zestawu komend API. Do realizacji tego procesu potrzebny jest program obsługujący zapytania HTTP, HTPPS np. Postman. Aby wykonać eksport nagrań potrzebne są:

- ID kanału wideo, z którego ma być nagranie,
- ID harmonogramu (domyślnie wartość 2 oznacza harmonogram Zawsze).

Obok zapytań zostały umieszczone przykładowe odpowiedzi z programu Postman.

Procedura pobierania nagrań przez API:

Pobranie ID kanału

GET https://localhost:8000/api/devices


```
{
    "id": 29001,
    "name": "NHDR-4116AHD",
    "type": "NVR",
    "children": [
        {
            "id": 30709,
            "name": "Channel 85",
            "type": "Channel",
            "children": [
                {
                    "id": 30629,
                    "name": "Stream 1",
                    "type": "Stream",
                    "children": [],
                    "parent": {
                        "id": 30709,
                        "name": "Channel 85",
                        "type": "Stream",
                        "children": null,
                        "parent": null
                    }
                },
                {
                    "id": 30630,
                    "name": "Stream 2",
                    "type": "Stream",
                    "children": [],
                    "parent": {
                        "id": 30709,
                        "name": "Channel 85",
                        "type": "Stream",
                        "children": null,
                        "parent": null
                    }
                }
            ],
```


Id kanału

Pobranie ID harmonogramu

GET https://localhost:8000/api/schedules


```
[
    {
        "id": 1,
        "name": "Never"
    },
    {
        "id": 2,
        "name": "Always"
    }
]
```


Stworzenie zadania eksportowego

POST https://localhost:8000/api/videoexport

JSON

Body


```
{
    "channelsId": [32452],
    "scheduleId": 2,
    "from": "2026-01-16T11:25:00Z",
    "to": "2026-01-16T11:30:00Z",
    "container": "avi",
    "isRemovalRestricted": false,
    "video": true,
    "audio": true
}
```



```
{
    "id": 761768,
    "audio": true,
    "channelsId": [
        32452
    ],
    "container": "avi",
    "created": "2026-01-16T13:27:21.5901411Z",
    "destinationPath": "C:\\WINDOWS\\system32\\config\\systemprofile\\Downloads",
    "progress": 0,
    "from": "2026-01-16T11:25:00Z",
    "operatorId": 11013,
    "isRemovalRestricted": false,
    "scheduleId": 2,
    "autoDownload": false,
    "state": "Waiting",
    "to": "2026-01-16T11:30:00Z",
    "video": true,
    "hasWatermark": false,
    "hasCameraName": false,
    "hasDeviceName": false,
    "hasTimeStamp": false
}
```


Id zadania

Opis parametrów:

channelsId - id kanału, jeden w przypadku formatów mp4 i avi oraz wiele kanałów przypadku pak

scheduleId - id harmonogramu

from, to - zakres dat w formacie ISO 8601 (UTC), np. "2025-11-19T10:35:55Z"

container - format pliku: "avi", "mp4" lub „pak”

isRemovalRestricted - określa, czy inni użytkownicy mogą usuwać to zadanie, opcja Tylko *administrator lub twórca może usunąć*

video - czy plik zawiera wideo

audio - czy plik zawiera audio

Sprawdzenie statusu zadania

GET https://localhost:8000/api/videoexport/{id zadania}


```
[
    {
        "id": 761768,
        "audio": true,
        "channelsId": [
            32452
        ],
        "container": "avi",
        "created": "2026-01-16T13:27:21.5901411Z",
        "destinationPath": "C:\\WINDOWS\\system32\\config\\systemprofile\\Downloads",
        "progress": 100,
        "from": "2026-01-16T11:25:00Z",
        "operatorId": 11013,
        "isRemovalRestricted": false,
        "scheduleId": 2,
        "autoDownload": false,
        "state": "ManualDownload",
        "to": "2026-01-16T11:30:00Z",
        "video": true,
        "hasWatermark": false,
        "hasCameraName": false,
        "hasDeviceName": false,
        "hasTimeStamp": false
    }
]
```

Sprawdzenie statusu wszystkich zadań znajdujących się na serwerze

GET https://localhost:8000/api/videoexport

UWAGA! Pole ***progress*** pokazuje poziom postępu eksportu (w %), a pole ***state*** wskazuje aktualny stan zadania. Jeśli wartość progress wynosi 100, oznacza to, że zadanie zostało ukończone i można pobrać informacje o plikach.

Dodatkowo należy pamiętać, że przy zmianie kodeka H.264 lub H.265 oprogramowanie może utworzyć więcej niż jeden plik dla jednego zadania eksportowego.

Sprawdzenie plików wygenerowanych dla konkretnego zadania eksportu

GET https://localhost:8000/api/videoexport/{id zadania}/files


```
[
    {
        "file": "C:\\Program Files (x86)\\NOVUS MANAGEMENT SYSTEM AC\\Server\\VideoExport\\61814\\NHDR-4116AHD_Channel_85_2025-11-27_09-20-00_part1.avi",
        "part": 1
    }
]
```

Pobranie pliku na dysk

GET https://localhost:8000/api/videoexport/{id zadania}/download/{id pliku}

Usunięcie zadania eksportowego z dysku

DELETE https://localhost:8000/api/videoexport/{id zadania}

ODPŁATNA UMOWA LICENCYJNA
Programu „NOVUS MANAGEMENT SYSTEM" – wersja AC

Informujemy, że instalacja oraz korzystanie z Programu „Novus Management System" – wersja AC oznacza automatycznie akceptację warunków niniejszej Umowy licencyjnej w imieniu Licencjobiorcy - Użytkownika. Producent informuje, że korzystanie z Programu może być niedostępne w niektórych krajach i językach. Jeżeli nie wyrażasz zgody na postanowienia niniejszej Umowy licencyjnej, przerwij natychmiast korzystanie z Programu, odinstaluj go oraz usuń z Twojego urządzenia.

1. DEFINICJE

1.1. „**Umowa**" – niniejsza umowa licencyjna, którą Użytkownik zawiera z Producentem, w celu uzyskania możliwości korzystania z Programu.

1.2. „**Prawa Autorskie i Prawa Pokrewne**" – każde z osobna i wszystkie razem prawa autorskie i prawa pokrewne, w tym w szczególności prawa autorskie, prawa do patentów, znaków towarowych, logo, jak również know-how oraz tajemnica handlowa, wchodzące w skład lub związane z Programem, stanowiące własność Producenta. Prawa autorskie i prawa pokrewne są chronione w szczególności przez ustawę z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. z 1994 r., nr 24, poz. 83 z późn. zm.).

1.3. „**Producent**" - AAT SYSTEMY BEZPIECZEŃSTWA SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ z siedzibą w Warszawie, ul. Puławska 431, 02-801 Warszawa, wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m. st. Warszawy, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego KRS 0000838329, NIP 9512500868, REGON 385953687, wysokość kapitału zakładowego: 17.005.000,00 zł.

1.4. „**Użytkownik**" - osoba fizyczna, prowadząca działalność gospodarczą, osoba prawna oraz jednostka organizacyjna niebędąca osobą prawną, której ustawa przyznaje zdolność prawną, która instaluje lub korzysta z Programu. Użytkownikiem nie może być osoba fizyczna, będąca konsumentem w rozumieniu ustawy Kodeks cywilny (Dz. U. z dnia 23 kwietnia 1964 r. (Dz.U. Nr 16, poz. 93 z późn.zm).

1.5. „**Program**" – oprogramowanie komputerowe, obejmujące całość zawartości plików dostarczonych drogą elektroniczną lub na nośniku, stanowiący Utwór w myśl Prawa Autorskiego i Praw Pokrewnych, opracowany przez Producenta lub do którego przysługują Producentowi autorskie prawa majątkowe, z którego może korzystać Użytkownik na zasadach określonych w Umowie.

1.6. „**Klucz licencji**" – wygenerowany przez Producenta kod numeryczny, przekazany Użytkownikowi, niezbędny do korzystania z Programu lub dodatkowych funkcjonalności lub rozszerzeń. Klucz licencji może być wykorzystany tylko raz i tylko na jednym urządzeniu.

1.7. „**Punkt licencyjny**" – punkty umożliwiające dodawanie przez Użytkownika urządzeń integrowanych do Programu.

2. POSTANOWIENIA OGÓLNE

2.1. Użytkownik może dokonywać instalacji i korzystać z Programu wyłącznie w sposób i na warunkach przewidzianych Umową, zgodnie z instrukcją obsługi Programu.

2.2. Umowa nie przenosi praw autorskich i praw pokrewnych na Użytkownika ani nie udziela Użytkownikowi tychże. Użytkownikowi przysługuje jedynie możliwość korzystania z Programu w określonym przez Umowę zakresie.

2.3. Użytkownik przyjmuje do wiadomości, że zakup Licencji wiąże się z obowiązkiem przestrzegania przez niego postanowień Umowy.

2.4. Producent niniejszym udziela Użytkownikowi licencji tylko na własny użytek, bez prawa wyłączności, bez prawa udzielenia licencji innym osobom, na terytorium wskazanym w formularzu rejestracyjnym, na pobieranie, instalację i korzystanie z Programu na komputerze stacjonarnym lub przenośnym.

2.5. Licencja zostaje udzielona Użytkownikowi odpłatnie. Opłata licencyjna została określona w dokumencie sprzedaży.

2.6. Opłaty licencyjne mogą zostać ukształtowane w różny sposób w zależności od miejsca, sposobu wykorzystywania Programu lub dodawanych funkcjonalności lub rozszerzeń. W szczególności opłata licencyjna może być opłatą jednorazową, okresową, uzależnioną od liczby Punktów licencyjnych lub dodatkowych funkcjonalności lub rozszerzeń.

3. LICENCJA I OGRANICZENIA

3.1. Producent udziela Użytkownikowi licencji uprawniającej do korzystania z Programu na polach eksploatacji wskazanych w pkt 4 poniżej.

3.2. Użytkownik ma prawo do zainstalowania i aktywacji Programu tylko raz i tylko na jednym, przeznaczonym do tego stanowisku komputerowym (w jednym komputerze) oraz do sporządzenia jednej kopii zapasowej.

3.3. Użytkownik nie może w żaden sposób użyczać, odsprzedawać, przekazywać, publikować, rozpowszechniać, czy w jakikolwiek sposób udostępniać Programu lub jego części, a także Klucza licencji osobom trzecim oraz naruszać jakichkolwiek praw odnoszących się do Programu lub jego części.

3.4. Użytkownik nie jest upoważniony i zobowiązuje się, że nie podejmie, nie spowoduje, nie wyrazi zgody ani nie upoważni żadnej osoby trzeciej do przeprowadzenia modyfikacji, edycji, tworzenia elementów pochodnych, dekompilacji, dezasemblacji lub łamania kodu Programu, jego części, a także żadnych plików i ich treści, składających się na Program lub dołączonych do Programu.

3.5. Użytkownik nie jest upoważniony do korzystania z Programu w celu tworzenia lub rozwijania produktu konkurencyjnego.

3.6. Producent zastrzega sobie wyłączne prawo do dokonywania modyfikacji, rozszerzenia, aktualizacji, tłumaczenia, a także naprawiania Programu według własnego uznania.

3.7. Producent nie jest zobowiązany do informowania Użytkownika o dokonanych modyfikacjach, dodatkowych funkcjonalnościach, rozszerzeniach, aktualizacjach, tłumaczeniach czy kolejnych wersjach Programu.

3.8. Producent nie jest zobowiązany do dostarczania Użytkownikowi kolejnych wersji Programu, jego dodatkowych funkcjonalności, rozszerzeń, aktualizacji, tłumaczeń i w każdym czasie może z tego zrezygnować.

3.9. Dostarczanie nowszych wersji Programu może odbywać się przez wywołanie opcji aktualizacji bezpośrednio z Programu, pod warunkiem podłączenia komputera do Internetu. Użytkownik może także pobierać i instalować udostępnione przez Producenta na jego stronie internetowej modyfikacje, dodatkowe funkcjonalności, rozszerzenia lub aktualizacje Programu na warunkach wskazanych w tych aktualizacjach.

3.10. Producent nie jest zobowiązany do świadczenia jakichkolwiek usług związanych z Programem, w szczególności pomocy technicznej, czy wsparcia.

4. POLA EKSPLOATACJI

4.1. Producent udziela Użytkownikowi licencji wyłącznie na następujących polach eksploatacji:

1) wprowadzanie Programu lub jego części do pamięci komputera lub innego urządzenia przeznaczonego do korzystania z Programu, w tym pobranie Programu ze strony internetowej Producenta lub innego nośnika oraz jego instalacja;
2) sporządzenie jednej kopii zapasowej, jeżeli jest to niezbędne do korzystania z Programu;
3) korzystanie z Programu na zasadach wskazanych w Umowie, w tym jego rejestracja, integracja z urządzeniami oraz korzystanie z dodatkowych funkcjonalności lub rozszerzeń Programu.

5. REJESTRACJA PROGRAMU

5.1. Producent udostępnia Użytkownikowi nieodpłatnie wersję testową Programu („**Trial**") na czas określony 60 dni, możliwą do aktywacji po zarejestrowaniu Programu. W trakcie tego okresu, Użytkownik powinien nabyć Klucz licencji oraz aktywować Program. W przypadku braku zakupu licencji, rejestracji Programu i jego aktywacji, licencja automatycznie wygasa, a Użytkownik traci prawo do korzystania z Programu.

5.2. Rejestracja Programu następuje bezpośrednio z poziomu Programu lub poprzez stronę internetową Producenta. Następnie Użytkownik powinien aktywować Program.

5.3. Rejestracja Programu polega na podaniu danych dotyczących Użytkownika, tj. danych instalatora oraz danych użytkownika licencji.

5.4. Rejestracja Programu wymaga dostępu do sieci Internet.

5.5. Aktywacja Programu polega na wpisaniu Klucza licencji.

5.6. Użytkownik może dodać do Programu funkcjonalności lub rozszerzenia dostępne w ofercie Producenta („**Funkcjonalności**"). Aktywacja Funkcjonalności polega na uiszczeniu dodatkowej opłaty licencyjnej (zakupie odpowiedniego Klucza licencji) oraz jego wpisaniu we właściwym miejscu w Programie.
5.7. Producent może zażądać dostępu do lokalizacji Programu, a także przeprowadzić kontrolę jego wykorzystywania.

6. OBOWIĄZYWANIE UMOWY

6.1. Umowa zostaje zawarta poprzez akceptację jej warunków przez Użytkownika w momencie wybrania przez Użytkownika przycisku „akceptuję" podczas instalacji Programu lub jego aktualizacji. W każdym przypadku przyjmuje się, że rozpoczęcie korzystania z Programu stanowi akceptację niniejszej Umowy.
6.2. W przypadku aktywacji wersji Trial, Umowa zostaje zawarta na czas określony 60 dni. Umowa ulega przekształceniu w Umowę na czas nieokreślony, pod warunkiem zakupu Klucza licencji oraz rejestracji i aktywacji Programu.
6.3. Umowa zostaje zawarta na czas nieokreślony pod warunkiem zakupu przez Użytkownika Klucza licencji, rejestracji i aktywacji Programu.
6.4. Umowa może zostać wypowiedziana przez każdą ze Stron z zachowaniem miesięcznego terminu wypowiedzenia, z tym że Użytkownik może wypowiedzieć Umowę bez zachowania miesięcznego terminu wypowiedzenia – przez usunięcie Programu i jego kopii zapasowej.
6.5. Producent może rozwiązać Umowę bez wypowiedzenia w razie naruszenia przez Użytkownika postanowień Umowy.
6.6. Producent może rozwiązać Umowę w trybie natychmiastowym, bez wypowiedzenia, w przypadku nieuiszczenia przez Użytkownika opłaty licencyjnej w całości (w przypadku opłaty jednorazowej) lub jej kolejnej części (w przypadku opłat dodatkowych, okresowych lub rozłożonych na raty) zgodnie z terminem wskazanym w dokumencie sprzedaży. W takiej sytuacji Producent jest uprawniony do wyłączenia i zablokowania Użytkownikowi możliwości korzystania z Programu lub jego danej Funkcjonalności.
6.7. Z chwilą rozwiązania Umowy, wygasają wszelkie prawa Użytkownika do Programu przekazane Umową. Użytkownik zobowiązany jest wówczas do zaprzestania korzystania z Programu oraz usunięcia Programu i jego kopii zapasowej z wszelkich nośników lub urządzeń.
6.8. Producent nie ponosi odpowiedzialności za jakiekolwiek szkody poniesione w związku z rozwiązaniem Umowy.

7. GWARANCJE ORAZ ODPOWIEDZIALNOŚĆ PRODUCENTA

7.1. Producent gwarantuje, że posiada zdolność do zawarcia oraz wykonywania Umowy.
7.2. Użytkownik gwarantuje, że posiada zdolność do zawarcia oraz wykonywania Umowy.
7.3. Producent dostarcza Program w stanie takim, w jakim się znajduje, bez żadnych gwarancji i nie ponosi odpowiedzialności za braki funkcjonalne Programu lub skutki korzystania z Programu, w szczególności w przypadkach wystąpienia nieprawidłowej pracy systemu komputerowego spowodowanej wadami sprzętu, niewłaściwą instalacją lub konfiguracją oprogramowania i sprzętu oraz w wypadkach wystąpienia nieprawidłowej obsługi Programu.
7.4. Rękojmia za wady, określona w przepisach Kodeksu cywilnego, zostaje wyłączona.
7.5. Producent nie ponosi odpowiedzialności z tytułu gwarancji w odniesieniu do Programu.
7.6. Producent nie ponosi odpowiedzialności za sposób korzystania z Programu przez Użytkownika, a w szczególności za korzystanie z Programu niezgodnie z Umową lub instrukcją obsługi, oraz za związane z tym szkody.
7.7. Producent nie ponosi odpowiedzialności za naruszenie Praw Autorskich i Praw Pokrewnych, a także za roszczenia osób trzecich, będące wynikiem korzystania przez Użytkownika z Programu w sposób sprzeczny z Umową.
7.8. W razie gdyby wyłączenie odpowiedzialności wskazanej w niniejszym pkt 7 nie było możliwe, zostaje ona wyłączona w maksymalnym możliwym zakresie. W szczególności odpowiedzialność Producenta za szkody, które mogłyby być wyrządzone umyślnie zostaje ograniczona do wysokości 500 euro i nie obejmuje prawa do domagania się zwrotu utraconych korzyści, czy odpowiedzialności za szkody pośrednie.

7.9. Powyższe postanowienia dotyczą także wszelkich Funkcjonalności Programu.

8. RYZYKO UŻYTKOWNIKA

8.1. Użytkownik przyjmuje do wiadomości i zgadza się, że całkowite ryzyko wynikające z korzystania z Programu w sposób określony Umową i instrukcją obsługi, dołączoną do Programu spoczywa na Użytkowniku w najszerszym zakresie dozwolonym przez przepisy prawa. Ponadto, w razie zaistnienia okoliczności, uniemożliwiających funkcjonowanie Programu – o ile bezpośrednią przyczyną tych okoliczności są przyczyny tkwiące w Programie – Użytkownik powinien niezwłocznie poinformować o tym Producenta pod rygorem wyłączenia wszelkiej odpowiedzialności Producenta mogącej wyniknąć z tego tytułu.

8.2. Użytkownik przyjmuje do wiadomości, że całkowite ryzyko wynikające z instalacji i aktywacji Programu na danym urządzeniu, a także integracji Programu z innymi programami lub urządzeniami, korzystanie z nich i ich instalacja spoczywa na Użytkowniku w najszerszym zakresie dozwolonym przez przepisy prawa. Niniejsza Umowa nie określa warunków korzystania z takich programów, czy urządzeń, a ich wykorzystywanie powinno odbywać się zgodnie z odpowiednimi warunkami licencji.

8.3. Użytkownik przyjmuje do wiadomości, że korzystanie z systemu operacyjnego, na którym uruchomiony jest Program, powinno się odbywać zgodnie z warunkami licencji tego systemu.

8.4. Użytkownik rozumie, że Program może nie realizować wszystkich jego indywidualnych wymagań, a Producent nie jest zobowiązany do oceny przydatności Programu do oczekiwań Użytkownika. Użytkownik przyjmuje całkowite ryzyko związane z odpowiednim doborem urządzeń oraz z właściwym zaprojektowaniem Programu do swoich potrzeb.

8.5. Użytkownik przyjmuje do wiadomości, że całkowite ryzyko wynikające z integracji Programu z Funkcjonalnościami, korzystanie z nich i ich aktywacja spoczywa na Użytkowniku w najszerszym zakresie dozwolonym przez przepisy prawa.

9. ZNAKI TOWAROWE/LOGO

9.1. Producent jest wyłącznie uprawniony do znaku towarowego NOVUS MANAGEMENT SYSTEM – prawnie chroniony krajowy znak towarowy wpisany do prowadzonego przez Urząd Patentowy RP Rejestru Znaków Towarowych pod numerem 213634, oraz widniejący pod numerem 1008732 World Intellectual Property Organization (WIPO) międzynarodowy znak towarowy, przeznaczony do oznaczania produktów w klasie 9 międzynarodowej nicejskiej klasyfikacji towarów i usług.

9.2. Wyżej wymieniony znak towarowy, a także nazwa Programu oraz logo są prawnie chronione i nie mogą być używane przez osoby trzecie bez zgody Producenta.

9.3. Nie można zmieniać wyżej wymienionego znaku towarowego lub logo, w szczególności nie można zmieniać ich rozmiaru, proporcji, kolorów ani w inny sposób modyfikować ich wyglądu.

9.4. Nie można umieszczać wyżej wymienionego znaku towarowego w publikacjach, witrynach internetowych oraz innych materiałach, których zawartość może dyskredytować Producenta lub Program, narusza własność intelektualną lub inne prawa bądź jest sprzeczna z prawem danego kraju lub prawem międzynarodowym.

10. SIŁA WYŻSZA

10.1. Strony nie ponoszą odpowiedzialności z tytułu niewykonania bądź nienależytego wykonania obowiązków wynikających z Umowy wyłącznie w sytuacji, gdy niewykonanie bądź nienależyte wykonanie zobowiązania jest następstwem siły wyższej.

10.2. Przez siłę wyższą Strony rozumieć będą zdarzenie, którego nie można przewidzieć przy zachowaniu należytej staranności, które jest zewnętrzne zarówno w stosunku do Producenta, jak i Użytkownika oraz od nich niezależne, któremu Strony nie mogły się przeciwstawić działając z należytą starannością. W szczególności za siłę wyższą uznaje się trzęsienia ziemi, powodzie, pożary, huragany, klęski żywiołowe, epidemie, inne zdarzenia spowodowane siłami przyrody, strajki, działania wojskowe, ograniczenia eksportowe i importowe.

10.3. Jeśli zdarzenia, o których mowa w pkt 10.2 mają charakter przejściowy, Strony zobowiązują się wykonać postanowienia Umowy, przy czym czas przewidziany na wypełnienie obowiązków wynikających z Umowy ulegnie przedłużeniu o czas trwania okoliczności powodujących opóźnienie.

11. ROZSTRZYGANIE EWENTUALNYCH SPORÓW

11.1. Wszelkie spory mogące powstać na tle wykonywania Umowy, Strony zobowiązują się rozstrzygać polubownie.

11.2. W przypadku niemożności ugodowego zakończenia sporu, wynikającego z Umowy, Strony przyjmują polskie prawo jako właściwe dla rozstrzygnięcia sporu, który poddadzą pod rozstrzygnięcie sądu właściwego dla siedziby Producenta.

11.3. Naruszenie Praw Autorskich i Praw Pokrewnych Producenta może pociągnąć odpowiedzialność cywilną oraz karną podmiotu naruszającego te prawa.

12. POSTANOWIENIA KOŃCOWE

12.1. Niniejsza Umowa nie przenosi na Użytkownika autorskich praw majątkowych w całości lub w części do Programu lub jego Funkcjonalności, a jedynie udziela prawa do korzystania z Programu, w tym jego Funkcjonalności, na warunkach w niej wskazanych.

12.2. Użytkownik wyraża zgodę na udostępnienie Producentowi w formularzu rejestracji Programu swoich danych osobowych i ich przetwarzanie przez Producenta. Klauzula informacyjna dołączona jest do formularza rejestracji Programu.

12.3. Producent może dokonać cesji praw do Programu, jego części, na osoby trzecie według swego wyboru, bez konieczności powiadamiania Użytkownika.

12.4. Użytkownik bez zgody Producenta nie może dokonać cesji praw uzyskanych na podstawie Umowy na osoby trzecie.

12.5. Użytkownik oświadcza, że zapoznał się z treścią Umowy przed rozpoczęciem korzystania z Programu i nie wnosi co do niej żadnych zastrzeżeń.

12.6. Jeżeli którekolwiek postanowienie Umowy okaże się niezgodne z prawem, albo prowadzi do obejścia prawa, będzie ono uważane za nieważne. Pozostałe postanowienia Umowy pozostają w mocy, chyba że z okoliczności wynika, iż nie zostałaby ona bez nich zawarta. Strony zobowiązują się, że w takiej sytuacji przystąpią do negocjacji w celu zastąpienia nieważnych postanowień, postanowieniami, które będą realizowały możliwie przybliżony cel gospodarczy.

12.7. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności. Strony oświadczają, iż zapoznały się z treścią Umowy, rozumieją ją i zdają sobie sprawę z zakresu przysługujących im praw i obowiązków.

12.8. W przypadku powstania innych wersji językowych niniejszej Umowy licencyjnej i wystąpienia w nich rozbieżności językowych, pierwszeństwo ma polska wersja językowa.

Lista zmian w oprogramowaniu

Wersja 6.05.044

Data: 07.04.2026

Kontrola dostępu HID® Aero ®

- Dodano obsługę wind przy użyciu kontrolerów HID® Aero®. Funkcja realizowana przy użyciu inteligentnych kontrolerów IP HID® Aero® X1100 oraz modułów rozszerzeń wyjść HID® Aero® X300 w przypadku systemu bez potwierdzeń wyboru piętra oraz dodatkowo z wykorzystaniem modułów rozszerzeń wejść HID® Aero® X200 w przypadku systemu z potwierdzeniem wyboru piętra.
- Maksymalna ilość pięter 128.

Kontrola dostępu - ogólne

- Dodano możliwość generowania kodu QR dla użytkowników typu Gość dla poziomów dostępu typu Użytkownik wraz z opcją jego wysyłania bezpośrednio na e-mail do wybranego użytkownika. Dzięki temu można skonfigurować system tak, aby używać kodu QR jako identyfikatora w systemie kontroli dostępu.
- Dodano nowe narzędzie Szczegóły wirtualnej strefy, umożliwiające wyświetlanie szczegółowych informacji dotyczących wybranych stref oraz zarządzanie tym, które informacje mają być wyświetlane: Pokaż limit, Pokaż czas wejścia oraz Pokaż czas w strefie.

Głośniki IP

- Dodano obsługę głośników IP marki NOVUS (obecnie NV-IPS8030/M). Dostępne funkcjonalności to dwukierunkowa komunikacja audio wraz z możliwością obsługi wielu głośników jednocześnie, odtwarzanie komunikatów głosowych poprzez scenariusze.

Ogólne

- Ulepszono poruszanie się pomiędzy oknami, zakładkami oraz elementami oprogramowania NOVUS MANAGEMENT SYSTEM AC przy użyciu skrótów, kombinacji klawiaturowych oraz strzałek.
- Dodano informację o liczbie punktów licencyjnych pobieranych przez urządzenie w zakładce Konfiguracja/ Urządzenia/Informacje.
- Dodano możliwość wyłączania wyświetlania zdarzeń na liście „ostatnich 50 zdarzeń” poprzez nowy checkbox w konfiguracji parametrów i zdarzeń.
- Dodano opcję zaznaczania i odznaczania wykonywania wszystkich scenariuszy.
- Ulepszono prezentację konfiguracji paneli w menu Panele (dodano informację do którego monitora przypisany jest dany panel).
- Ograniczono widoczność operatorów w grupie dla innych operatorów należących do tej samej grupy.
- Dodano konfigurację dostępu do opcji Blokowanie ekranu, Zamknięcie okna, Zmiana okna, Minimalizowanie okna w zakładce Grupy i operatorzy/Uprawnienia podstawowe.
- Dodano możliwość definiowania, które grupy operatorów może edytować dana grupa operatorów (zmiana hasła, dodawanie operatorów, usuwanie operatorów itd.).

- Dla narzędzia Ostrzeżenia dodano funkcję Nie powtarzaj, która powoduje, że na liście bieżących ostrzeżeń nie będę wyświetlane powtarzające się zdarzenia. Funkcja przydatna w przypadku, gdy na obiekcie występują już znane i powtarzające się awarie/alarmy tych samych elementów utrudniając możliwość reagowania na faktycznie istotne awarie/alarmy.
- Dodano możliwość stworzenia anonimowej kopii diagnostycznej.
- Dodano funkcję potwierdzania logowania przez innego operatora.
- Dodano opcję Zmień operatora na górnym pasku aplikacji obok opcji Wyloguj.
- Dodano możliwość wyłączenia tła podczas modyfikacji ikon na panelach. Pozwala to na lepsze wykorzystanie miejsca dostępnego dla ikony.

Telewizja dozorowa

- Dodano możliwość wielokrotnego pobierania na stacje operatorskie nagrań wyeksportowanych z rejestratorów na serwer.
- Dodano możliwość definiowania czy przy tworzeniu zadań eksportu opcja Pobierz automatycznie po wyeksportowaniu w ustawieniach Zdarzenia/Eksport wideo ma być domyślnie zaznaczona czy nie.
- Dodano możliwość wyboru poszczególnych kanałów, dla których generowany jest raport o nazwie Raport z nagrań.
- Dodano możliwość eksportu plików wideo poprzez API, w tym tworzenie zadań eksportu nagrań, ich wyszukiwania, usuwania oraz pobierania wygenerowanych plików.
- Dodano możliwość eksportu nagrań z wielu kanałów do jednego pliku w formacie .pak oraz weryfikacji integralności zapisanych nagrań.
- Dodano możliwość blokowania usuwania zadań eksportu przez innych operatorów niż ten który zadania eksportu stworzył.
- Dodano mechanizm umożliwiający kontynuację pobierania nagrań w przypadku wystąpienia przerwy w połączeniu sieciowym.
- Dodano nowe dane w raportach generowanych przy użyciu funkcji Raport z nagrań: Brama domyślna oraz Maska podsieci.

Rozpoznawanie tablic rejestracyjnych

- Dodano funkcję awizacji gościa w strefie LPR, co pozwala na wjazd gościa w określonym przedziale czasowym do strefy bez konieczności generowania biletu QR.
- Kontrola dostępu - Kantech
- Dodano możliwość filtrowania użytkowników po stanie karty systemu Kantech.
- Zmodyfikowano sposób wyświetlania informacji o statusie identyfikatora w przypadku poziomów dostępu zawierających różne systemu kontroli dostępu.
- Dodano wyświetlanie ostatnio ustawionej grupy dostępu dla kontrolerów Kantech.
- Dodano możliwość pobierania informacji z pól informacyjnych kart systemu Kantech.

Rejestracja czasu pracy

- Dodano harmonogram nienormowany w rejestracji czasu pracy, który umożliwia elastyczne definiowanie czasu pracy bez sztywno określonych przedziałów godzinowych. Dla obiektów takich jak np. szpitale, gdy pracownik przychodzi do pracy np. w poniedziałek i wychodzi w środę.

Poprawki i usprawnienia:

Ogólne

- Poprawiono sposób przesuwania urządzeń na liście urządzeń w zakładce Konfiguracja/Urządzenia.
- Poprawiono działanie paneli podczas zmiany ikony na inny typ.
- Poprawiono działanie konfiguracji paneli (lista urządzeń nie zwija się po zapisaniu) oraz listy elementów struktury w zakładce Struktura firmy.
- Wzmocniono bezpieczeństwo danych w logach systemowych.
- Zwiększono prędkość pobierania plików z serwera na stacje klienckie (dotyczy np. kopii zapasowych konfiguracji, eksportu nagrań wideo itd.)
- Rozwiązano problem powodujący wyświetlanie wszystkich zdarzeń podczas tworzenia filtrów elementów i zdarzeń. Od teraz lista prezentuje wyłącznie zdarzenia przypisane do wybranych elementów.

Telewizja dozorowa

- Zmodyfikowano listę urządzeń w oknie tworzenia zadań eksportu (dodano możliwość wyszukiwania oraz opcje zwiń wszystko/rozwiń wszystko).
- Zmodyfikowano działanie ikony odtwarzania, umożliwiając wybór domyślnego czasu odtwarzania (od 1 sekundy do 5 minut wstecz).
- Usprawniono proces eksportu nagrań plików wideo oraz dodawania kanałów, nawet w przypadku niepełnego załadowania danych, w grafie odtwarzania (istotne dla systemów z ograniczonymi łączami sieciowymi).

Kontrola dostępu - ogólne

- Zoptymalizowano domyślne zdarzenia kontroli dostępu - wszystkie elementy zapisują te same zdarzenia, a na panelu wyświetlane jest tylko potwierdzenie alarmu.
- Poprawiono dodawanie kart do użytkowników z zakładki Karty.
- Usprawniono edycję scenariuszy, śluz oraz formatów kart - po zapisaniu system nie wraca już do pierwszego scenariusza, lecz pozostaje na tym, który był edytowany.
- Poprawiono zarządzanie komendami dla pięter.

Kontrola dostępu HID® Aero®

- Usprawniono działanie komend operatora, multi-odczytu HID® oraz czytników HID® - dodano potwierdzenie wykonania multi-odczytu na OSDP, a stan ikony czytnika HID® wygasa teraz automatycznie zgodnie z czasem dostępu do pięter.
- Usprawniono obsługę poziomów dostępu - dodawanie poziomów z windą HID® do innych poziomów, wyświetlanie kolejności kontrolerów oraz działanie harmonogramów dla wind.
- Usprawniono działanie edycji poziomów dostępu użytkowników.
- Usprawniono działanie drzewa urządzeń. W nowej wersji drzewo nie zwija się po zapisie dokonanych zmian.

Kontrola dostępu - KaDe

- Poprawiono działanie identyfikacji karty i pinu dla kontrolerów KDH-KS3012-IP-II oraz KDH-KS3024-IP-II.
- Usprawniono weryfikację urządzeń KS3000 oraz automatyczne uzupełnianie danych sieciowych. Dodatkowo zmieniono nazwy trybów identyfikacji z Tryb identyfikacji w czasie aktywnym na Tryb identyfikacji w czasie harmonogramu dostępu czy Tryb identyfikacji poza czasem aktywnym na Tryb identyfikacji poza czasem harmonogramu dostępu.

Wersja 6.04.030

Data: 17.10.2025

- Dodano nowe dane w raportach generowanych przy użyciu funkcji Raport z nagrań: numer portu, adres MAC, stan komunikacji, status ustawień DST i NTP oraz nazwę modelu urządzenia
- Dodano możliwość podglądu adresu IP urządzenia po najechaniu kursorem na jego nazwę na narzędziu Drzewo urządzeń
- Poprawiono mechanizm usuwania urządzeń oraz zapisu wprowadzonych zmian
- Poprawiono import dużej liczby urządzeń z plików .xml generowanych z oprogramowania NOVUS MANAGEMENT SYSTEM VSS
- Poprawiono działanie systemu podczas jednoczesnego logowania wielu operatorów do jednego serwera
- Poprawiono działanie systemu w przypadku cyklicznego przełączania paneli
- Poprawiono działanie funkcji Rozłącz przez operatora dla rejestratorów serii 4000
- Poprawiono wyświetlanie nazw modeli rejestratorów w zakładce Szczegóły
- Poprawiono działanie funkcji Raport z nagrań w przypadku zmian ustawień dotyczących nadpisywania nagrań w rejestratorach serii 4000
- Zmodyfikowano sposób naliczania punktów licencyjnych dla rejestratorów 128-kanałowych

Wersja 6.04.021

Data: 08.09.2025

- Dodano opcję filtrowania zdarzeń po zawartości pola opis w wyszukiwarce zdarzeń
- Dodano nowy firmware dla urządzeń KDH-KS3000-IP-ELVS3024-IP
- Dodano zdarzenie informujące o nieprawidłowym trybie identyfikacji dla kontrolerów KS/KZ 3000.
- Dodano możliwość zakańczania alarmów z belki alarmów
- Dodano informację o postępie aktualizacji systemu Kantech
- Rozwiązano problem z potwierdzaniem alarmu jako alarm lub awarię
- Poprawiono działanie śluz na urządzeniach HID® Aero® oraz kontrolerach KaDe serii 3000
- Poprawiono mechanizm wyświetlania zdarzeń przy użyciu filtru „Urządzenie”
- Poprawiono problem występujący przy aktualizacji firmware'u na urządzeniach HID® Aero®
- Naprawiono problem z obsługą kart usuniętych z zakładki Użytkownicy – po usunięciu, karta nie traci już funkcjonalności, a kod PIN działa poprawnie na kontrolerach HID® Aero®
- Rozwiązano problem z długim uruchamianiem serwera po imporcie użytkowników z systemu Kantech
- Rozwiązano problem z zmianą ustawień centrali alarmowej Satel
- Rozwiązano problem z konfiguracją dla użytkowników systemu Kantech
- Rozwiązano problem z trybem odtwarzania
- Rozwiązano problem z przechodzeniem pomiędzy zakładkami przy dużej bazie danych oraz dużej ilości urządzeń
- Rozwiązano problem z działaniem systemu przy wykorzystaniu wolniejszych połączeń sieciowych

Wersja 6.03.032

Data: 9.05.2025

- Poprawiono działanie mechanizmu usuwającego karty dostępu w urządzeniach HID® Aero® oraz kontrolerach KaDe serii 3000
- Poprawiono problemy przydzielania poziomów dostępu dla użytkowników i przesyłania ich na urządzenia HID® Aero® oraz kontrolery KaDe serii 3000
- Poprawiono działanie systemu w przypadku obsługi dużej ilości rejestratorów NOVUS serii 4000
- Przyspieszono responsywność systemu w przypadku obsługi dużej ilości urządzeń oraz bardzo rozbudowanej konfiguracji
- Poprawiono funkcjonalności RCP – tryb pracy nocnej, działanie listy obecności, poprawne liczenie czasu pracy oraz poprawne generowanie e-mail z podsumowania dnia pracy, wprowadzanie odpracowań
- Dodano narzędzie Drzewo urządzeń – narzędzie umieszczane jest na panelu i wyświetla listę wszystkich urządzeń telewizji dozorowej dodanych do systemu. Umożliwia tworzenie z poziomu panelu nowych widoków wideo poprzez przeciąganie kanałów wideo lub całych urządzeń na okno narzędzia Wideo
- Dodano możliwość przeciągania na narzędzie Wideo na panelu urządzeń telewizji dozorowej z poziomu narzędzia Tablica synoptyczna. Dzięki temu możliwe jest tworzenie z poziomu panelu nowych widoków wideo.
- Dodano możliwość generowania raportów z rejestratorów serii 4000, 6000 oraz NMS VSS zawierających następujące informacje: adres IP, stan dysków, całkowity czas nagrań, zakres nagrań, różnicę czasu na urządzeniu (w stosunku do serwera, z którego został wygenerowany raport), wersja oprogramowania lub programu.
- W zakładce Operacje dodano przycisk umożliwiający przejście do konfiguracji urządzeń z poziomu przeglądarki internetowej
- Usunięto problem z tworzeniem automatycznej kopii zapasowej
- Zoptymalizowano działanie mechanizmu zabezpieczającego bazę danych przed przepełnianiem
- Dodano funkcję łączenia urządzeń telewizji dozorowej na żądanie
- Zmodyfikowano sposób łączenia z centralami alarmowymi Satel (uwierzytelnienie za pomocą kodu administratora)
- Dodano możliwość obsługi urządzeń jednostrumieniowych telewizji dozorowej (umożliwia to np. obsługę funkcji dwukierunkowej komunikacji audio dla głośników Zenitel ELSII-10LHM, ELSII-10HM)
- Poprawiono wyświetlanie drzewa urządzeń

Wersja 6.00.004

Data: 27.06.2024

- Dodano wizualizację systemu sygnalizacji pożaru POLON 6000
- Dodano możliwość budowy systemu kontroli dostępu w oparciu o kontrolery HID®Aero® X1100 oraz moduły rozszerzeń X100, X200, X300
- Dodano szyfrowane połączenie OSDP dla urządzeń HID
- Dodano Antypassback czasowy dla stref
- Zmiana wyglądu ikon
- Dodano możliwość zwolnienia z trybu antypassbacku czasowego dla VIP-ów
- Dodano licencje (rozszerzenia): NOVUS MANAGEMENT SYSTEM AC KaDe OP v6, NOVUS MANAGEMENT SYSTEM AC ULPR OP v6, NOVUS MANAGEMENT SYSTEM AC HID OP v6

Wersja 5.00.107

- Rozszerzono możliwość konfiguracji uprawnień dla operatorów
- Dodano nowe absencje
- Dodano obsługę dostępu do API
- Modyfikacja sposobu generowania delegacji
- Poprawiono rozliczanie nocnych godzin
- Poprawiono rozliczanie nadgodzin
- Zmiany w generowaniu raportów czasu pracy
- Poprawiono aktualizację w trybie multiserwerowości
- Poprawiono problem ze ścieżkami dla eksportu wideo
- Poprawiono problem z konfiguracją wyzwalaczy
- Poprawiono problem z hasłami RCP zaczynającymi się od zera
- Poprawiono problem z ustawieniem widoeweryfikacji

Wersja 5.00.90

- Dodano obsługę zmodyfikowanego sposobu naliczania punktów licencyjnych
- Dodano obsługę rozszerzenia NOVUS MANAGEMENT SYSTEM AC NMS VSS OP
- Dodano możliwość filtrowania dni w wyzwalaczach
- Poprawiono usuwanie logów

Wersja 5.00.71

- Możliwość zmiany kolejności urządzeń w oknie urządzeń
- Dodano możliwość zwinięcia okna zdarzeń na stałe do wyłączenia
- Poprawiono zapamiętywanie przypięcia okna zdarzeń
- Poprawiono przewijanie w oknie wyboru podziału wideo
- Poprawiono wyświetlanie na ekranach 4K
- Poprawiono działanie funkcji hot spot
- Poprawiono funkcję wysyłania maili
- Dodano możliwość klonowania poziomów dostępu
- Poprawiono walidację przy tworzeniu automatycznych raportów RCP
- Poprawiono problem z edycją automatyczny raportów RCP
- Poprawiono scenariusz otwierania paneli
- Dodano możliwość filtrowania zdarzeń archiwalnych po wpisanym zapytaniu
- Poprawiono automatyczne przeskakiwanie kursora z pola godzin na pole minut przy wpisywaniu godziny
- Zmieniono domyślne nazwy szablonów RCP
- Pole przerw w harmonogramach domyślnie zwiększa minuty po użyciu +
- Dodano komunikat o niekompatybilnej wersji w trybie multiserwerowym
- Pole informujące o statusie licencji przenosi do okna licencji po kliknięciu

- Poprawiono problem z rejestracją licencji w kraju innym niż Polska
- Dodano informacje o licencji Trial
- Poprawiono tłumaczenie niektórych komunikatów informacyjnych
- RCP - Konfiguracja/Terminale RCP / Operacje - synchronizacja - pobranie zdarzeń z terminala od określonej daty komendą operatora.
- Dodano warunek w scenariuszach “Analiza obrazu - rozpoznanie tablicy rejestracyjnej”
- Zmieniono sposób dodawania kanałów dla NMS oraz Novus Management System VSS
- Usunięto pola właściwości data urodzin, stanowisko, telefon, adres oraz wykształcenie
- Dodano możliwość ograniczenia czasu edycji korekty zdarzeń
- Zmieniono domyślny zakres czasów dla raportów RCP
- RCP: dodano nowe statusy: Wyjście prywatne bez powrotu oraz Wyjście służbowe bez powrotu
- Poprawiono eksport i import użytkowników
- Modyfikacje licencji
- RCP - Sortowanie kolumn w oknie definiowania szablonów RCP.
- RCP - Możliwość definiowania nazw własnych dla kolumn w szablonie raportów RCP
- RCP - Raporty niestandardowe - suma raportów indywidualnych dla całego działu lub firmy w jednym pliku.
- RCP - Rozliczanie zmianowego systemu czasu pracy - od 1 do 4 zmian w ciągu doby.
- RCP – Modyfikacja sposobu komunikacji z terminalami rejestracji czasu pracy.
- Automatyka budynkowa - integracja z urządzeniem LANKON-008

Wersja 5.00.035

- Zakładka Okno diagnostyczne przeniesiona do zakładki Ustawienia serwerów
- Zmiany w oknie Kopia zapasowa tworzenie, usuwanie i przywracanie kopii są teraz w jednym miejscu
- Logi Diagnostyczne przeniesione do zakładki Ustawienia klienta
- Zmiany Zakładki Licencje: Dodano formularz rejestracyjny oraz klauzulę RODO w pod zakładce Rejestracja
- Pod zakładka licencje wyświetla obecnie używane klucze, liczbę punktów licencyjnych, maksymalną ilość pojazdów LPR oraz użytkowników RCP, wyświetlanie multiserwerowości i identyfikatora sprzętowego
- Możliwość aktywacji i dezaktywacji kluczy licencyjnych.
- Dodano przycisk synchronizacji z serwerem licencji
- Dodano przycisk eksportu informacji o licencji do pliku pdf
- Dodano przycisk aktywacji licencji trial
- Dodano integrację z centralą alarmową Satel
- Zmieniono organizację identyfikatorów użytkownika w zakładce Użytkownicy
- Dodano przycisk “Wygeneruj Szablon Importu” w zakładce Użytkownicy
- Dodano przycisk klonowania w zakładce scenariuszy i paneli
- Zmieniono organizację w zakładce Dni świąteczne
- Dodano pole wyszukiwania w zakładce Widoki wideo
- Dodano trzeci stan przycisku przypięcia powiadomień, można teraz zablokować okno powiadomień, żeby nie rozwijało się przy zdarzeniu.
- Eksport wideo ma obecnie dwie zakładki, “Lista zadań” i “Ustawienia”
- Dodano Niestandardowy raport czasu pracy

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. Karola Olszewskiego 5B lok. 6, 20-481 Lublin tel. Kom. +48 602 785 010 e-mail: aat.lublin@aat.pl, www.aat.pl	Lublin
ul. Kolejowa 12C lok. 4/2 , 15-701 Białystok tel. 85 688 32 33 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