



Instrukcja instalacji i programowania

NOVUS MANAGEMENT SYSTEM AC

OPROGRAMOWANIE DO INTEGRACJI,
KONFIGURACJI I WIZUALIZACJI
SYSTEMÓW BEZPIECZEŃSTWA



Wersja programu 6.06.017 Aktualizacja: 11-08-2026



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

Rozdział 1 Wstęp	05
1.1 Informacje wstępne	05
1.2 Funkcje i parametry systemu	07
1.3 Schemat blokowy systemu	17
Rozdział 2 Instalacja i uruchomienie programu	18
2.1 Wymagania minimalne na PC	18
2.2 Licencje.....	20
2.3 Instalacja programu	21
2.4 Aktualizacja programu	29
2.5 Uruchomienie programu	30
2.6 Pulpit operatora i nawigacja w oknie programu	35
2.7 Menu programu	37
2.8 Ikony występujące w oknach programu	38
2.9 Skróty oraz kombinacje klawiaturowe	39
Rozdział 3 Konfiguracja systemu	
3.1 Urządzenia - Kontrola dostępu - Kontrolery.....	40
3.2 Urządzenia - Kontrola dostępu - Kontroler - Drzwi	47
3.3 Urządzenia - Kontrola dostępu - Kontroler - Drzwi - Czytnik	49
3.4 Urządzenia - Kontrola dostępu - Kontroler - Linie dozorowe	51
3.5 Urządzenia - Kontrola dostępu - Kontroler - Wyjścia sterujące	53
3.6 Urządzenia - Kontrola dostępu - Kontroler windowy	55
3.7 Urządzenia - Kontrola dostępu - Kontroler windowy - Winda	57
3.8 Urządzenia - Kontrola dostępu - Kontroler windowy - Winda - Czytnik	58
3.9 Urządzenia - Kontrola dostępu - Kontroler windowy - Winda - Czytnik - Piętro	60
3.10 Urządzenia - Telewizja dozorowa	61
3.11 Urządzenia - Głośniki IP	63
3.12 Urządzenia - Terminale do Rejestracji Czasu Pracy	67
3.13 Urządzenia - Drukarka biletów	72
3.14 Urządzenia - System sygnalizacji włamania i napadu.....	73
3.15 Urządzenia - System sygnalizacji pożarowej POLON 6000.....	75
3.16 Urządzenia - Operacje	77
3.17 Urządzenia - Informacje	81
3.18 Urządzenia - Grupy	82
3.19 Konfiguracja - Struktura firmy	83
3.20 Konfiguracja - Parametry zdarzeń	84
3.21 Konfiguracja - Formaty kart	85
3.22 Konfiguracja - Scenariusze	85
Rozdział 4. Użytkownicy, karty i uprawnienia	96
4.1 Harmonogramy	96
4.2 Poziomy dostępu	97

4.2.1 Poziomy dostęp - Systemy sygnalizacji włamania i napadu.....	98
4.3 Karty	99
4.4 Użytkownicy	100
4.4.1 Użytkownicy - Systemy sygnalizacji włamania i napadu.....	106
Rozdział 5. Szablony	107
5.1 Widoki wideo	107
Rozdział 6. Panele	108
Rozdział 7. Zdarzenia i raporty	112
7.1 Lista zdarzeń	112
7.2 Lista ostrzeżeń	113
7.3 Automatyczne raporty	114
7.4 Pliki na serwerze	115
Rozdział 8. Ustawienia systemowe	116
8.1 Ustawienia serwerów	116
8.2 Grupy i operatorzy	119
8.3 Ustawienia klienta (stacji operatora)	123
8.4 Licencje	124
8.5 Kopia zapasowa	128
Rozdział 9. Funkcje zaawansowane.....	131
9.1 Grupy serwerów	131
9.2 Strefy globalne	135
9.3 Śluzę globalne	139
9.4 Rejestracja czasu pracy	140
9.5 Integracja z urządzeniami VSS	159
9.5.1 Narzędzia do integracji VSS - Wideo	160
9.5.2 Narzędzia do integracji VSS - Odtwarzacz	161
9.5.3 Narzędzia do integracji VSS - Sterowanie PTZ	162
9.5.4 Narzędzia do integracji VSS - Drzewo urządzeń.....	163
9.5.5 Narzędzia do integracji VSS - Tablica synoptyczna	164
9.5.6 Wyświetlanie strumieni wideo w reakcji scenariusza	165
9.5.7 Generowanie raportów nagrań w reakcji scenariusza	166
9.6 Rozpoznawanie tablic rejestracyjnych LPR	168
9.6.1 LPR - rozpoznawanie tablic rejestracyjnych	169
9.6.2 Dodawanie kamer LPR	169
9.6.3 Strefy LPR	170
9.6.3.1 Konfiguracja stref	171
9.6.3.2 Obsługa wyjazdu gościa z użyciem kontrolera z czytnikiem, drukarki QR i kamery LPR ..	172
9.6.3.3 Awizacja gościa w strefie LPR	174
9.6.4 Poziomy dostęp - parking	174
9.6.5 Pojazdy	176
9.6.6 Narzędzia w panelu LPR	177
9.6.7 Użytkownicy - Identyfikatory	180
9.6.8 Przypisanie wygenerowanego kodu QR do użytkownika typu Gość.....	181
9.7 Eksport nagrań	183
9.7.1 Eksport nagrań z poziomu menu głównego	183
9.7.2 Eksport nagrań z poziomu odtwarzacza	188

9.8 Pobieranie zrzutów ekranu	189
9.9 Integracja z Systemami sygnalizacji włamania i napadu	190
9.10 Narzędzie obsługi ostrzeżeń: wizualizacja i raportowanie	191
9.11 Integracja (wizualizacja) z systemami sygnalizacji pożaru Polon 6000	193
9.12 Integracja (wizualizacja) z systemem kontroli dostępu KANTECH	196
9.13 Integracja (wizualizacja) z systemem kontroli dostępu marki SALTO.....	202
9.14 Integracja z oprogramowaniem NOVUS MANAGEMENT SYSTEM AC przy użyciu API	205
Warunki umowy licencyjnej	219
Lista zmian w oprogramowaniu	224

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.

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:

Kontrola dostępu (KD): system kontroli dostępu Kantech (za pośrednictwem oprogramowania EntraPass Global lub Corporate od wersji 7.40), system kontroli dostępu SALTO (za pośrednictwem oprogramowania SALTO ProAccess Space od wersji 6.11.2.1).

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 dostęp, 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 stopką 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 podstawie 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, Salto
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./zarygłow. drzwi kartą	TAK
- odrygłowanie zgodnie z terminarzem po odczycie 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-służa 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
Sposób integracji	Za pośrednictwem oprogramowania EntraPass Corporate lub Global (od wersji 7.40)
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

Kontrola dostępu (KD) marki SALTO	
Nazwa parametru lub funkcji	Wartość parametru lub opis funkcji
Sposób integracji	Za pośrednictwem oprogramowania SALTO ProAccess Space (od wersji 6.11.2.1)
Komendy	Odrygluj czasowo Otwórz Awaryjnie Zamknij Awaryjnie Koniec Stanu Awaryjnego Użytkownicy
Zdarzenia	Drzwi - dostęp dozwolony Drzwi - dostęp zabroniony Awaria Drzwi - Sforsowane Drzwi - powrót do stanu normalnego Drzwi - Otwarte (<i>nie dotyczy klamek bezprzewodowych</i>) Drzwi - Przetrzymane Kontroler - Brak komunikacji (tylko ikona) Kontroler - Powrót komunikacji (tylko ikona)
Zarządzanie użytkownikami	Import Użytkowników
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

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
Kalendarze dodatkowe	TAK
Raporty zdarzeń	Filtrowane, zapis w formacie csv, html (pdf)
Raporty RCP (z terminali lub z czytników KD)	Rozliczanie czasu pracy na podstawie harm.

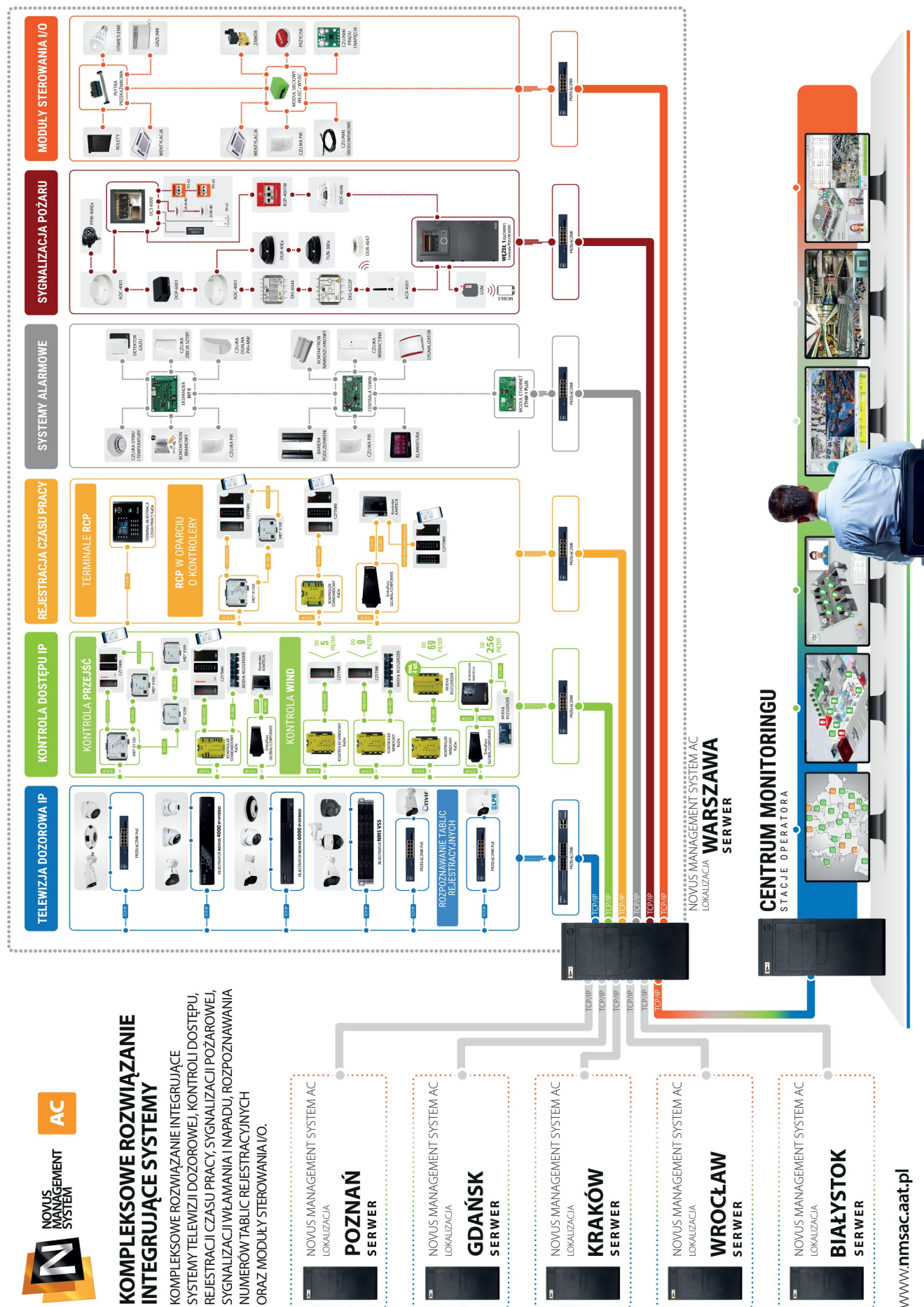
Telewizja dozorowa VSS	
Nazwa parametru lub funkcji	Wartość parametru lub opis funkcji
Wideo	TAK
Wspierane urządzenia	Kamery IP Novus serii 4000/6000/8000, Kamery IP ONVIF/RTSP, Rejestratory IP Novus serii 4000/6000, Rejestratory multistandard Novus serii 4000/6000 Rejestratory IP NOVUS MANAGEMENT SYSTEM 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 połączone 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 dostęp	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 Przekaznik 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 przekaznika 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 eeprom Element liniowy - załączony izolator zwarc Element liniowy - uszkodzenie sprzętowe

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 ściśle 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 raportu zdarzeń RCP jest realizowane przy użyciu licencji **NOVUS MANAGEMENT SYSTEM AC Raport zdarzeń RCP 365 v6**.

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 rozproszonym, 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 muliserwerowego (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.

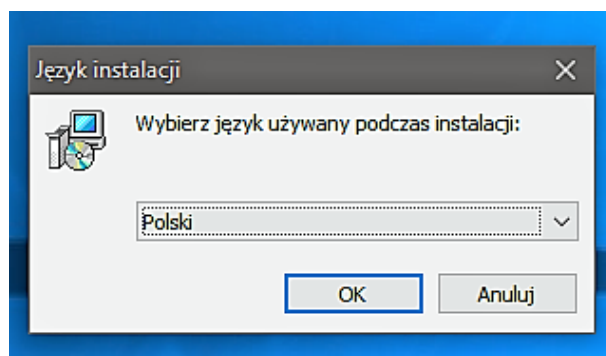
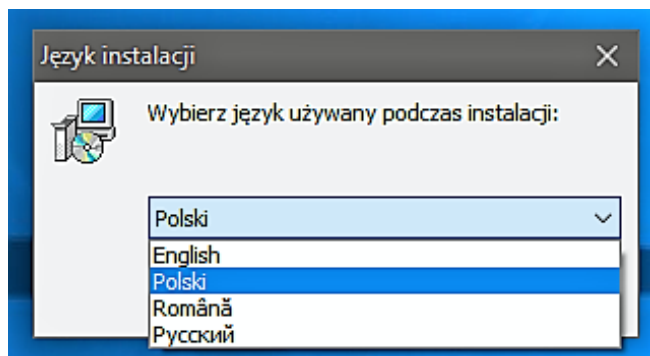
Dostępna jest również licencja testowa programu (**TRIAL**), czas jej trwania wynosi 60 dni. Zawiera ona pełną funkcjonalność oraz limit 500 000 punktów licencyjnych, 500 000 użytkowników RCP, 500 000 pojazdów LPR oraz 100 stacji operatora. W celu uzyskania szczegółowych informacji prosimy o kontakt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

2.3 Instalacja programu

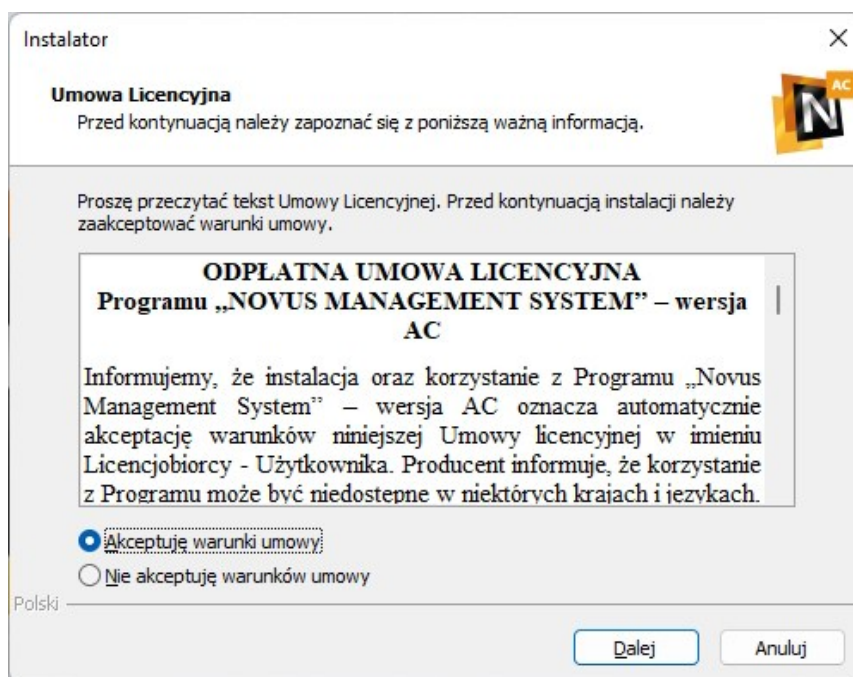
W celu uruchomienia procesu instalacji należy kliknąć na pliku NOVUS MANAGEMENT SYSTEM AC_full_X.XX.XXX.exe lub polecenie *Uruchom* z menu kontekstowego. W celu uzyskania wersji instalacyjnej oprogramowania Novus Management System AC w wersji 6 należy skontaktować się z działem handlowym AAT SYSTEMY 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*).

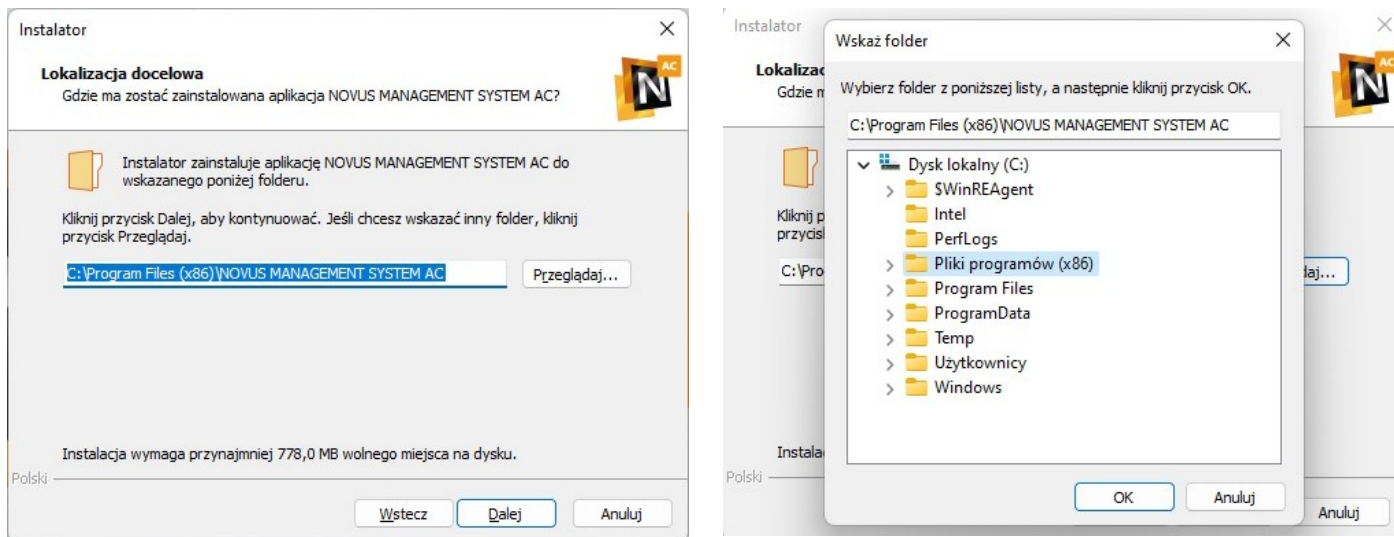
Po uruchomieniu instalatora programu NOVUS MANAGEMENT SYSTEM AC na ekranie pojawi się okno widoczne poniżej. Z rozwijanej listy należy wybrać język instalatora i zatwierdzić przyciskiem **OK**.



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**.



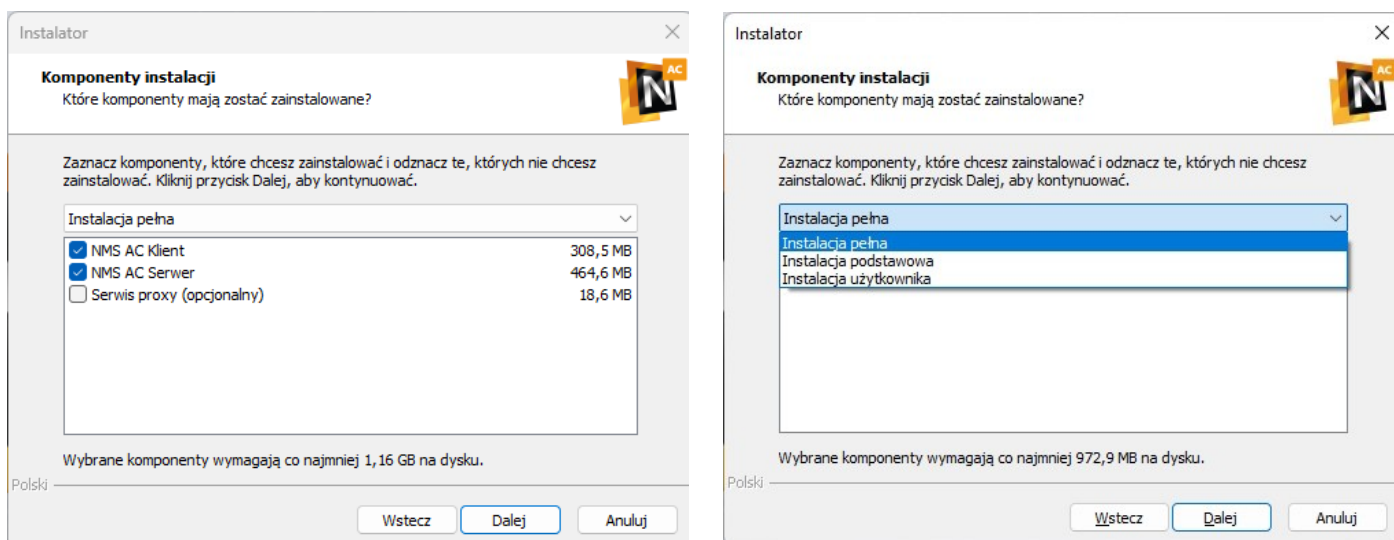
W widocznym na poniższych rysunkach oknie należy wybrać ścieżkę instalacji programu. Domyślną ścieżkę można edytować w polu tekstowym lub wybrać z drzewa katalogów po kliknięciu przycisku **Przeglądaj...** i zatwierdzić przyciskiem **OK**. Po wybraniu ścieżki instalacji NOVUS MANAGEMENT SYSTEM AC należy 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**.

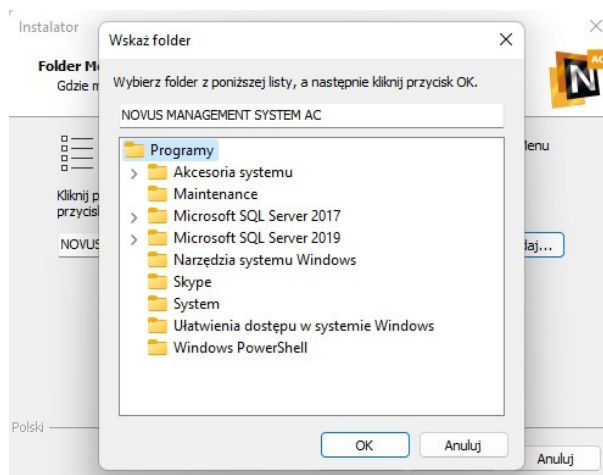


Na etapie konfiguracji bazy danych należy z rozwijanej listy poniżej wybrać jedną z trzech opcji.

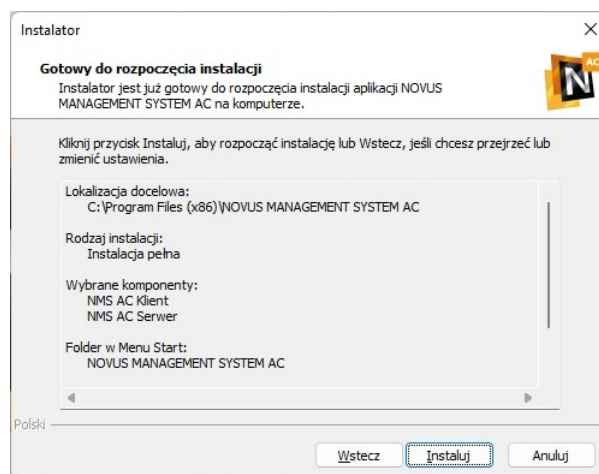
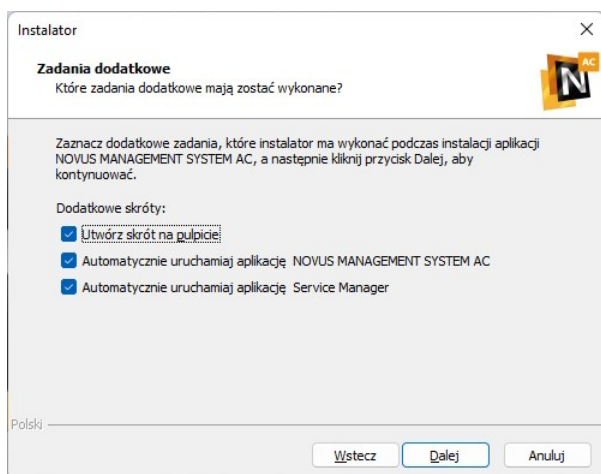
Nowa lokalna instalacja - instaluje na komputerze serwer SQL, tworzy nową instancję SQL oraz bazę danych o nazwach podanych w polach tekstowych.

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.

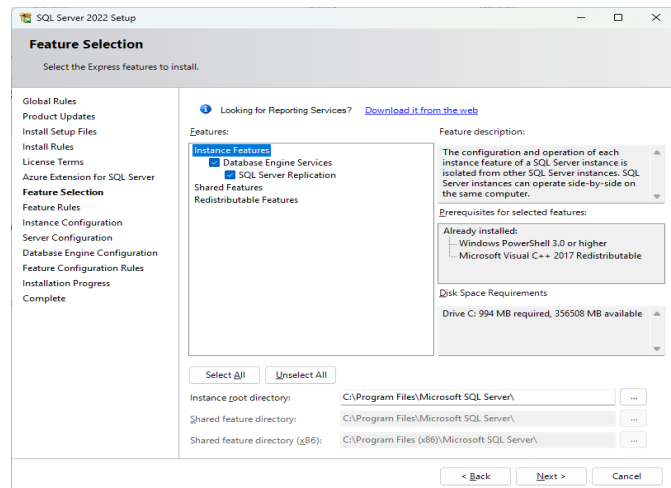
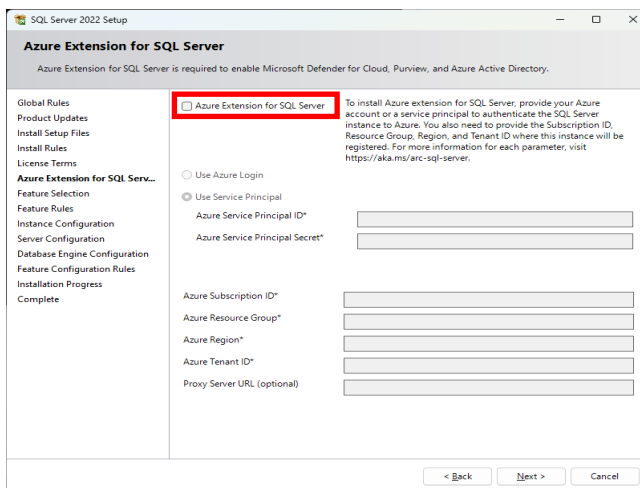
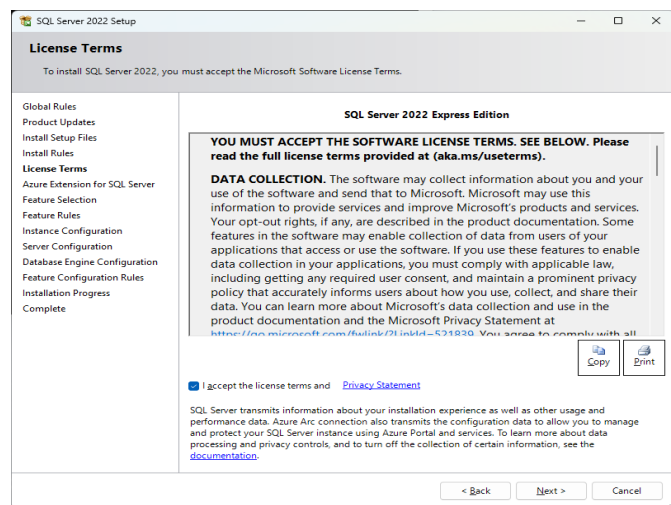
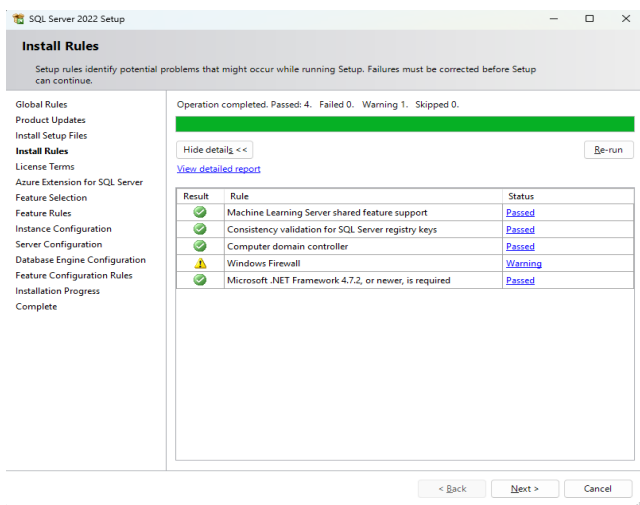
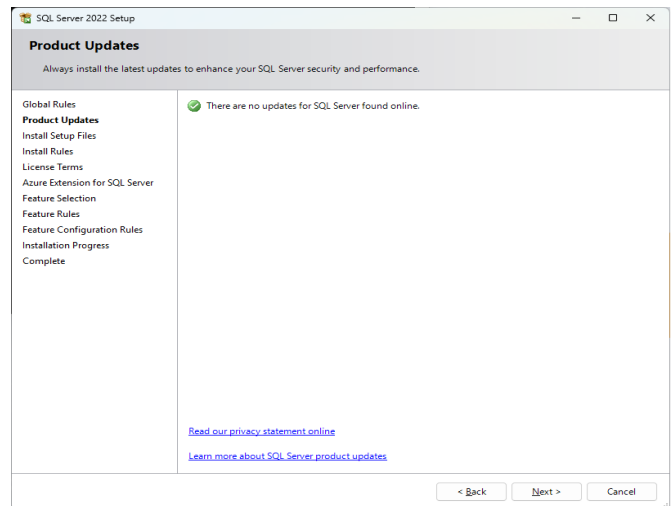
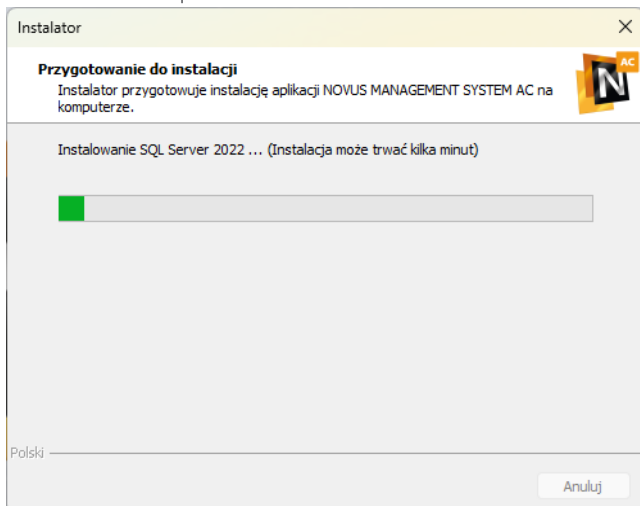


Po naciśnięciu przycisku **Dalej** pojawi się widoczne po prawej okno gotowości do instalacji podsumowujące dotychczas wybrane ustawienia. Do tego etapu można swobodnie wracać do poprzednich kroków konfiguracji instalacji przy pomocy przycisku **Wstecz**. Kiedy ustawienia w podsumowaniu są prawidłowe,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

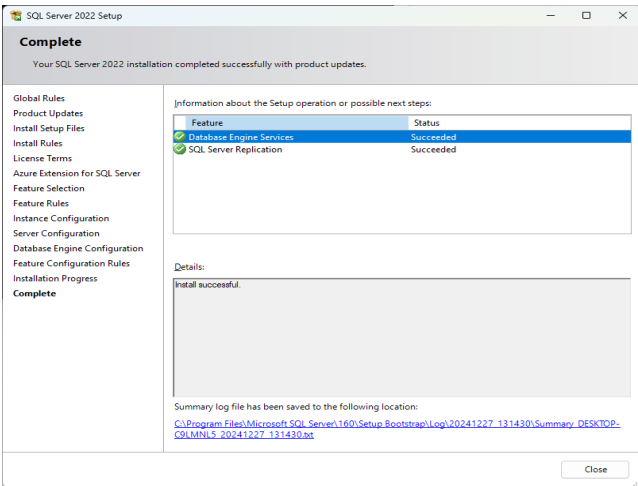
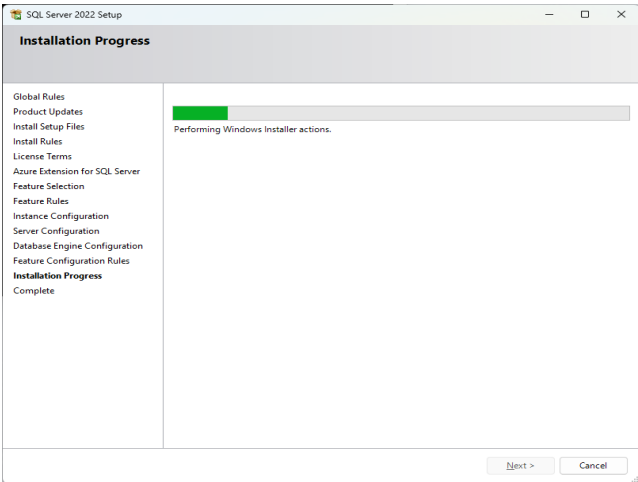
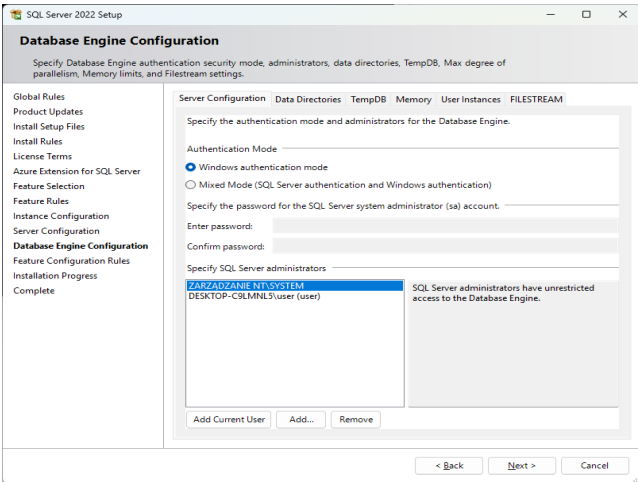
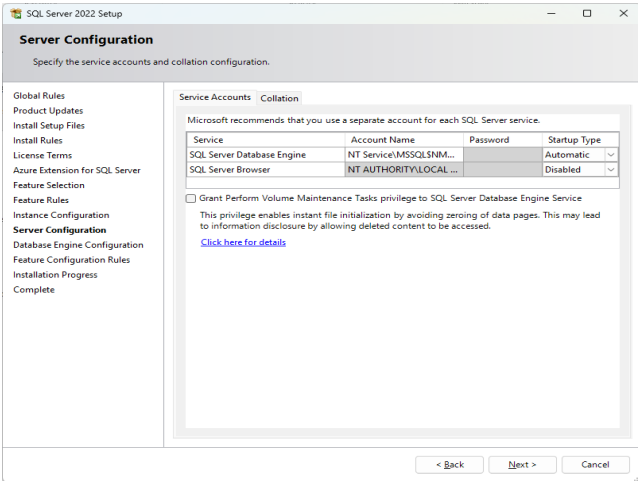
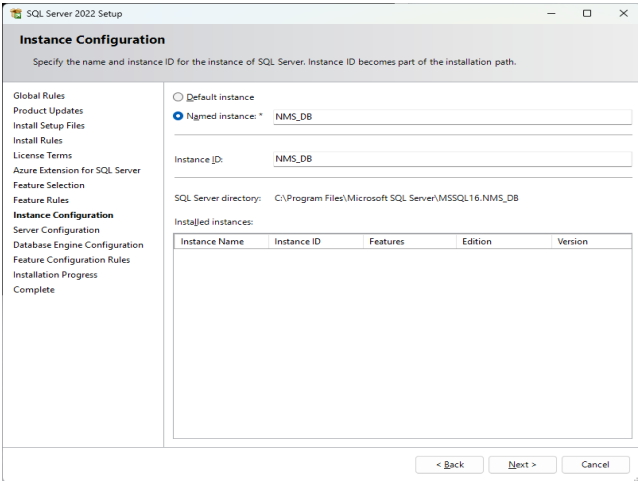
Na tym etapie po wybraniu lokalizacji i nazw rozpoczyna się właściwy proces instalacji oprogramowania.

W pierwszej kolejności zostanie zainstalowana baza danych SQL zgodnie z wybraną 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**.

NOVUS MANAGEMENT SYSTEM AC – Instrukcja instalacji i obsługi



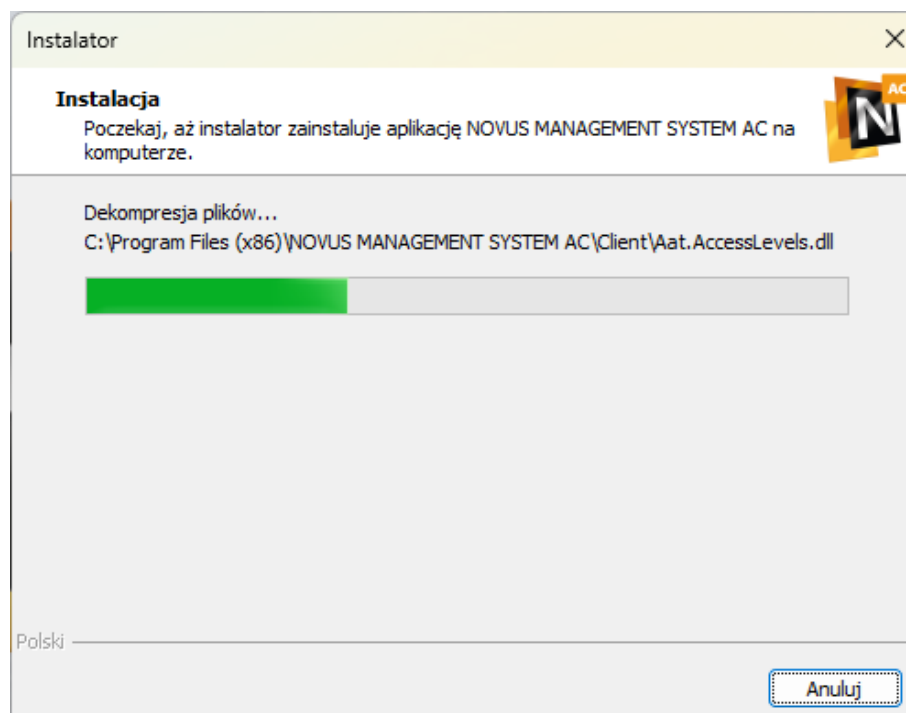
Na tym etapie w kolejnych oknach należy klikać przycisk **Dalej (Next)**, a w oknie **License Terms** zaznaczyć pole akceptacji licencji (I accept the license terms and Privacy Statement). W oknie **Azure Extension for SQL Server** należy odznaczyć opcję Azure Extension for SQL Server.



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.

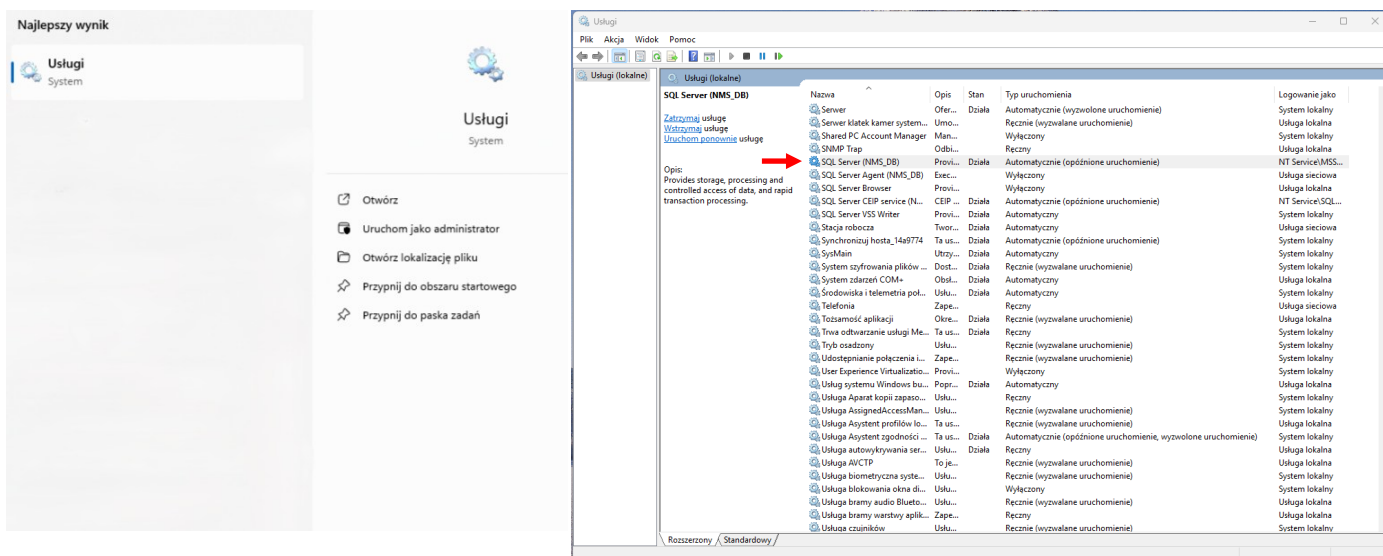


Po zainstalowaniu aplikacji pojawia się okno informacyjne widoczne poniżej. Można od razu uruchomić program NOVUS MANAGEMENT SYSTEM AC klikając przycisk **Zakończ** przy jednocześnie zaznaczonym polu wyboru **Uruchom aplikację NOVUS MANAGEMENT SYSTEM AC**. Odznaczenie tego pola i kliknięcie przycisku 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**.

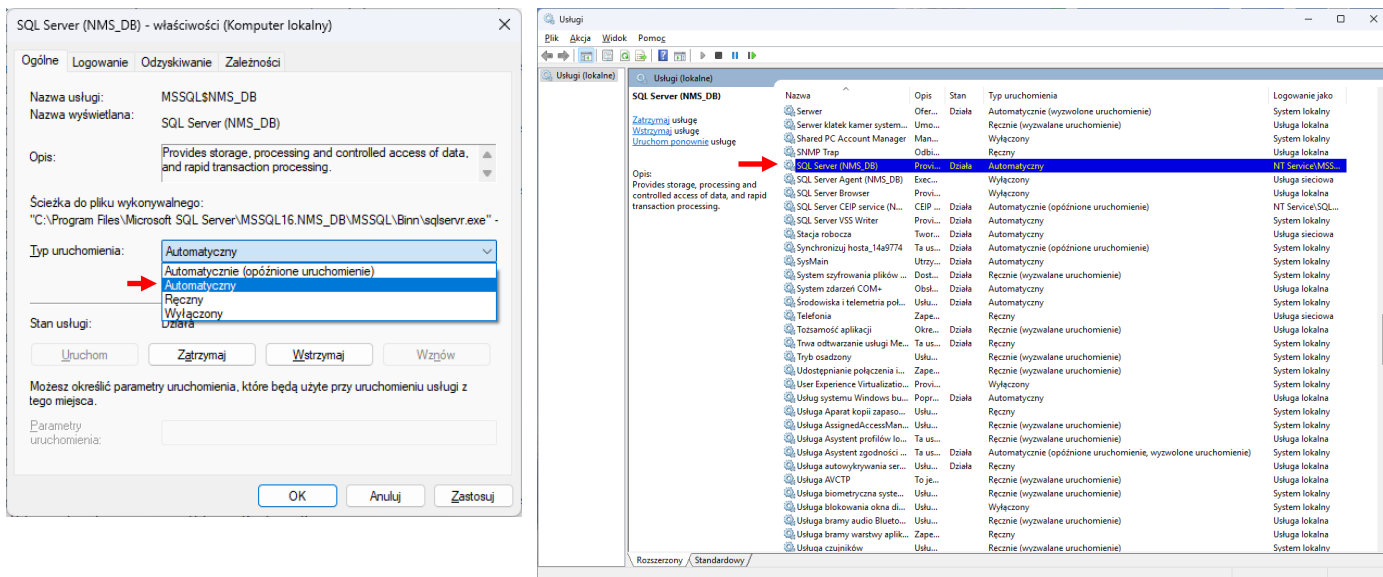


UWAGA!

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.

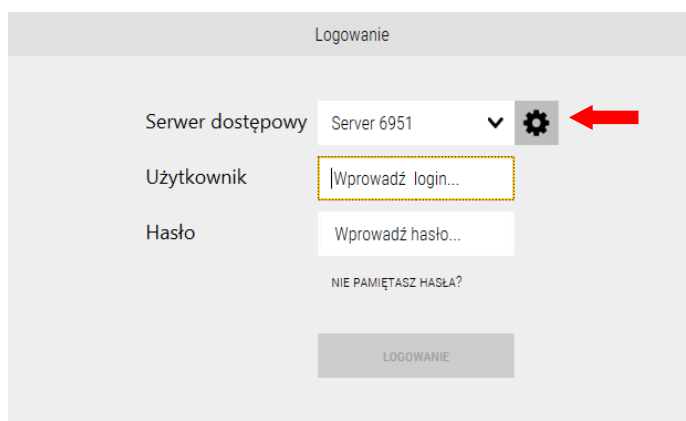
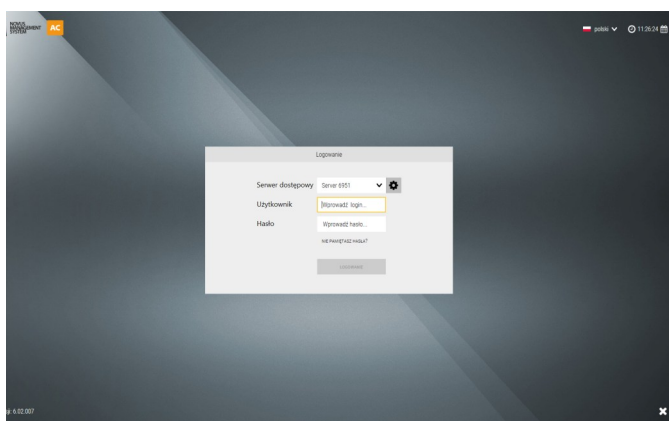
W celu przeprowadzenia aktualizacji należy postępować w analogiczny sposób jak zostało to opisane w rozdziale dotyczącym instalacji programu.

2.5 Uruchomienie programu

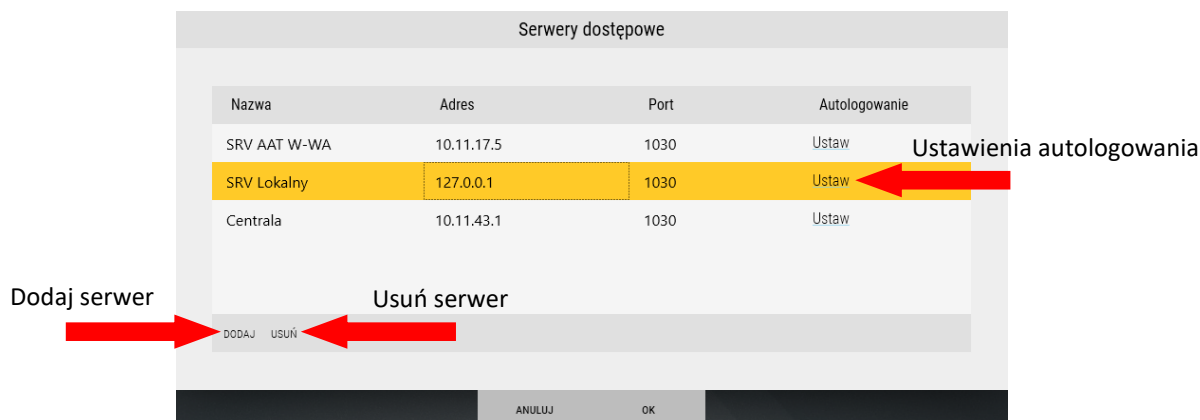
Po zainstalowaniu oprogramowania NOVUS MANAGEMENT SYSTEM AC domyślnie na pulpicie pojawi się ikona widoczna poniżej, a w menu start systemu Windows utworzona zostanie grupa NOVUS MANAGEMENT SYSTEM AC. Za ich pomocą można uruchomić program.



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 WYŚLAĆ GO PONOWNIE.** Jeżeli email dalej nie przychodzi należy sprawdzić w skrzynce mailowej folder **SPAM.**

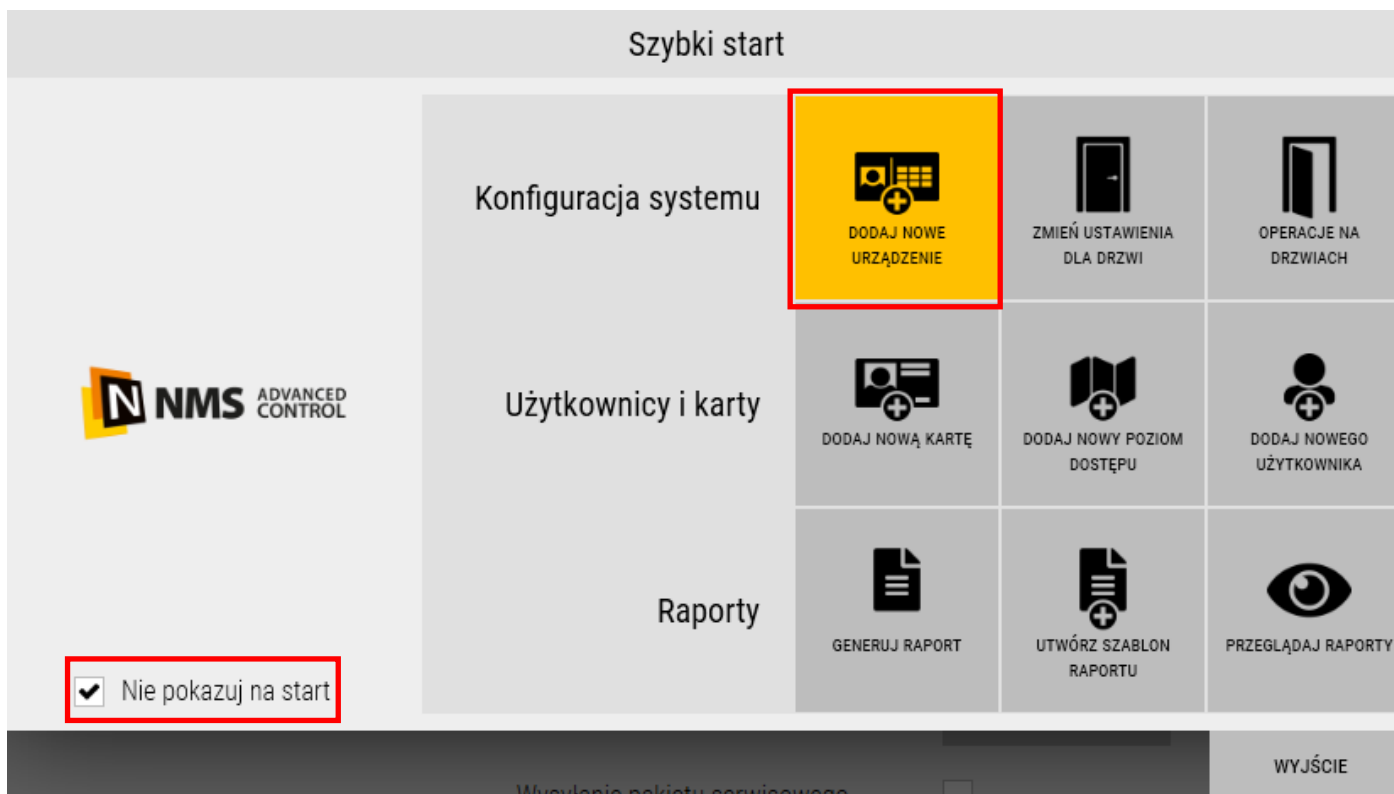
Po wpisaniu nazwy i hasła oraz kliknięciu przycisku **LOGOWANIE**, w dolnej części okna może się pojawić komunikat *SERWER W TRAKCIE URUCHAMIANIA*. Oznacza to, że należy poczekać, ponieważ uruchamia się usługa serwera (np. po restarcie).

The screenshot shows a login window titled "Logowanie". It contains three input fields: "Serwer" with a dropdown menu showing "Local 127.0.0.1:1030" and a gear icon, "Użytkownik" with the text "root", and "Hasło" with four black dots. Below the password field are four small circles, with the third one being larger. At the bottom, an orange banner displays the text "SERWER W TRAKCIE URUCHAMIANIA".

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.

The screenshot shows the same login window as above, but the bottom banner is red and displays the text "SERWER NIE ODPOWIADA. SPRAWDŹ ADRES I PORT LUB POŁĄCZENIE SIECIOWE." (Server not responding. Check address and port or network connection).

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

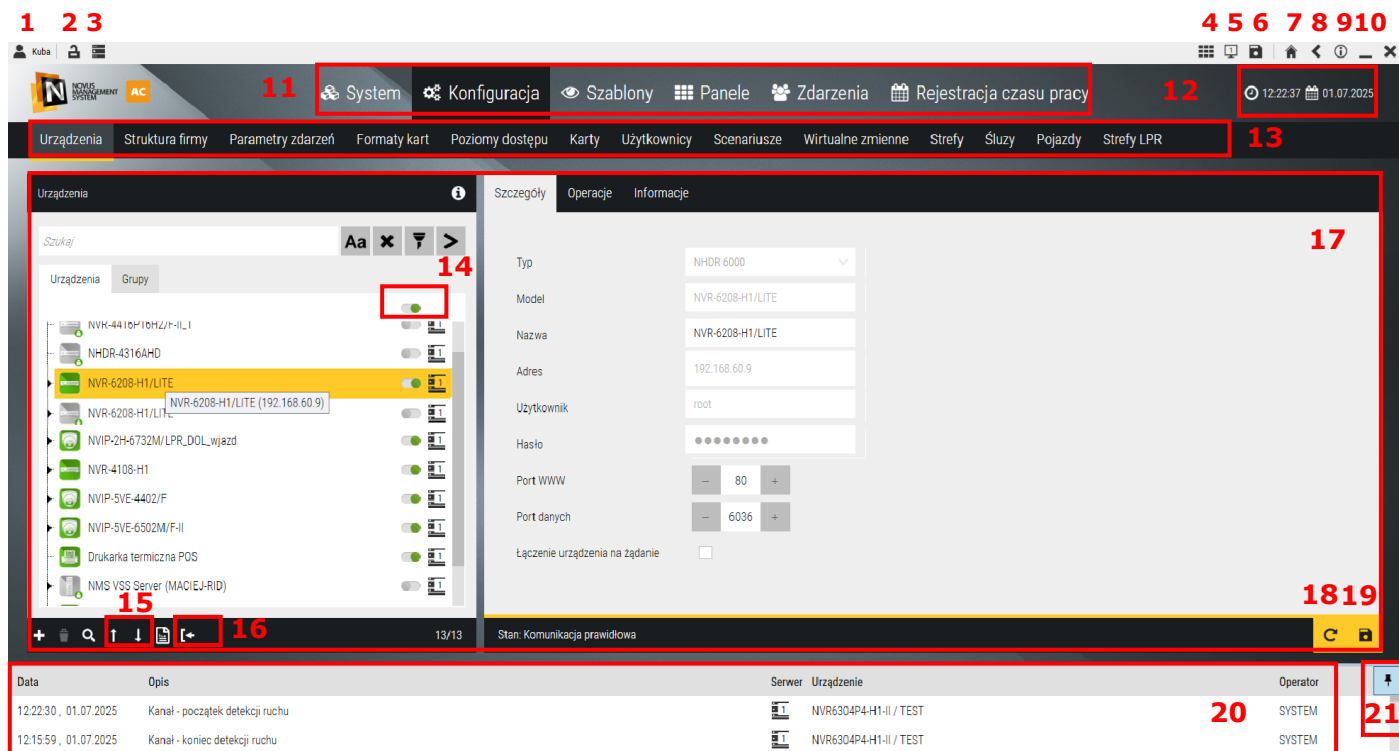
3. Raporty

- **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**.

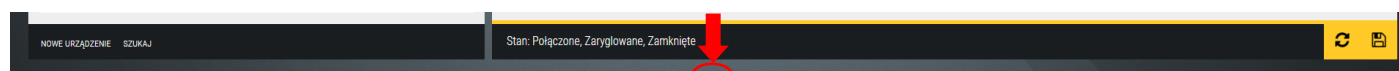
2.6 Pulpit operatora i nawigacja w oknie programu

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

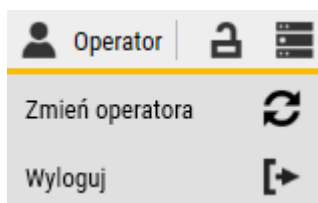


- Wyświetla okno z dwoma dostępnymi opcjami **Zmiana operatora** oraz **Wyloguj**.
- Przycisk **Blokada ekranu** - blokuje dostęp do menu programu, odblokowanie wymaga wpisania hasła.
- Wyświetla bieżący serwer lub listę serwerów w grupie (jeżeli została utworzona).
- Wyświetla listę paneli w możliwości otwarcia wybranego z listy.
- Wyświetla numer aktualnego monitora.
- Zapisuje aktualny układ okien wyświetlanych na poszczególnych monitorach.
- Przycisk **Szybki start** - otwiera okno **Szybki start**.
- Przycisk **Wstecz** - wyświetla poprzednie okno lub ekran, umożliwiając szybki powrót do wcześniej używanego widoku.
- Przycisk **O aplikacji** - otwiera okno z numerem wersji oprogramowania i link do treści licencji.
- Przycisk **Minimalizuj** - minimalizuje okno NOVUS MANAGEMENT SYSTEM AC.
- Pasek wyboru sekcji - kliknięcie na odpowiednią sekcję pozwala na konfigurację lub podgląd opcji.
- Aktualna godzina i data serwera.
- Pasek zakładek - umożliwia przechodzenie pomiędzy poszczególnymi zakładkami wybranej sekcji.
- Przycisk połącz/rozłącz wszystkie urządzenia na liście.
- 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.
- Przycisk importu listy urządzeń z pliku wyeksportowanego z programu NOVUS MANAGEMENT SYSTEM VSS.
- Obszar roboczy - właściwości wybranego w lewym oknie elementu
- Przycisk odświeżania - odświeża wyświetlane dane
- Przycisk zapisu - zapisuje zmiany wprowadzone w konfiguracji systemu
- Okno logów systemowych - wyświetla logi dotyczące zmian w konfiguracji systemu oraz innych zdarzeń w systemie.
- 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 najechniu na ikonę  pojawia się nowe okno z dwoma opcjami Wyloguj  oraz Zmiana operatora. 



Opcja *Wyloguj* - wylogowuje aktualnego operatora i otwiera ekran logowania.

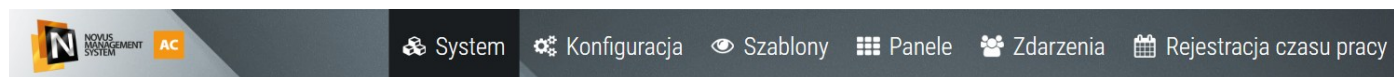
Opcja *Zmiana operatora* - po wybraniu tej opcji pojawia się nowe okno z polami do wprowadzenia nowych danych logowania innego operatora.

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

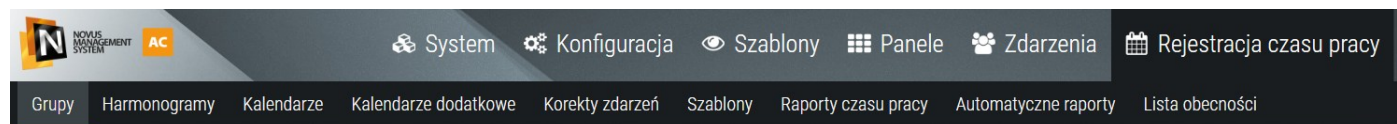
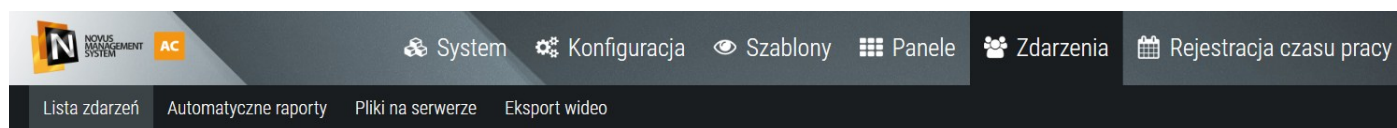
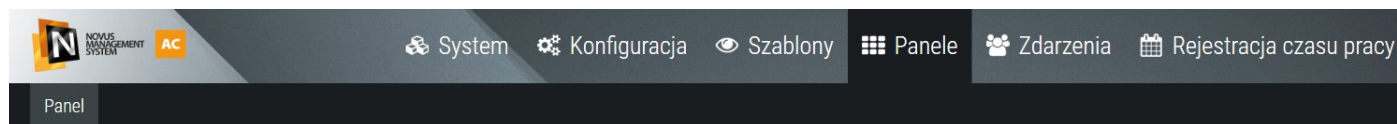
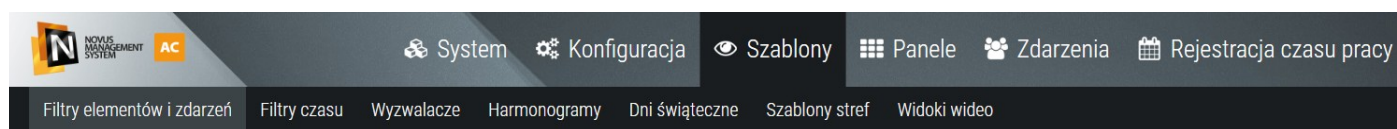
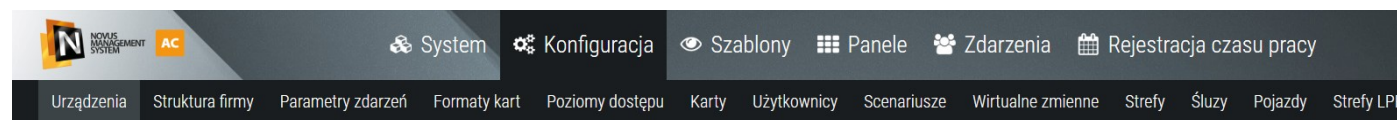
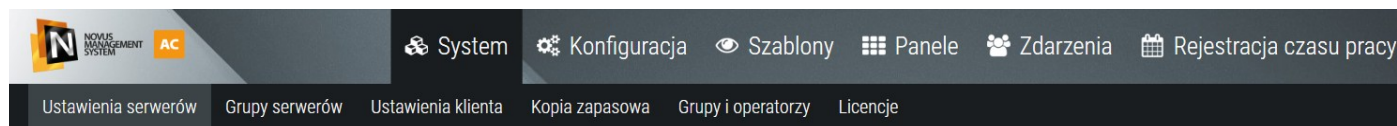
2.7 Menu programu

Menu programu zawiera dwa paski.

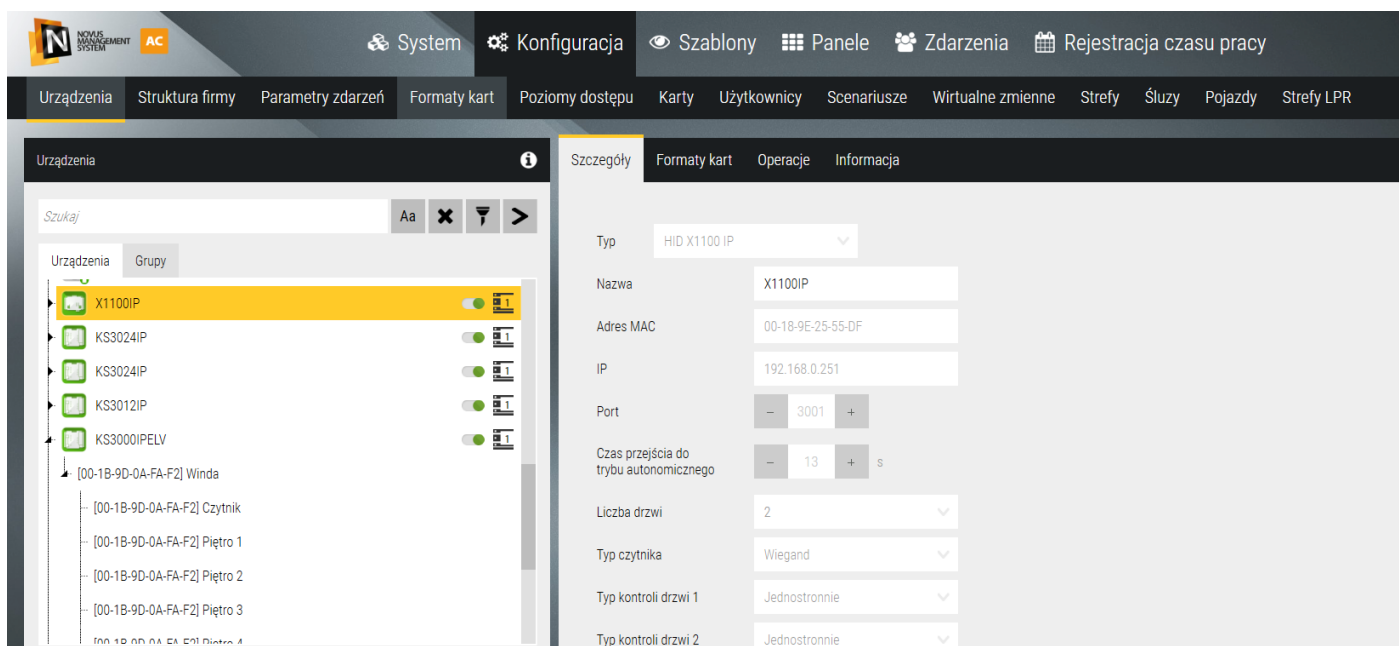
Pasek główny:



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:



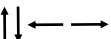
2.8 Ikony występujące w oknach programu

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 konfiguracji	Górny pasek
	Zablokuj ekran	Górny pasek
	Lista serwerów	Górny pasek
	Lista paneli	Górny pasek
	Zapis okien na monitorach	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.

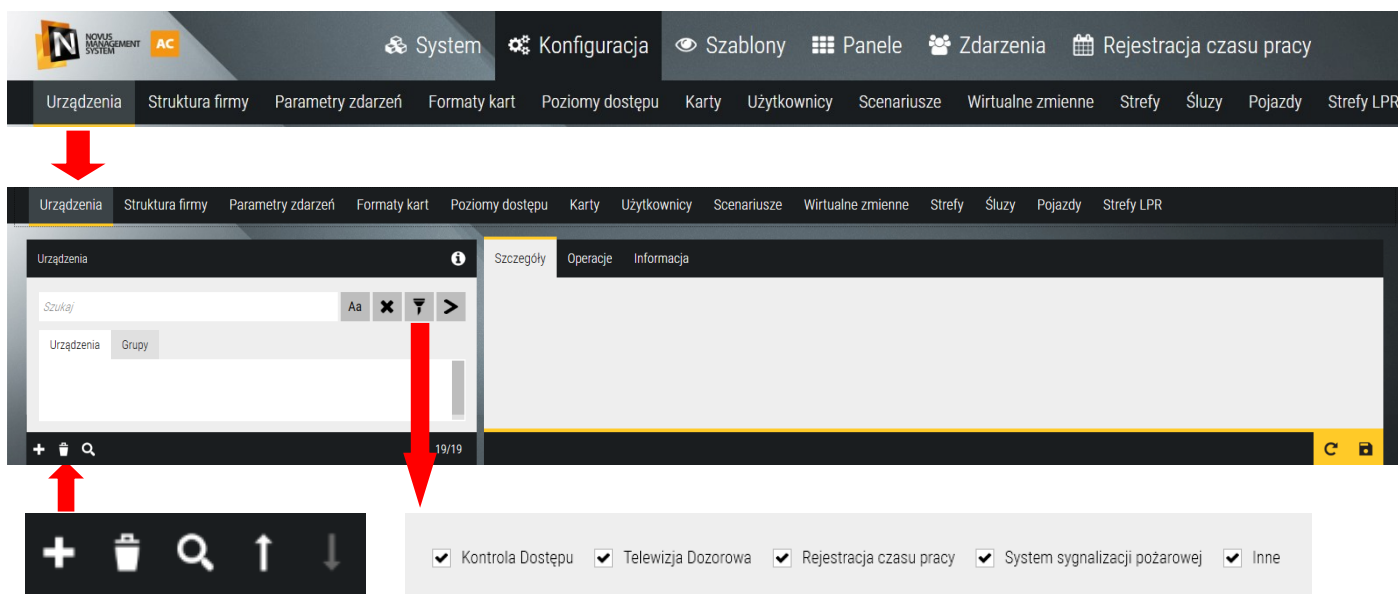
Kombinacja	Sposób użycia	Działanie
CTRL	Przytrzymaj	Pozwala zaznaczyć wiele elementów na liście (oddzielnych)
SHIFT	Przytrzymaj	Pozwala zaznaczyć wiele elementów w ciągłym zakresie
TAB	Naciśnij	Przejdź do następnego elementu
TAB + SHIFT	Przytrzymaj SHIFT, naciśnij TAB	Przejdź do poprzedniego elementu
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	Przejdź 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*.



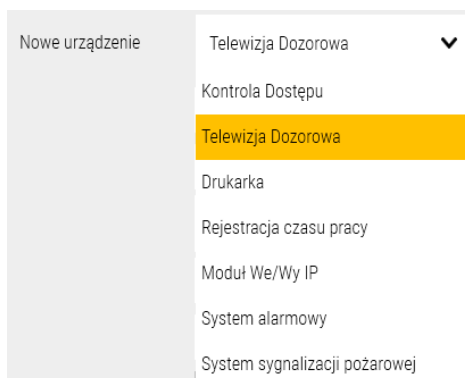
- dodaj nowe urządzenie
- usuń
- wyszukaj
- zmień kolejność urządzeń góra/dół

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:

The image shows three screenshots of the 'Nowe urządzenie' (New Device) configuration window in the NOVUS MANAGEMENT SYSTEM AC software. Each window is for a different device series and contains the following fields:

- Nowe urządzenie:** Kontrola Dostępu (dropdown)
- Seria:** HID (dropdown)
- Typ:** HID X1100 IP AC (dropdown)
- Nazwa:** Nowy Kontroler HID X1100 IP
- Adres MAC:** 00-00-00-00-00-00
- IP:** 192.168.0.251
- Port:** 3001 (range: - 3001 +)
- Czas przejścia do trybu autonomicznego:** 13 s (range: - 13 +)
- Liczba drzwi:** 2 (dropdown)
- Typ czytnika:** OSDP (dropdown)
- Typ kontroli drzwi 1:** Dwustronnie (dropdown)
- Typ kontroli drzwi 2:** Dwustronnie (dropdown)
- Czytnik - Secure Channel:** ☐ (with warning icon)
- Automatyczna synchronizacja czasu:** ☒

The third screenshot (Seria 3000) includes additional fields:

- Seria:** KS 3000 (dropdown)
- Typ:** KDH-KS3012-IP (dropdown)
- Nazwa:** Nowy Kontroler KDH-KS3012-IP
- Adres MAC:** 00-00-00-00-00-00
- IP:** 192.168.0.245
- Port:** 50000 (range: - 50000 +)
- Czas przejścia do trybu autonomicznego:** 5 s (range: - 5 +)
- Liczba drzwi:** 2 (dropdown)
- Typ modułu:** Brak (dropdown)
- Wiegand format:** Wiegand 26 (dropdown)
- Hasło komunikacyjne:** (empty field)
- Kod do kasowania alarmu:** (empty field)
- Automatyczna synchronizacja czasu:** ☒

At the bottom of each window are buttons: ANULUJ, OK, and a status indicator (Brak komunikacji).

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

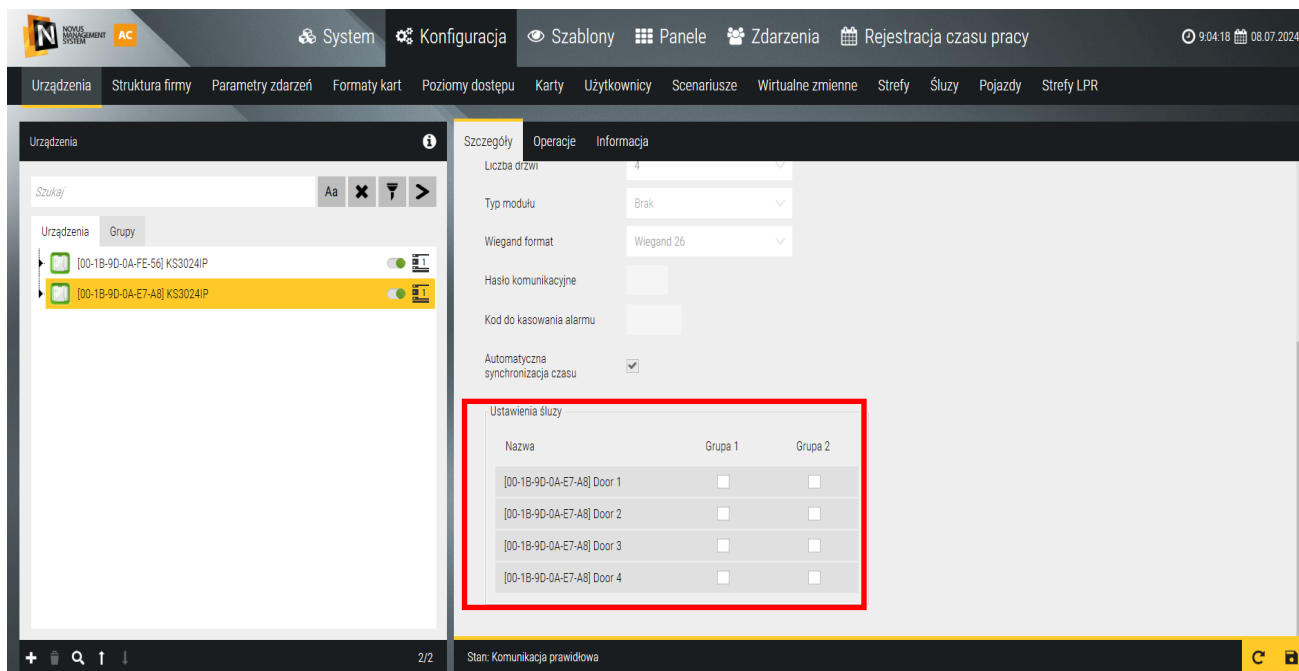
Opcje dla kontrolerów zintegrowanych:

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)

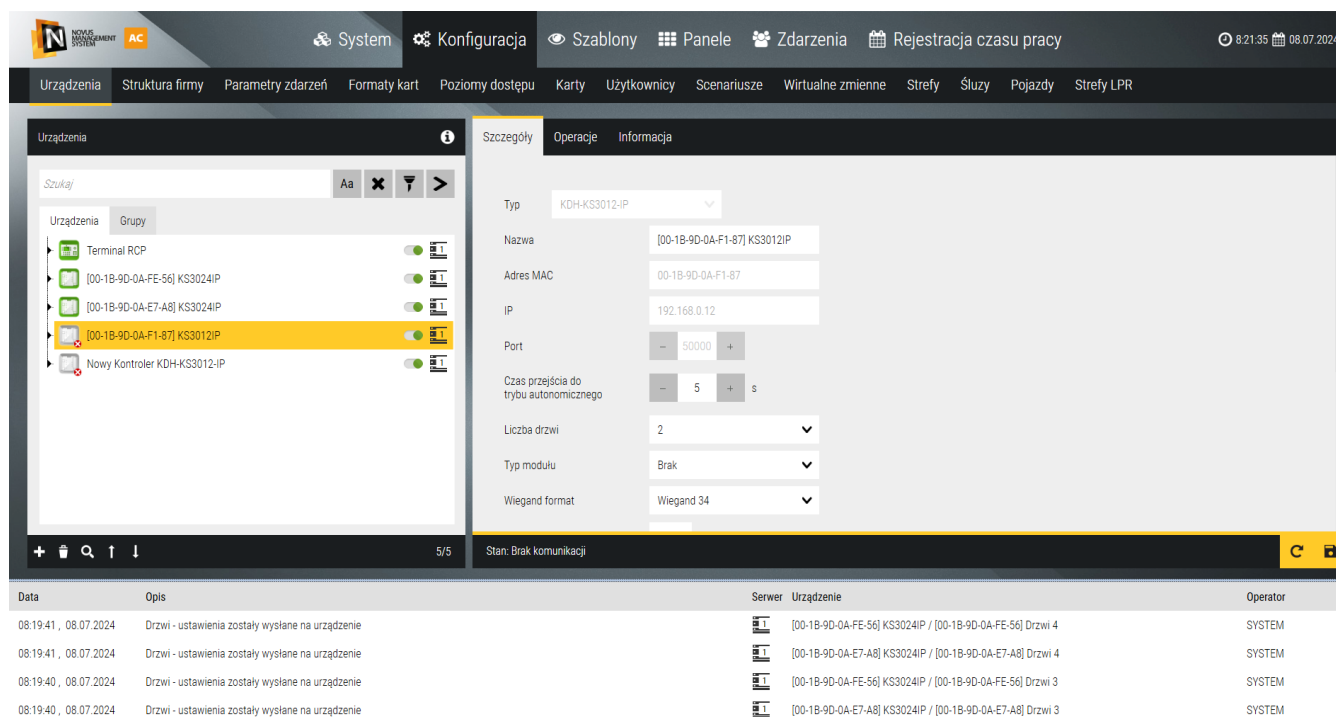
Alarm sforsowania drzwi - włączenie/wyłączenie alarmu sforsowania drzwi (dotyczy KDH-KZ3000-IP-U lub M)

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



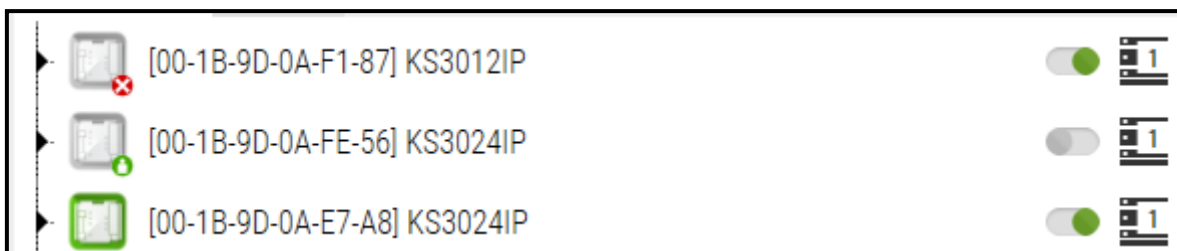
W przypadku kontrolerów KDH-KS3012/24-IP w prawym dolnym oknie pojawiają się dodatkowe pola umożliwiające dodanie drzwi i czytników kontrolera do jednej lub dwóch grup. Dotyczy to funkcji służby (czyli wzajemnej kontroli stanu skrzydła drzwi). Pola te nie występują w przypadku kontrolera windowego.

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.

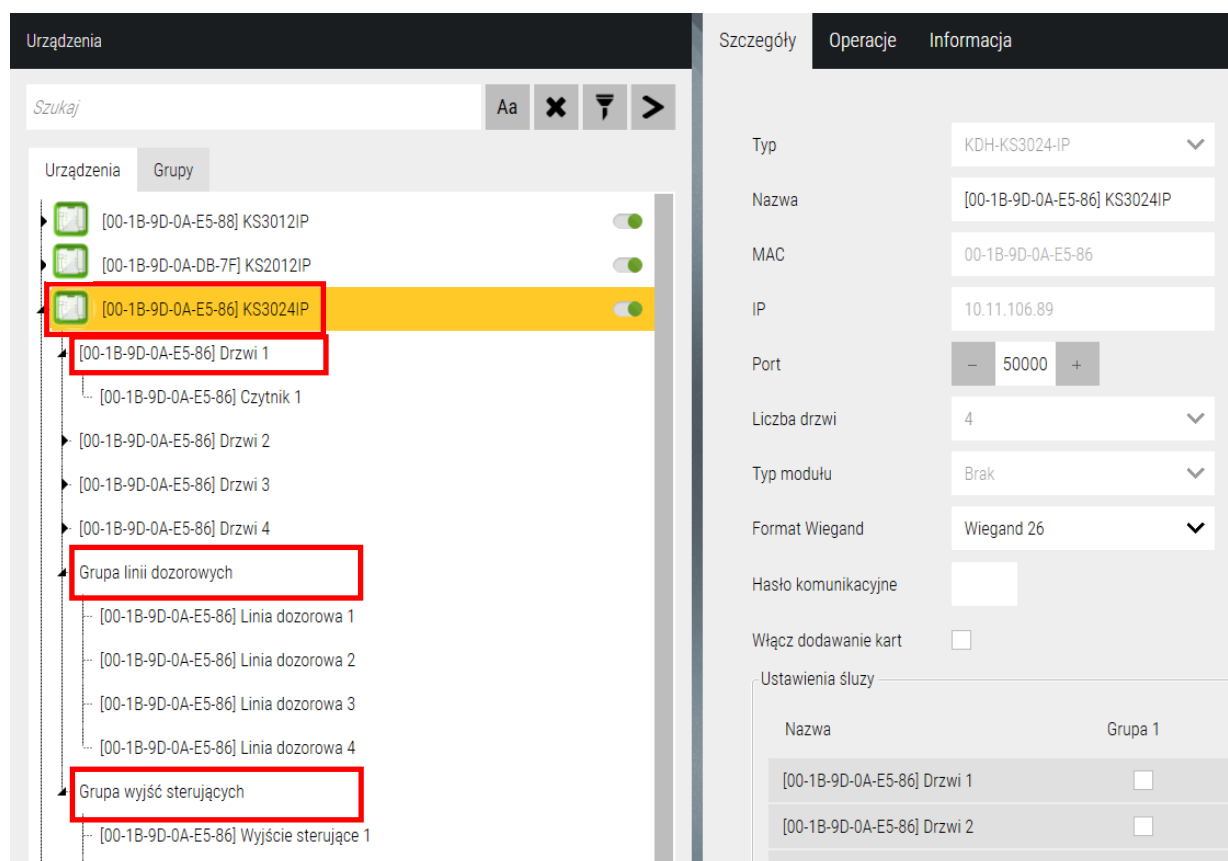


Po zapisaniu ustawień stan ikon może pokazywać jedną z trzech sytuacji:

- 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



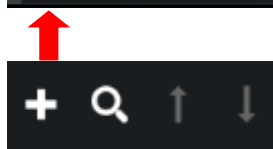
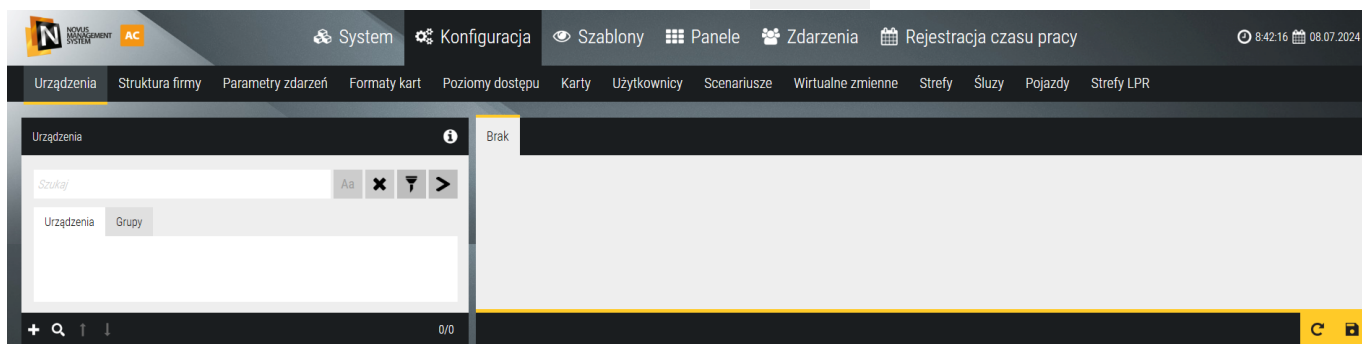
Ikony **kontrolera** można rozwinąć klikając na czarny trójkąt na linii głównego drzewa i wyświetlić elementy współpracujące. Zaznaczając wybrany element na rozwiniętej liście możemy edytować jego ustawienia.



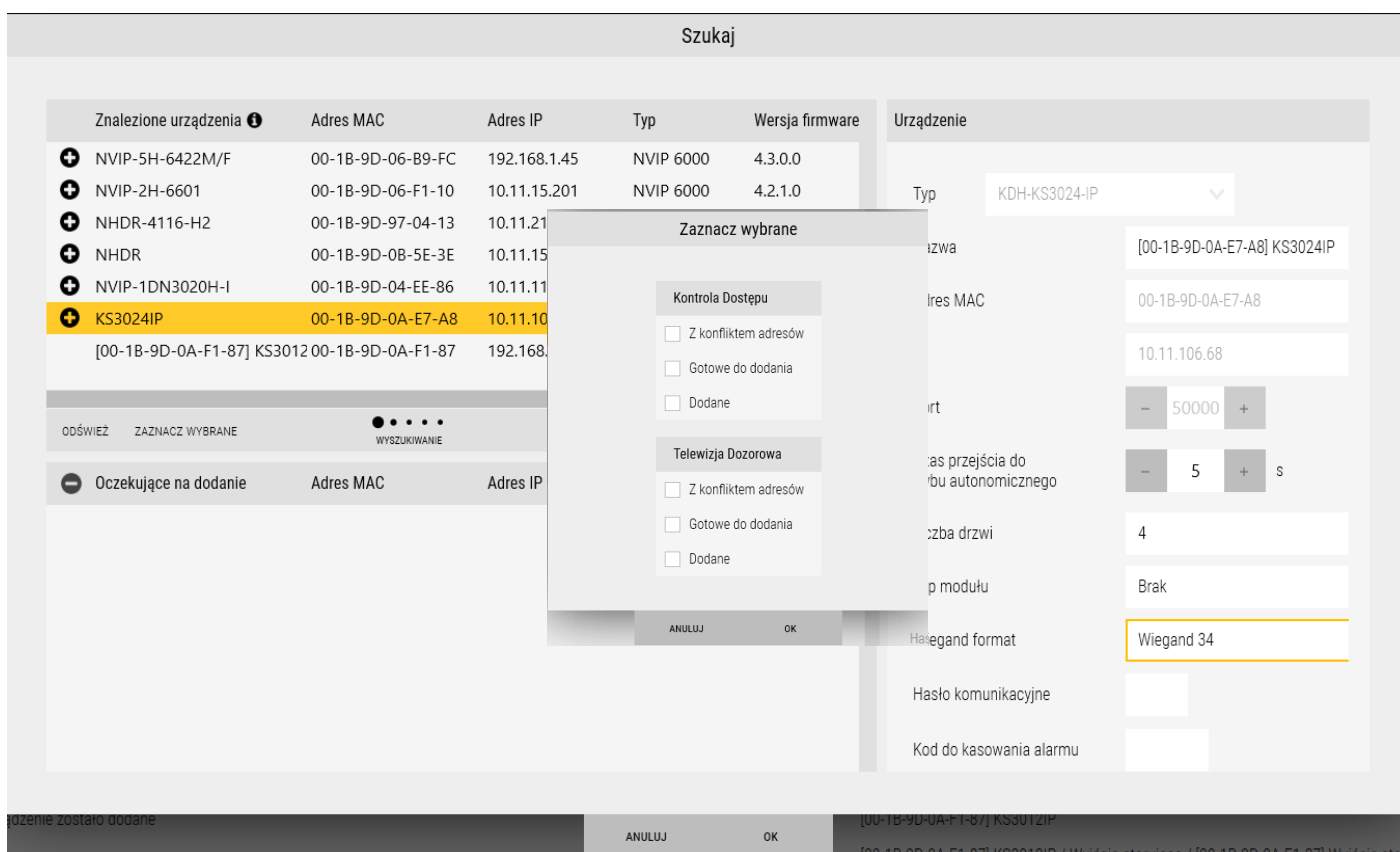
Dotyczy to takich elementów jak: drzwi, czytniki, linie dozoru i wyjścia sterujące. Po zaznaczeniu wybranego elementu, w prawym oknie wyświetlane są jego ustawienia, które można edytować. Wybrany element podświetlany jest na żółto. Po zmianie ustawień należy je zapisać klikając na dyskietkę w prawym 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 dyskietkę **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



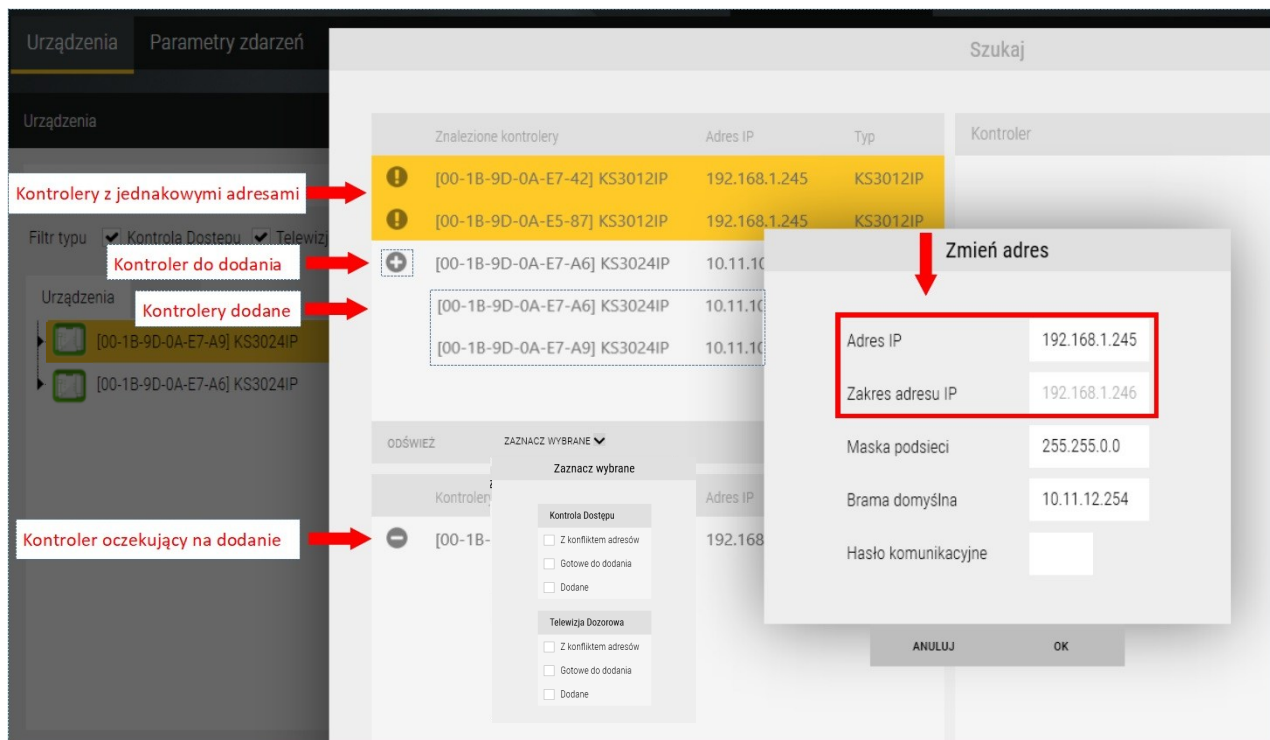
Gdy kontrolery zostały zainstalowane na obiekcie, podłączone do sieci Ethernet i zasilania, to w celu dodania ich do bazy systemu zaleca się skorzystać z dostępnej w programie wyszukiwarki. Przyspiesza to znacznie ten proces. Aby uruchomić wyszukiwarkę należy kliknąć na przycisk **Szukaj** na dole okna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



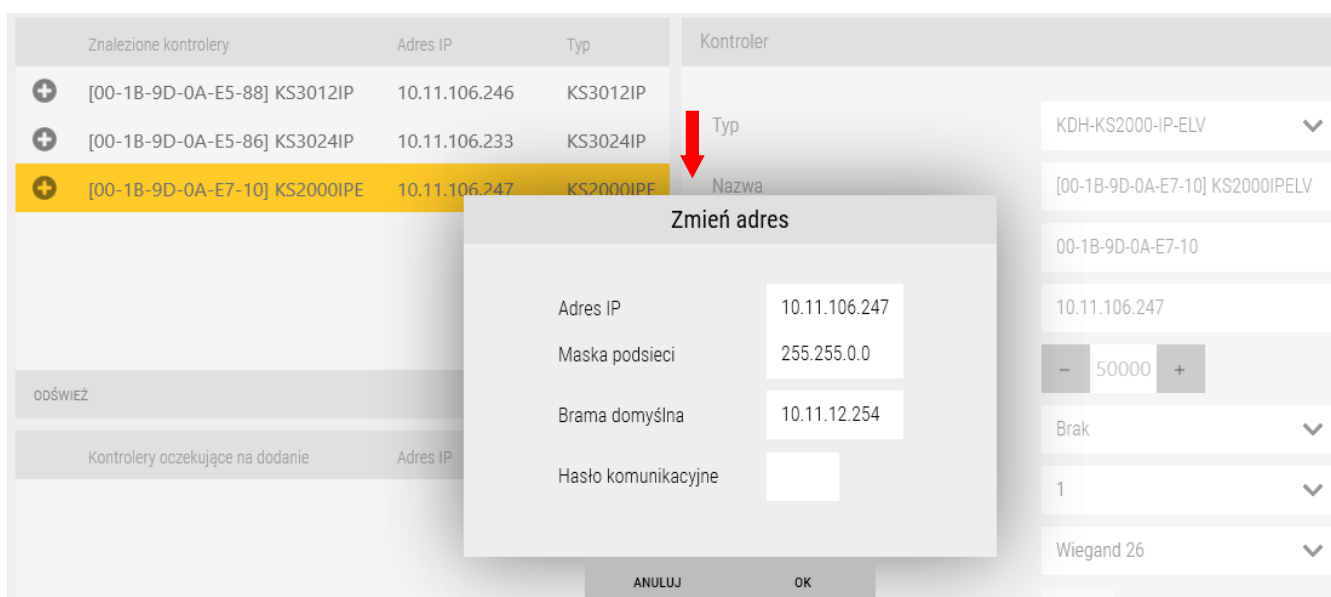
Wyszukane w sieci kontrolery wyświetlane są w lewej górnej części okna z ikonami informującymi o ich statusie:

- ! - 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 **+** zmieniają 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.



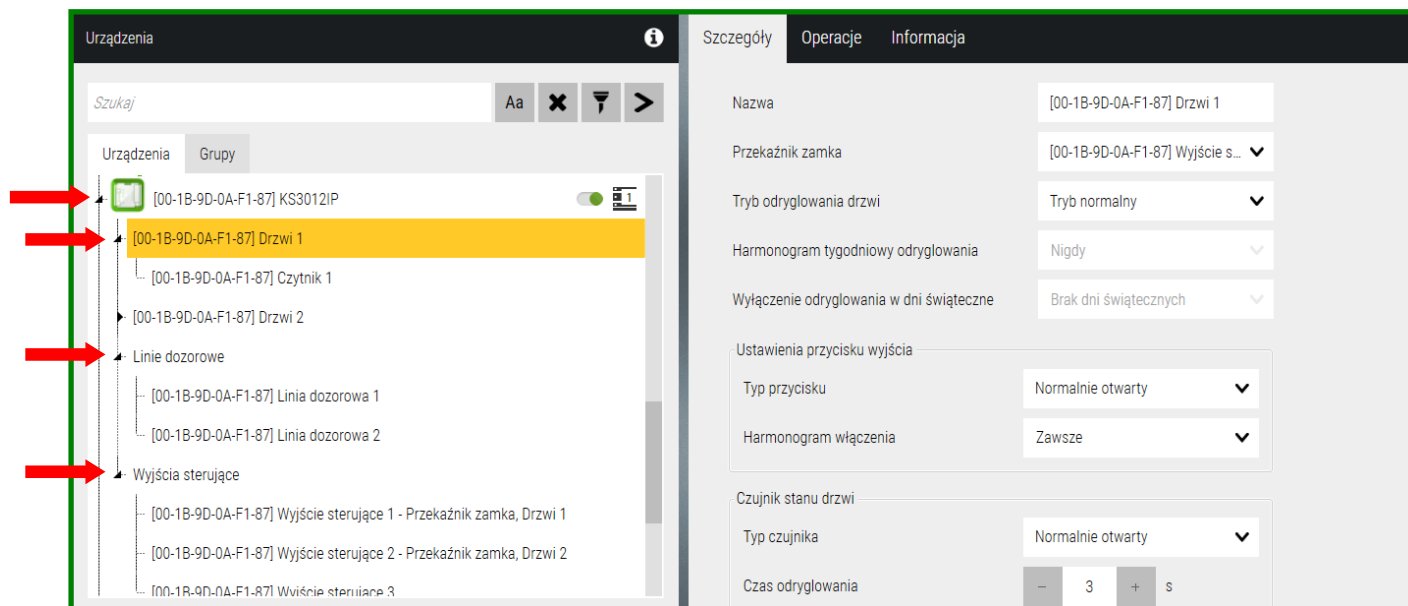
Na rozwijanej liście możemy wybrać, którą grupę kontrolerów chcemy zaznaczyć. W przypadku gdy chcemy zmienić adres jednego wyszukanego kontrolera, zaznaczamy go na liście w górnym oknie i klikamy na przycisku **Zmień adres**.



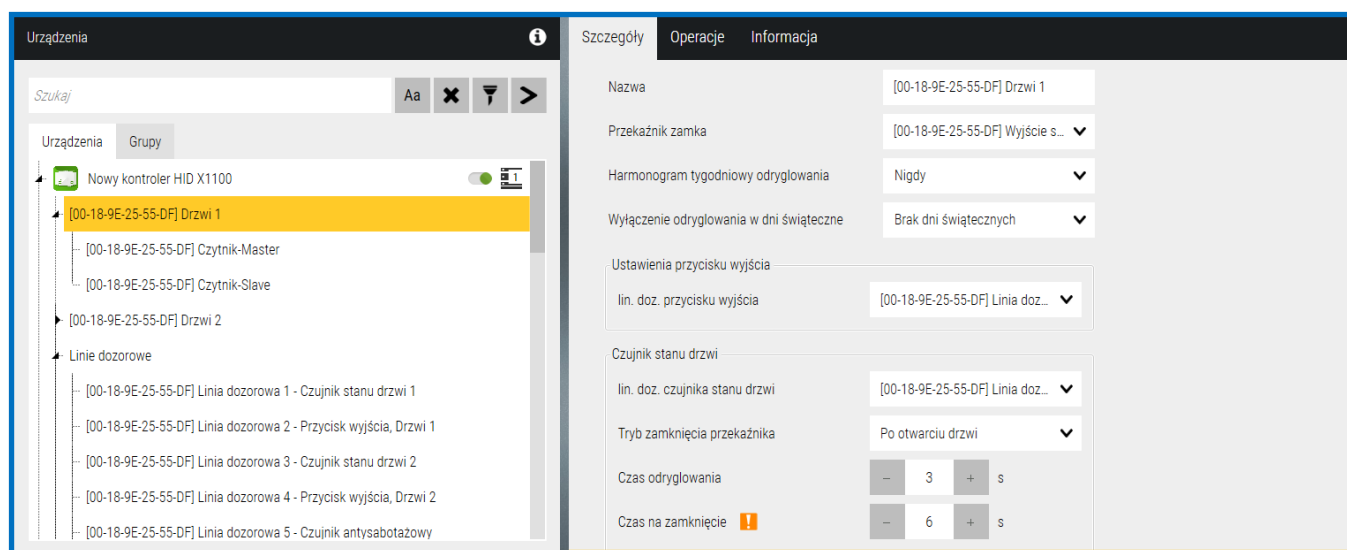
Po ustawieniu adresów i dodaniu wszystkich kontrolerów do listy w dolnym oknie należy kliknąć na przycisk **OK**. Dodane kontrolery pojawią się w oknie **Urządzenia**.

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



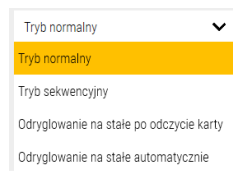
Seria HID®

Ustawienia drzwi

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

Przełącznik zamka - z rozwijanej listy można wybrać wyjście sterujące (przełącznik), które będzie sterowało zamkiem, domyślnie przypisane są przełączniki 1-2 lub 1-4, a przełącznik 3 lub 5 jest przełącznikiem 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 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 otwarcia 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).

Wideoeweryfikacja - umożliwia przypisanie do czytnika zainstalowanej nad nim (lub wbudowanej) kamery do rejestracji stopklatki w chwili odczytu karty. Stopklatka jest dołączana do zdarzenia na stosie i w raporcie na ekranie.

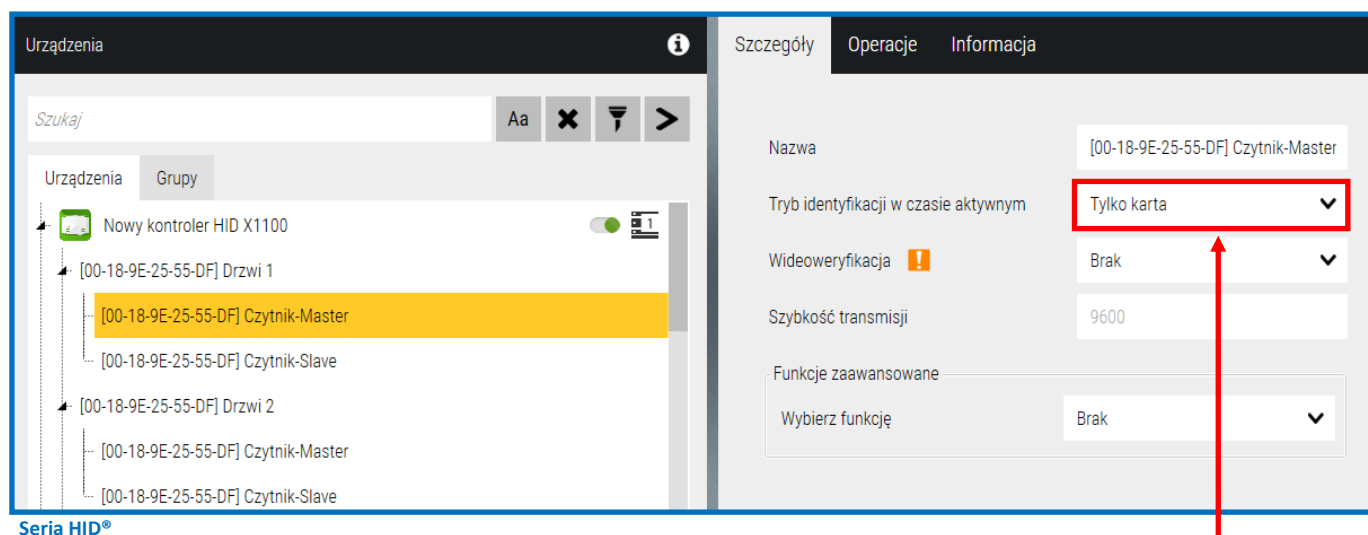
Funkcje zaawansowane - wybór jak w oknie poniżej:

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.



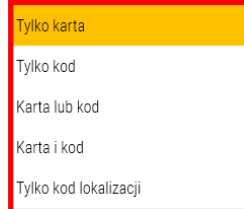
Seria HID®:

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:

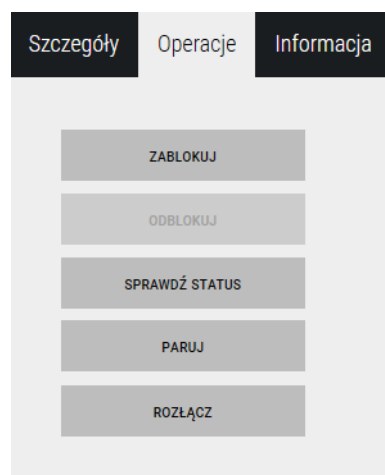
Potwierdzenie przez operatora - po zaznaczeniu uzyskanie dostępu z tego czytnika będzie wymagało odczytu ważnej karty oraz potwierdzenia przez operatora w specjalnym wyskakującym okienku. Opcję tą należy wybrać tylko, gdy system pracuje w trybie on-line i przy stacji obecny jest operator lub pracownik 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®

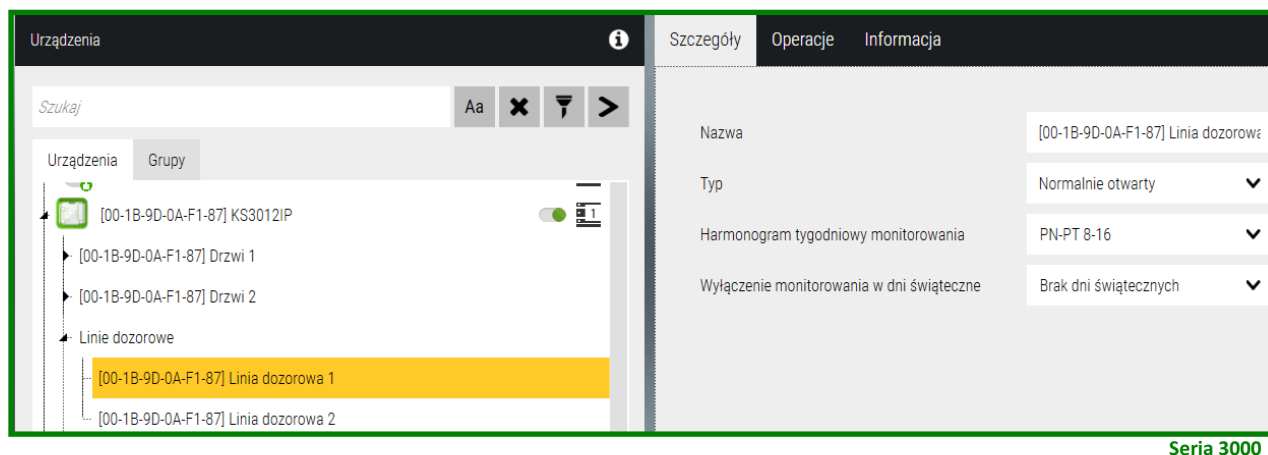
Zablokuj / Odblokuj czytnik - umożliwia zablokowanie czytnika przez operatora

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 **Install Mode i Secure Mode**

3.4 Urządzenia - Kontrola dostępu - Kontroler - Linie dozоровe



Seria 3000

Linie dozоровe 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 dozоровe i 4 na module rozszerzeń KDH-MOD2000INOUT dla **serii 3000** oraz 7 linii dozоровych dla **serii HID®** X1100 i X100, 19 linii dozоровych dla modułu X200 i 5 linii dla X300.

Seria 3000

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

Typ linii dozоровej - 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 dozоровych na module rozszerzeń jeżeli został zaimplementowany.

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

Ustawienia przycisku wyjścia

Typ przycisku

Normalnie otwarty

▼

Terminarz wyłączenia

Nigdy

▼

Czujnik stanu drzwi

Typ czujnika

Normalnie otwarty

▼

Seria HID®

Seria HID®

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

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

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

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

Czas do powtórnej reakcji - ustawienie opóźnienia powtórnej reakcji linii dozоровej 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 dozоровych na modułach rozszerzeń jeżeli został zaimplementowany.

Stany linii dozоровych:



Linia monitorowana
przez harmonogram
- stan normalny



Linia monitorowana
przez operatora
- stan normalny



Alarm



Usterka/zwarcie



Sabotaż

3.5 Urządzenia - Kontrola dostępu - Kontroler - Wyjścia sterujące

Szukaj [Aa] [X] [F] [P]

Urządzenia | **Grupy**

- [00-1B-9D-0A-F1-87] KS3012IP
 - [00-1B-9D-0A-F1-87] Drzwi 1
 - [00-1B-9D-0A-F1-87] Drzwi 2
 - Linie dozоровe
 - Wyjścia sterujące
 - [00-1B-9D-0A-F1-87] Wyjście sterujące 1 - Przekaznik zamka, Drzwi 1
 - [00-1B-9D-0A-F1-87] Wyjście sterujące 2 - Przekaznik zamka, Drzwi 2
 - [00-1B-9D-0A-F1-87] Wyjście sterujące 3**

Nazwa: [00-1B-9D-0A-F1-87] Wyjście steruj

Harmonogram tygodniowy włączenia: Nigdy

Wyłączenie przełączenia w dni świąteczne: Brak dni świątecznych

Tryb pracy: Synchronicznie ze stanem linii...

Powiązane linie dozоровe

- ☐ [00-1B-9D-0A-F1-87] Linia dozоровa 1
- ☐ [00-1B-9D-0A-F1-87] Linia dozоровa 2

Powiązane czujniki stanu drzwi

- ☐ Czujnik stanu drzwi 1
- ☐ Czujnik stanu drzwi 2

Powiązane przyciski wyjścia

- ☐ Przycisk wyjścia 1
- ☐ Przycisk wyjścia 2

Powiązane czynniki - dostęp dozwolony

- ☐ [00-1B-9D-0A-F1-87] Czujnik 1
- ☐ [00-1B-9D-0A-F1-87] Czujnik 2

Powiązane czynniki - dostęp niedozwolony

- ☐ [00-1B-9D-0A-F1-87] Czujnik 1
- ☐ [00-1B-9D-0A-F1-87] Czujnik 2

Powiązane czynniki - dyskretny alarm

- ☐ [00-1B-9D-0A-F1-87] Czujnik 1
- ☐ [00-1B-9D-0A-F1-87] Czujnik 2

Seria 3000

Szukaj [Aa] [X] [F] [P]

Urządzenia | **Grupy**

- Wyjścia sterujące
 - Wyjście sterujące 1**
 - Wyjście sterujące 2
 - Wyjście sterujące 3
 - Wyjście sterujące 4
 - Wyjście sterujące 5

Nazwa: Wyjście sterujące 1

Tryb pracy: Normalny

Stan w trybie offline: Bez zmian

Czas włączenia: 3 s

Harmonogram tygodniowy włączenia: Nigdy

Wyłączenie przełączenia w dni świąteczne: Brak dni świątecznych

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 (przekazniki) są zsynchronizowane z wyjściami sterującymi zamek elektryczny i mogą służyć na przykład do podłączenia sterowania diodami LED na czujnikach. Zalecane w przypadku gdy potrzebny jest impuls sterujący diodą LED podczas występowania 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 przekaznika.

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.

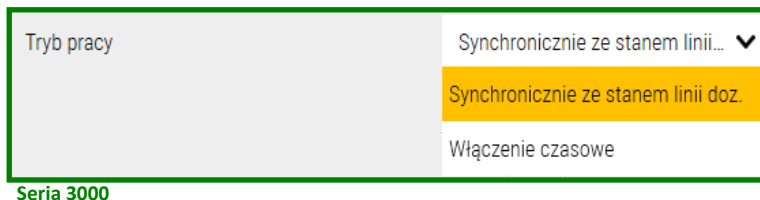
Harmonogram tygodniowy włączenia - z rozwijanej listy można wybrać zdefiniowany uprzednio terminarz zgodnie, z którym wyjście będzie automatycznie przełączać.

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



Tryb pracy

Synchronicznie ze stanem linii... ▼

Synchronicznie ze stanem linii doz.

Włączenie czasowe

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)



Tryb pracy

Włączenie czasowe ▼

Czas trwania alarmu

– 10 + 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



Czas włączenia

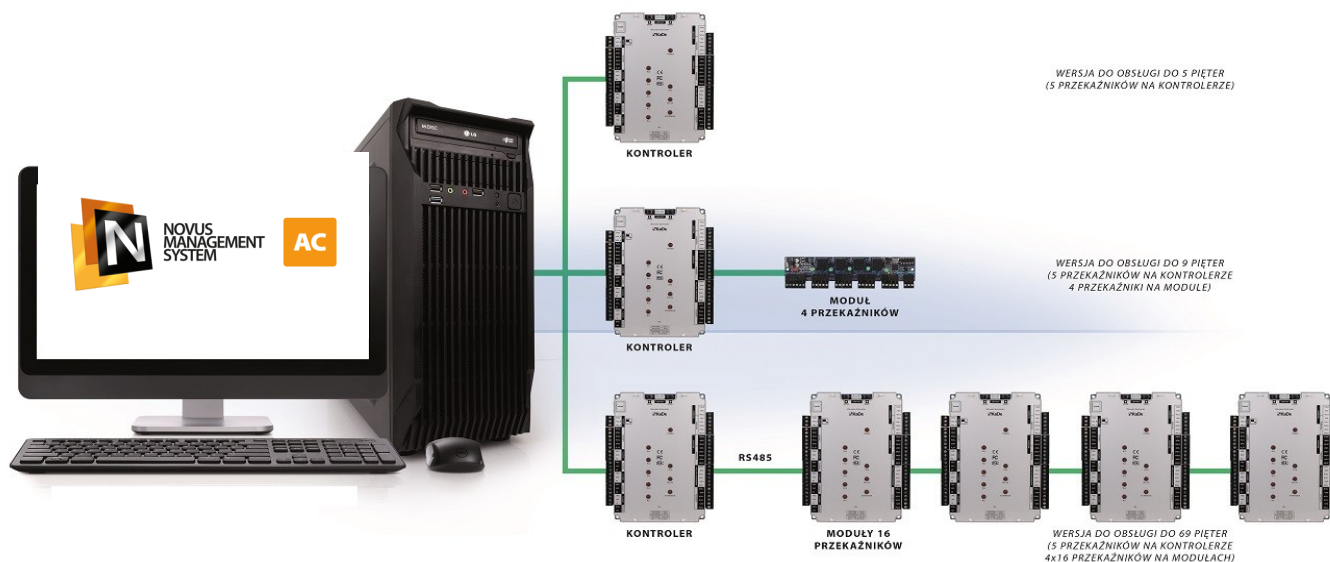
– 3 + s

Seria HID®

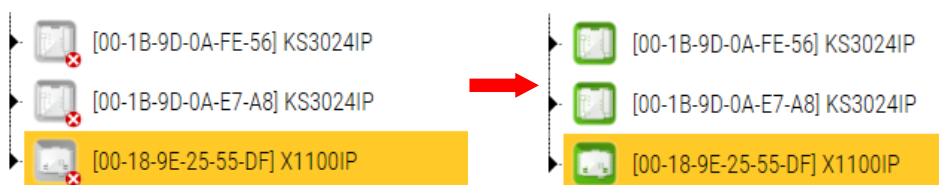
3.6 Urządzenia - Kontrola dostępu - Kontroler windy

Seria 3000

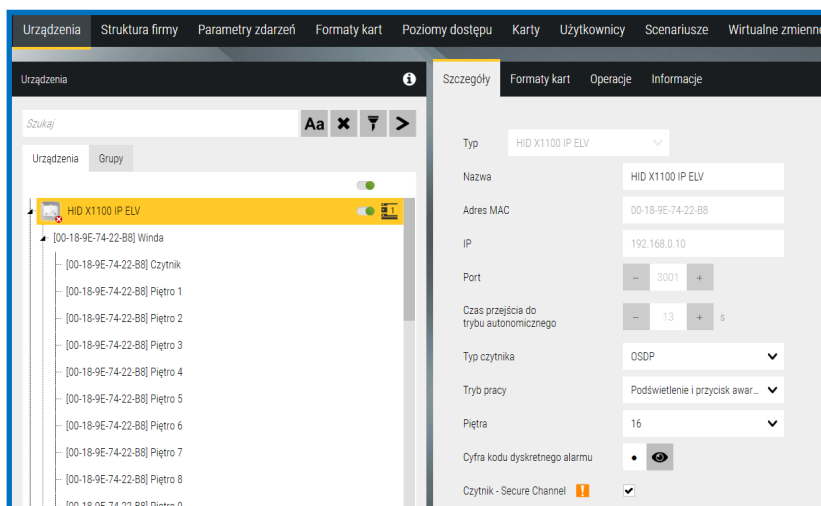
W przypadku kontrolera KDH-KS3000-IP-ELV można również dodać moduły rozszerzające. Do wyboru mamy dwa typy modułów. W zależności od ilości pięter jakie ma obsłużyć winda mamy następujące kombinacje.



Po wykonaniu wszystkich ustawień dla każdego z kontrolerów (analogicznie jak w przypadku dodawania kontrolerów w trybie off-line), należy kliknąć na ikonę **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** zmieniają 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

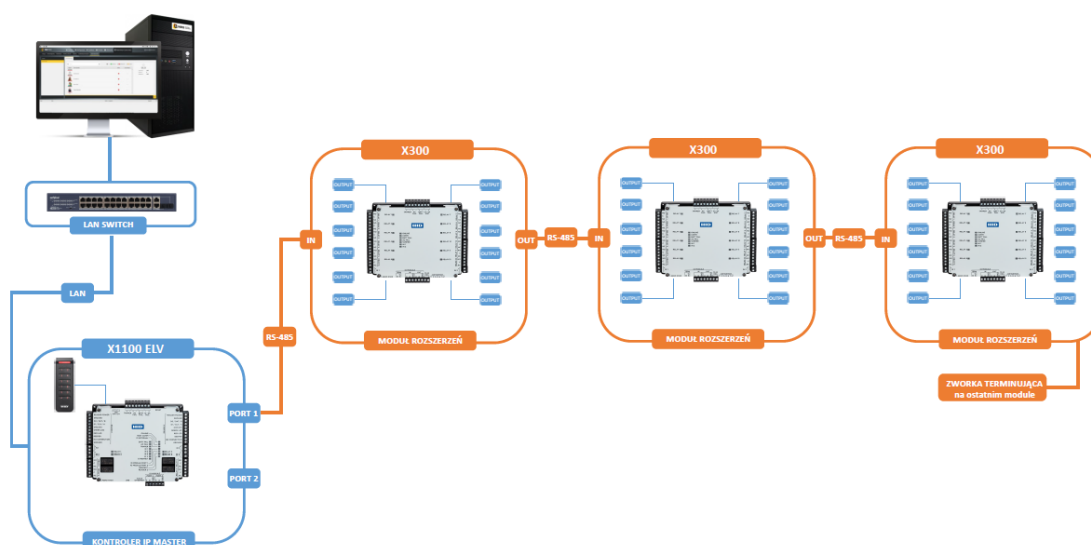
Piętra - wybór od 1 do 128 pięter na jednej magistrali z wykorzystaniem modułów rozszerzeń X300 i X200

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 alarmu

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 windy - 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 windy - 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:

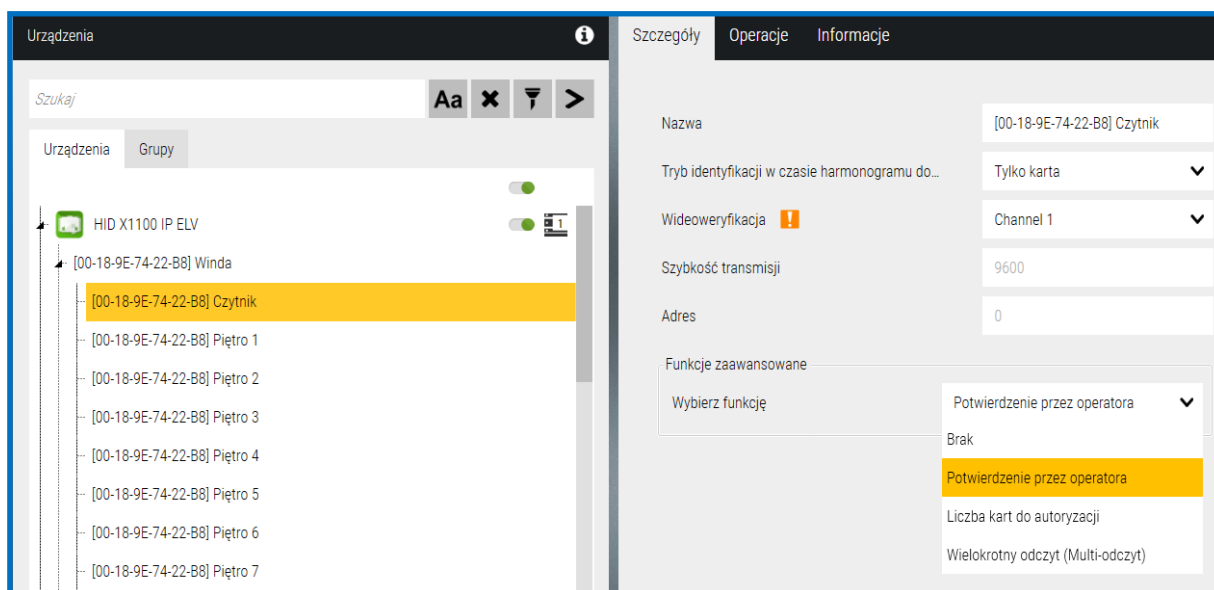
Tryb identyfikacji poza czasem aktywnym - z rozwijanej listy można wybrać:

(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.

Wideoverifyfikacja - 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

Wideoverifyfikacja - umożliwia przypisanie do czytnika zainstalowanej nad nim kamery

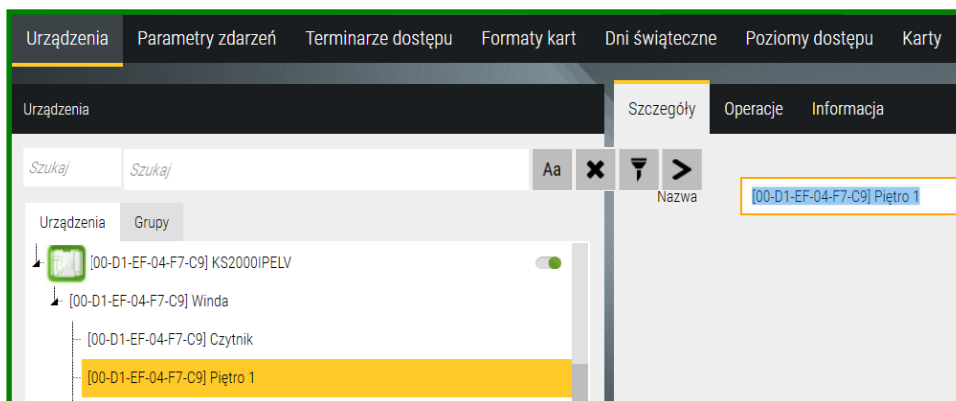
Szybkość transmisji i Adres - Ustawienia wymagane przy konfiguracji czytników - **tylko dla czytników OSDP**

Funkcje zaawansowane:

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

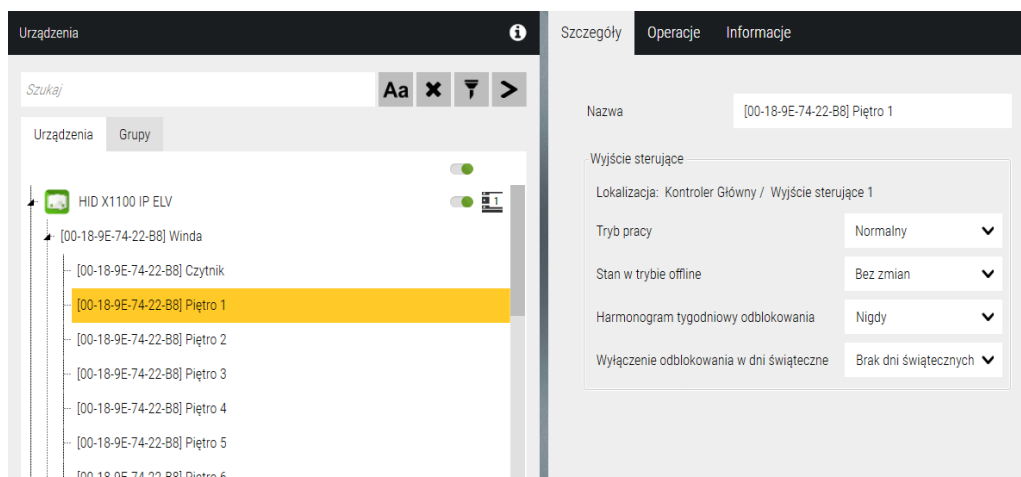
3.9 Urządzenia - Kontrola dostępu - Kontroler windy - Winda - Piętro

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

Nowe urządzenie

Nowe urządzenie	Telewizja Dozorowa ▼
Typ	NVIP 6000 ▼
Model	NVIP-2H-6732M/LPR
Nazwa	NVIP-2H-6732M/LPR_GORA_wjazd
Adres	192.168.43.55
Użytkownik	root
Hasło	●●●●●●●●
Port WWW	– 80 +
Port RTSP	– 554 +
Port zdarzeń	– 0 +
Metoda zdarzeń	BaseSubscription ▼
Łączenie urządzenia na żądanie	☐

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 dyskietkę 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*.

NVR6304P4-H1-II 1

TEST

Strumień 1

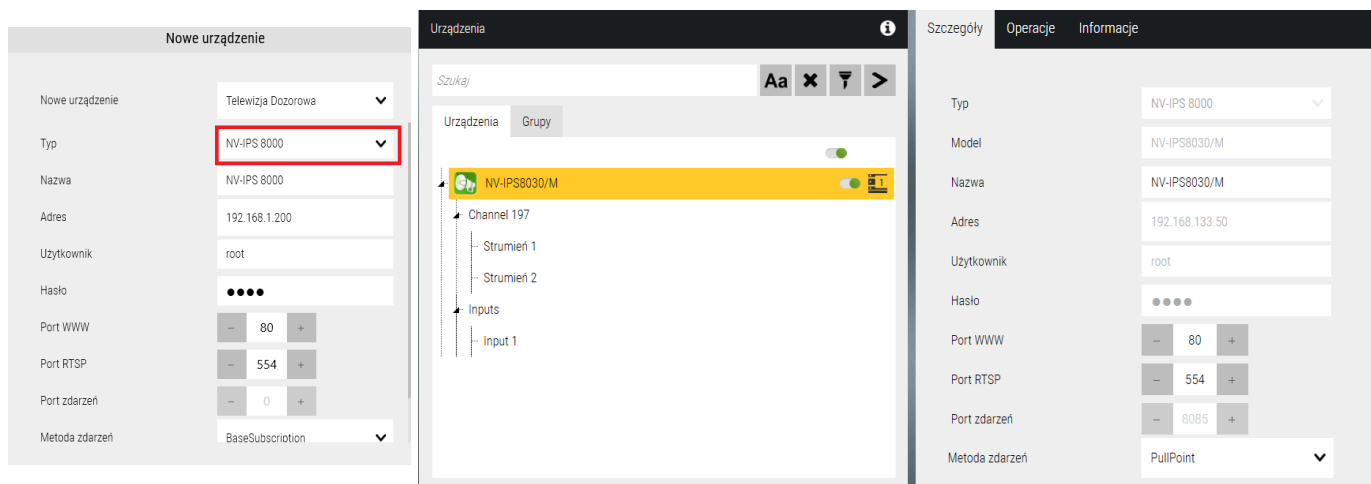
Strumień 2

Nazwa TEST

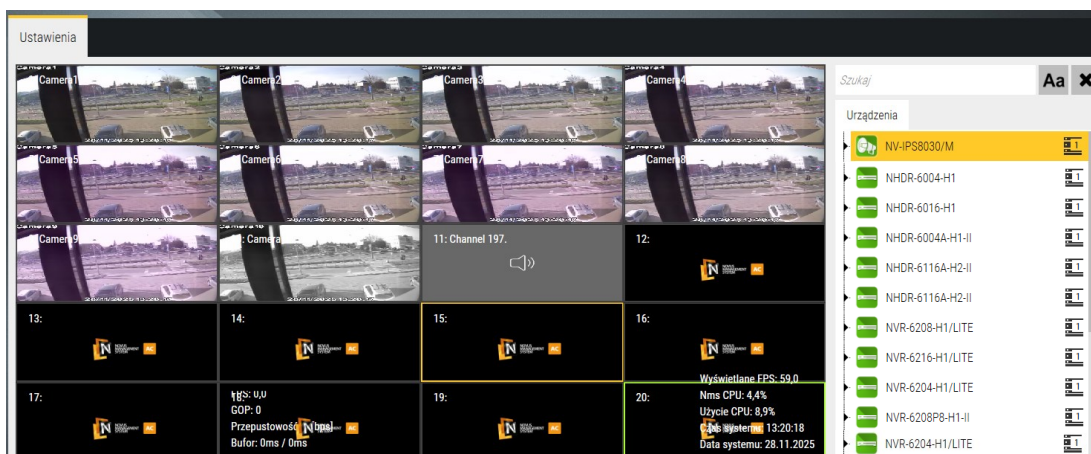
Użyj tylko strumienia głównego ☐

3.11 Urządzenia - Głośniki IP

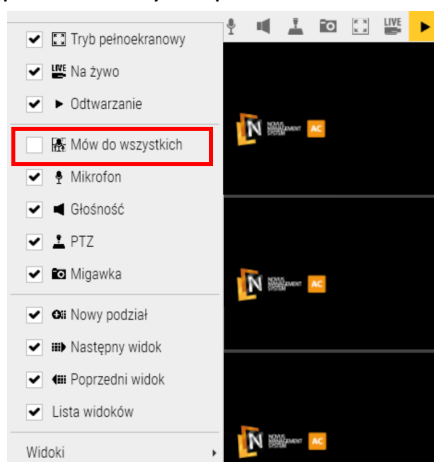
Oprogramowanie NOVUS MANAGEMENT SYSTEM AC umożliwia korzystanie z głośników IP. Głośniki IP zapewniają dwukierunkową komunikację audio oraz odtwarzanie komunikatów głosowych. Wygłoszenie komunikatów można zaplanować poprzez utworzenie odpowiedniego scenariusza.



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.

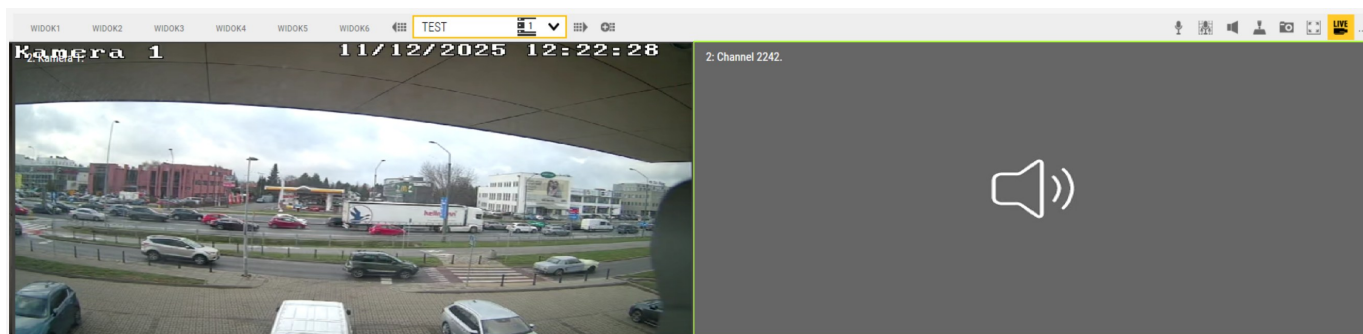


Aby korzystać ze wszystkich funkcji głośnika, należy dodać nową ikonę do narzędzia *Wideo* znajdującego się na panelu. Opcja *Mów do wszystkich* jest domyślnie ukryta. Aby ją włączyć, należy prawym przyciskiem myszy kliknąć górny pasek narzędzi *Wideo*, a następnie zaznaczyć odpowiedni checkbox.



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.

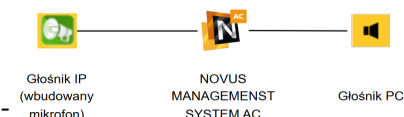


Tryby pracy:

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



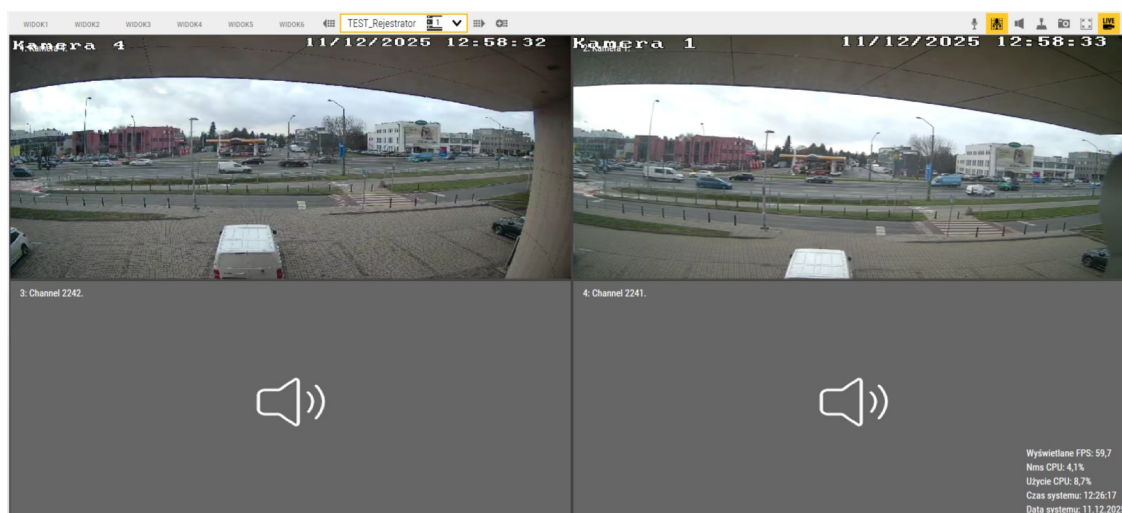
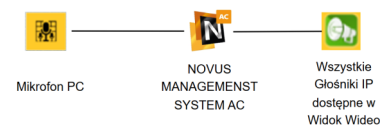
Głośnik (odstuch audio) - umożliwia odstuch dźwięku z głośnika IP (nadawanie dźwięku poprzez wbudowany mikrofon) do zewnętrznego głośnika (podłączony do komputera).



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



Wyłączenie komunikatu za pomocą scenariusza

Aby zdefiniować scenariusz polegający na wyłączeniu 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 *Wyłącz 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:

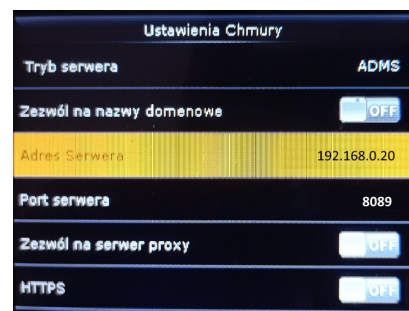
Konfiguracja terminala rejestracji czasu pracy.

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 działał 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 - konfiguracja* i zdefiniować datę oraz czas początku oraz końca zmiany czasu. Standardowo jest to ostatnia niedziela października o godzinie 3:00 oraz ostatnia niedziela marca o godzinie 2:00.

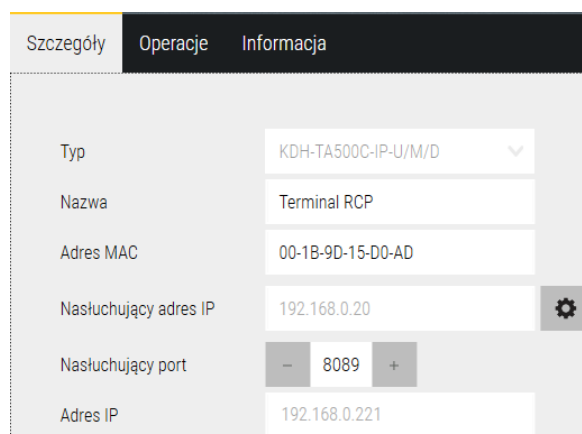
Ustawienia adresu IP terminala

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)

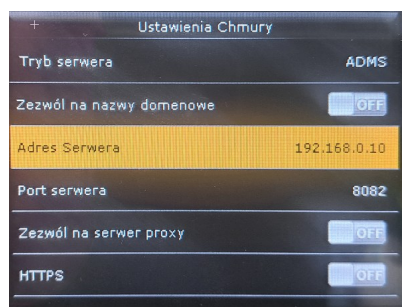


Po kliknięciu na ikonie **Komunikacja** należy zaznaczyć poz. **Ethernet** i kliknąć **OK** w polu kursorów - prawy górny róg terminala.

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 łączący się terminal. Tylko ta pozycja jest potrzebna do współpracy z NOVUS MANAGEMENT SYSTEM AC.

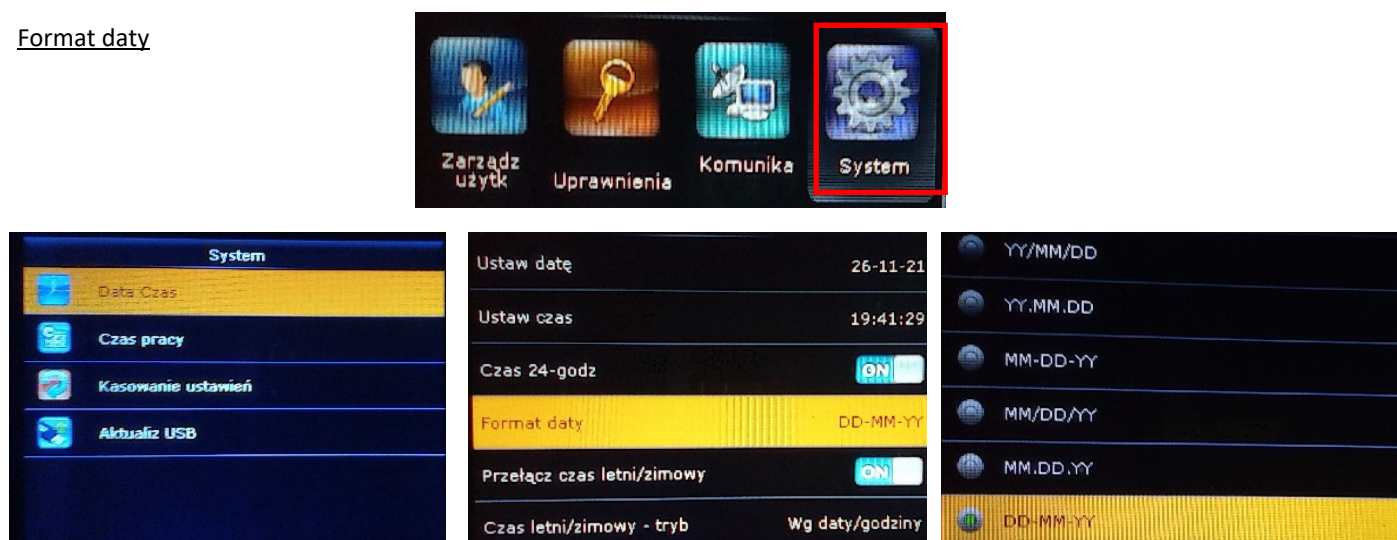


Przyciskiem **ESC** na klawiaturze wychodzimy z menu.

Wybór języka

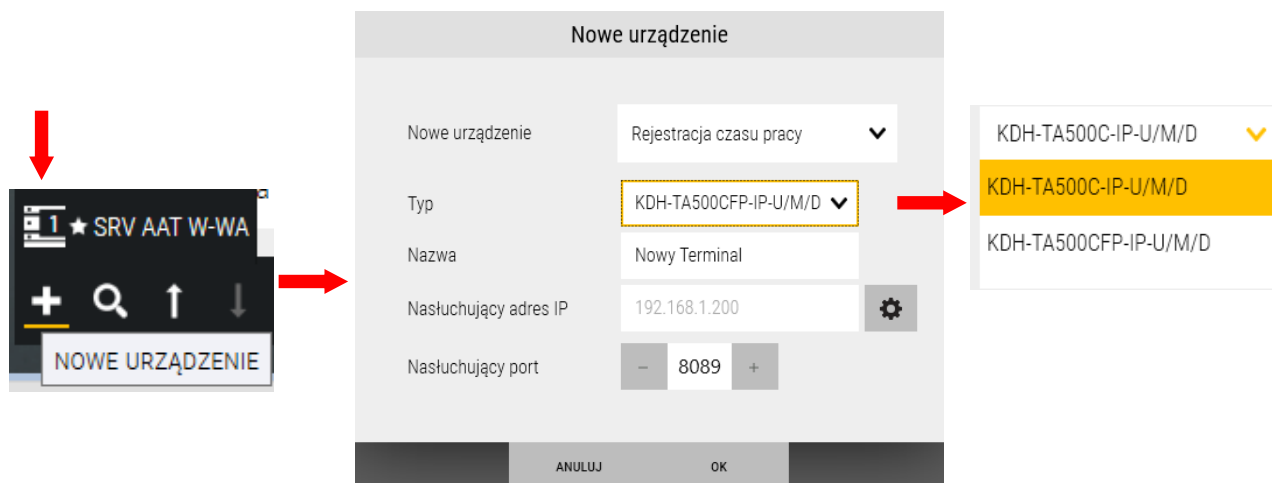
Po kliknięciu na ikonie **Personalizacja** należy zaznaczyć poz. *Interfejs użytkownika*, a w następnym oknie **Język**.

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.

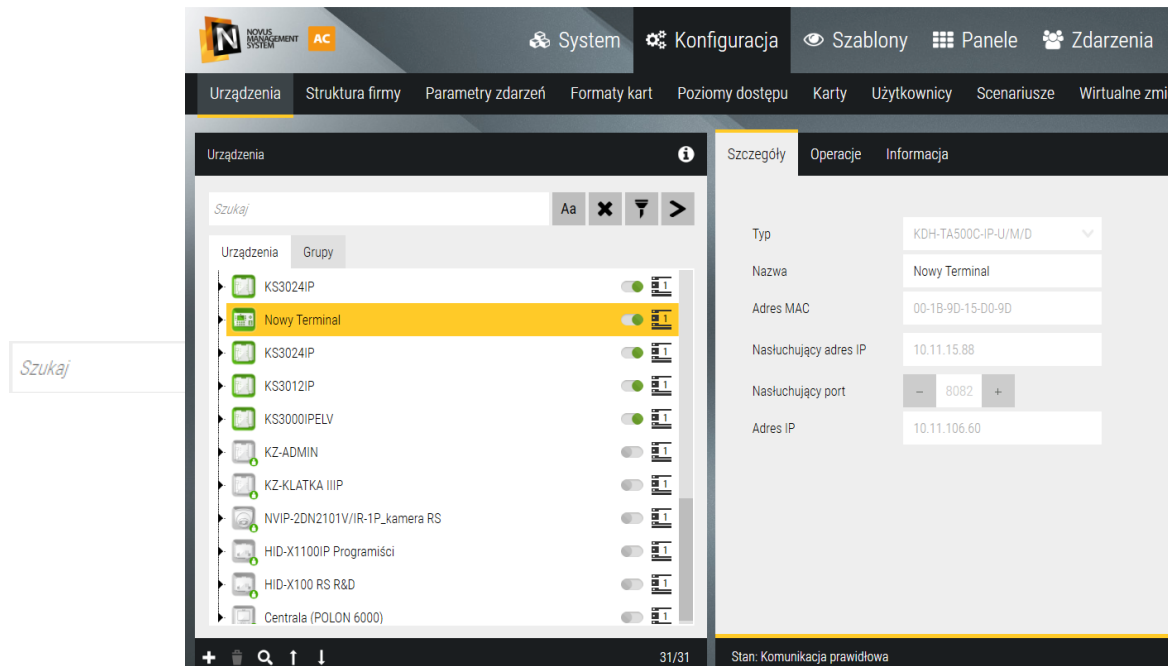
Typ - w pierwszej kolejności należy wybrać typ urządzenia z rozwijanej listy jak powyżej. Do wyboru: model: KDH-TA500C-IP-UMD lub KDH-TA500CFP-IP-UMD ze skanerem biometrii.

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.

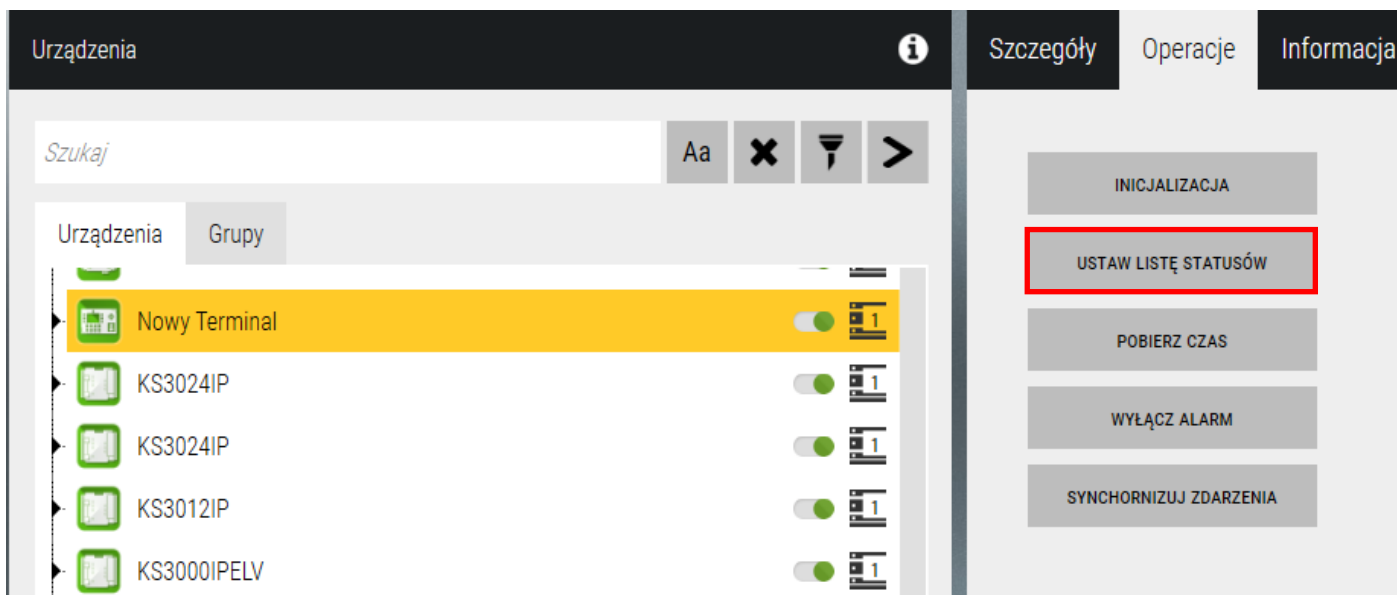
Od tego momentu wejście do menu terminala wymaga użycia hasła administratora.

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.

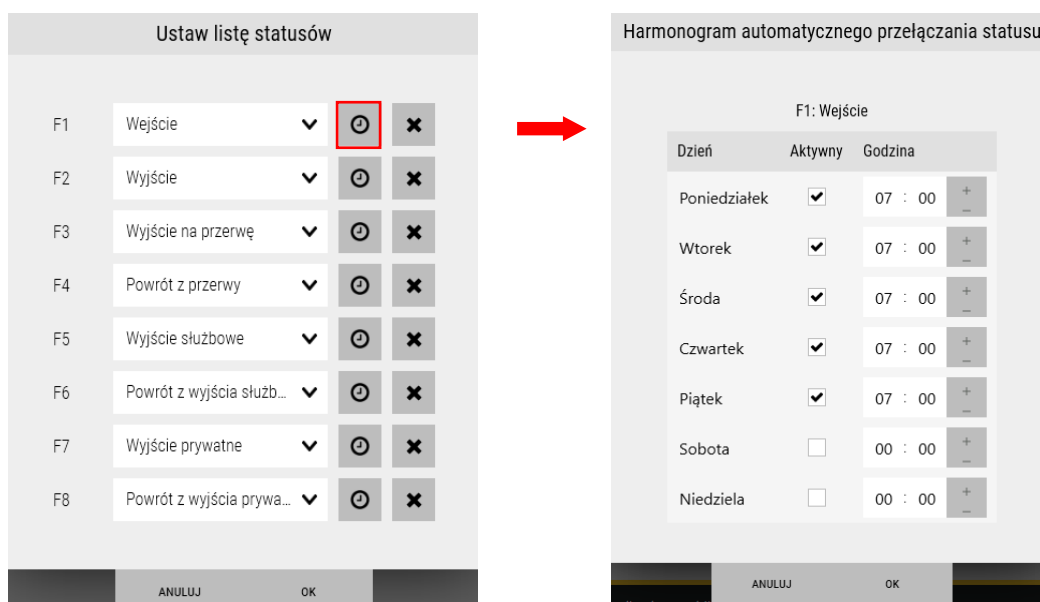
Dodawanie odcisków palców do terminala FP poprzez skaner USB opisane jest w zakładce *Użytkownicy*.

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 w bazie programu co objawia się brakiem tych zdarzeń w raporcie RCP.

The screenshot shows the main interface of the NOVUS MANAGEMENT SYSTEM AC. The top bar has three tabs: 'Urządzenia' (selected), 'Szczegóły', 'Operacje', and 'Informacja'. Below the 'Urządzenia' tab, there is a search bar and a list of devices. The device 'Terminal testowy #1' is highlighted in yellow. To the right, the 'Operacje' tab is active, showing a list of operations. The 'SYNCHRONIZUJ ZDARZENIA' button is highlighted with a red rectangle.

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

The dialog box titled 'Synchronizuj zdarzenia' contains the following fields and buttons:

- Od:** 14.03.2023 15:08 (with a calendar icon)
- Do:** 15.03.2023 15:08 (with a calendar icon)
- Powiadomienia:** ☐
- Buttons:** ANULUJ, OK

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 pracowników. Warto je włączyć jeżeli sytuacja dotyczy dnia bieżącego i brak powiadomień z rana. Po kliknięciu **OK** na panelu ze stosiem 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**.

The dialog box titled 'Nowe urządzenie' contains the following fields and buttons:

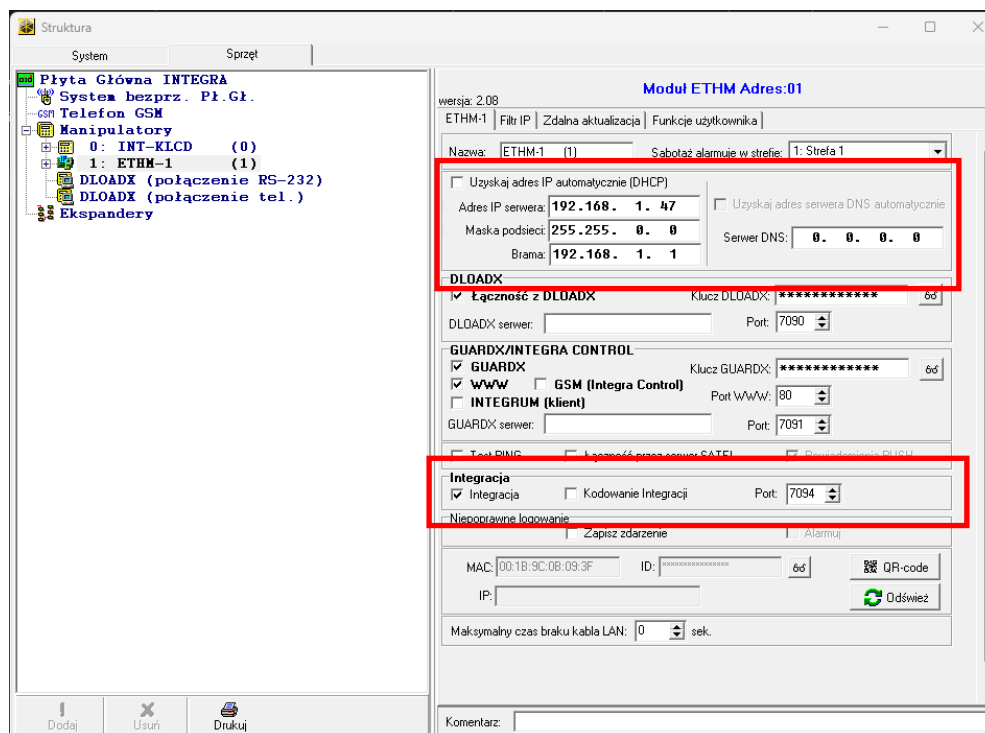
- Nowe urządzenie:** Drukarka (dropdown menu)
- Typ:** Sieciowa (dropdown menu)
- Nazwa:** Drukarka termiczna POS
- IP:** 192.168.123.100
- Buttons:** ANULUJ, OK

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	Integra	
IP	192.168.1.47	
Port	7094	
Czas ważności pierwszego kodu	00 : 01 : 00 gg:mm:ss	
Minimalna długość kodu dla nowego użytkownika (skonfigurowana w centrali)	4	
Liczba partycji	2	
Czy w systemie są prefiksy?	☒	
Partycja	Prefiks	Kod administratora
Partycja 1		
Partycja 2		

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 dyskiecie 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.

Nazwa	Integra	
IP	192.168.1.47	
Port	- 7094 +	
Czas ważności pierwszego kodu	00 : 01 : 00 + - gg:mm:ss	
Minimalna długość kodu dla nowego użytkownika (skonfigurowana w centrali)	4 ▼	
Liczba partycji	2 ▼	
Czy w systemie są prefiksy?	☒	
Partycja	Prefiks	Kod administratora
Partycja 1	••	••••
Partycja 2	••	••••

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

Nowe urządzenie	
Nowe urządzenie	System sygnalizacji pożarowej ▼
Typ	Centrala ▼
Nazwa	Centrala (POLON 6000)
IP	192.168.1.1
Port danych	502
Widok elementów liniowych	według linii ▼
ANULUJ OK	

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

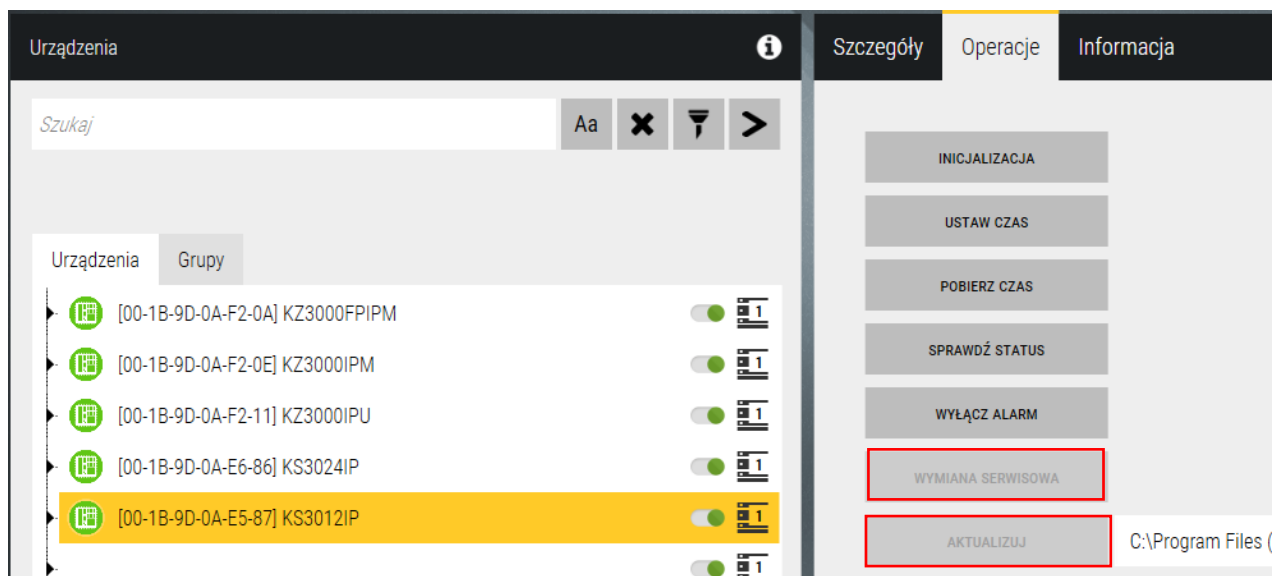
B) Wczytanie konfiguracji wyeksportowanej z centrali

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

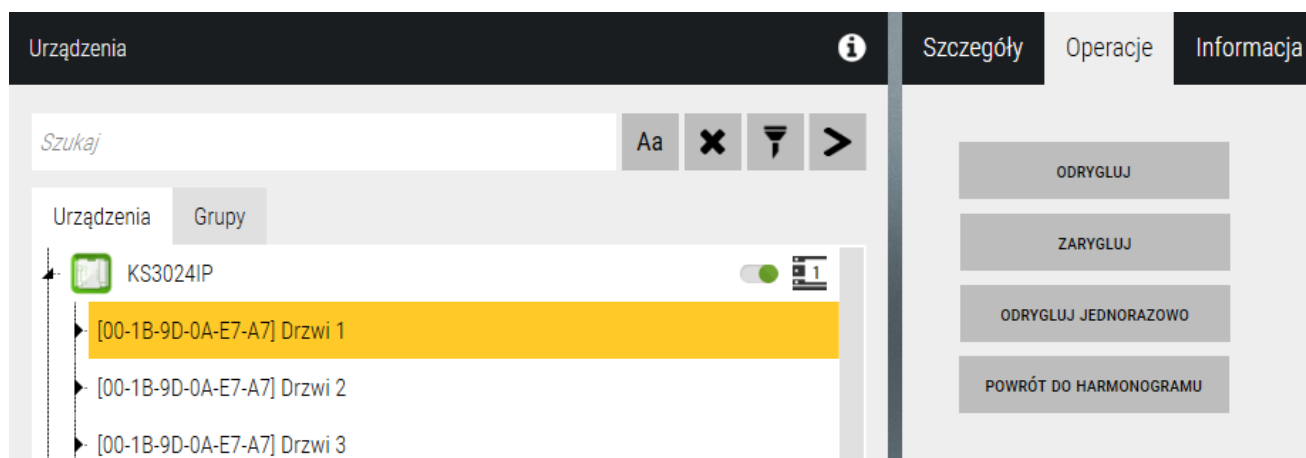


Nowe przyciski:

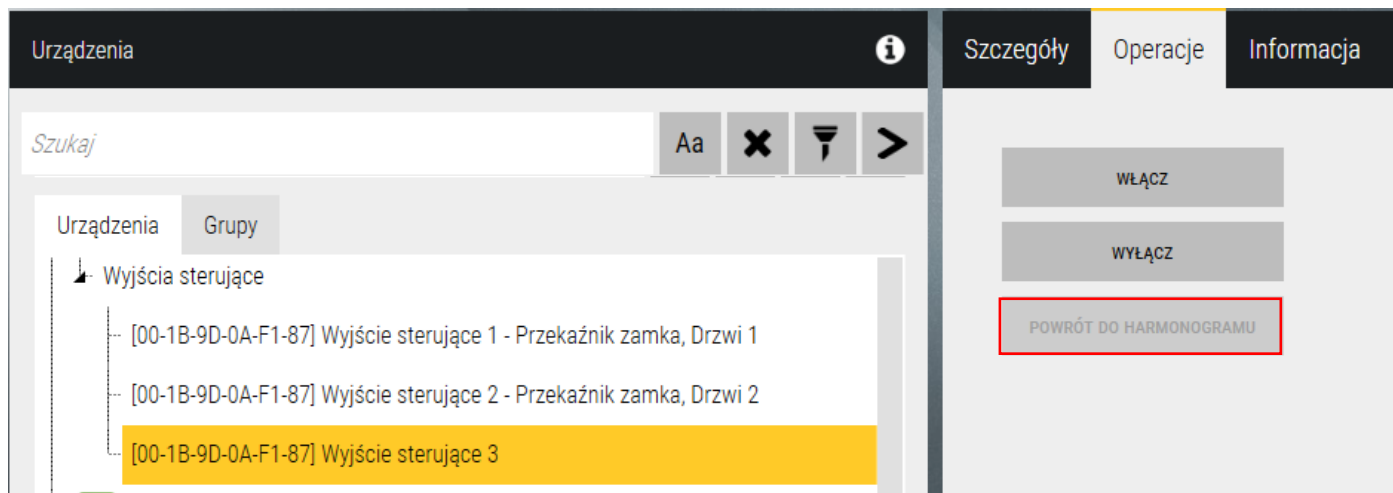
„WYMIANA SERWISOWA” - pozwala wymienić kontroler na nowy, który należy podłączyć z takim samym adresem IP

„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


Urządzenia

Szukaj

Urządzenia Grupy

KS3000IPELV

[00-1B-9D-0A-E5-86] Winda

[00-1B-9D-0A-E5-86] Czytnik

[00-1B-9D-0A-E5-86] Piętro 1

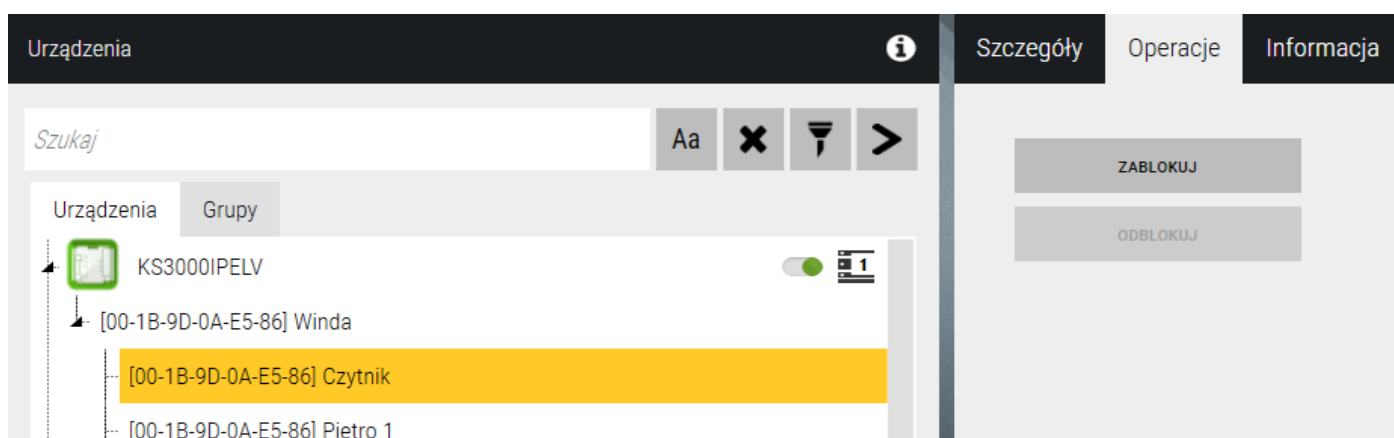
Szczegóły Operacje Informacja

ODBLOKUJ WSZYSTKIE PIĘTRA

ZABLOKUJ WSZYSTKIE PIĘTRA

ODBLOKUJ JEDNORAZOWO

POWRÓT DO HARMONOGRAMU

Czytnik


Urządzenia

Szukaj

Urządzenia Grupy

KS3000IPELV

[00-1B-9D-0A-E5-86] Winda

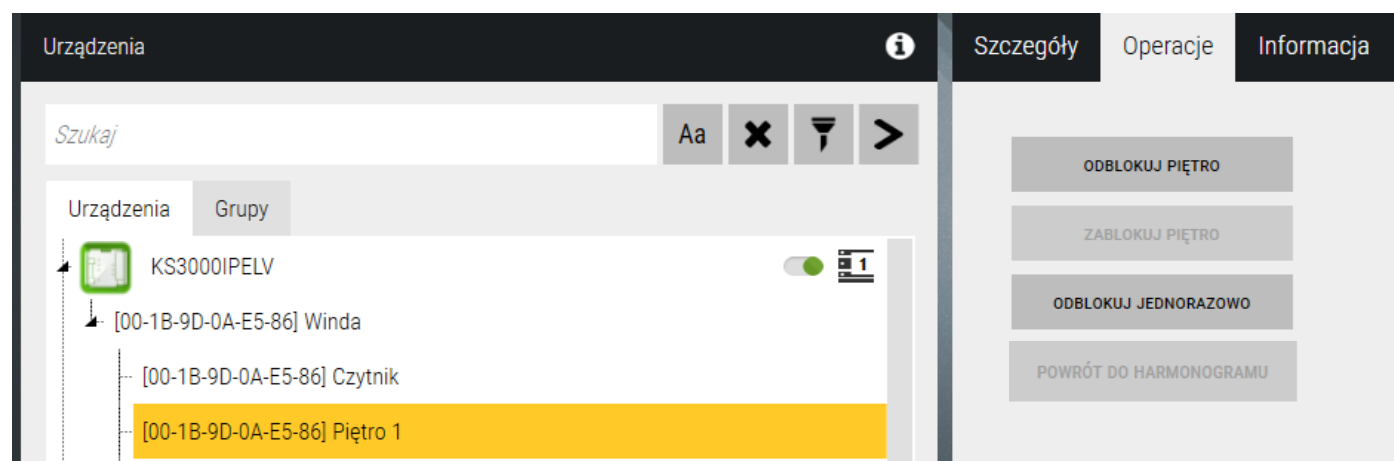
[00-1B-9D-0A-E5-86] Czytnik

[00-1B-9D-0A-E5-86] Piętro 1

Szczegóły Operacje Informacja

ZABLOKUJ

ODBLOKUJ

Piętro


Urządzenia

Szukaj

Urządzenia Grupy

KS3000IPELV

[00-1B-9D-0A-E5-86] Winda

[00-1B-9D-0A-E5-86] Czytnik

[00-1B-9D-0A-E5-86] Piętro 1

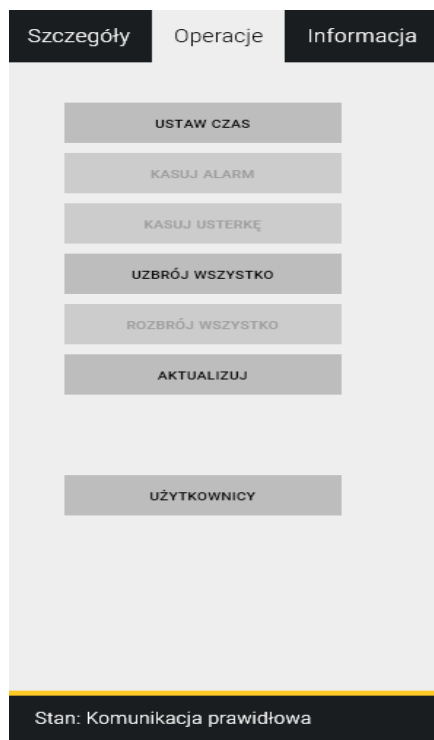
Szczegóły Operacje Informacja

ODBLOKUJ PIĘTRO

ZABLOKUJ PIĘTRO

ODBLOKUJ JEDNORAZOWO

POWRÓT DO HARMONOGRAMU

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.

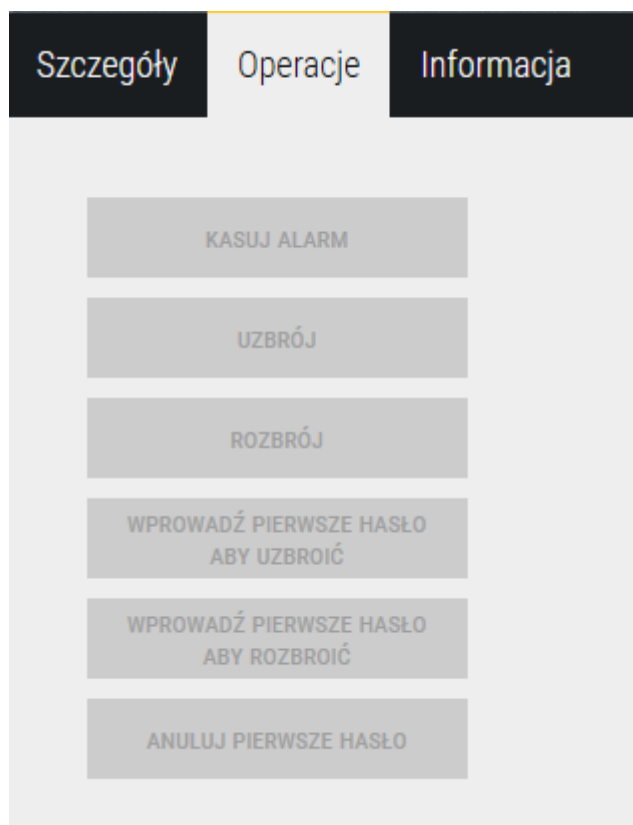
Użytkownicy - w tym oknie można sprawdzić wszystkich użytkowników centrali, zarówno dodanych przez NOVUS MANAGEMENT SYSTEM AC jak i klawiaturę/DLOADX.

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.

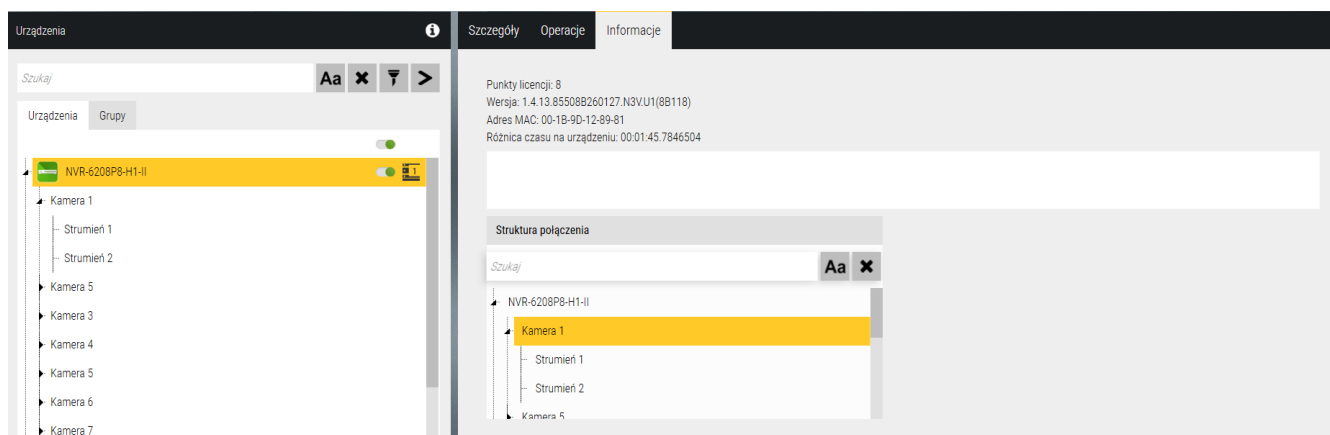
Wprowadź pierwsze hasło aby rozbroić - przycisk wprowadza pierwsze hasło aby rozbroić dla odpowiednio skonfigurowanej strefy. Czas ważności pierwszego hasła ustawiany jest przy dodaniu centrali.

Anuluj pierwsze hasło - przycisk anuluje wprowadzenie pierwszego hasła.

3.17 Urządzenia - Informacje

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

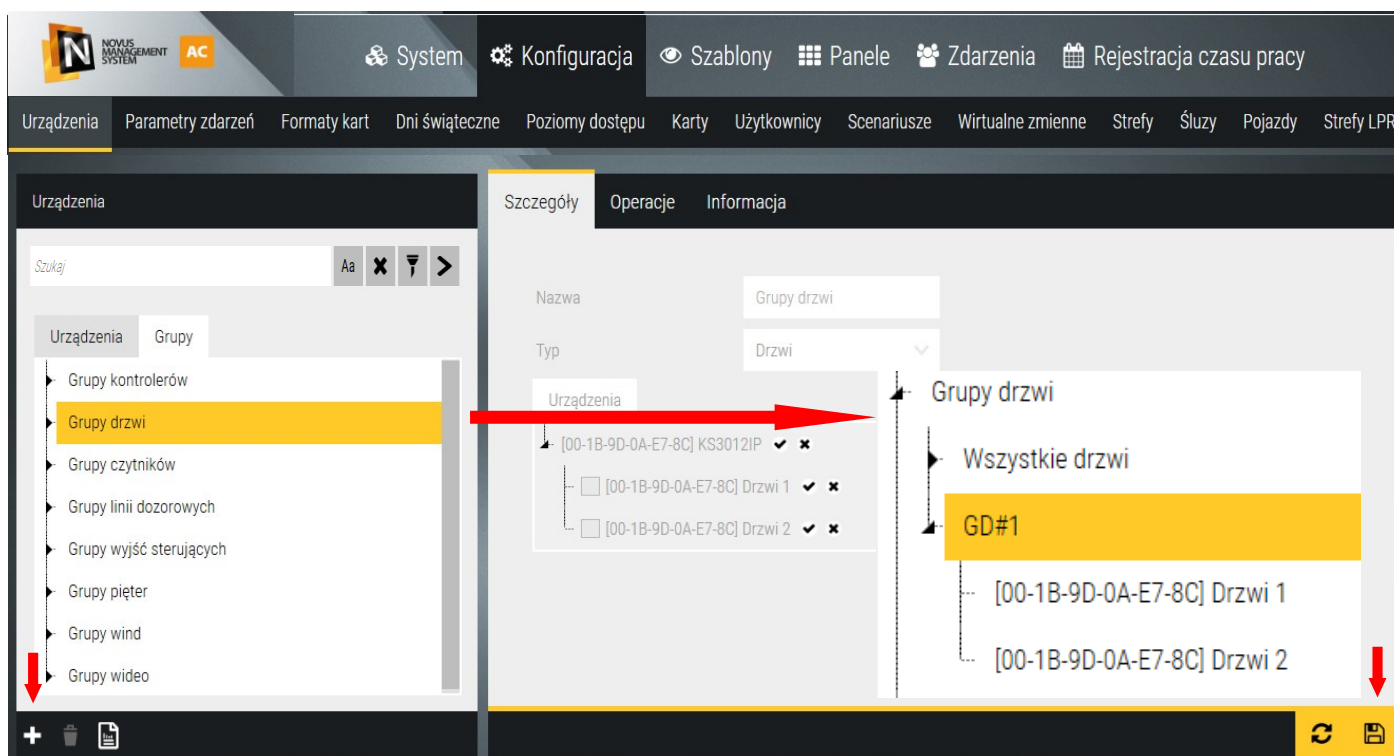
- Liczba punktów licencji pobieranych przez dany element.
- Wersja oprogramowania (firmware) urządzenia.
- Adres MAC urządzenia.
- Informacja o różnicy czasu pomiędzy urządzeniem a serwerem systemu.
- Struktura połączenia urządzenia przedstawiona w formie rozgałęzionej listy.
- Pole opisu, w którym można 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.

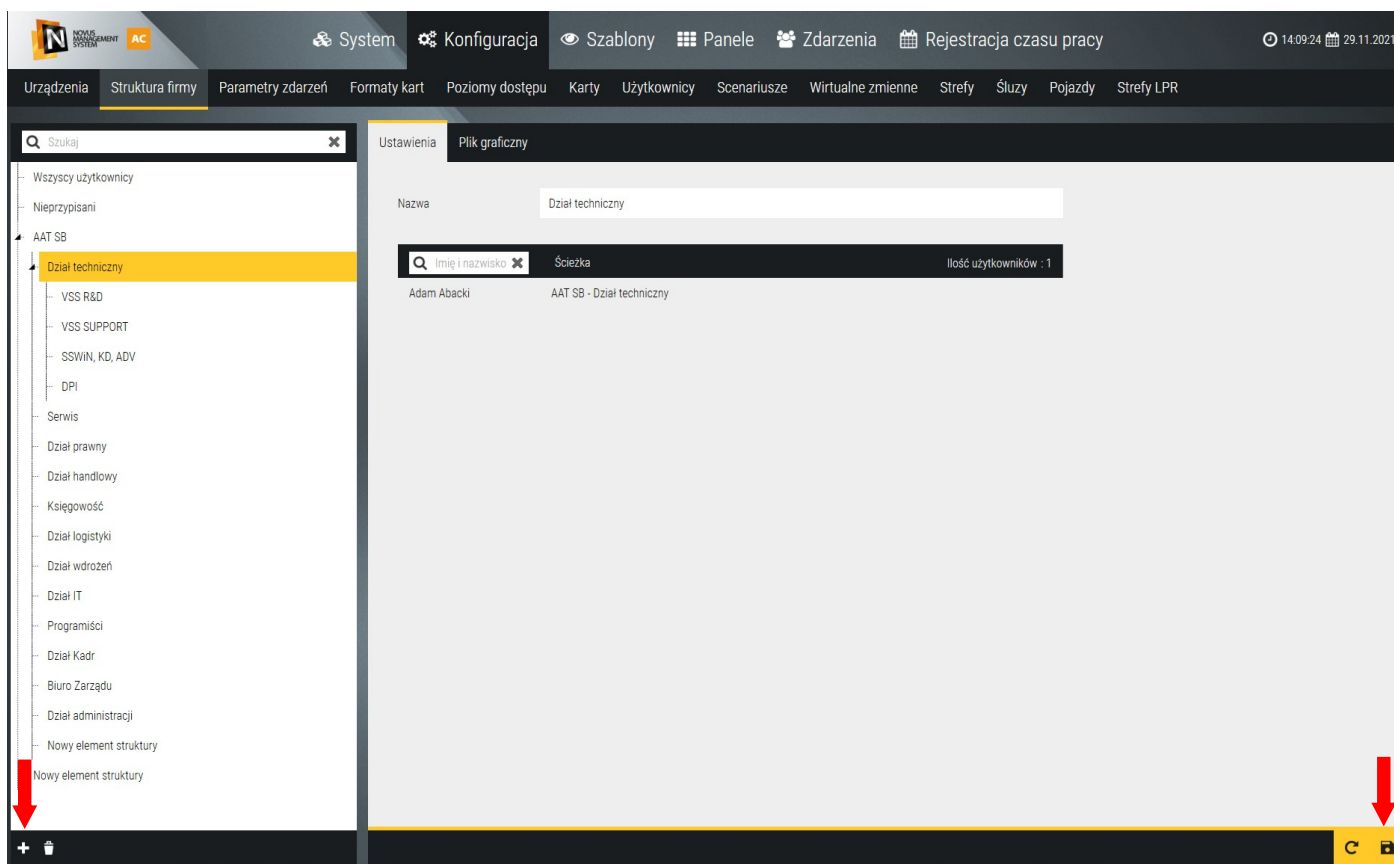
Aby dodać nową grupę w drzewie głównym nie może być zaznaczona żadna z grup. Jeżeli jest takie zaznaczenie (żółty pasek) to należy kliknąć na nim trzymając równocześnie naciśnięty przycisk **CTRL**. Grupa dodana w drzewie głównym może zawierać elementy różnych typów. Można to wykorzystać do tworzenia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



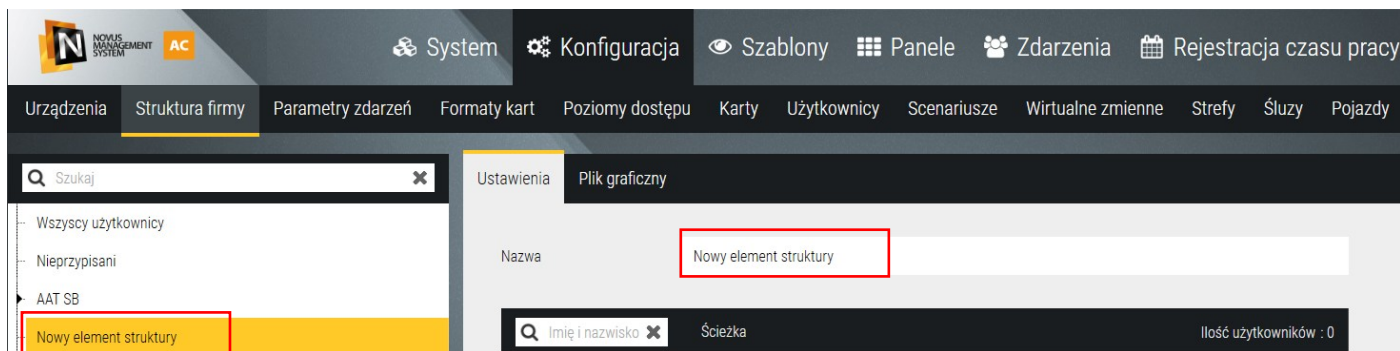
Wszyscy - wyświetla w prawym oknie listę wszystkich użytkowników dodanych do bazy

Nieprzypisani - wyświetla w prawym oknie listę użytkowników nieprzypisanych do struktury

Po dodaniu użytkowników (ręcznie lub poprzez import) obie listy są takie same.

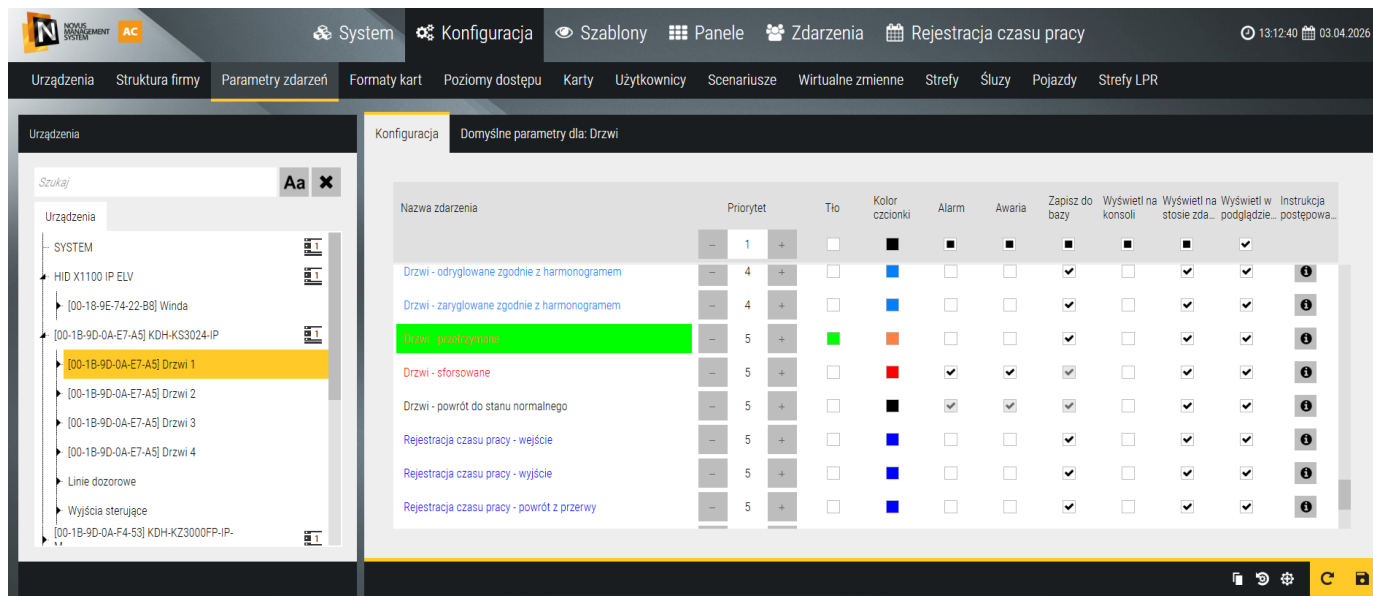
Aby dodać strukturę firmy należy kliknąć na przycisku **Dodaj** w lewym dolnym rogu.

W drzewie pojawi się nowa pozycja. Żeby dodać nową pozycję 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.

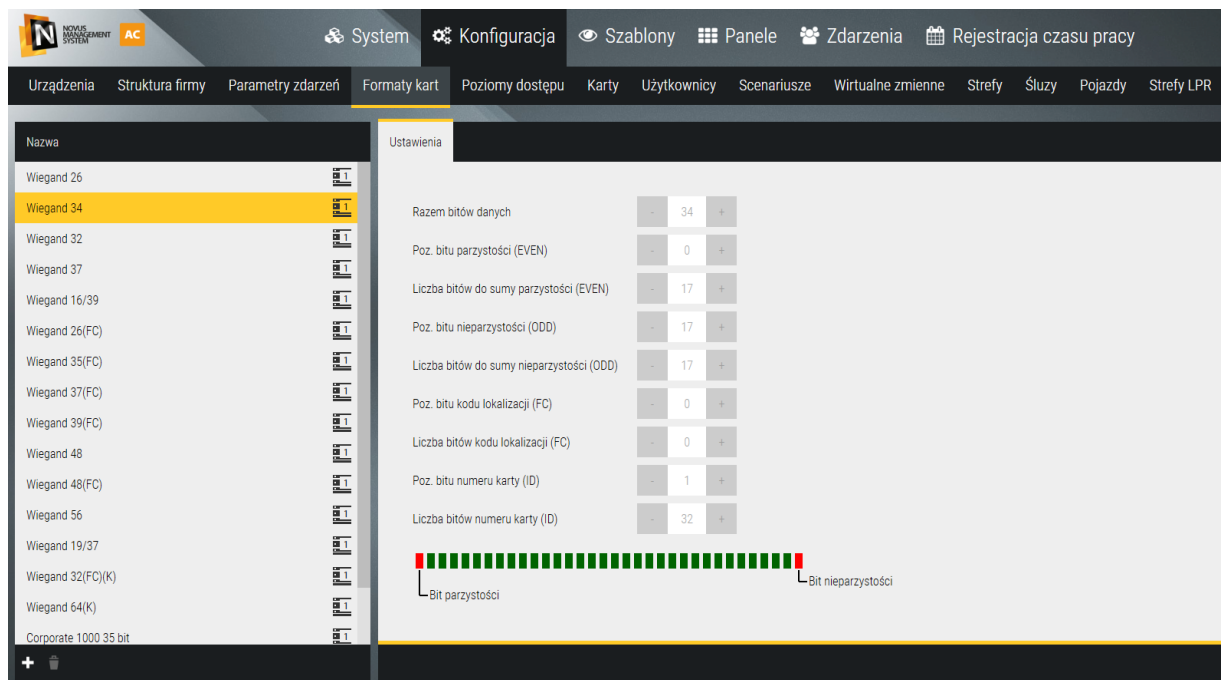
Priorytet - określenie wartości priorytetu od 1 do 5 (5 - najwyższy priorytet zdarzenia)

Tło - kolor tła wyświetlanych logów zdarzeń

Kolor czcionki - kolor czcionki wyświetlanych logów zdarzeń

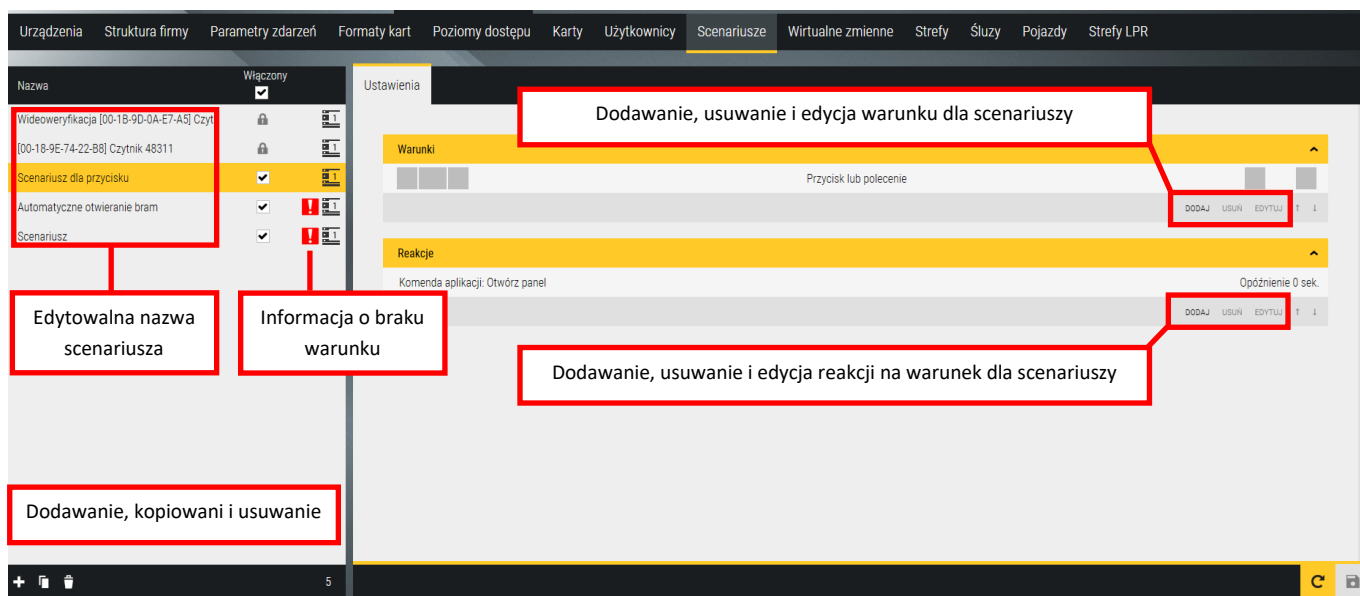


3.21 Konfiguracja - Formaty kart



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.

The screenshot shows the 'Warunki' configuration window. The 'Odpowiedź na' (Response to) dropdown is set to 'Harmonogram'. The 'Spójnik logiczny' (Logical connector) is set to 'LUB' (OR). The 'Harmonogram' section contains a list of time-based conditions with checkboxes: 'Never', 'Always', 'Pn-PT 8-16', 'Codziennie 7-9 i 15-16' (checked), 'Sobota', and 'Niedziela'.

The screenshot shows the 'Warunki' configuration window. The 'Odpowiedź na' dropdown is set to 'Święto'. The 'Spójnik logiczny' is set to 'LUB'. The 'Święto' section contains a list of holiday-based conditions with checkboxes: 'Święta 2025', 'Święta 2026' (checked), and 'Święta 2027'.

Harmonogram- ustawienia warunków według skonfigurowanych harmonogramów czasowych.

Święta - ustawienie warunków według skonfigurowanych dni świątecznych.

The screenshot shows the 'Warunki' configuration window. The 'Odpowiedź na' dropdown is set to 'Przycisk lub polecenie' (highlighted with a yellow border). The 'Spójnik logiczny' is set to 'LUB'. The main area is labeled 'Przycisk lub polecenie'.

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

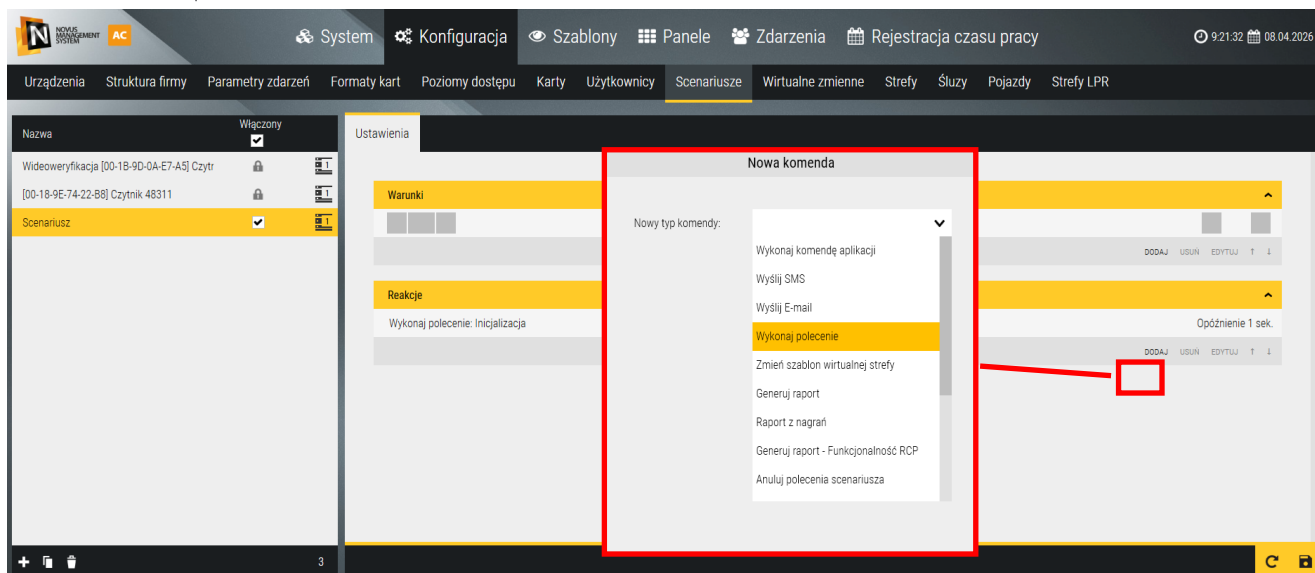
The screenshot shows the 'Warunki' configuration window. The 'Odpowiedź na' dropdown is set to 'Zmiana wartości zmiennej' (highlighted with a yellow border). The 'Spójnik logiczny' is set to 'LUB'. The main area is labeled 'Zmiana wartości zmiennej'.

Zmiana wartości zmiennej - ustawienie warunku na zmianę wartości zmiennej.

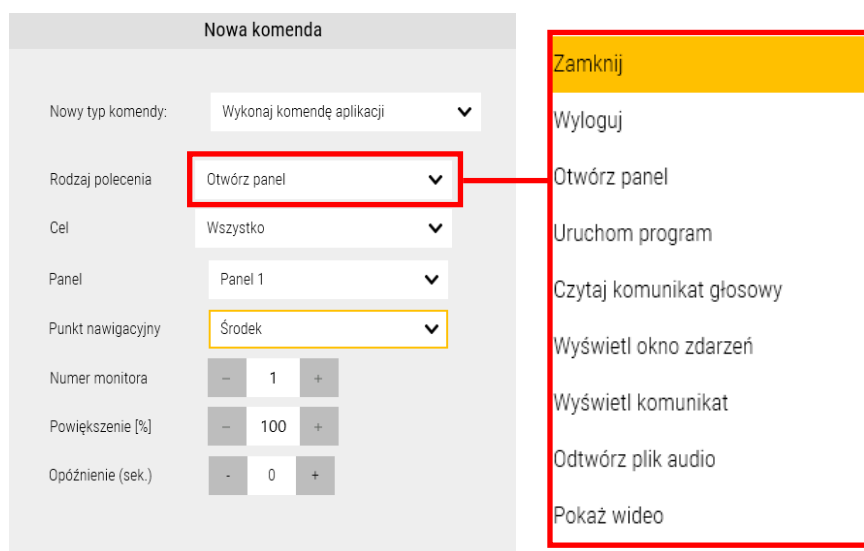
Zmiana szablonu wirtualnej strefy - ustawienie warunku dotyczącego zmiany szablonu wirtualnej strefy, wymaga wcześniejszego skonfigurowania wirtualnej strefy.

Wyzwalacz - ustawiamy warunek dotyczący wyzwalacza.

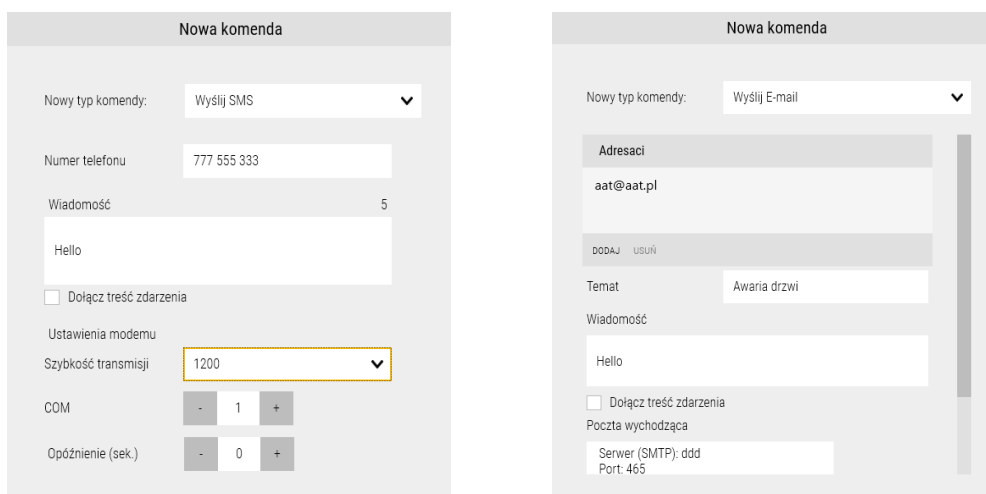
Zdarzenie strefy - określamy warunek dla wystąpienia konkretnego zdarzenia dotyczącego strefy Strefa pusta, Strefa zajęta, Strefa pełna lub Strefa przepełniona.



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 wystania wiadomości tekstowej SMS lub e-mail.

Nowa komenda

Nowy typ komendy:

Wykonaj polecenie

Polecenie

Zarygluj

Szukaj

Aa X 🔍 ➤

Urządzenia

☐ [00-1B-9D-0A-E7-A5] KDH-KS3024-IP

☒ [00-1B-9D-0A-E7-A5] Drzwi 1

☐ [00-1B-9D-0A-E7-A5] Drzwi 2

☐ [00-1B-9D-0A-E7-A5] Drzwi 3

☐ [00-1B-9D-0A-E7-A5] Drzwi 4

Opóźnienie (sek.)

- 0 +

Inicjalizacja	Zarygluj	Odblokuj piętro	Włącz czasowo
Ustawianie czasu	Odrygluj jednorazowo	Zablokuj piętro	PTZ
Pobieranie czasu	Powrót do harmonogramu	Odblokuj wszystkie piętra	Aktualizuj nazwę urządzenia
Sprawdź status	Zablokuj	Zablokuj wszystkie piętra	Aktualizuj nazwy kanałów
Wyłącz alarm	Odblokuj	Odblokuj jednorazowo	Synchronizacja z NTP
Przywracanie ustawień fabrycznych	Włącz monitorowanie	Paruj	
Wymiana serwisowa	Wyłącz monitorowanie	Rozłącz	
Aktualizuj	Włącz	Odrygluj czasowo	
Odrygluj	Wyłącz	Jednorazowy dostęp swobodny	

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

Nowa komenda

Nowy typ komendy:

Zmień szablon wirtualnej strefy

Rodzaj polecenia

Ustaw wybrany

Szablon

Szablon strefy 1

Wirtualna strefa

Wirtualna strefa 1 [Panel 4]

Opóźnienie (sek.)

- 0 +

Ustaw wybrany

Ustaw domyślny

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

Nowa komenda

Nowy typ komendy:

Generuj raport

Nazwa

Raport

Filtr czasu

Wybierz

Filtr elementów i zdarzeń

Wybierz

Priorytety

1 2 3 4 5

Raport

PDF ☒ CSV ☐ HTML ☐

Orientacja

Pionowo

Podgląd

Język

polski

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.

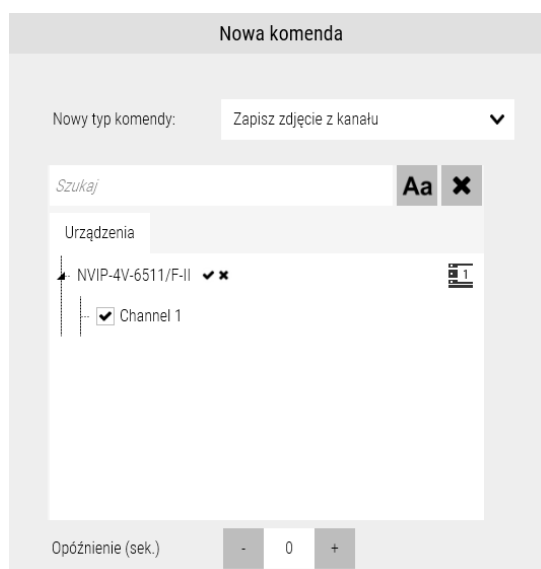
Generuj raport - Funkcjonalność RCP - ustawienie reakcji do wykonania raportów RCP, Indywidualnych, Grupowych lub z listy obecności, z wyborem zakresu czasu, rodzaju szablonu i formatu pliku raportu.

Anuluj polecenie scenariusza - ustawienie reakcji anulowania innego działającego scenariusza.

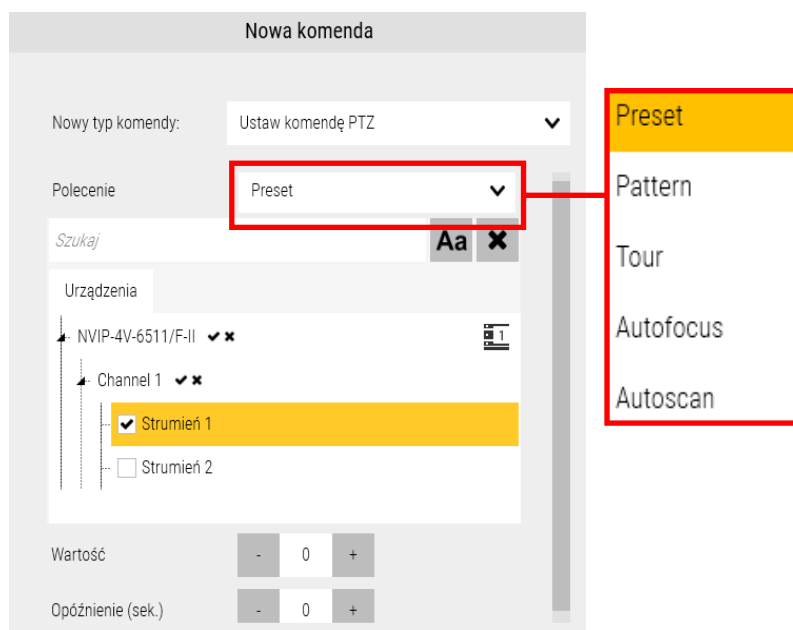
Wykonaj scenariusz - ustawienie reakcji dla wykonania innego skonfigurowanego scenariusza.

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

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.

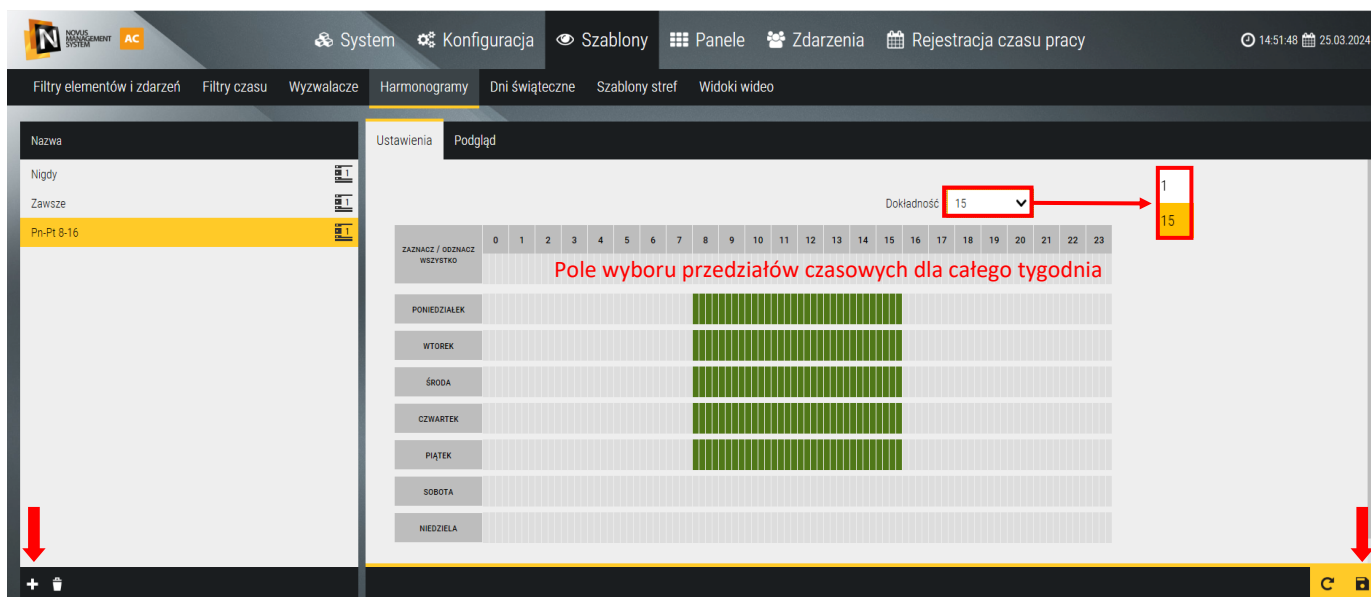
Zmodyfikuj identyfikator - ustawienie reakcji związanej z modyfikacją identyfikatorów wybranych użytkowników:

- 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 usunąć 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.

ZAZNACZ / OZNAJAZD	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Wszystko																								
PONIEDZIAŁEK																								
WTOREK																								
ŚRODA																								
CZWARTEK																								
PIĄTEK																								
SOBOTA																								
NIEDZIELA																								

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 checkbox *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

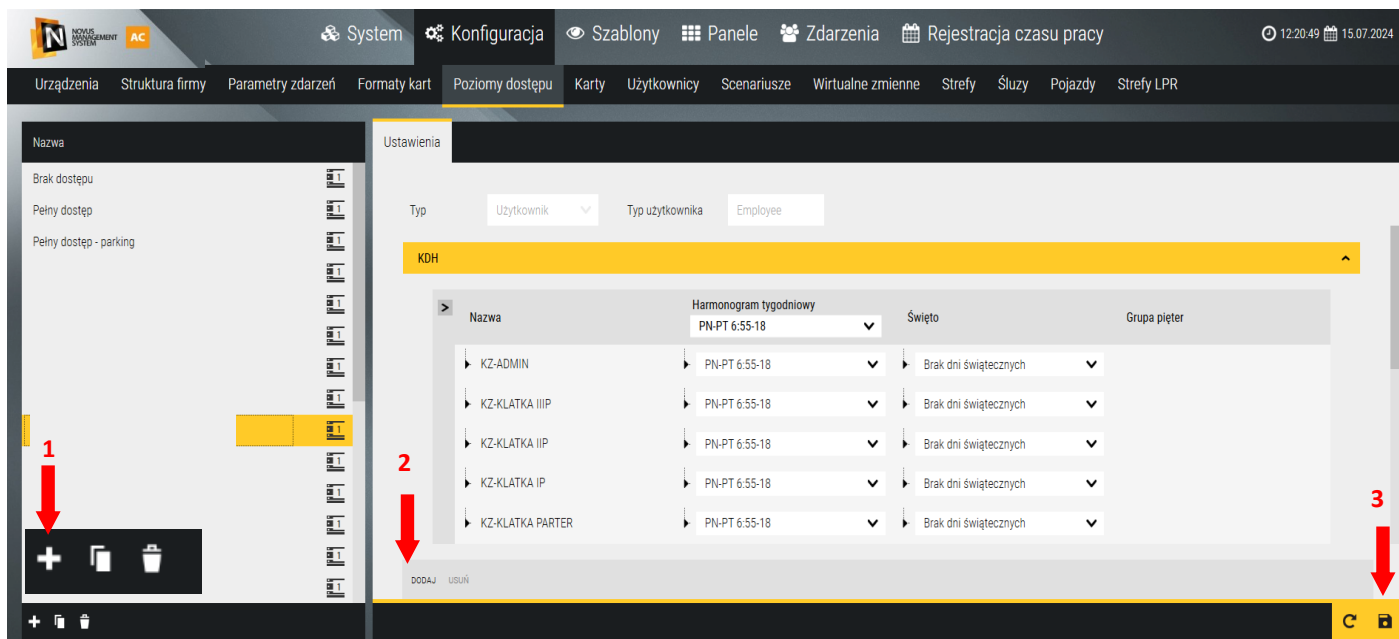
Nigdy	
Zawsze	
HARM. PN-PT 8-17	
HARM. PN-PT 06-07 - 12-13 - 17-18	

Terminarz dostępu		Święto	
Poniedziałek	Wtorek	Środa	Czwartek
06 : 00 - 07 : 00	06 : 00 - 07 : 00	12 : 00 - 13 : 00	17 : 00 - 18 : 00

Dni specjalne			
↑	↓	↕	PRZEWIŃ DO AKTUALNEGO TYGODNIA
08	11	2021	☐ Dzień specjalny
09	11	2021	☐ Dzień specjalny
10	11	2021	☐ Dzień specjalny
11	11	2021	☒ Dzień specjalny ☒ Powtarzaj co roku
12	11	2021	☐ Dzień specjalny
13	11	2021	☐ Dzień specjalny
14	11	2021	☐ Dzień specjalny

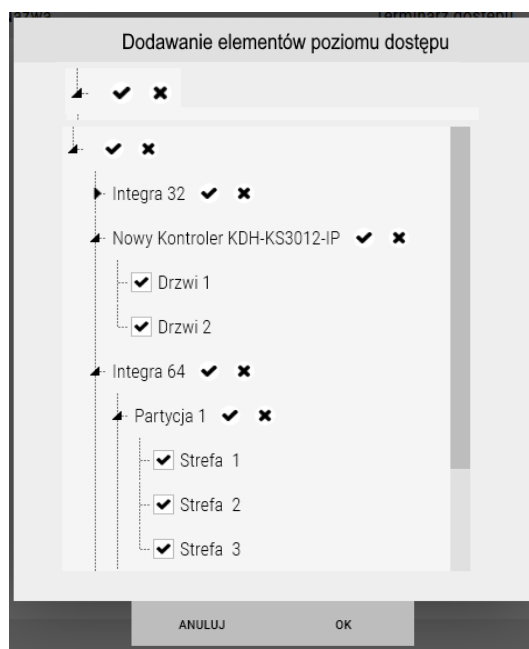
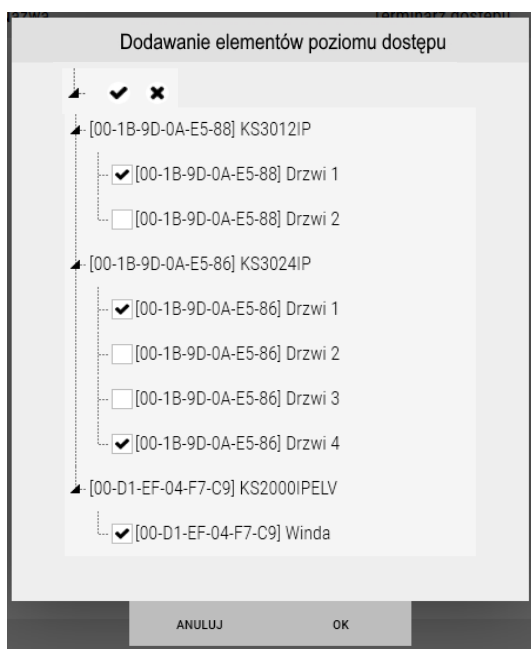
Zdefiniowany harmonogram można edytować lub usuwać zaznaczając go na liście i klikając na przycisk **Usuń** w lewym dolnym rogu okna.

4.2 Poziomy dostęp



Zakładka *Poziomy dostęp* umożliwia zdefiniowanie poziomów dostępu przeznaczonych dla użytkowników kart oraz uprawnień decydujących o tym, do których partycji/stref centrali alarmowej użytkownik będzie miał dostęp. Poziomy dostęp 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 *Identyfikator/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 usunąć lub edytować. Żeby dodać nowy poziom dostępu należy kliknąć na przycisku **Dodaj** w lewym 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.

KDH			
Nazwa	Harmonogram tygodniowy	Święto	Grupa pięter
	PN-PT 6:55-20		
KS3024IP	PN-PT 6:55-20	święta 2024	
KS3012IP	PN-PT 6:55-20	święta 2024	
KS3000IPELV	PN-PT 6:55-20	święta 2024	Piętra 1-4

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 ikonę **dyskiety** 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.

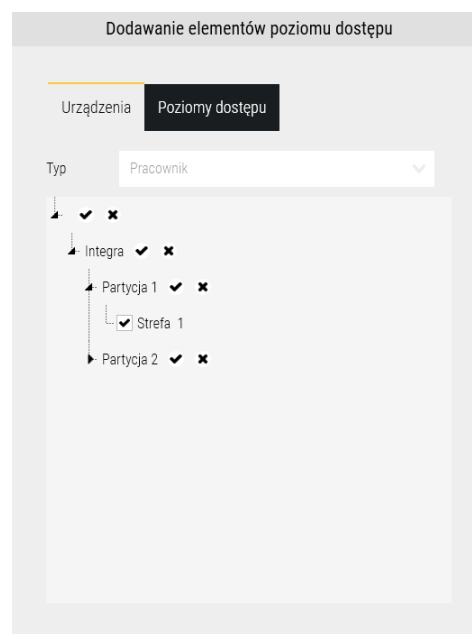
Żeby dodać nowy poziom dostępu należy kliknąć na przycisku  w lewy dolny rogu ekranu. Domyślną nazwę na żółtym polu można zmienić na własną.

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

Wyświetli się okno zawierające listę wszystkich dodanych uprzednio urządzeń.

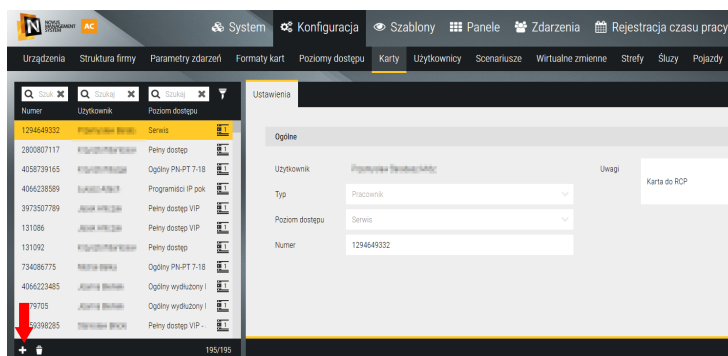
Należy zaznaczyć partycje oraz strefy, do których dany poziom będzie posiadał uprawnienia dotyczące dostępu i potwierdzić przyciskiem **OK**.

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:

The 'Dodaj' (Add) dialog box is shown. It has a title bar 'Dodaj'. Below it, there are several fields with dropdown menus: 'Typ' (set to 'Pracownik'), 'Tryb' (set to 'Wpisz numer'), 'Wiegand format' (set to 'Wiegand 34'), and 'Prezentacja numeru karty' (set to 'DEC'). There is a 'Numer' field with the value '1' and a 'DODAJ' button next to it. To the right of these fields is a section titled 'Lista kart do dodania' which is currently empty. At the bottom of the dialog, there is a message 'NACIŚNIJ PRZYCIŚK "DODAJ" ABY DODAĆ KARTĘ' and two buttons: 'ANULUJ' and 'OK'.

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.

The screenshot displays the 'Użytkownicy' (Users) management interface. On the left, there is a list of users with columns for 'Imię' (Name) and 'Nazwisko' (Surname). A filter icon is highlighted with a red box. Below the list, a 'Wyczyść' (Clear) button is visible. On the right, the 'Ogólne' (General) tab is active, showing a form for user details. A dropdown menu for 'Typ' (Type) is highlighted with a red box, showing options 'Pracownik' (Employee) and 'Gość' (Guest). Another dropdown for 'Struktura firmy' (Company structure) is also highlighted with a red box, showing 'Nieprzypisani' (Not assigned). A red arrow points to the bottom toolbar, which contains icons for adding, deleting, and exporting data.

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).

The 'Eksportuj' (Export) dialog box is shown. It includes a 'CSV' tab and a 'Lokalizacja zapisu pliku' (File save location) field. The 'Separator' is set to ';' and the 'Kodowanie' (Encoding) is set to 'Unicode (UTF-8)'. Under the 'Eksportuj' (Export) section, there are checkboxes for 'Użytkownik' (checked), 'Karta' (checked), 'Pojazd' (checked), and 'Kod QR' (checked). At the bottom, there are 'ANULUJ' (Cancel) and 'EKSPORTUJ' (Export) buttons.

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.

Widok interfejsu użytkownika z listą użytkowników i ustawieniami RCP. W sekcji 'Server 2961' widoczne są następujące ustawienia:

Ustawienie	Wartość
Akronim	2
Grupa czasu pracy	Brak
Kalendarz RCP podstawowy	Brak
Kalendarz RCP dodatkowy	Brak
Identyfikator RCP	Karta: 7484855

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.

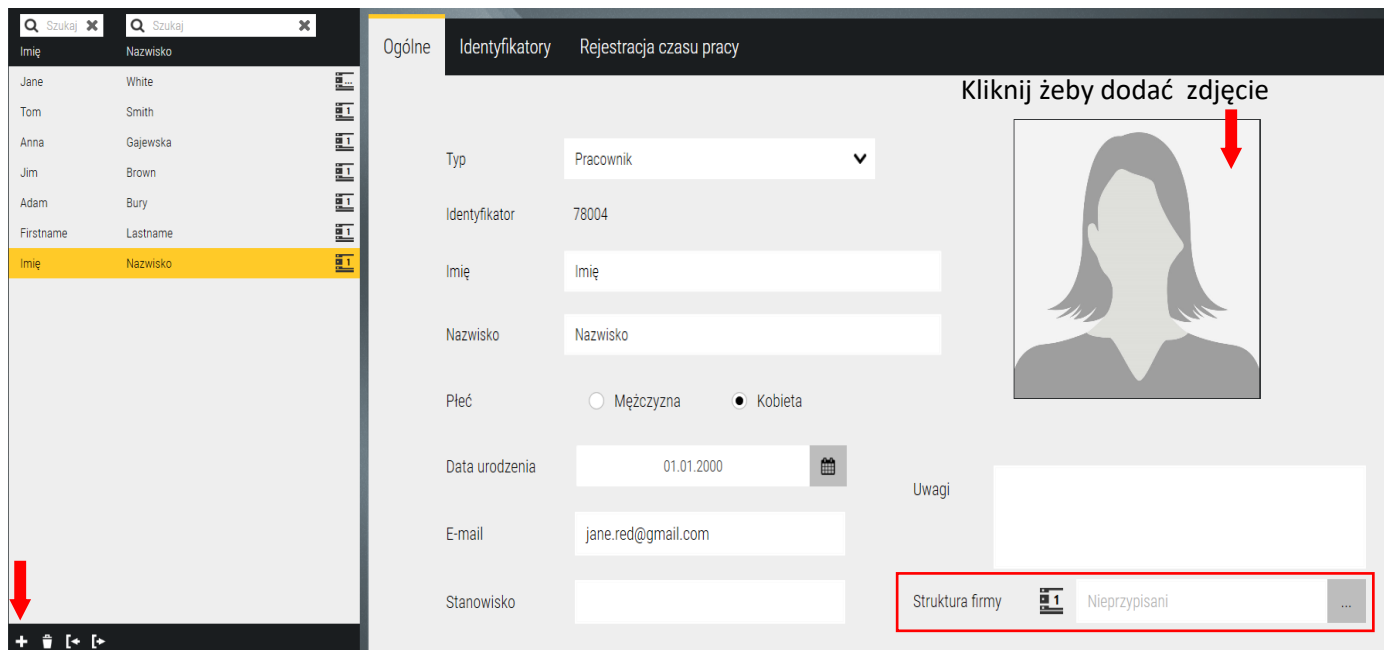
Widok wyeksportowanego pliku CSV:

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:



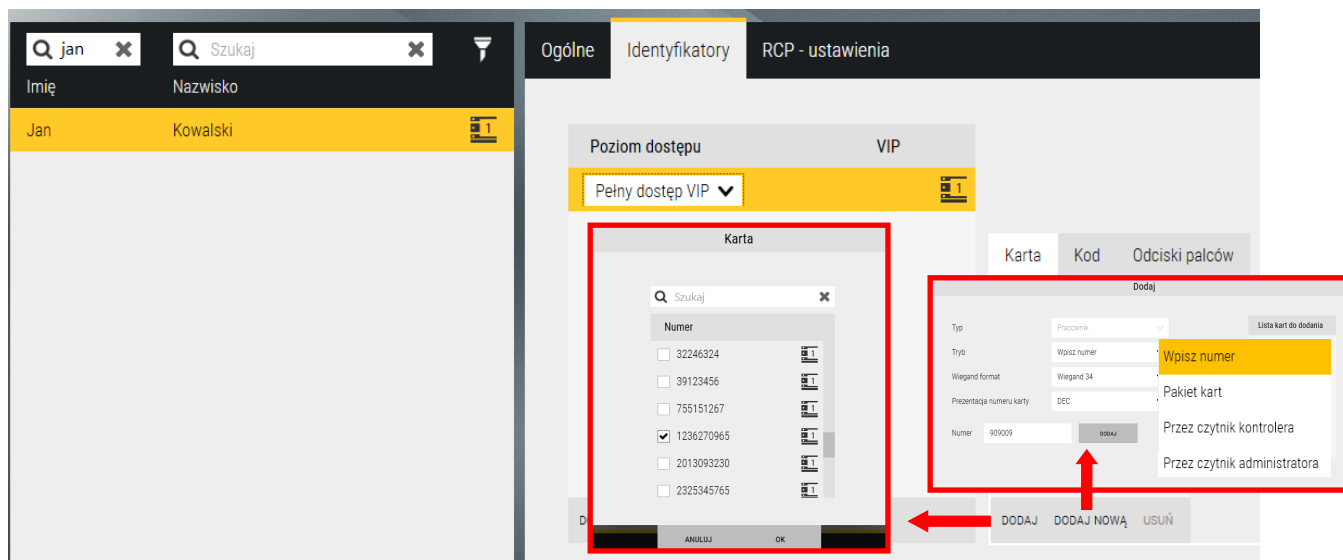
Dodawanie nowego użytkownika - kliknąć na przycisku **Dodaj (+)** w lewym dolnym rogu okna (żeby usunąć należy zaznaczyć i kliknąć **Usuń** ). Następnie należy wypełnić pola formularza w prawym oknie. Oprócz pola z imieniem i nazwiskiem pozostałe pola nie są obowiązkowe. Można również dodać zdjęcie użytkownika 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

Wpisz numer

Pakiet kart

Przez czytnik kontrolera

Przez czytnik administratora

Dodaj

Typ

Przebieg

Wpisz numer

Wzrost 25

Prezentacja numeru karty

DEC

Numer

15578

DODAJ

Lista kart do dodania

15578

Dodaj

Typ

Przebieg

Pakiet kart

Wzrost 25

Prezentacja numeru karty

DEC

Od

10010

Do

10015

DODAJ

Lista kart do dodania

10010

10011

10012

10013

10014

10015

Dodaj

Typ

Przebieg

Przez czytnik kontrolera

Wzrost 34

Prezentacja numeru karty

DEC

Kontroler

K2-ADMN

DODAJ

Lista kart do dodania

Dodaj

Typ

Przebieg

Przez czytnik administratora

Wzrost 34

Prezentacja numeru karty

DEC

DODAJ

Lista kart do dodania

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

Ogólne

Identyfikatory

RCP - ustawienia

Poziom dostępu

VIP

Ogólny PN-PT 7-18

Karta

Kod

Odciski palca

Numer

755151267

DODAJ

USUŃ

Ogólne

Numer

755151267

Uwagi

KDH

Kasowanie alarmu (kod + karta)

Multi-odczyt

Pierwsza karta otwierająca

HID

Zwolnienie z kodu dla trybu "Karta i kod"

Wydłużony czas dostępu

Multi-odczyt

Data początkowa

15.07.2024 12:00

Data końcowa

29.08.2025 09:00

✓ Data końcowa

29.08.2025 09:00

Karta

Kod

Odciski palców

Kod

Kod

.....

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 włączoną 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.

AAT SYSTEMY BEZPIECZEŃSTWA Sp. z o.o.
Wszelkie prawa zastrzeżone.

104

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

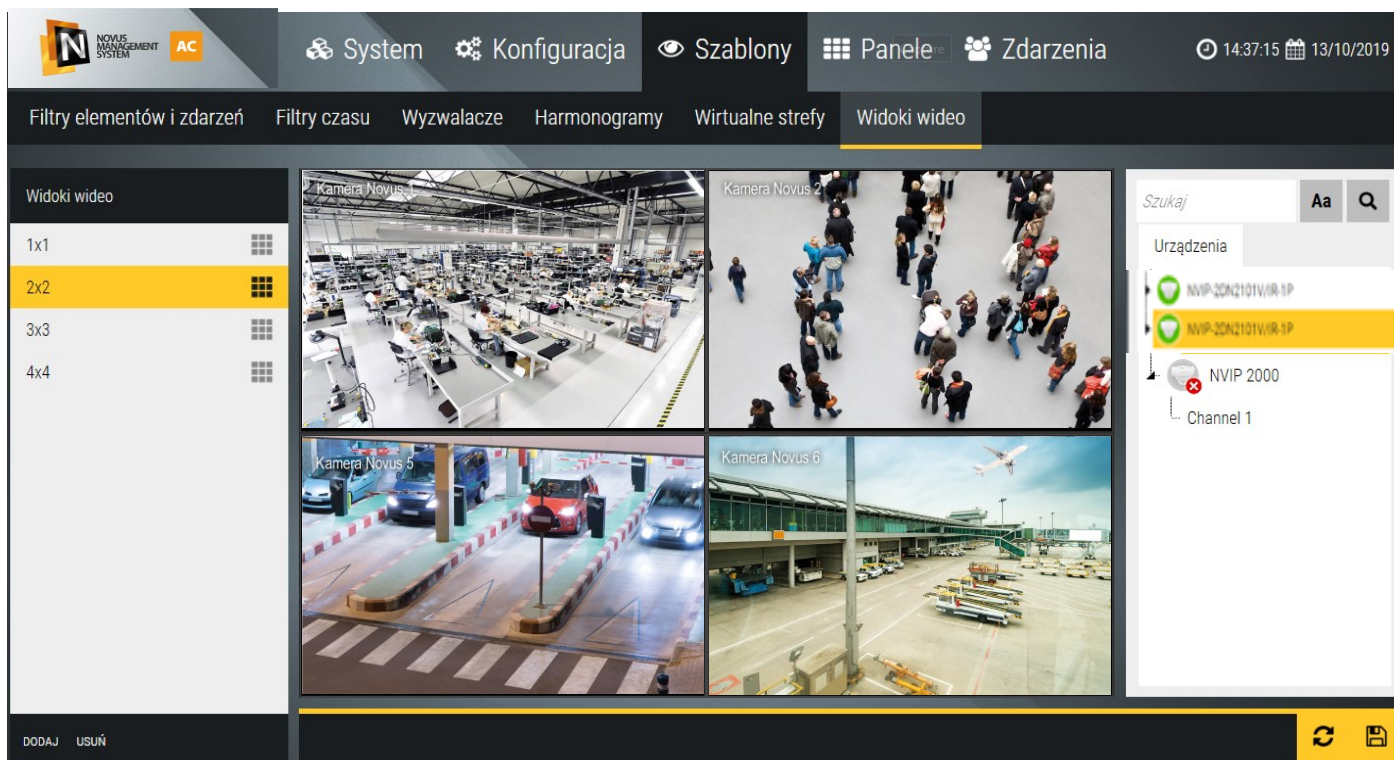
Dodawanie hasła użytkownika - po dodaniu identyfikatora zawierającego poziom dostępu z centralą alarmową przejść do zakładki *System alarmowy*.

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).

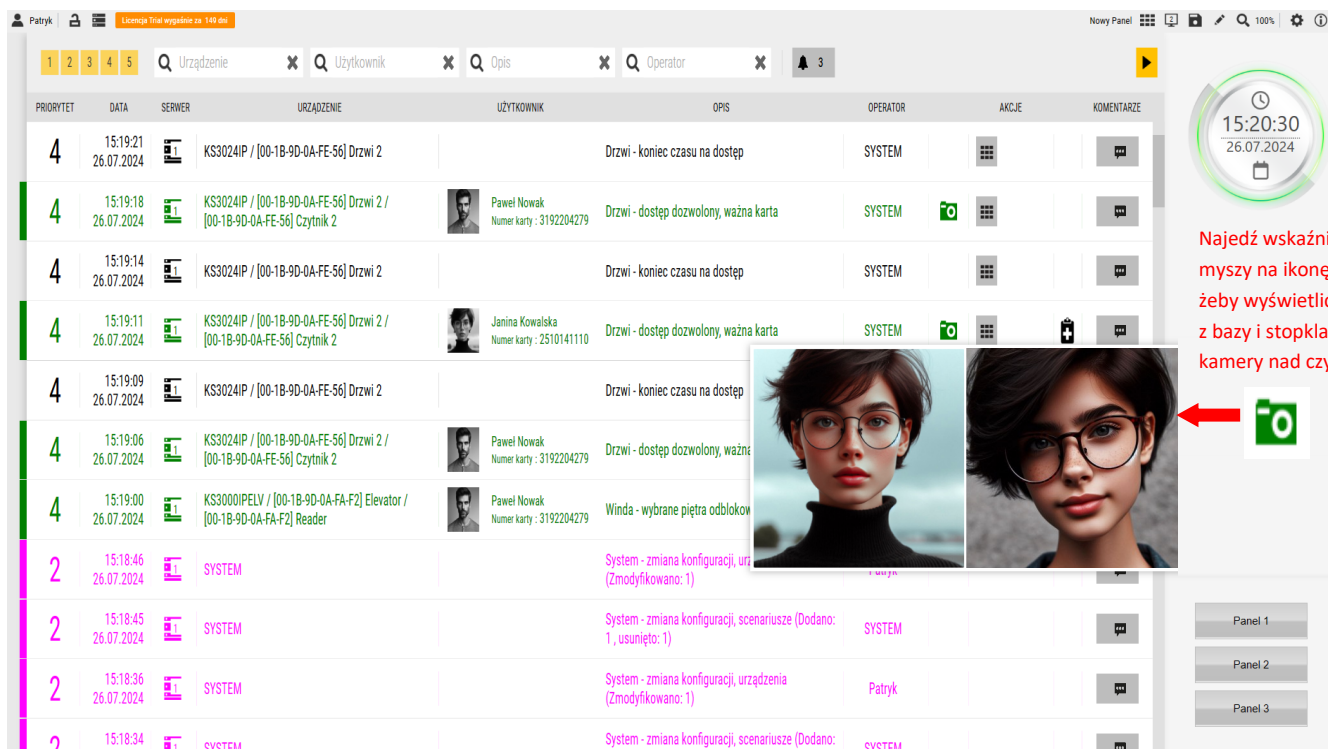
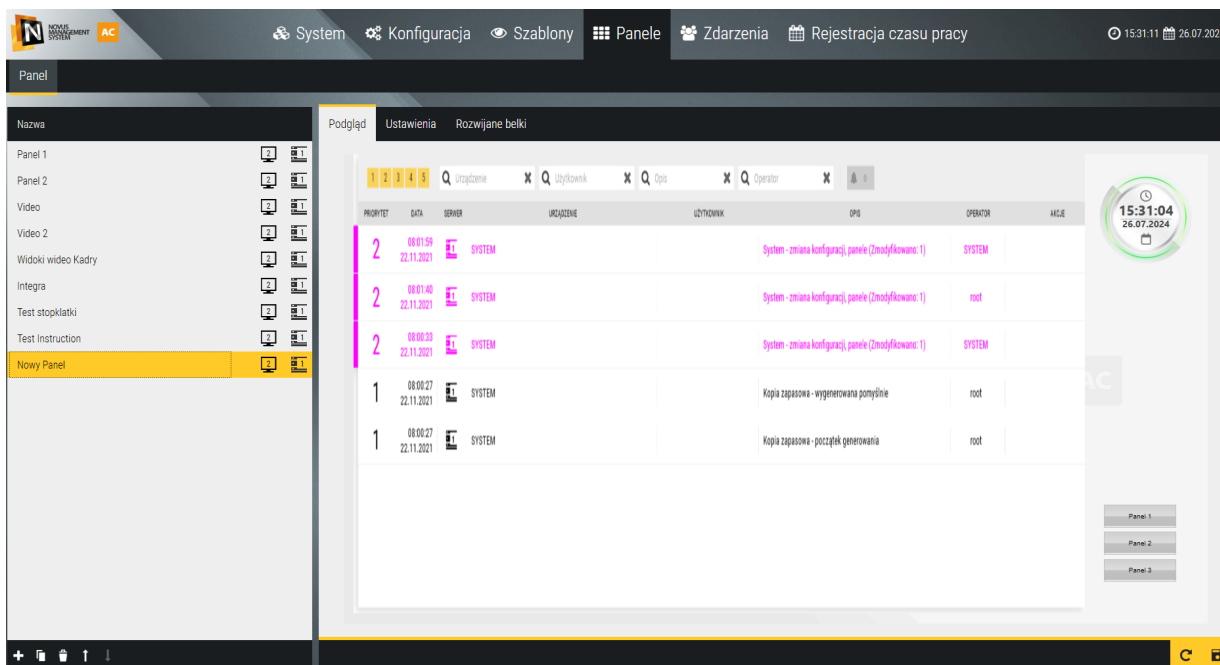
Po zdefiniowaniu widoków wideo kliknąć na przycisku **Zapisz** w prawym dolnym rogu.

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 35.

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.

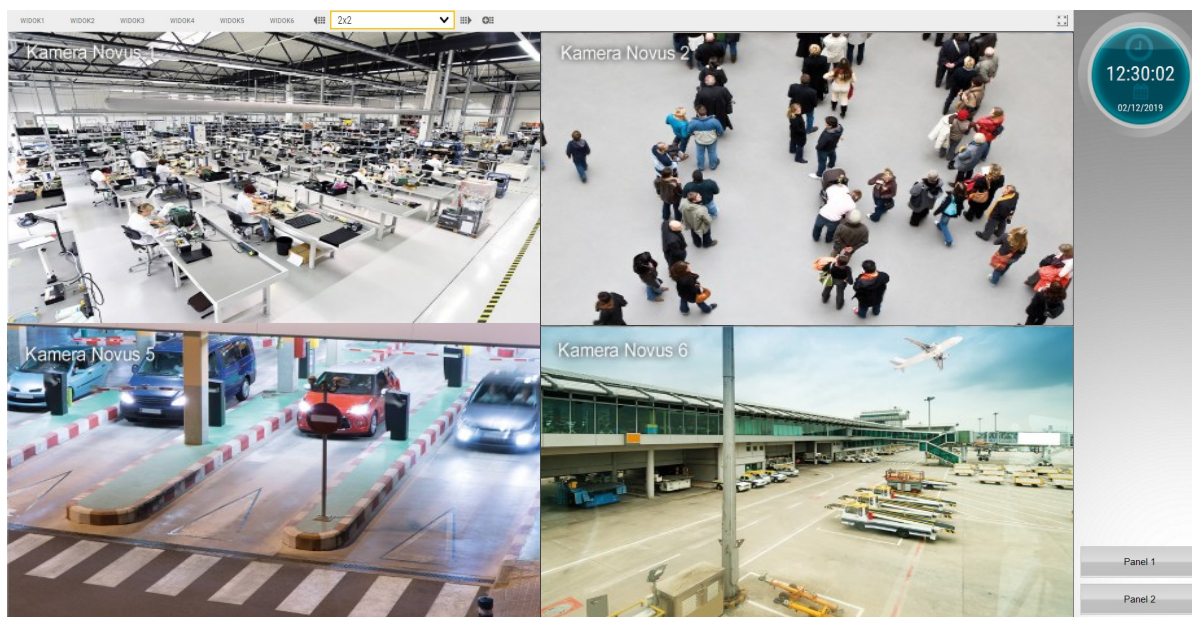
Panel 2 zawiera tablicę synoptyczną, do której dopisywane są automatycznie kolejne dodawane kontrolery wraz z elementami współpracującymi (drzwi, linie dozоровe, wyjścia sterujące, windy, piętra) oraz urządzenia telewizji dozоровej w postaci ikon przedstawiających ich aktualny stan. Stan ikon jest aktualizowany 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 :

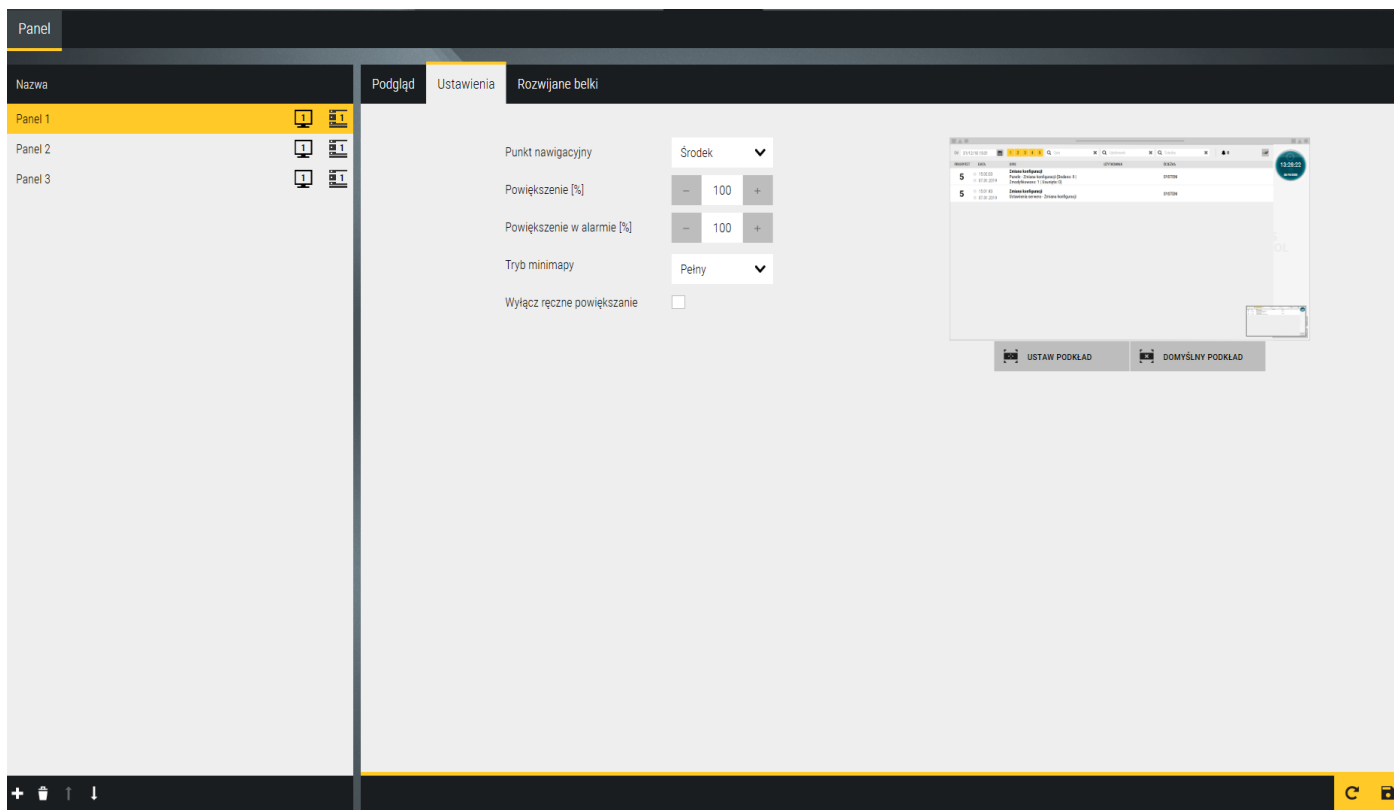
- Filtr główny - zdefiniowany w zakładce *Szablony/Filtr elementów i zdarzeń* i ustawiony w trybie edycji panelu
- Filtr typu - umożliwia wyświetlanie elementów tylko jednego typu spośród dostępnych aktualnie na tablicy.

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 dozоровej.



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.

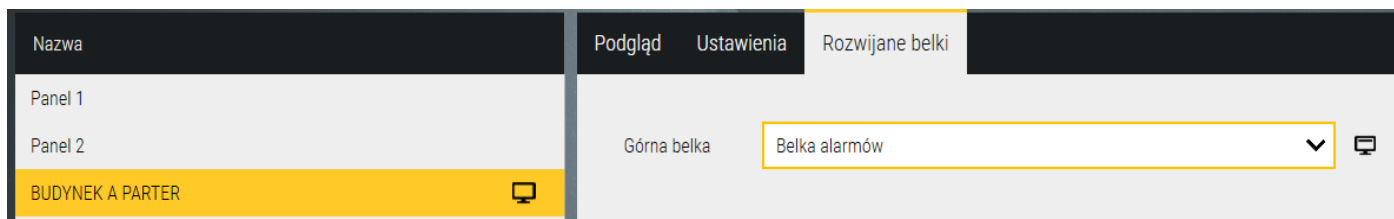
Zakładka **Ustawienia**

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 zdarzenia 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

UWAGA! Maksymalny rozmiar pliku graficznego używanego jako podkład wynosi 30 MB.

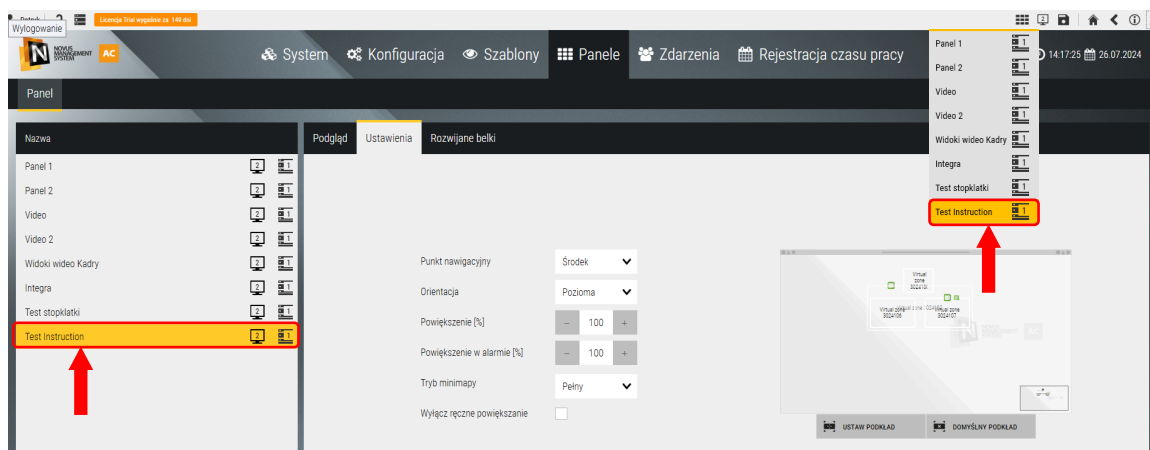
Zakładka **Rozwijane belki**

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

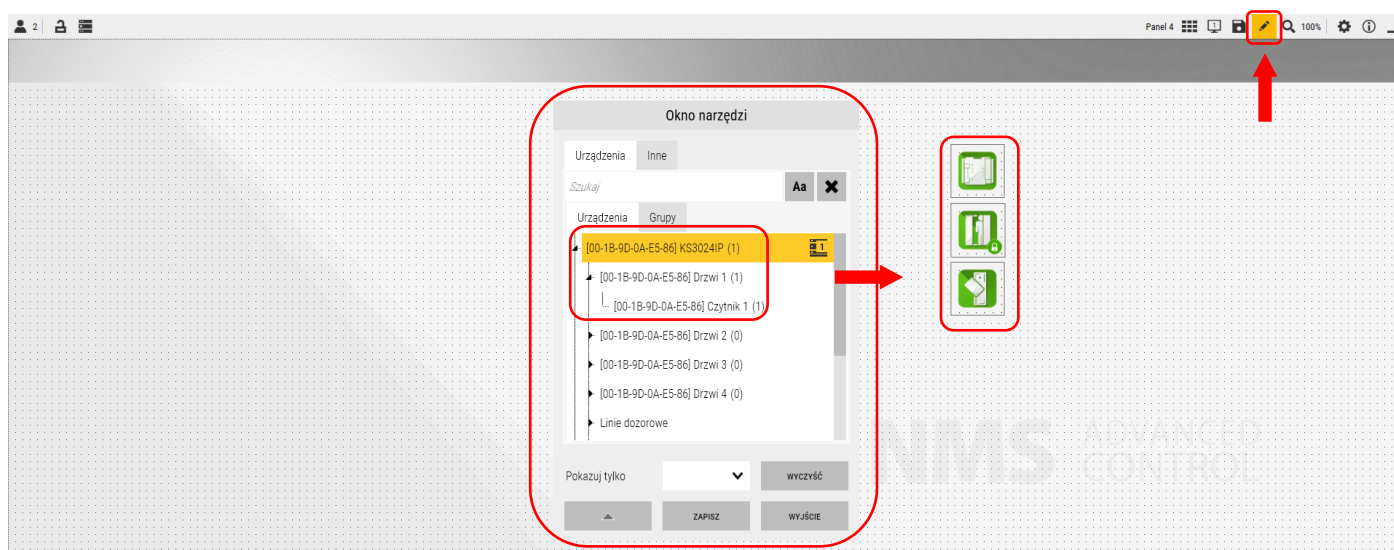
Po zdefiniowaniu zapisać ustawienia dla nowego panelu klikając na ikonie **dyskiety** w prawym dolnym rogu.

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

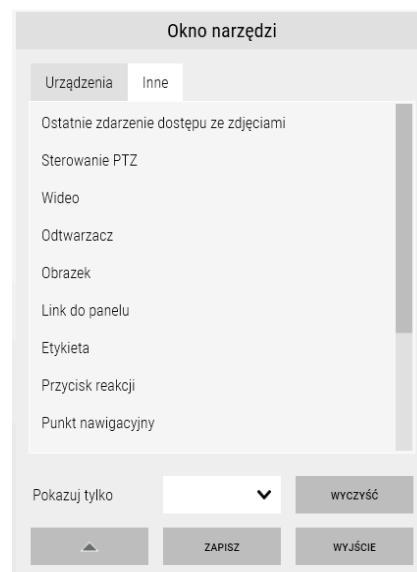
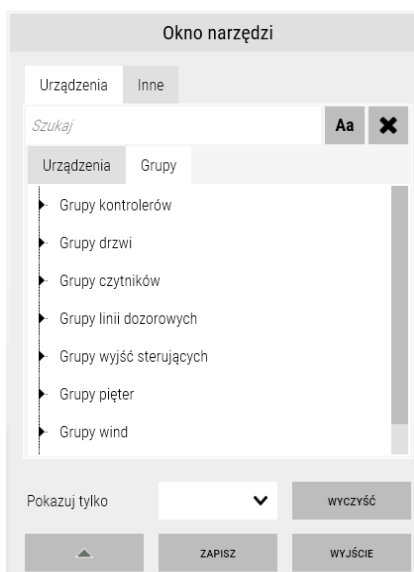
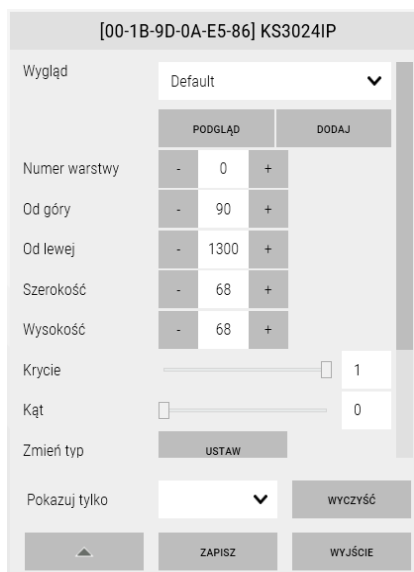
Konfiguracja zdefiniowanego panelu



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**.



UWAGA! Funkcja zoomowania panelu jest aktywowana po naciśnięciu kombinacji klawiszy **CTRL + SHIFT** oraz przewijaniu kółkiem myszy (scrollowaniem), gdy kursor myszy znajduje się nad dowolną kontrolką.

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).

The screenshot displays the 'Lista ostrzeżeń' (Warning List) section of the NOVUS MANAGEMENT SYSTEM AC. The interface includes a top navigation bar with options like System, Konfiguracja, Szablony, Panele, Zdarzenia, and Rejestracja czasu pracy. Below this, there's a sub-navigation bar with 'Lista zdarzeń', 'Lista ostrzeżeń' (selected), 'Automatyczne raporty', 'Pliki na serwerze', and 'Eksport wideo'. The main area shows a table of warnings with the following columns: OSTRZEŻENIE, DATA POZOSTAŁA, DATA KOŃCOWA, SERWER, UZAGADNIENIE, OPIS, OPERATOR OBSŁUGI, STAN, HISTORIA, KOMENTARZ, and INSTRUKCJA. The table contains four entries, all related to NVR configuration updates. The interface also includes filters for date, time, and elements, and buttons for clearing filters and generating reports.

OSTRZEŻENIE	DATA POZOSTAŁA	DATA KOŃCOWA	SERWER	UZAGADNIENIE	OPIS	OPERATOR OBSŁUGI	STAN	HISTORIA	KOMENTARZ	INSTRUKCJA
1	09:59:41 02.01.2025	09:59:41 02.01.2025	NVR-6304P4-H1-II		Alarm: Rejestrator - konfiguracja dla modelu została ustawiona NVR-6304P4-H1-II	root	Zakończono			
2	09:38:51 02.01.2025	09:38:51 02.01.2025	NVR-6304P4-H1-II		Alarm: Rejestrator - konfiguracja dla modelu została ustawiona NVR-6304P4-H1-II. Potwierdzono przez root 9:36:54, 2.01.2025		Zakończono (Potwierdzono)			
3	09:06:53 02.01.2025	09:06:53 02.01.2025	NVR-6432-H2/F		Alarm: Rejestrator - konfiguracja dla modelu została ustawiona NVR-6432-H2/F. Potwierdzono przez root 9:14:45, 2.01.2025		Zakończono (Potwierdzono)			
4	09:04:48 02.01.2025	09:04:48 02.01.2025		Uzagedzenie usunięte	Alarm: Rejestrator - konfiguracja dla modelu została ustawiona NVR-6304P4-H1-II. Potwierdzono przez root 9:08:19, 2.01.2025		Zakończono (Potwierdzono)			

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

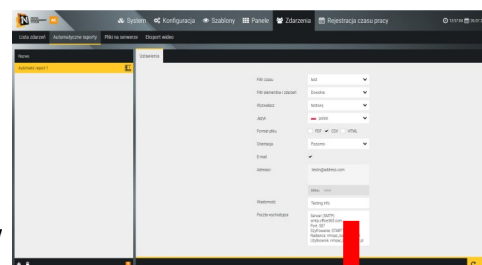
Język - do wyboru z rozwijanej listy: polski, angielski, rosyjski, azerski. Następne języki w trakcie tłumaczenia.

Format pliku - do wyboru jedno 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.

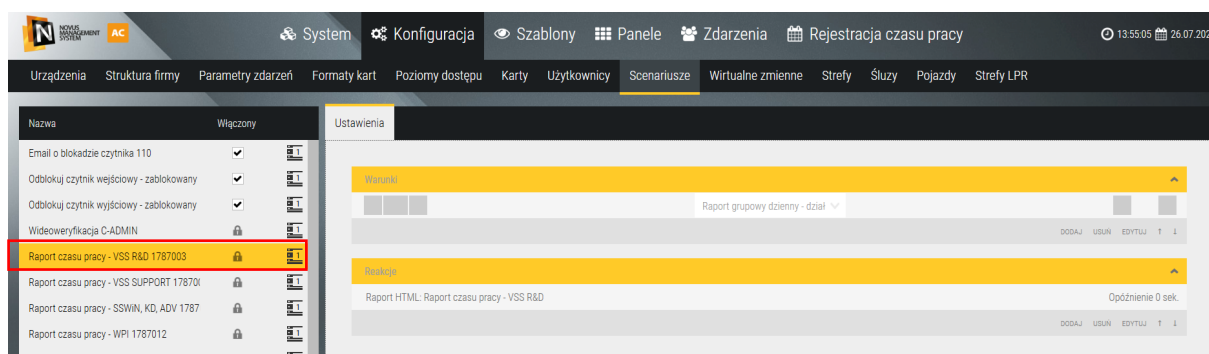
Email - pole do zaznaczenia jeżeli raport ma zostać wysłany jako email.

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.



Configuration window for 'Rejestracja czasu pracy' (Time Registration). The window contains several sections with dropdown menus and input fields:

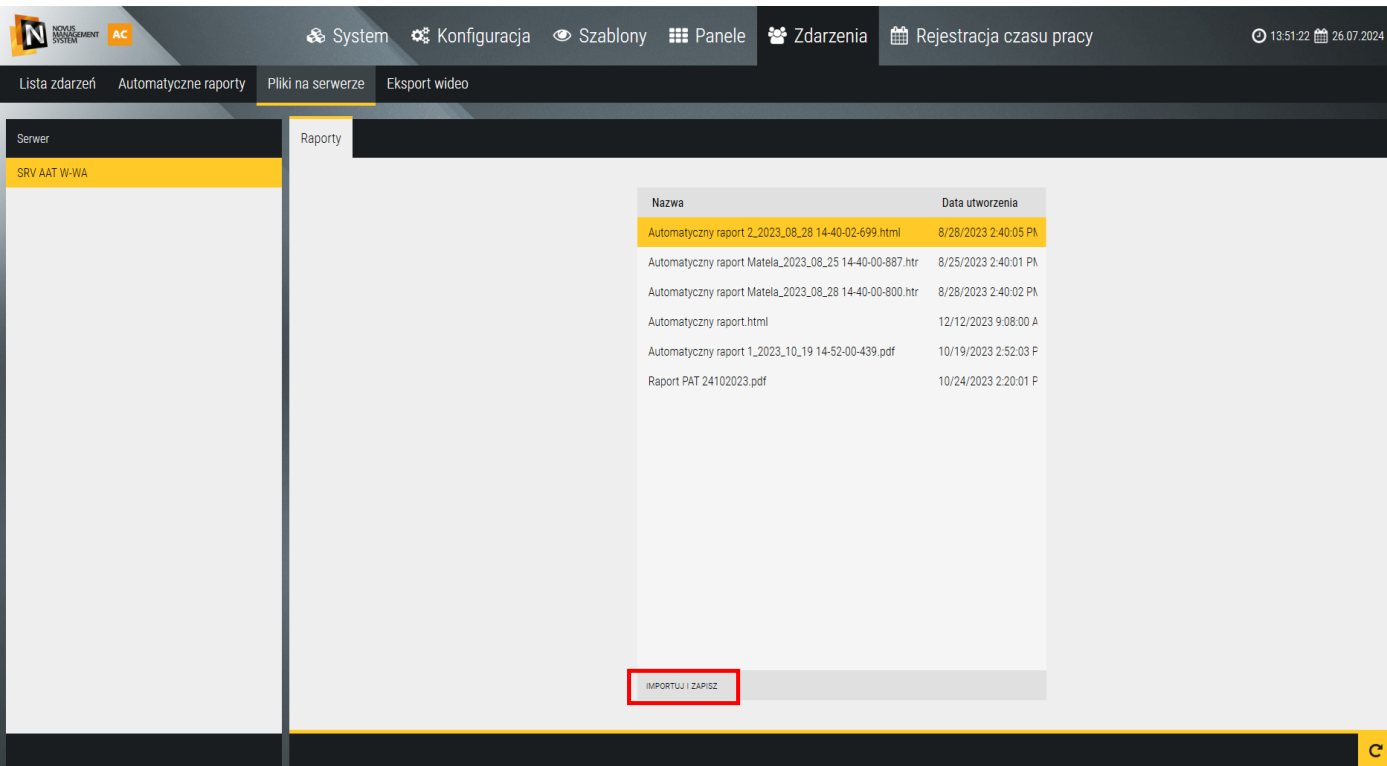
- Filtr czasu**: test
- Filtr elementów i zdarzeń**: Dowlone
- Wyzwalacz**: testowy
- Język**: polski
- Format pliku**: ☐ PDF ☒ CSV ☐ HTML
- Orientacja**: Poziomo
- E-mail**: ☒
- Adresaci**: testin@address.com
- DODAJ** and **USUŃ** buttons
- Wiadomość**: Testing info
- Poczta wychodząca**:
 - Server (SMTP): smtp.office365.com
 - Port: 587
 - Szyfrowanie: STARTTLS
 - Nadawca: nmsac_kadry@aat.pl
 - Użytkownik: nmsac_kadry@aat.pl



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*.



The screenshot shows the 'Pliki na serwerze' (Files on server) tab in the NOVUS MANAGEMENT SYSTEM AC interface. The left sidebar shows the 'Serwer' (Server) section with 'SRV AAT W-WA' selected. The main area displays a table of reports:

Nazwa	Data utworzenia
Automatyczny raport 2_2023_08_28 14-40-02-699.html	8/28/2023 2:40:05 PM
Automatyczny raport Matela_2023_08_25 14-40-00-887.htr	8/25/2023 2:40:01 PM
Automatyczny raport Matela_2023_08_28 14-40-00-800.htr	8/28/2023 2:40:02 PM
Automatyczny raport.html	12/12/2023 9:08:00 A
Automatyczny raport 1_2023_10_19 14-52-00-439.pdf	10/19/2023 2:52:03 P
Raport PAT 24102023.pdf	10/24/2023 2:20:01 P

At the bottom of the table, there is a button labeled 'IMPORTUJ / ZAPISZ' (Import / Save), which is highlighted with a red box in the image.

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 Ustawienia serwerów

Zakładka *Ustawienia serwerów* umożliwia konfigurację parametrów pracy serwera oraz monitorowanie jego stanu

Ścieżka raportów - lokalizacja, w której zapisywane są generowane raporty systemowe. Możliwe jest wskazanie zarówno lokalnej ścieżki na serwerze, jak i zasobu sieciowego.



UWAGA! W polu *Ścieżka sieciowa* należy podać ścieżkę do udostępnionego zasobu sieciowego w formacie UNC, np. \\Serwer\Raporty

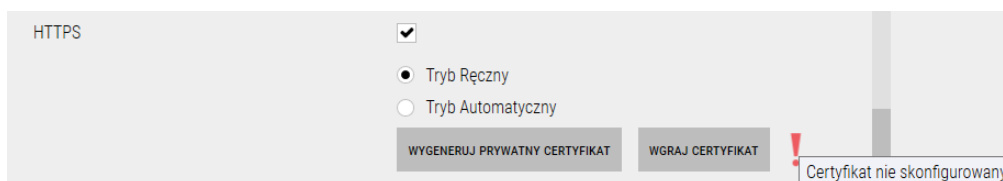
Wskazany zasób musi być udostępniony w sieci oraz dostępny z poziomu serwera NOVUS MANAGEMENT SYSTEM AC. Konto, na którym uruchomiona jest usługa serwera, musi posiadać uprawnienia do odczytu i zapisu w wybranej lokalizacji.

Certyfikat HTTPS

HTTPS - umożliwia korzystanie z szyfrowanego protokołu HTTPS podczas komunikacji z serwerem, zwiększając bezpieczeństwo przesyłanych danych. Zaznaczenie opcji powoduje wykorzystanie protokołu HTTPS, natomiast odznaczenie pola oznacza komunikację za pomocą nieszyfrowanego protokołu HTTP.

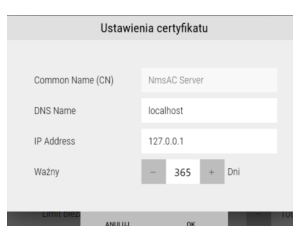
UWAGA! Ustawienie ma zastosowanie zarówno do komunikacji z aplikacją webową (opcja dostępna w przyszłości) NOVUS MANAGEMENT SYSTEM AC, jak i do komunikacji realizowanej za pośrednictwem interfejsu API.

Wyświetlenie ikony czerwonego wykrzyknika z komunikatem „Certyfikat nieskonfigurowany” oznacza, że do serwera nie został jeszcze przypisany żaden certyfikat HTTPS. W takim przypadku należy wygenerować certyfikat za pomocą opcji *Wygeneruj prywatny certyfikat* lub zaimportować własny certyfikat przy użyciu opcji *Wgraj certyfikat*.



Tryb ręczny – umożliwia ręczne przypisywanie użytkowników do stref przez operatora systemu.

Wygeneruj prywatny certyfikat - umożliwia automatyczne wygenerowanie samopodpisanego certyfikatu SSL/TLS, który może zostać wykorzystany do zabezpieczenia połączeń HTTPS z serwerem.



Ustawienia certyfikatu

Okno *Ustawienia certyfikatu* służy do konfiguracji parametrów samopodpisanego certyfikatu SSL/TLS wykorzystywanego przez serwer podczas komunikacji HTTPS.

Common Name (CN) - nazwa certyfikatu identyfikująca serwer. Zaleca się podanie nazwy hosta lub nazwy serwera, z której będą korzystali użytkownicy podczas nawiązywania połączenia.

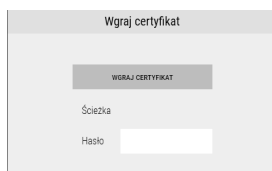
DNS Name - nazwa domenowa serwera, dla której generowany jest certyfikat, np. nms.example.com. Nazwa ta powinna odpowiadać adresowi używanemu do połączenia z serwerem.

IP Address - adres IP serwera, który zostanie uwzględniony w certyfikacie. Opcja ta jest przydatna w przypadku łączenia się z serwerem bez użycia nazwy domenowej.

Ważny - okres ważności certyfikatu wyrażony w dniach. Po upływie wskazanego czasu certyfikat wygasa i konieczne jest wygenerowanie nowego lub wgranie aktualnego certyfikatu.

UWAGA! Dla poprawnej weryfikacji certyfikatu zaleca się, aby wartości pól *DNS Name* oraz *IP Address* odpowiadały rzeczywistemu adresowi, pod którym dostępny jest serwer NOVUS MANAGEMENT SYSTEM AC.

Wgraj certyfikat - umożliwia zaimportowanie istniejącego certyfikatu SSL/TLS do serwera NOVUS MANAGEMENT SYSTEM AC. Pozwala to na stosowanie certyfikatów wydanych przez zaufane urzędy certyfikacji (CA) lub certyfikatów firmowych.



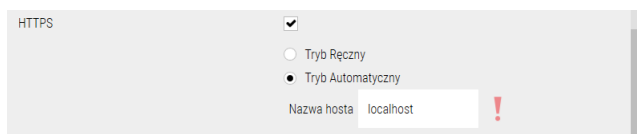
Okno zawiera następujące pola:

Wgraj certyfikat - umożliwia wskazanie pliku certyfikatu w formacie .pfx (np. server.pfx).

Ścieżka - wyświetla lokalizację wybranego pliku certyfikatu.

Hasło - hasło zabezpieczające plik .pfx, zdefiniowane podczas jego tworzenia. Hasło jest wymagane do poprawnego zaimportowania certyfikatu wraz z kluczem prywatnym.

Tryb automatyczny - powoduje automatyczne ustalenie nazwy hosta serwera na potrzeby konfiguracji certyfikatu HTTPS. System sam pobiera i aktualizuje nazwę hosta, eliminując konieczność jej ręcznego wprowadzania. Powinna odpowiadać adresowi, pod którym użytkownicy łączą się z serwerem.

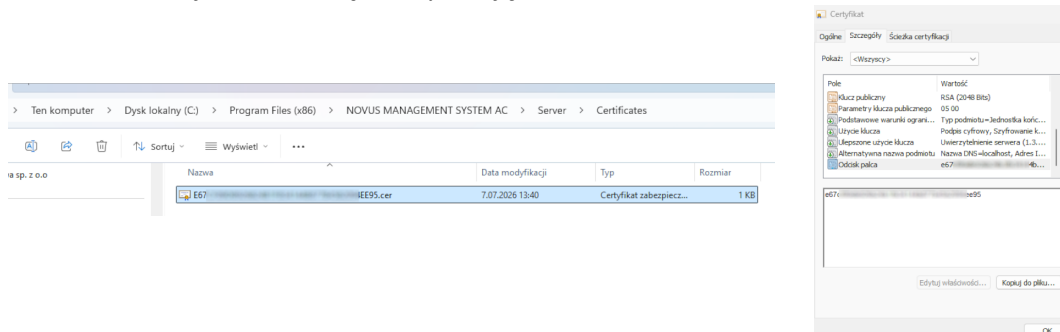


Zmiana ikonki z  na  oznacza, że certyfikat HTTPS został poprawnie wygenerowany lub zaimportowany i przypisany do serwera. Oznacza to, że konfiguracja certyfikatu została zakończona pomyślnie i może być wykorzystana do zabezpieczenia komunikacji za pomocą protokołu HTTPS.

Ikonka informacji  umożliwia wyświetlenie szczegółów aktualnie używanego certyfikatu HTTPS. Po kliknięciu ikony pojawia się okienko zawierające najważniejsze informacje o certyfikacie, takie jak: sygnatura (odcisk palca), nazwa certyfikatu, nazwa DNS, adres IP oraz data ważności.

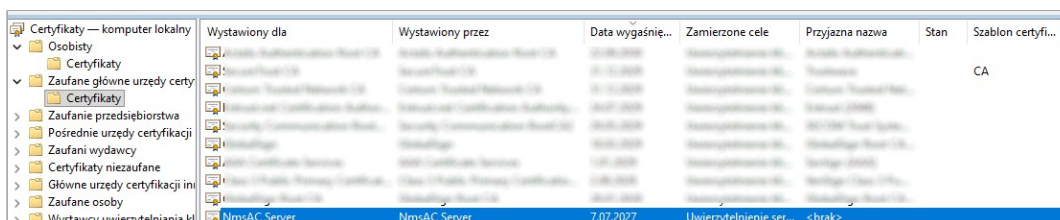
UWAGA! W przypadku wielokrotnego wgrywania lub generowania certyfikatów wyświetlane będą dane ostatnio wgranego certyfikatu.

Podczas generowania certyfikatu tworzony jest również certyfikat publiczny w formacie .cer, który zostaje zapisany w katalogu Certificates znajdującym się w katalogu serwera NOVUS MANAGEMENT SYSTEM AC. Nazwa pliku zawiera odcisk palca, co ułatwia jednoznaczną identyfikację.

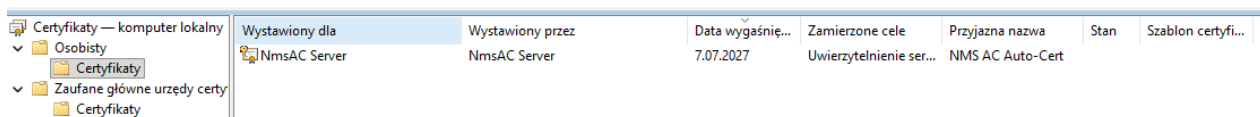


Dodatkowo certyfikat jest automatycznie instalowany w magazynach certyfikatów systemu Windows:

- Zaufane główne urzędy certyfikacji - zapisywany jest certyfikat publiczny bez klucza prywatnego, dzięki czemu jest on uznawany za zaufany przez system.



- Osobisty/Certyfikaty - zapisywany jest certyfikat wraz z kluczem prywatnym, wykorzystywany przez serwer NOVUS MANAGEMENT SYSTEM AC do zestawienia szyfrowanych połączeń TLS/HTTPS dla aplikacji webowej oraz interfejsu API.

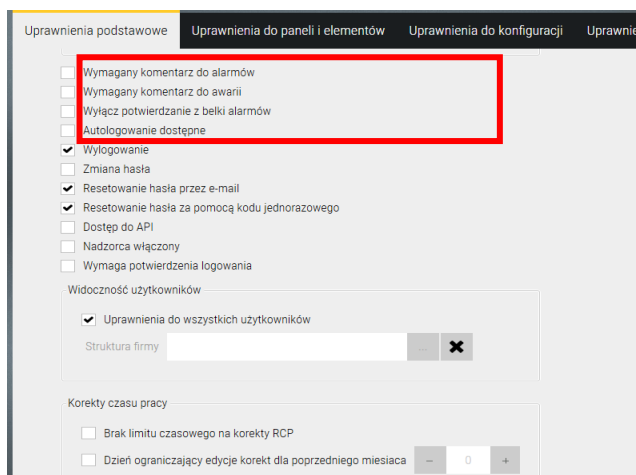
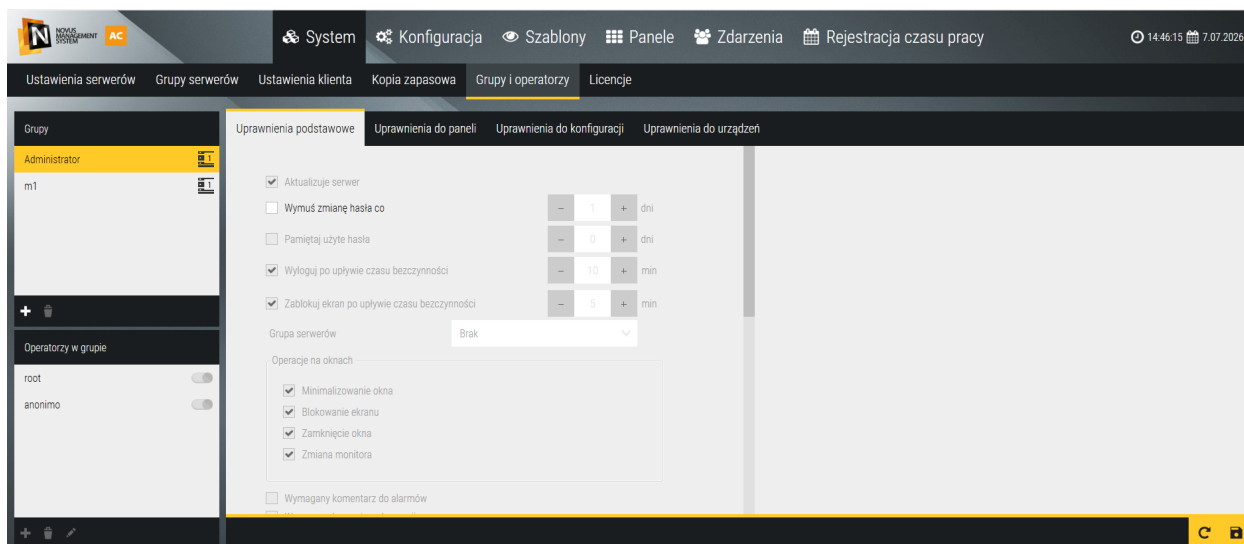


8.2 Grupy i operatorzy

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.



UWAGA! Dla grupy *Administrator* dodawanie, usuwanie oraz edycja operatorów są zablokowane.

Dla tej grupy domyślnie utworzeni są dwaj operatorzy: **root** oraz **anonimo**.

Konto **root** jest domyślnym kontem administratora i zapewnia pełny dostęp do systemu, w tym do wszystkich danych użytkowników, operatorów oraz pojazdów.

Operator **anonimo** posiada takie same uprawnienia jak operator **root**, jednak dane wrażliwe są ukrywane. Aby zalogować się na to konto, należy użyć loginu **anonimo** oraz hasła identycznego jak dla operatora **root**.

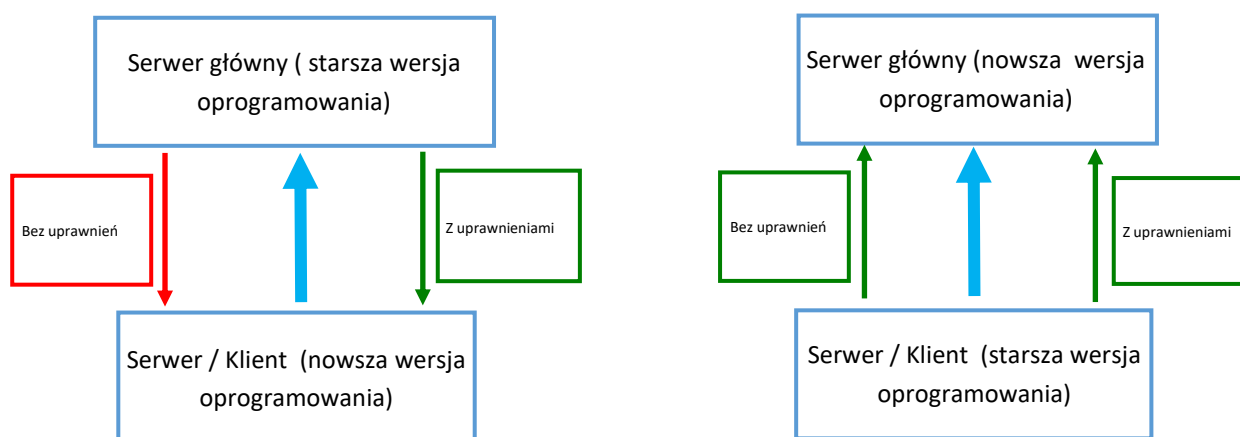
Uprawnienia podstawowe

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 zamknięcie 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 wysłanego 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

Grupy	Uprawnienia podstawowe	Uprawnienia do paneli i elementów	Uprawnienia do konfiguracji	Uprawnienia do urządzeń
Dział prawny				
Dział IT				
Dział księgowości				
Dział logistyki				
Dział wdrożeń				
Dział serwisu				

Uprawnienia do paneli i elementów		Uprawnienia
Panele	Elementy	
☐ Panel 1		
☒ Panel 2		
☐ Video		
☒ Video 2		

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 podstawowe	Uprawnienia do paneli i elementów	Uprawnienia do konfiguracji	Uprawnienia do urządzeń
☐ Pełne uprawnienia do paneli			
Panele Panel 2 Video 2	Elementy Zegar Link do panelu (Stos zdarzeń bieżących) Link do panelu (Widoki wideo)	Uprawnienia ☒ Ukryty	

Uprawnienia do konfiguracji

Grupy	Uprawnienia podstawowe	Uprawnienia do paneli i elementów	Uprawnienia do konfiguracji	Uprawnienia do urządzeń
Dział prawny				
Dział IT				
Dział księgowości				
Dział logistyki				
Dział wdrożeń				
Dział serwisu				
Operatorzy w grupie				
Wojtek_B				

Uprawnienia do konfiguracji				Szczegóły
	Pokaż	Modyfikuj	Usuń	
	☐	☐	☐	
Ustawienia serwera	☐	☐	☐	
Kopia zapasowa	☐	☐	☐	
Ustawienia klienta	☒	☒	☐	
Okno diagnostyczne	☒	☐	☐	
Grupy i operatorzy	☐	☐	☐	
Licencje	☒	☐	☒	
Grupy serwerów	☐	☐	☐	
Recorder	☐	☐	☐	
Urządzenia	☐	☐	☐	

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*.

8.3 Ustawienia klienta (stacji operatora)

	Informacje	Ostrzeżenia	Błędy	Debugowanie
System	☒	☒	☒	☐
Kontrola Dostępu	☐	☒	☒	☐
Wideo	☐	☒	☒	☐
Odtwarzanie	☐	☒	☒	☐
Renderowanie obrazu	☐	☒	☒	☐
Funkcjonalność RCP	☐	☐	☐	☐

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.

8.4 Licencje

System **Konfiguracja** **Szablony** **Panele** **Zdarzenia** **Rejestracja czasu pracy**

Ustawienia serwerów Ustawienia klienta Kopia zapasowa Grupy i operatorzy **Licencje**

Serwer
Server 6757

Rejestracja

Dane instalatora

Kraj: Polska ▼
Ulica i numer: Jest wymagane
Miejscowość: Jest wymagane
Kod pocztowy: Jest wymagane
Nazwa firmy: Jest wymagane
NIP: Jest wymagane
REGON: Jest wymagane
Imię i nazwisko: Jest wymagane
Adres e-mail: Jest wymagane
Potwierdź Email: Jest wymagane
Numer telefonu: Jest wymagane

Dane użytkownika licencji

Kraj: Polska ▼
Ulica i numer: Jest wymagane
Miejscowość: Jest wymagane
Kod pocztowy: Jest wymagane
Nazwa firmy/obiektu: Jest wymagane
NIP: Jest wymagane
REGON: Jest wymagane
Imię i nazwisko: Jest wymagane
Adres e-mail: Jest wymagane
Potwierdź Email: Jest wymagane
Numer telefonu: Jest wymagane
Typ obiektu: Bank ▼

[KLAUZULA INFORMACYJNA RODO](#) **REGISTER**

Operacje

SYNCHRONIZUJ Ustaw aktualny stan korzystając z serwera licencji **DRUKUJ DO PDF** Eksportuje plik pdf ze wszystkimi informacjami

Korzystanie z programu NOVUS MANAGEMENT SYSTEM AC wymaga jego zarejestrowania oraz aktywowania odpowiednich licencji. Aktywacja licencji jest możliwa dopiero po zarejestrowaniu programu.

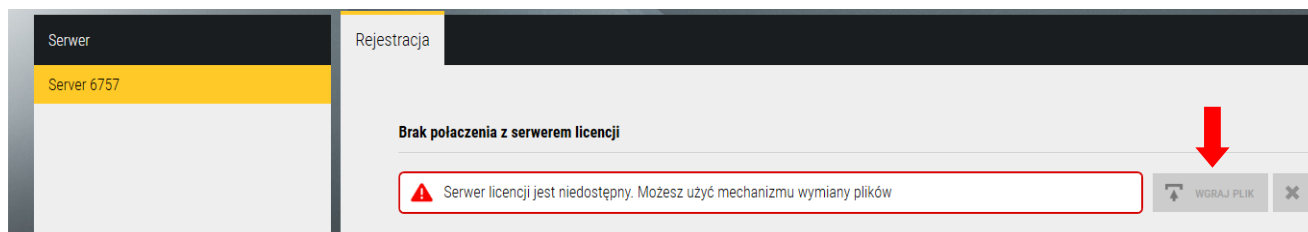
W celu dokonania rejestracji programu należy wypełnić wszystkie wymagane pola przedstawione na obrazie powyżej.

UWAGA!

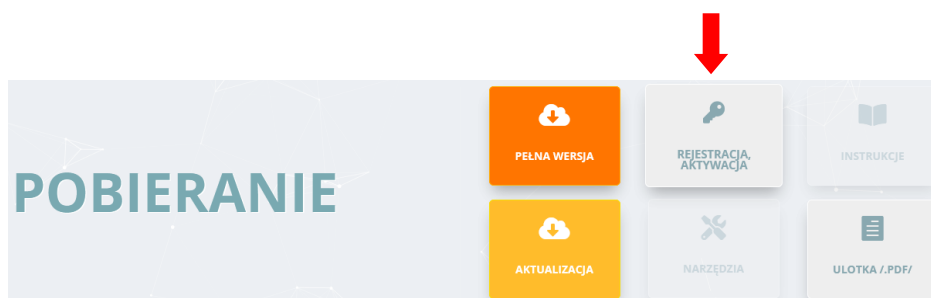
Po zakończeniu procesu rejestracji edycja danych w sekcji Dane użytkownika licencji nie będzie możliwa. W celu modyfikacji tych danych należy skontaktować się z AAT SYSTEMY BEZPIECZEŃSTWA sp. z o.o. za pośrednictwem adresu e-mail: kontakt@aat.pl.

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

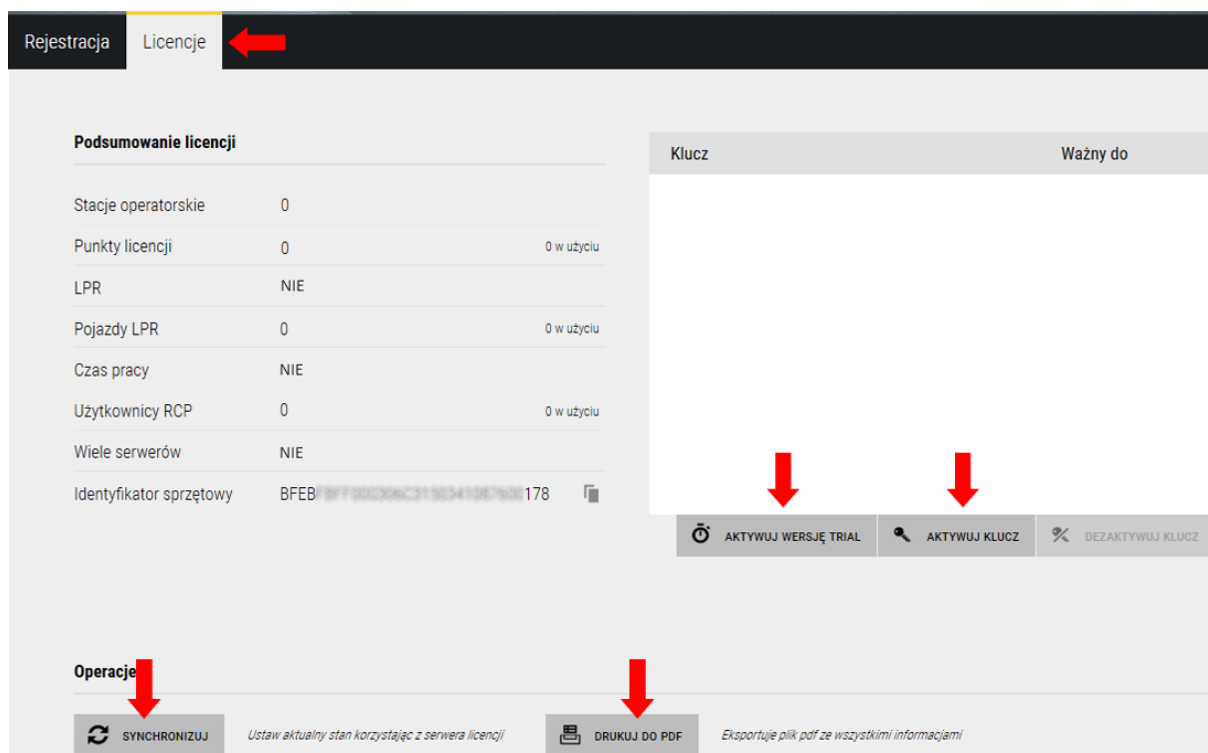
W przypadku rejestracji z komputera nie posiadającego dostępu do sieci Internet w oknie **Rejestracja** pojawi się następująca opcja.



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.



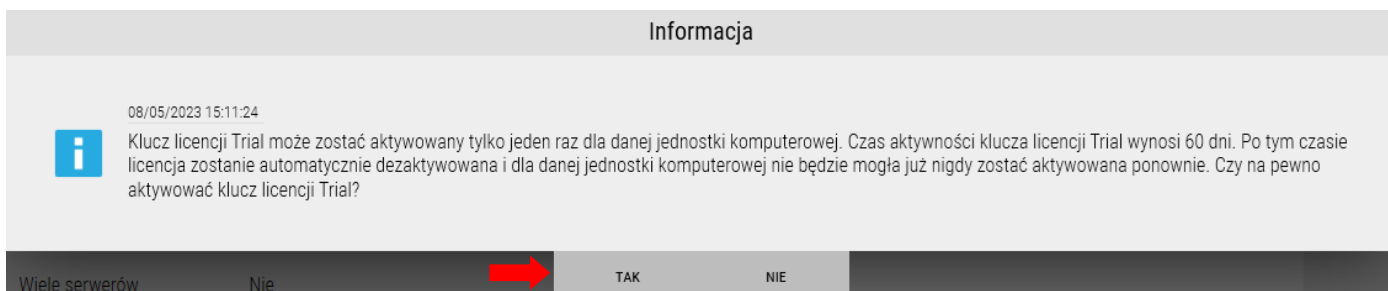
Licencje oparte są na ciągach znaków i nie wymagają kluczy sprzętowych.

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 zostało odinstalowane i zainstalowane ponownie użycie przycisku **SYNCHRONIZUJ** spowoduje załadowanie 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 jej 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**.

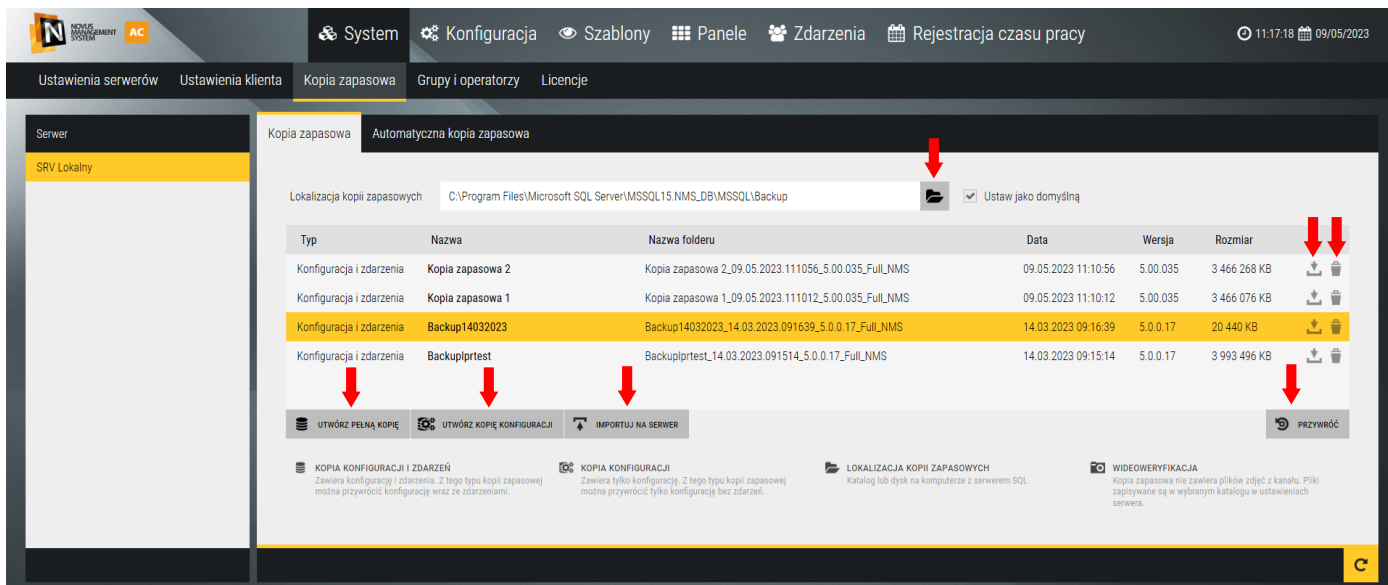


Jeśli komputer ma aktualnie dostęp do sieci Internet licencja TRIAL zostanie aktywowana. W przeciwnym wypadku zostanie wygenerowany plik *request.nlic*. W celu dokończenia procesu aktywacji licencji należy postępować analogicznie jak zostało to opisane dla procesu rejestracji bez dostępu do sieci Internet (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.



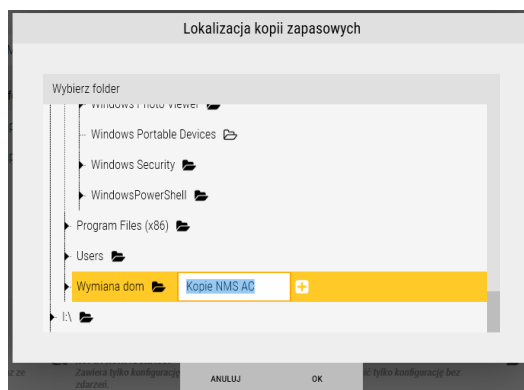
8.5 Kopia zapasowa



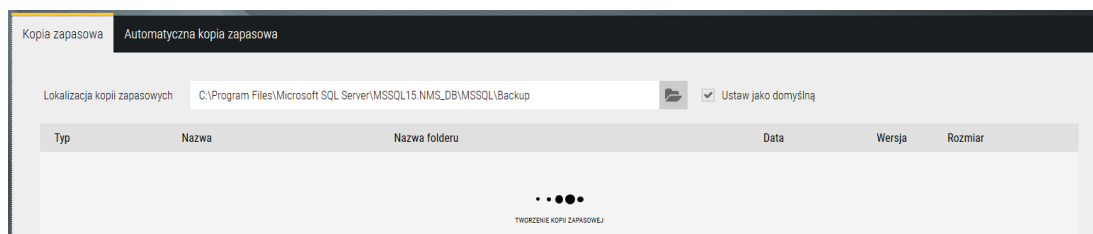
W tej zakładce można wykonać lub przywrócić kopię systemu.

Tworzenie kopii zapasowej

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 umożliwiającą jej usunięcie oraz ikona umożliwiającą 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.

System Konfiguracja Szablony Panele Zdarzenia Rejestracja czasu pracy

Ustawienia serwerów Ustawienia klienta **Kopia zapasowa** Grupy i operatorzy Licencje

Serwer **Kopia zapasowa** Automatyczna kopia zapasowa

SRV Lokalny

Twórz automatyczną kopię zapasową Cotygodniowo ☐ Usuń po [dni]

Lokalizacja kopii zapasowych C:\Program Files\Microsoft SQL Server\MSSQL15.NMS_DB\MSSQL\Backup

Godzina 12 : 00 : 00

Powtarzaj co [tygodnie] - 1 +

☒ Poniedziałek ☐ Wtorek ☐ Środa
☐ Czwartek ☐ Piątek
☐ Sobota ☐ Niedziela

USTAW

Kopia zapasowa Automatyczna kopia zapasowa

Twórz automatyczną kopię zapasową Codziennie ☐ Usuń po [dni]

Lokalizacja kopii zapasowych C:\Program Files\Microsoft SQL Server\MSSQL15.NMS_DB\MSSQL\Backup

Godzina 12 : 00 : 00

Powtarzaj co [dni] - 1 +

USTAW

Kopia zapasowa

Automatyczna kopia zapasowa

Twórz automatyczną kopię zapasową

Comiesięcznie

☐ Usuń po [dni]

Lokalizacja kopii zapasowych

C:\Program Files\Microsoft SQL Server\MSSQL15.NMS_DB\MSSQL\Backup

Godzina

12 : 00 : 00

Miesiąc

☐ Styczeń

☐ Luty

☐ Marzec

☐ Kwiecień

☐ Maj

☐ Czerwiec

☐ Lipiec

☐ Sierpień

☐ Wrzesień

☐ Październik

☐ Listopad

☐ Grudzień

Dzień miesiąca

☐ 1☐ 2☐ 3☐ 4☐ 5☐ 6☐ 7☐ 8☐ 9☐ 10☐ 11☐ 12☐ 13☐ 14☐ 15☐ 16☐ 17☐ 18☐ 19☐ 20☐ 21☐ 22☐ 23☐ 24☐ 25☐ 26☐ 27☐ 28☐ 29☐ 30☐ 31☐ Ostatni

USTAW

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.

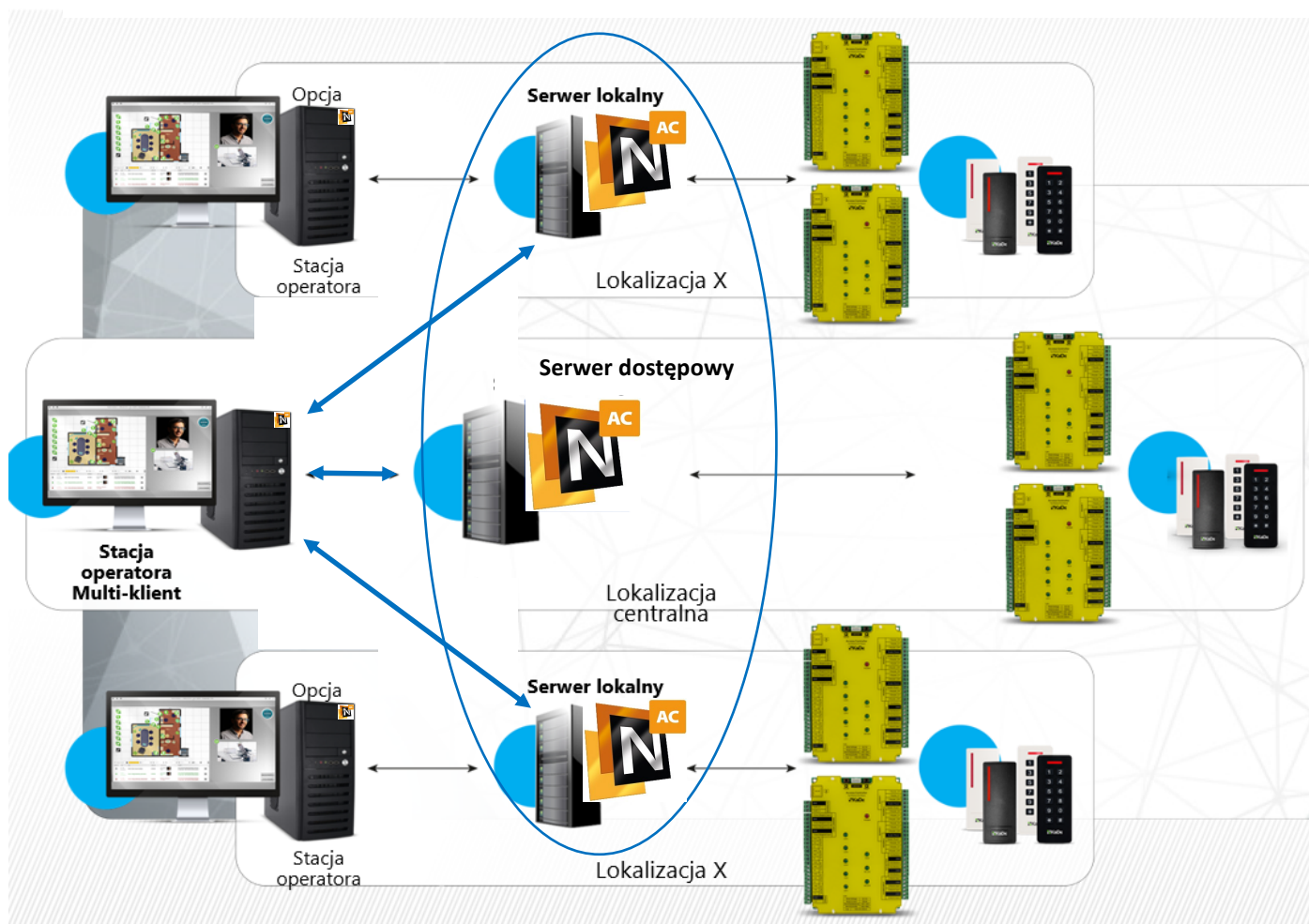
Serwery NOVUS MANAGEMENT SYSTEM AC zainstalowane w każdej z lokalizacji obsługują lokalne systemy oraz komunikują się z lokalnymi stacjami klienckimi tak jak w systemie bez multiserwerowości. Ta opcja pozwala połączyć wybrane serwery z grupą w celu równoczesnej konfiguracji i monitorowania tych podsystemów 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.

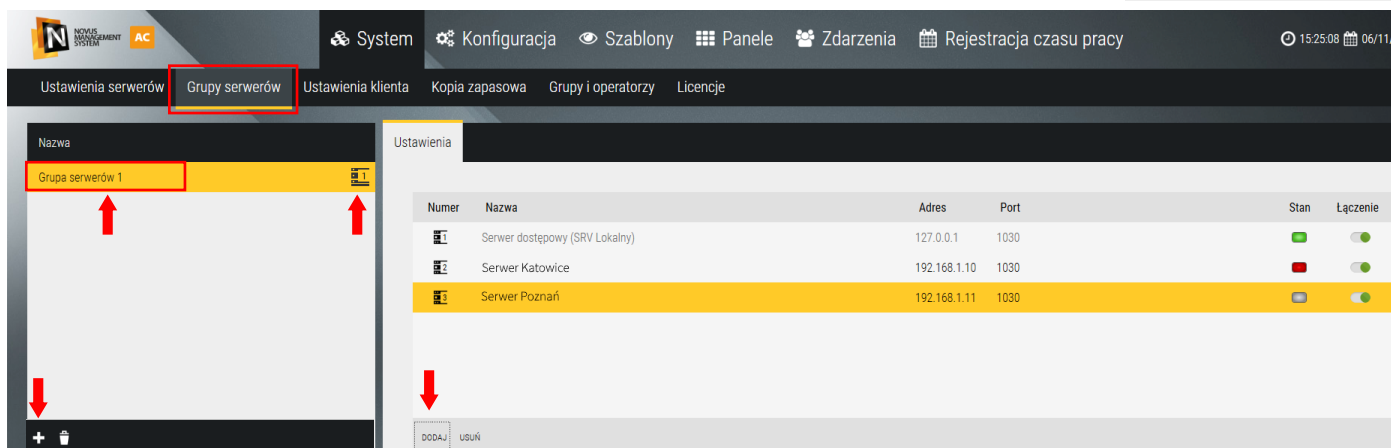
Multi-klient - stacja operatora (NOVUS MANAGEMENT SYSTEM AC Client) zalogowana do serwera dostępowego przez operatora posiadającego login wspólny dla wszystkich serwerów z grupy.

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 .

Podsumowanie licencji	
Stacje operatorskie	2
Punkty licencji	350
Funkcjonalność LPR	Tak
Pojazdy LPR	10
Funkcjonalność RCP	Tak
Użytkownicy RCP	10
Wiele serwerów	Tak
Identyfikator sprzętowy	



Dodaj - aby utworzyć grupę serwerów należy kliknąć na przycisku **+** (**Dodaj**) lewym dolnym rogu okna. Następnie w polu nazwy należy wpisać nazwę definiowanej grupy serwerów.

Nazwa

Po zdefiniowaniu grupy można do niej dodawać serwery, do których zostały dodane licencje na multiserverowość.

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.

Dodaj serwer

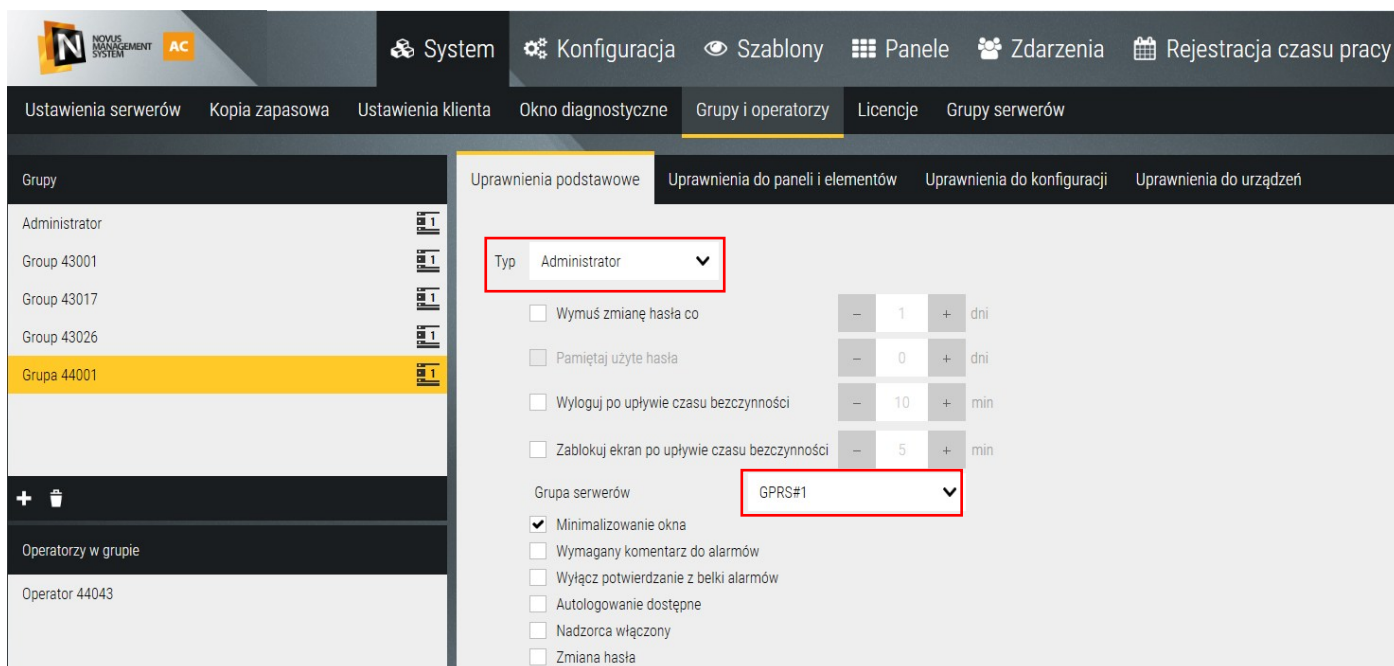
Adres:

Port:

ANULUJ OK

Status	Nazwa	Adres
 	Server 2071	127.0.0.1:1030
 	Server 8807	10.11.106.103:1030
 	Server 5723	10.11.106.199:1030

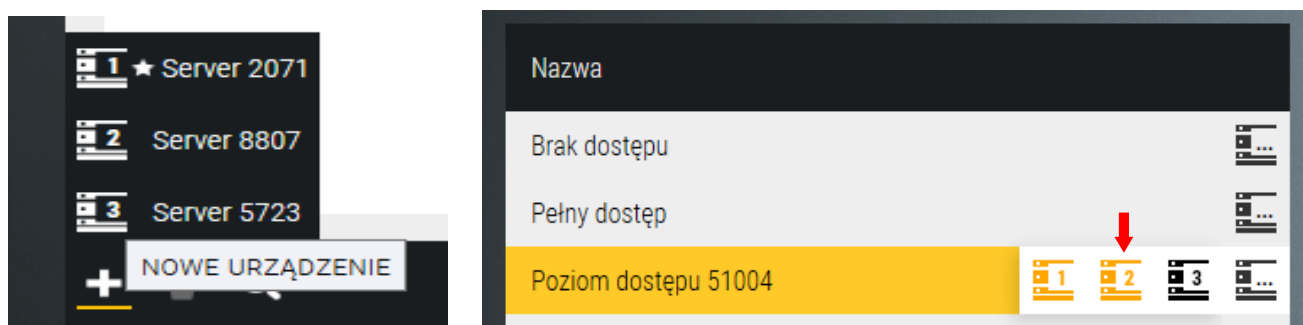
Po utworzeniu grupy serwerów należy zdefiniować na każdym z nich operatora przypisanego do tej grupy. To pozwoli uzyskać dostęp do podsystemów w obrębie grupy po zalogowaniu na jednej ze stacji klienckich w ramach tej grupy. Po dodaniu licencji na multi-serwerowość w zakładce definiowania operatorów 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.

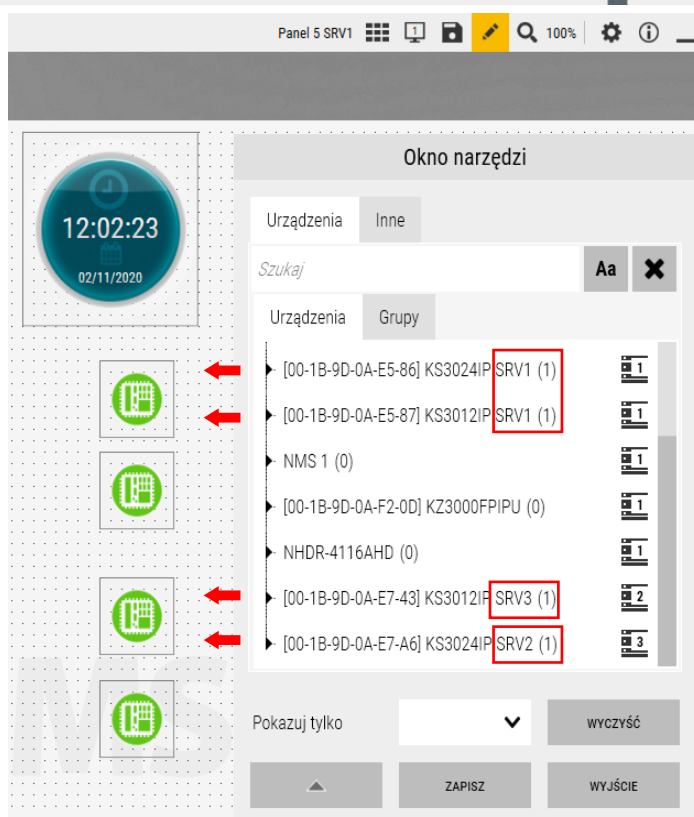


Jeżeli nowo dodany np. panel ma zawierać elementy skomunikowane z różnymi serwerami lokalnymi (kontrolery, drzwi itp.) to po dodaniu go do listy należy go przypisać do pozostałych serwerów w grupie, zapisać nowy panel i dopiero przejść do trybu edycji panelu.

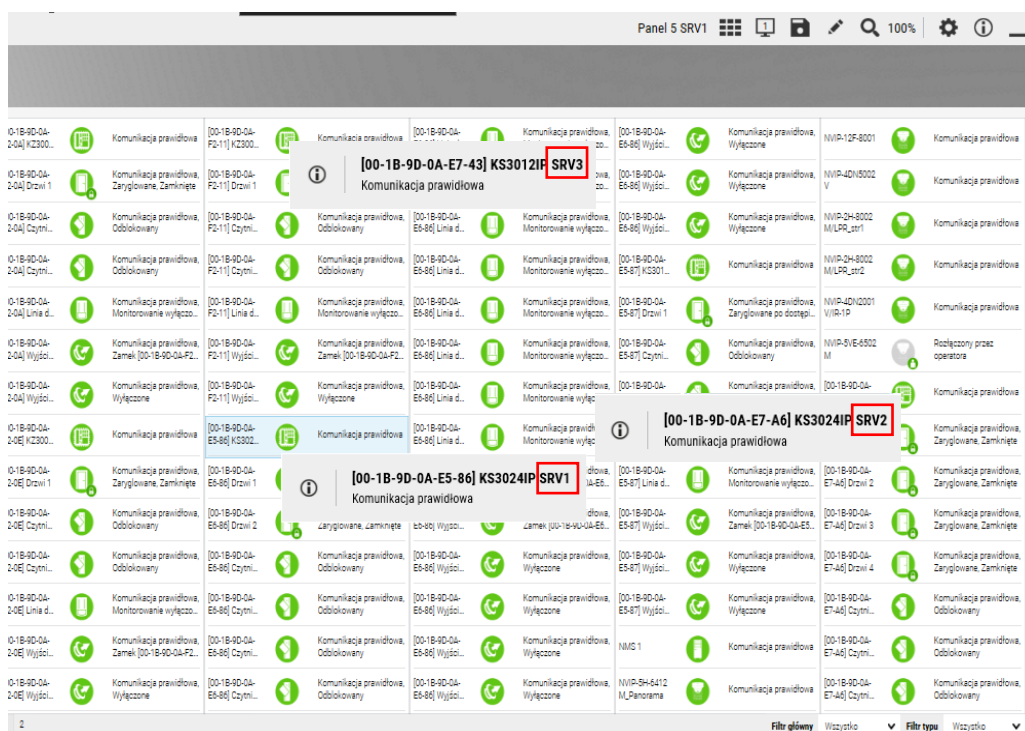
Panel 5 SRV1



Server 2071, Server 8807, Server 3230



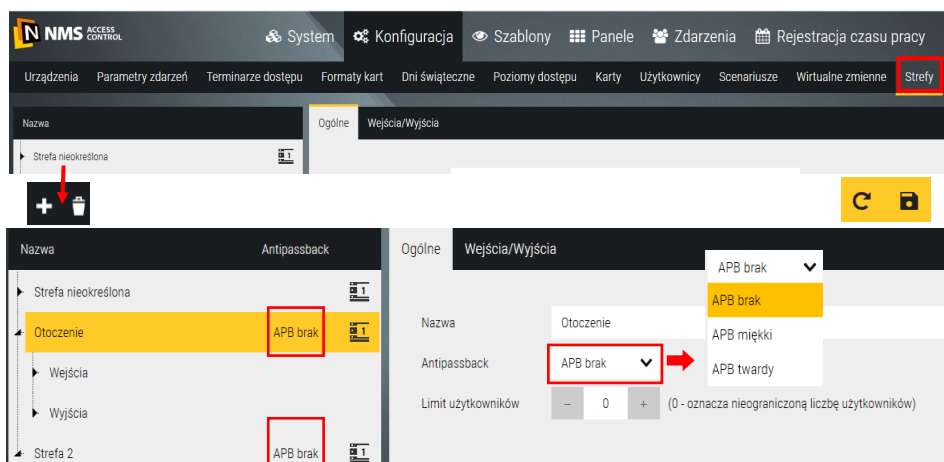
Podobnie ma to miejsce z przypadku tablicy synoptycznej.



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 antipassback 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.

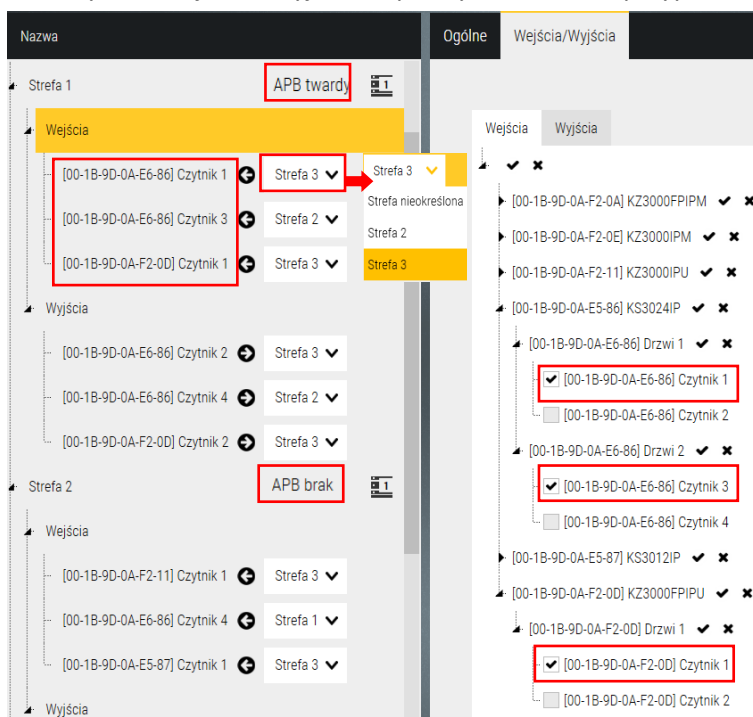
Na liście wyświetlana jest domyślna *Strefa nieokreślona*, która zawiera listę nowych użytkowników, którzy jeszcze nie poruszali się po obiekcie. Przed uruchomieniem tej funkcjonalności znajdują się w niej wszyscy użytkownicy dodani do bazy systemu. Po każdym odczycie karty na czytniku przypisanym do 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.

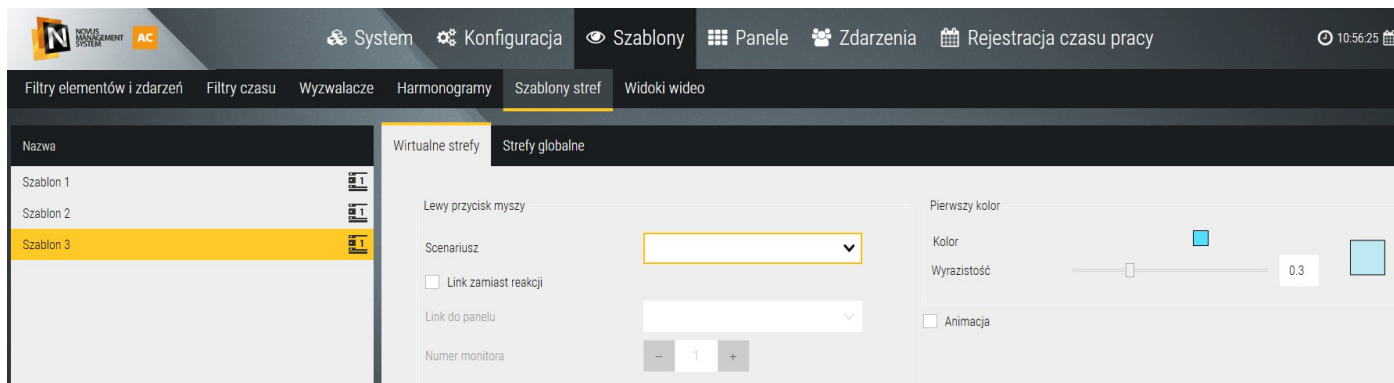
Po kliknięciu na przycisku **Dodaj** na liście w lewym oknie pojawia się nowa pozycja *Strefa X* - możemy do niej przypisać czytniki wejścia i wyjścia w prawym oknie. Po przypisaniu czytników wejściowych i wyjściowych należy przejść

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.

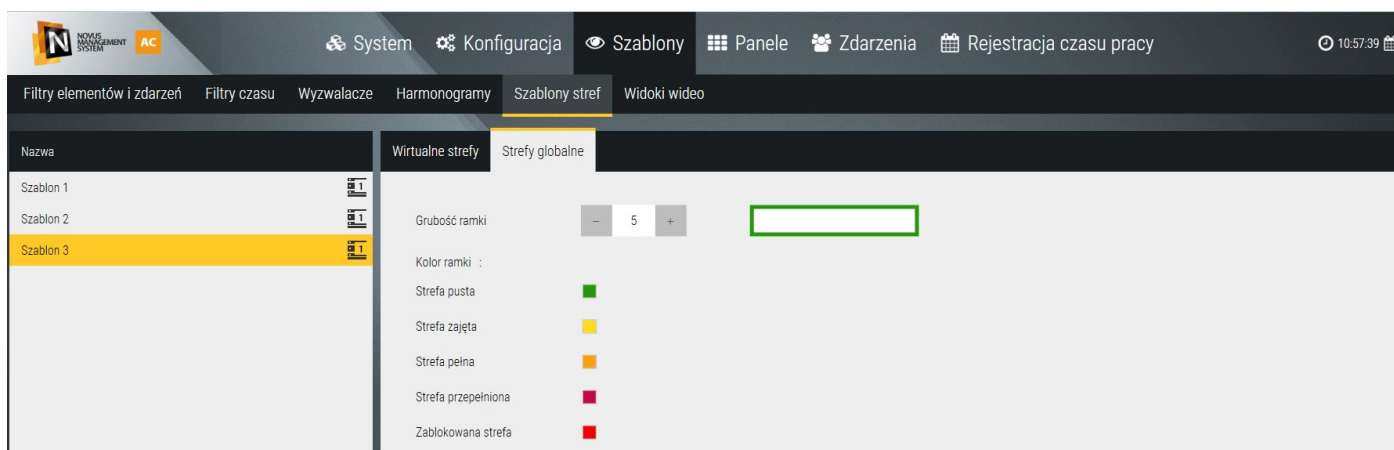


Wizualizacja stref globalnych na panelach

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.



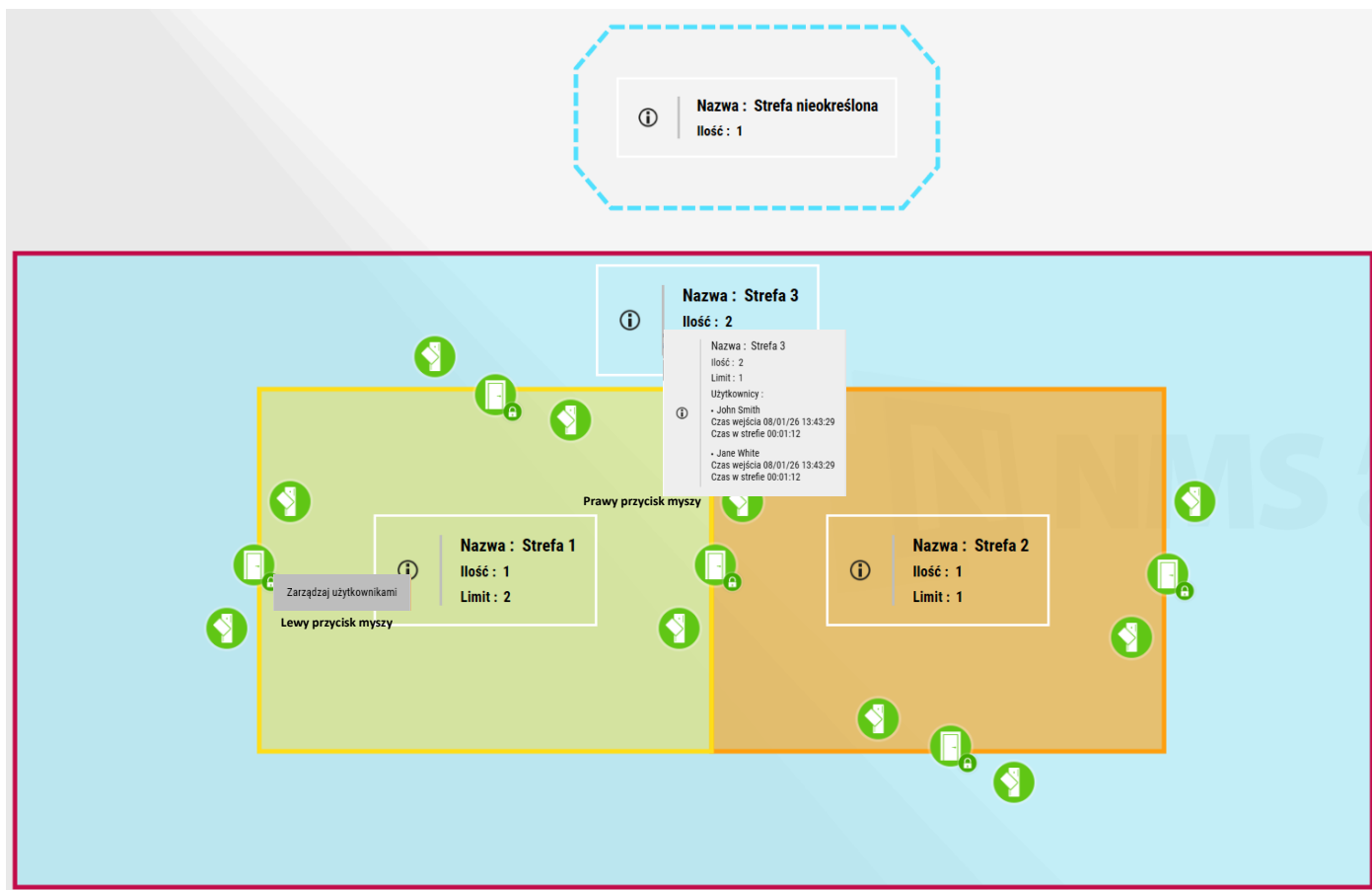
Parametry stref wirtualnych pokazane są powyżej. W przypadku użycia ich do wizualizacji stref globalnych należy dobrać zróżnicowaną kolorystykę tła. Następnie należy przejść do zakładki *Strefy globalne* i ustalić grubość ramki na obrzeżu strefy wirtualnej, której kolor sygnalizuje status strefy zgodnie z legendą.



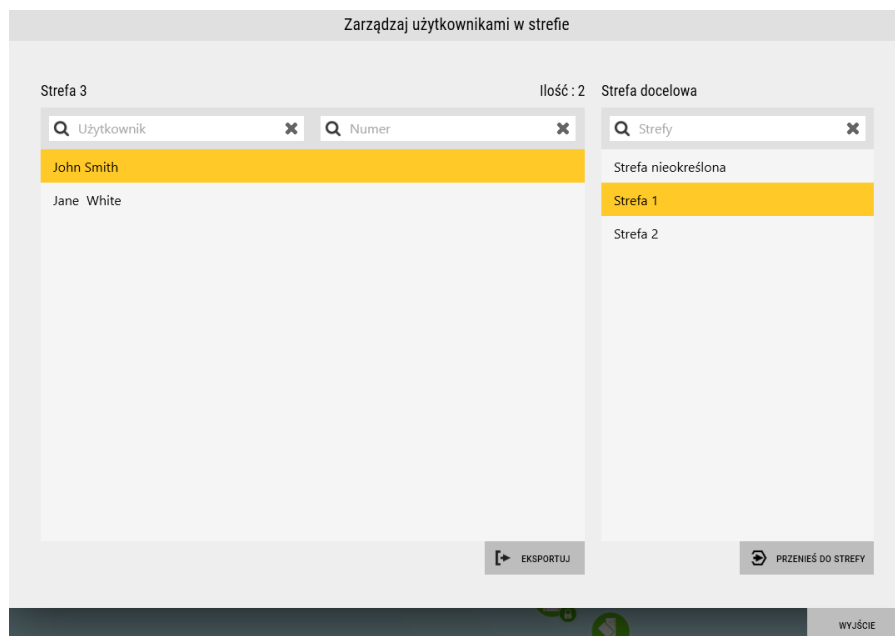
Po przejściu na panel należy wejść w tryb edycji i dodać wirtualną strefę, przypisać jej szablon oraz strefę globalną. Następnie należy zmodyfikować parametry strefy wirtualnej oraz globalnej (położenie, wielkość, skala) i zapisać.



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*.

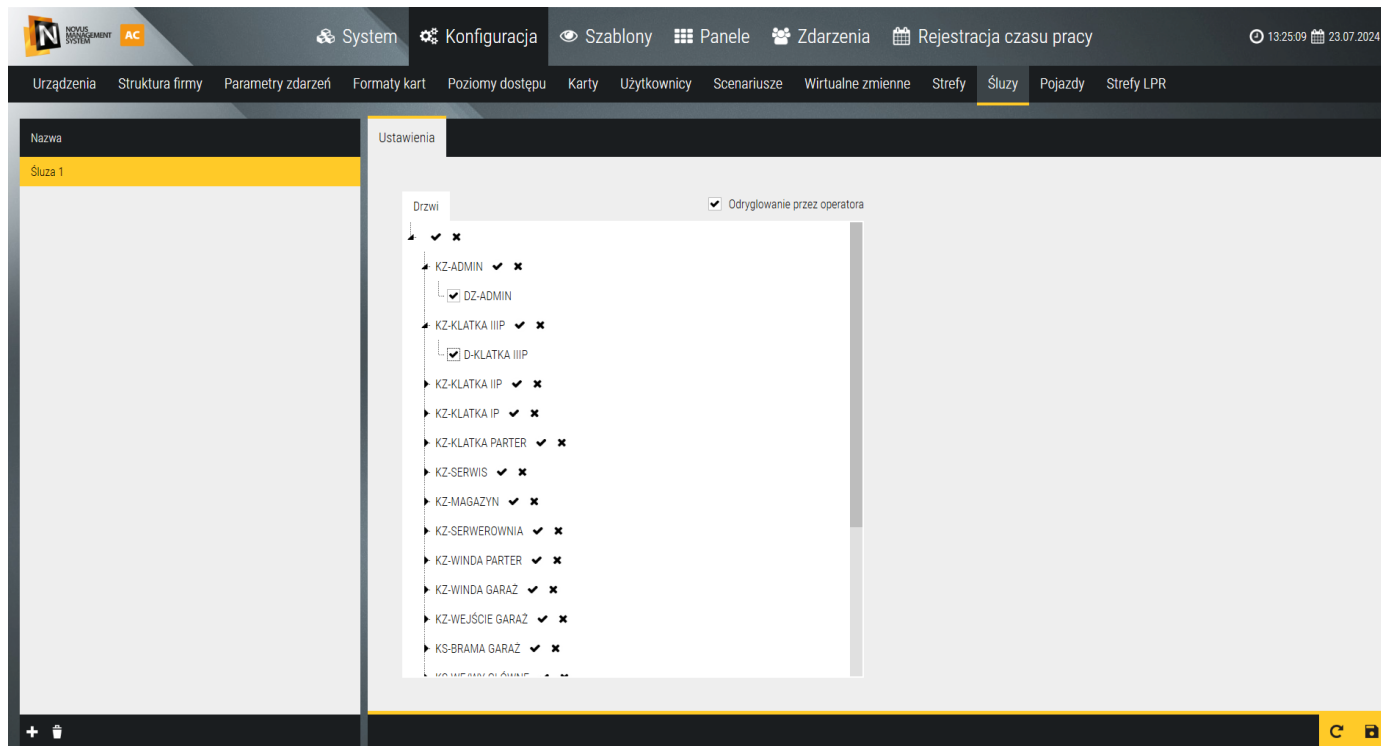
Nazwa: Strefa 1		
Ilość:	6	
Limit:	15	
Edward Asnyk		
Czas wejścia:	08/01/26 13:55:24	
Czas w strefie:	00:31:18	
Tomasz Kaśko		
Czas wejścia:	08/01/26 13:55:42	
Czas w strefie:	00:30:59	
Bartłomiej Nalepka		
Czas wejścia:	08/01/26 13:55:56	
Czas w strefie:	00:30:46	
Iwona Lułak		
Czas wejścia:	08/01/26 13:57:09	
Czas w strefie:	00:29:33	
Patryk Podstawka		
Czas wejścia:	08/01/26 13:57:30	
Czas w strefie:	00:29:12	
Amelia Paćko		
Czas wejścia:	08/01/26 13:57:39	
Czas w strefie:	00:29:03	

Nazwa: Strefa LPR 1		
Ilość:	0	
Limit:	Brak	
DWL88VE		
Maciej Atlas	Czas wejścia:	23/03/26 13:10:04
	Czas w strefie:	01:01:01
WSCUP19		
Stanisław Nasko	Czas wejścia:	23/03/26 13:10:04
	Czas w strefie:	01:01:01
WL6729H		
Maciej Nalewka	Czas wejścia:	23/03/26 13:10:04
	Czas w strefie:	01:01:01
WGM65CP		
Iwona Lułak	Czas wejścia:	23/03/26 13:10:04
	Czas w strefie:	01:01:01
WZY62NL		
Patryk Podstawka	Czas wejścia:	23/03/26 13:10:04
	Czas w strefie:	01:01:01
CT0552M		
Edward Asnyk	Czas wejścia:	23/03/26 13:10:04
	Czas w strefie:	01:01:01
WW488XA		
Patrycja Nowak	Czas wejścia:	23/03/26 13:10:04
	Czas w strefie:	01:01:01
WGM8LL3		
Agnieszka Malak		

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.

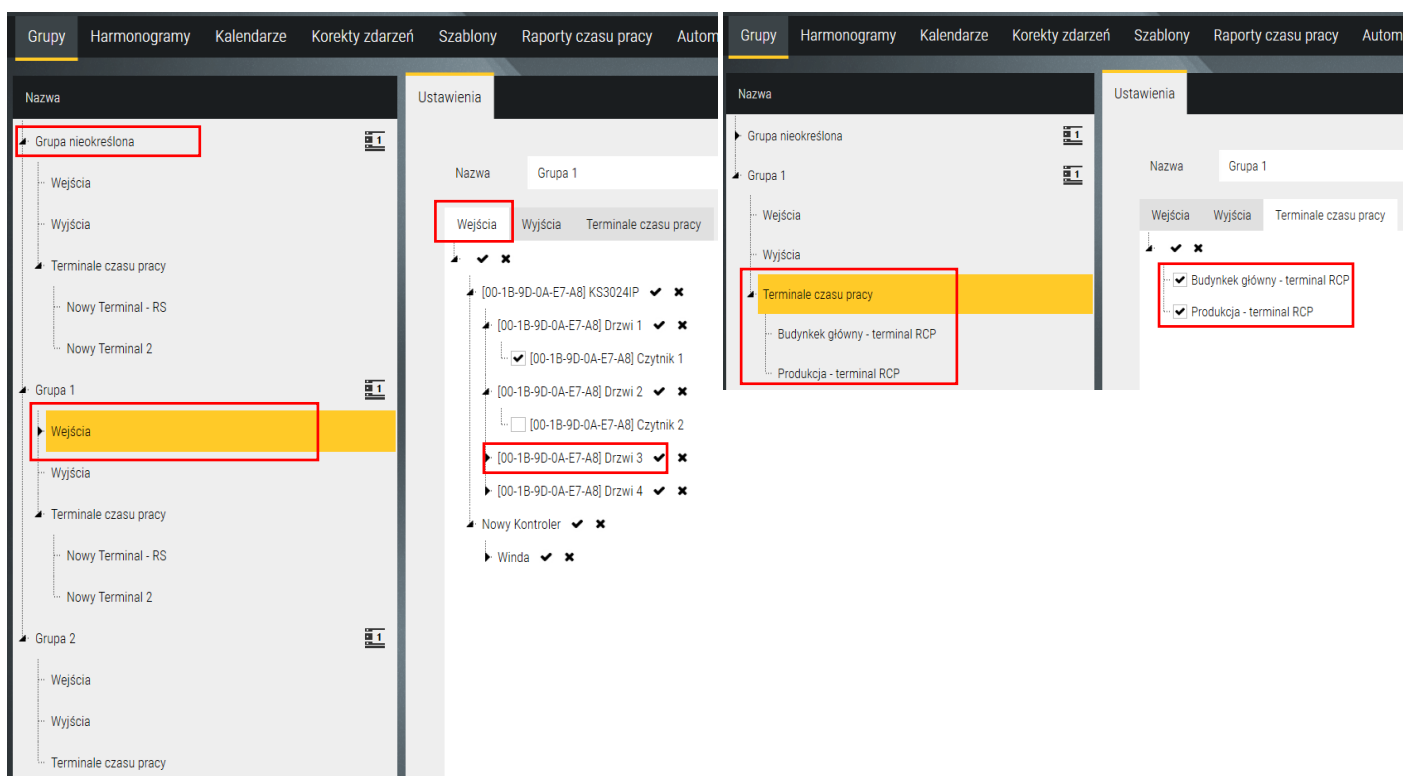
Terminal RCP umożliwia rejestrację dodatkowych we/wy w czasie pracy: na przerwę, służbowe, prywatne.

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:

Staly - oznacza, że pracownik ma stały czas pracy w ustalonych godzinach z przerwą.

Dobowa norma pracy - dobową normą czasu pracy.

Czas przerwy - czas odliczany od zarejestrowanego czasu pracy w procesie generowania raportu.

Dopuszczalny czas spóźnień i wcześniejszych wyjść - oznacza, że 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 skutkowałą 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 skutkowałą 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.

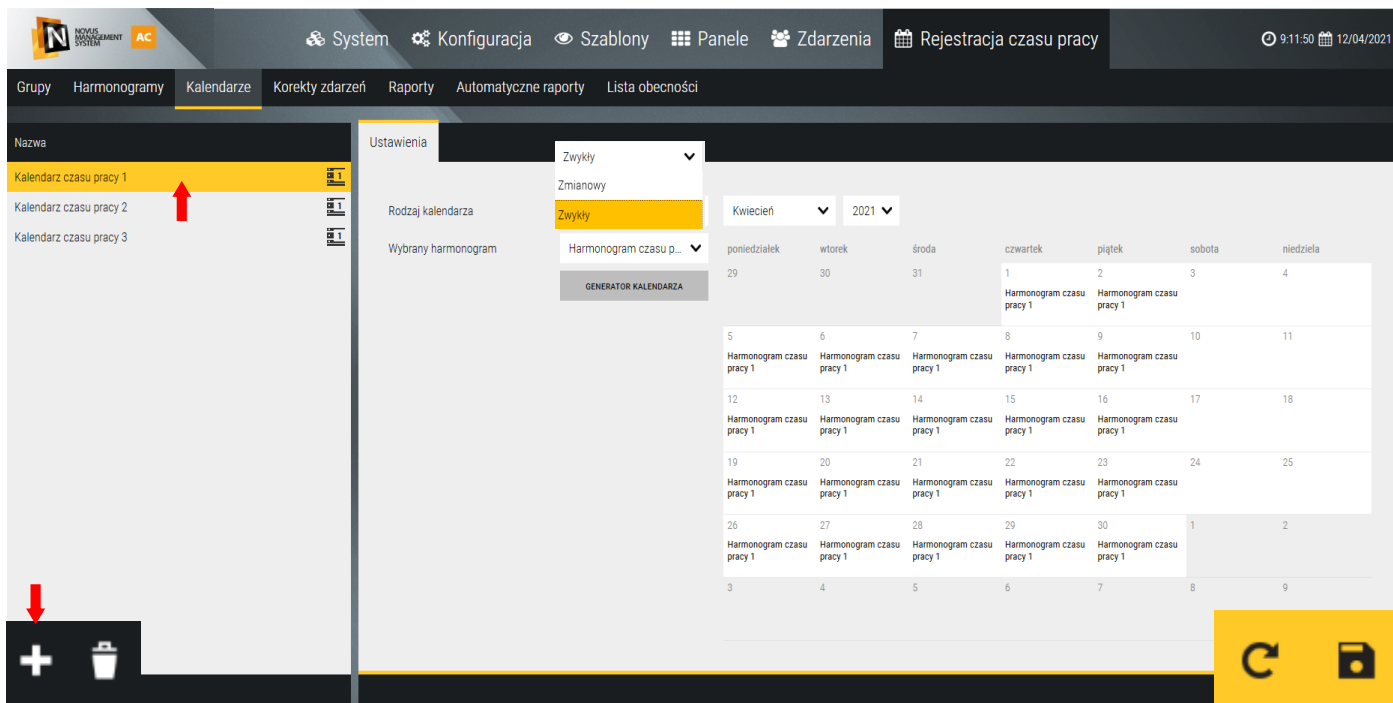
Kolor - kolor opisu harmonogramu jaki będzie wyświetlany w kalendarzu, ważne dla systemu zmianowego.

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.

Nienormowany - oznacza, że pracownik nie jest rozliczany według ustalonej dobowej ani miesięcznej normy czasu pracy. Harmonogram ten pozwala na elastyczne rejestrowanie czasu pracy bez konieczności definiowania sztywnych przedziałów godzin rozpoczęcia i zakończenia pracy. System ewidencjonuje rzeczywisty czas obecności na podstawie zarejestrowanych wejść i wyjść, nawet jeśli obejmują one wiele dób.

Kalendarze

Kalendarze są potrzebne do rozliczenia czasu pracy w zadanym okresie zgodnie z normą. W trakcie ich definiowania 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.

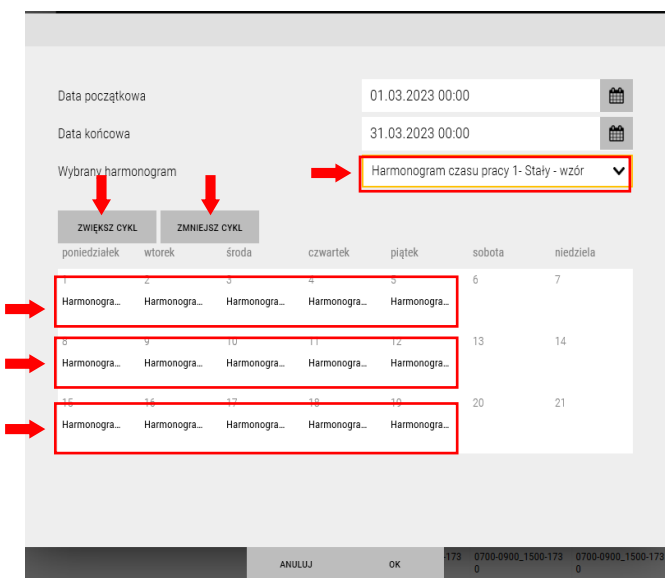


Ustawienia

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**.



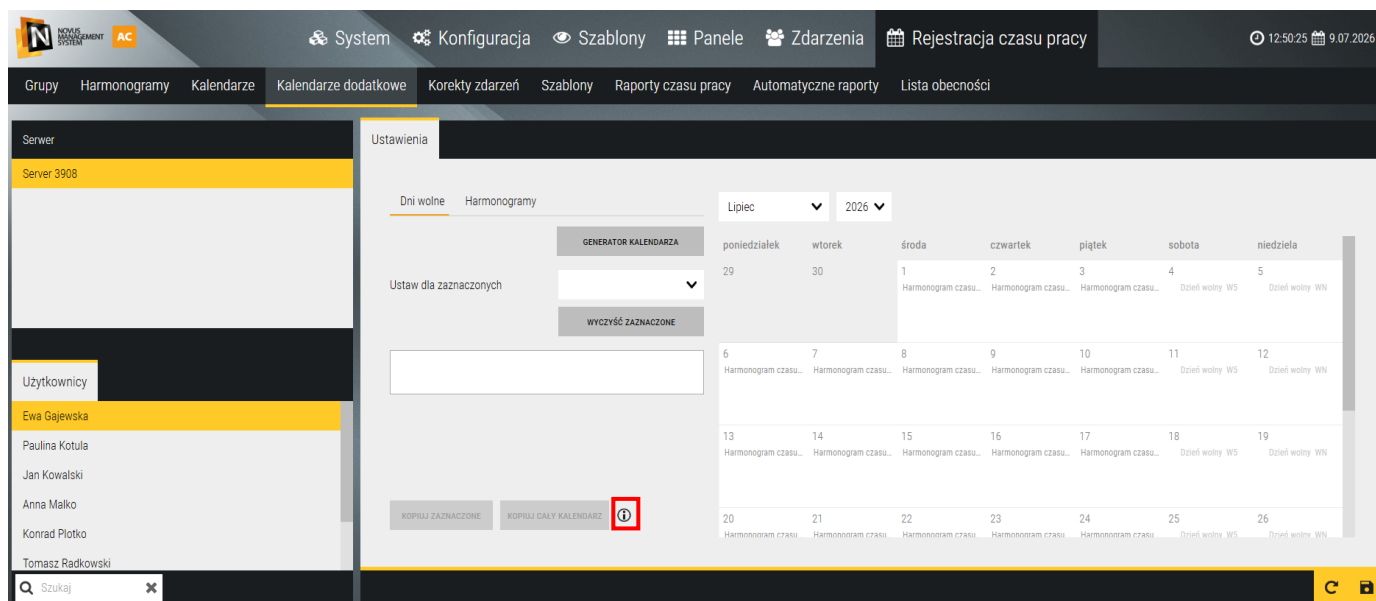
- ustawić datę początkową i końcową kalendarza
- wybrać harmonogram z rozwijanej listy
- klikając lewym przyciskiem myszy na dniach
- tygodnia dodać wybrany harmonogram

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.

Kalendarze dodatkowe

Kalendarze dodatkowe umożliwiają definiowanie indywidualnych wyjątków od standardowego kalendarza pracy przypisanego użytkownikowi. Dzięki temu można w prosty sposób modyfikować harmonogram pracy lub oznaczać wybrane dni jako dni wolne bez konieczności zmiany głównego kalendarza.

Przykładowo, użytkownik może posiadać standardowy harmonogram pracy od poniedziałku do piątku, przy czym sobota i niedziela są dniami wolnymi. W przypadku wystąpienia wyjątków, takich jak dodatkowy dzień wolny, praca w weekend lub zmiana godzin pracy w konkretnym dniu, możliwe jest wprowadzenie odpowiednich modyfikacji w kalendarzu dodatkowym.



UWAGA! Po najechnaniu kursorem na ikonę informacji wyświetlony zostanie szczegółowy opis zasad działania kalendarzy dodatkowych, w tym sposób nadpisywania harmonogramów i dni wolnych oraz reguły kopiowania zmian pomiędzy użytkownikami.

Moduł składa się z dwóch podzakładek:

Dni wolne - służy do przypisywania wybranym dniom określonych rodzajów dni wolnych.

Harmonogramy - umożliwia przypisywanie alternatywnych harmonogramów pracy dla wskazanych dni.

Mimo podziału na dwie podzakładki, widok kalendarza jest wspólny, dzięki czemu w jednym miejscu prezentowane są zarówno nadpisane dni wolne, jak i zmodyfikowane harmonogramy pracy.

Dla wybranego użytkownika można:

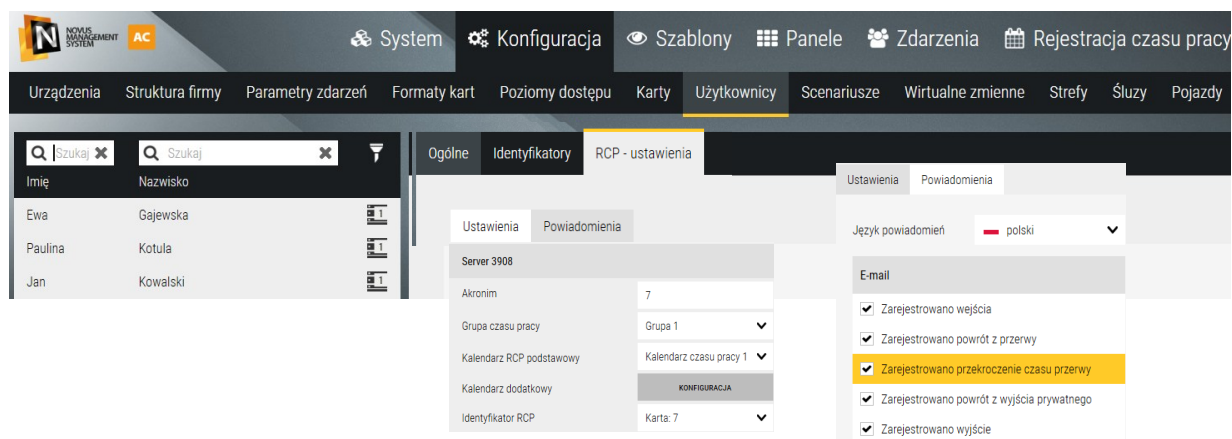
- przypisać określony rodzaj dnia wolnego do jednego lub wielu dni,
- zastąpić standardowy harmonogram innym harmonogramem pracy,
- usunąć wcześniej wprowadzone nadpisanie,
- kopiować zaznaczone zmiany do innego użytkownika,
- kopiować cały kalendarz dodatkowy wraz ze wszystkimi wprowadzonymi modyfikacjami do innego użytkownika.

Poniżej przedstawiono przykład nadpisania wybranych dni innym harmonogramem pracy lub oznaczenia ich jako dni wolne.

UWAGA! Aby poprawnie skopiować kalendarz dodatkowy, po wybraniu użytkowników, do których mają zostać przeniesione dane, należy zapisać zmiany, klikając ikonę *Zapisz* (dyskietka). W przeciwnym razie operacja kopiowania nie zostanie wykonana.

Możliwe jest również przejście do kalendarzy dodatkowych z poziomu ustawień użytkownika. W tym celu należy wybrać użytkownika, przejść do zakładki *RCP - ustawienia*, a następnie kliknąć przycisk **Konfiguracja**.

Użytkownicy - RCP

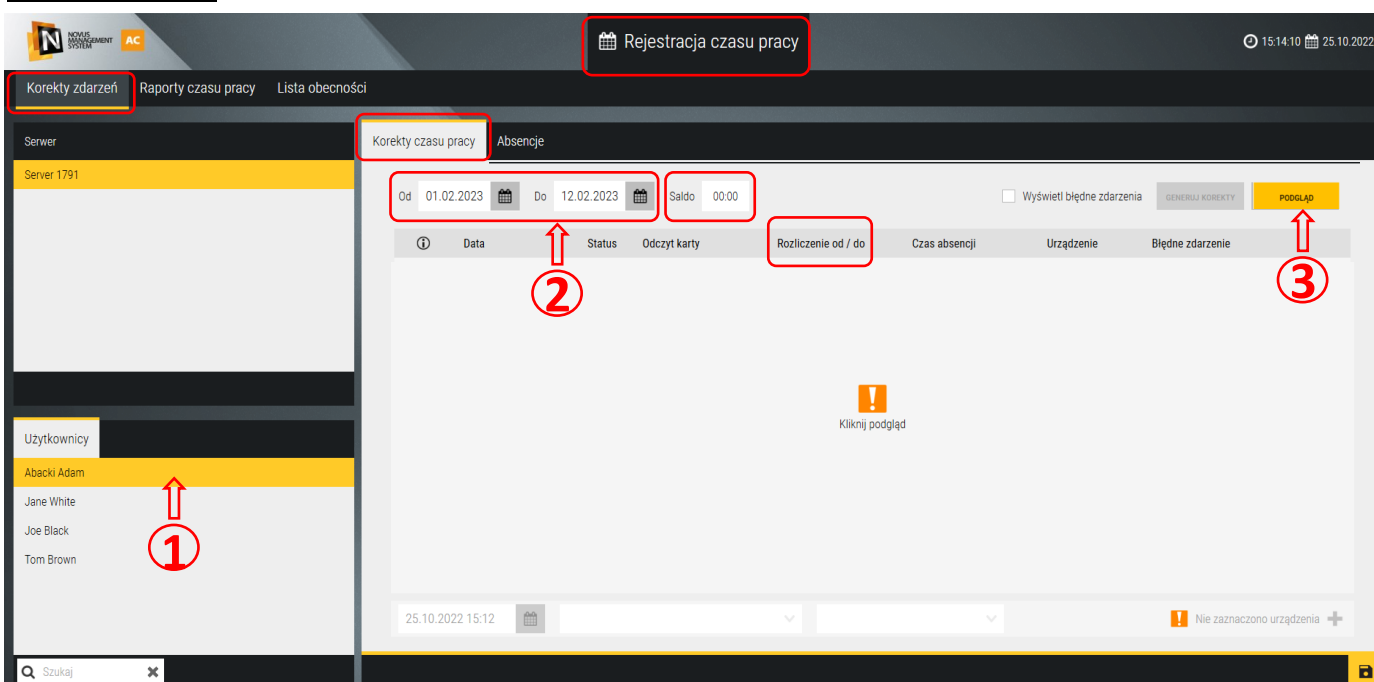


W tej zakładce można przypisać użytkownikowi grupę i kalendarz czasu pracy oraz powiadomienia. To umożliwia rejestrację we/wy na terminalu lub wybranych czytnikach oraz generowanie raportów czasu pracy.

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 wtedy 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.

The screenshot shows the 'Korekty czasu pracy' window with the 'Absencje' tab selected. The date range is from 01.02.2023 to 07.02.2023. The current balance is -00:15. The table below shows the work record for 07.02.2023.

Data	Status	Odczyt karty	Rozliczenie od / do	Czas absencji	Urządzenie	Błędne zdarzenie
07.02.2023	Wejście	07:00	07:30	--:--	TERMINAL R	☐
07.02.2023	Wyjście	17:00	15:30	--:--	TERMINAL R	☐
07.02.2023	Wyjście	17:00	15:45	--:--	TERMINAL R	☐

Red arrows indicate the change from 15:30 to 15:45 in the 'Rozliczenie od / do' column and the click of the 'Zatwierdź' icon.

„Rezerwa” czasowa na wyjściu wynosi 01:30 godziny w dniu 07.02.2023.

Saldo i godzina końca pracy po korekcie odpracowania.

The screenshot shows the same window after the correction. The balance is now 00:00. The table below shows the updated work record for 07.02.2023.

Data	Status	Odczyt karty	Rozliczenie od / do	Czas absencji	Urządzenie	Błędne zdarzenie
07.02.2023	Wejście	07:00	07:30	--:--	TERMINAL R	☐
OD 07.02.2023	Wyjście	17:00	15:45	--:--	TERMINAL R	☐

The 'OD' (odpracowanie) label is now visible at the start of the second row. The end time remains 15:45.

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.

PZ	08.02.2023	Wejście	08:00	08:00	--:--	TERMINAL RCF	☐		
PZ	08.02.2023	Wyjście	16:00	16:00	--:--	TERMINAL RCF	☐		

Jeśli wszystkie parametry zostały ustawione poprawnie, wprowadzone zmiany należy zapisać, korzystając z symbolu **Dyskietki**. Po zapisie ikona **Kosza** znika.

08.02.2023 08:00



TERMINAL RCP W-WA I

▼

Wejście

▼

Odczyt karty (OK)

▼

+



Odczyt karty (OK)

Praca zdalna (PZ)



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 pojawia 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**).

Generator korekt

Data początkowa

23.03.2023



Data końcowa

24.03.2023



Godziny korekt

08 : 00

+

-

16 : 00

+

-

Powód korekt

Odczyt karty (OK)



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*).

Od	01.09.2022 00:00	Do	30.09.2022 23:59	☒ Wyświetl błędne zdarzenia	GENERUJ KOREKTY	PODGLĄD
Data	Status	Czas	Urządzenie	Błędne zdarzenie		
OK	01.09.2022	Wejście	08:00:00	Terminal RCP W-WA I	☒	
OK	01.09.2022	Wyjście	16:30:00	Terminal RCP W-WA I	☐	
	02.09.2022	Wejście	13:59:00	Terminal RCP W-WA I / Drzwi	☐	

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 indywidualnych, 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 mają 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 ją przesunąć w górę lub w dół.

Sortowanie (występuje tylko dla raportów Lista obecności) - umożliwia definiowanie wielopoziomowego sortowania wyświetlanych danych. Sortowanie wykonywane jest zgodnie z kolejnością określoną w kolumnie *Kolejność*, gdzie poziom 1 ma najwyższy priorytet i jest stosowany jako pierwszy.

W przedstawionym przykładzie 1 dane są w pierwszej kolejności sortowane według kolumny *Ostatni odczyt* w kierunku malejącym, a następnie według kolumny *Nazwisko* w kierunku rosnącym.

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:

Zakres czasu: Miesięczny ▼ Marzec ▼ 2023 ▼ Szablon: Szablon 10 - grupowy - AAT testy ▼ PODGLĄD

W zakresie czasu mamy wyboru trzy opcje:

1. Z całego miesiąca (domyślnie poprzedniego)

Zakres czasu: Comiesięcznie ▼ Listopad ▼ 2020 ▼

2. Z zakresu czasu ustawionego w wybranym filtrze czasu

Zakres czasu: Filtr ▼ Filtr czasu 46002 ▼

3. Z zakresu zdefiniowanego według kalendarza

Zakres czasu: Własny ▼ Od: 01/11/20 00:00 Do: 30/11/20 23:59

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**.

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.

Użytkownik: Jane White, Dział: Programiści, Zakres czasu: 01.02.2023 - 28.02.2023, Norma pracy (godz.): 184:00

Generuj raport

Format pliku: PDF ▼ PDF
Tytuł: Raport
Orientacja: Poziomo ▼
Ścieżka: C:\Program Files (x86)\NMS
Podsumowanie: Od: 01.03.2023 00:00:00, Do: 31.03.2023 23:59:59, Ilość: 0

ANULUJ OK 144

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

Imię i nazwisko	Numer karty	Dział	Stanowisko	Zakres czasu	Zarejestrowany cza...	Nadgodziny	Saldo ujemne
Jane White	3175667	Handlowy		01.03.2021 - 31.03.2021	00:15	00:00	-167:45
Ewa Gajewska	8457969	Handlowy		01.03.2021 - 31.03.2021	00:00	00:00	-184:00
Jan Kowalski	2628269842	Handlowy		01.03.2021 - 31.03.2021	00:00	00:00	-184:00
Tom Brown	274648418	Handlowy		01.03.2021 - 31.03.2021	00:05	00:00	-167:55
Adam Czarny	2628395666	Handlowy		01.03.2021 - 31.03.2021	00:00	00:00	-168:00

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:

Zakres czasu: Miesięczny, Marzec, 2023, Szablon: Szablon 10 - grupowy - AAT testy, PODGLĄD

W zakresie czasu mamy wyboru trzy opcje:

1. Z całego miesiąca (domyślnie poprzedniego).

Zakres czasu: Comiesięcznie, Listopad, 2020

2. Z zakresu czasu ustawionego w wybranym filtrze czasu

Zakres czasu: Filtr, Filtr czasu 46002

3. Z zakresu zdefiniowanego według kalendarza

Zakres czasu: Własny, Od: 01/11/20 00:00, Do: 30/11/20 23:59

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

Jednostka: Programiści, Zakres czasu: 01.02.2023 - 28.02.2023, Użytkownicy: 10

Generuj raport

Format pliku: PDF, Tytuł: Raport, Orientacja: Poziomo, Ścieżka: C:\Program Files (x86)\NMS

Podsumowanie: Od: 01.03.2023 00:00:00, Do: 31.03.2023 23:59:59, Ilość: 0

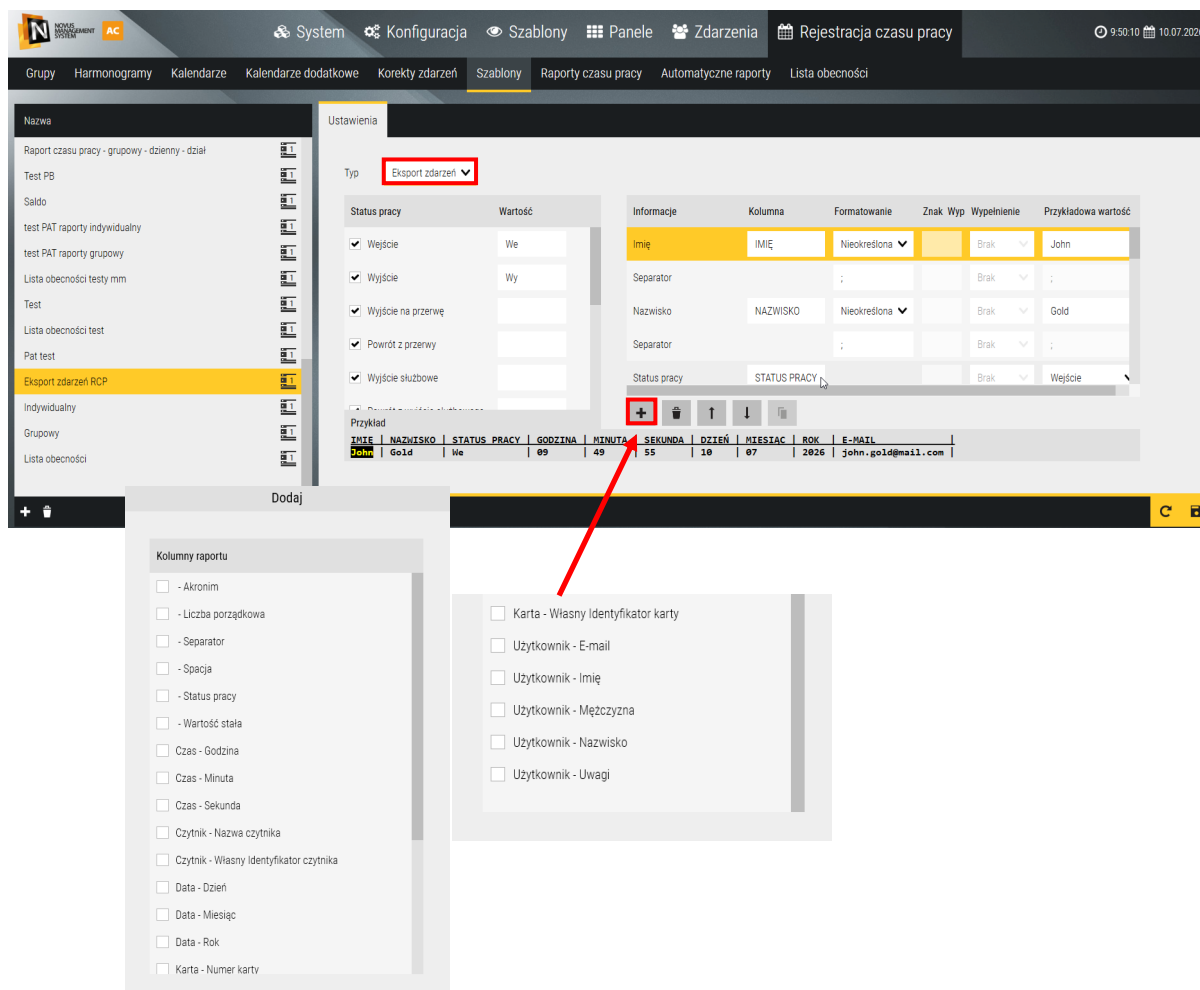
ANULUJ OK

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

Eksport zdarzeń RCP

Funkcjonalność Eksport zdarzeń RCP służy do tworzenia własnego formatu eksportu zdarzeń RCP. Dzięki temu można przygotować pliki zgodne z wymaganiami systemów kadrowo-płacowych lub zewnętrznych programów do rozliczania czasu pracy. Aby skonfigurować raport typu Eksport zdarzeń RCP, należy przejść do zakładki *Szablony* i wybrać typ **Eksport zdarzeń**. Po wybraniu tego typu wyświetlone zostanie okno konfiguracji szablonu.



W sekcji *Status pracy* znajduje się lista statusów pracy, które mają zostać uwzględnione i zapisane do raportu. Dla każdego statusu można określić własną wartość w polu **Wartość**, która zostanie zapisana w wygenerowanym pliku.

Status pracy	Wartość
☒ Wejście	We
☒ Wyjście	Wy
☒ Wyjście na przerwę	
☒ Powrót z przerwy	
☒ Wyjście służbowe	
☐ Powrót z przerwy służbowej	

Obok znajduje się sekcja służąca do definiowania kolumn eksportu. Za pomocą przycisku dodawania można wybrać informacje, które mają zostać uwzględnione w raporcie, np. imię, nazwisko, status pracy oraz datę i czas zdarzenia. Data może zostać wyeksportowana w postaci oddzielnych pól: dzień, miesiąc i rok, natomiast czas jako osobne pola: godzina, minuta i sekunda.

Informacje	Kolumna	Formatowanie	Znak Wyp	Wypełnienie	Przykładowa wartość
Imię		Nieokreślona ▼		Brak ▼	John
Separator		:		Brak ▼	:
Nazwisko		Nieokreślona ▼		Brak ▼	Gold
Separator		:		Brak ▼	:
Status pracy				Brak ▼	Wejście

+
-
↑
↓

Po dodaniu nazwy co najmniej jednej kolumnie w dolnej części okna zostanie wyświetlony podgląd przykładowego raportu. Wygenerowany raport będzie zawierał wybrane pola danych w postaci kolejnych kolumn.

IMIE	NAZWISKO	STATUS PRACY	GODZINA	MINUTA	SEKUNDA	DZIEŃ	MIESIAC	ROK
John	Gold	We	10	58	12	10	07	2026

Gdy do szablonu nie zostanie dodana żadna kolumna zawierająca nazwę pola, eksportowane informacje będą rozdzielane wyłącznie za pomocą zdefiniowanych separatorów, bez nagłówków kolumn. W zależności od wymagań programu odbierającego dane można zastosować separatory: ; , |

Przykład

John;Gold;We;09;49;55;10;07;2026;john.gold@mail.com;

Domyślnie dla każdej kolumny opcja *Formatowanie* ustawiona jest na wartość **Nieokreślona**. Po wybraniu konkretnej wartości liczbowej określana jest maksymalna liczba znaków, która może zostać wyeksportowana dla danego pola. Jeżeli długość danych przekroczy wskazaną wartość, informacje zostaną skrócone.

Opcja *Wypełnienie* określa sposób skracania danych:

- **Początek** - usuwane są znaki znajdujące się na początku tekstu.
- **Koniec** - usuwane są znaki znajdujące się na końcu tekstu.

Wypełnienie

Początek ▼

Początek

Koniec

Formatowanie

Nieokreślona ▼

Nieokreślona

1

2

3

4

5

6

7

8

Przykład poniżej zmiana opcji *Formatowanie* na **2** oraz opcji *Wypełnienie* **Początek**, eksportowana wartość zostanie ograniczona do dwóch ostatnich znaków. W rezultacie dwa pierwsze znaki imienia John zostały usunięte, a w raporcie wyświetlona zostanie wartość: hn.

IMIE	NAZWISKO	STATUS PRACY	GODZINA	MINUTA	SEKUNDA	DZIEŃ	MIESIAC	ROK	E-MAIL
hn	Gold	We	09	49	55	10	07	2026	john.gold@mail.com

Natomiast, jeśli w opcji *Formatowanie* zostanie ustawiona wartość większa niż liczba znaków eksportowanej informacji, brakujące miejsca zostaną uzupełnione znakami zdefiniowanymi w opcji *Znak Wypełnienia*.

Informacje	Kolumna	Formatowanie	Znak Wyp	Wypełnienie	Przykładowa wartość
Imię	IMIĘ	6	▼	Początek ▼	John

IMIĘ	NAZWISKO	STATUS PRACY	GODZINA	MINUTA	SEKUNDA	DZIEŃ	MIESIĄC	ROK
John	Gold	We	10	58	12	10	07	2026

Na dole widoczny jest podgląd przykładowego wiersza w wygenerowanym raporcie eksportu zdarzeń RCP. Dostępne są raporty w formatach .csv oraz .txt.

Indywidualny

Grupowy

Zakres czasu

Wlasny

▼

Od

01.07.2026 00:00

Do

15.07.2026 23:59

Szablon

Eksport zdarzeń RCP

▼

PODGLĄD

IMIĘ	NAZWISKO	STATUS PRACY	GODZINA	MINUTA	SEKUNDA	DZIEŃ	MIESIĄC	ROK	E-MAIL
TEST	TEST1	We	08	00	00	01	07	2026	test@test.com
TEST	TEST1	Wy	16	00	00	01	07	2026	test@test.com
TEST	TEST1	We	08	00	00	02	07	2026	test@test.com
TEST	TEST1	Wy	16	00	00	02	07	2026	test@test.com
TEST	TEST1	We	08	00	00	03	07	2026	test@test.com
TEST	TEST1	Wy	16	00	00	03	07	2026	test@test.com
TEST	TEST1	We	08	00	00	06	07	2026	test@test.com
TEST	TEST1	Wy	16	00	00	06	07	2026	test@test.com
TEST	TEST1	We	08	00	00	07	07	2026	test@test.com

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:

Ścieżka 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
Pracownik 1	1	Serwis	01.07.2024 - 31.07.2024	32:00
Pracownik 2	2	Serwis	01.07.2024 - 31.07.2024	72:00
Pracownik 3	2	Serwis	01.07.2024 - 31.07.2024	72:00
Pracownik 4	1	Serwis	01.07.2024 - 31.07.2024	72:00
Pracownik 5	3	Serwis	01.07.2024 - 31.07.2024	72:00
Pracownik 6	4	Serwis	01.07.2024 - 31.07.2024	72:00
Podsumowanie				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			
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
Pełni Ł...
01.07.2024 00:00 - 31.07.2024 23:59

Data	We-Wy nawrot	Zarejestrowana godzina wyjścia	Czas nagotowania pracy	Zarejestrowana godzina wyjścia	Czas zakazania pracy	Spóźnienie	Wczesniejsze wyjście	We-Wy przerwy	Zarejestrowany czas przerwy na przerwy	Zarejestrowany czas przerwy 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 sześciu stanów: obecność, nieobecność, absencje oraz wyjścia w czasie pracy. 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**. Dodatkowo dostępna jest opcja **Automatyczne odświeżanie**, która powoduje automatyczne odświeżenie listy po upływie 10 sekund od zarejestrowania pierwszego zdarzenia RCP.

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.

Po kliknięciu nagłówka dowolnej kolumny dane zostają posortowane zgodnie z wybranym kryterium. Pierwsze kliknięcie zawsze powoduje sortowanie w kolejności malejącej, natomiast kolejne kliknięcie zmienia kierunek sortowania na rosnący. Jednocześnie tworzony jest tymczasowy szablon oznaczony jako „Own”, zawierający aktualnie zastosowane ustawienia sortowania. Szablon ten może zostać następnie wykorzystany do wygenerowania raportu z zachowaniem wybranego sposobu sortowania.

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.

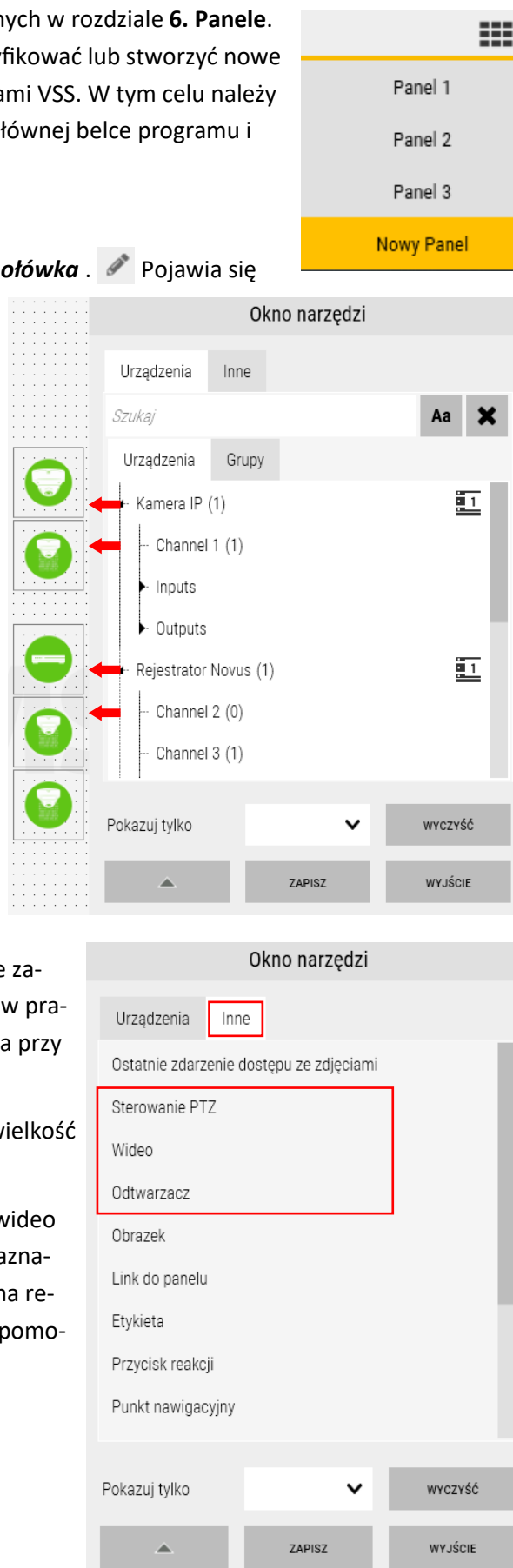
Po wyborze panelu można przejść do jego edycji za pomocą ikony **ołówka** . Pojawia się wtedy **Okno narzędzi**, w którym znajdują się wszystkie elementy do konfiguracji panelu. W zakładce *Urządzenia* możemy znaleźć dodane wcześniej urządzenia VSS. Można je przenieść na panel przeciągając samo urządzenie lub strumień 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:

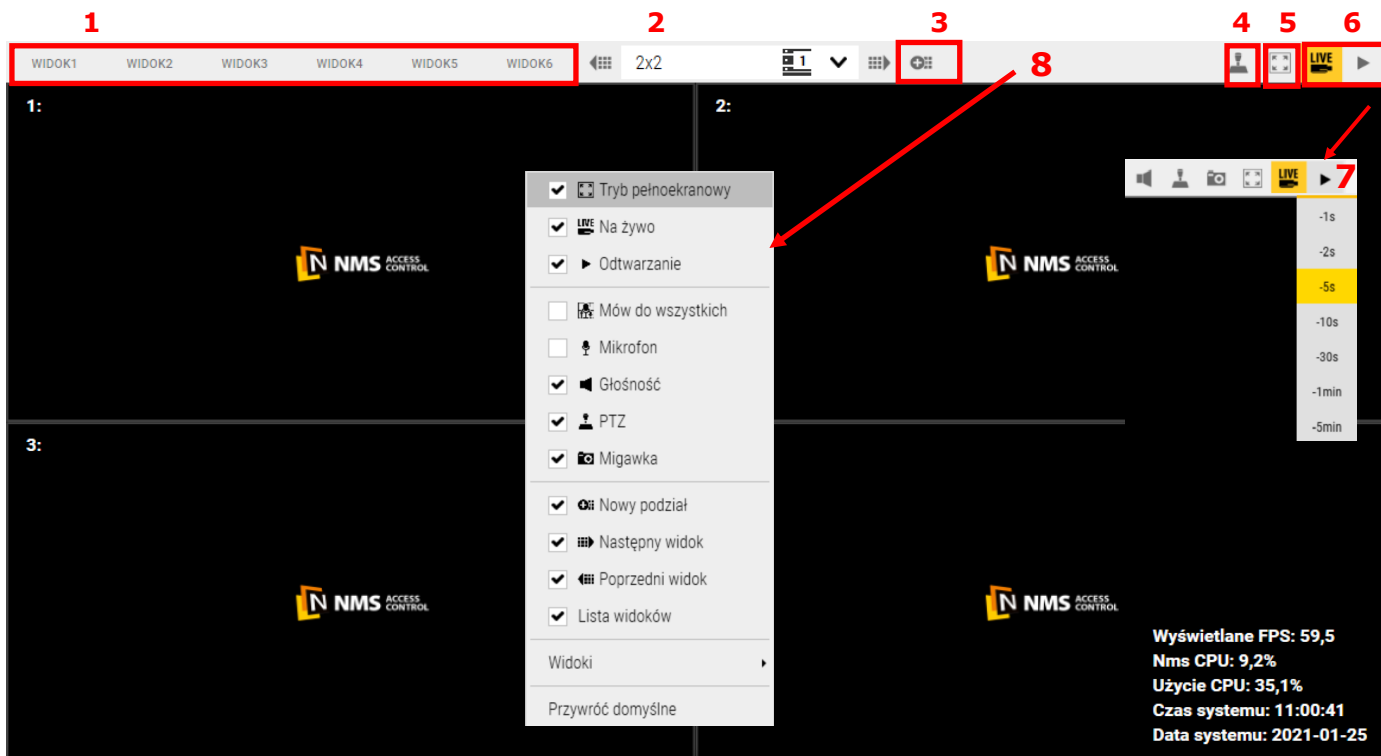
- Włącz OSD - checkbox włączający wyświetlanie w obrazie parametrów strumienia wideo.
- Zostaw podgląd otwarty - po zaznaczeniu tego checkboxa strumień wideo będzie się wyświetlał dopóki użytkownik nie zamknie go za pomocą czerwonego krzyżyka znajdującego się w prawym górnym rogu okienka. Przy wyłączonej 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 lista 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 któregośkolwiek 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.

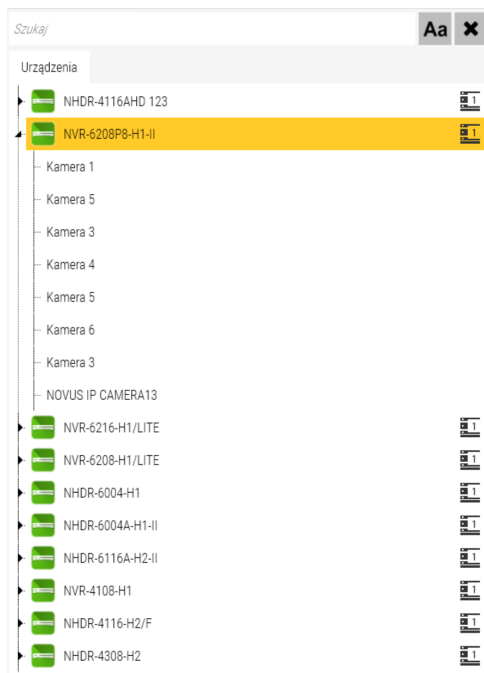
1. Przycisk **Preset** - służy do wywoływania presetu. Domyślnie jest wyszarzona, uaktywnia się po wybraniu numeru w niższej części narzędzia.
2. Przycisk **Pattern** - służy do wywoływania trasy obserwacji. Domyślnie jest wyszarzona, uaktywnia się po wybraniu numeru w niższej części narzędzia.
3. Przycisk **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.



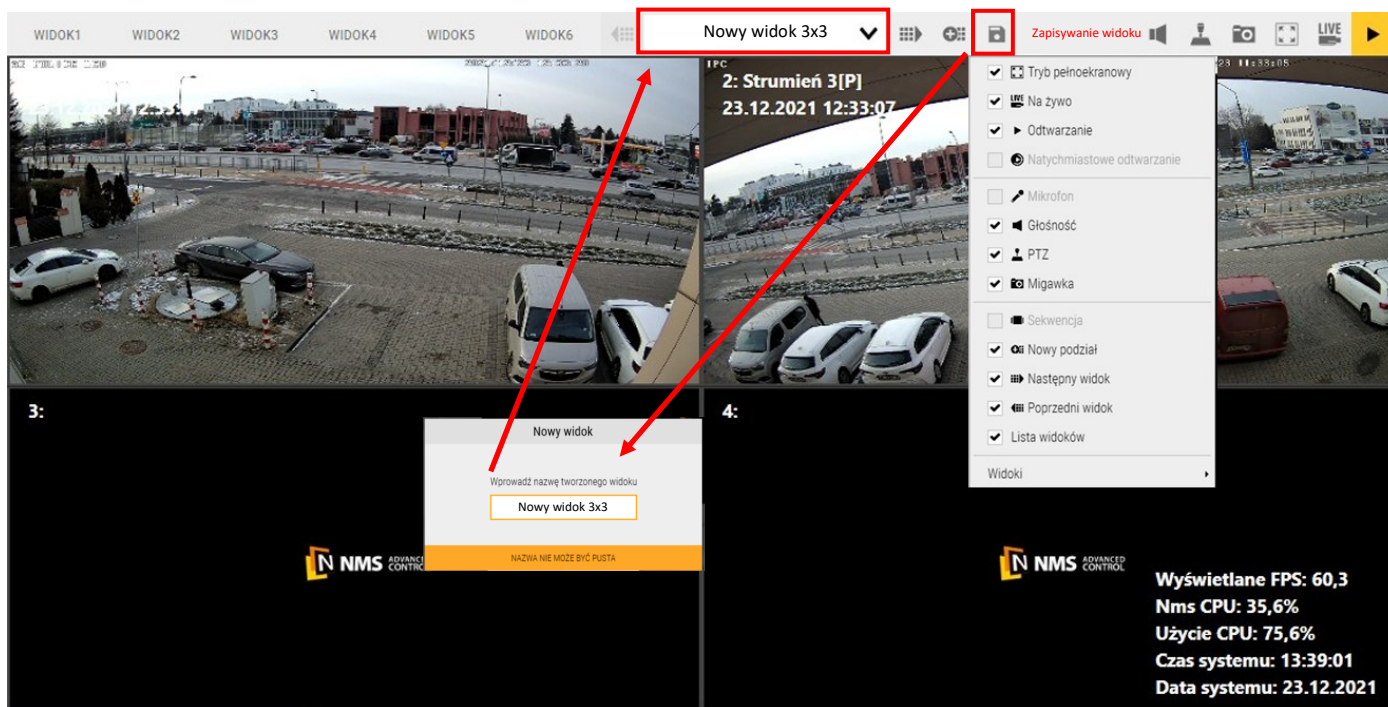
UWAGA! Dostępność poszczególnych funkcji zależy od funkcjonalności danego modelu kamery.

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

NVR-6432-H2/F		Rozłączony przez operatora	Strefa 1	Input 3		Komunikacja prawidłowa, Wyłączony
NVR-4416P16 H2/F-II_1		Rozłączony przez operatora		Input 4		Komunikacja prawidłowa, Wyłączony
NHDR-4316AH D		Rozłączony przez operatora		Input 5		Komunikacja prawidłowa, Wyłączony
NVR6304P4-H1-II		Komunikacja prawidłowa		Input 6		Komunikacja prawidłowa, Wyłączony
TEST		Komunikacja prawidłowa		Input 7		Komunikacja prawidłowa, Wyłączony
LPR DOL		Niedostępny		Output 0		Komunikacja prawidłowa, Wyłączony
LPR GORA		Niedostępny		Output 1		Komunikacja prawidłowa, Wyłączony
NOVUS IP CAMERA		Komunikacja prawidłowa		Output 2		Komunikacja prawidłowa, Wyłączony
Input 1		Komunikacja prawidłowa, Wyłączony		NVIP-2H-6732 M/LPR_GORA...		Rozłączona przez operatora
Input 2		Komunikacja prawidłowa, Wyłączony		Channel 2		Rozłączony przez operatora

1 2 3 4

2 3

Filtr główny Wszystko

Filtr typu Wszystko

4

- Okno urządzeń** - wyświetla wszystkie urządzenia, kanały, wejścia i wyjścia dostępne w systemie.
- Wybór strony** - umożliwia przełączanie między stronami z listą urządzeń i elementów systemu.
- Filtr główny** - opcja pozwalająca na wybór filtrów zdefiniowanych wcześniej w zakładce *Filtry elementów i zdarzeń*
- Filtr typu** - umożliwia zawężenie listy do wybranych kategorii, m.in.:
 - *Wszystko*
 - *Kontrolery*
 - *Kamery*
 - *Czytniki*
 - *Linie dozorowe*

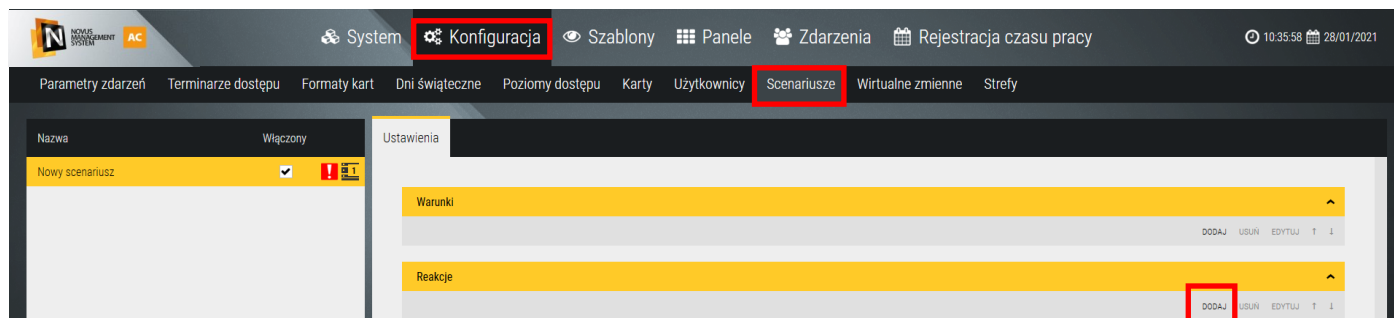
Aby zobaczyć obraz z danego urządzenia, należy przytrzymać kursor na ikonie **kanału** i przeciągnąć go na wybrany widok w narzędziu *Wideo*.

UWAGA! Funkcja działa tylko na ikonach **kanałów**, nie na całych urządzeniach.

9.5.6 Wyświetlanie strumieni wideo w reakcji scenariusza

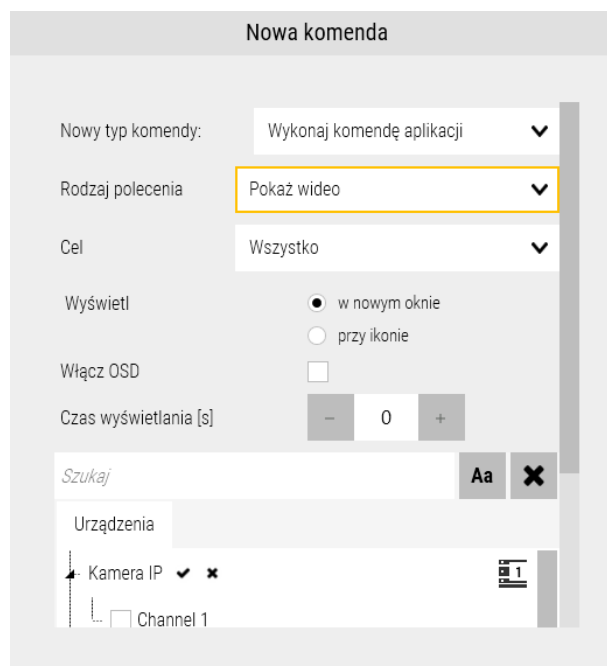
Integracja oprogramowania NOVUS MANAGEMENT SYSTEM AC z urządzeniami VSS dotyczy również wyświetlania strumieni wideo jako reakcję na dowolne zdarzenia dostępne w systemie. Ustawienia reakcji dokonuje się w menu *Konfiguracja*, zakładka *Scenariusze*.

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**. Pojawiają się dalsze opcje, jako rodzaj polecenia należy ustawić **Pokaż wideo**.



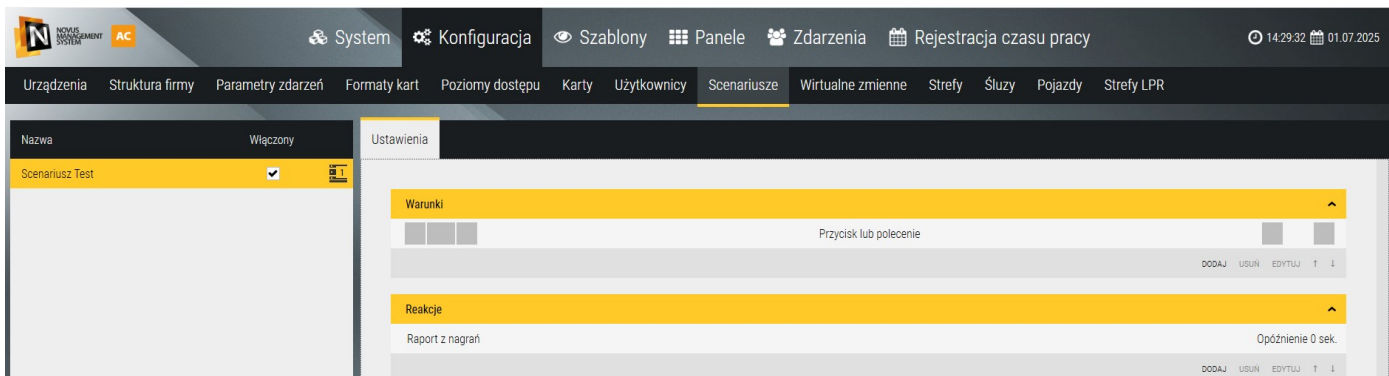
Pojawiają się dodatkowe opcje dotyczące wyświetlania:

- 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.



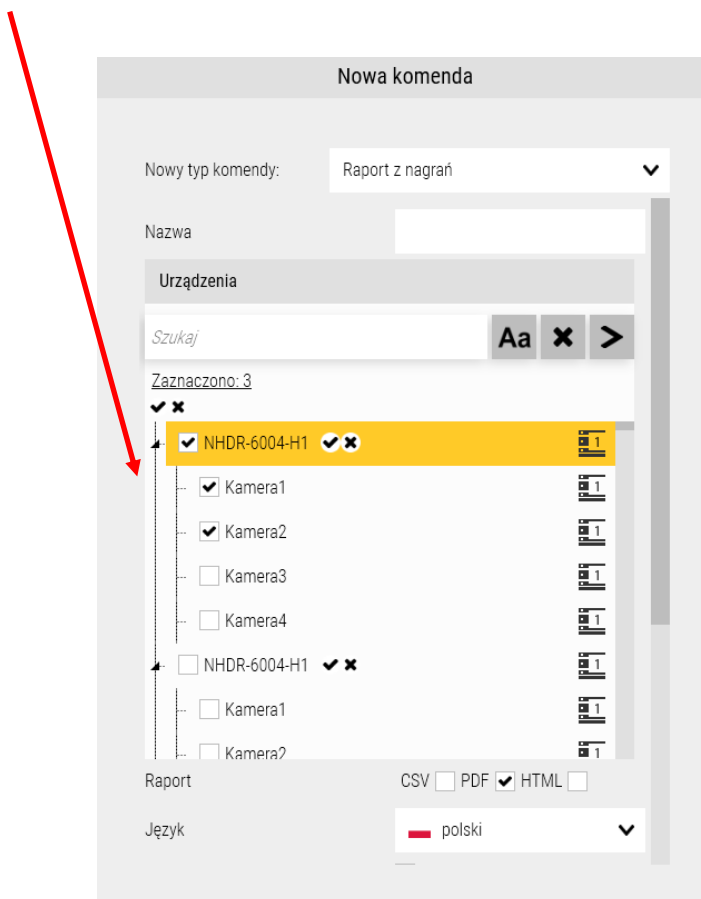
9.5.7 Generowanie raportów nagrań w reakcji scenariusza

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 określone 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
NVR-6208P8-H1-II, pierwszy	Kamera 1 Główny	LAN1: 192.168.6.10 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, Strumieniowanie	OK	20d 03:41:50	31.03.2026 04:28	20.04.2026 08:10	0d 00:03:35	Wyłączony	Wyłączony	NVR-6208P8-H1-II	1.4.13.85508B260127.N3V.U1(08118)
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 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 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 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 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 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 8 Główny						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: 192.168.6.10 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 00:15:44	27.04.2026 11:42:58	27.04.2026 11:58:42	0d 00:00:11	Wyłączony	Wyłączony	NVR-6208P8-H1-II	1.4.13.85508B260127.N3V.U1(08118)
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 funkcjonalności 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

DATA	NUMER REJESTRACYJNY	ZDJĘCIE	OPIS	UŻYTKOWNIK	INFORMACJA	AKCJE
16:09:33 23.11.2023	GGW5EE2		Wjazd - żądanie dostępu [GGW5EE2]	Nieznaný użytkownik		 GENERUJ BILET
16:09:16 23.11.2023	GKW2222		Wjazd - dostęp dozwolony, ważna rejestracja pojazdu [GKW2222] (UnknownZone -> Strefa LPR 1)	Jan Kowalski		
16:09:16 23.11.2023	GKW2222		Strefa - Nieprawidłowy przejazd dozwolony (GKW2222) (z Strefa LPR 1 do Strefa LPR 1)	Jan Kowalski		
16:08:59 23.11.2023	GKW52E2		Wjazd - żądanie dostępu [GKW52E2]	Nieznaný użytkownik		 GENERUJ BILET
16:08:32 23.11.2023	KKG5555		Wjazd - dostęp dozwolony, ważna rejestracja pojazdu [KKG5555] (UnknownZone -> Strefa LPR 1)	Anna Nowak		
16:08:32 23.11.2023	KKG5555		Strefa - Nieprawidłowy przejazd dozwolony (KKG5555) (z Strefa LPR 1 do Strefa LPR 1)	Anna Nowak		
16:08:09 23.11.2023	GEW55E2		Wjazd - żądanie dostępu [GEW55E2]	Nieznaný użytkownik		 GENERUJ BILET

NIEODCZYTANA TABLICA

Nazwa : Strefa nieokreślona
Liczba : 0

Nazwa : Strefa T+O
Liczba : 0
Limit : 128

Nazwa : Strefa Hala
Liczba : 0
Limit : 128

9.6.1 LPR - rozpoznawanie tablic rejestracyjnych

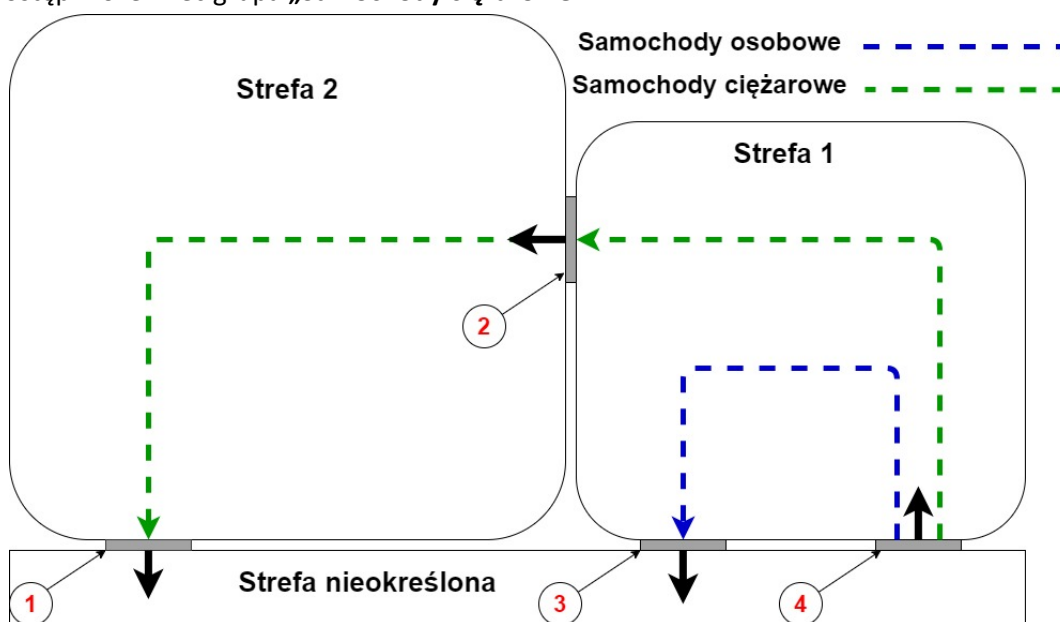
Oprogramowanie NOVUS MANAGEMENT SYSTEM AC zintegrowane z kamerami IP wyposażonymi w funkcję LPR pozwala na kontrolę dostępu pojazdów do zdefiniowanych wcześniej stref.

Przy założeniu, że:

Użytkownik chce mieć kontrolę 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 przełączników sterujących urządzeniami takimi jak np. szlabany czy bramy.

Konfiguracja programu powinna przebiegać w następujący sposób:

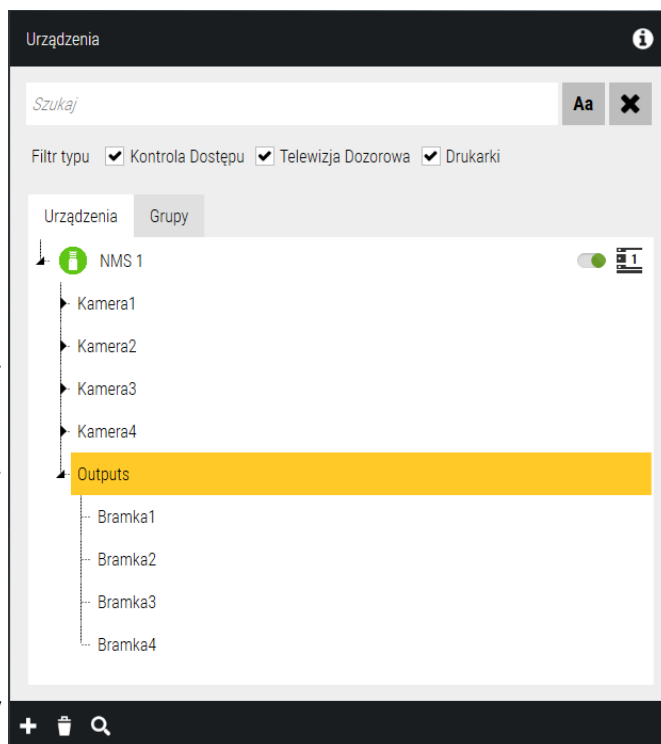
9.6.2 Dodawanie urządzeń

W celu zapewnienia kontroli nad pojazdami wjeżdżającymi jak i wyjeżdżającymi z określonych stref, należy przy wjeździe/wyjeździe ze strefy zamontować kamery wyposażone w funkcję 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**.

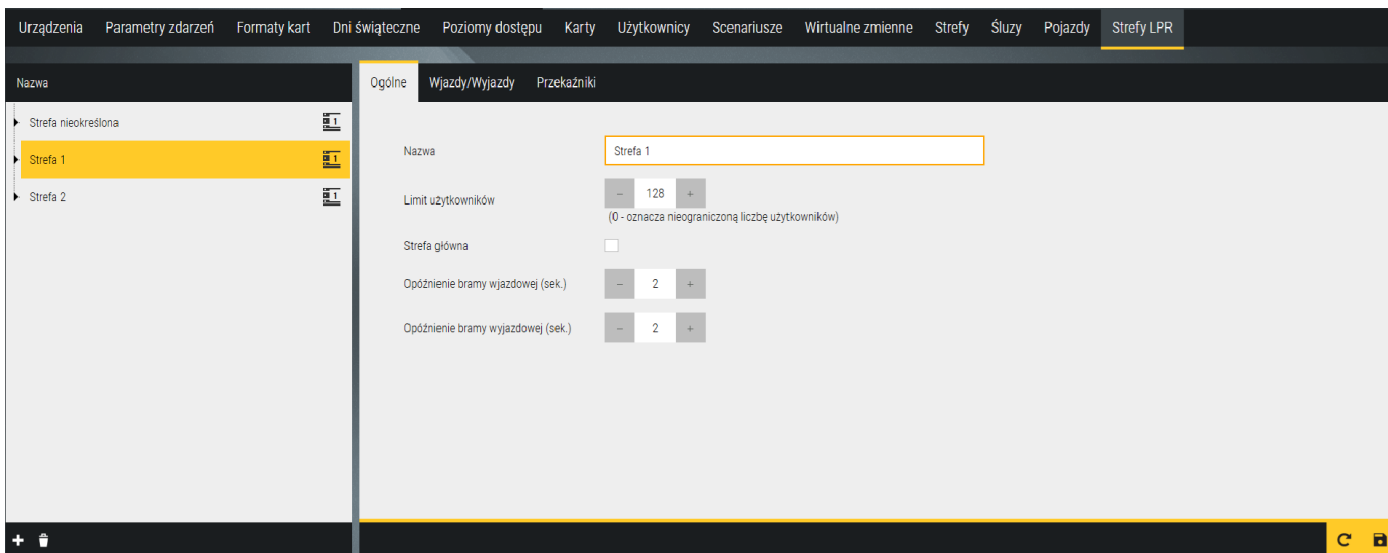
Ustawienie to należy zastosować indywidualnie dla każdej kamery.



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.



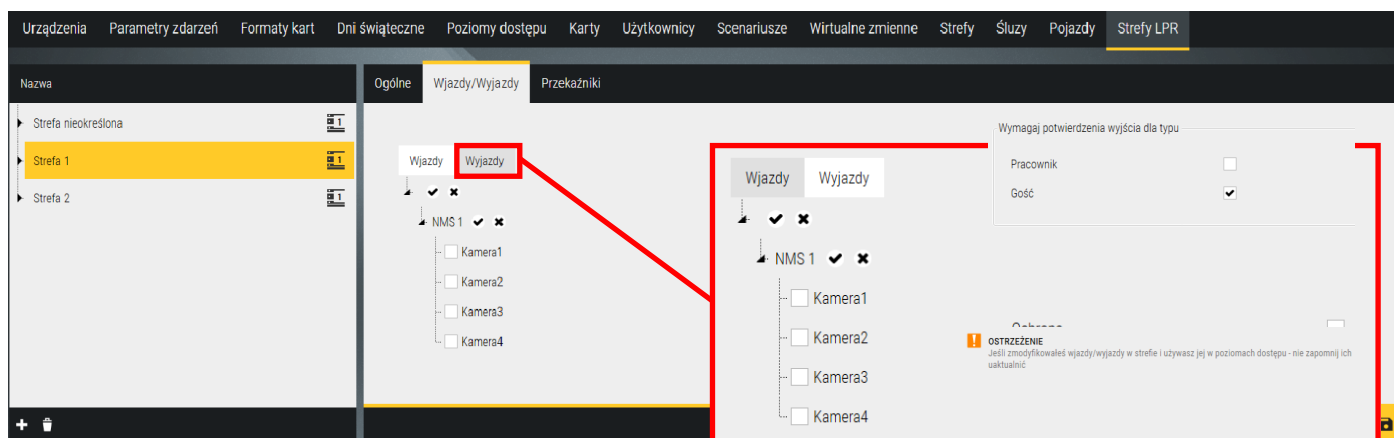
Po kliknięciu na wybraną strefę, w zakładce *Ogólne* znajdują się pola:

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 przełącznikowego sterującego bramą wjazdową/wyjazdową.

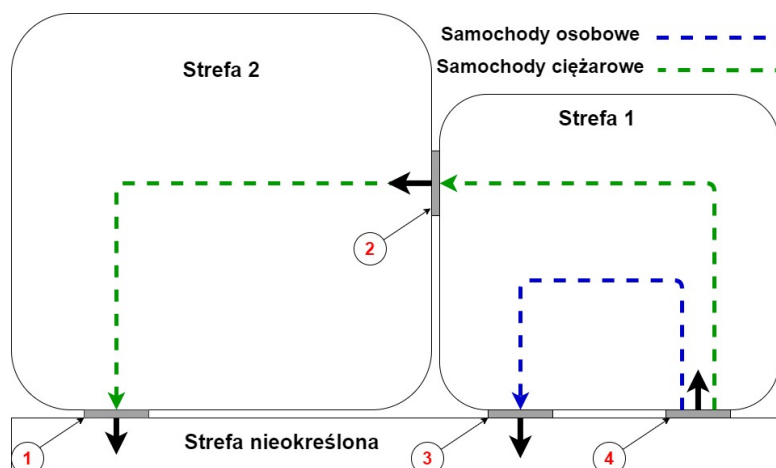


W zakładce *Wjazdy/Wyjazdy* można przyporządkować poszczególne kamery odpowiednio do wjazdów i wyjazdów z zaznaczonej żółtym kolorem strefy.

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)**.

Przełączniki

Etap konfiguracji Stref LPR można zakończyć przypisaniem przełączników do odpowiednich urządzeń. Nazwy urządzeń i przełączników, 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, przełączniki 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.

Wjazdy Wyjazdy Wjazdy Wyjazdy

Samochody osobowe Samochody ciężarowe

NMS 1 NMS 1

Kamera1 Kamera1

Kamera2 Kamera2

Kamera3 Kamera3

Kamera4 Kamera4

1

Nazwa

Strefa nieokreślona

Wejścia

Kamera3 Strefa 1

Kamera1 Strefa 2

Wyjścia

Kamera4 Strefa 1

Strefa 1

Wejścia

Kamera4 Strefa nieokreślona

Wyjścia

Kamera2 Strefa 2

Kamera3 Strefa nieokreślona

2

Urządzenie	Przełącznik
Kamera1	Bramka1
Kamera2	Bramka2
Kamera3	Bramka3
Kamera4	Bramka4
	Bramka1
	Bramka2
	Bramka3
	Bramka4

3

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:

Typ	KDH-KS3012-IP
Nazwa	KDH-KS3012-IP
Adres MAC	00-1B-9D-0A-F1-DD
IP	192.168.81.30
Port	50000
Czas przejścia do trybu autonomicznego	5 s
Liczba drzwi	2
Typ modułu	Brak
Wiegand format	Wiegand 34
Hasło komunikacyjne	[eye icon]
Kod do kasowania alarmu	[eye icon]

Nazwa	[00-1B-9D-0A-F1-DD] Czytnik 2
Tryb identyfikacji w czasie aktywnym	Kod QR lub karta
Tryb identyfikacji poza czasem aktywnym	Brak dostępu
Użyty kod dyskretnego alarmu	[eye icon]
Pierwsza karta otwierająca	Wyłączony
Wideoverifikacja	Brak
Funkcje zaawansowane	Wybierz funkcję
	Brak

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 *Przełączniki* 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.

Typ	Urządzenie	Przełącznik
Wjazd	Channel 2	NVIP-2H-6732M/LPR_GORA_wjazd /
Wyjazd	Channel 3	NVIP-2H-6732M/LPR_DOL_wjazd / O
Wyjazd	[00-1B-9D-0A-F1-DD] Czytnik 2	NVIP-2H-6732M/LPR_DOL_wjazd / O

W rezultacie, po przyłożeniu biletu QR do czytnika, w logach powinny pojawić się wpisy potwierdzające prawidłowy wyjazd ze strefy LPR z ważnym biletem.

DATA	SERWER	URZĄDZENIE	UŻYTKOWNIK	ZDARZENIE	OPERATOR	KOMENTARZE	INSTRUKCJA
14:29:53 02.07.2025		KDH-KS3012-IP / [00-1B-9D-0A-F1-DD] Drzwi 2 / [00-1B-9D-0A-F1-DD] Czytnik 2	Gość 81075	Wjazd - dostęp dozwolony, ważna rejestracja pojazdu [RJA48808] (Strefa LPR 1 -> UnknownZone)	SYSTEM		
14:29:53 02.07.2025		KDH-KS3012-IP / [00-1B-9D-0A-F1-DD] Drzwi 2 / [00-1B-9D-0A-F1-DD] Czytnik 2	Gość 81075 Numer karty : 18622476	Drzwi - dostęp dozwolony, ważna karta	SYSTEM		
14:29:47 02.07.2025		KDH-KS3012-IP / [00-1B-9D-0A-F1-DD] Drzwi 2 / [00-1B-9D-0A-F1-DD] Czytnik 2	Gość 81064	Wjazd - dostęp dozwolony, ważna rejestracja pojazdu [WGM98NK] (Strefa LPR 1 -> UnknownZone)	SYSTEM		
14:29:47 02.07.2025		KDH-KS3012-IP / [00-1B-9D-0A-F1-DD] Drzwi 2 / [00-1B-9D-0A-F1-DD] Czytnik 2	Gość 81064 Numer karty : 31722880	Drzwi - dostęp dozwolony, ważna karta	SYSTEM		

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.

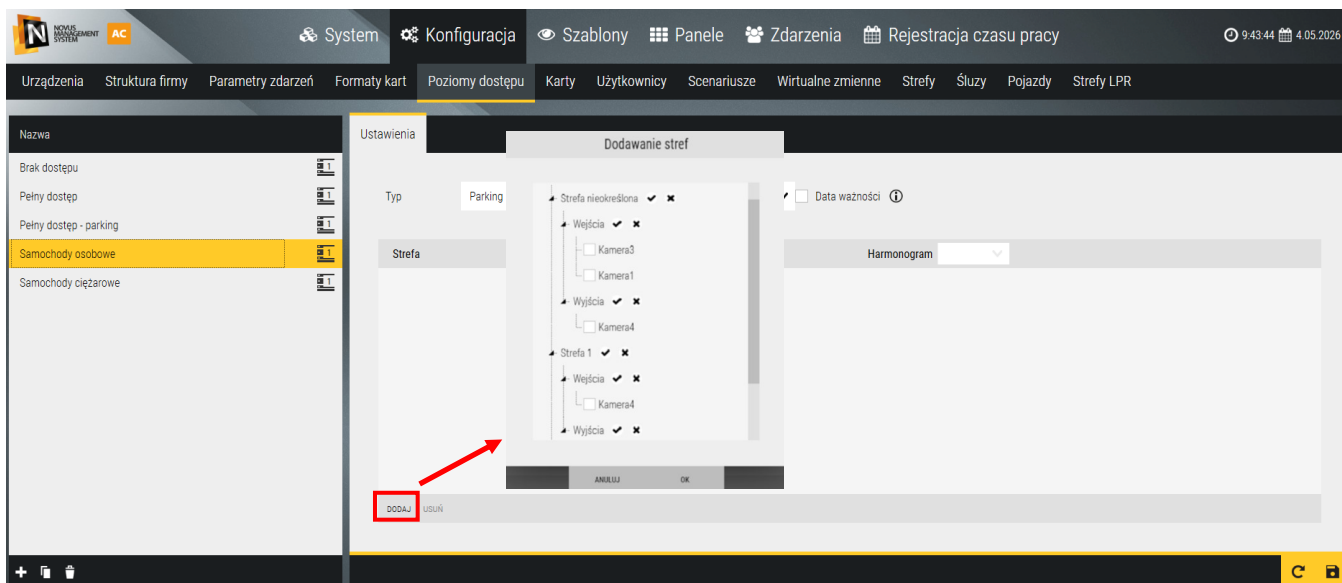
Wjazd gościa do strefy LPR przed rozpoczęciem okresu awizacji, status **W przygotowaniu**.

Wjazd podczas okresu awizacji do strefy LPR, status **Ważny**.

Po upływie terminu ważności awizacji -> zmiana statusu na **Nieważny**, przy kolejnym wjeździe do strefy konieczne będzie ponowne wygenerowanie biletu.

9.6.4 Poziomy dostęp - parking

Menu poziomy dostęp zostało opisane w rozdziale **4.2 Poziomy dostęp**, 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.

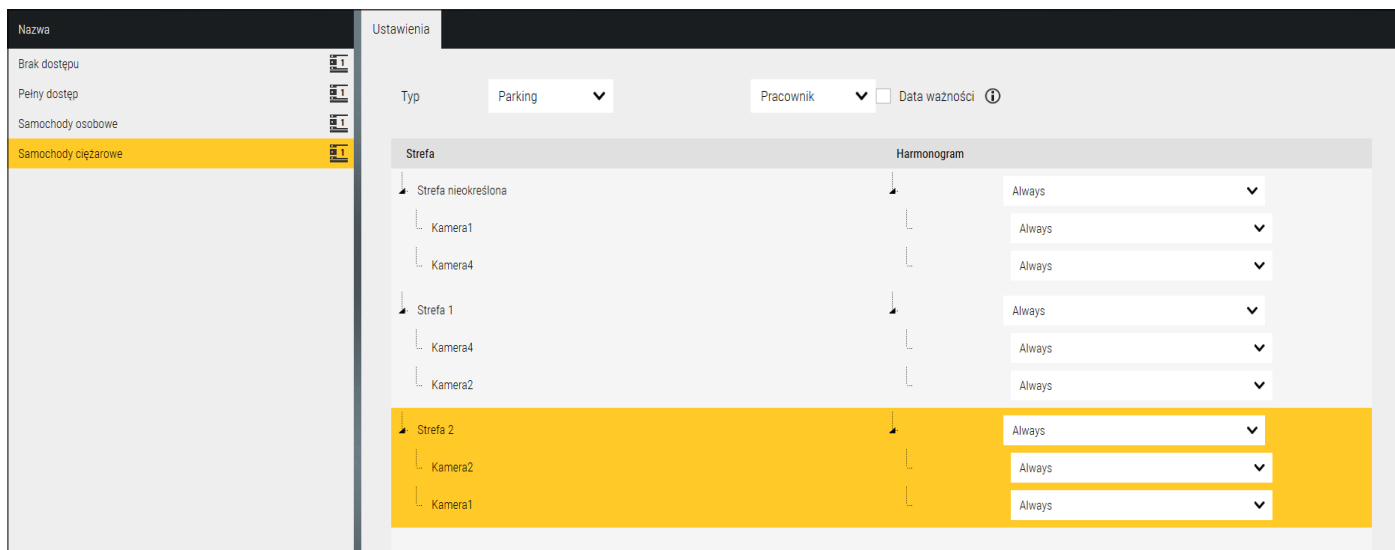


W przykładowym projekcie należy stworzyć dwa poziomy dostęp:

Samochody osobowe - które będą miały dostęp do **Strefy 1** i będą miały możliwość przejazdu przez bramki **3 i 4**.

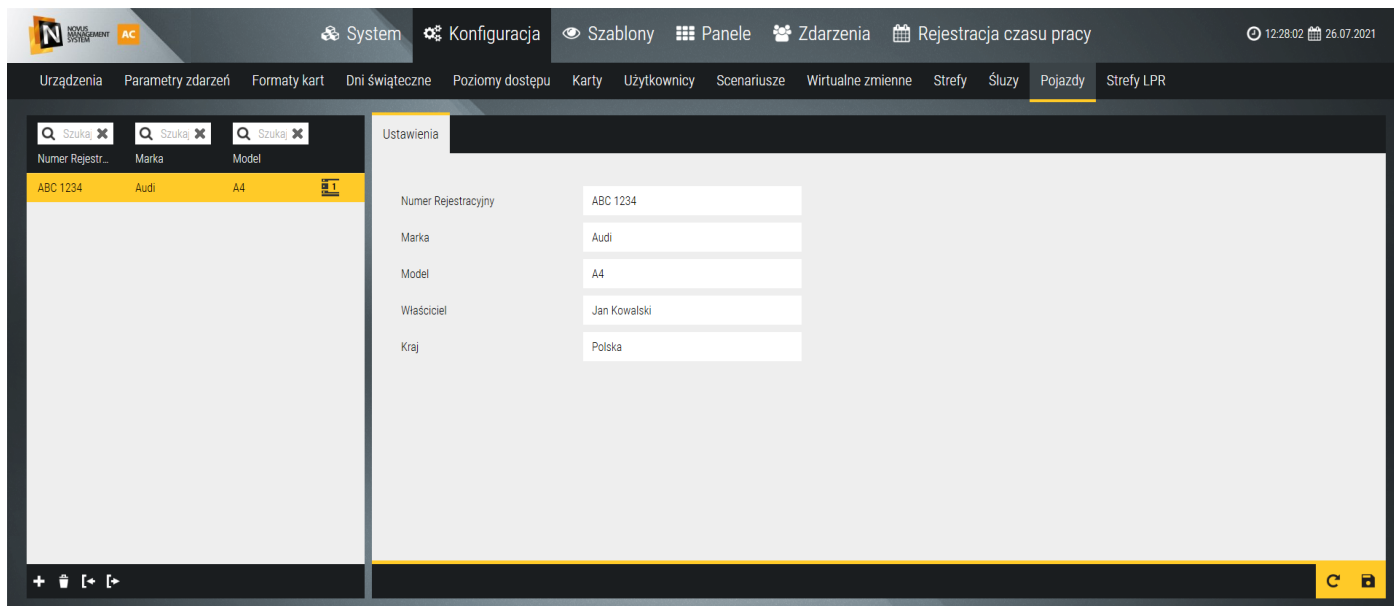
Samochody ciężarowe - które będą miały dostęp do **Strefy 1** i **Strefy 2** i będą miały możliwość przejazdu przez bramki **1,2,4**.

Aby to zrobić należy kliknąć ikonę **+** i dodać dwa powyższe poziomy dostęp. 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

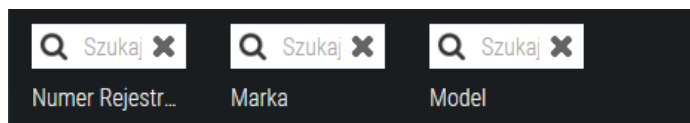
Zakładka *Pojazdy* służy do tworzenia bazy pojazdów. Przechowywane są tam informacje takie jak: numer rejestracyjny, marka, model, właściciel i kraj. Program umożliwia również zdefiniowanie czasu po którym pojazd będzie usunięty z bazy. Aby dodać pojazd do bazy należy kliknąć ikonę , następnie w celu 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, umożliwiającą 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 innymi: informacje na temat przemieszczania się pojazdów między strefami; informacje na temat udzielenia, bądź nie udzielenia pojazdowi 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**.

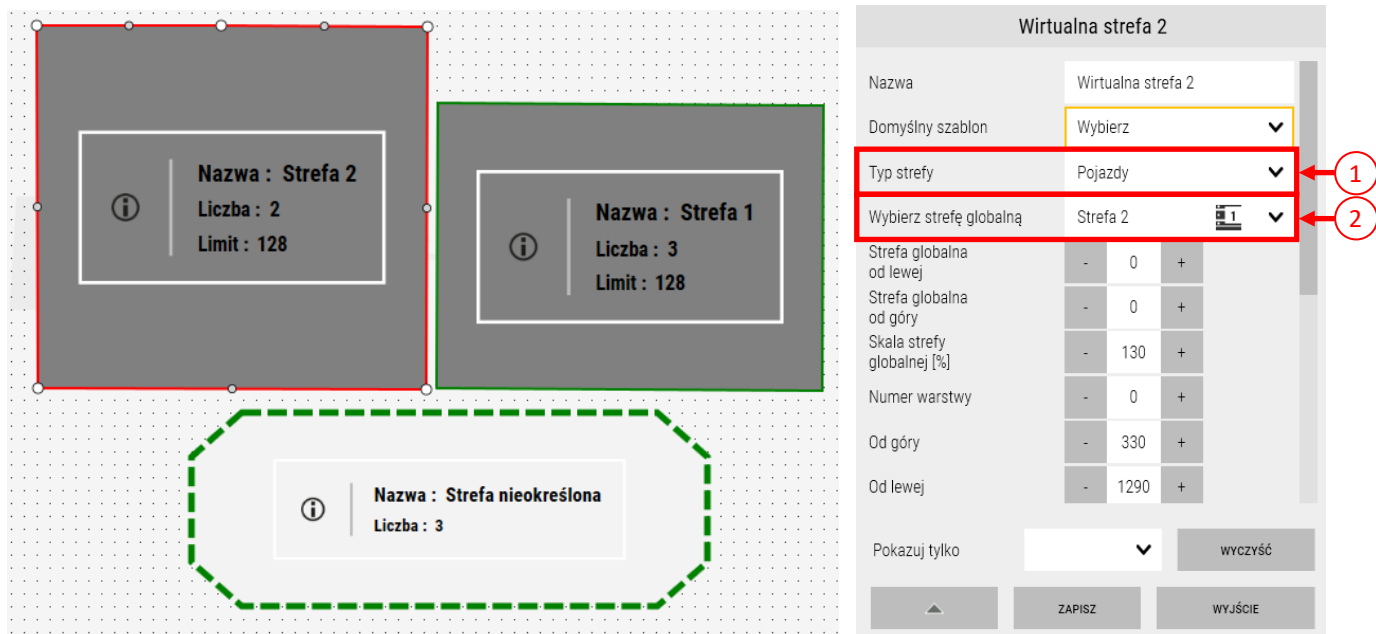
Przykładowy bilet dla pojazdu z rejestracją „ABC 1234” jest pokazany na rysunku obok. Bilet poza informacjami uzupełnionymi przy jego generowaniu posiada unikalny kod QR (możliwość wykorzystania funkcjonalności kodu QR będzie dostępna w przyszłości).



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)**.

Zarządzaj pojazdami

Wyszukaj we wszystkich strefach

Q Użytkownik ✕

Q Numer ✕

Q Strefa ✕

Strefa nieokreślona

Strefa 1

Strefa 2

1

Q Użytkownik ✕

Agnieszka K.

ABC 1234

Aleksandra R.

DEF 1234

Monika S.

GHJ 1234

2

Q Strefa docelowa ✕

Strefa nieokreślona

Strefa 1

Strefa 2

3

Ilość : 3

➔ EKSPORTUJ

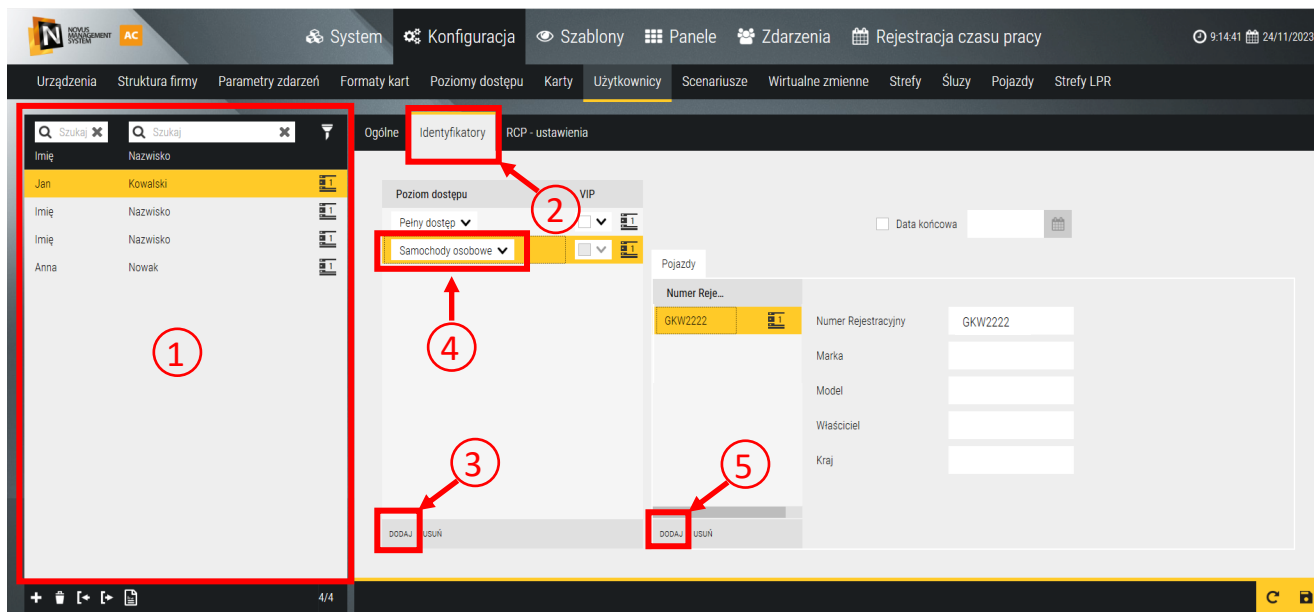
➔ PRZENIEŚ DO STREFY

4

WYJŚCIE

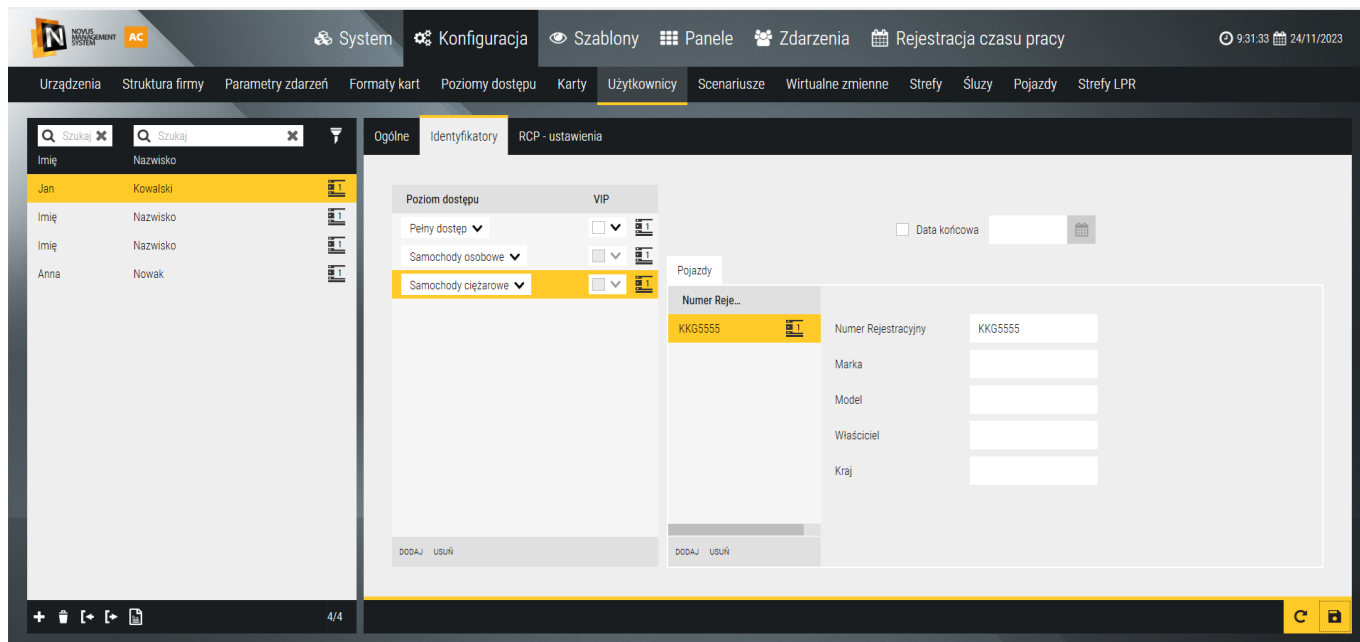
9.6.7 Użytkownicy - Identyfikatory

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.

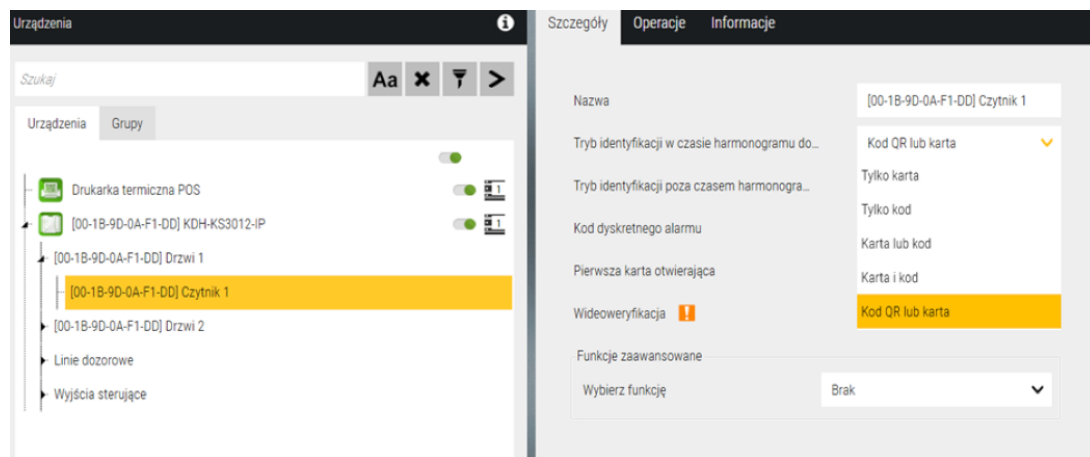


9.6.8 Przypisanie wygenerowanego kodu QR do użytkownika typu Gość

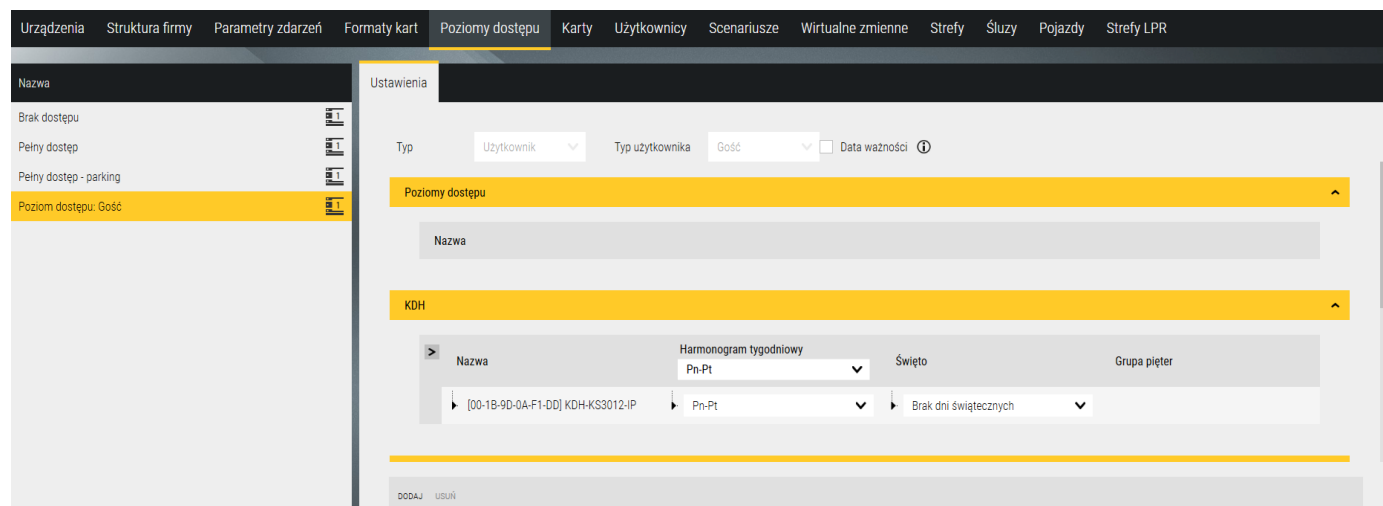
Kolejną funkcją oprogramowania NOVUS MANAGEMENT SYSTEM AC jest możliwość przypisania wygenerowanego kodu QR do użytkownika typu **Gość** oraz wysłania go poprzez e-mail. Funkcja ta pozwala utworzyć jednorazowy lub czasowy kod QR, który umożliwia użytkownikowi wejście i wyjście bez konieczności używania 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.

jakubkucharski17ent@gmail.com
Dro: Jakub Kucharski

Twój kod QR:



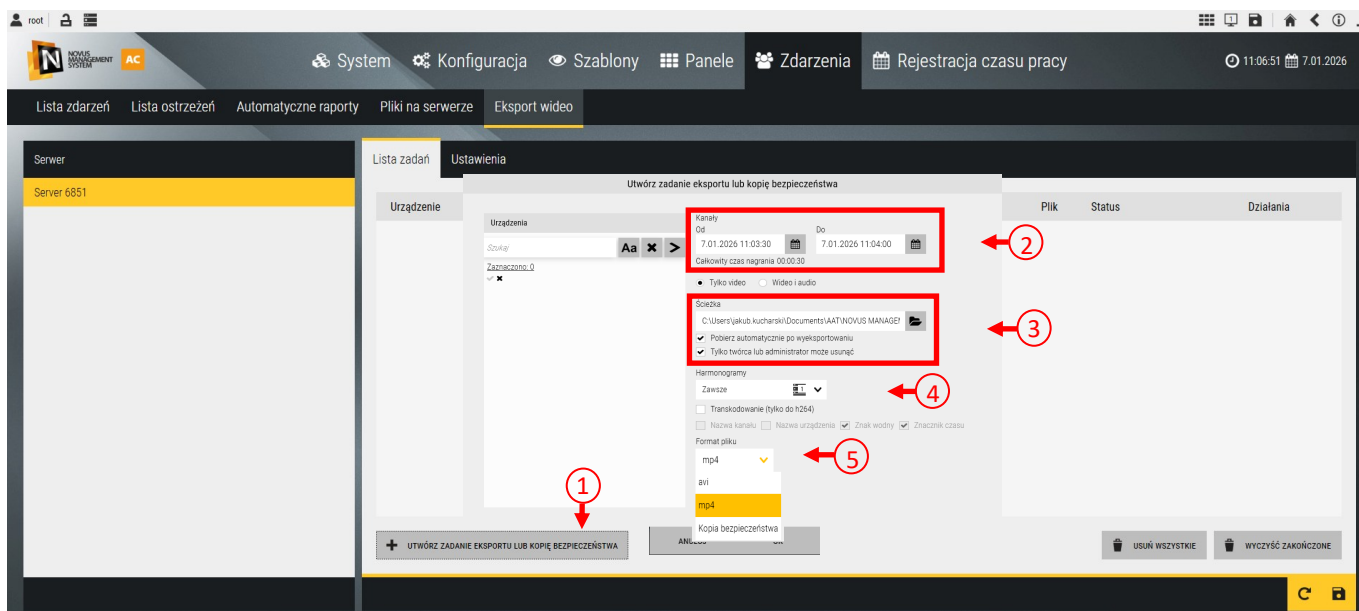
W rezultacie prawidłowej konfiguracji, a następnie po zeskanowaniu kodu QR przez czytnik, w logach kontrolera powinny pojawić się wpisy potwierdzające poprawne odczytanie i przetworzenie kodu QR, podobne do tych przedstawionych poniżej.

4	12:53:54 05.03.2026	[00-1B-9D-0A-F1-DD] KDH-KS3012-IP / [00-1B-9D-0A-F1-DD] Drzwi 2	Drzwi - koniec czasu na dostęp	SYSTEM				
4	12:53:51 05.03.2026	[00-1B-9D-0A-F1-DD] KDH-KS3012-IP / [00-1B-9D-0A-F1-DD] Drzwi 2 / [00-1B-9D-0A-F1-DD] Czytnik 2	Imię Nazwisko Numer karty : 36000007	Drzwi - dostęp dozwolony, ważna karta	SYSTEM			
4	12:53:51 05.03.2026	[00-1B-9D-0A-F1-DD] KDH-KS3012-IP / [00-1B-9D-0A-F1-DD] Drzwi 2	Imię Nazwisko Numer karty : 36000007	Strefa - prawidłowe przejście (z Strefa 1 do Strefa 2)	SYSTEM			
4	12:52:09 05.03.2026	[00-1B-9D-0A-F1-DD] KDH-KS3012-IP / [00-1B-9D-0A-F1-DD] Drzwi 1 / [00-1B-9D-0A-F1-DD] Czytnik 1	Imię Nazwisko Numer karty : 36000007	Drzwi - dostęp dozwolony, ważna karta	SYSTEM			
5	12:52:00 05.03.2026	[00-1B-9D-0A-F1-DD] KDH-KS3012-IP	Koniec awarii: Kontroler - powrót komunikacji	SYSTEM				

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 **dyskiety**  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.



Lista zadań

Ustawienia

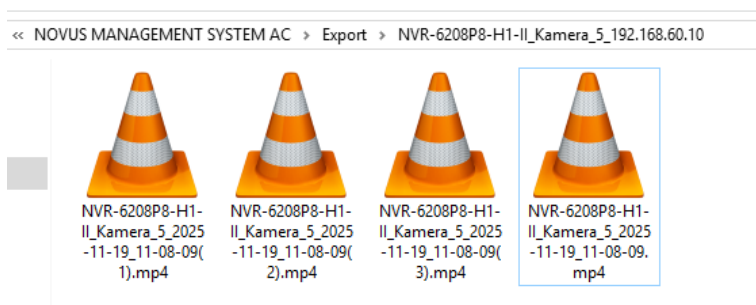
Operator, który stworzył zadania eksportu

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.

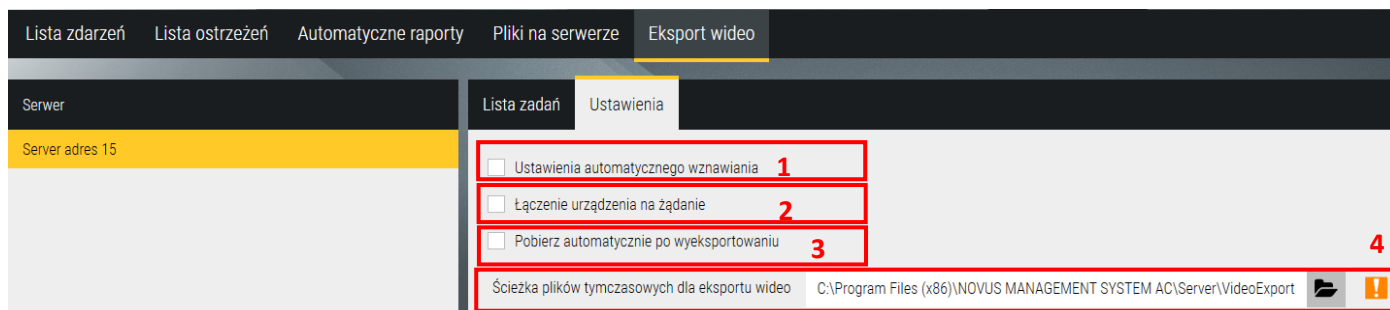
NVR-6208P8-H1-II	Kamera 5	Operator	Tak	Zawsze	19/11/2025 11:08:09	19/11/2025 11:09:40	mp4	Zakończono	  	
									Gotowy do pobrania	

Poniżej przedstawiono folder ze ścieżką przypisaną do plików nagrań, w którym znajdują się trzy kopie pliku, pobranego kilkakrotnie.



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.

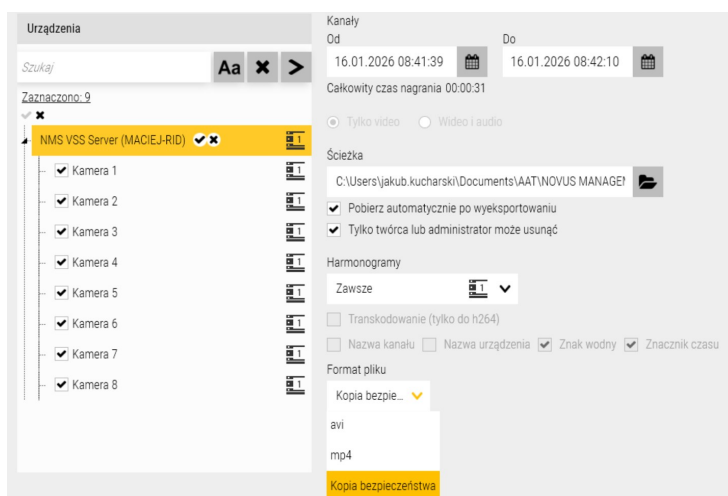
Dzięki tym opcjom możliwe jest zmniejszenie obciążenia sieci i serwera, przy jednoczesnym zachowaniu pełnej funkcjonalności systemu.

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.

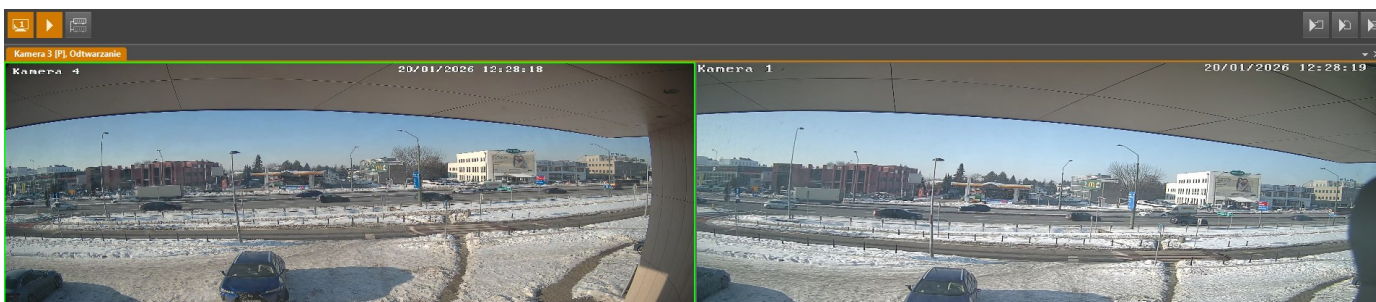
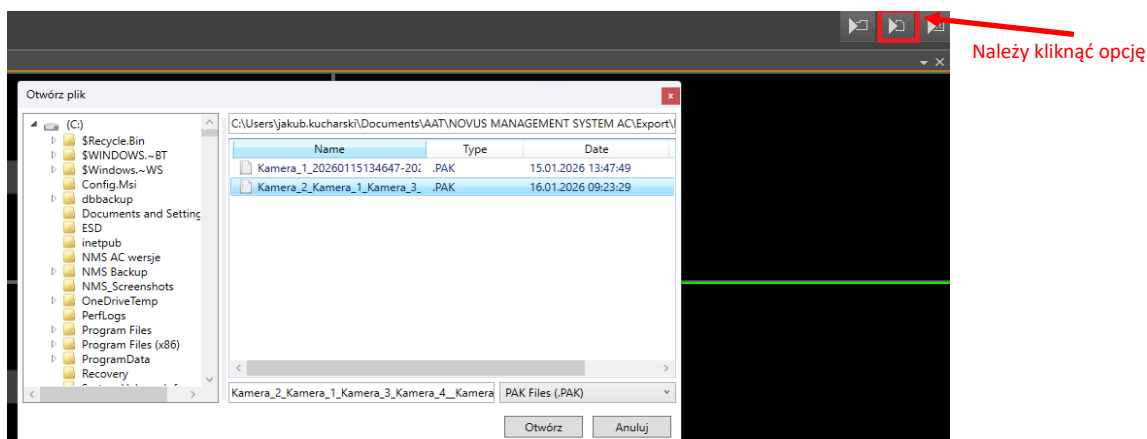
Format .pak jest specjalnym formatem tworzenia kopii bezpieczeństwa materiału wideo bez wprowadzania jakichkolwiek modyfikacji w stosunku do materiału źródłowego. Dodatkowo format .pak pozwala na łączenie nagrań z kilku kanałów w jeden plik, w przeciwieństwie do formatów .avi i .mp4.

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.

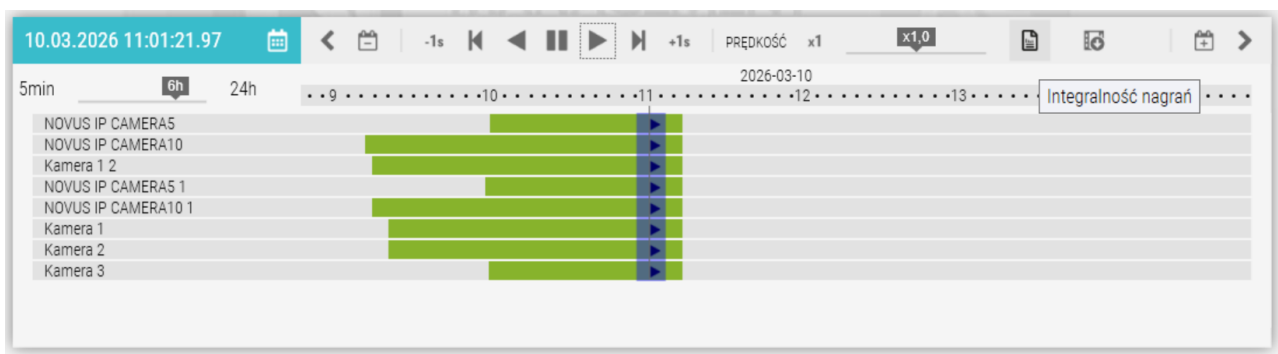


UWAGA! Aby wykonać kopię bezpieczeństwa, należy dodać serwer NMS VSS i nawiązać z nim połączenie.

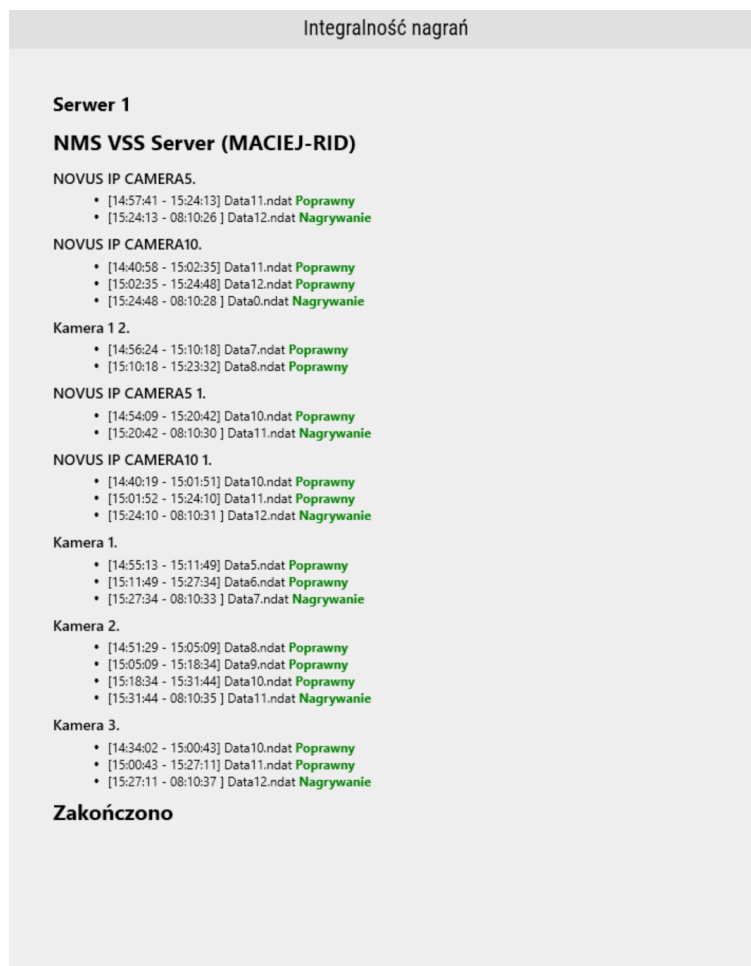
Po udanym wykonaniu kopii w celu jej odtworzenia należy odtworzyć nowo powstały plik w programie NMS VSS Player, wybierając opcję *Plik*. Następnie zostanie wyświetlone okno z nagraniami.



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*.

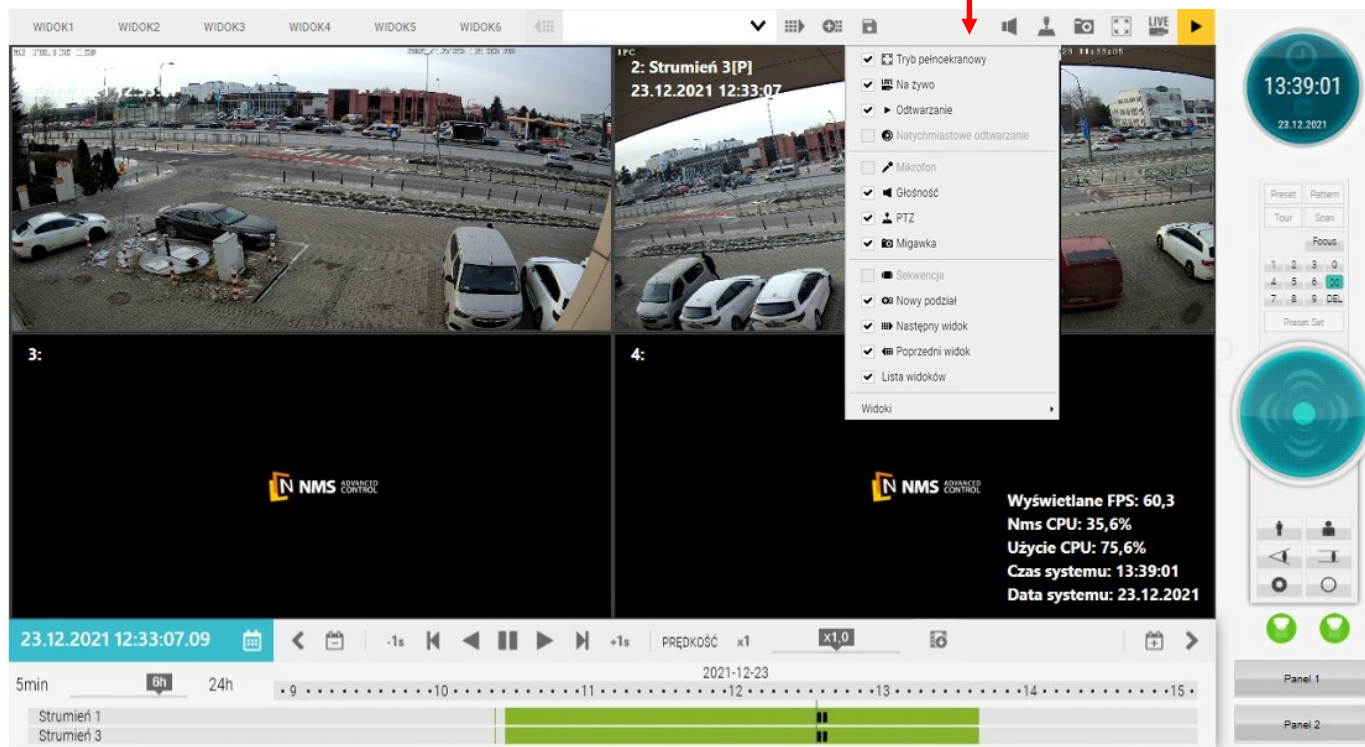


W zakładce *Rejestrator*, dla każdego kanału, należy włączyć nagrywanie obu strumieni, zaznaczając opcję *Utwórz przestrzeń do nagrywania dla strumieni pomocniczych*.

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.

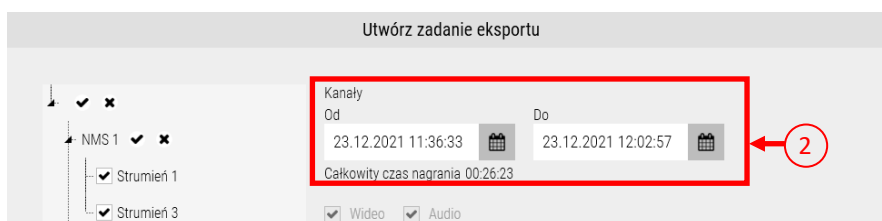
Kliknij na pasku żeby wyświetlić menu



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.

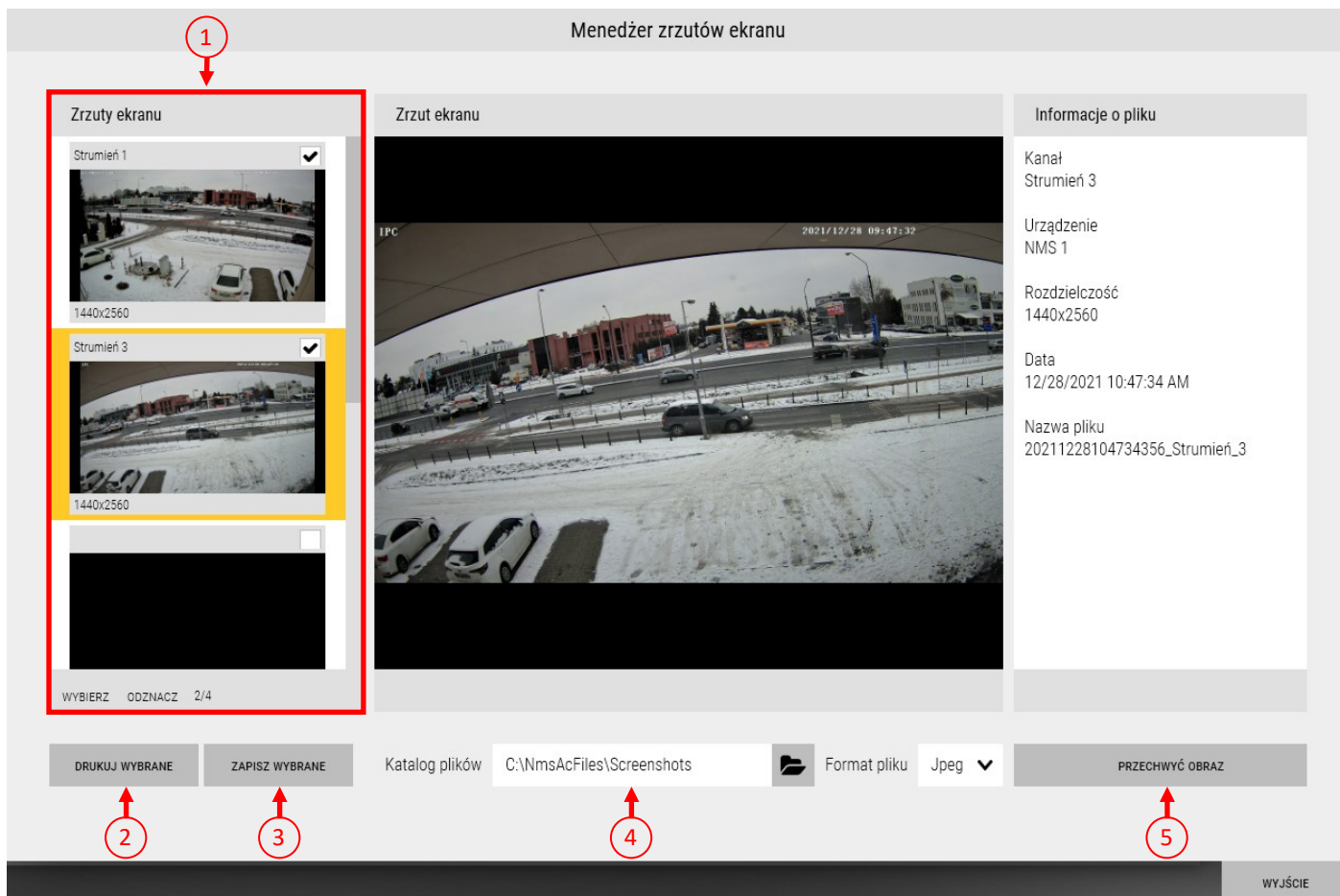


Aby wyeksportować i pobrać nagranie należy postępować analogicznie jak jest to opisane w rozdziale **Eksport nagrań z poziomu menu głównego** z poprzedniej strony.

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, partycję, strefę lub wejście.

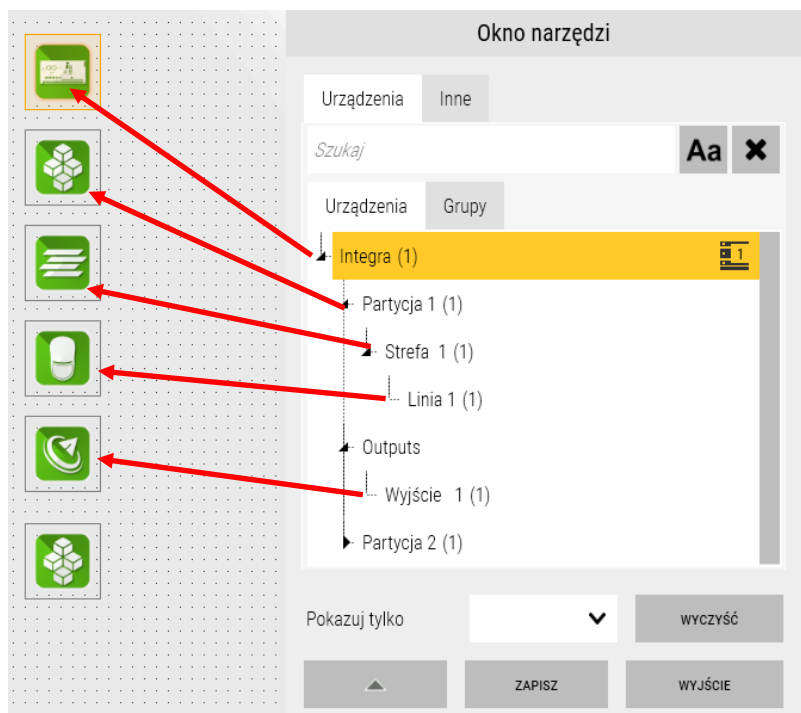
Po wyjściu z trybu edycji kliknięcie myszką na ikonę **urządzenia** pozwala wyświetlić jego listę zdarzeń.

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 generowanie 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).

Lista bieżących ostrzeżeń											
1	2	3	4	5	Q Serwer	Q Urządzenie	Q Opis	1	1	1	1 / 1
PRIORYTET	DATA POZATKOWA	DATA KOŃCOWA	SERWER	URZĄDZENIE	OPIS	OPERATOR OBSŁUGUJĄCY	STAN	AKCJE	HISTORIA	KOMENTARZE	INSTRUKCJA...
5	08:42:25 27.01.2025			[00-1B-9D-0A-F1-DD] KDH-KS3012-IP / [00-1B-9D-0A-F1-DD] Drzwi 1	Awarja: Drzwi - sforsowane		Aktywne				
Pamięć niepotwierdzonych ostrzeżeń											
1	2	3	4	5	Q Serwer	Q Urządzenie	Q Opis	9	0	0	9 / 9
PRIORYTET	DATA POZATKOWA	DATA KOŃCOWA	SERWER	URZĄDZENIE	OPIS	OPERATOR OBSŁUGUJĄCY	STAN	AKCJE	HISTORIA	KOMENTARZE	INSTRUKCJA...
5	10:20:54 27.01.2025	10:40:09 27.01.2025		[00-1B-9D-0A-F1-DD] KDH-KS3012-IP	Awarja: Kontroler - utrata komunikacji		Zakończone				
5	15:55:36 24.01.2025	08:07:52 27.01.2025		[00-1B-9D-0A-F1-DD] KDH-KS3012-IP	Awarja: Kontroler - utrata komunikacji		Zakończone				
5	15:03:53 24.01.2025	15:04:04 24.01.2025		[00-1B-9D-0A-F1-DD] KDH-KS3012-IP / [00-1B-9D-0A-F1-DD] Drzwi 1	Awarja: Drzwi - sforsowane		Zakończone				
5	11:32:44 24.01.2025	11:32:45 24.01.2025		[00-1B-9D-0A-F1-DD] KDH-KS3012-IP / [00-1B-9D-0A-F1-DD] Drzwi 1	Awarja: Drzwi - sforsowane		Zakończone				
5	09:41:06 24.01.2025	09:48:35 24.01.2025		[00-1B-9D-0A-F1-DD] KDH-KS3012-IP	Awarja: Kontroler - utrata komunikacji		Zakończone				
1	13:34:05 23.01.2025	13:34:05 23.01.2025		NVR-6432-H2/F	Alarm: Rejestrator - konfiguracja dla modelu została ustawiona NVR-6...		Zakończone				
5	10:25:02 23.01.2025	10:25:02 23.01.2025		Urządzenie usunięte	Alarm: Rejestrator - konfiguracja dla modelu została ustawiona NVR-6...		Zakończone				
5	10:23:43 23.01.2025	10:23:43 23.01.2025		Urządzenie usunięte	Alarm: Rejestrator - konfiguracja dla modelu została ustawiona NVR-6...		Zakończone				

W kolumnie **AKCJE** dostępne są opcje pozwalające zmienić stan ostrzeżenia na potwierdzony lub je zakończyć (dotyczy ostrzeżenia bieżącego), a także przejść obsługę nad danym ostrzeżeniem.

Zmień stan

☐ Potwierdź
 ☐ Zakończ

ANULUJ OK

Ostrzeżenie

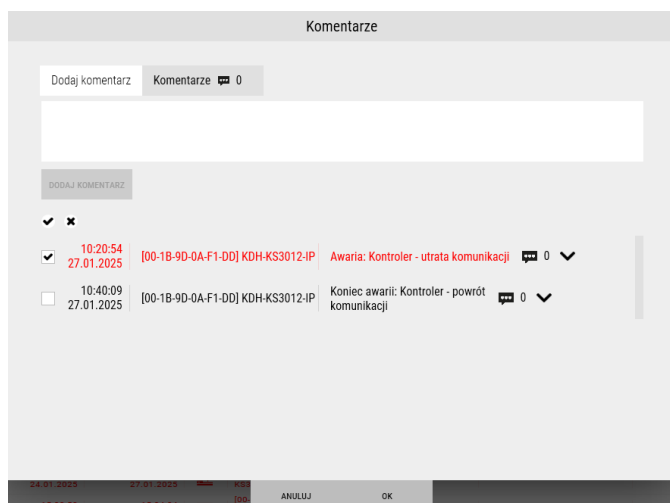
 29/01/2025 14:55:21
Czy chcesz zająć się tym ostrzeżeniem?

TAK NIE

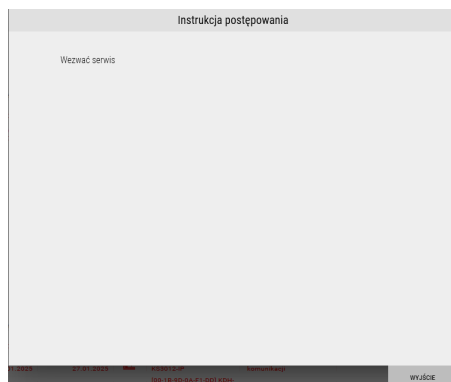
Kolumna **HISTORIA** pozwala zobaczyć historię zdarzeń związaną z ostrzeżeniem.

Historia		
29.01.2025	14:56:44	Rezygnacja z obsługi przez root
29.01.2025	14:55:46	Przejęcie obsługi przez root
27.01.2025	10:40:09	Zakończenie przez SYSTEM
27.01.2025	10:20:54	Początek
		WYJŚCIE

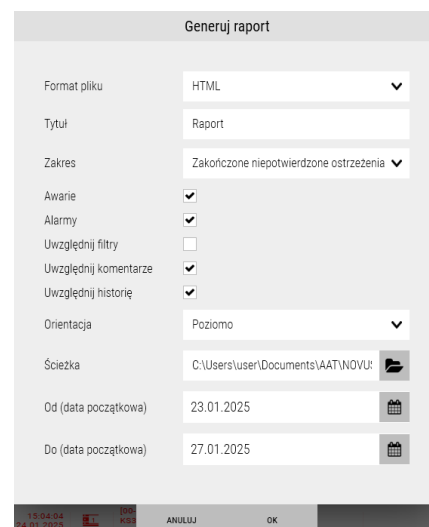
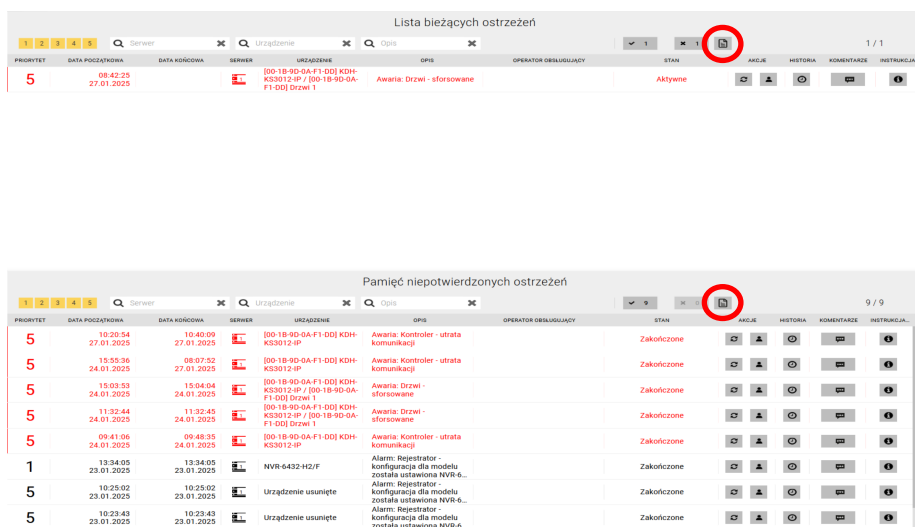
Kolumna **KOMENTARZE** pozwala dodać lub odczytać komentarz do ostrzeżenia oraz końca ostrzeżenia.



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.



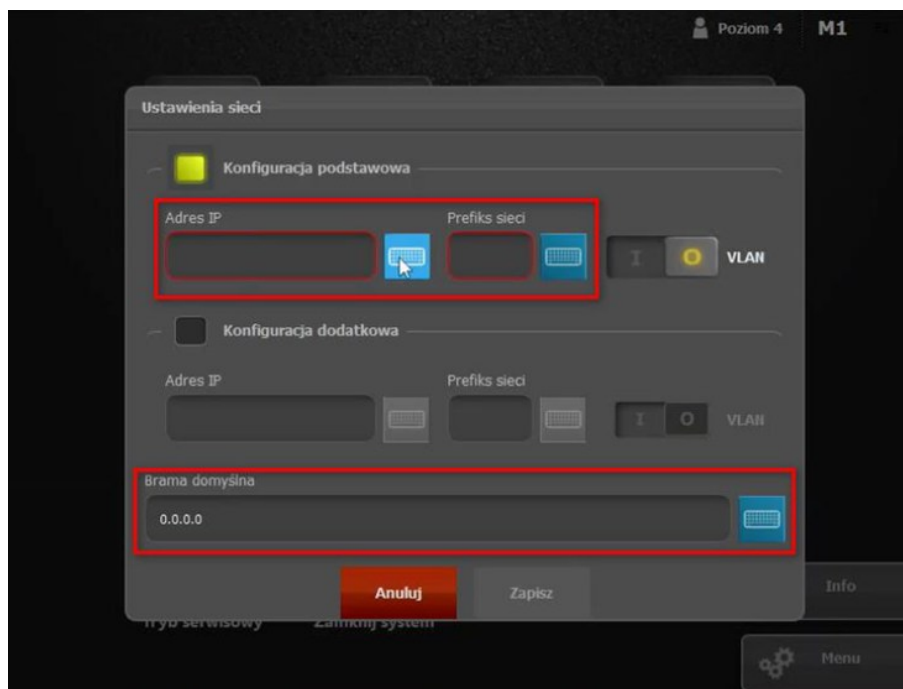
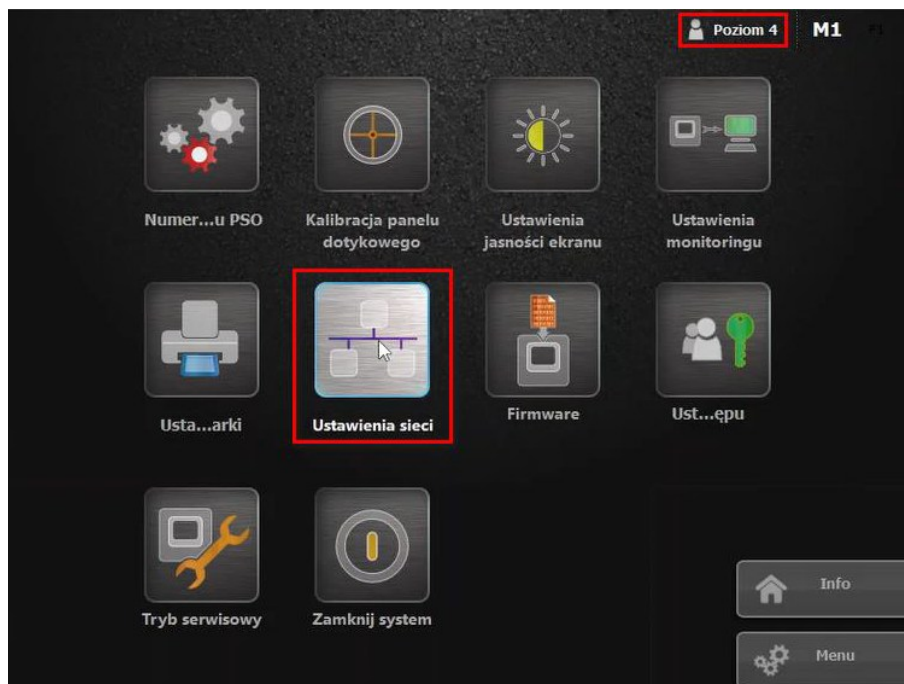
9.11 - Integracja (wizualizacja) z systemami sygnalizacji pożaru Polon 6000

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:

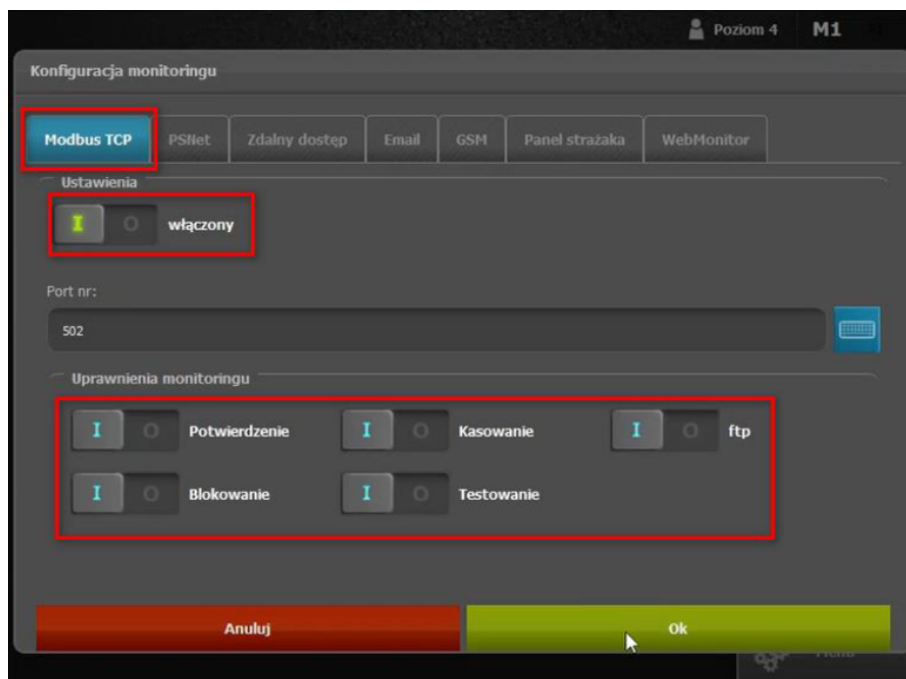
Menu -> Konfiguracja PSO -> Ustawienia sieć



- Przejść do

Menu -> Konfiguracja PSO -> Ustawienia monitoringu

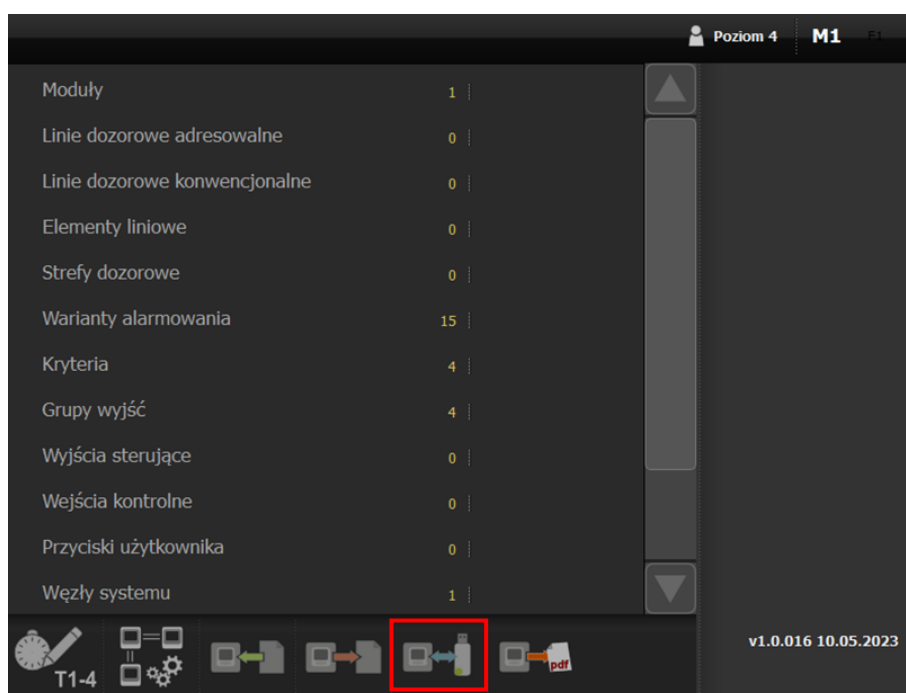
MODBUS TCP -> włączony



UWAGA! Po włączeniu funkcji Modbus należy wykonać restart modułu PSO

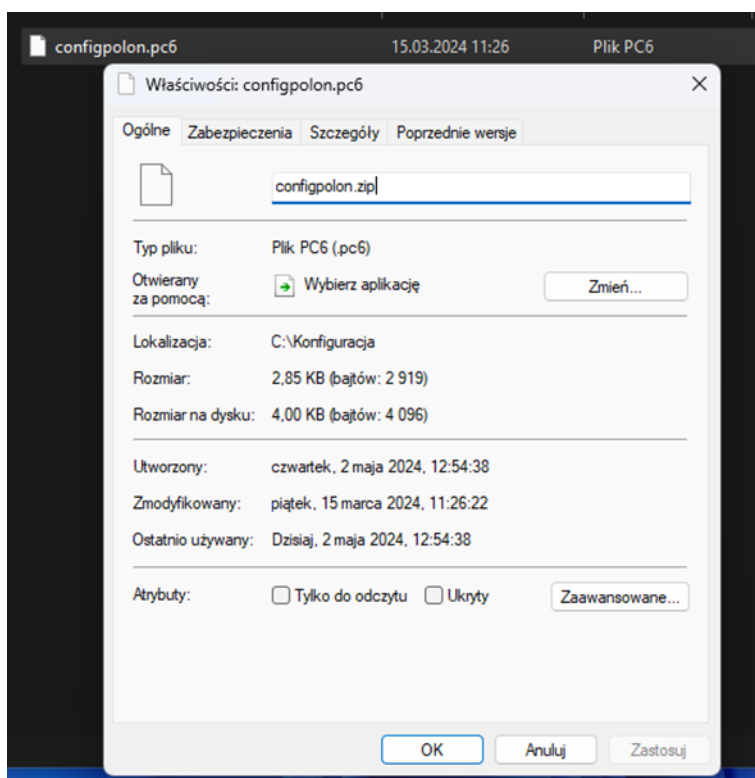
Eksport konfiguracji z centrali Polon 6000 oraz jej import do oprogramowania NOVUS MANAGEMENT SYSTEM AC

- Po zalogowaniu się do centrali przechodzimy do konfiguracji systemu (kopiowanie konfiguracji)



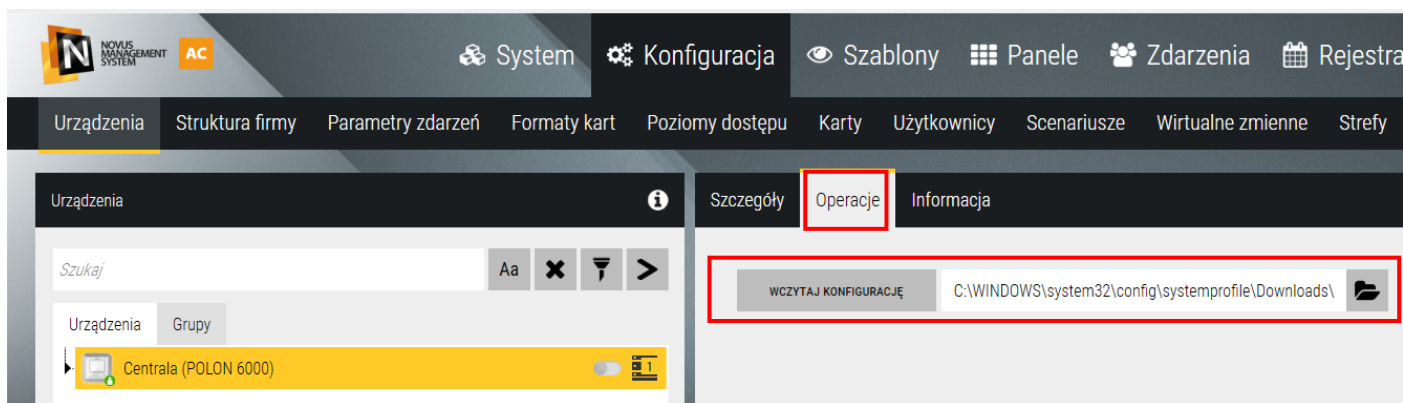
- Eksportujemy konfigurację na Pendrive.

- 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

Nazwa	Typ
config.xml	Plik XML
config_modbus.xml	Plik XML
filters.xml	Plik XML



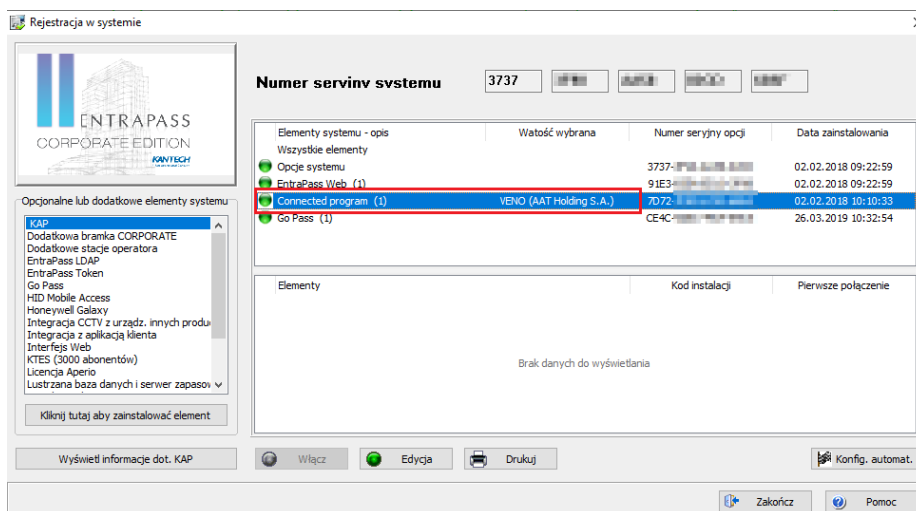
Uwaga! Import konfiguracji powoduje zastąpienie (nadpisanie) całej konfiguracji znajdującej się aktualnie na serwerze. Nie ma możliwości wczytania konfiguracji jedynie w celu dodania nowych elementów, czy wprowadzonych modyfikacji. Jeśli zachodzi potrzeba modyfikacji konfiguracji już dodanego systemu Polon 6000, należy przeprowadzić ją ręcznie poprzez dodawanie, usuwanie, modyfikację urządzeń na liście.

9.12 Integracja (wizualizacja) z systemem kontroli dostępu KANTECH

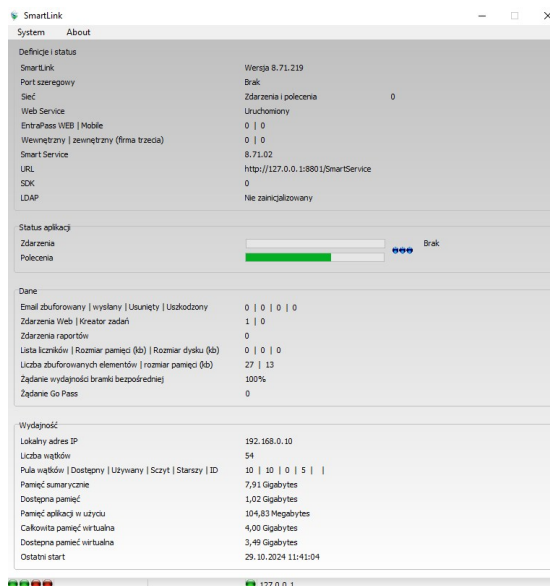
Konfiguracja oprogramowania EntraPass pod kątem współpracy z oprogramowaniem NOVUS MANAGEMENT SYSTEM AC

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

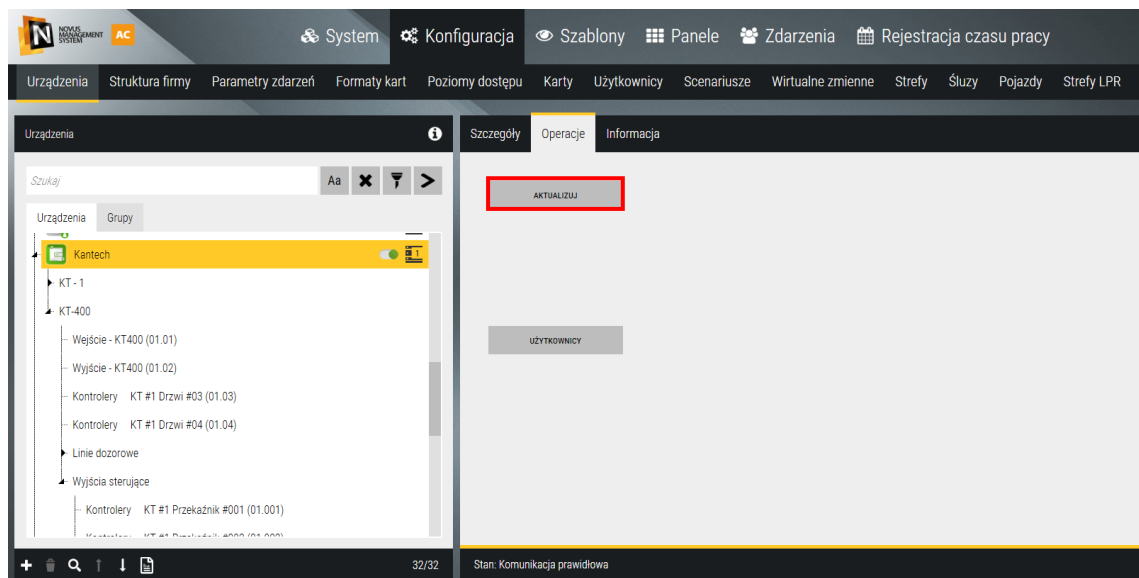
Port - Port aplikacji SmartLink konfigurowany w zakładce *Smartlink Web i API* w oprogramowaniu EntraPass
- Port Web Service

Użytkownik - nazwa użytkownika/operatora dla systemu Entrapass

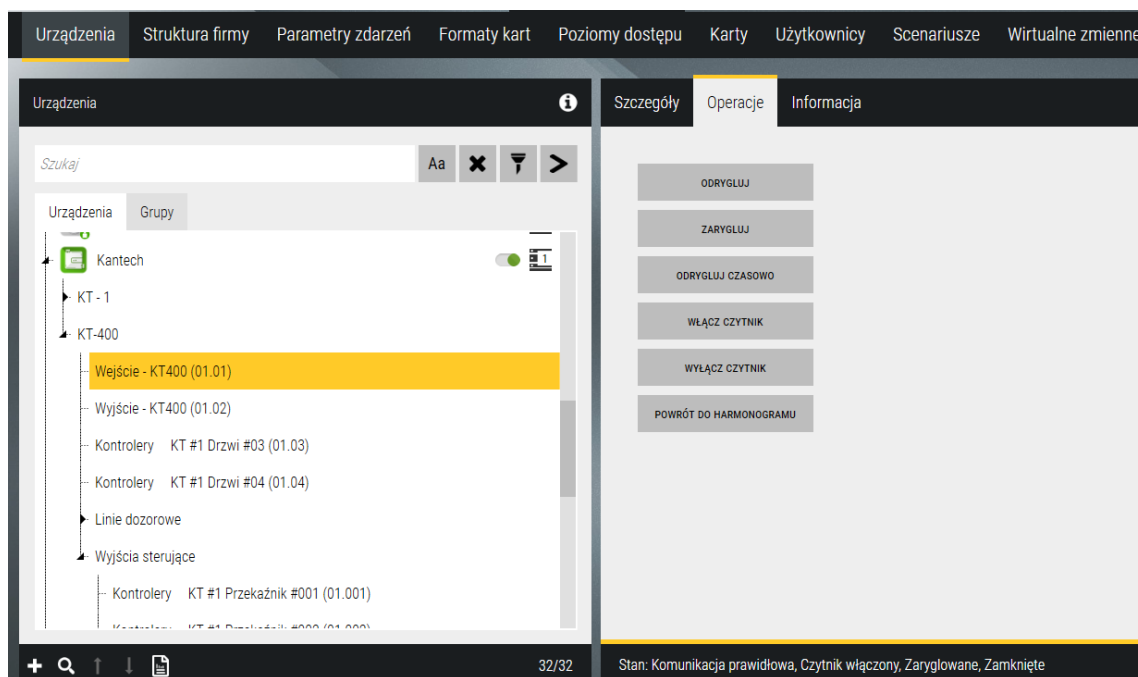
Hasło - hasło użytkownika/operatora dla systemu Entrapass

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**.



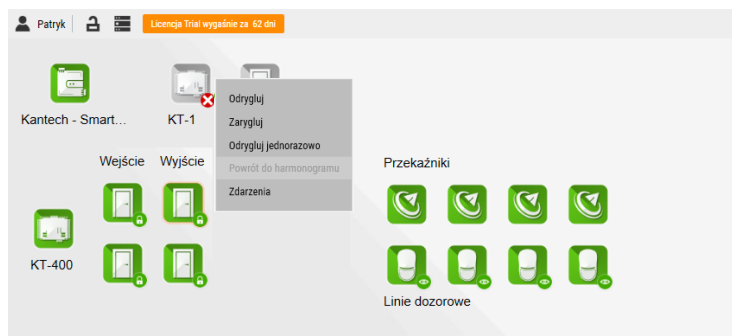
W zakładce **Operacje** możemy wykonywać polecenia dotyczące dodanych urządzeń, wejść i wyjść:

Drzwi - odrygluj/zarygluj/odrygluj czasowo/włącz czytnik/wyłącz czytnik/powrót do harmonogramu

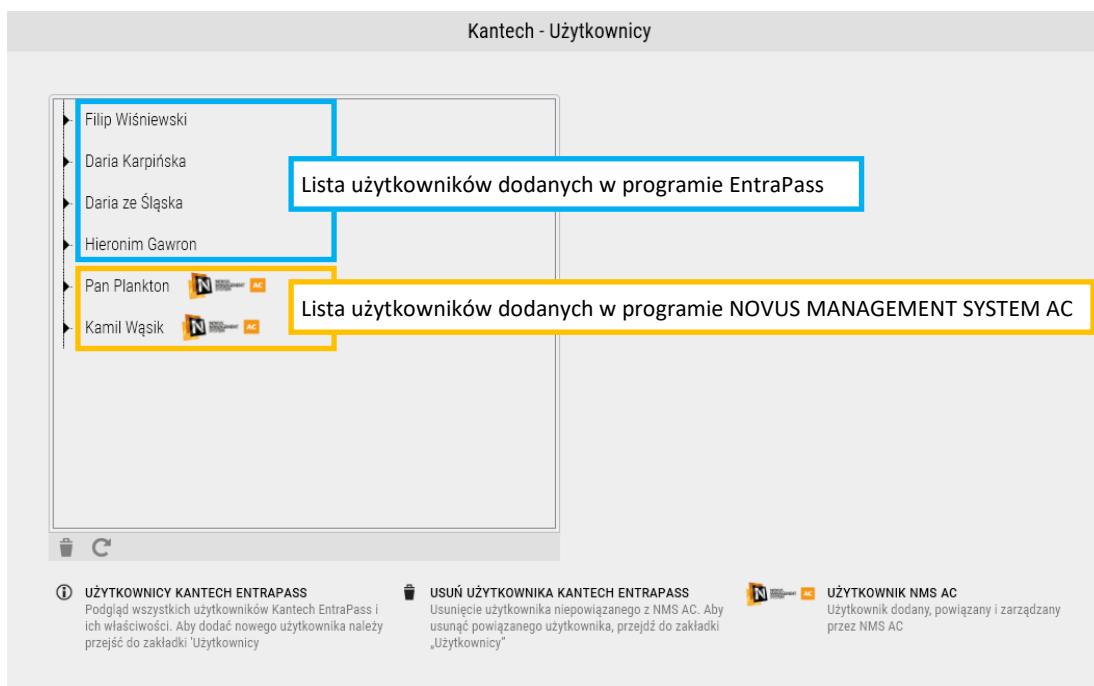
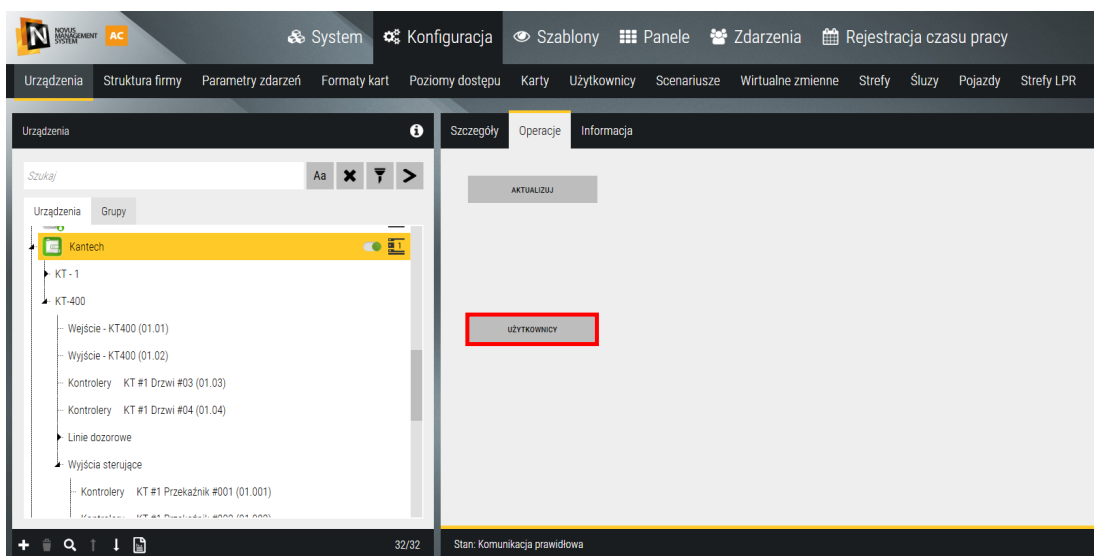
Wyjścia sterujące - włącz/wyłącz/włącz czasowo/powrót do harmonogramu

Linie dozorowe - włącz monitorowanie/wyłącz monitorowanie/powrót do harmonogramu

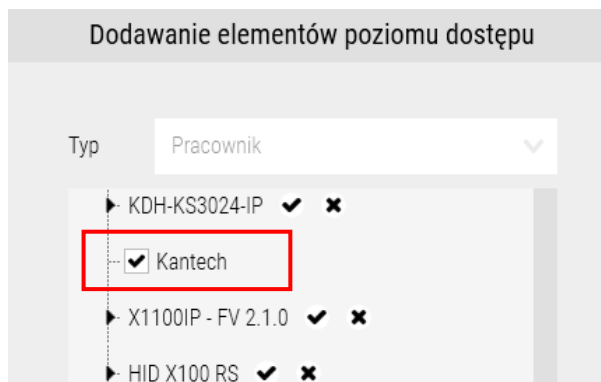
Wszystkie z wyświetlanych w urządzeniach elementów możemy umieszczać na panelach i sterować nimi z pozycji operatora.



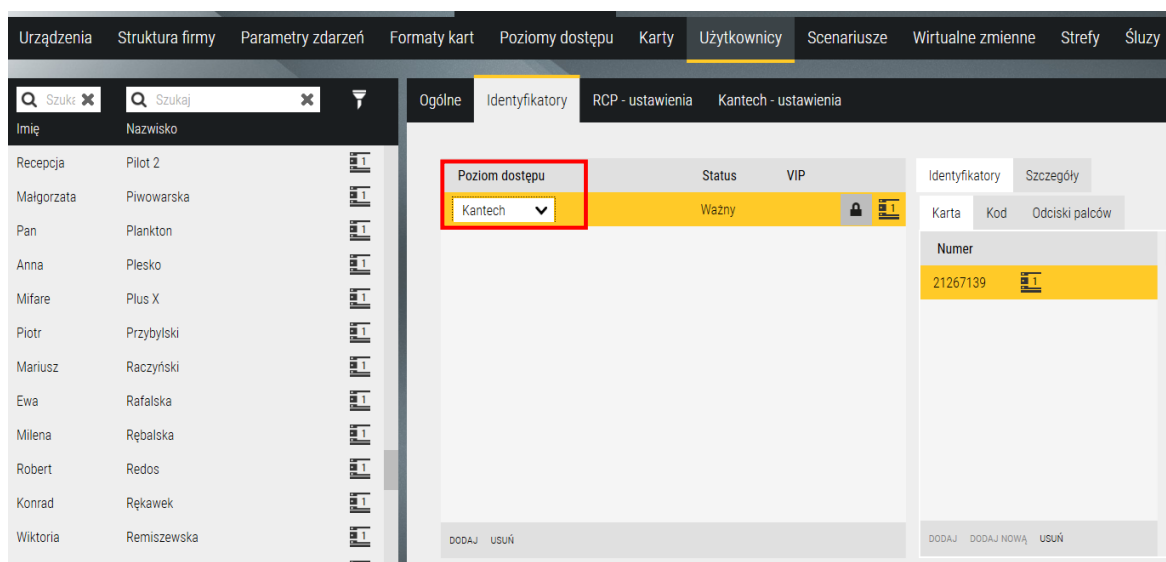
Użytkownicy - wyświetla listę użytkowników przypisanych do oprogramowania EntraPass



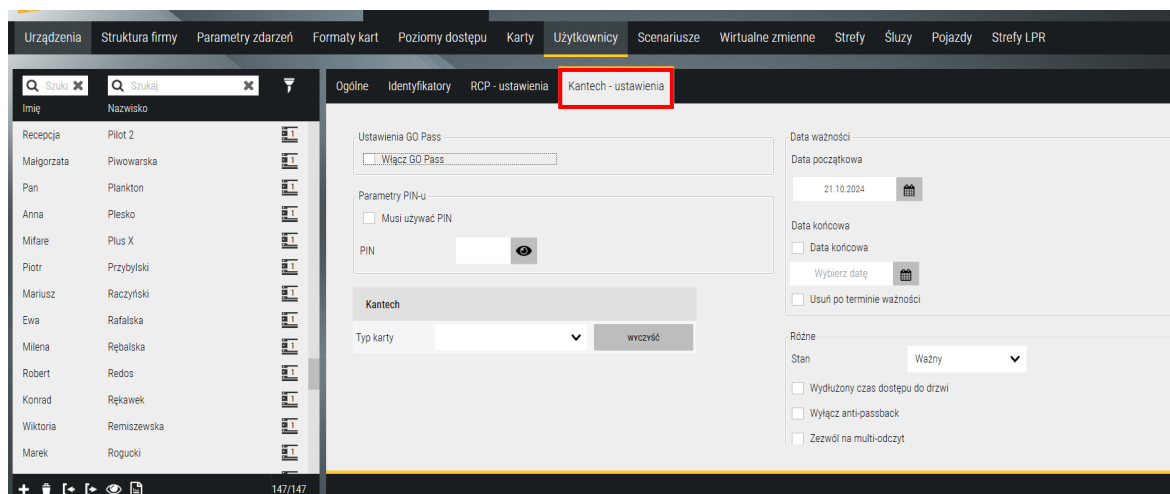
Dodawanie użytkowników - W celu dodania nowego użytkownika dla systemu Kantech EntraPass musimy najpierw stworzyć poziom dostępu dla dodanego systemu z pozycji *Konfiguracja/Poziomy Dostęp*



Następnie dodajemy użytkownika analogicznie jak w przypadku innych użytkowników systemu, poprzez zakładkę *Konfiguracja/Użytkownicy*. W pozycji *Poziomy dostęp* 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*

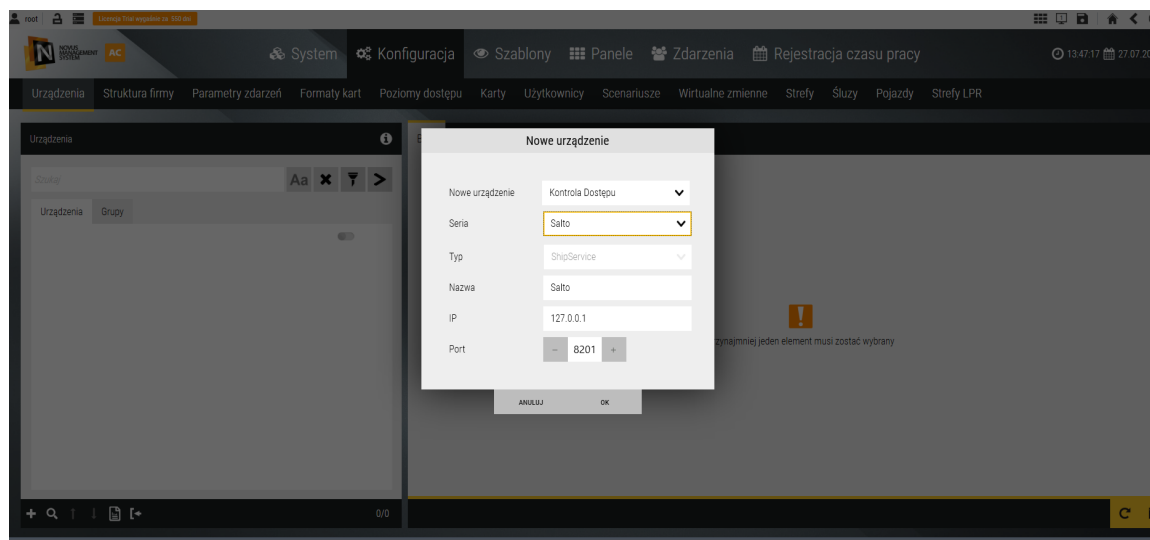
Włączenie dodatkowych funkcjonalności dla identyfikatora: Wydłużony czas na dostęp, Wyłączenie z anti-passbacku, zezwolenie na multi-odczyt

Wykaz funkcjonalności w integracji **NOVUS MANAGEMENT SYSTEM AC** z oprogramowaniem **Kantech EntraPass**

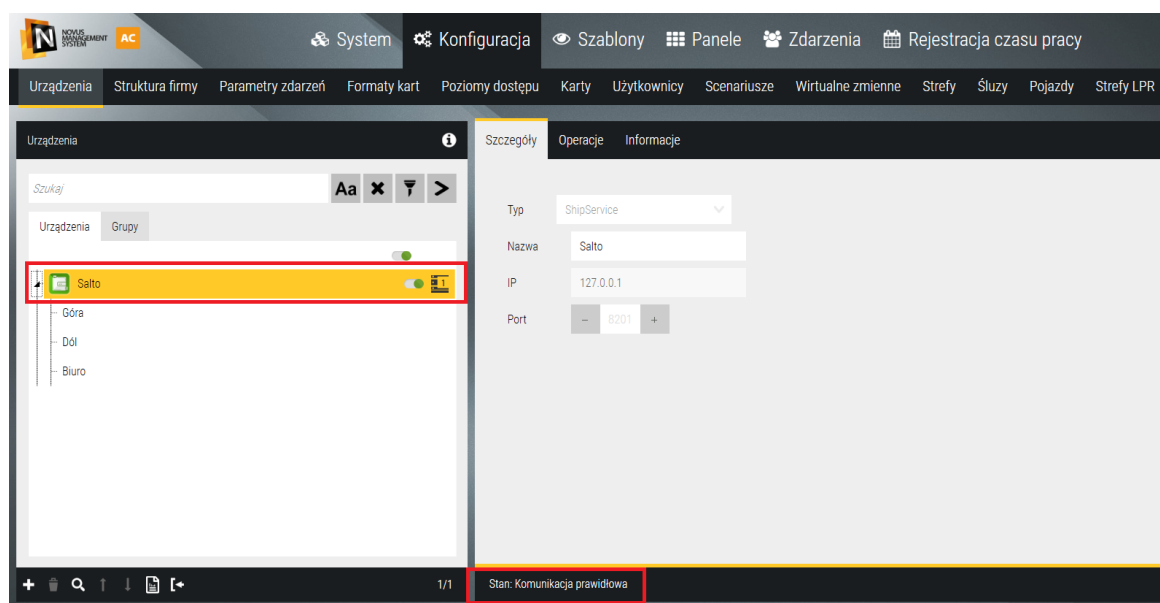
Komendy	Zdarzenia	Zarządzanie użytkownikami
Aktualizuj	Alarm	Podgląd użytkowników i kart skonfigurowanych za pomocą EntraPass
Zarygluj / odrygluj drzwi	Uszkodzenie kontrolera	
Odrygluj drzwi czasowo	Drzwi zaryglowane / odryglowane	Dodawanie i usuwanie użytkowników i kart z poziomu NMS AC
Powrót do terminarza	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 (wizualizacja) z systemem kontroli dostępu marki SALTO

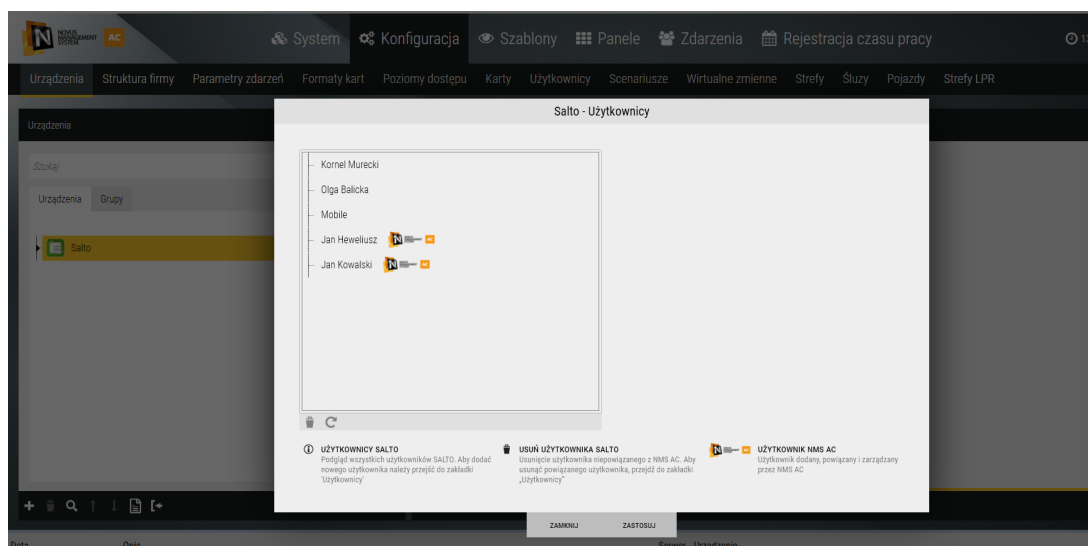
Konfiguracja oprogramowania NOVUS MANAGEMENT SYSTEM AC pod kątem współpracy z programem nadzorczym SALTO Pro Access Configurator marki SALTO



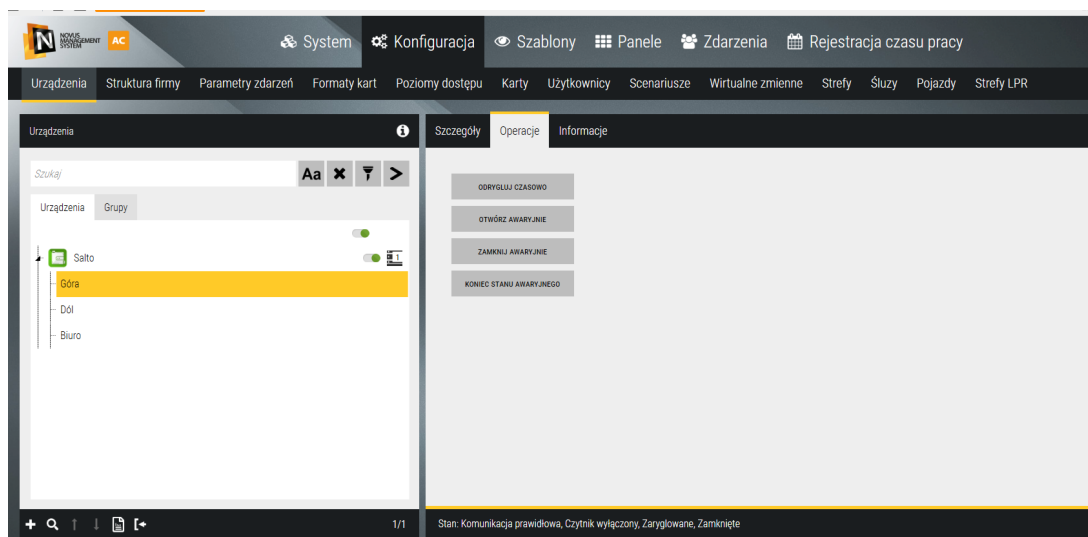
W zakładce Konfiguracja/Urządzenia wybieramy ikonę „+” nowe urządzenie, następnie Kontrola Dostępu typ Salto. Podajemy nazwę naszej integracji, adres i port komunikacyjny z aplikacją SALTO.



Po zapisaniu sprawdzamy stan komunikacji z aplikacją SALTO i poszczególnymi kontrolerami przejść.



Zakładka **Salto/Operacje/Użytkownicy** - umożliwia wyświetlenie wszystkich użytkowników systemu Salto, zarówno tych zaimportowanych do programu Novus Management System AC (z logiem systemu) jak i niezaimportowanych.



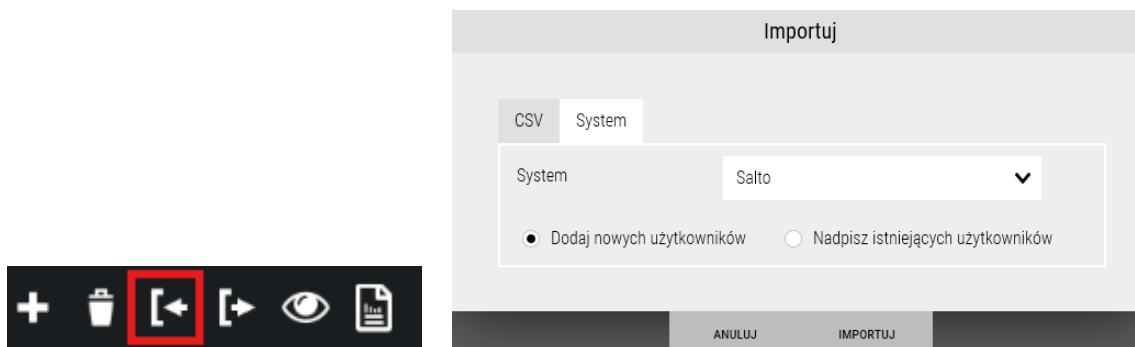
Zakładka **Salto/Kontrolery/Operacje** - zakładka umożliwia przeprowadzanie podstawowych operacji na kontrolerach przejść SALTO przez operatora Novus Management System AC.

Odrygluj czasowo - Czasowe, jednorazowe odryglowanie przejścia, czas liczony według konfiguracji w oprogramowaniu SALTO

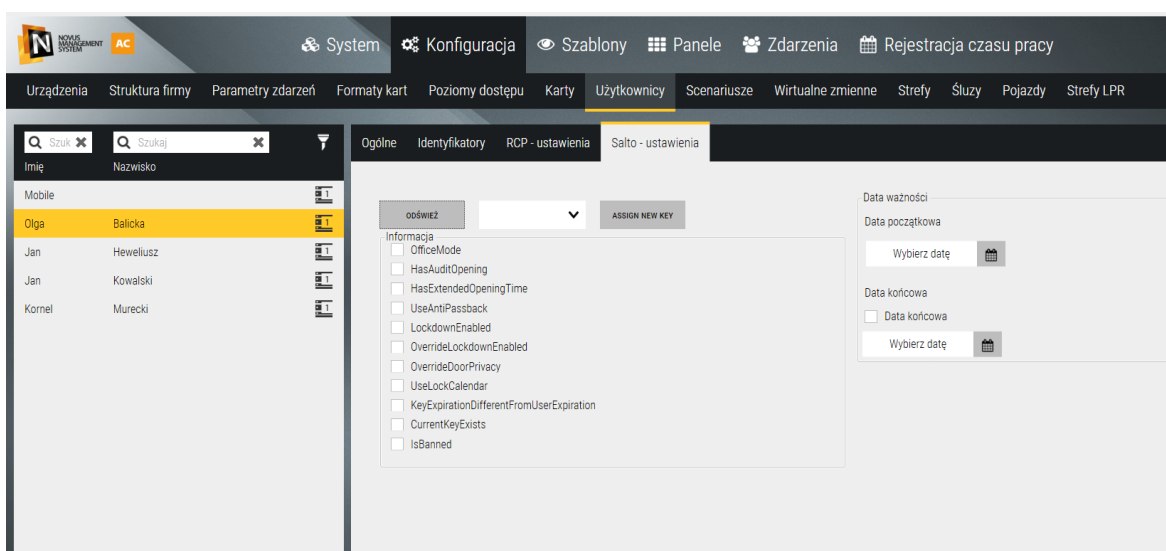
Otwórz Awaryjnie - Stałe odryglowanie przejścia przez operatora

Zamknij Awaryjnie - Zaryglowanie przejścia przez operatora

Koniec Stanu Awaryjnego - Powrót z awaryjnego odryglowania/zaryglowania do harmonogramu



Import użytkowników - Aby zaimportować użytkowników z programu SALTO do NOVUS MANAGEMENT SYSTEM AC należy przejść do zakładki **Konfiguracja/Użytkownicy** - Wybrać ikonę importu, przejść do zakładki System i wybrać połączenie SALTO z którego zaimportujemy użytkowników



Po imporcie, dla użytkowników SALTO pojawi się dodatkowa zakładka konfiguracyjna **Ustawienia** wraz z wybranymi parametrami do konfiguracji system SALTO.

9.14 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.

The screenshot displays the NOVUS MANAGEMENT SYSTEM AC configuration interface. The top navigation bar includes 'System', 'Konfiguracja', 'Szablony', 'Panele', and 'Zdarzenia'. The main menu on the left shows 'Ustawienia serwerów', 'Grupy serwerów', 'Ustawienia klienta', 'Kopia zapasowa', 'Grupy i operatorzy' (selected), and 'Licencje'. The 'Grupy i operatorzy' section is divided into three tabs: 'Uprawnienia podstawowe', 'Uprawnienia do paneli i elementów', and 'Uprawnienia do konfiguracji'. The 'Uprawnienia podstawowe' tab is active, showing a list of groups on the left and a list of operators on the right. The 'Grupa API' is highlighted in the groups list, and the 'Operator API' is highlighted in the operators list. The 'Uprawnienia podstawowe' section contains several checkboxes for basic permissions, including 'Aktualizuje serwer', 'Wymuś zmianę hasła co', 'Pamiętaj użyte hasła', 'Wyloguj po upływie czasu bezczynności', 'Zablokuj ekran po upływie czasu bezczynności', 'Minimalizowanie okna', 'Wymagany komentarz do alarmów', 'Wymagany komentarz do awarii', 'Wyłącz potwierdzanie z belki alarmów', 'Autologowanie dostępne', 'Zmiana hasła', 'Dostęp do API' (checked), and 'Nadzorca włączony'. The 'Uprawnienia do paneli i elementów' section contains checkboxes for 'Wyloguj po upływie czasu bezczynności' and 'Zablokuj ekran po upływie czasu bezczynności', both of which are checked. The 'Uprawnienia do konfiguracji' section contains checkboxes for 'Minimalizowanie okna' and 'Wymagany komentarz do alarmów', both of which are checked. The 'Widoczność użytkowników' section contains a checkbox for 'Uprawnienia do wszystkich użytkowników', which is checked. The 'Struktura firmy' field is visible at the bottom of the 'Widoczność użytkowników' section.

Dodatkowo należy tej grupie nadać odpowiednie uprawnienia do zasobów które będą modyfikowane.

W przypadku pojazdów:

The screenshot shows the 'Grupy i operatorzy' section of the NOVUS MANAGEMENT SYSTEM AC. The 'Grupa API' is selected in the left sidebar. The 'Uprawnienia do paneli i elementów' tab is active, displaying a table of permissions for various resources. The 'Pojazdy' resource is highlighted with a red box, and its permissions for 'Pokaż', 'Modyfikuj', and 'Usuń' are all checked. Other resources like 'Użytkownicy' and 'Identyfikatory' also have their permissions checked.

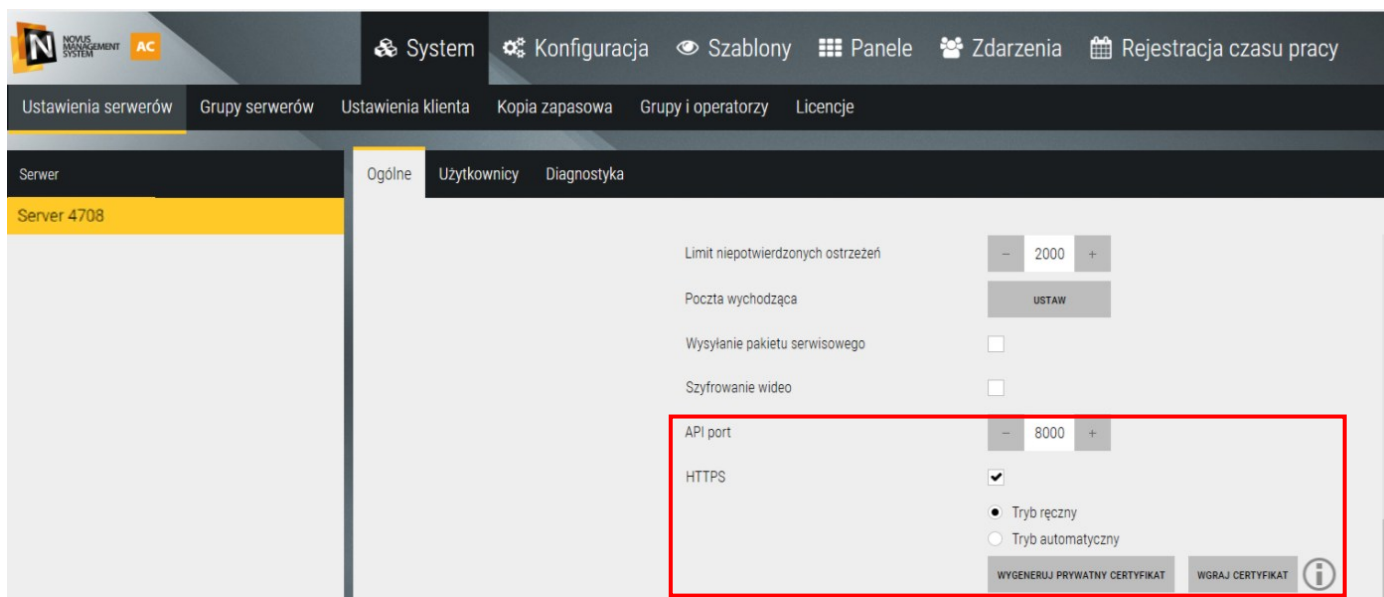
Resource	Pokaż	Modyfikuj	Usuń
Formaty kart	☐	☐	☐
Poziomy dostępu	☒	☐	☐
Karty	☐	☐	☐
Użytkownicy	☒	☒	☒
Identyfikatory	☒	☒	☒
Kody dostępu	☐	☐	☐
Kody systemu alarmowego	☐	☐	☐
Odciski palców	☐	☐	☐
RCP - ustawienia	☐	☐	☐
Scenariusze	☐	☐	☐
Wirtualne zmienne	☐	☐	☐
Strefy	☐	☐	☐
Śluz	☐	☐	☐
Pojazdy	☒	☒	☒

W przypadku kart:

The screenshot shows the 'Grupy i operatorzy' section of the NOVUS MANAGEMENT SYSTEM AC. The 'Grupa API' is selected in the left sidebar. The 'Uprawnienia do paneli i elementów' tab is active, displaying a table of permissions for various resources. The 'Karty' resource is highlighted with a red box, and its permissions for 'Pokaż', 'Modyfikuj', and 'Usuń' are all checked. Other resources like 'Użytkownicy' and 'Identyfikatory' also have their permissions checked.

Resource	Pokaż	Modyfikuj	Usuń
Formaty kart	☐	☐	☐
Poziomy dostępu	☒	☐	☐
Karty	☒	☒	☒
Użytkownicy	☒	☒	☒
Identyfikatory	☒	☒	☒

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.

W przypadku używania protokołu HTTPS i problemów z połączeniem do API z powodu certyfikatu, 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.

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.

Dostępny jest również endpoint umożliwiający dodawanie wielu pojazdów w ramach pojedynczego żądania:

POST <https://localhost:8000/api/vehicles/bulk>

W żądaniu należy przekazać listę pojazdów do utworzenia, co pozwala na ich zbiorcze dodanie bez konieczności wysyłania osobnych żądań dla każdego pojazdu.

Dostępny jest także endpoint umożliwiający masowe usuwanie pojazdów:

DELETE <https://localhost:8000/api/vehicles/bulk>

W żądaniu należy przekazać listę identyfikatorów pojazdów przeznaczonych do usunięcia. Dzięki temu możliwe jest jednoczesne usunięcie wielu pojazdów za pomocą jednego wywołania API.

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 użytkownikaPOST <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 dostępuGET <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]
}
```

W przypadku przypisywania kart do poświadczenia należy w polu cards przekazać listę identyfikatorów kart.

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": []
}
```

Poziom dostępu przypisany do Credentials można również modyfikować za pomocą dedykowanego endpointu.

PATCH <https://localhost:8000/api/credentials/{credentialId}>

JSON BODY

```
{
  "accessLevelId": 0
  "vehicles": [id1,id2,...]
}
```

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}>

Do usuwania wielu pojazdów oraz wielu poświadczeń (credentials) jednocześnie można również wykorzystać dedykowane endpointy.

```
DELETE https://localhost:8000/api/credentials/bulk
```

JSON BODY

```
[
```

```
  Id1,
```

```
  id2,
```

```
  Id3,
```

```
  ...
```

```
]
```

```
DELETE https://localhost:8000/api/vehicles/bulk
```

JSON BODY

```
[
```

```
  Id1,
```

```
  id2,
```

```
  Id3,
```

```
  ...
```

```
]
```

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:

GET <https://localhost:8000/api/itemsAndEventsfilters>

Odpowiedź zawiera dostępne elementy systemu oraz filtry, które mogą zostać wykorzystane podczas pobierania zdarzeń.

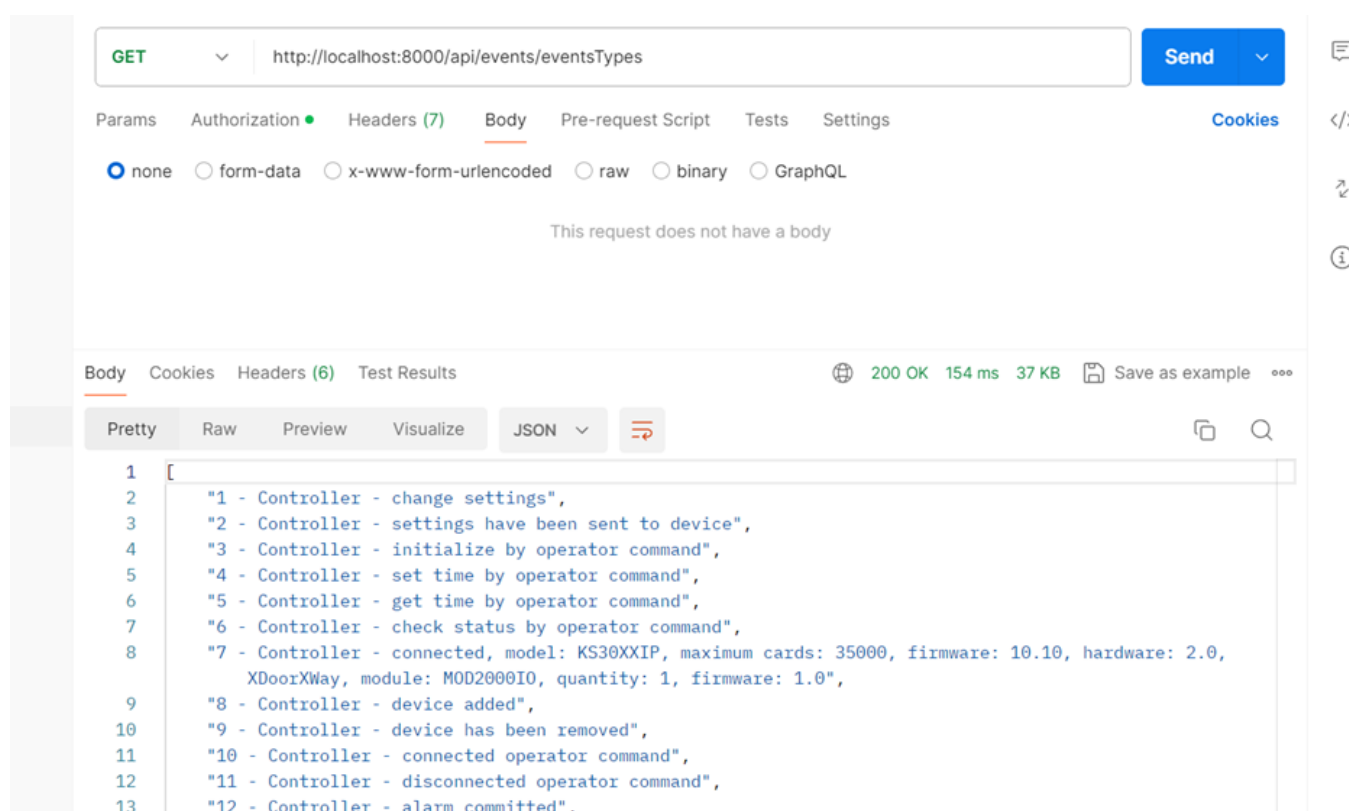
Parametry wykorzystywane do pobierania zdarzeń obejmują między innymi:

Limit - określa maksymalną liczbę zdarzeń zwróconych dla wybranego zakresu czasu.

Language - określa język tłumaczenia opisów zdarzeń (pl - język polski, en - język angielski).

Listę wszystkich możliwych identyfikatorów zdarzeń (EventTypeID) wraz z ich opisami (Details) można wylistować za pomocą:

GET <https://localhost:8000/api/events/eventTypes>



Lista urządzeń

Aby pobrać listę urządzeń dostępnych w systemie, należy wykonać zapytanie:

GET <https://localhost:8000/api/devices>

W odpowiedzi zwracana jest hierarchiczna struktura urządzeń, kanałów oraz strumieni dostępnych w systemie, np.

```
{
  "id": 11007,
  "name": "NVR-6316-H1-II",
  "type": "NVR",
  "children": [
    {
      "id": 10020,
      "name": "PtzCam",
      "type": "Channel",
      "children": [
        {
          "id": 10014,
          "name": "Stream 1",
          "type": "Stream",
          "children": [],
          "parent": {
            "id": 10020,
            "name": "PtzCam",
            "type": "Stream",
            "children": null,
            "parent": null
          }
        },
        {
          "id": 10015,
          "name": "Stream 2",
          "type": "Stream",
          "children": [],
          "parent": {
            "id": 10020,
            "name": "PtzCam",
            "type": "Stream",
            "children": null,
            "parent": null
          }
        }
      ]
    }
  ],
  ...
}
```


Type określa typ elementu w strukturze drzewa, np.:

NVR - rejestrator,

Channel - kanał urządzenia,

Stream - strumień wideo przypisany do kanału.

Id - unikalny identyfikator elementu w systemie.

Name - nazwa elementu wyświetlana w systemie, np. PTzCam, Stream 1 lub NVR-6316-H1-II.

Children - lista elementów podrzędnych powiązanych z danym elementem. Przykładowo rejestrator (NVR) może zawierać kanały (Channel), a kanał może zawierać strumienie (Stream).

Parent - element nadrzędny. Pole to wskazuje obiekt, do którego należy dany element. Przykładowo strumień (Stream) posiada jako element nadrzędny kanał (Channel), z którym jest powiązany.

Lista harmonogramów

GET <https://localhost:8000/api/schedules>

Zapytanie zwróci listę harmonogramów

```
[
  {
    "id": 1,
    "name": "Never"
  },
  {
    "id": 2,
    "name": "Always"
  }
]
```

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, HTTPS np. Postman. Aby wykonać eksport nagrań potrzebne są:

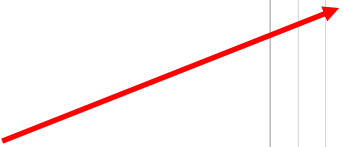
- ID kanału wideo, z którego ma być nagranie,
- ID harmonogramu (domyślnie wartość 2 oznacza harmonogram Zawsze).

Obok zapytań zostały umieszczone przykładowe odpowiedzi z programu Postman.

Procedura pobierania nagrań przez API:

Pobranie ID kanału

GET <https://localhost:8000/api/devices>



```

{
  "id": 29801,
  "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
          }
        }
      ]
    }
  ]
}

```

Pobranie ID harmonogramu

GET <https://localhost:8000/api/schedules>



```

1 [
2   {
3     "id": 1,
4     "name": "Never"
5   },
6   {
7     "id": 2,
8     "name": "Always"
9   }
10 ]

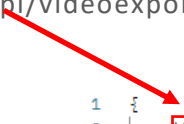
```

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
}

```

```

1 {
2   "id": 761768,
3   "audio": true,
4   "channelsId": [
5     32452
6   ],
7   "container": "avi",
8   "created": "2026-01-16T13:27:21.5901411Z",
9   "destinationPath": "C:\\WINDOWS\\system32\\config\\systemprofile\\Downloads",
10  "progress": 0,
11  "from": "2026-01-16T11:25:00Z",
12  "operatorId": 11013,
13  "isRemovalRestricted": false,
14  "scheduleId": 2,
15  "autoDownload": false,
16  "state": "Waiting",
17  "to": "2026-01-16T11:30:00Z",
18  "video": true,
19  "hasWatermark": false,
20  "hasCameraName": false,
21  "hasDeviceName": false,
22  "hasTimeStamp": false
23 }

```

Opis parametrów:

channelId - 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

```

1  [
2    {
3      "id": 761768,
4      "audio": true,
5      "channelId": [
6        32452
7      ],
8      "container": "avi",
9      "created": "2026-01-16T13:27:21.6901411Z",
10     "destinationPath": "C:\\WINDOWS\\system32\\config\\systemprofile\\Downloads",
11     "progress": 100,
12     "from": "2026-01-16T11:25:00Z",
13     "operatorId": 11013,
14     "isRemovalRestricted": false,
15     "scheduleId": 2,
16     "autoDownload": false,
17     "state": "ManualDownload",
18     "to": "2026-01-16T11:30:00Z",
19     "video": true,
20     "hasWatermark": false,
21     "hasCameraName": false,
22     "hasDeviceName": false,
23     "hasTimeStamp": false
24   }
25 ]

```

Id zadania

Poziom postępu eksportu

Stan zadania

Sprawdzenie statusu zadania

GET https://localhost:8000/api/videoexport/{id zadania}

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

```

1  [
2    {
3      "file": "C:\\Program Files (x86)\\NOVUS MANAGEMENT SYSTEM AC\\Server\\VideoExport\\61814\\NHDR-416AHD_Channel_05_2025-11-27_09-20-00_part1.avi",
4      "part": 1
5    }
6  ]

```

Id pliku

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}

Strefy LPR

Użytkownik może odpytać o aktualnie stworzone strefy LPR poleceniem:

```
GET http://127.0.0.1:8000/api/LPRZones
```

Odpowiedź zawiera listę stref wraz z podstawowymi informacjami:

```
[
  {
    "id": 1,
    "name": "UnknownZone",
    "capacity": 2147483647
  },
  {
    "id": 2,
    "name": "StrefaParkingowaHotel",
    "capacity": 128
  }
]
```

Gdzie:

Id - unikalny identyfikator strefy,

Name - nazwa strefy,

Capacity - maksymalna liczba pojazdów, które mogą jednocześnie znajdować się w strefie.

Dostępny jest również endpoint zwracający informacje o pojazdach aktualnie przebywających w wybranej strefie.

```
GET http://127.0.0.1:8000/api/LPRZones/{IdStrefy}
```

Gdzie *{IdStrefy}* należy zastąpić identyfikatorem strefy zwróconym przez endpoint */api/LPRZones*.

Odpowiedź zawiera informacje o:

- liczbie pojazdów aktualnie znajdujących się w strefie,
- pojazdach przypisanych do strefy, które znajdują się w niej w danym momencie,
- podstawowych danych tych pojazdów.

ODPŁATNA UMOWA LICENCYJNA
Programu „NOVUS MANAGEMENT SYSTEM” – wersja AC
[Wersja licencji: ac_vl_20260714]

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. Aktualizacja Programu może odbywać się przez uruchomienie pliku aktualizacji lub automatycznie przy połączeniu aplikacji klienta Programu z aplikacją serwera Programu – na warunkach wskazanych w tych aktualizacjach. 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, jeśli takie zostaną udostępnione przez Producenta.
- 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. *Dostęp do niektórych funkcjonalności Programu może być ograniczony i uzależniony od wniesienia dodatkowej Opłaty licencyjnej, zgodnie z niniejszą Umową lub umowami licencyjnymi funkcjonalności.*

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. 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 jakiegokolwiek 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 poniesionej przez Użytkownika Opłaty licencyjnej* 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 wynikać 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 doбором 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. FUNKcjONALNOŚCI

- 10.1. Użytkownik może dodać do Programu funkcjonalności lub rozszerzenia dostępne w ofercie Producenta („**Funkcjonalności**”). Funkcjonalność jest częścią Programu i podlega instalacji razem z nim. Aktywacja Funkcjonalności polega na uiszczeniu dodatkowej opłaty licencyjnej (zakupie odpowiedniego Klucza licencji), uruchomieniu Funkcjonalności oraz wpisaniu Klucza licencji we właściwym miejscu w Programie.
- 10.2. W przypadku braku odrębnej umowy licencyjnej dotyczącej Funkcjonalności, zastosowanie mają poniższe postanowienia. Jeżeli nie wyrażasz zgody na niniejsze postanowienia, przerwij natychmiast korzystanie z Funkcjonalności i dezaktywuj ją.
- 10.3. Dana Funkcjonalność może być kompatybilna z odpowiednią wersją Programu. Użytkownik jest świadomy, że dana Funkcjonalność może nie być kompatybilna z przeszłymi lub przyszłymi wersjami Programu. Warunkiem korzystania z Funkcjonalności jest posiadanie przez Użytkownika aktywnej licencji do odpowiedniej wersji Programu.
- 10.4. W przypadku zakupu przez Użytkownika licencji na daną Funkcjonalność, Producent udziela Użytkownikowi licencji tylko na własny użytek, bez prawa wyłączności, bez prawa udzielenia licencji innym osobom, na okres wskazany w dokumencie sprzedaży (zgodnie z pkt 10.6 Umowy), na terytorium wskazanym w formularzu rejestracyjnym Programu, na korzystanie z tej Funkcjonalności na komputerze stacjonarnym lub przenośnym zgodnie z niniejszą Umową. Postanowienia pkt 4 Umowy stosuje się odpowiednio.
- 10.5. W przypadku zakupu przez Użytkownika licencji na daną Funkcjonalność, częścią Umowy jest dokument zakupu.
- 10.6. Po upływie okresu Trial Programu, o którym mowa w pkt 6.2. Umowy, Umowa ulega przekształceniu w Umowę na czas określony, wskazany w dokumencie sprzedaży, liczony od dnia aktywacji danej Funkcjonalności (wpisania Klucza licencji), pod warunkiem zakupu licencji oraz aktywacji Funkcjonalności. W przypadku braku wskazania w dokumencie sprzedaży czasu obowiązywania Umowy w zakresie danej Funkcjonalności, Strony przyjmują, iż jest ona zawarta na czas nieokreślony.
- 10.7. W przypadku zakończenia obowiązywania Umowy przed końcem okresu, o którym mowa w pkt 10.6, Użytkownikowi nie przysługuje zwrot Opłaty licencyjnej za niewykorzystany okres trwania Umowy licencyjnej.
- 10.8. W pozostałym, nieuregulowanym w niniejszym punkcie zakresie, do Funkcjonalności mają odpowiednie zastosowanie postanowienia Umowy dotyczące Programu.

11. SIŁA WYŻSZA

- 11.1. 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.
- 11.2. 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.
- 11.3. 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.

12. ROZSTRZYGANIE EWENTUALNYCH SPORÓW

- 12.1. Wszelkie spory mogące powstać na tle wykonywania Umowy, Strony zobowiązują się rozstrzygać polubownie.

- 12.2. 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.
- 12.3. Naruszenie Praw Autorskich i Praw Pokrewnych Producenta może pociągnąć odpowiedzialność cywilną oraz karną podmiotu naruszającego te prawa.

13. POSTANOWIENIA KOŃCOWE

- 13.1. 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.
- 13.2. 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.
- 13.3. Producent może dokonać cesji praw do Programu, jego części, na osoby trzecie według swego wyboru, bez konieczności powiadamiania Użytkownika.
- 13.4. Użytkownik bez zgody Producenta nie może dokonać cesji praw uzyskanych na podstawie Umowy na osoby trzecie.
- 13.5. Użytkownik oświadcza, że zapoznał się z treścią Umowy przed rozpoczęciem korzystania z Programu i nie wnosi co do niej żadnych zastrzeżeń.
- 13.6. 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 zostałyby 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.
- 13.7. 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.
- 13.8. 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 6.06.017

Data: 11.08.2026

Kontrola dostępu – SALTO

- Dodano integrację z systemem kontroli dostępu SALTO (integracja za pośrednictwem serwera SALTO ProAccess Space, szczegóły w instrukcji obsługi oprogramowania NOVUS MANAGEMENT SYSTEM AC).

Rejestracja czasu pracy

- Dodano nową funkcjonalność raportu zdarzeń rejestracji czasu pracy w postaci nowego typu raportu „Eksport zdarzeń”. Funkcjonalność powiązana z nową licencją „NOVUS MANAGEMENT SYSTEM AC Raport zdarzeń RCP 365 v6”. Umożliwia dopasowanie formatu raportu na potrzeby integracji z programami kadrowo-płacowymi.
- Zmodyfikowano funkcjonalność kalendarzy dodatkowych, umożliwiając definiowanie indywidualnych wyjątków od standardowego kalendarza pracy użytkownika.

Ogólne

- Dodano operatora zanonimizowanego, który umożliwia pracę w systemie z uprawnieniami administratora (konto root) przy jednoczesnym ukryciu danych osobowych użytkowników.
- Dodano możliwość definiowania lokalizacji raportów na dysku sieciowym w polu Ścieżka raportów w ustawieniach serwera.
- Dodano nową reakcję Zmodyfikuj użytkownika w zakładce Scenariusze.
- Dodano identyfikator sprzętowy (Hardware ID) do dokumentu licencyjnego generowanego za pomocą opcji Drukuj do PDF w zakładce Licencje.
- Dla wybranych urządzeń w podzakładce Informacje dodano takie informacje jak wersja oprogramowania (firmware), adres MAC czy różnica czasu pomiędzy urządzeniem, a serwerem systemu.
- Dodano opcję „Zaznacz wszystkie uprawnienia”, umożliwiającą jednoczesne nadawanie lub odbieranie wszystkich uprawnień dla wybranego urządzenia w zakładce Uprawnienia do urządzeń.
- Usprawniono generowanie certyfikatów HTTPS. Dodano obsługę trybu ręcznego i automatycznego oraz możliwość generowania i wgrywania certyfikatów. Certyfikaty są zapisywane w katalogu Certificates na serwerze.
- Poprawiono możliwość wykonywania zanonimizowanej kopii zapasowej dla dużych konfiguracji.
- Usprawniono działanie wyszukiwarki urządzeń podczas filtrowania po adresie MAC.
- Poprawiono styl rozwijanych menu, w tym menu użytkownika, narzędzia Stos zdarzeń bieżących oraz menu edycji elementów na panelu.
- Usprawniono działanie zakładki Scenariusze oraz narzędzi panelowych, eliminując problem rozszerzania okien po wprowadzeniu zbyt długich ciągów znaków.
- Usprawniono działanie kopiowania scenariuszy zawierających wyłącznie warunek.
- Poprawiono działanie edycji elementów systemu POLON 6000.

- Ukryto klucze licencyjne w zakładce Licencje. Pełna wartość klucza licencji wyświetlana jest dopiero po najechaniu kursorem.
- Poprawiono bezpieczeństwo zarządzania operatorami oraz grupami użytkowników, uniemożliwiając tworzenie grup oraz operatorów posiadających uprawnienia wyższe niż uprawnienia operatora wykonującego konfigurację.
- Dodano możliwość zoomowania panelu za pomocą kombinacji klawiszy SHIFT+CTRL oraz rolki myszy.

Telewizja dozorowa

- Poprawiono raport nagrań dla systemu NOVUS MANAGEMENT SYSTEM VSS.
- Poprawiono rozmieszczenie ikon na pasku narzędzia Wideo.
- Usprawniono działanie funkcji wideoweryfikacji w przypadku rozbieżności czasu pomiędzy serwerem, a rejestratorem.
- Poprawiono szybkość ładowania się strumieni wideo w przypadku współpracy z 64-kanalowymi rejestratorami serii 6000.

Głośnik IP

- Dodano możliwość wykonania polecenia Wygłoś komunikat z poziomu ikony głośnika na panelu.
- Zmieniono typ urządzenia na Głośnik IP.

Kontrola dostępu

- Dodano możliwość kopiowania numerów nieznanymi kart z poziomu menu podglądu zdarzeń.
- Usprawniono proces przypisywania kart do użytkowników z poziomu zakładki Karty.
- Przetłumaczono komunikaty logów związane ze zmianą trybu identyfikacji karty.

Kontrola dostępu - HID® Aero®

- Zmieniono nazwę pola Nazwa na Własny identyfikator dla czytników w przypadku kontrolerów HID® Aero® w podzakładce Szczegóły dostępnej po wybraniu czytnika w zakładce Urządzenia.
- Dodano nowe biblioteki dla kontrolerów HID® Aero®.
- Poprawiono działanie kontrolerów HID® Aero® po zaniku i powrocie zasilania.

Kontrola dostępu – Kantech

- Poprawiono wygląd okna podczas dodawania urządzeń kontroli dostępu Kantech.
- Poprawiono widok zakładki Szczegóły dla urządzeń typu Kontrola dostępu.

Kontrola dostępu – SALTO

- Dodano integrację z systemem kontroli dostępu SALTO (integracja za pośrednictwem serwera SALTO ProAccess Space, szczegóły w instrukcji obsługi oprogramowania NOVUS MANAGEMENT SYSTEM AC).

Rejestracja czasu pracy

- Dodano nową funkcjonalność raportu zdarzeń rejestracji czasu pracy w postaci nowego typu raportu „Eksport zdarzeń”. Funkcjonalność powiązana z nową licencją „NOVUS MANAGEMENT SYSTEM AC Raport zdarzeń RCP 365 v6”. Umożliwia dopasowanie formatu raportu na potrzeby integracji z programami kadrowo-płacowymi.
- Dodano możliwość generowania raportu typu „Eksport zdarzeń” z poziomu scenariusza.
- Dodano możliwość wyboru czasu (dotychczas dostępny był jedynie wybór daty), podczas generowania ręcznych raportów RCP.
- Zmodyfikowano funkcjonalność kalendarzy dodatkowych, umożliwiając definiowanie indywidualnych wyjątków od standardowego kalendarza pracy użytkownika.
- Dodano możliwość sortowania kolumn listy obecności w kolejności rosnącej i malejącej oraz tworzenia tymczasowych szablonów raportów typu Lista obecności wraz z możliwością ich generowania z uwzględnieniem zdefiniowanego sortowania.
- Dodano regułę raportu umożliwiającą uwzględnianie w raporcie tylko pierwszego wejścia i ostatniego wyjścia.
- Naprawiono działanie scenariusza wykorzystującego warunek Rejestracja czasu pracy wraz ze statusami czasu pracy.
- Poprawiono raport Lista obecności z uwzględnieniem rodzaju statusu czasu pracy.
- Poprawiono generowanie automatycznych raportów.
- Poprawiono działanie harmonogramów zmianowych w przypadku zmian przechodzących na kolejny dzień oraz dni wolnych wynikających z harmonogramu.

Rozpoznawanie tablic rejestracyjnych

- Modyfikacja działania API pod kątem poprawy obsługi funkcji dotyczących rozpoznawania numerów tablic rejestracyjnych.

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 będą 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 systemy 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, słuz 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 słuz 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 przepełnieniem
- 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 multiserverowości
- 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 zwinienia 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 multiserverowym
- 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 multiserverowości 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. Raclawicka 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