Roger Access Control System 5v2

Nota aplikacyjna nr 025

Wersja dokumentu: Rev. A

Tryby autoryzacji

Uwaga: Niniejszy dokument dotyczy RACS 5 v2.0.8 lub nowszy

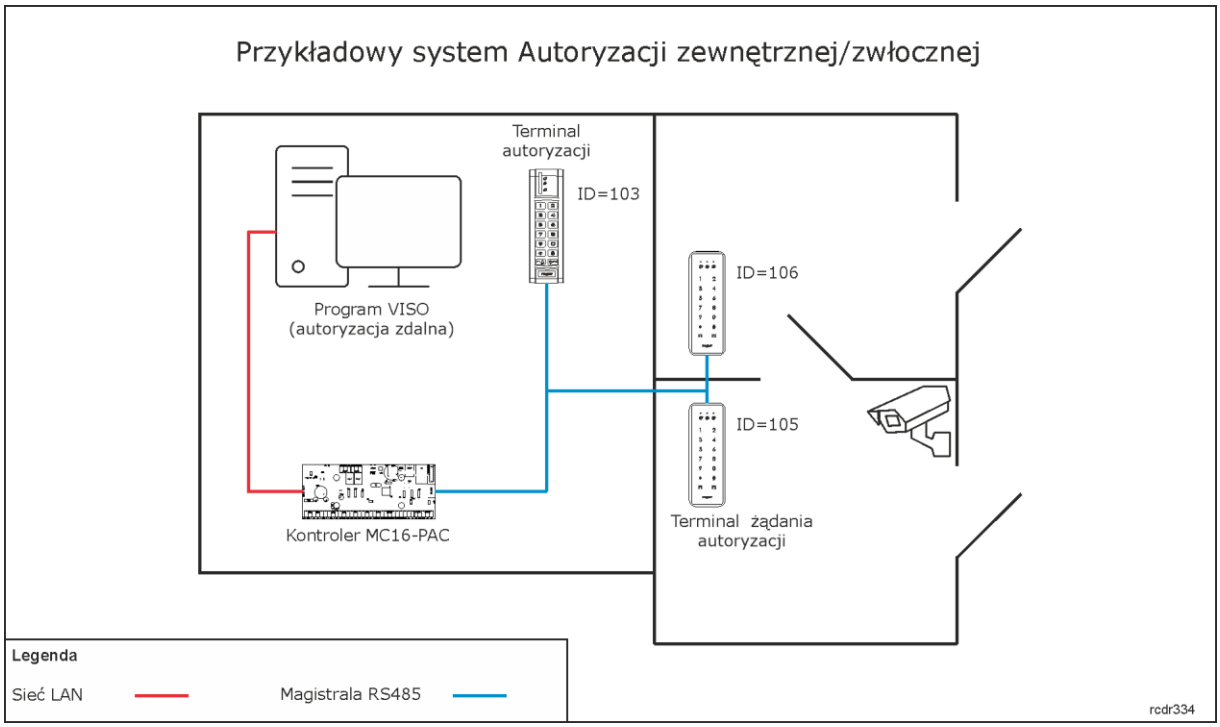
Wprowadzenie

W systemie RACS 5 istnieje możliwość stosowania Trybów autoryzacji na Punktach identyfikacji (czytnikach) systemu. Tryby autoryzacji określają sposób podejmowania decyzji o przyznawaniu lub odmowie dostępu.

Dostępne Tryby autoryzacji:

- Autoryzacja normalna – dostęp zależy od Uprawnień użytkownika.
- Autoryzacja pozytywna – dostęp nie wymaga Uprawnień więc każdy użytkownik zdefiniowany w systemie może uzyskiwać dostęp.
- Autoryzacja negatywna – odmowa dostępu bez względu na posiadane Uprawnienia (nie dotyczy Identyfikatorów z wyjątkiem Master).
- Autoryzacja zewnętrzna – dostęp oprócz Uprawnienia wymaga dodatkowej zgody zewnętrznej z wykorzystaniem funkcji wejściowej *[185]* lub na poziomie programu VISO.
- Autoryzacja zwłoczna – dostęp wynikający z Uprawnienia jest opóźniany i w trakcie jego odliczania można wywołać odmowę dostępu z wykorzystaniem funkcji wejściowej *[186]* lub na poziomie programu VISO.
- Autoryzacja wyłączona – odmowa dostępu bez względu na posiadane Uprawnienia (dotyczy Identyfikatorów z wyjątkiem Master)

Niniejsza nota skupia się na trybach Autoryzacji zewnętrznej i Autoryzacji zwłocznej. Oba tryby znajdują swoje zastosowanie np. w jednostkach wojskowych, aresztach, więzieniach, szpitalach zamkniętych i innych obiektach, w których wymagany jest dodatkowy nadzór strażnika nad wybranymi przejściami systemu KD. W takim scenariuszy pracy, strażnik może zatwierdzać bądź blokować żądanie przyznania dostępu za strony użytkownika systemu zarówno za pomocą terminala systemu jak też zdalnie za pomocą oprogramowania VISO lub oprogramowania firm trzecich jeżeli zostało one zintegrowane z systemem RACS 5 za pośrednictwem tzw. Serwera integracji z pakietu oprogramowania RogerSVC.

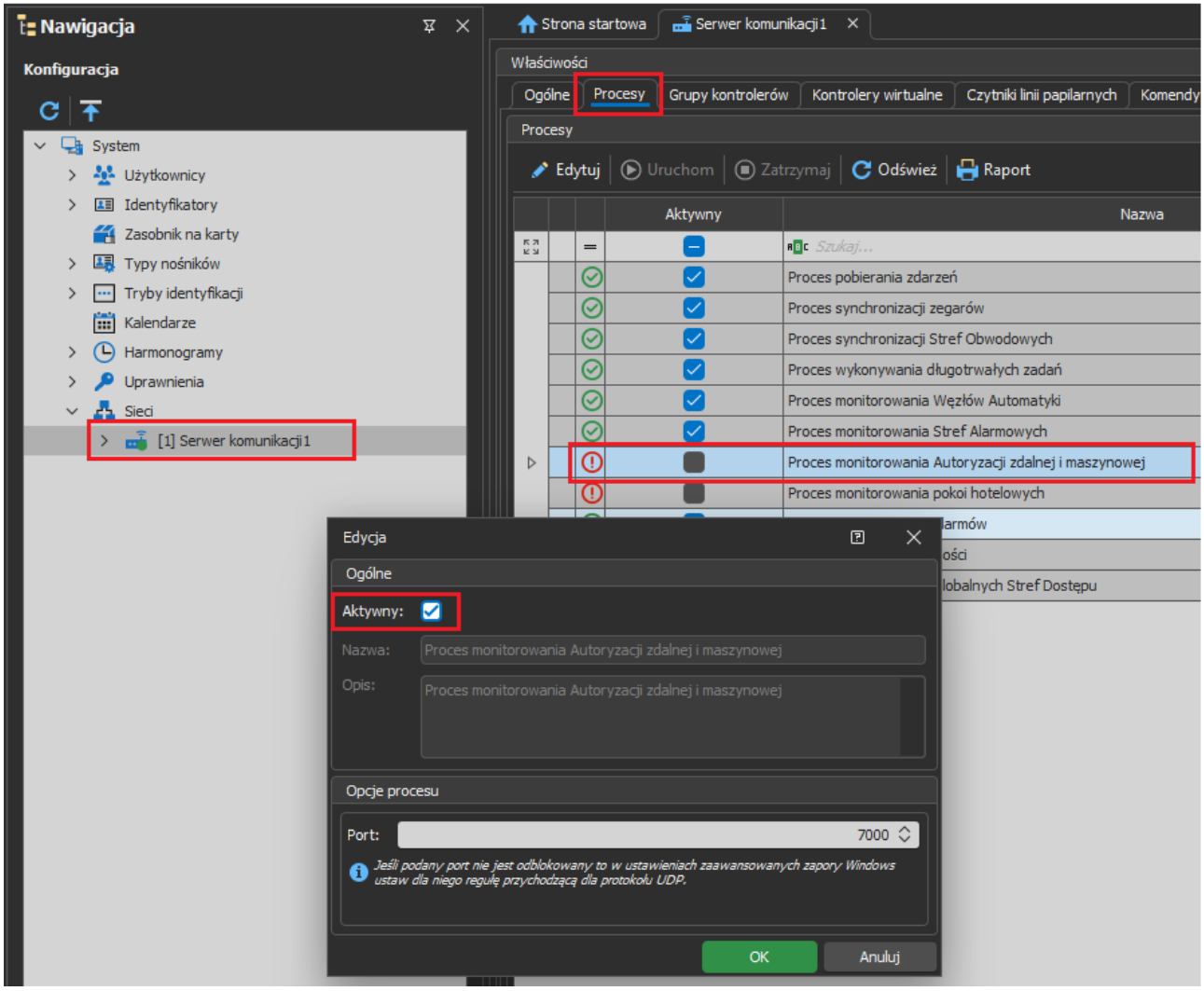


Uwagi do rysunku:

- Zasilanie w przedstawionym przykładzie można zapewnić poprzez zastosowanie kontrolera MC16-PAC w zestawie MC16-PAC-2-KIT.
- Całkowita ilość urządzeń MCT/MCX na magistrali RS485 danego kontrolera nie może przekroczyć dostępnej puli 16 adresów z zakresu ID=100-115. Podane na rysunku adresy czytników na magistrali RS485 są przykładowe.
- Maksymalna długość magistrali RS485 to 1200m i wszystkie urządzenia na tej magistrali powinny mieć wspólny minus zasilania.

Konfiguracja wstępna systemu

- Skonfiguruj system RACS 5 zgodnie z notą aplikacyjną AN006 w zakresie konfiguracji niskopoziomowej, bazy danych, serwisów i detekcji kontrolera z jego urządzeniami peryferyjnymi.
- Jeżeli ma być zastosowana zdalna autoryzacja dostępu za pomocą oprogramowania VISO, którą opisano w dalszej części noty to dwukrotnie kliknij dany Serwer komunikacji w drzewku programu VISO i następnie wybierz zakładkę *Procesy*.
- Kliknij prawym przyciskiem myszy *Proces monitorowania Autoryzacji zdalnej i maszynowej* i następnie wybierz *Edytuj*.
- Uruchom proces i zdefiniuj port komunikacyjny (domyślnie 7000).



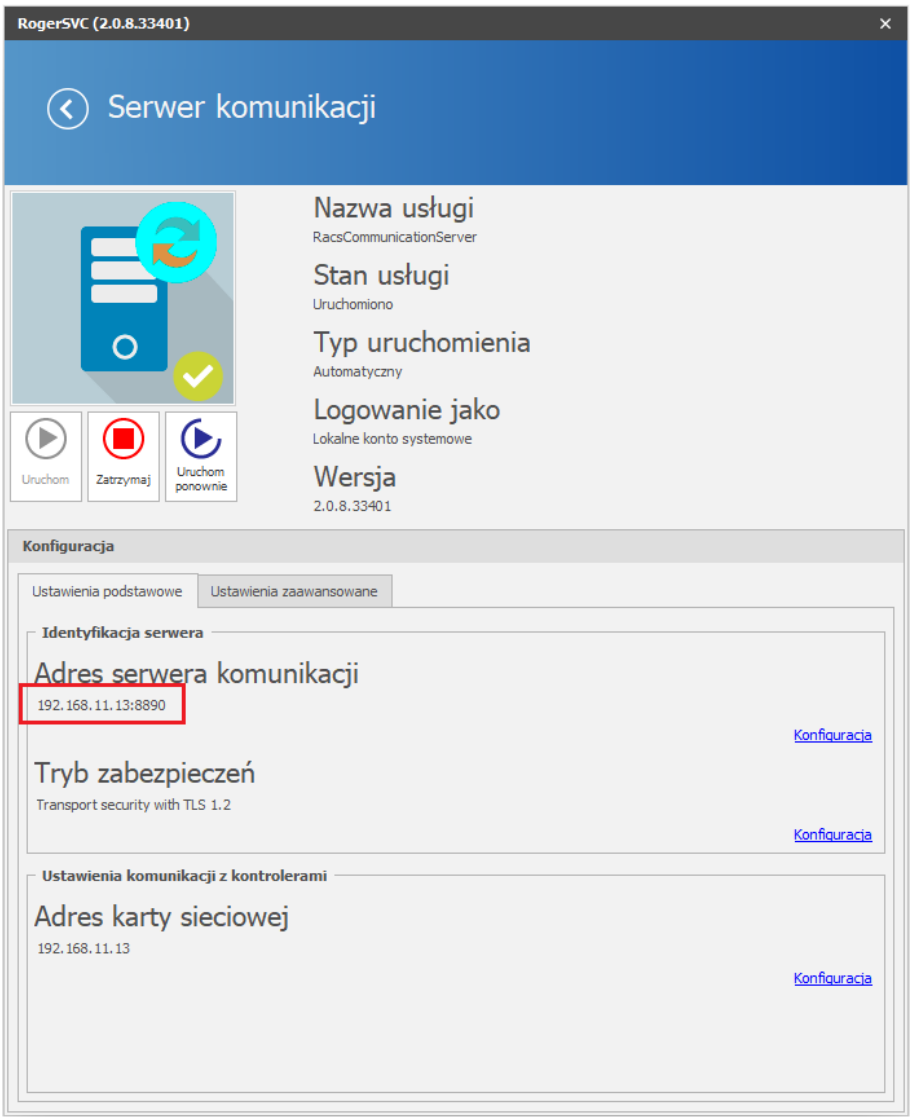
Dodatkowo konfiguracja niskopoziomowa

Jeżeli ma być zastosowana autoryzacja dostępu za pomocą oprogramowania VISO, którą opisano w dalszej części noty to w takiej sytuacji kontroler MC16 wymaga nie tylko typowej konfiguracji niskopoziomowej za pomocą programu RogerVDM lub VISO v2 ale również dodatkowej konfiguracji z wykorzystaniem jego karty pamięci. W tym celu:

- Wyłącz zasilanie kontrolera MC16.
- Naciśnij kartę pamięci by wyjąć ją z gniazda zamontowanego pod baterią CR2032 na płycie kontrolera.
- Za pomocą standardowego czytnika kart pamięci Flash podłącz kartę do portu USB komputera.
- Dodaj przykładową zawartość w pliku DEBUG.CFG na karcie pamięci:

STP=7001
VRI=192.168.11.13
VRP=7000

gdzie:
STP – dowolny niezajęty port UDP do wykorzystania w komunikacji z kontrolerem.
VRI – adres IP komputera z Serwerem komunikacji z pakietu oprogramowania RogerSVC.
VRP – port UDP procesu autoryzacji zewnętrznej, który jest definiowany w ramach wcześniej opisanego *Procesu monitorowania Autoryzacji zdalnej i maszynowej* w programie VISO.



Uwaga: Plik DEBUG.CFG musi być zakończony pustą linią, co oznaczą że na końcu linii VRP należy nacisnąć Enter by przejść do kolejnej linii i dopiero wtedy zapisać plik na karcie pamięci.

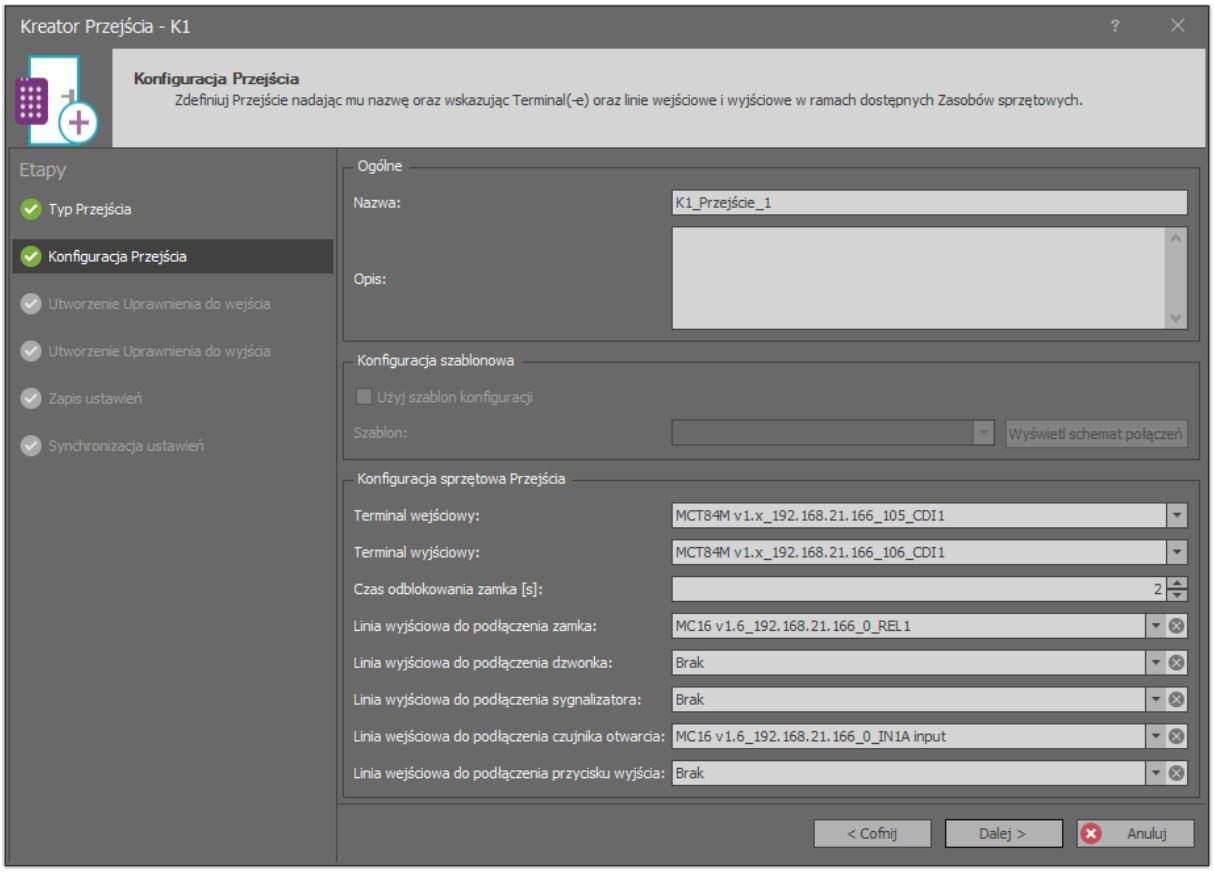
Uwaga: Może być wymagane odblokowanie portów STP i VRP w zaporze komputera z Serwerem komunikacji systemu RACS 5.

- Zamontuj z powrotem kartę w gnieździe kontrolera.
- Włącz zasilanie kontrolera.

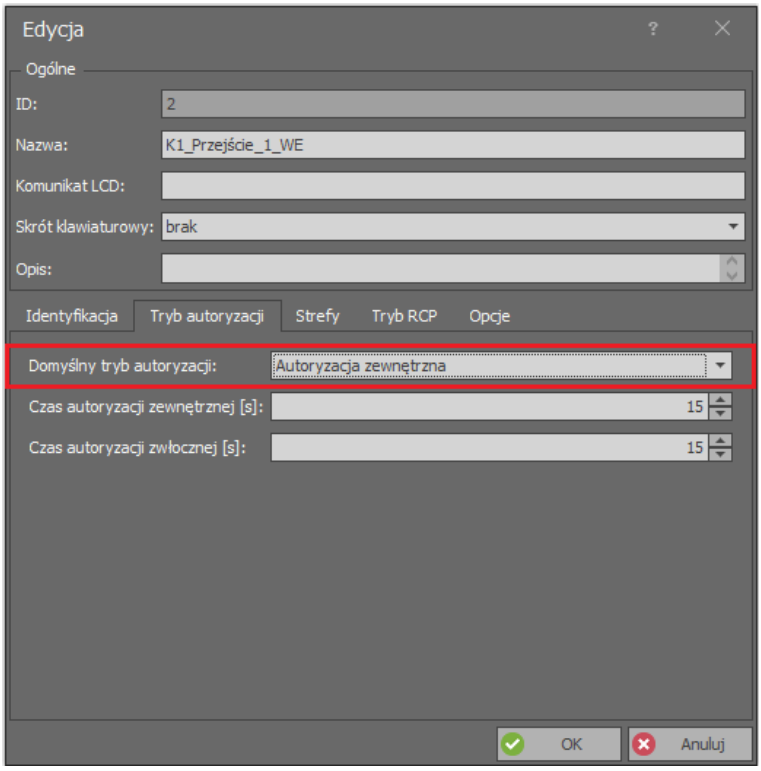
Konfiguracja Przejścia i Punktów identyfikacji

Aby skonfigurować Przejście zgodnie z podanym wcześniej rysunkiem:

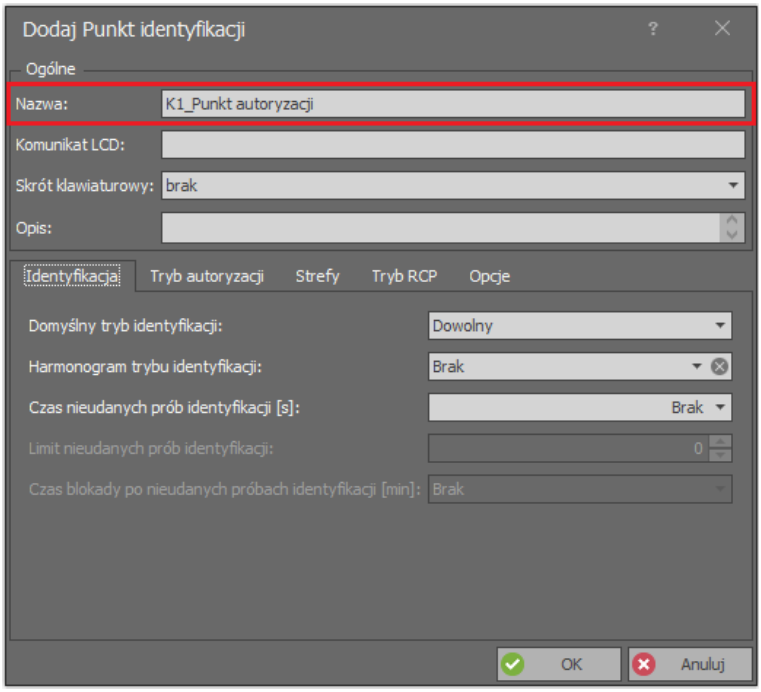
- W menu górnym programu VISO wybierz *Kreatory* i następnie *Kreator Przejścia*.
- Zdefiniuj przejście dwustronne z przykładowymi czytnikami ID=105 i ID=106 tak jak w nocie aplikacyjnej AN006.
- Dodaj użytkownika za pomocą kreatora Dodaj Osobę online przypisując mu Uprawnienia do Przejścia oraz kartę i/lub PIN.



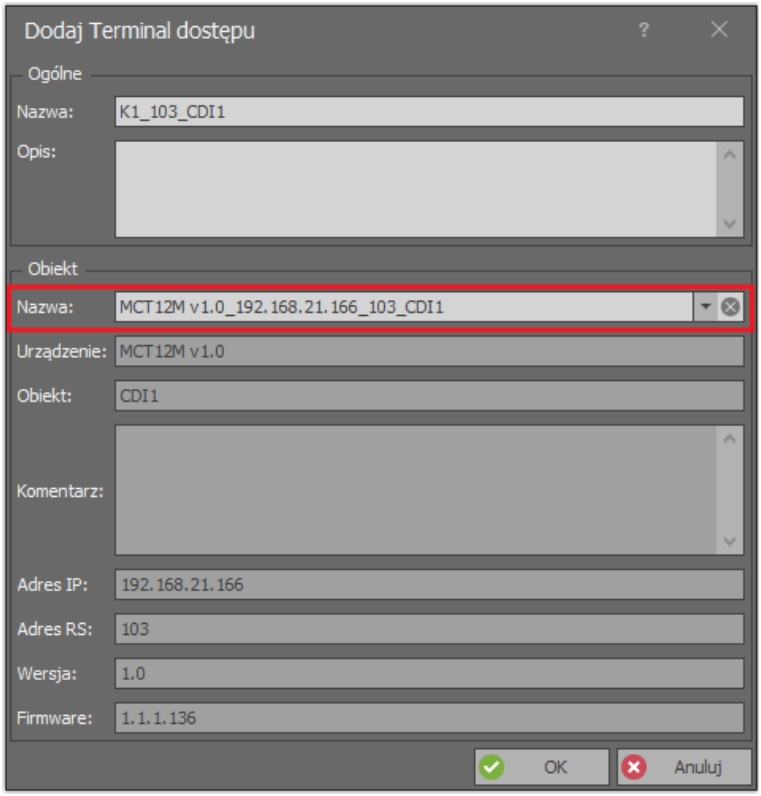
- Po zakończeniu pracy kreatora, rozwiń kontroler w drzewku nawigacyjnym programu VISO i dwukrotnie kliknij polecenie *Punkty identyfikacji*.
- W otwartym oknie wskaż utworzony kreatorem Punkt identyfikacji *K1_Przejście_1_WE* z czytnikiem ID=105 i następnie wybierz *Edytuj*.
- W otwartym oknie w zakładce *Tryb autoryzacji* w zależności od potrzeb wybierz *Autoryzacja zewnętrzna* lub *Autoryzacja zwłoczna*. Opcjonalnie za pomocą dostępnych parametrów można zmienić domyślne czasy oczekiwania dla obu autoryzacji. Zamknij okno przyciskiem *OK*.



- W oknie Punktów identyfikacji wybierz *Dodaj* by utworzyć kolejny Punkt identyfikacji tym razem do autoryzacji przyznania dostępu na Przejściu. Nadaj nazwę punktowi i zamknij okno przyciskiem *OK*.



- Dla utworzonego punktu, w dolnej części ekranu wybierz zakładkę *Terminale dostępu*, następnie *Dodaj* i w otwartym oknie wskaż przykładowy czytnik ID=103. Zamknij okno przyciskiem *OK*.



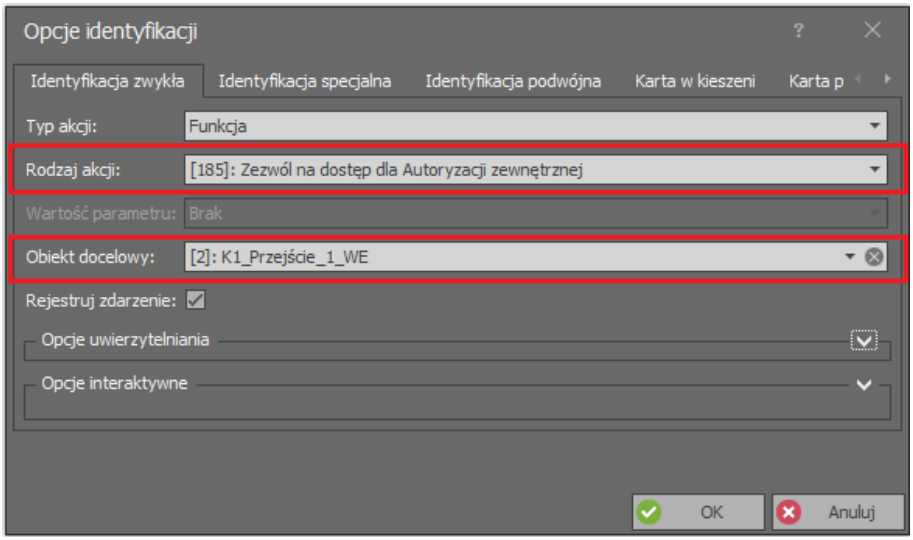
Autoryzacja dostępu za pomocą urządzenia

Istnieje kilka metod zatwierdzania bądź blokowania żądania przyznania dostępu dla użytkownika identyfikującego się na Punkcie identyfikacji. Do tego celu można wykorzystać odczyt karty na czytniku, wprowadzenie kodu PIN na klawiaturze czytnika, wciśnięcie przycisku podłączonego do linii wejściowej

kontrolera/czytnika/ekspandera lub użycie klawisza funkcyjnego na klawiaturze czytnika. W przypadku użycia przycisku lub klawisza funkcyjnego można ustawić wymóg identyfikacji (karta, PIN) użytkownika zatwierdzającego w celu weryfikacji jego Uprawnień do autoryzacji.

Autoryzacja Nośnikiem (karta, PIN)

- W oknie Punktów identyfikacji wskaż *K1_Punkt autoryzacji* czyli Punkt identyfikacji z czytnikiem ID=103 gdzie dostęp ma być autoryzowany.
- W dolnej części ekranu wybierz zakładkę *Opcje identyfikacji* i następnie *Edytuj*.
- W zależności od ustawionego wcześniej Trybu autoryzacji, w otwartym oknie ustaw funkcję *[185]: Zezwól na dostęp dla Autoryzacji zewnętrznej* lub funkcję *[186]: Odmowa dostępu dla Autoryzacji zwłocznej*.
- W polu *Obiekt docelowy* wskaż *K1_Przejście_1_WE* czyli Punkt identyfikacji z czytnikiem ID=105 gdzie ma być generowane żądanie autoryzacji dostępu.



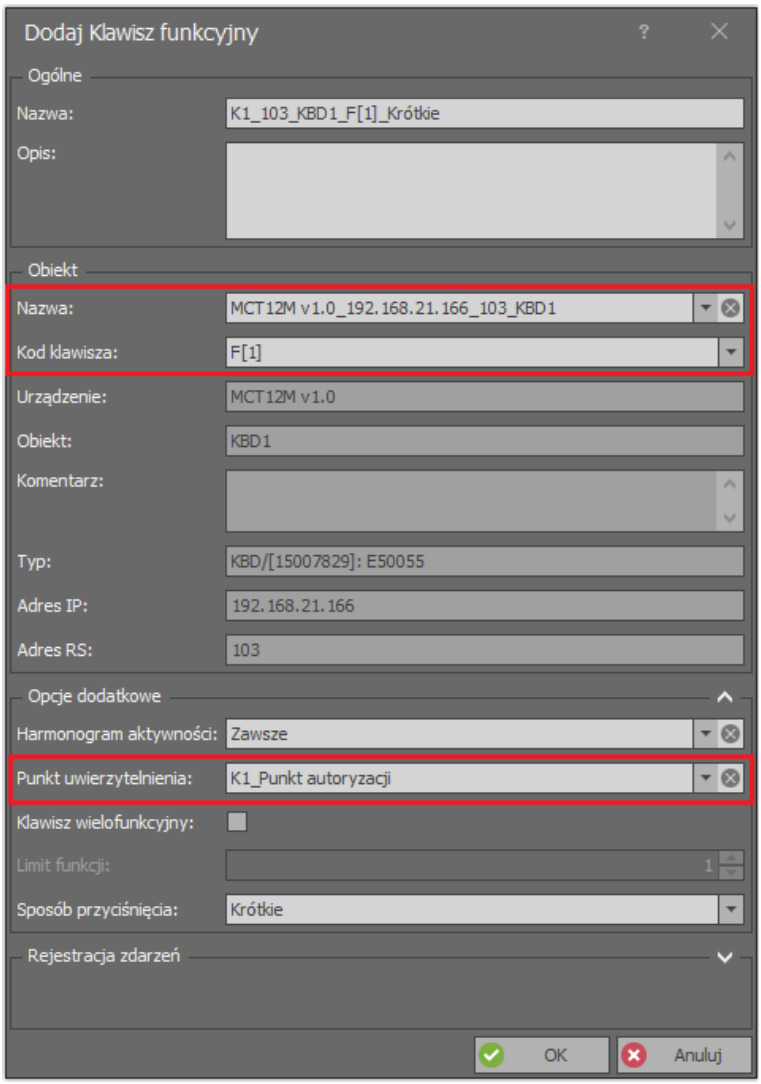
Autoryzacja klawiszem funkcyjnym bez weryfikacji

- W oknie Punktów identyfikacji wskaż *K1_Przejście_1_WE* czyli Punkt identyfikacji z czytnikiem ID=105 gdzie ma być generowane żądanie autoryzacji dostępu.
- W dolnej części ekranu wybierz zakładkę *Klawisze funkcyjne* i następnie *Dodaj*.
- W otwartym oknie wybierz przycisk  po to by wskazać lokalizację klawisza funkcyjnego.
- W kolejnym oknie w polu *Nazwa* obszaru *Obiekt* wskaż terminal z klawiszami funkcyjnymi (ID=103), następnie wskaż kod klawisza np. F1 i zamknij okno przyciskiem *OK*.
- W zależności od ustawionego wcześniej Trybu autoryzacji, w otwartym oknie ustaw funkcję *[185]: Zezwól na dostęp dla Autoryzacji zewnętrznej* lub funkcję *[186]: Odmowa dostępu dla Autoryzacji zwłocznej*. Zamknij okno przyciskiem *OK*.
- Prześlij ustawienia do kontrolera.

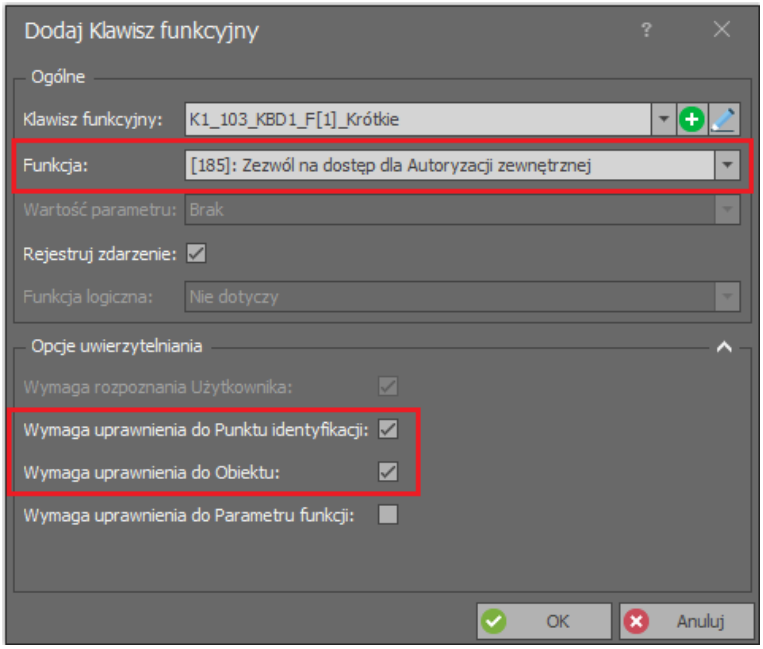
Analogicznie można zdefiniować linię wejściową do autoryzacji wybierając zakładkę *Linie wejściowe*.

Autoryzacja klawiszem funkcyjnym z weryfikacją

- W oknie Punktów identyfikacji wskaż *K1_Przejście_1_WE* czyli Punkt identyfikacji z czytnikiem ID=105 gdzie ma być generowane żądanie autoryzacji dostępu.
- W dolnej części ekranu wybierz zakładkę *Klawisze funkcyjne* i następnie *Dodaj*.
- W otwartym oknie wybierz przycisk  po to by wskazać lokalizację klawisza funkcyjnego.
- W kolejnym oknie w polu *Nazwa* obszaru *Obiekt* wskaż terminal z klawiszami funkcyjnymi (ID=103) i następnie wskaż kod klawisza np. F1.
- W tym samym oknie rozwiń obszar *Opcje dodatkowe* i w polu *Punkt uwierzytelniania* wskaż Punkt identyfikacji, na którym ma być weryfikowane użycie klawisza funkcyjnego. Może to być Punkt identyfikacji z czytnikiem na którym zdefiniowany został klawisz funkcyjny lub dowolny inny Punkt identyfikacji z czytnikiem w ramach tego samego kontrolera MC16. Zamknij okno przyciskiem *OK*.



- W zależności od ustawionego wcześniej Trybu autoryzacji, w otwartym oknie ustaw funkcję *[185]: Zezwól na dostęp dla Autoryzacji zewnętrznej* lub funkcję *[186]: Odmowa dostępu dla Autoryzacji zwłocznej*. Dodatkowo zaznacz *Wymaga uprawnienia do Punktu identyfikacji* i *Wymaga uprawnienia do Obiektu* w *Opcjach uwierzytelniania*. Zamknij okno przyciskiem *OK*.

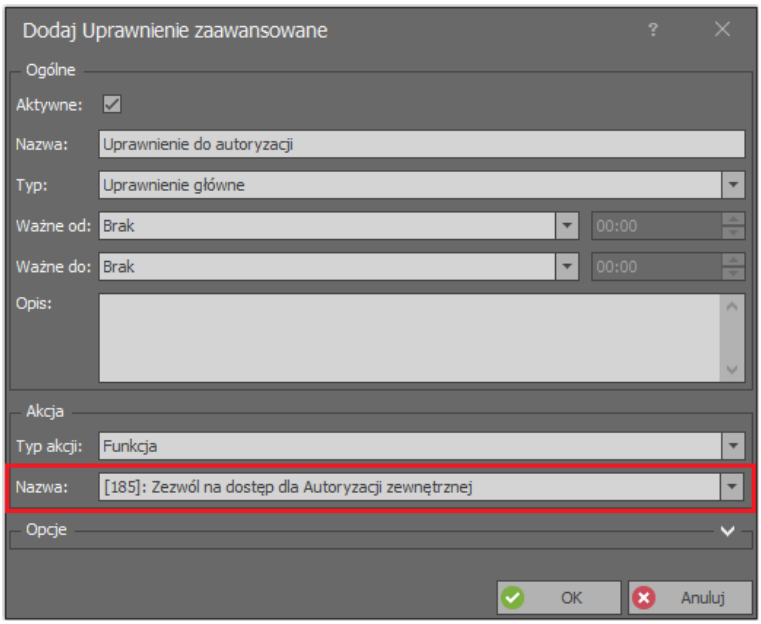


Analogicznie można zdefiniować linię wejściową do autoryzacji wybierając zakładkę *Linie wejściowe*.

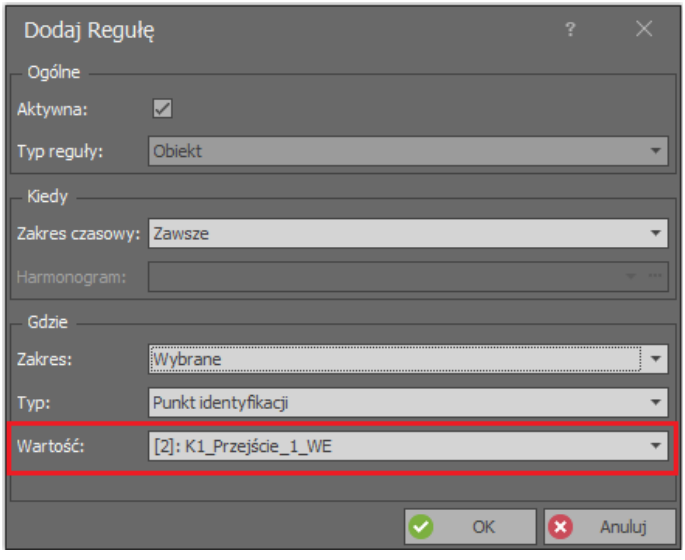
Uprawnienie do autoryzacji

W przypadku autoryzacji Nośnikiem jak też autoryzacji klawiszem funkcyjnym z weryfikacją czy linią wejściową z weryfikacją konieczne jest zdefiniowanie Uprawnienia dla użytkownika, który będzie dokonywał autoryzacji czyli Uprawnienia zaawansowanego do funkcji *[185]* lub *[186]* w zależności od stosowanego Trybu autoryzacji. Aby zdefiniować takie Uprawnienie:

- W drzewku nawigacyjnym programu VISO rozwiń pole *Uprawnienia,* dwukrotnie kliknij polecenie *Uprawnienia zaawansowane* i w otwartym oknie wybierz *Dodaj*.



- W zależności od ustawionego wcześniej Trybu autoryzacji, w otwartym oknie ustaw funkcję *[185]: Zezwól na dostęp dla Autoryzacji zewnętrznej* lub funkcję *[186]: Odmowa dostępu dla Autoryzacji zwłocznej*. Zamknij okno przyciskiem *OK*.
- W dolnej części ekranu wybierz zakładkę *Reguły zezwalające* i następnie przycisk *Dodaj*.
- W otwartym oknie opcjonalnie wybierz *Wybrane* jako *Zakres czasowy* jeżeli Uprawnienie ma być ograniczone czasowo harmonogramem. Własny harmonogram okresowy można utworzyć poleceniem *Harmonogramy* w drzewku nawigacyjnym programu VISO.
- W tym samym oknie wybierz *Wybrane* jako *Zakres* i następnie wskaż Punkt identyfikacji dla którego docelowo ma być realizowana autoryzacja czyli przykładowy *K1_Przejście_1_WE* z czytnikiem ID=105.



- Prześlij ustawienia do kontrolera.
- Przypisz nowe uprawnienie użytkownikowi, który ma dokonywać autoryzacji uruchamiając kreator *Dodaj osobę online* lub *Edytuj osobę online* wybierając w menu górnym programu VISO polecenie *Kreatory*.

Więcej informacji na temat Uprawnień podano w nocie aplikacyjnej AN003 dostępnej na www.roger.pl.

Autoryzacja dostępu za pomocą oprogramowania VISO

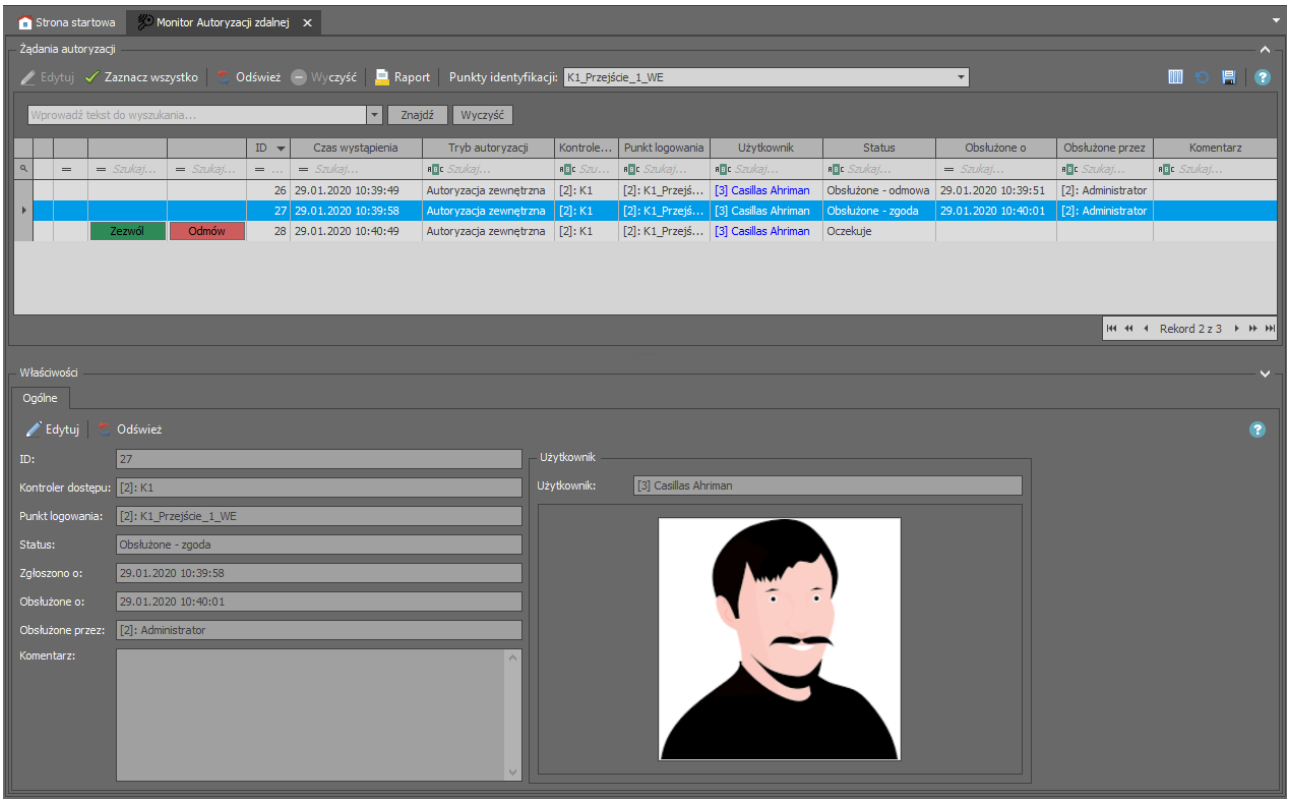
Oprogramowanie VISO umożliwia operatorowi zdalną autoryzację dostępu użytkownika na przejściu. W ramach autoryzacji można dodatkowo wykorzystywać kamery CCTV jeżeli są one zintegrowane z systemem RACS 5. Więcej informacji na temat takiej integracji podano w nocie aplikacyjnej AN007.

Monitor Autoryzacji zdalnej

Monitor Autoryzacji zdalnej jest dostępny w programie VISO po wybraniu w menu górnym *Autoryzacja zdalna* i następnie *Monitor Autoryzacji zdalnej*.

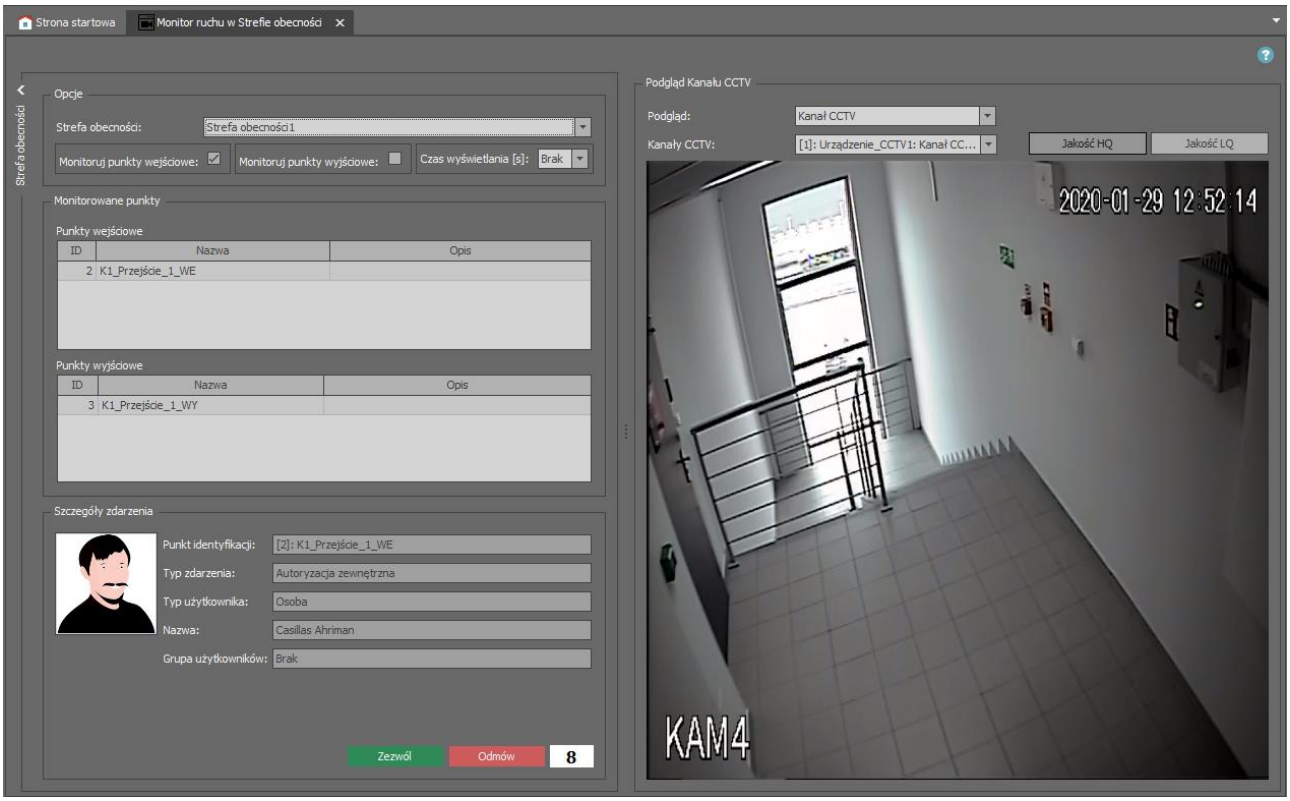
Monitor umożliwia:

- Wskazanie, które Punkty identyfikacji z trybami Autoryzacji zewnętrznej lub zwłocznej mają być w nim monitorowane.
- Zdalne zatwierdzanie lub odrzucanie żądania przyznania dostępu ze strony użytkownika.
- Wyświetlanie danych osoby zgłaszającej żądanie przyznania dostępu oraz zdjęcia jeżeli zostało one jej przypisane.
- Filtrowanie, sortowanie i czyszczenie listy żądań przyznania dostępu.



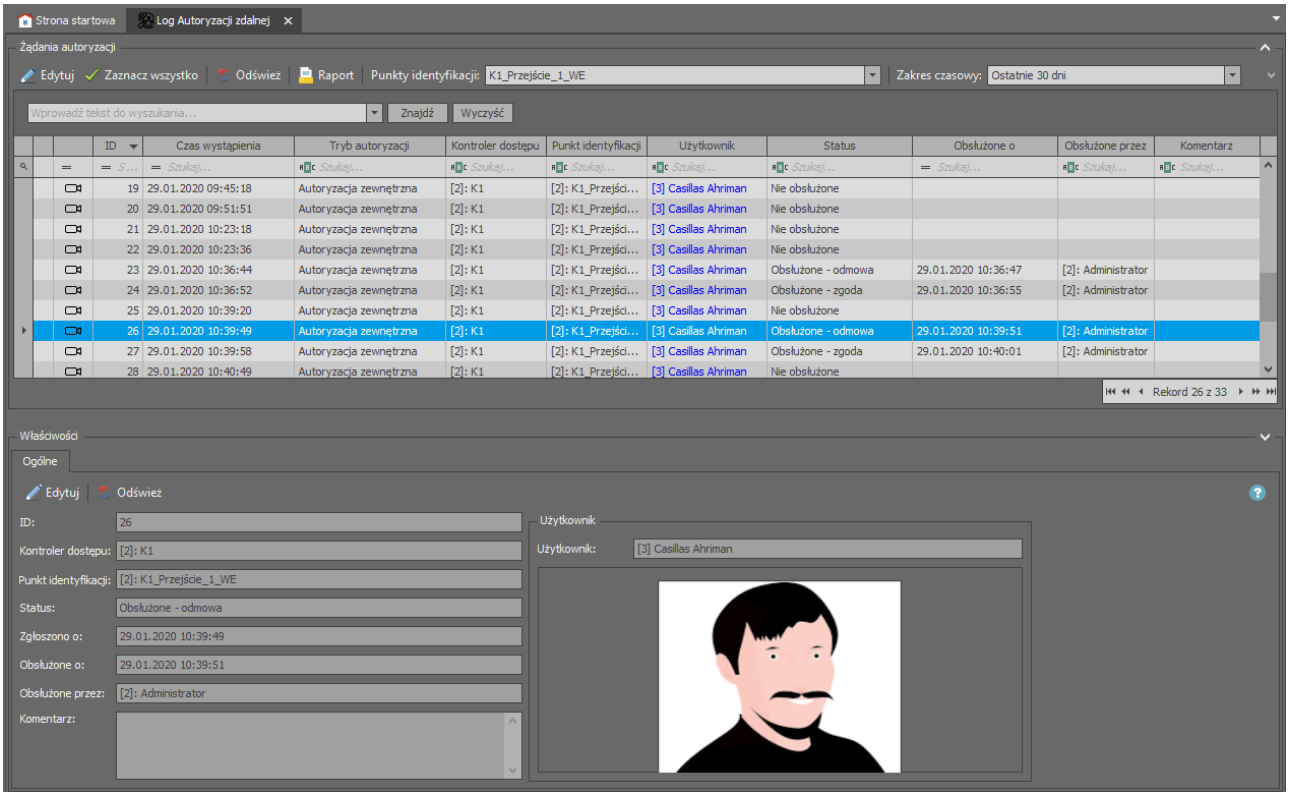
Monitor ruchu w Strefie obecności

Monitor ruchu w Strefie obecności, którego konfiguracja jest omówiona w nocie aplikacyjnej AN007 umożliwia monitorowanie osób identyfikujących się na wybranych Punktach identyfikacji. Monitor po odpowiednim skonfigurowaniu może wyświetlać dane i zdjęcie identyfikującej się osoby jak też obraz wideo z powiązanej z Punktem identyfikacji kamery CCTV. Gdy monitorowany Punkt identyfikacji ma ustawioną Autoryzację zewnętrzną lub zwłoczną to dodatkowo dostępne są przyciski do autoryzacji żądania przyznania dostępu przez operatora programu.



Log Autoryzacji zdalnej

Log Autoryzacji zdalnej jest dostępny w programie VISO po wybraniu w menu górnym *Autoryzacja zdalna* i następnie *Log Autoryzacji zdalnej*. Log zawiera zarejestrowane żądania przyznania dostępu wraz z informacjami na temat użytkowników i operatorów.



Operatorzy Autoryzacji zdalnej

System RACS 5 może być zarządzany wielostanowiskowo przez Operatorów z dostępem do różnych obszarów programu VISO. Możliwe jest więc zdefiniowanie Roli dla Operatora, która będzie dawała dostęp

jedynie do monitorów autoryzacji zdalnej. Więcej informacji na temat Operatorów i Ról podano w nocie aplikacyjnej AN040.

Przełączanie i sygnalizacja Trybów autoryzacji

Na poziomie Punktu identyfikacji możliwe jest ustawienie domyślnego Trybu autoryzacji. Istnieje również możliwość przełączania trybów za pomocą funkcji wejściowych *[177] – [184]*, które można wywoływać za pomocą odczytu karty, wprowadzenia kodu PIN, linii wejściowej lub klawisza funkcyjnego. Dodatkowo załączenie danego Trybu autoryzacji może być sygnalizowane za pomocą funkcji wyjściowych *[80] – [85]* a stan oczekiwania na autoryzację dla Autoryzacji zewnętrznej oraz zwłocznej może być sygnalizowany za pomocą funkcji wyjściowej *[86]*. Funkcję tą można przypisać do linii wyjściowej i w ten sposób sygnalizować użytkownikowi stan oczekiwania np. za pomocą wskaźników LED lub głośnika na czytniku jak też za pomocą zewnętrznego urządzenia sygnalizacyjnego podłączonego do linii wyjściowej.

Kontakt:
Roger sp. z o.o. sp.k.
82-400 Sztum
Gościszewo 59
Tel.: +48 55 272 0132
Faks: +48 55 272 0133
Pomoc tech.: +48 55 267 0126
Pomoc tech. (GSM): +48 664 294 087
E-mail: pomoc.techniczna@roger.pl
Web: www.roger.pl