Roger Access Control System 5v2

Nota aplikacyjna nr 003

Wersja dokumentu: Rev. A

Uprawnienia

Uwaga: Niniejszy dokument dotyczy RACS 5 v2.0.4 lub nowszy

Wprowadzenie

W systemie RACS 5 wykonanie danej akcji przez użytkownika systemu, może być uwarunkowane posiadaniem przez niego odpowiedniego Uprawnienia definiowanego dla konkretnej funkcji (np. żądanie przyznania dostępu). Możliwe jest definiowanie Uprawnień podstawowych, które dotyczą grup funkcji np. z zakresu dostępu, automatyki, przezbrajania, itd. jak też definiowanie Uprawnień zaawansowanych, w przypadku których wskazywana jest konkretna funkcja oraz reguły zezwalające i blokujące. Dodatkowo same Uprawnienia mogą być grupowane po to by ułatwić zarządzanie typowymi Uprawnieniami użytkowników (np. prawa dostępu na głównych przejściach w budynku).

Uprawnienia mogą być przypisywane:

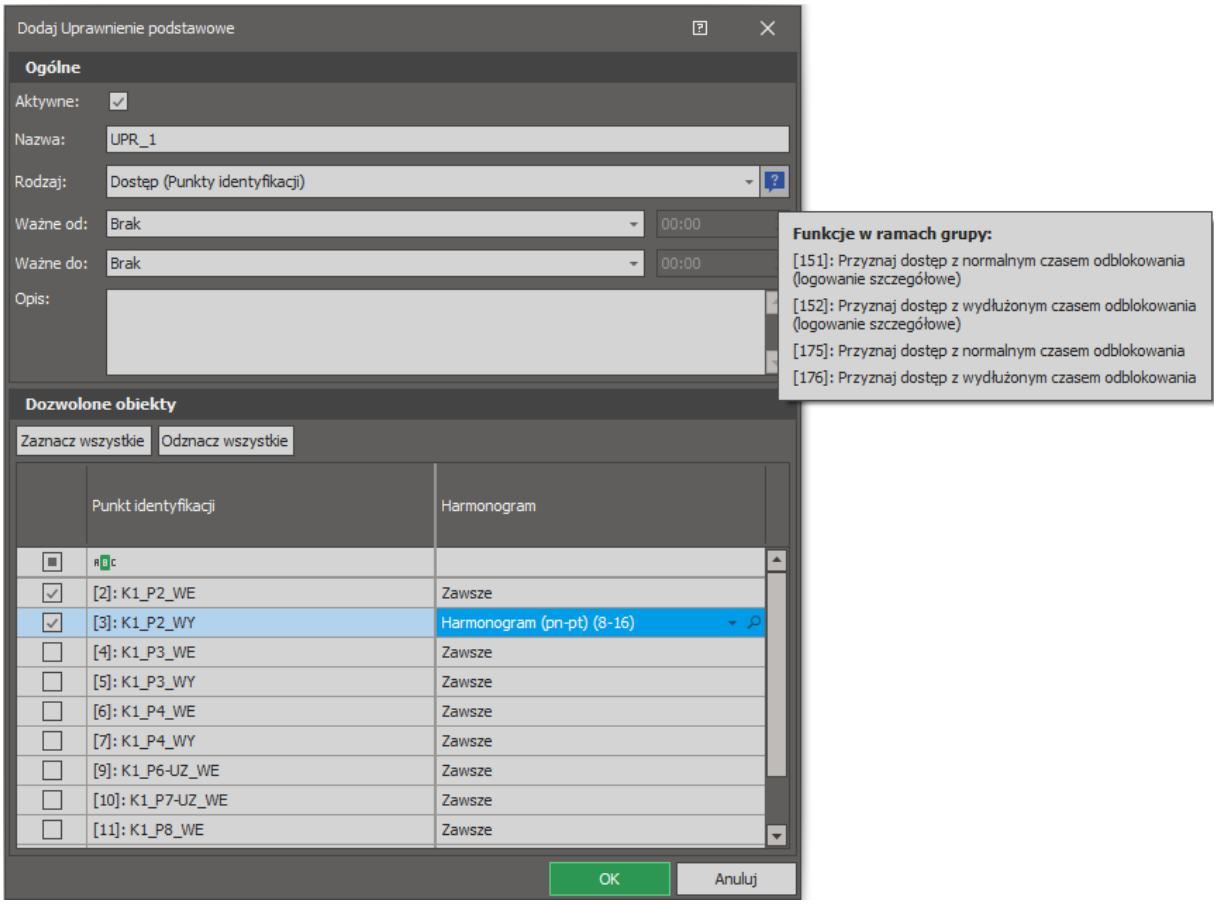
- Użytkownikom (Osobom, Gościom i Wyposażeniu)
- Identyfikatorom użytkowników
- Grupom użytkowników

Uprawnienia danego użytkownika są sumą Uprawnień przypisanych na różnych poziomach (samego użytkownika, jego grupy i Identyfikatora).

Uprawnienia podstawowe

W systemie RACS 5 możliwe jest definiowanie Uprawnień podstawowych, które obejmują grupy typowych funkcji np. w zakresie dostępu, przezbrajania, automatyki, itd. Celem wprowadzenia Uprawnień podstawowych jest ułatwienie definiowania i stosowania typowych uprawnień systemu kontroli dostępu. Aby zdefiniować Uprawnienie podstawowe:

- W drzewku nawigacyjnym programu VISO rozwiń *Uprawnienia* i dwukrotnie kliknij *Uprawnienia podstawowe*.
- W otwartym oknie wybierz *Dodaj*.
- W kolejnym oknie wybierz *Rodzaj*. Po wskazaniu ikony znaku zapytania jak na rysunku poniżej możliwe jest uzyskanie informacji na temat tego jakie funkcje wchodzą w skład danego rodzaju.
- W dolnej części ekranu wskaż elementy, których Uprawnienie ma dotyczyć np. Punkty identyfikacji w przypadku Uprawnienia rodzaju *Dostęp (Punkty identyfikacji)* i opcjonalnie przypisz Harmonogramy, które definiuje się po wybraniu polecenia *Harmonogramy* w drzewku nawigacyjnym programu VISO. Harmonogramy pozwalają ograniczyć Uprawnienie czasowo.



Uprawnienia podstawowe rodzaju *Dostęp (punkty identyfikacji)* są domyślnie tworzone gdy konfigurowane jest Przejście za pomocą *Kreatora Przejścia* tak jak to opisano w nocie aplikacyjnej AN006.

Uprawnienia zaawansowane

W przypadku Uprawnień zaawansowanych zakres możliwych ustawień jest dużo szerszy niż w przypadku Uprawnień podstawowych i obejmuje on wszystkie dostępne funkcje, opcje autoryzacji, reguły zezwalające i blokujące wraz z regułami szczegółowymi. Celem wprowadzenia Uprawnień zaawansowanych jest umożliwienie definiowania uprawnień w zależności od szczególnych wymagań danej instalacji. W danym systemie RACS 5 można definiować i stosować oba typy uprawnień tj. podstawowe i zaawansowane.

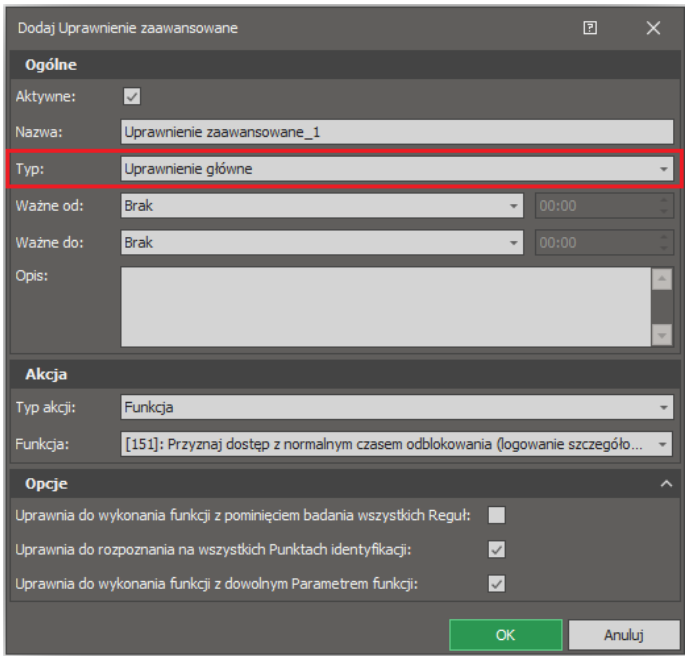
Typy Uprawnień zaawansowanych

Uprawnienia zaawansowane mogą być typu Głównego lub Uzupełniającego.

- Uprawnienie główne składa się ze wszystkich, wymaganych dla danej funkcji Reguł szczegółowych i samodzielnie może rozstrzygać o możliwości wykonania lub niewykonania funkcji.
- Uprawnienie uzupełniające składa się z Reguł szczegółowych odnoszących się do miejsca rozpoznania użytkownika i parametru funkcji. Uprawnienie samodzielnie nie może rozstrzygać o możliwości wykonania lub niewykonania funkcji.

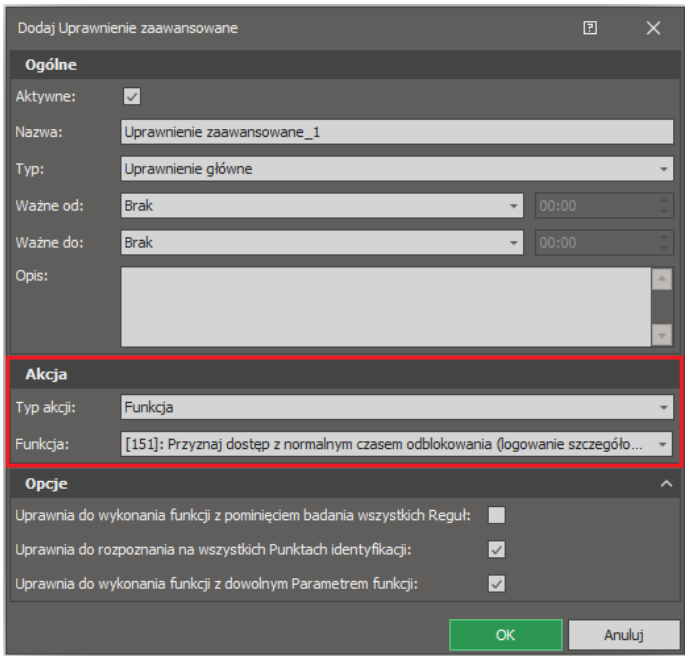
W Uprawnieniach uzupełniających definiowane są wyłącznie Reguły zezwalające. Reguły zezwalające znajdujące się w Uprawnieniach uzupełniających dodają się do Reguł zezwalających znajdujących się w Uprawnieniach głównych. Jeśli w trakcie analizy Uprawnienia głównego okaże się, że brakuje jakiejś zezwalającej Reguły szczegółowej to kontroler może ją pobrać z Uprawnienia uzupełniającego. Powszechnie stosowane są Uprawnienia główne, natomiast Uprawnienia

uzupełniające znajdują swoje zastosowanie w specyficznych scenariuszach obsługi kontroli dostępu w windach oraz szafkach.



Akcja

Uprawnienie zaawansowane odnosi się do wybranej funkcji lub grupy funkcji (jak w Uprawnieniach podstawowych). Możliwe jest więc definiowanie uprawnień do szeregu działań realizowanych w systemie RACS 5 takich jak na przykład przyznanie dostępu, odblokowanie przejścia, przezbrajanie strefy alarmowej, ustawiania trybu RCP, obsługi węzła(-ów) automatyki, rejestracji zdarzeń, itd.

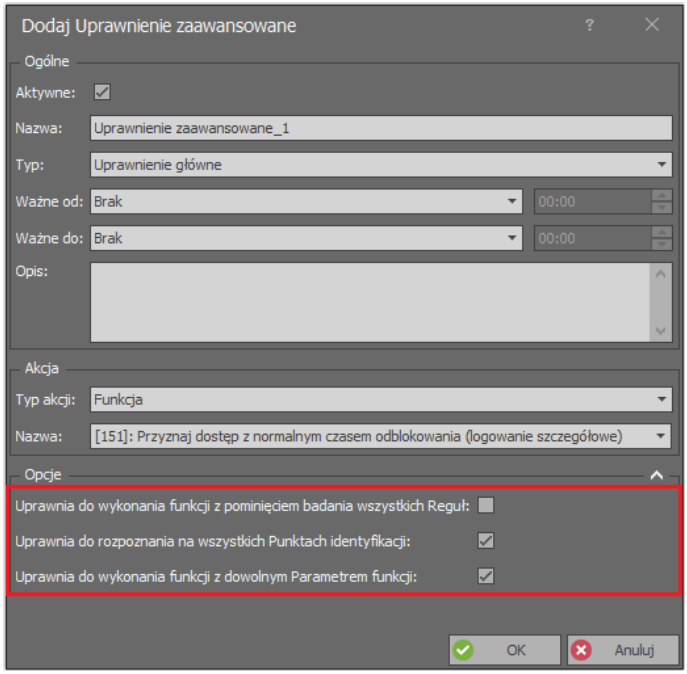


Opcje

Definicja Uprawnienia zaawansowanego zawiera trzy opcje, których zadaniem jest uproszczenie procesu definiowania Uprawnień w przypadku, gdy wyższy poziom szczegółowości nie jest wymagany.

- Gdy opcja *Uprawnia do wykonania funkcji z pominięciem badania wszystkich Reguł* jest załączona, kontroler uznaje, że posiadacz tego Uprawnienia posiada komplet Reguł szczegółowych wymaganych do wykonania danej funkcji w dowolnym miejscu i czasie.
- Gdy opcja *Uprawnia do rozpoznania na wszystkich Punktach identyfikacji* jest załączona, kontroler uznaje, że posiadacz tego Uprawnienia może dokonać rozpoznania na dowolnym Punkcie identyfikacji i pomija sprawdzanie reguł określających miejsce rozpoznania użytkownika.
- Gdy opcja *Uprawnia do wykonania funkcji z dowolnym Parametrem funkcji* jest załączona, użytkownik posiadający to Uprawnienie może wykonać funkcję z dowolnym Parametrem funkcji i pomija sprawdzanie reguły określającej dozwolone Parametry funkcji.

Domyślnie, nowotworzone *Uprawnienie* ma załączoną opcję *Uprawnia do rozpoznania na wszystkich Punktach identyfikacji* i ewentualnie opcję *Uprawnia do wykonania funkcji z dowolnym Parametrem funkcji*, co powoduje, że w dalszych krokach konfiguracji Uprawnienia wymagane jest tylko zdefiniowanie Reguły szczegółowej określającej obiekt, którego funkcja dotyczy. W przypadku funkcji *[151]: Przyznaj dostęp z normalnym czasem odblokowania (logowanie szczegółowe)* tym obiektem jest Punkt identyfikacji lub Strefa dostępu gdzie dostęp ma być przyznawany.



Reguły zezwalające oraz Reguły blokujące

W skład Uprawnienia wchodzą Reguły zezwalające oraz Reguły blokujące. Reguły zezwalające określają warunki gdy dana funkcja może być wykonana, natomiast Reguły blokujące określają warunki gdy dana funkcja nie może być wykonana. Reguły blokujące mają wyższy priorytet niż Reguły zezwalające. Zachodzi zależność, że jeśli przynajmniej w jednym z Uprawnień, które posiada użytkownik systemu, występuje przynajmniej jedna spełniona w danych warunkach Reguła blokująca, to funkcja nie może być wykonana. Gdy to nie zachodzi, następuje sprawdzenie czy przynajmniej w jednym z Uprawnień posiadanych przez użytkownika istnieje przynajmniej jedna Reguła zezwalająca, która w danych warunkach jest spełniona. Jeśli to zachodzi to funkcja może być wykonana.

Reguły szczegółowe

Zarówno Reguły blokujące jak i Reguły zezwalające składają się z Reguł szczegółowych, które określają:

- Obiekt
- Punkt identyfikacji

- Parametr funkcji

W Regule zezwalającej/blokującej może istnieć wiele Reguł szczegółowych tego samego typu. Reguły szczegółowe tego samego typu ulegają sumowaniu.

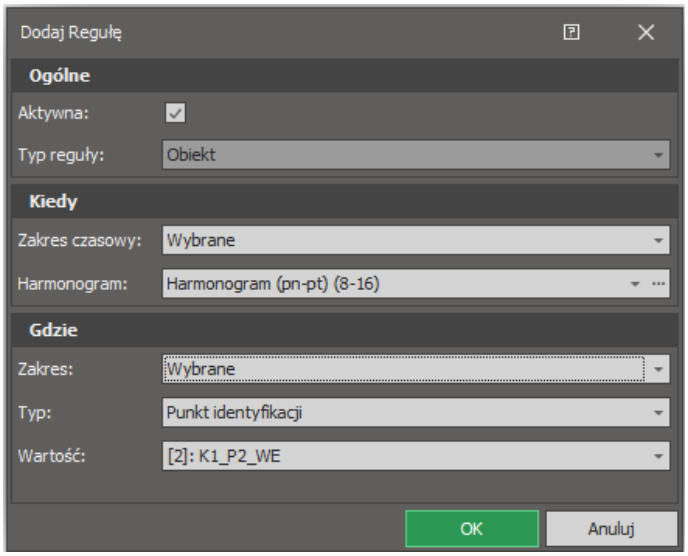
Reguła zezwalająca/blokująca jest spełniona, gdy w danym momencie zawiera przynajmniej po jednej z wymaganych Reguł szczegółowych. Proces analizy Reguły polega na sprawdzeniu czy:

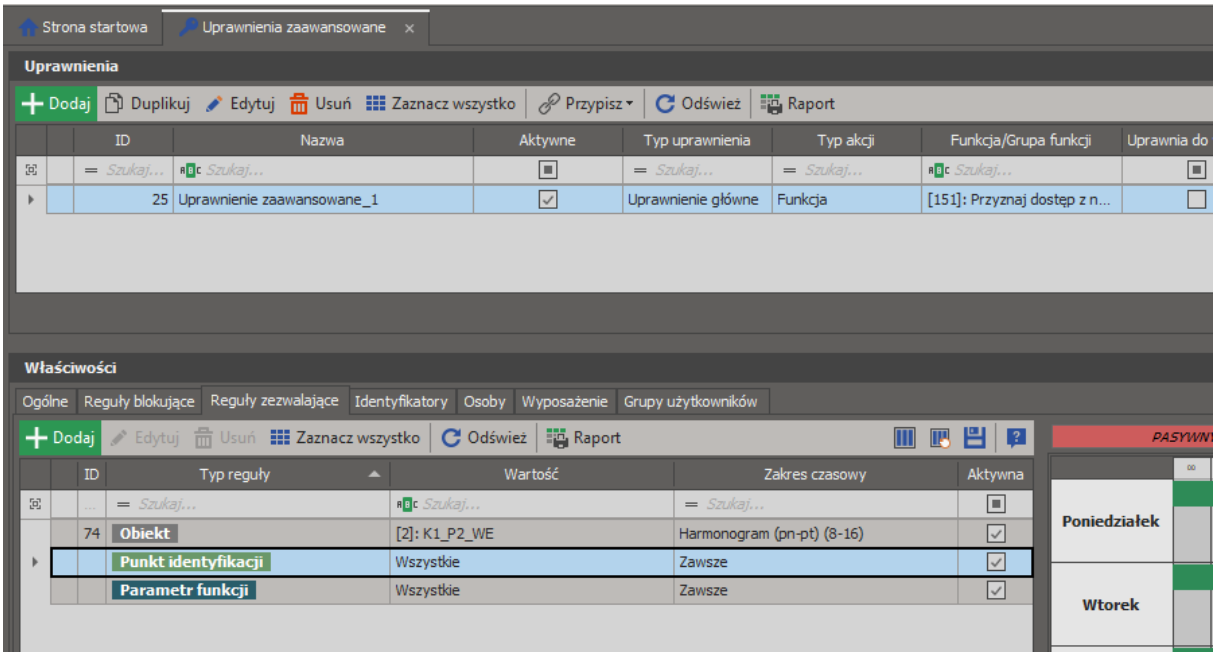
- użytkownik jest uprawniony aby dokonać rozpoznania na danym Punkcie identyfikacji
- użytkownik jest uprawniony aby wykonać funkcję na danym Obiekcie
- użytkownik jest uprawniony aby wykonać funkcję z danym Parametrem funkcji

Sprawdzanie reguły typu Miejsce rozpoznania użytkownika można wyłączyć załączając opcję *Uprawnia do rozpoznania na wszystkich Punktach identyfikacji.*

Sprawdzanie reguły typu Parametr funkcji można wyłączyć załączając opcję *Uprawnia do wykonania funkcji z dowolnym Parametrem funkcji*.

Każda Reguła szczegółowa dodatkowo może mieć przypisany zakres czasowy (Harmonogram), który określa, kiedy jest ona ważna. Harmonogramy definiuje się za pomocą polecenia *Harmonogramy* w drzewku nawigacyjnym programu VISO.

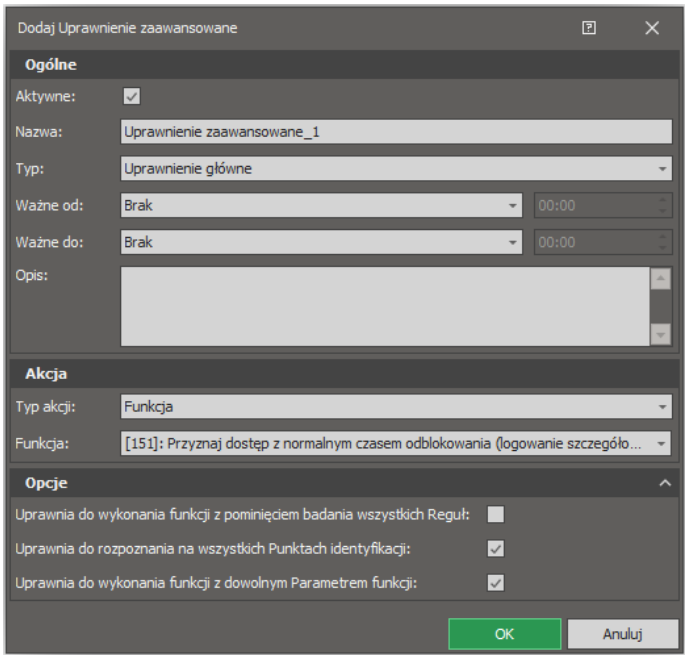




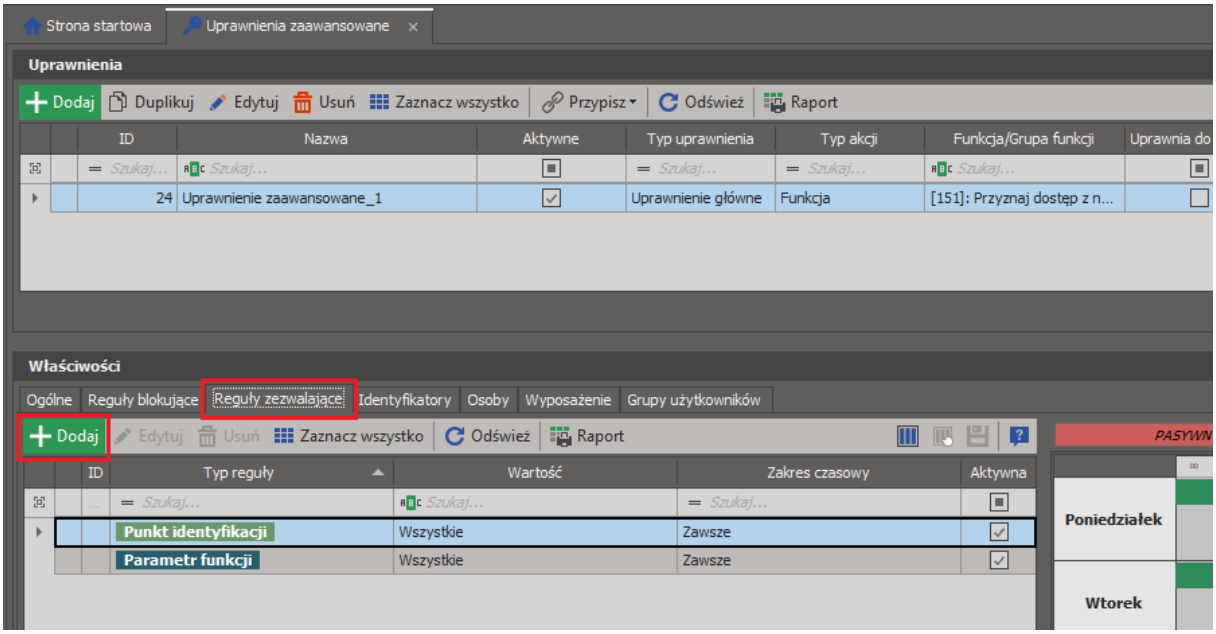
Typowa konfiguracja

Aby skonfigurować Uprawnienie zaawansowane w zakresie kontroli dostępu z wykorzystaniem typowej funkcji *[151]*:

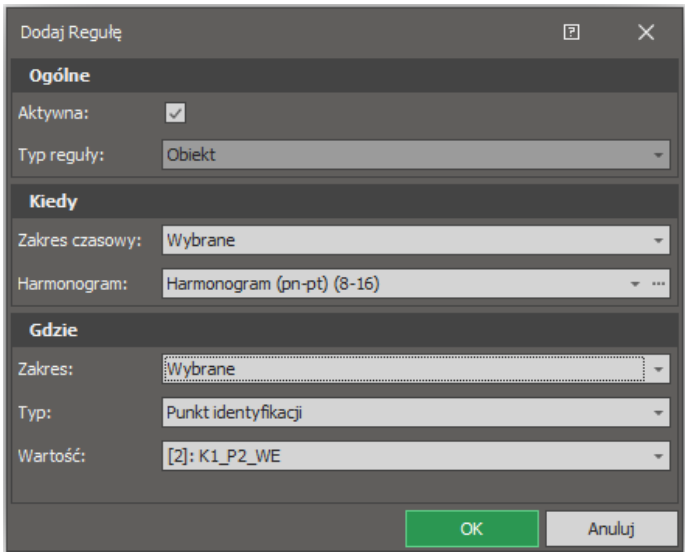
- W drzewku nawigacyjnym programu VISO rozwiń *Uprawnienia* i dwukrotnie kliknij *Uprawnienia zaawansowane*.
- W otwartym oknie wybierz *Dodaj*.
- Wybierz z listy funkcję *[151]: Przyznaj dostęp z normalnym czasem odblokowania (logowanie szczegółowe)* i zamknij okno przyciskiem *OK*.



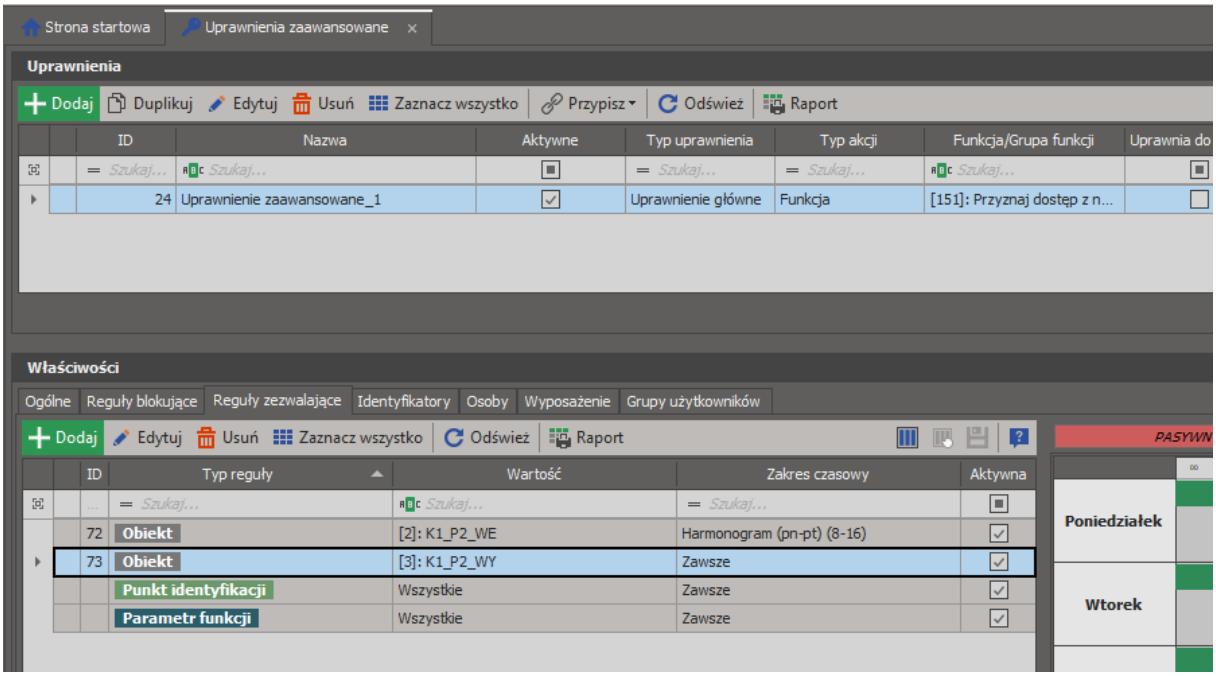
- Dla utworzonego Uprawnienia w dolnej części ekranu wybierz zakładkę *Reguły zezwalające* i następnie *Dodaj*.



- W kolejnym oknie wybierz typ *Obiekt*, opcjonalnie wskaż Harmonogram by ograniczyć regułę w czasie i następnie wybierz Punkt identyfikacji gdzie będzie można uzyskiwać dostęp na bazie tego Uprawnienia. Harmonogram musi być wcześniej zdefiniowany po wybraniu polecenia *Harmonogramy* w drzewku nawigacyjnym programu VISO.



- W razie potrzeby zdefiniuj kolejne Reguły zezwalające tak by Uprawnienie mogło dotyczyć większej ilości Punktów identyfikacji.



- Analogicznie zdefiniuj kolejne Uprawnienia tak by mogły one być przypisane bezpośrednio użytkownikom albo za pośrednictwem takich kreatorów jak *Dodaj Osobę online* oraz *Edytuj Osobę online*.

Grupy uprawnień

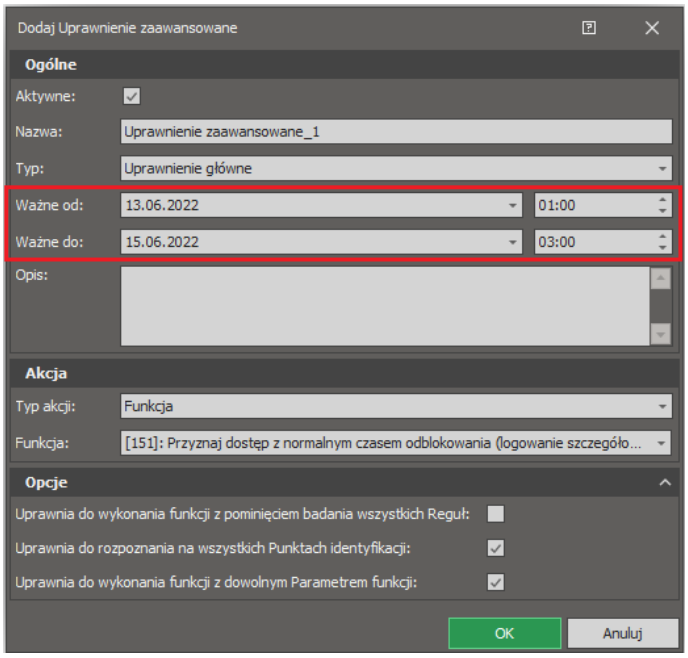
Program VISO umożliwia grupowanie Uprawnień po by ułatwić zarządzanie nimi. Jest to zwykle przydatne gdy na obiekcie zdefiniowane są Uprawnienia do przejść wspólnych oraz wejść głównych W takim układzie można je przypisać do grup(-y) i następnie przypisywać całe Grupy uprawnień do użytkowników. Grupy uprawnień można definiować po rozwinięciu *Uprawnienia* w drzewku nawigacyjnym programu VISO i następnie dwukrotnym kliknięciu *Grupy Uprawnień*.

Przypisywanie Uprawnień

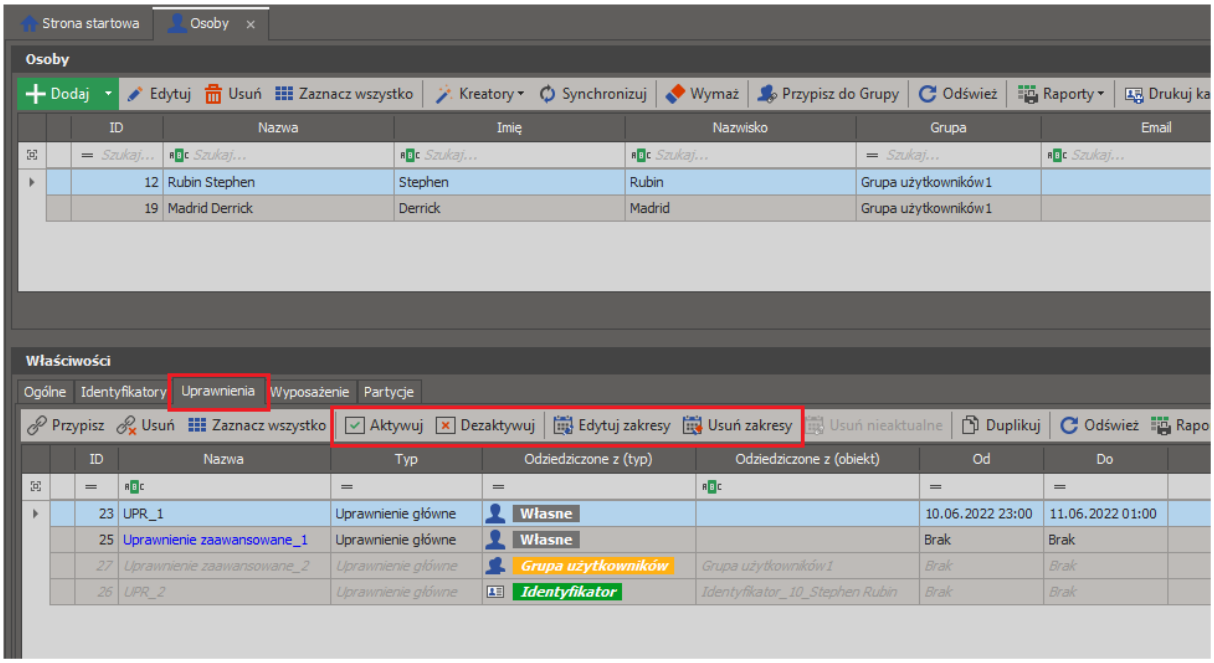
W systemie RACS 5, Uprawnienia mogą być przypisywane do Identyfikatorów, do Użytkowników oraz do Grup użytkowników. Zalecane jest przypisywanie Uprawnień za pomocą kreatorów *Dodaj Osobę online* oraz *Edytuj Osobę online*, które są dostępne po wybraniu *Kreatory* w menu górnym programu VISO. W procesie weryfikacji Uprawnienia do wykonania funkcji, kontroler sprawdza wszystkie Uprawnienia przypisane bezpośrednio do Identyfikatora za pomocą, którego użytkownik się zalogował, wszystkie Uprawnienia przypisane do użytkownika, który jest właścicielem Identyfikatora oraz wszystkie Uprawnienia przypisane do Grup użytkowników, do których dany użytkownik należy. Uprawnienia podlegają sumowania. Sumowanie dotyczy zarówno Reguł zezwalających jak i Reguł blokujących.

Czasowe ograniczanie uprawnień

Zgodnie z wcześniejszym opisem Reguły szczegółowe mogą ograniczać Uprawnienie na bazie Harmonogramów. Podczas definiowania Uprawnienia podstawowego jak też zaawansowanego możliwe jest również wskazanie zakresu czasowego, w którym Uprawnienie będzie w ogóle aktywne. Poza wskazanym okresem Uprawnienie nie będzie pozwalało w ogóle realizować swojej funkcji. Takie ograniczenie będzie jednak miało wpływ na wszystkich użytkowników, którym dane Uprawnienie zostało przypisane.



Dodatkowo możliwe jest również czasowe zarządzanie Uprawnieniami danej Osoby. W takim układzie modyfikacja Uprawnienia nie wpływa na inne Osoby z tym samym Uprawnieniem. Takie zarządzanie jest jednak możliwe jedynie w przypadku Uprawnień, które zostały przypisane bezpośrednio do Osoby a nie na poziomie Identyfikatora lub Grupy użytkowników. W tym samym oknie można również Uprawnienie aktywować i deaktywować dla danej Osoby. Okno do czasowego zarządzania Uprawnieniami jest dostępne po wybraniu *Konfiguracja* w menu górnym programu VISO, następnie *Osoby* i dla danej Osoby zakładki *Uprawnienia* w dolnej części ekranu.



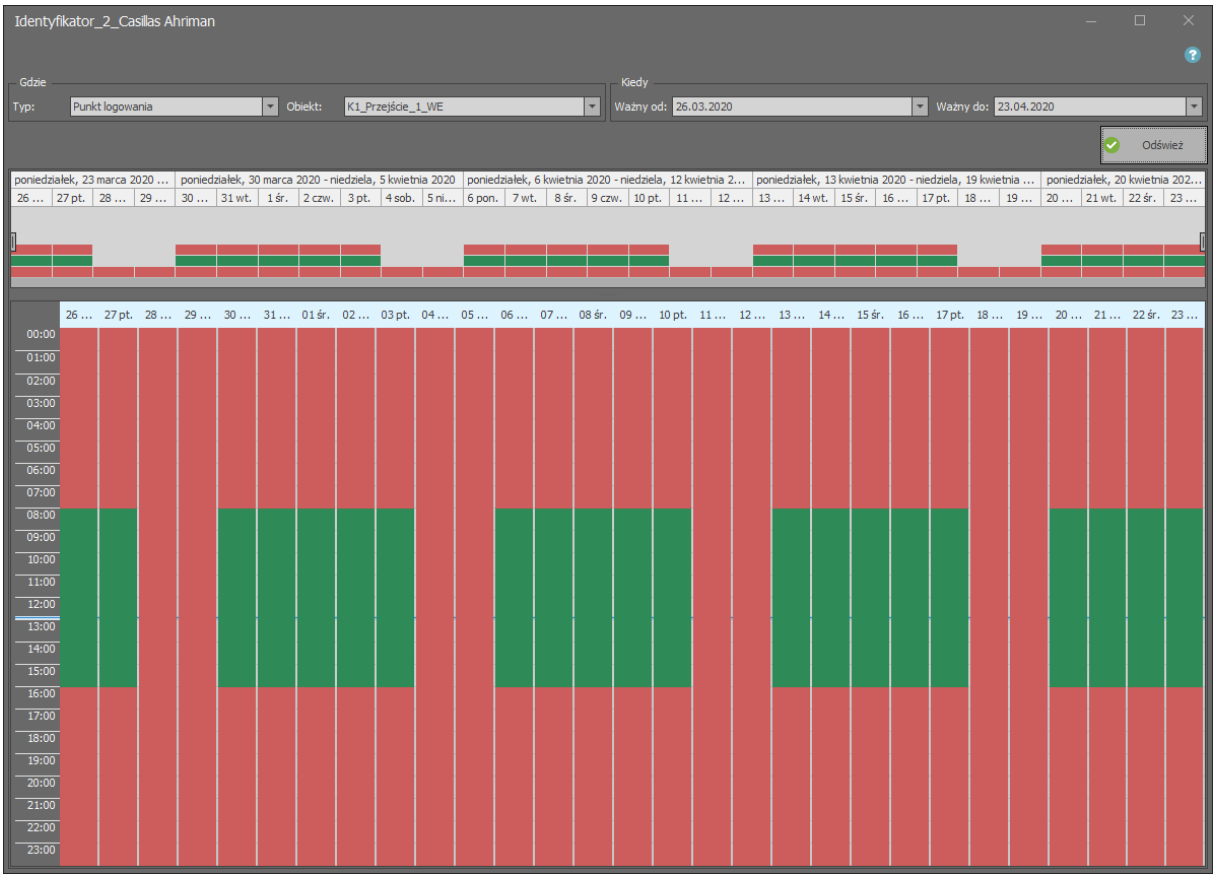
Diagnostyka Uprawnień użytkowników

Uprawnienia użytkowników mogą być definiowane na różnych poziomach, przez co ustalenie faktycznych wynikowych Uprawnień może nie zawsze być oczywiste. Uprawnienia użytkownika mogą wynikać z:

- Przypisania do Grupy użytkowników, która ma zdefiniowane Uprawnienia.
- Przypisania indywidualnych Uprawnień do Identyfikatora użytkownika.
- Przypisania Grup Uprawnień do Identyfikatora użytkownika.
- Przypisania indywidualnych Uprawnień do użytkownika.

Aby uzyskać informację na temat wynikowych Uprawnień dostępu użytkownika na danym Przejściu lub w danej strefie:

- W menu górnym programu VISO wybierz *Konfiguracja* i następnie *Identyfikatory*.
- W otwartym oknie dla Identyfikatora danego użytkownika wybierz *Schemat dostępu*.
- W kolejnym oknie wybierz Punkt identyfikacji albo Strefę dostępu, dla której wyświetlony ma być schemat i wybierz *Odśwież* by załadować dane.



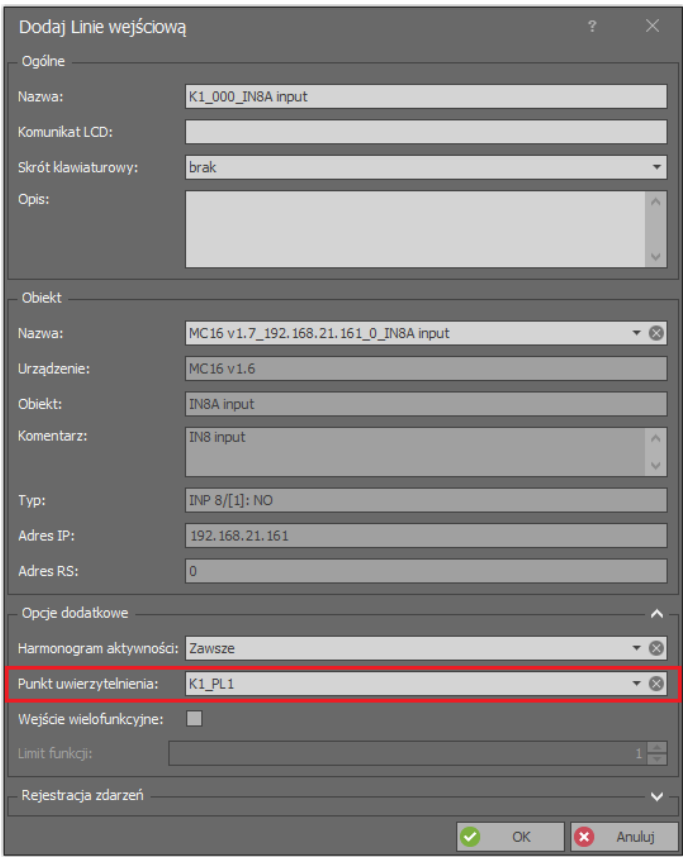
Aby uzyskać informację na temat tego kto ma prawa dostępu na danym Przejściu:

- W menu górnym programu VISO wybierz *Konfiguracja* i następnie *Przejścia*.
- W otwartym oknie rozwiń jeden z kontrolerów, wskaż dane Przejście i następnie wybierz przycisk *Użytkownicy* lub *Identyfikatory* w menu górnym tego okna.

Sposoby wywołania funkcji (źródła funkcji)

W ogólnym przypadku, funkcje wykonywane w systemie mogą być wywoływane na kilka sposobów, które dzieli się na osobowe i bezosobowe. Sposoby osobowe to takie, którym towarzyszy identyfikacja użytkownika, który wywołuje funkcję. Sposoby bezosobowe to takie, które nie są wywoływane przez użytkownika lub są wywoływane przez użytkownika, ale nie towarzyszy im identyfikacja. Typowym sposobem osobowym wywołania funkcji jest identyfikacja na terminalu dostępu (np. za pomocą karty) oraz zdalna komenda wydana przez operatora systemu. Typowym sposobem bezosobowym wywołania funkcji jest wyzwolenie linii wejściowej (bez uwierzytelniania), naciśnięcie klawisza funkcyjnego (bez uwierzytelniania) lub automatyczne uruchomienie funkcji z

poziomu harmonogramu czasowego. Uprawnienia mogą być sprawdzane wyłącznie wtedy, gdy funkcja jest wywoływana w sposób osobowy. W przypadku bezosobowego wywołania funkcji zwykle istnieje możliwość wskazania *Punktu uwierzytelniania*. W takiej sytuacji użycie linii wejściowej czy klawisza funkcyjnego podlegające autoryzacji staje się wywołaniem osobowym bo wymaga zatwierdzenia na danym Punkcie identyfikacji i jest możliwe jedynie w przypadku posiadania odpowiednich Uprawnień w zależności od ustawionych Opcji uwierzytelniania.



Opcje identyfikacji

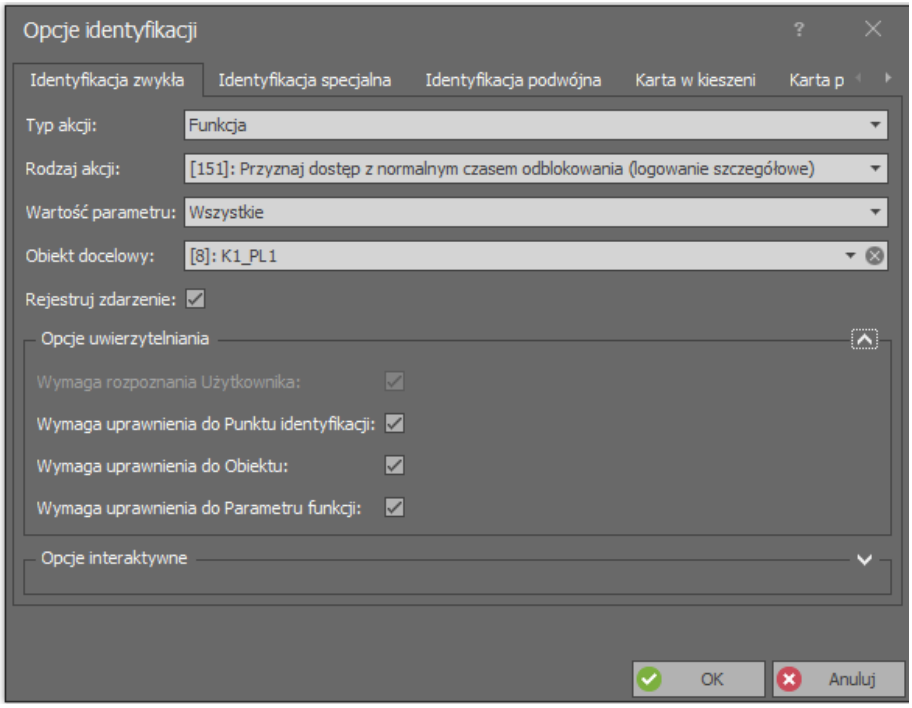
Przez termin identyfikacji w systemie RACS 5, rozumie się zestaw czynności, jakie użytkownik musi wykonać, aby system mógł go rozpoznać. W zależności od aktualnie obowiązującego na Punkcie identyfikacji sposobu rozpoznania zwanego Trybem identyfikacji, użytkownik musi użyć jednej lub więcej metod identyfikacji (karta, PIN, odcisk palca itd.)

Dodatkowo kontroler rozróżnia pięć Opcji identyfikacji na poziomie Punktu identyfikacji:

- Identyfikacja zwykła (np. jednokrotny odczyt karty)
- Identyfikacja specjalna (np. długi odczyt karty)
- Identyfikacja podwójna (np. dwukrotny odczyt karty)
- Karta w kieszeni (dotyczy terminali z kieszenią np. MCT82M-IO-CH)
- Karta poza kieszenią (dotyczy terminali z kieszenią np. MCT82M-IO-CH)

Każdemu ze sposobów identyfikacji można przypisać osobną Funkcję. Opcje identyfikacji są więc metodami wywołania funkcji (np. przyznania dostępu) a Uprawnienia pozwoleniami na ich wywołanie. Poszczególne Opcje identyfikacji mogą służyć nie tylko do wywoływania pojedynczych funkcji ale również wywoływania całych grup funkcji definiowanych za pomocą Komend lokalnych. W przypadku Komendy lokalnej sprawdzanie uprawnień jest wykonywane osobno dla każdej funkcji, co oznacza że gdy użytkownik wywoła Komendę lokalną nie posiadając Uprawnień do

wszystkich funkcji tej komendy to Komenda lokalna zostanie wywołana ale będzie ograniczona do funkcji dla których użytkownik posiada Uprawnienia.



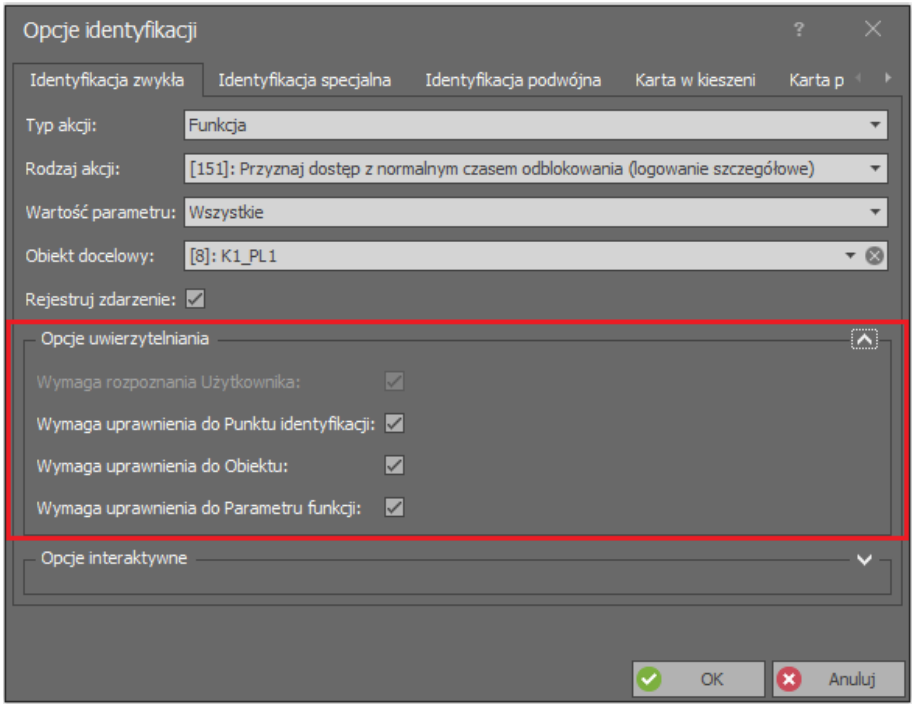
Opcje uwierzytelniania

Dla wywołań funkcji istnieje możliwość załączenia Opcji uwierzytelniania, które wymuszą wymóg identyfikacji użytkownika oraz określą zasady weryfikacji jego Uprawnień. Przykładowo gdy wszystkie Opcje uwierzytelniania są nieaktywne to do wywołania funkcji nie są potrzebne żadne Uprawnienia więc może ją wywoływać każdy użytkownik.

Opcje uwierzytelniania można definiować dla funkcji na poziomie:

- Punktu identyfikacji (dla każdej Opcji identyfikacji)
- Linii wejściowej
- Klawisza funkcyjnego
- Funkcji składowych Komendy lokalnej

W przypadku linii wejściowych i klawiszy funkcyjnych korzystanie z Opcji uwierzytelniania wymaga wskazania Punktu uwierzytelniania, na którym następować ma weryfikowanie Uprawnień.


Opcje identyfikacji
Identyfikacja zwykła
Identyfikacja specjalna
Identyfikacja podwójna
Karta w kieszeni
Karta p
Typ akcji:
Funkcja
Rodzaj akcji:
[151]: Przyznaj dostęp z normalnym czasem odblokowania (logowanie szczegółowe)
Wartość parametru:
Wszystkie
Obiekt docelowy:
[8]: K1_PL1
Rejestruj zdarzenie:
Opcje uwierzytelniania
Wymaga rozpoznania Użytkownika:
Wymaga uprawnienia do Punktu identyfikacji:
Wymaga uprawnienia do Obiektu:
Wymaga uprawnienia do Parametru funkcji:
Opcje interaktywne
OK
Anuluj

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