Roger Access Control System 5

Nota aplikacyjna nr 003

Wersja dokumentu: Rev. C

Uprawnienia

Uwaga: Niniejszy dokument dotyczy RACS v5.6.6 (VISO 1.6.6 lub nowszy)

Wprowadzenie

W systemie RACS 5, wykonanie dowolnej funkcji przez użytkownika systemu, może być uwarunkowane posiadaniem przez niego odpowiedniego Uprawnienia definiowanego dla konkretnej funkcji (np. żądanie przyznania dostępu) i określającego warunki, w których dana funkcja może być wykonana i/lub warunki, gdy nie może być ona wykonana. Uprawnienie może być również definiowane dla grupy funkcji i wtedy dotyczy ono wszystkich funkcji wchodzących w skład danej grupy.

Wiele funkcji stosowanych w systemie RACS 5 domyślnie nie wymaga Uprawnienia (np. na poziomie linii wejściowej). Niemniej w razie potrzeby można taki wymóg ustawić i to w sposób szczegółowy a nie jedynie globalny. Konieczne jest wtedy zdefiniowanie odpowiednich Uprawnień i przypisanie ich użytkownikom.

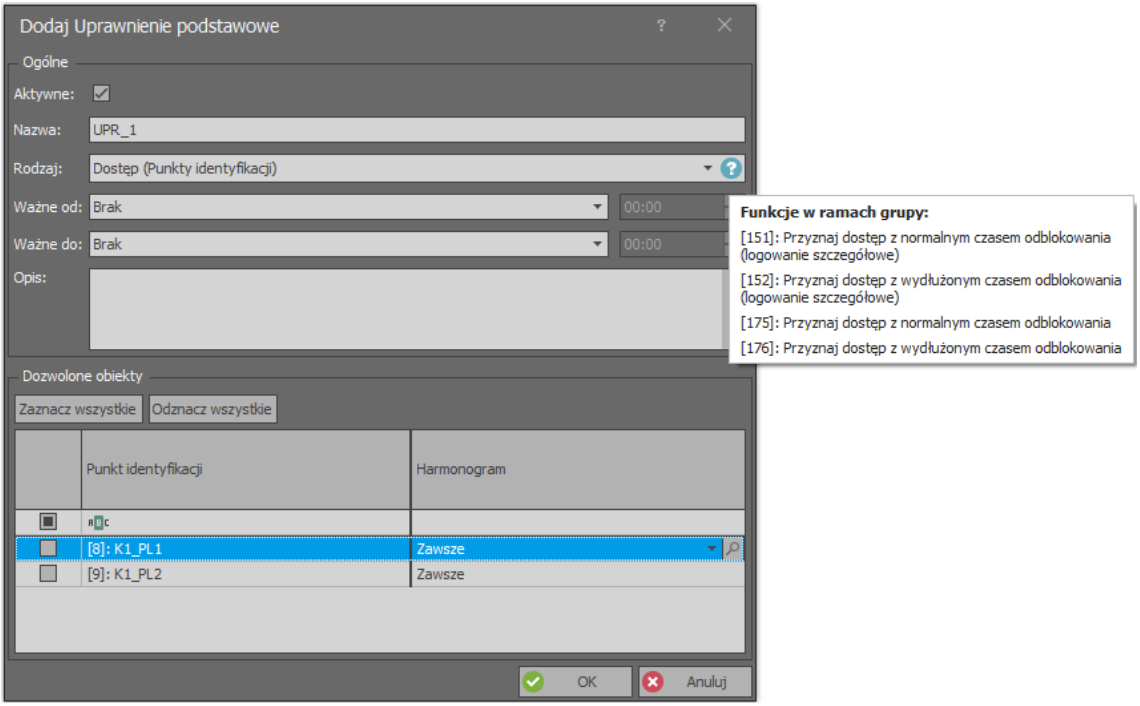
Uprawnienia mogą być przypisywane:

- 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).Dodatkowo same Uprawnienia mogą być łączone w grupy po to by ułatwić dodawania typowych Uprawnień użytkownikom (np. prawa dostępu na głównych przejściach w budynku).

Uprawnienia podstawowe

W systemie RACS 5 możliwe jest definiowanie Uprawnień podstawowych, które obejmują grupy typowych funkcji np. w zakresie dostępu, przezbrajania, automatyki, itd. Po wybraniu możliwe jest uzyskanie informacji na temat tego jakie funkcje wchodzą w skład danej grupy. W przypadku uprawnień podstawowych można stosować harmonogramy. Celem wprowadzenia Uprawnień podstawowych jest ułatwienie definiowania i stosowania typowych uprawnień systemu kontroli dostępu.



Uprawnienia zaawansowane

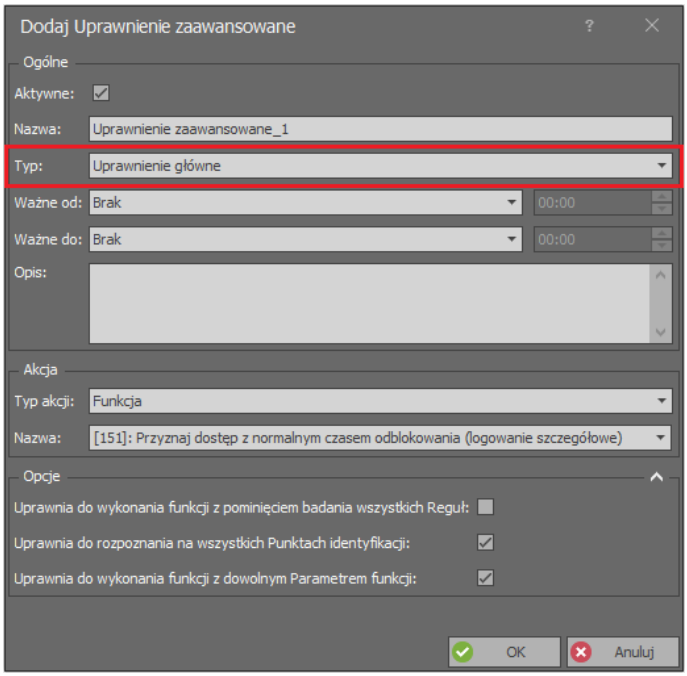
W przypadku Uprawnień zaawansowanych zakres możliwych ustawień jest dużo szerszy niż w przypadku Uprawnień podstawowych i obejmuje on wszystkie dostępne funkcje, opcje autoryzacji, reguły zezwalające i blokujące wraz z regułami szczegółowymi. Celem wprowadzenia Uprawnień zaawansowanych jest umożliwienie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

Typy Uprawnień zaawansowanych

Uprawnienia zaawansowane mogą być typu Głównego lub Uzupełniającego.

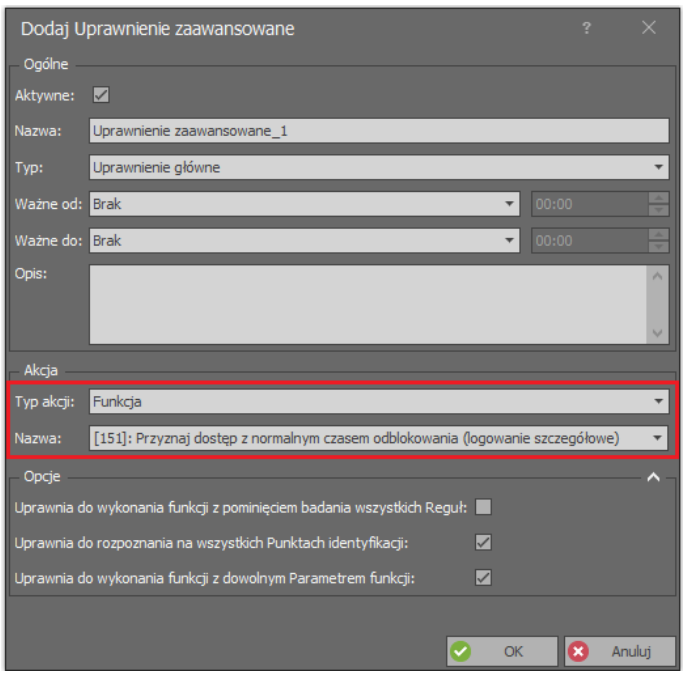
- Uprawnienie główne składa się ze wszystkich, wymaganych dla danej funkcji Reguł szczegółowych i samodzielnie może rozstrzygać o możliwości wykonania lub niewykonania funkcji.
- Uprawnienie uzupełniające składa się z Reguł szczegółowych odnoszących się do miejsca rozpoznania użytkownika i parametru funkcji i 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. Uprawnienia uzupełniające znajdują swoje zastosowanie przede wszystkim w kontroli dostępu wind oraz szafek.



Akcja Uprawnienia zaawansowanego

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.

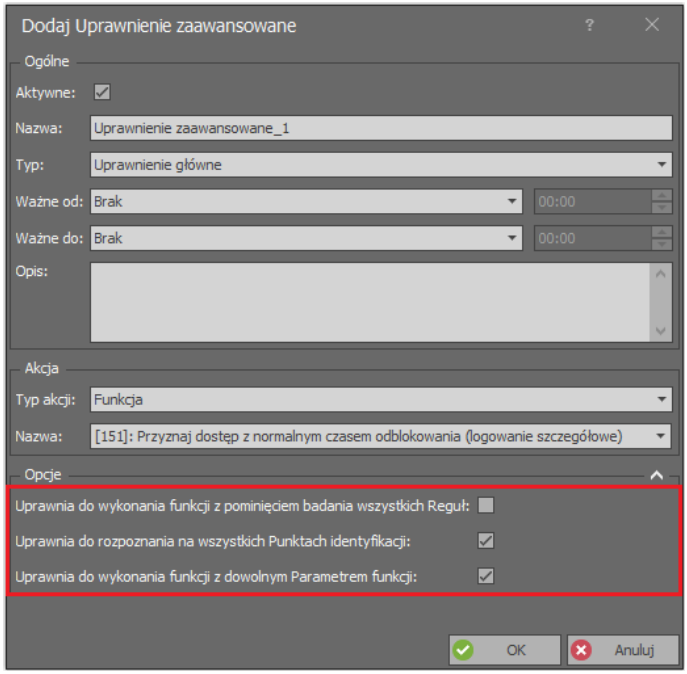


Opcje Uprawnienia zaawansowanego

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 Uprawnienia zaawansowanego

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 Uprawnienia zaawansowanego

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.

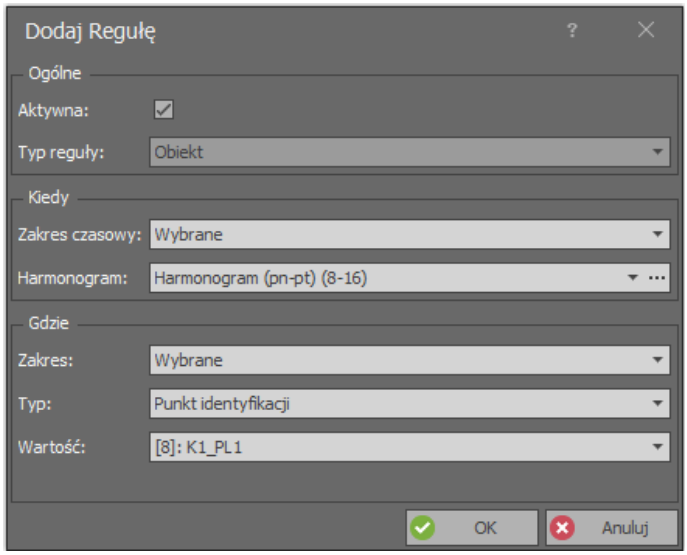
Reguła zezwalająca/blokująca jest spełniona, gdy w danym momencie zawiera przynajmniej po jednej z wymaganych Reguł szczegółowych. Proces analizy Reguły polega na sprawdzeniu czy:

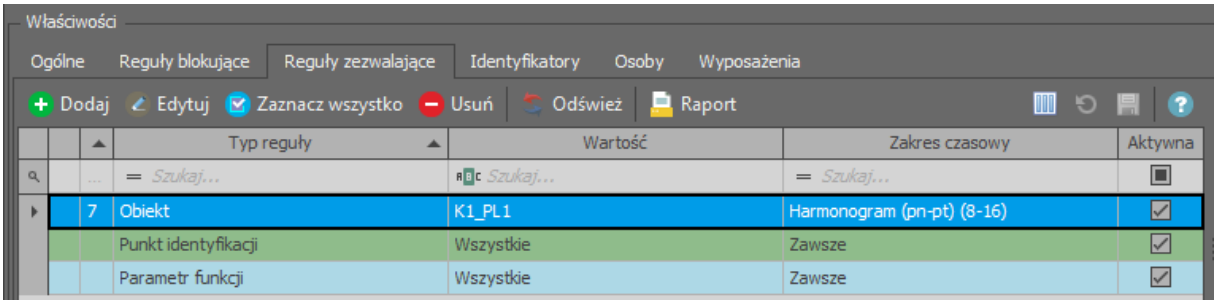
- użytkownik jest uprawniony aby dokonać rozpoznania na danym Punkcie identyfikacji
- użytkownik jest uprawniony aby wykonać funkcję na danym Obiekcie
- użytkownik jest uprawniony aby wykonać funkcję z danym Parametrem funkcji

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.



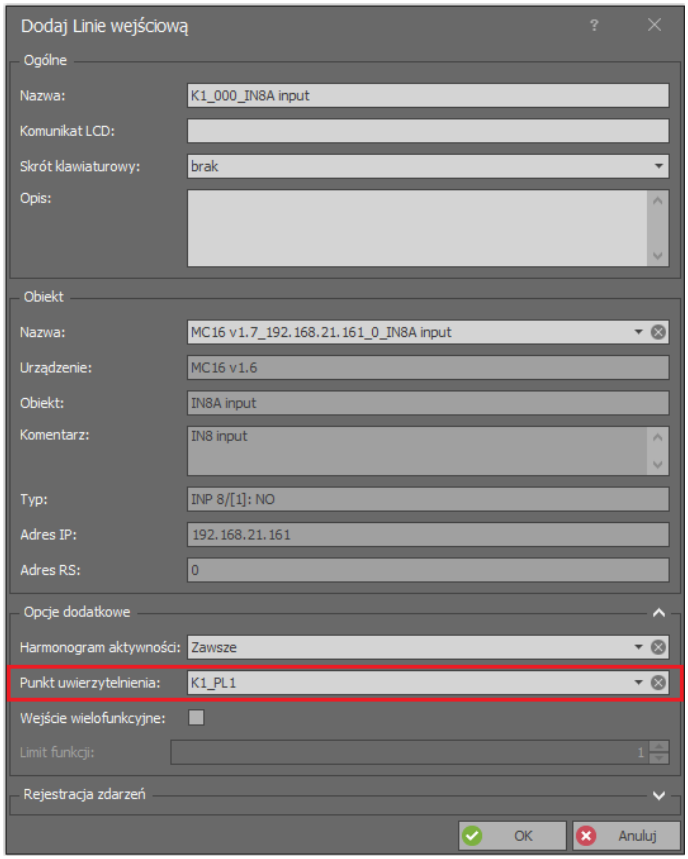


Przypisywanie Uprawnień

W systemie RACS 5, Uprawnienia mogą być przypisywane do Identyfikatorów, do Użytkowników oraz do Grup użytkowników. 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.

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.



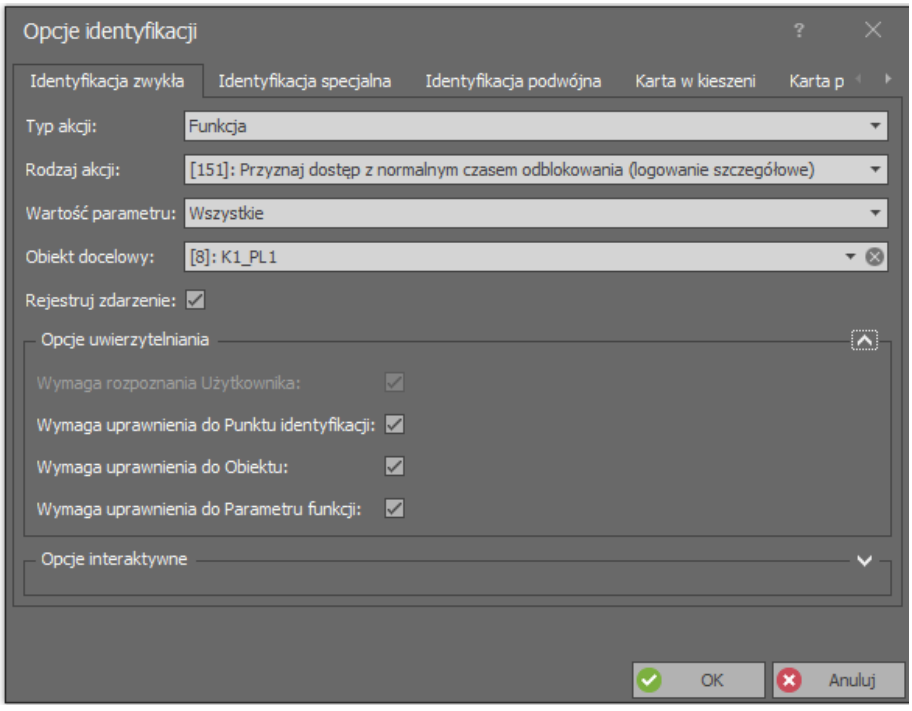
Opcje identyfikacji

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

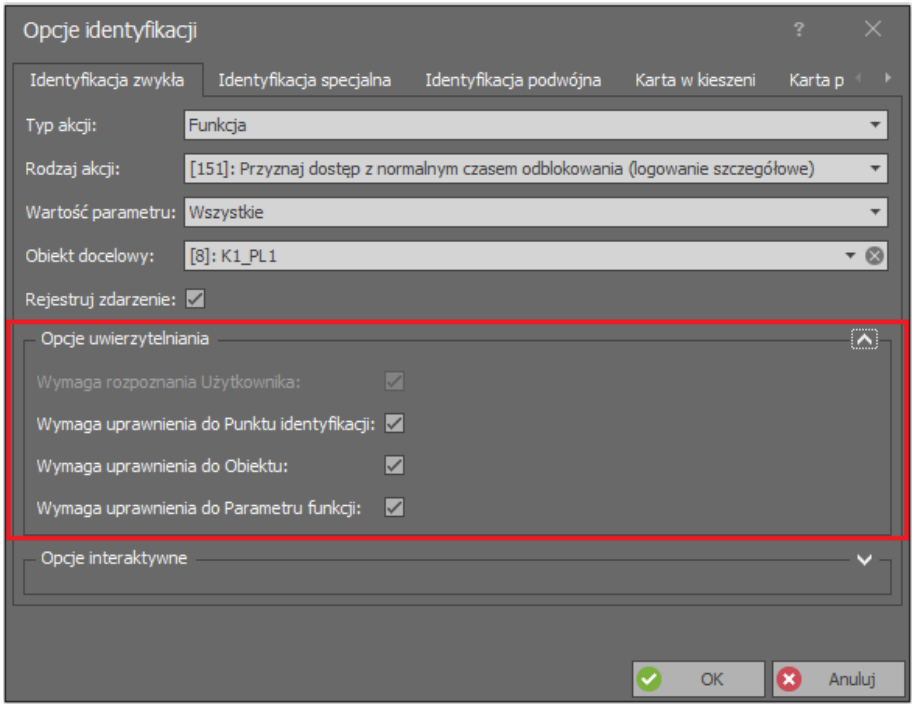
Dla wywołań funkcji istnieje możliwość załączenia Opcji uwierzytelniania, które wymuszą wymóg identyfikacji użytkownika oraz określą zasady weryfikacji jego Uprawnień. Przykładowo gdy wszystkie Opcje uwierzytelniania są nieaktywne to do wywołania funkcji nie są potrzebne żadne Uprawnienia więc może ją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

Opcje uwierzytelniania można definiować dla funkcji na poziomie:

- Punktu identyfikacji (dla każdej Opcji identyfikacji)
- Linii wejściowej

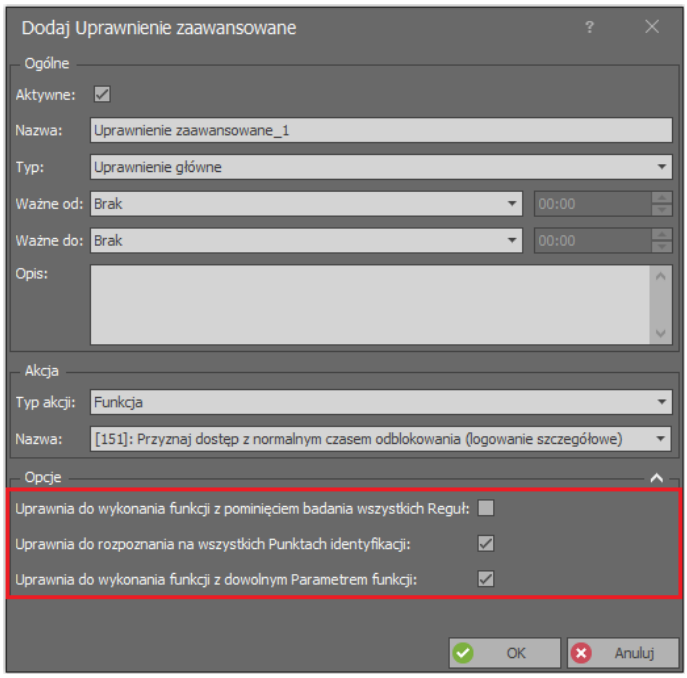
- Klawisza funkcyjnego
- Funkcji składowych Komendy lokalnej

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



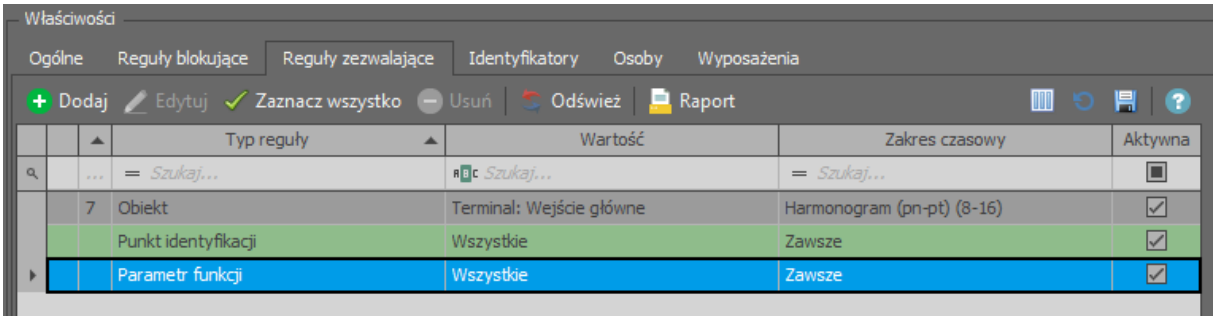
Uprawnienie zaawansowane do dostępu

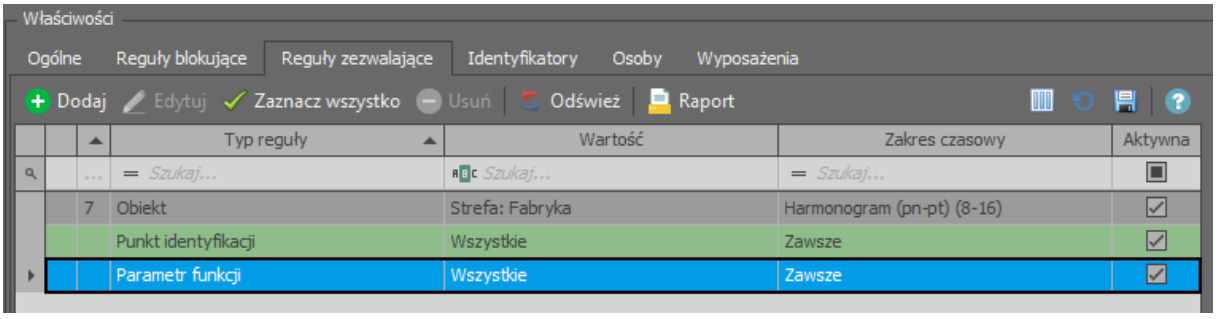
W systemie RACS 5, prawa dostępu zwykle definiuje się poprzez utworzenie Uprawnienia do funkcji *[151]: Przyznaj dostęp z normalnym czasem odblokowania (logowanie szczegółowe)*. W typowych przypadkach, gdy dostęp odbywa się przez odczyt Identyfikatora na terminalu dostępu, to można załączyć opcję *Uprawnia do rozpoznania na wszystkich Punktach identyfikacji,* która usuwa konieczność definiowania Reguł szczegółowych określających Punkty identyfikacji, na których użytkownik może dokonać rozpoznania. Jeśli dodatkowo, terminal dostępu kontroluje dostęp tylko do jednego Przejścia, to można załączyć opcję *Uprawnia do wykonania funkcji z dowolnym Parametrem Funkcji*, która usunie konieczność definiowania Reguł szczegółowych typu Parametr funkcji określających, które z Przejść kontrolowanych z danego Punktu identyfikacji może zostać odblokowane w momencie przyznania dostępu.



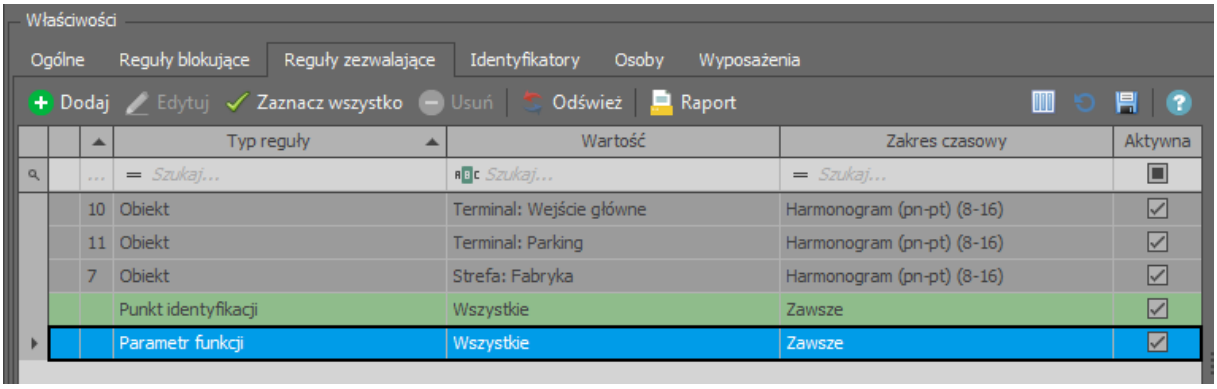
Podczas tworzenia nowego Uprawnienia zaawansowanego obie wymienione opcje są domyślnie załączone więc definiowanie Reguł szczegółowych w ramach Reguł zezwalających i blokujących jest ograniczone jedynie do reguły typu Obiekt, która określi Punkty identyfikacji lub Strefy dostępu, do których będzie możliwy dostęp.

W mniejszych systemach powszechnie praktykowane jest podejście, w którym dla każdego Punktu identyfikacji lub Strefy dostępu tworzone jest osobne Uprawnienie. W takim przypadku, nadawanie prawa dostępu użytkownikowi wymaga przypisania mu osobnego Uprawnienia do każdego Punktu identyfikacji lub Strefy dostępu, do której ma mieć on dostęp. Przykłady takiego podejścia pokazano na rysunkach poniżej.





Możliwe jest również podejście, w którym jedno uprawnienie zawiera komplet praw dostępu. W takim przypadku, przypisanie użytkownikowi jednego zbiorczego Uprawnienia może całkowicie wystarczać, aby określić jego prawa dostępu. Przykład takiego podejścia pokazano na rysunku poniżej.



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