Roger Access Control System 5v2

Nota aplikacyjna nr 004

Wersja dokumentu: Rev. A

Strefy dostępu i Anti-passback

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

Wprowadzenie

System RACS 5 umożliwia kontrolę przemieszczania się osób na poziomie Stref dostępu, Stref obwodowych oraz Globalnych stref dostępu. Za funkcjonowanie Stref dostępu odpowiada kontroler MC16, natomiast za Strefy obwodowe oraz Globalne strefy dostępu odpowiada Serwer komunikacji z pakietu oprogramowania RogerSVC. Oznacza to, że Strefy dostępu można definiować jedynie w ramach danego kontroler natomiast Strefy obwodowe oraz Globalne strefy dostępu można definiować na poziomie całego systemu RACS 5.

Strefa dostępu to obszar do którego wejście odbywa się przez Punkty identyfikacji (czytniki) zwane Punktami wejściowymi, natomiast wyjście odbywa się przez Punkty identyfikacji zwane Punktami wyjściowymi. Dodatkowo, w skład Strefy dostępu mogą wchodzić Punkty wewnętrzne, które kontrolują dostęp do pomieszczeń znajdujących się wewnątrz strefy. Punkt identyfikacji może być jednocześnie Punktem wejściowym do jednej strefy oraz Punktem wyjściowym z innej strefy i odwrotnie. W ogólnym przypadku, Strefa dostępu może obejmować rozległy obszar do którego wejście i wyjście kontrolowane jest przez wiele Punktów identyfikacji w ramach tego samego kontrolera dostępu. W minimalnym przypadku, Strefa dostępu może obejmować obszar jednego pomieszczenia, do którego dostęp odbywa się przez jedno przejście. Uprawnienia dostępu w systemie RACS 5 można definiować nie tylko na poziomie poszczególnych Punktów identyfikacji ale także na poziomie Stref dostępu i wtedy takie Uprawnienie umożliwia wejście do strefy przez jej dowolny Punkt wejściowy.

Strefy dostępu umożliwiają:

- Kontrolę i weryfikację liczby użytkowników w strefie (dolny i górny limit obecności)
- Realizację funkcji Anti-passback
- Kontrolę przemieszczenia się użytkowników pomiędzy strefami (sąsiedztwo stref)
- Dodatkową kontrolę dostępu na przejściach wewnętrznych strefy (Punkty wewnętrzne)

Strefy obwodowe podobnie jak Strefy dostępu to obszary z Punktami wejściowymi, wyjściowy i wewnętrznymi. Punkty wewnętrzne Strefy obwodowej można wykorzystać do dodatkowej kontroli dostępu na przejściach wewnętrznych.

Globalne strefy dostępu to obszary z Punktami wejściowymi i wyjściowy. Strefy te służą przede wszystkim do realizacji funkcji Anti-passback na poziomie całego systemu a nie jedynie w ramach pojedynczego kontrolera jak ma to miejsce w przypadku Stref dostępu.

Uwaga: Funkcjonalności na poziomie wszystkich typów stref dostępu bazują na rozpoznawaniu i zliczaniu Identyfikatorów. Jeżeli każdy z użytkowników dysponuje nie więcej niż jednym Identyfikatorem to można uznać, że te funkcjonalności w istocie dotyczą użytkowników.

Uwaga: Informacje na temat dodatkowego ilościowego limitowania dostępu z wykorzystaniem kontrolera MC16-AZC podano w nocie aplikacyjnej AN031.

Strefy dostępy

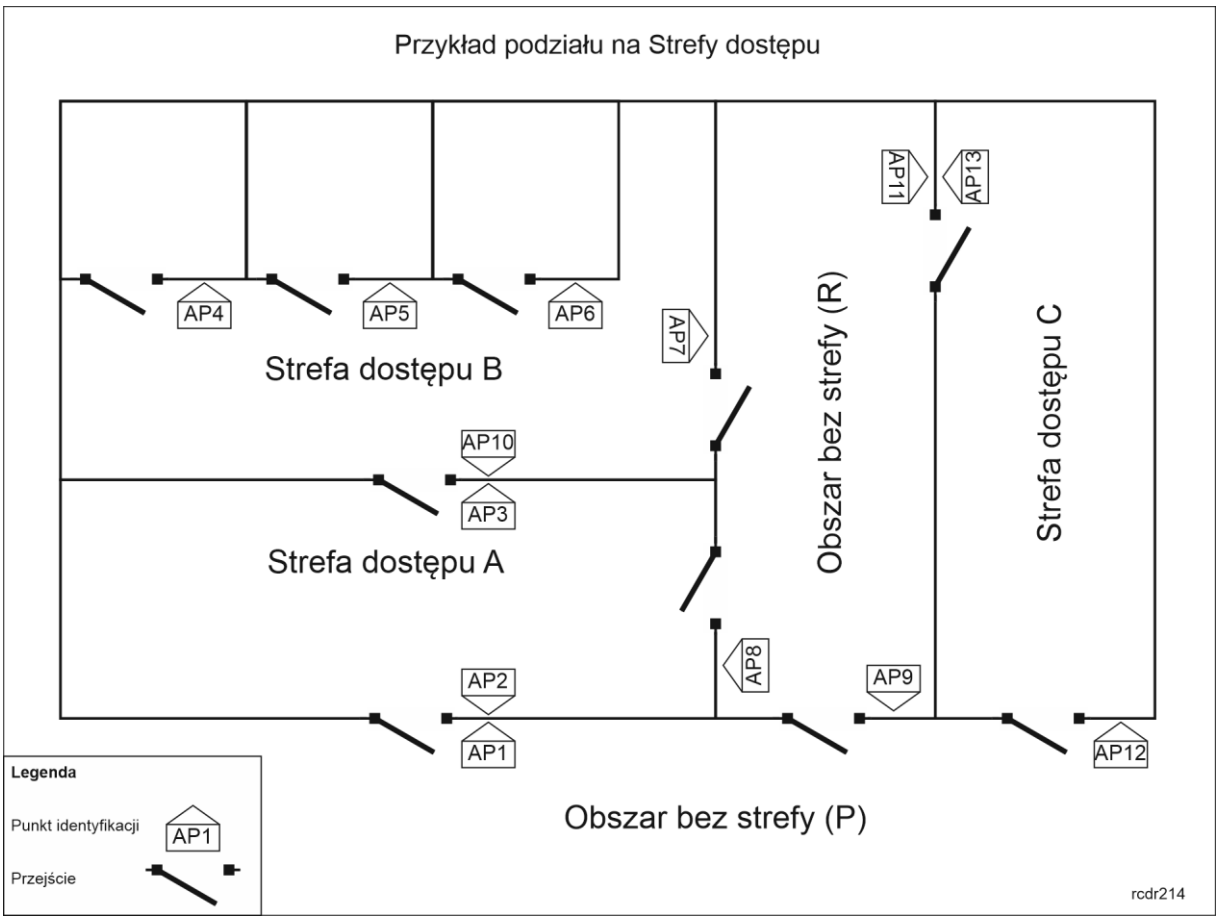
Konfiguracja strefy

Strefę dostępu konfiguruję się w ramach danego kontrolera dostępu w następujących krokach:

- W drzewku nawigacyjnym programu VISO w ramach danego kontrolera dostępu dwukrotnie kliknij *Strefy dostępu*.
- W nowo otwartym oknie wybierz przycisk *Dodaj*, nadaj strefie nazwę i następnie kliknij przycisk *OK*.
- W dolnej części okna zdefiniuj Punkty wejściowe, wyjściowe i w razie potrzeby Punkty wewnętrzne przypisując wcześniej zdefiniowane w systemie Punkty identyfikacji. Punkty identyfikacji z Terminalami dostępu zwykle tworzone są podczas definiowania Przejść np. za pomocą kreatora po wybraniu *Kreatory* w menu górnym programu VISO.
- Prześlij ustawienia do kontrolera.

Przykładowy podział na Strefy dostępu przedstawiono na poniższym rysunku gdzie:

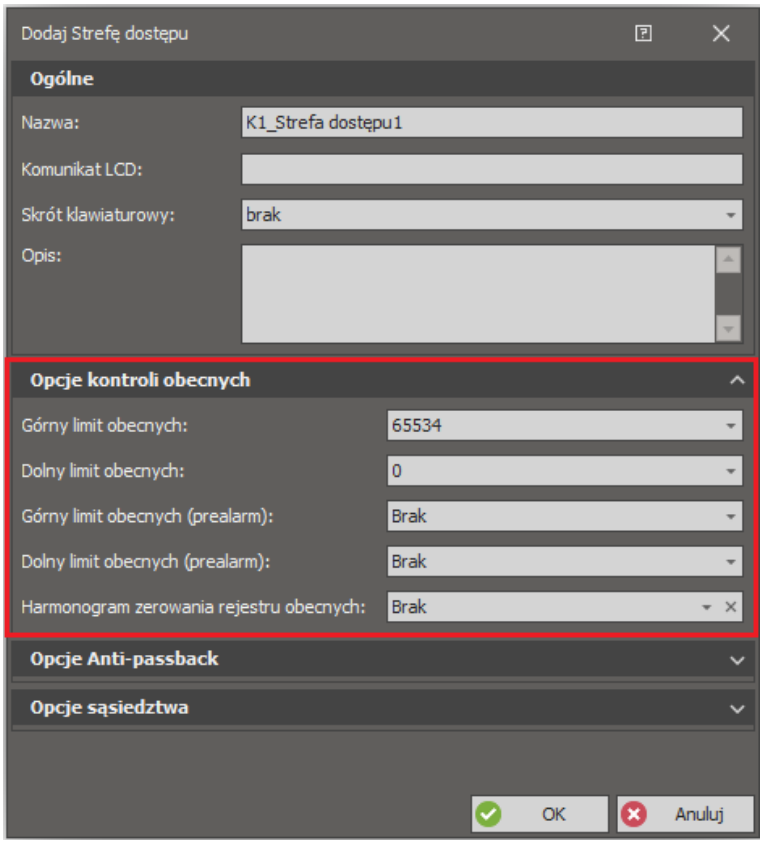
- Punkt identyfikacji AP1 jest Punktem wejściowym do Strefy dostępu A.
- Punkt identyfikacji AP2 jest Punktem wyjściowym ze Strefy dostępu A.
- Punkt identyfikacji AP3 jest Punktem wejściowym do Strefy dostępu B.
- Punkty identyfikacji AP4, AP5, AP6 są Punktami wewnętrznym w Strefie dostępu B.
- Punkt identyfikacji AP7 jest Punktem wyjściowym ze Strefy dostępu B.
- Punkt identyfikacji AP8 jest Punktem wejściowym do Strefy dostępu A.
- Punkt identyfikacji AP9 jest punktem nienależącym do żadnej Strefy dostępu.
- Punkt identyfikacji AP10 jest Punktem wejściowym do Strefy dostępu A i jednocześnie Punktem wyjściowym ze Strefy dostępu B.
- Punkt identyfikacji AP11 jest Punktem wejściowym do Strefy dostępu C.
- Punkt identyfikacji AP13 jest Punktem wyjściowym ze Strefy dostępu C.
- Punkt identyfikacji AP12 jest Punktem wejściowym do Strefy dostępu C.
- Strefy dostępu A i B są strefami sąsiednimi.
- Strefa dostępu C nie sąsiaduje z żadną inną Strefą dostępu.
- Obszary R oraz P, nie są objęte żadną Strefą dostępu.



Kontrola i weryfikacja liczby użytkowników w strefie

Użytkownik systemu, który uzyskał dostęp na Punkcie wejściowym do Strefy dostępu uzyskuje status Użytkownika przebywającego w danej strefie. Użytkownik systemu, który uzyskał dostęp na Punkcie wyjściowym ze Strefy dostępu jest uznawany za Użytkownika, który opuścił daną strefę i ewentualnie wszedł do innej strefy, o ile dany Punkt wyjściowy jest jednocześnie Punktem wejściowym do innej strefy.

Liczba osób przebywających w strefie może być ograniczona zarówno od góry jaki i od dołu. Kontrolę liczby użytkowników załącza się w ramach tworzenie Strefy dostępu. Istnieje możliwość zdefiniowania Górnego i Dolnego limitu obecnych, prealarmów dla limitów jak też przypisania Harmonogramu zerowania rejestru obecnych.



Górny i dolny limit obecnych

Parametr *Górny limit obecnych* blokuje wejście do strefy kolejnym użytkownikom jeśli ich liczba wewnątrz strefy osiągnęła górny limit. Parametr *Dolny limit obecnych* blokuje możliwość opuszczenia strefy jeśli ilość przebywających w niej użytkowników osiągnęła dolny limit.

Górny limit obecnych najczęściej znajduje zastosowanie na parkingach, gdzie system musi blokować wjazd na parking kolejnym samochodom jeśli wszystkie wolne miejsca zostały już wykorzystane. Dolny limit obecnych najczęściej znajduje zastosowanie w miejscach gdzie wymagana jest stała obecność jednej lub więcej osób np. dyspozytornia.

Prealarmy limitów obecnych

Parametry *Górny limit obecnych (prealarm)* oraz *Dolny limit obecnych (prealarm)* mogą być wykorzystywane do generowania ostrzeżeń gdy liczba użytkowników w strefie zbliża się odpowiednio do Górnego limitu obecnych lub Dolnego limitu obecnych. Osiągniecie limitów określonych przez prealarmy skutkuje załączeniem linii wyjściowych z funkcjami *[247]..[250]* co można wykorzystać do akustycznego lub wizualnego sygnalizowania danego prealarmu.

Harmonogram zerowania rejestru obecnych

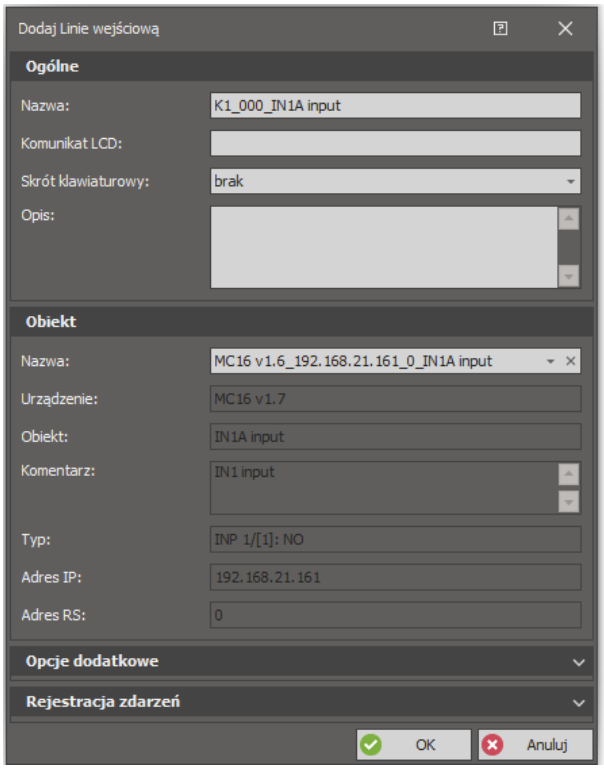
Harmonogram ten określa kiedy ma następować automatyczne zerowanie Rejestru obecnych dla wszystkich Identyfikatorów użytkowników zarejestrowanych w strefie. Po wykonaniu zerowania, kontroler od nowa zlicza obecność w strefie. Dla celów zerowania Rejestru obecnych można wykorzystać dowolny, wcześniej zdefiniowany Harmonogram typu *Chwilowy*. Harmonogram tego typu składa się z momentów czasowych w ramach tygodnia, w których ma nastąpić wykonanie jakiejś akcji w systemie. W tym przypadku jest to akcja polegająca na wyzerowaniu Rejestru obecnych w konkretnej Strefie dostępu. Harmonogramy można definiować wybierając polecenie *Harmonogramy* w drzewku nawigacyjnym programu VISO.

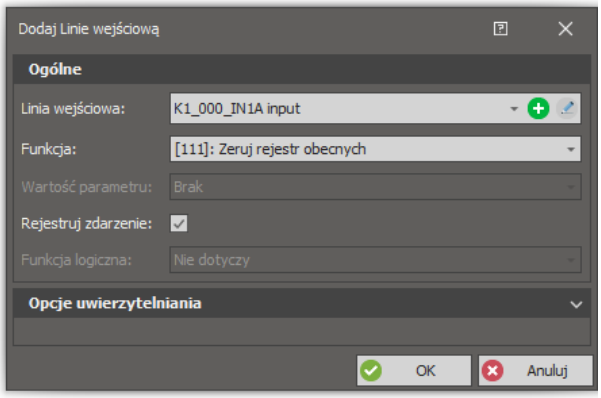
Zerowanie Rejestru obecnych Linią wejściową, Klawiszem funkcyjnym i Komendą lokalną

Rejestr obecnych można zerować na żądanie za pomocą dowolnej linii wejściowej w obrębie kontrolera i jego urządzeń peryferyjnych lub też za pomocą klawisza funkcyjnego na dowolnym czytniku podłączonym do kontrolera dostępu i wyposażonym w klawiaturę z takimi klawiszami.

Aby zdefiniować taką linie wejściową na poziomie Strefy dostępu:

- W drzewku nawigacyjnym programu VISO w ramach danego kontrolera dostępu dwukrotnie kliknij polecenie *Strefy dostępu*.
- W otwartym oknie wybierz jedną z wcześniej utworzonych stref.
- W dolnej części ekranu wybierz zakładkę *Linie wejściowe* i następnie *Dodaj*.
- W otwartym oknie wybierz przycisk ⊕ po to by w kolejnym oknie wskazać lokalizację linii (np. IN1 kontrolera MC16) i zamknij okno przyciskiem *OK*.
- Przypisz funkcję *[111]: Zeruj rejestr obecnych* i następnie zamknij okno przyciskiem *OK*.
- Prześlij ustawienia do kontrolera.





Konfiguracja klawisza funkcyjnego zerującego Rejestr obecnych jest realizowana w analogiczny sposób w zakładce *Klawisze funkcyjne* danej Strefy dostępu.

W ramach Strefy dostępu w zakładce *Komendy lokalne* możliwe jest również zdefiniowanie Komendy lokalnej z funkcją *[111]*. Komenda lokalna może być zastosowana w ramach Opcji identyfikacji danego Punktu identyfikacji a jej wywołanie czyli w tym wypadku zerowanie rejestru może być realizowane poprzez użycie Identyfikatora (np. krótki, długi lub podwójny odczyt karty na wybranym czytniku). Stosowanie Komendy lokalnej wymaga utworzenia Uprawnienia zaawansowanego z funkcją *[111]* i przypisanie go użytkownikowi. Więcej informacji na temat Komend lokalnych podano w nocie aplikacyjnej AN048.

Uwaga: Zerowanie Rejestru obecnych powoduje również wyzerowanie Rejestru APB.

Zerowanie Rejestru obecnych Komendą zdalną

Program VISO umożliwia zerowanie rejestru obecnych Komendę zdalną. Można ją wywołać klikając prawym przyciskiem myszy daną Strefę dostępu w drzewku nawigacyjnym, w oknie Stref dostępu

jak też z poziomu mapy. Użycie komendy zdalnej wymaga Uprawnienia przypisanego do operatora programu VISO. Aby operator mógł zdalnie zerować rejestr obecnych to musi być on przypisany do użytkownika z Uprawnieniem do funkcji *[111]* dla danej Strefy dostępu. Takie powiązanie użytkownika z operatorem jest realizowane we właściwościach użytkownika w zakładce *Zdalne zarządzanie* w polu *Operator*. Najprostszą metodą nadania wszystkich możliwych Uprawnień operatorowi jest przypisanie go do użytkownika z Identyfikatorem, który ma załączoną opcję *Wyjątek Master.* Więcej informacji na ten temat podano w nocie aplikacyjnej AN040.

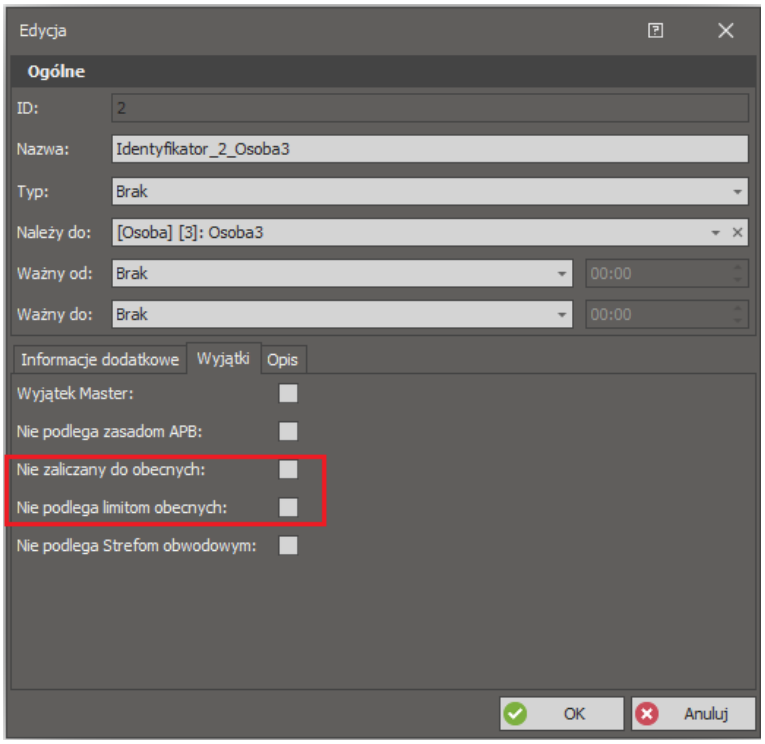
Sygnalizacja stanów obecności za pomocą linii wyjściowych

Stan rejestru obecnych można sygnalizować za pomocą dowolnej linii wyjściowej w obrębie kontrolera i jego urządzeń peryferyjnych. Liniom można przypisywać funkcje opisane w instrukcji obsługi kontrolera MC16 z zakresu *[52]..[57]* oraz *[247]..[252]*. Aby zdefiniować linię wyjściową na poziomie Strefy dostępu:

- W drzewku nawigacyjnym programu VISO dwukrotnie kliknij polecenie *Strefy dostępu*.
- W otwartym oknie wybierz jedną z wcześniej utworzonych stref.
- W dolnej części ekranu wybierz zakładkę *Linie wyjściowe* i następnie *Dodaj*.
- W otwartym oknie wybierz przycisk po to by w kolejnym oknie wskazać lokalizację linii (np. OUT1 kontrolera MC16) i zamknij okno przyciskiem OK.
- Przypisz wymaganą funkcję i następnie zamknij okno przyciskiem *OK*.
- Prześlij ustawienia do kontrolera.

Wyłączenie Identyfikatora z reguł zliczania obecności

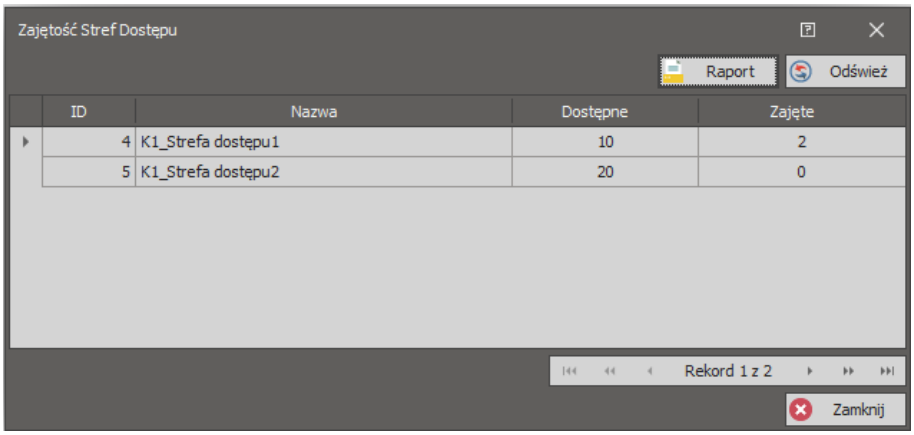
Identyfikator użytkownika może zostać wyłączony z działania funkcji limitów obecności poprzez załączenie opcji w jego właściwościach. W przypadku załączenia opcji *Nie zaliczany do obecnych*, użytkownik z takim Identyfikatorem nie jest uwzględniany przy zliczaniu obecnych w strefie. W przypadku opcji *Nie podlega limitom obecnych* użytkownik z takim Identyfikatorem jest uwzględniany przy wyznaczaniu liczby obecnych w strefie ale nie obowiązują go limity obecnych. Opcja *Wyjątek Master* zawiera w sobie wszystkie pozostałe wyjątki i dodatkowo nadaje wszystkie możliwe Uprawnienia w systemie.



Weryfikacja ilości użytkowników w strefach

Aby sprawdzić aktualną ilość użytkowników w Strefach dostępu:

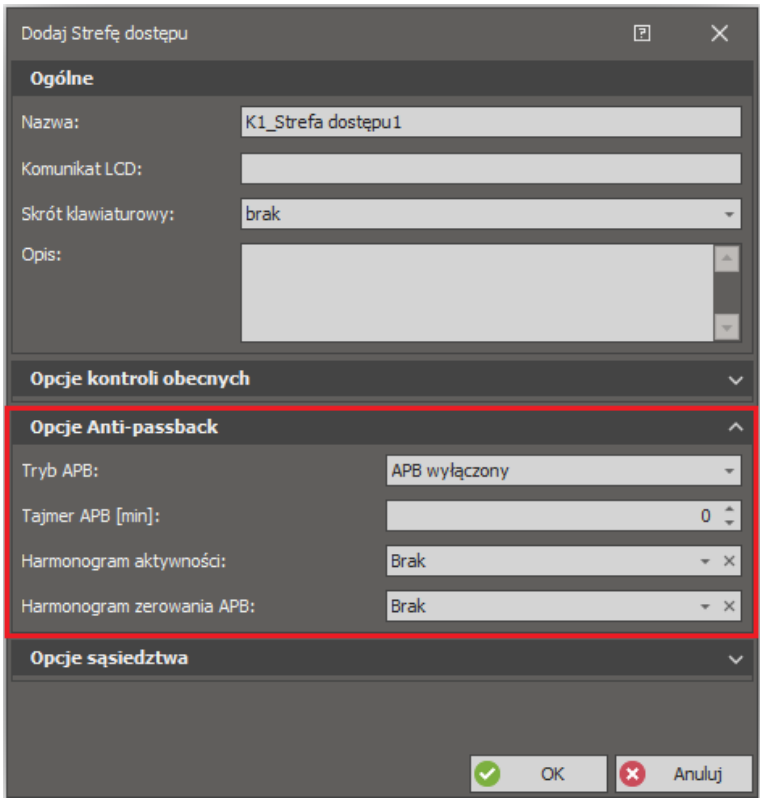
- W drzewku nawigacyjnym programu VISO dwukrotnie kliknij polecenie *Strefy dostępu*.
- W otwartym oknie wybierz przycisk *Zajętość stref*.



Wartość w kolumnie *Dostępne* zależy od parametru *Górny limit obecnych* a wartość w kolumnie *Zajęte* zależy od aktualnej ilości użytkowników w strefie.

Funkcja Anti-passback

Funkcja Anti-passback (APB) ma na celu wykrycie i ewentualnie zablokowanie próby wejścia do Strefy dostępu, w której użytkownik aktualnie wg systemu już się znajduje. Inaczej mówiąc funkcja APB zapobiega dwukrotnemu zastosowaniu tego samego Identyfikatora (np. karty) na Punktach wejściowych do Strefy dostępu i wymusza naprzemienne stosowanie danego Identyfikatora na Punktach wejściowych i wyjściowych. Funkcja APB ma zapobiegać nieuprawnionemu przekazywaniu kart pomiędzy użytkownikami w celu uzyskania wielokrotnego dostępu do danej strefy za pomocą tego samego Identyfikatora i znajduje ona swoje zastosowanie np. na płatnych parkingach.



Funkcję anti-passbacku załącza się w ramach tworzenie Strefy dostępu. Istnieje możliwość wybrania Trybu APB, zdefiniowania Tajmera APB oraz przypisania Harmonogramu aktywności i Harmonogramu zerowania APB.

Tryby APB

APB Twardy blokuje możliwość ponownego wejścia do strefy w przypadku naruszenia zasad APB i dodatkowo skutkuje rejestracją zdarzenie związanego z takim naruszeniem. APB Miękki nie blokuje ponownego wejścia do strefy a naruszenie zasad APB skutkuje jedynie rejestracją zdarzenia związanego z takim naruszeniem.

Tajmer APB

Tajmer APB jest licznikiem czasu który określa przez jaki czas od momentu wejścia do strefy kontroler będzie blokował ponowne do niej wejście. Po upływie czasu określonego przez Tajmer APB użytkownik może ponownie wejść do strefy pomimo tego, że jej wcześniej nie opuścił. Załączenie opcji Tajmer APB umożliwia samoczynne, po zdefiniowanym czasie, odblokowanie możliwości poruszania się użytkownika bez interwencji operatora systemu, który w przeciwnym przypadku musiałby wyzerować rejestr APB. Ta funkcjonalność może być stosowana także w przypadku drzwi kontrolowanych jednostronnie.

Harmonogram aktywności

Harmonogram aktywności definiuje kiedy reguły APB będą w ogóle obowiązywać użytkowników. Do tego celu można wykorzystać dowolny Harmonogram typu *Okresowy*, który można zdefiniować za pomocą polecenia *Harmonogramy* w drzewku nawigacyjnym programu VISO.

Harmonogram zerowania APB

Harmonogram ten określa kiedy ma następować automatyczne zerowanie rejestru APB dla wszystkich Identyfikatorów zarejestrowanych w strefie. Po wykonaniu zerowania, kontroler zezwala na wejście do strefy pomimo tego, że Identyfikator nie był wcześniej użyty na wyjściu ze strefy. W praktyce, zerowanie rejestru APB wykonuje się w godzinach nocnych, tak aby w godzinach porannych nie blokować ruchu użytkowników którzy poprzedniego dnia nie zarejestrowali opuszczenia strefy. Dla celów zerowania funkcji APB można wykorzystać dowolny, wcześniej zdefiniowany Harmonogram typu *Chwilowy*. Harmonogram tego typu składa się z momentów czasowych w ramach tygodnia, w których ma nastąpić wykonanie jakiejś akcji w systemie. W tym przypadku jest to akcja polegająca na wyzerowaniu rejestru APB konkretnej Strefy dostępu. Harmonogram można utworzyć wybierając polecenie *Harmonogramy* w drzewku nawigacyjnym programu VISO.

Zerowanie rejestru APB linią wejściową, klawiszem funkcyjnym i komendą lokalną

Linię wejściową, klawisz funkcyjny jak też Komendę lokalną zerujące rejestr APB definiuje się w taki sam sposób jak w przypadku wcześniej opisanego zerowania rejestru obecnych. Różnica polega na tym że stosuje się funkcję *[112]: Zeruj rejestr APB* zamiast funkcji *[111]: Zeruj rejestr obecności*.

Zerowanie rejestru APB komendą zdalną

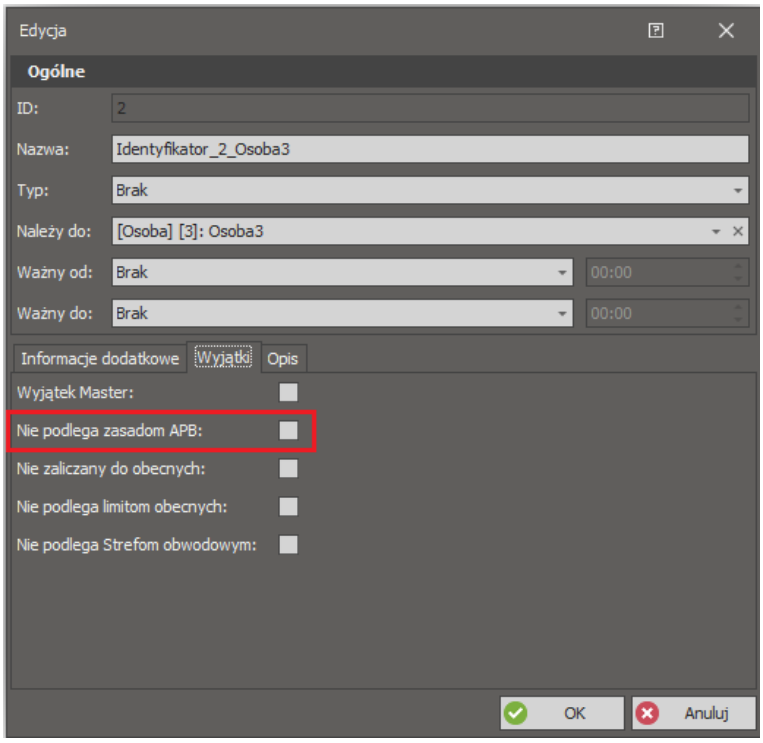
Zerowanie rejestru APB komendą zdalną realizuje się w taki sam sposób jak wcześniej opisane zerowanie rejestru obecnych. Różnica polega na tym że stosuje się funkcję *[112]: Zeruj rejestr APB* zamiast funkcji *[111]: Zeruj rejestr obecności*.

Sygnalizacja stanu APB za pomocą linii wyjściowej

Linię wyjściową do sygnalizacji naruszenia stanu APB definiuje się w taki sam sposób jak w przypadku wcześniej opisanego rejestru obecnych ale stosuje się funkcję wyjściową *[51]*.

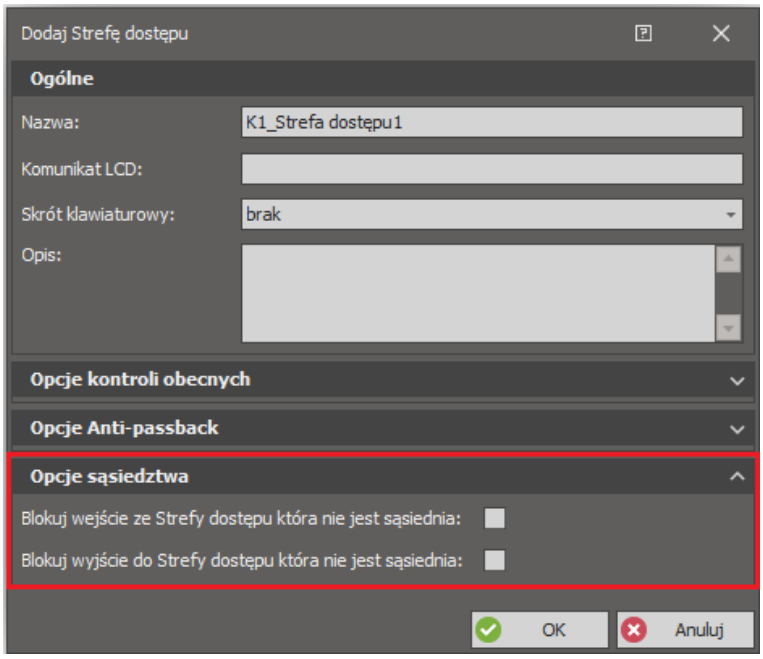
Wyłączenie Identyfikatora z zasad APB

Identyfikator użytkownika może zostać wyłączony z działania funkcji APB poprzez załączenie opcji *Nie podlega zasadom APB* we właściwościach Identyfikatora. Opcja *Wyjątek Master* zawiera w sobie wszystkie pozostałe wyjątki i dodatkowo nadaje wszystkie możliwe Uprawnienia w systemie.



Kontrola przemieszczenia się użytkowników pomiędzy strefami

W systemie RACS 5 możliwe jest kontrolowanie przemieszczania się użytkowników pomiędzy sąsiednimi Strefami dostępu. Dwie strefy są uznawane jako strefy sąsiednie jeśli w ramach definicji przynajmniej jednej z nich znajduje się Punkt identyfikacji, który jest jednocześnie Punktem wyjściowym z jednej strefy oraz Punktem wejściowym do drugiej strefy. Kontrolę sąsiedztwa załącza się w ramach tworzenie Strefy dostępu poprzez wybór jednej z opcji blokowania.

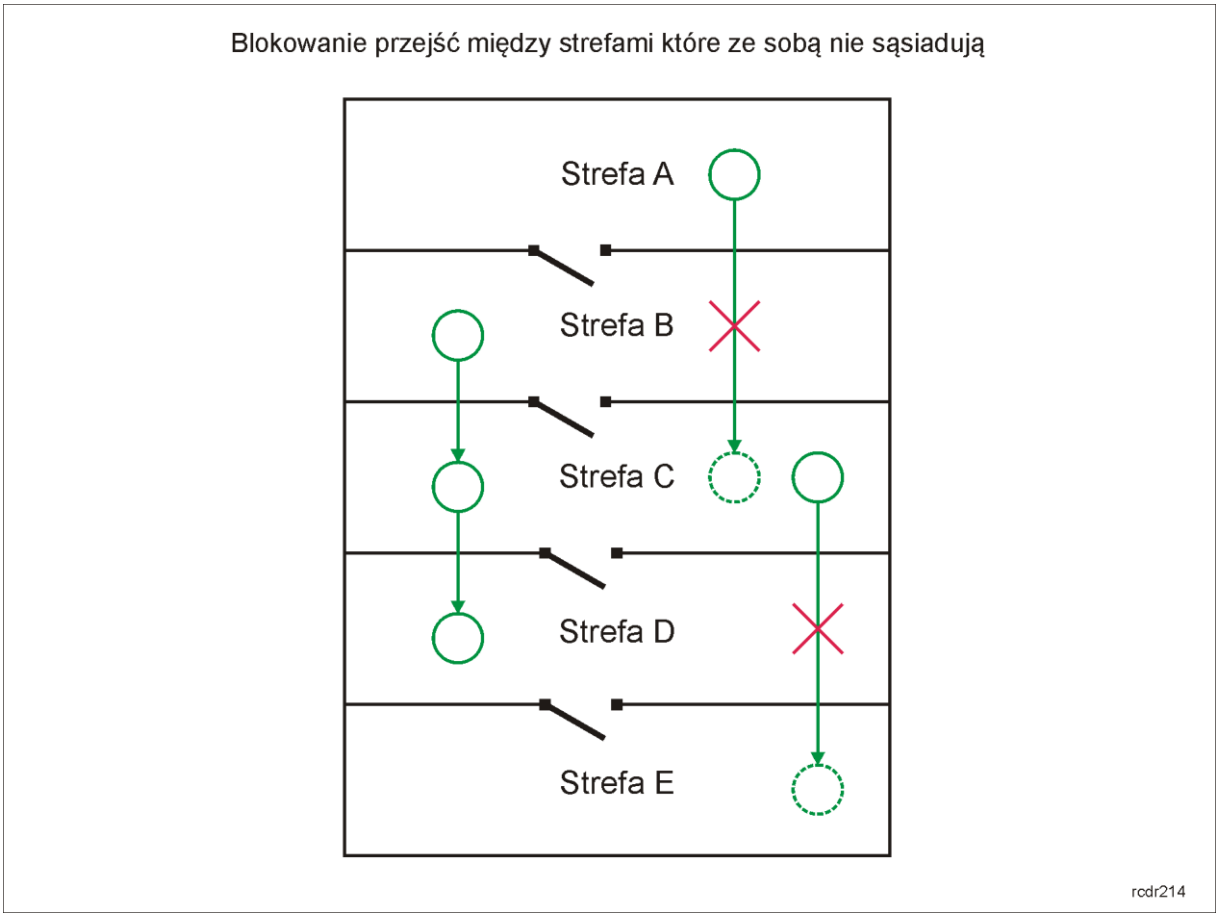


Opcje sąsiedztwa

Gdy opcja *Blokuj wejście ze Strefy dostępu która nie jest sąsiednia* jest załączona, to kontroler nie pozwala na wejście do strefy, o ile strefa którą opuszcza użytkownik z nią nie sąsiaduje.

Gdy opcja *Blokuj wyjście do Strefy dostępu która nie jest sąsiednia* jest załączona, to kontroler nie pozwala na opuszczenie strefy w której aktualnie użytkownik przebywa, jeśli strefa do której chce wejść użytkownik nie sąsiaduje ze strefa którą zamierza opuścić.

Koncepcja sąsiedztwa stref



W przedstawionym powyżej przykładzie załączenie opcji *Blokuj wejście ze Strefy dostępu która nie jest sąsiednia* we właściwościach strefy C blokuje przejście ze strefy A do C ale zezwala na przejście ze strefy B do C.

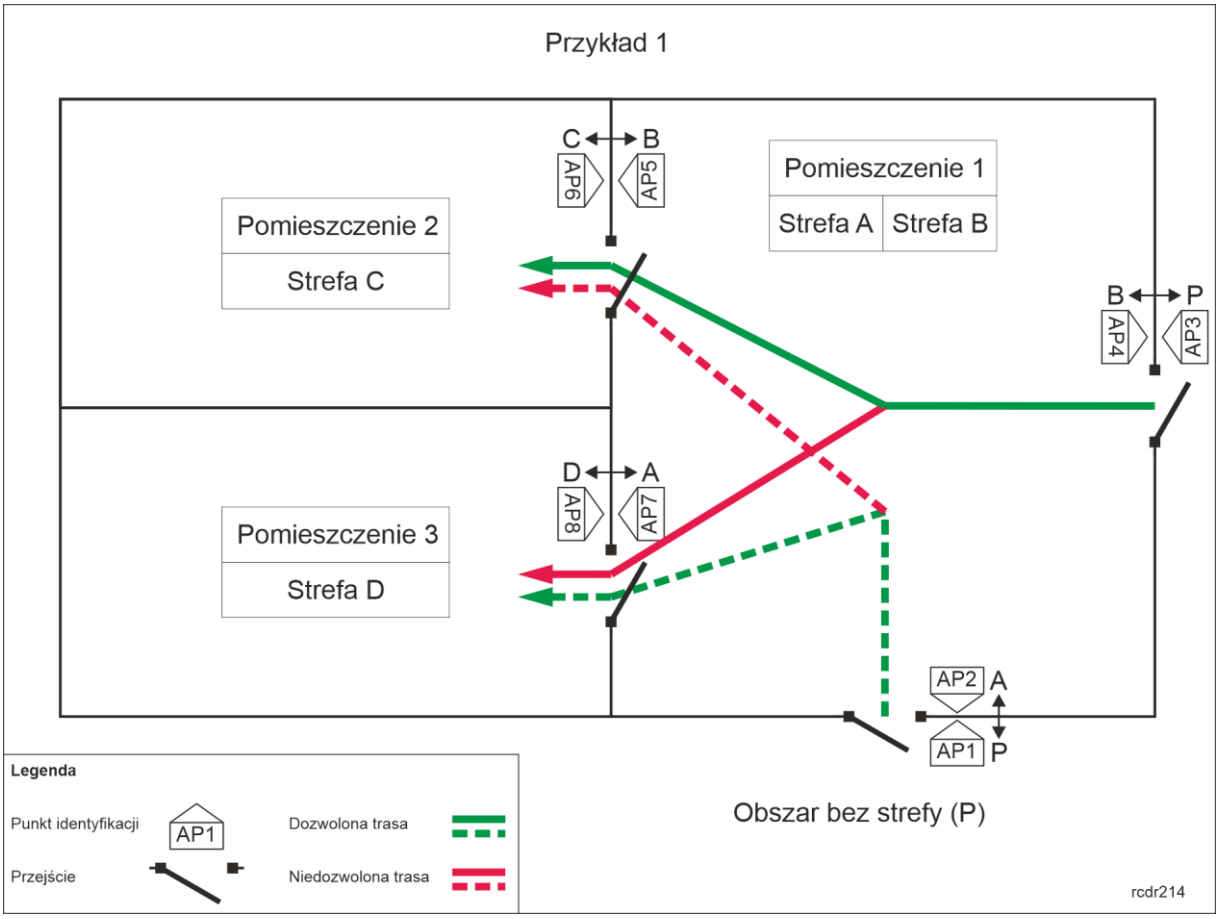
W przedstawionym powyżej przykładzie załączenie opcji *Blokuj wyjście do Strefy dostępu która nie jest sąsiednia* we właściwościach strefy C blokuje przejście ze strefy C do E ale zezwala na przejście ze strefy C do D.

Opcje sąsiedztwa mają wpływu na ruch użytkowników wyłącznie w przypadku gdy ruch ten odbywa się pomiędzy Strefami dostępu. Jeśli przejście odbywa się z obszaru, lub do obszaru który nie jest objęty żadną Strefą dostępu to opcje sąsiedztwa nie mają zastosowania. Gdy Identyfikator użytkownika ma załączoną opcję *Nie zaliczany do obecnych* to taki użytkownik nie musi przestrzegać zasad wynikających z sąsiedztwa Stref Dostępu.

W praktyce, opcje sąsiedztwa umożliwiają wymuszanie ruchu użytkowników wg ustalonych tras i mają na celu przeciwdziałanie przemieszczaniu się użytkowników z pominięciem określonych Punktów identyfikacji systemu kontroli dostępu.

Przykład 1

Zgodnie z poniższym rysunkiem, użytkownik z Uprawnieniami dostępu na wszystkich czterech przejściach, który wejdzie do Pomieszczenia 1 przez Punkt wejściowy AP3 może wejść do Pomieszczenia 2 ale nie może wejść do Pomieszczenia 3. Jeżeli ten sam użytkownik wejdzie do Pomieszczenia 1 przez Punkt wejściowy AP1 to z kolei może wejść do Pomieszczenia 3 ale nie może wejść do Pomieszczenia 2. W tym przykładzie fizycznie istniejącemu Pomieszczeniu 1 odpowiadają logicznie dwie Strefy dostępu A i B z Punktami wejściowymi odpowiednio AP1 i AP3.



Aby skonfigurować ograniczenia w przemieszczeniu użytkowników zgodnie z Przykładem 1:

- Skonfiguruj wszystkie cztery Przejścia za pomocą *Kreatora przejścia* z uwzględnieniem wszystkich Uprawnień dostępu.
- Zdefiniuj użytkownika za pomocą kreatora *Dodaj Osobę online* przypisując Nośnik(i) oraz wszystkie Uprawnienia dostępu.
- Skonfiguruj cztery Strefy dostępu przypisując:
  - AP1 i AP8 jako Punkty wejściowe Strefy A.
  - AP2 i AP7 jako Punkty wyjściowe Strefy A.
  - AP3 i AP6 jako Punkty wejściowe Strefy B.
  - AP4 i AP5 jako Punkty wyjściowe Strefy B.
  - AP5 jako Punkt wejściowy Strefy C.
  - AP6 jako Punkt wyjściowy Strefy C.
  - AP7 jako Punkt wejściowy Strefy D.
  - AP8 jako Punkt wyjściowy Strefy D.

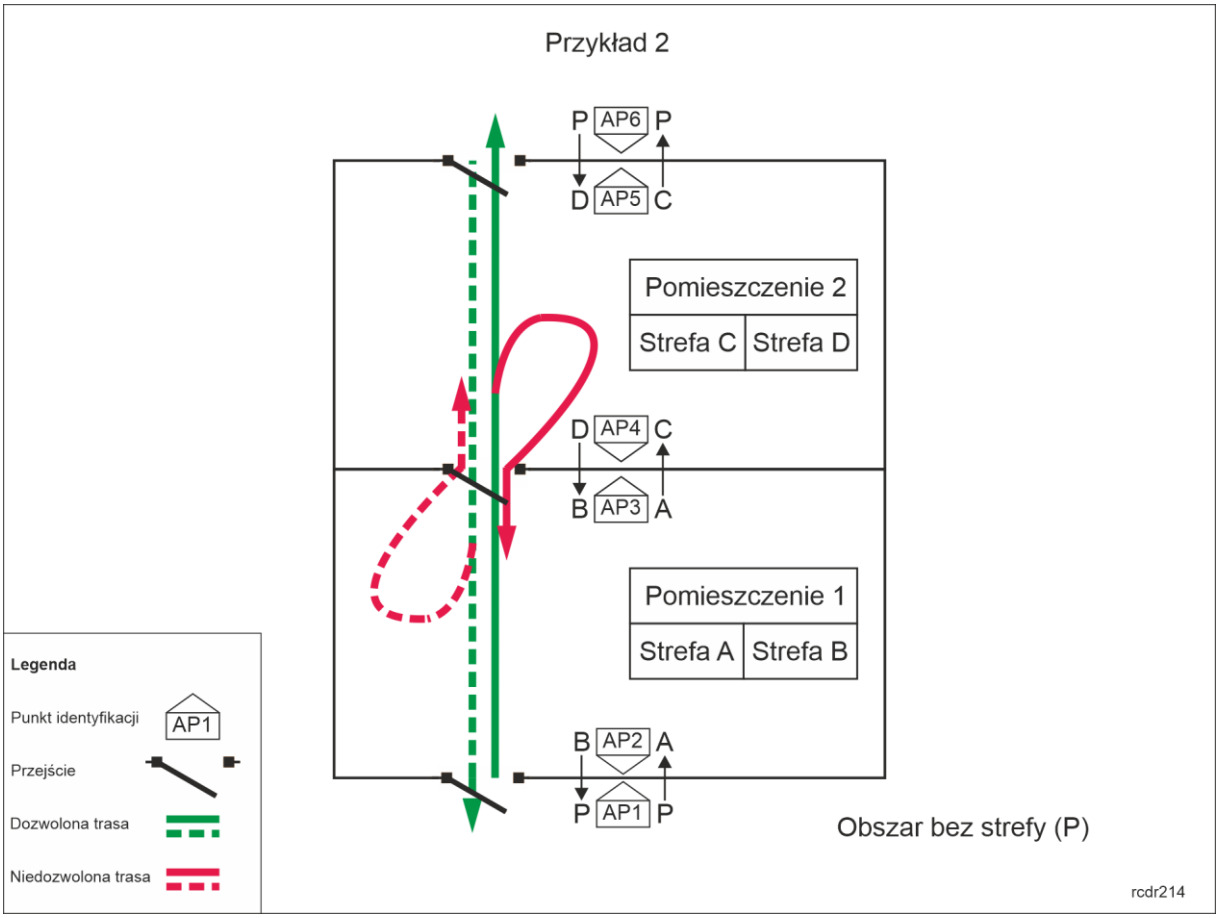
  Punkt dostępu AP5 (jak też AP6) określa sąsiedztwo Stref B i C.
  Punkt dostępu AP7 (jak też AP8) określa sąsiedztwo Stref A i D.
  Strefy A i C nie są strefami sąsiednimi.
  Strefy B i D nie są strefami sąsiednimi.

Strefy A i B nie są strefami sąsiednimi.
Strefy C i D nie są strefami sąsiednimi.

- Załącz opcję *Blokuj wejście ze Strefy dostępu która nie jest sąsiednia* dla Stref C i D albo załącz opcję *Blokuj wyjście do Strefy dostępu która nie jest sąsiednia* dla Stref A i B. W pierwszym przypadku możliwe będzie opuszczenie budynku dowolnym przejściem a w drugim konieczne jest użycie tego samego przejścia co przy wejściu do budynku.
- Prześlij ustawienia do kontrolera.

Przykład 2

Zgodnie z poniższym rysunkiem, użytkownik z Uprawnieniami dostępu na wszystkich trzech przejściach może przemieszczać się jedynie do przodu bez względu na punkt startowy. Gdy użytkownik przejdzie do Pomieszczenia 2 z Pomieszczenia 1 to nie będzie mógł się cofnąć do Pomieszczenia 1 ale może przejść dalej do Obszaru P. Gdy użytkownik przejdzie do Pomieszczenia 1 z Pomieszczenia 2 to nie będzie mógł się cofnąć do Pomieszczenia 2 ale może przejść dalej do Obszaru P. W tym przykładzie fizycznie istniejącemu Pomieszczeniu 1 odpowiadają logicznie dwie Strefy dostępu A i B z Punktami wejściowymi odpowiednio AP1 i AP4. Analogiczna sytuacja występuje dla Pomieszczenia 2 i Stref C oraz D z Punktami wejściowymi odpowiednio AP3 i AP6.



Aby skonfigurować ograniczenia w przemieszczeniu użytkowników zgodnie z Przykładem 2:

- Skonfiguruj wszystkie trzy Przejścia za pomocą *Kreatora przejścia* z uwzględnieniem wszystkich Uprawnień dostępu.
- Zdefiniuj użytkownika za pomocą kreatora *Dodaj Osobę online* przypisując Nośnik(i) oraz wszystkie Uprawnienia dostępu.
- Skonfiguruj cztery Strefy dostępu przypisując:
  - AP1 jako Punkt wejściowy Strefy A.
  - AP3 jako Punkt wyjściowy Strefy A.

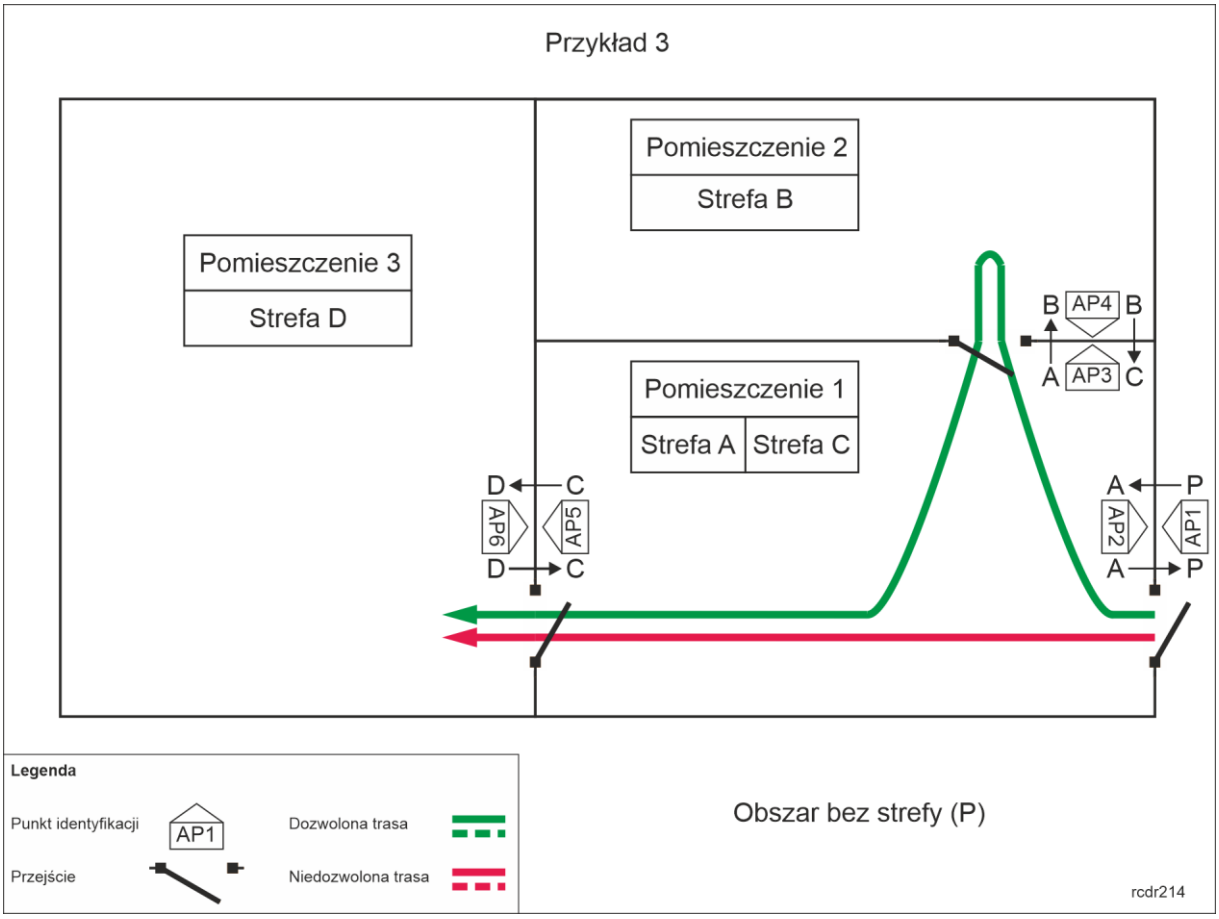
- AP4 jako Punkt wejściowy Strefy B.
- AP2 jako Punkt wyjściowy Strefy B.
- AP3 jako Punkt wejściowy Strefy C.
- AP5 jako Punkt wyjściowy Strefy C.
- AP6 jako Punkt wejściowy Strefy D.
- AP4 jako Punkt wyjściowy Strefy D.

Punkt dostępu AP3 określa sąsiedztwo Stref A i C.
Punkt dostępu AP4 określa sąsiedztwo Stref B i D.
Strefy A i D nie są strefami sąsiednimi.
Strefy B i C nie są strefami sąsiednimi.
Strefy A i B nie są strefami sąsiednimi.
Strefy C i D nie są strefami sąsiednimi.

- Załącz opcję *Blokuj wejście ze Strefy dostępu która nie jest sąsiednia* dla Stref B i C albo załącz opcję *Blokuj wyjście do Strefy dostępu która nie jest sąsiednia* dla Stref B i C. W obu przypadkach efekt będzie taki sam.
- Prześlij ustawienia do kontrolera.

Przykład 3

Zgodnie z poniższym rysunkiem, użytkownik z Uprawnieniami dostępu na wszystkich trzech przejściach może wejść do Pomieszczenia 3 tylko wtedy jeżeli wcześniej odwiedził Pomieszczenie 2 i zidentyfikował się na Punkcie dostępu AP4. W tym przykładzie fizycznie istniejącemu Pomieszczeniu 1 odpowiadają logicznie dwie Strefy dostępu A i C z Punktami wejściowymi odpowiednio AP1 i AP4.



Aby skonfigurować ograniczenia w przemieszczeniu użytkowników zgodnie z Przykładem 3:

- Skonfiguruj wszystkie trzy Przejścia za pomocą *Kreatora przejścia* z uwzględnieniem wszystkich Uprawnień dostępu.
- Zdefiniuj użytkownika za pomocą kreatora *Dodaj Osobę online* przypisując Nośnik(i) oraz wszystkie Uprawnienia dostępu.
- Skonfiguruj cztery Strefy dostępu przypisując:
  - AP1 jako Punkt wejściowy Strefy A.
  - AP2 i AP3 jako Punkty wyjściowe Strefy A.
  - AP3 jako Punkt wejściowy Strefy B.
  - AP4 jako Punkt wyjściowy Strefy B.
  - AP4 i AP6 jako Punkty wejściowe Strefy C.
  - AP5 jako Punkt wyjściowy Strefy C.
  - AP5 jako Punkt wejściowy Strefy D.
  - AP6 jako Punkt wyjściowy Strefy D.

  Punkt dostępu AP3 określa sąsiedztwo Stref A i B.
  Punkt dostępu AP4 określa sąsiedztwo Stref B i C.
  Punkt dostępu AP5 (jak też AP6) określa sąsiedztwo Stref C i D.
  Strefy A i D nie są strefami sąsiednimi.
  Strefy B i D nie są strefami sąsiednimi.
  Strefy A i C nie są strefami sąsiednimi.
- Załącz opcję *Blokuj wejście ze Strefy dostępu która nie jest sąsiednia* dla Strefy D.
- Prześlij ustawienia do kontrolera.

Dodatkowa kontrola dostępu na przejściach wewnętrznych strefy

Definicja Strefy dostępu wymaga przypisania Punktów wejściowych oraz wyjściowych. Dodatkowo można również zdefiniować Punkty wewnętrzne. Zasada ich funkcjonowania polega na tym, że użytkownik bez względu na swoje Uprawnienia nie może uzyskać dostępu na Punktach wewnętrznych strefy jeżeli wg systemu nie znajduje się wewnątrz tej strefy czyli nie zidentyfikował się na jednym z jej Punktów wejściowych. Ten mechanizm ma zapobiegać sytuacjom, w których użytkownik posiadający Uprawnienia do poruszania się po obiekcie, celowo lub nieumyślnie pominął identyfikację na Punktach wejściowych stosowanych przykładowo do rejestracji czasu pracy.

Punkty wewnętrzne definiuje się tak samo jak Punkty wejściowe i wyjściowe strefy czyli poprzez przypisanie istniejących w systemie Punktów identyfikacji obejmujących czytniki kontroli dostępu. Wymogi związane z Punktami wewnętrznymi mają wpływ na ruch użytkowników wyłącznie w przypadku gdy ruch ten odbywa się pomiędzy Strefami dostępu. Jeśli przejście odbywa się z obszaru, lub do obszaru który nie jest objęty żadną Strefą dostępu to te wymogi nie mają zastosowania. Gdy Identyfikator użytkownika ma załączoną opcję *Nie zaliczany do obecnych* to taki użytkownik nie musi przestrzegać zasad związanych z Punktami wewnętrznymi.

Przykład 4

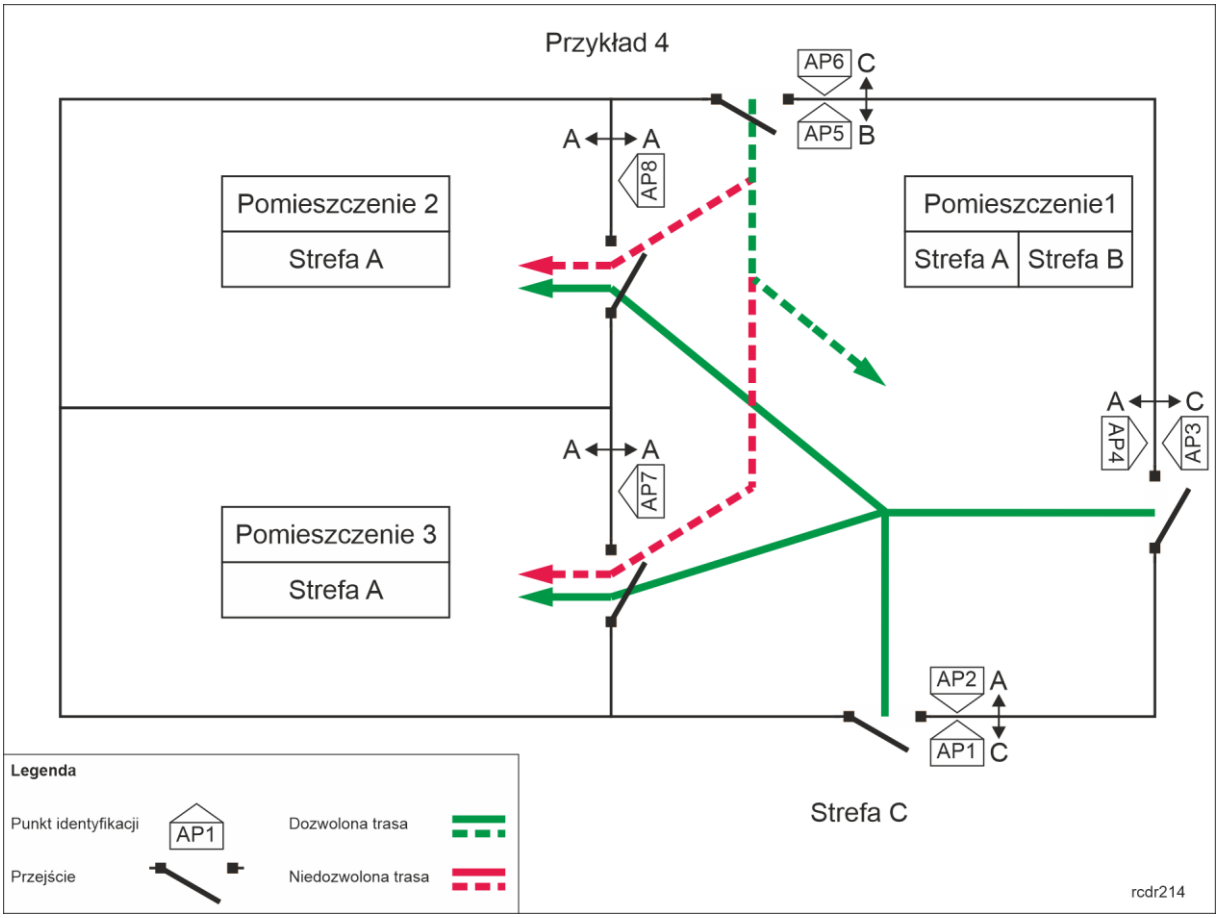
Zgodnie z poniższym rysunkiem, użytkownik z Uprawnieniami dostępu na wszystkich czterech przejściach może wejść do Pomieszczeń 2 i 3 tylko wtedy jeżeli wcześniej wszedł do Pomieszczenia 1 identyfikując się na Punkcie identyfikacji AP1 lub AP3. W poniższym przykładzie Punkty identyfikacji AP7 i AP8 to Punkty wewnętrzne Strefy A, na których można uzyskać dostęp jedynie wtedy gdy użytkownik prawidłowo wszedł do Strefy A (bez pomijania Punktów wejściowych wchodząc za innym użytkownikiem). Dodatkowo ustawione zostało, że użytkownik identyfikując się na Punkcie identyfikacji AP6 wchodzi do Strefy B i wtedy też nie może uzyskać dostępu na Punktach identyfikacji AP7 i AP8.

Aby skonfigurować ograniczenia w przemieszczeniu użytkowników zgodnie z Przykładem 4:

- Skonfiguruj wszystkie pięć Przejść za pomocą *Kreatora przejścia* z uwzględnieniem wszystkich Uprawnień dostępu.
- Zdefiniuj użytkownika za pomocą kreatora *Dodaj Osobę online* przypisując Nośnik(i) oraz wszystkie Uprawnienia dostępu.
- Skonfiguruj trzy Strefy dostępu przypisując:

- AP1 i AP3 jako Punkty wejściowe Strefy A.
- AP2 i AP4 jako Punkty wyjściowe Strefy A.
- AP7 i AP8 jako Punkty wewnętrzne Strefy A.
- AP6 jako Punkt wejściowy Strefy B.
- AP5 jako Punkt wyjściowy Strefy B.
- AP2, AP4 i AP5 jako Punkty wejściowe Strefy C.
- AP1, AP3 i AP6 jako Punkty wyjściowe Strefy C.

- Prześlij ustawienia do kontrolera.



Strefy obwodowe

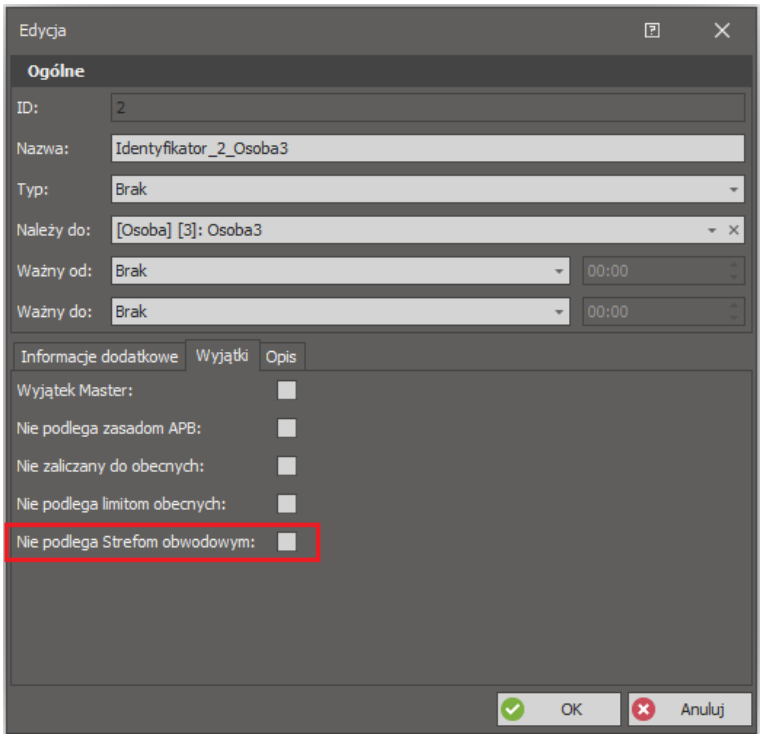
Strefy obwodowe podobnie jak Strefy dostępu obejmują Punkty wejściowe, wyjściowe oraz wewnętrzne. W Strefach obwodowych wykorzystuje się przede wszystkim możliwość definiowania Punktów wewnętrznych, które funkcjonują tak jak Punkty wewnętrzne w Strefach dostępu. Różnica polega na tym, że mogą one być definiowane na poziomie całego systemu a nie pojedynczego kontrolera dostępu bo za ich funkcjonowanie odpowiada Serwer komunikacji z pakietu oprogramowania RogerSVC.

Zasada funkcjonowania Punktów wewnętrznych polega na tym, że użytkownik bez względu na swoje Uprawnienia nie może uzyskać dostępu na Punktach wewnętrznych strefy jeżeli wg systemu nie znajduje się wewnątrz tej strefy czyli nie zidentyfikował się na jednym z jej Punktów wejściowych. Ten mechanizm ma zapobiegać sytuacjom, w których użytkownik posiadający Uprawnienia do poruszania się po obiekcie, celowo lub nieumyślnie pominął identyfikację na Punktach wejściowych stosowanych przykładowo do rejestracji czasu pracy.

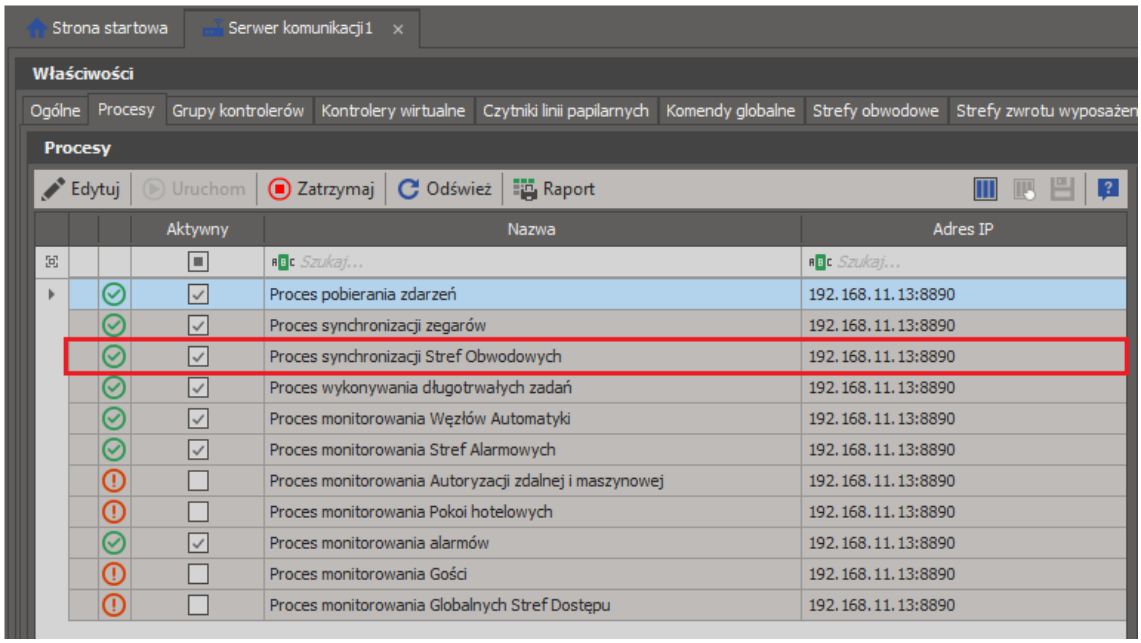
Aby zdefiniować Strefę obwodową:

- Skonfiguruj wszystkie wymagane Przejścia za pomocą *Kreatora przejścia* z uwzględnieniem wszystkich Uprawnień dostępu.
- Zdefiniuj użytkowników za pomocą kreatora *Dodaj Osobę online* przypisując Nośnik(i) oraz wszystkie Uprawnienia dostępu.
- W drzewku nawigacyjnym programu VISO w ramach danego Serwera komunikacji dwukrotnie kliknij polecenie *Strefy obwodowe* lewym przyciskiem myszki.
- W nowo otwartym oknie wybierz przycisk *Dodaj*, nadaj strefie nazwę i następnie kliknij przycisk *OK*.
- W dolnej części okna zdefiniuj Punkty wejściowe, wyjściowe i Punkty wewnętrzne wybierając wcześniej zdefiniowane w systemie Punkty identyfikacji.
- Prześlij ustawienia do systemu.

W przypadku Stref obwodowych istnieje możliwość ustawienia wyjątku *Nie podlega Strefom Obwodowym* we właściwościach Identyfikatora. Użytkownika z takim Identyfikatorem nie obowiązują ograniczenia na poziomie Strefy obwodowej. Opcja *Wyjątek Master* zawiera w sobie wszystkie pozostałe wyjątki i dodatkowo nadaje wszystkie możliwe Uprawnienia w systemie.



Strefy obwodowe wymagają uruchomionego Procesu synchronizacji Stref obwodowych, który jest dostępny w zakładce *Procesy* po dwukrotnym kliknięciu Serwera komunikacji w drzewku nawigacyjnym programu VISO.



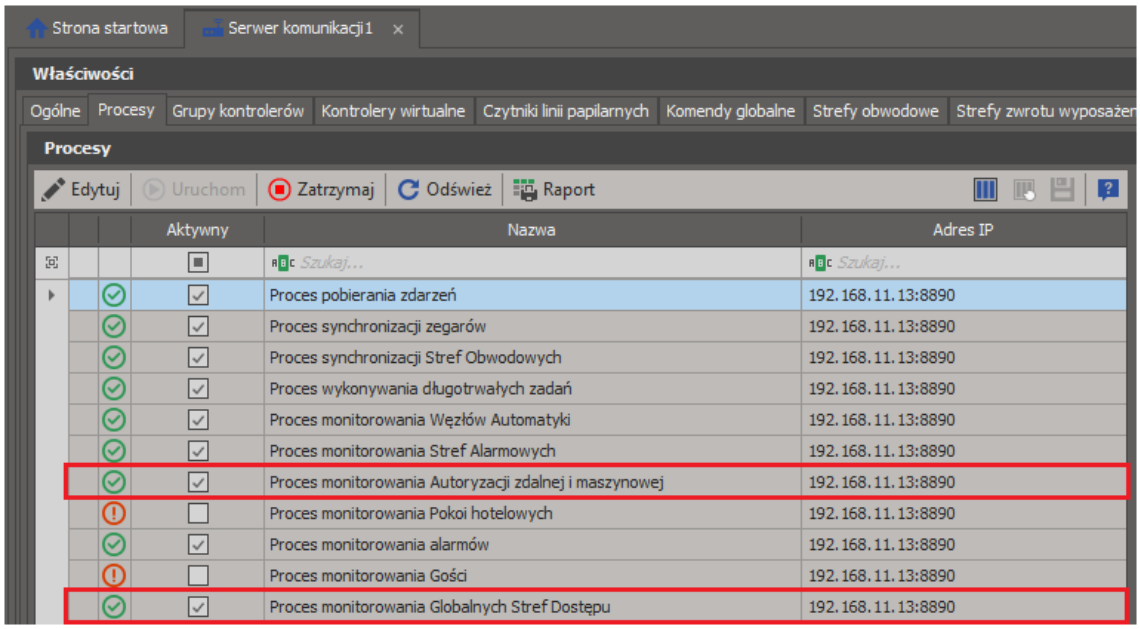
Globalne strefy dostępu

Globalne strefy dostępu obejmują Punkty wejściowe i wyjściowe. Strefy te są wykorzystywane do realizacji Globalnego Anti-passbacku ale w odróżnieniu od Stref dostępu nie są one ograniczone do pojedynczego kontrolera i mogą być definiowane na poziomie całego systemu bo za ich funkcjonowanie odpowiada Serwer komunikacji z pakietu oprogramowania RogerSVC.

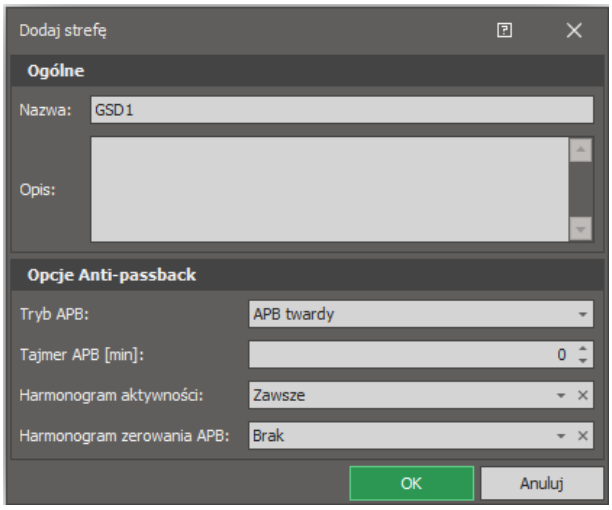
Funkcja Anti-passback (APB) zapobiega dwukrotnemu zastosowaniu tego samego Identyfikatora (np. karty) na Punktach wejściowych do strefy i wymusza naprzemienne stosowanie danego Identyfikatora na Punktach wejściowych i wyjściowych. Funkcja APB ma zapobiegać nieuprawnionemu przekazywaniu kart pomiędzy użytkownikami w celu uzyskania wielokrotnego dostępu do danej strefy za pomocą tego samego Identyfikatora i znajduje ona swoje zastosowanie np. na płatnych parkingach.

Aby zdefiniować Globalną strefę dostępu:

- Kliknij dwukrotnie dany Serwer komunikacji w drzewku nawigacyjnym VISO.
- Przejdź do zakładki *Procesy* i uaktywnij *Proces monitorowania Autoryzacji zdalnej i maszynowej* oraz *Proces monitorowania Globalnych Stref Dostępu*.

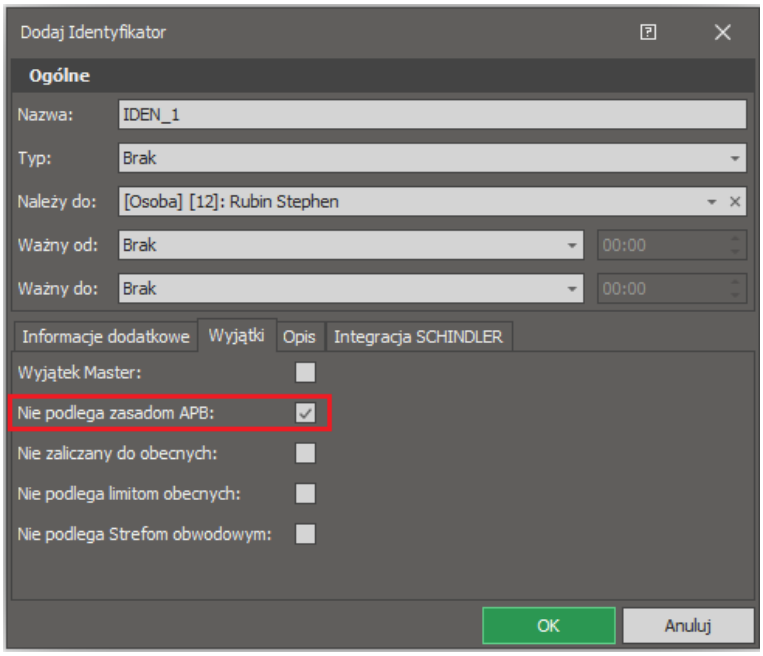


- Kliknij dwukrotnie *Globalne strefy dostępu* w ramach danego Serwera komunikacji w drzewku nawigacyjnym programu VISO.
- W otwartym oknie wybierz *Dodaj*.
- W kolejnym oknie nadaj nazwę strefie, załącz APB i ewentualnie pozostałe parametry strefy. Opcje Anti-passbacku funkcjonują tak samo jak wcześniej opisane opcje Anti-passback dla Strefy dostępu. Zamknij okno przyciskiem *OK*.



- W dolnej części okna zdefiniuj Punkty wejściowe i wyjściowe wybierając wcześniej zdefiniowane w systemie Punkty identyfikacji.
- Prześlij ustawienia do systemu.

Identyfikator danego użytkownika może zostać wyłączony z działania funkcji APB poprzez załączenie opcji *Nie podlega zasadom APB* we właściwościach Identyfikatora. Podobnie zadziała opcja *Wyjątek Master*, która zawiera w sobie wszystkie pozostałe wyjątki i dodatkowo nadaje wszystkie możliwe Uprawnienia w systemie.


Dodaj Identyfikator
Ogólne
Nazwa:
IDEN_1
Typ:
Brak
Należy do:
[Osoba] [12]: Rubin Stephen
Ważny od:
Brak
00:00
Ważny do:
Brak
00:00
Informacje dodatkowe
Wyjątki
Opis
Integracja SCHINDLER
Wyjątek Master:
Nie podlega zasadom APB:
Nie zaliczany do obecnych:
Nie podlega limitom obecnych:
Nie podlega Strefom obwodowym:
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