Access Management System

AMS configuration and operation

pl Instrukcja obsługi oprogramowania

Spis treści

1 Korzystanie z pomocy

Jak korzystać z tego pliku pomocy.

Przyciski na pasku narzędzi

Przycisk	Funkcja	Opis
	Ukryj	Kliknij ten przycisk, aby ukryć panel nawigacyjny (wraz z kartami Spis treści, Indeks i Wyszukaj), pozostawiając na ekranie jedynie panel pomocy.
	Show (Pokaż)	Po kliknięciu przycisku Ukryj zostaje on zastąpiony przyciskiem Pokaż. Kliknięcie tego przycisku umożliwia ponowne wyświetlenie panelu nawigacyjnego.
	Wstecz	Klikając ten przycisk, można się cofać do wyświetlanych ostatnio stron pomocy.
	Dalej	Klikając ten przycisk, można przeglądać kolejne strony pomocy.
	Drukuj	Przycisk ten służy do drukowania. Do wyboru są opcje: „Drukuj wybrany temat” oraz „Drukuj wybrany nagłówek i wszystkie tematy podrzędne”.

Karty

Spis treści Karta ta zawiera przedstawiony hierarchicznie spis treści. Kliknij ikonę książki  , aby ją otworzyć  , a następnie kliknij ikonę tematu  , aby obejrzeć dany temat.

Index (Indeks) Karta ta zawiera indeks haseł w kolejności alfabetycznej. Wybierz temat z listy lub wpisz słowo kluczowe, aby znaleźć temat/tematy zawierające dane słowo kluczowe.

Search (Wyszukaj) Karta ta umożliwia wyszukiwanie dowolnego tekstu. Wpisz tekst w polu i kliknij przycisk **List Topics (Lista tematów)**, aby wyświetlić tematy zawierające wszystkie podane słowa.

Zmiana rozmiaru okna pomocy

Przeciągnij róg lub krawędź okna do pożądanego rozmiaru.

Dalsze konwencje użyte w tej dokumentacji

- Elementy interfejsu użytkownika (etykiety) są **wytłuszczone**.
  Np. **Tools (Narzędzia), File (Plik), Save As (Zapisz jako)...**
- Sekwencje kliknięć są łączone w ciąg za pomocą znaku **>** (znak większości).
  Np. **File (Plik) > New (Nowy) > Folder**

- Zmiany typu elementu sterującego (np. menu, przycisk opcji, pole wyboru, karta) w sekwencji są wskazywane tuż przed etykietą danego elementu sterującego.
  Np. Kliknij menu: **Dodatki > Opcje >** karta: **Widok**
- Kombinacje klawiszy są zapisywane na dwa sposoby:
  - Ctrl+Z oznacza, że należy wcisnąć i przytrzymać pierwszy klawisz, naciskając jednocześnie drugi.
  - Alt, C oznacza, że należy wcisnąć i zwolnić pierwszy klawisz, a następnie nacisnąć drugi.
- Funkcje przycisków w postaci ikon są dodawane w nawiasach kwadratowych za samą ikoną.
  Np. [Zapisz]

2 Informacje o tym dokumencie

To jest główny podręcznik obsługi oprogramowania Access Management System.
Omawia korzystanie z głównego programu do zarządzania oknami dialogowymi, zwanego dalej AMS.

– Konfiguracja systemu kontroli dostępu w systemie AMS.
– Obsługa skonfigurowanego systemu przez operatorów.

Pokrewna dokumentacja

Następujące zagadnienia omówiono w osobnych dokumentach:

– Instalacja systemu AMS i jego programów pomocniczych.
– Obsługa programu AMS - Map View.

3 Przegląd systemu AMS

Access Management System to zaawansowany, specjalistyczny system kontroli dostępu, który pracuje niezależnie lub we współpracy z BVMS — flagowym systemem Bosch do zarządzania danymi wizyjnymi.
Jego siła wynika z wyjątkowego połączenia najnowocześniejszych technologii z technologiami już sprawdzonymi:

- Zaprojektowany z myślą o użyteczności: praktyczny interfejs użytkownika z aplikacją Map View obsługującą metodę „przeciągnij i upuść” oraz zoptymalizowane okna dialogowe rejestracji biometrycznej.
- Zaprojektowany z myślą o bezpieczeństwie danych: obsługuje najnowsze standardy (EU-GDPR 2018), systemy operacyjne, systemy bazodanowe i szyfrowane interfejsy systemowe.
- Zaprojektowany z myślą o odporności na błędy: główne kontrolery dostępu działające w warstwie pośredniej zapewniają automatyczne przełączanie awaryjne i uzupełnianie funkcjonalności lokalnych kontrolerów dostępu w przypadku awarii sieci.
- Zaprojektowany z myślą o przyszłości: regularne aktualizacje i innowacyjne ulepszenia.
- Zaprojektowany pod kątem skalowalności: można go skonfigurować do obsługi małej i dużej liczby użytkowników.
- Zaprojektowany pod kątem współdziałania: interfejsy API typu RESTful umożliwiające współpracę z systemem Bosch do zarządzania danymi wizyjnymi, systemami obsługi zdarzeń i specjalistycznymi rozwiązaniami naszych partnerów.
- Zaprojektowany z myślą o ochronie inwestycji: może pracować na bazie zainstalowanych urządzeń kontroli dostępu, przy okazji poprawiając ich efektywność.

4 Licencjonowanie systemu

Wymagania wstępne

– System został pomyślnie zainstalowany.
– Jesteś użytkownikiem zalogowanym na komputerze serwera systemu AMS, najlepiej jako Administrator.

Procedura dla zakupionych licencji

Wymagania wstępne : Kupiono licencje na podstawie sygnatury tego komputera. Aby uzyskać instrukcje, skontaktuj się z przedstawicielem handlowym.
Ścieżka w oknie dialogowym: **Konfiguracja** > **Licencje**

1. Zaloguj się do systemu zarządzania dostępem AMS.
   Uwaga: Jeśli system AMS jest zainstalowany w folderze Program Files w systemie Windows, zaloguj się przy użyciu praw administratora systemu Windows.
2. Wybierz kolejno opcje **Konfiguracja** > **Licencje**.
3. Kliknij opcję **Uruchom Menedżera licencji**.
4. W oknie **Menedżer licencji** zaznacz pole wyboru zakupionego pakietu podstawowego.
5. W wyskakującym oknie **Aktywacja licencji**:
   – Wklej **sygnaturę komputera** serwera programu Access Manager.
   – Wklej **klucz aktywacji licencji** otrzymany dla pakietu podstawowego.
   – Kliknij przycisk **Aktywuj...**
6. W oknie **Menedżer licencji** sprawdź, czy pakiet podstawowy, na który właśnie aktywowano licencję, ma teraz status **Ważna aktywacja**.
7. W oknie **Menedżer licencji** :
   – Kliknij opcję **Importuj informacje o pakiecie**, a następnie przejrzyj i aktywuj pakiety licencji kupione i otrzymane w formie plików.
   – Kliknij opcję **Importuj licencję**, a następnie przejrzyj i aktywuj poszczególne licencje kupione i otrzymane w formie plików.
8. Kliknij przycisk **Zamknij**, aby zamknąć **Menedżera licencji**.
9. Po powrocie do głównego okna dialogowego **Licencje** sprawdź, czy kupione funkcje są wyświetlane z odpowiednimi liczbami jednostek.

Procedura dla trybu demonstracyjnego

Tryb demonstracyjny przyznaje licencje do wszystkich funkcji systemu na ograniczony czas. Trybu demonstracyjnego należy używać tylko w środowiskach nieprodukcyjnych, aby wypróbować funkcje przed ich zakupem.

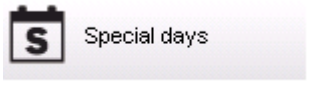
1. Zaloguj się do programu Access Manager.
2. Wybierz kolejno opcje **Konfiguracja** > **Licencje**.
3. Kliknij przycisk **Aktywuj tryb demonstracyjny**.
4. Sprawdź, czy funkcje są wyświetlane w oknie dialogowym **Licencje**.

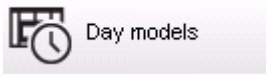
Tryb demonstracyjny jest aktywowany na 5 godzin. Czas do końca aktywności trybu jest wyświetlany w górnej części okna dialogowego **Licencje** oraz na paskach tytułu większości okien dialogowych.

5 Konfigurowanie kalendarza

Planowanie czynności kontroli dostępu jest regulowane przez **modele czasowe**.
Model czasowy to abstrakcyjna sekwencja jednego lub więcej dni, z których każdy jest opisany przez **model dzienny**.
Modele czasowe po zastosowaniu do bazowego **kalendarza** systemu kontroli dostępu kontrolują działania.
Kalendarz systemu kontroli dostępu jest oparty na kalendarzu systemu operacyjnego komputera hosta, ale uzupełnia go do **dni specjalne**, które może dowolnie definiować administrator systemu kontroli dostępu.
Dni specjalne można przypisać do określonej daty w kalendarzu lub zdefiniować w odniesieniu do wydarzenia kulturalnego, takiego jak Wielkanoc. Mogą się powtarzać lub nie.
W celu skonfigurowania skutecznego kalendarza dla swojego systemu kontroli dostępu należy wykonać następujące kroki.

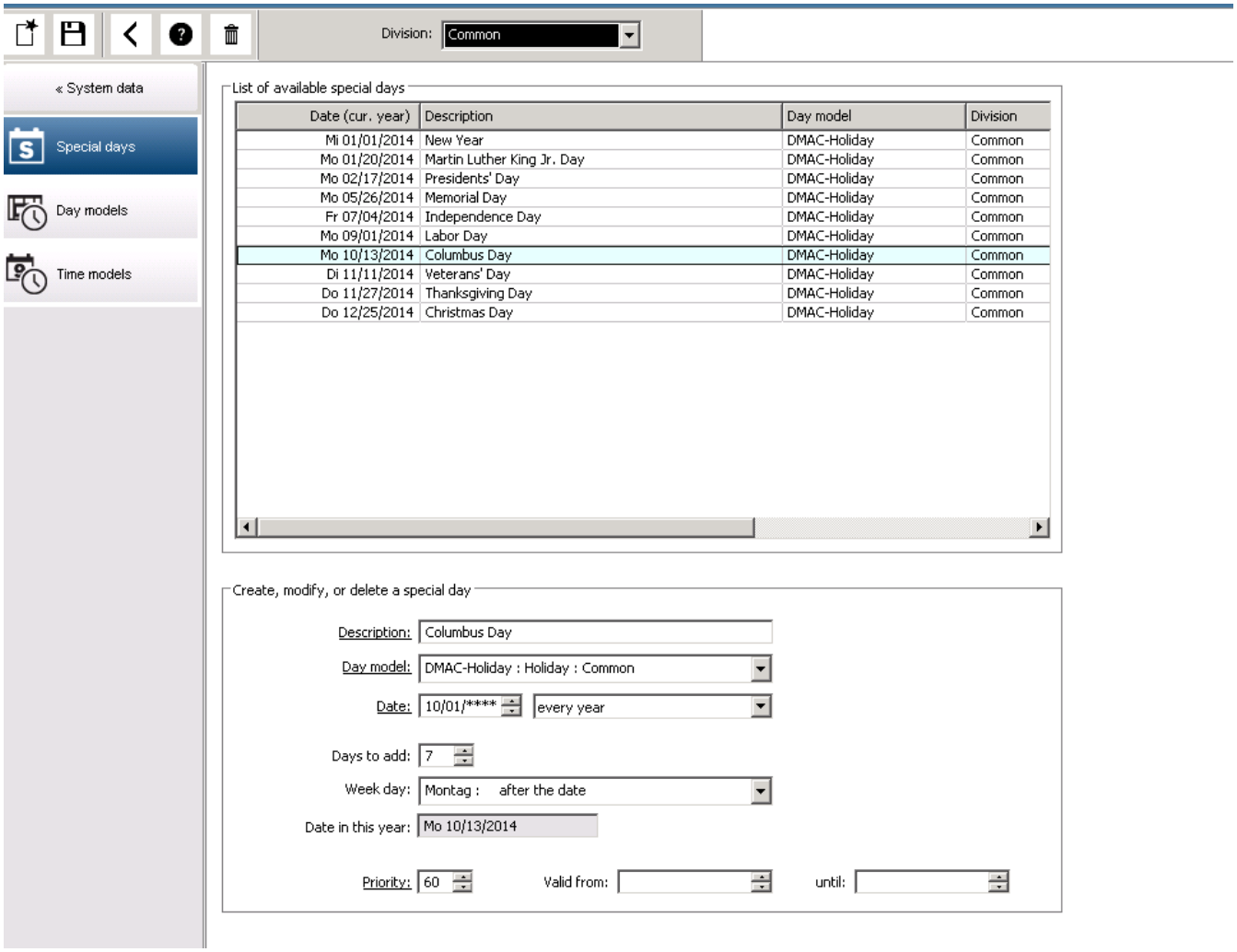
1. Zdefiniuj **dni specjalne** kalendarza dla swojej lokalizacji.
2. Zdefiniuj **modele dzienne**, które opisują aktywne i nieaktywne okresy w każdym typie dnia. Na przykład model dnia dla święta państwowego będzie się różnił od modelu dla zwykłego dnia roboczego. Na rodzaj i liczbę potrzebnych modeli dziennych będzie również wpływać praca zmianowa.
3. Zdefiniuj **modele czasowe** składający się z jednego lub więcej modeli dziennych.
4. Przypisz modele czasowe do posiadaczy kart, uprawnień i wejść.





5.1 Definiowanie dni specjalnych

Po otwarciu tego okna dialogowego w jego w górnym polu listy pojawia się lista wszystkich zdefiniowanych dni świątecznych. Uwaga: wszystkie widoczne daty dni świątecznych odnoszą się tylko do bieżącego roku. Kalendarz jest jednak aktualizowany z roku na rok zgodnie z wprowadzonymi danymi.
Pod listą znajdują się różne pola dialogowe do tworzenia nowych dni specjalnych i modyfikowania lub usuwania dotychczasowych. Aby dodać nowy dzień specjalny, należy wypełnić co najmniej trzy pola wprowadzania danych. Najpierw należy w odpowiednich polach wstawić **opis** i **datę**. Następnie należy na odpowiedniej liście wyboru wskazać **klasę**, do której należy ten dzień specjalny.



Datę określa się w kilku krokach. Po pierwsze w polu **Data** wprowadza się datę podstawową. Na tym etapie data wskazuje zdarzenie w bieżącym roku. Jeśli użytkownik określi teraz na liście wyboru obok pola daty częstotliwość powtarzania, elementy daty objęte cyklicznością zostają zastąpione „symbolami wieloznacznymi” (*).

raz	__.__.____
raz do roku	__.__.****
raz w miesiącu przez okres jednego roku	__.**.____
raz w miesiącu w każdym roku	__.**.****
zależnie od Świąt Wielkanocnych	**.**.****

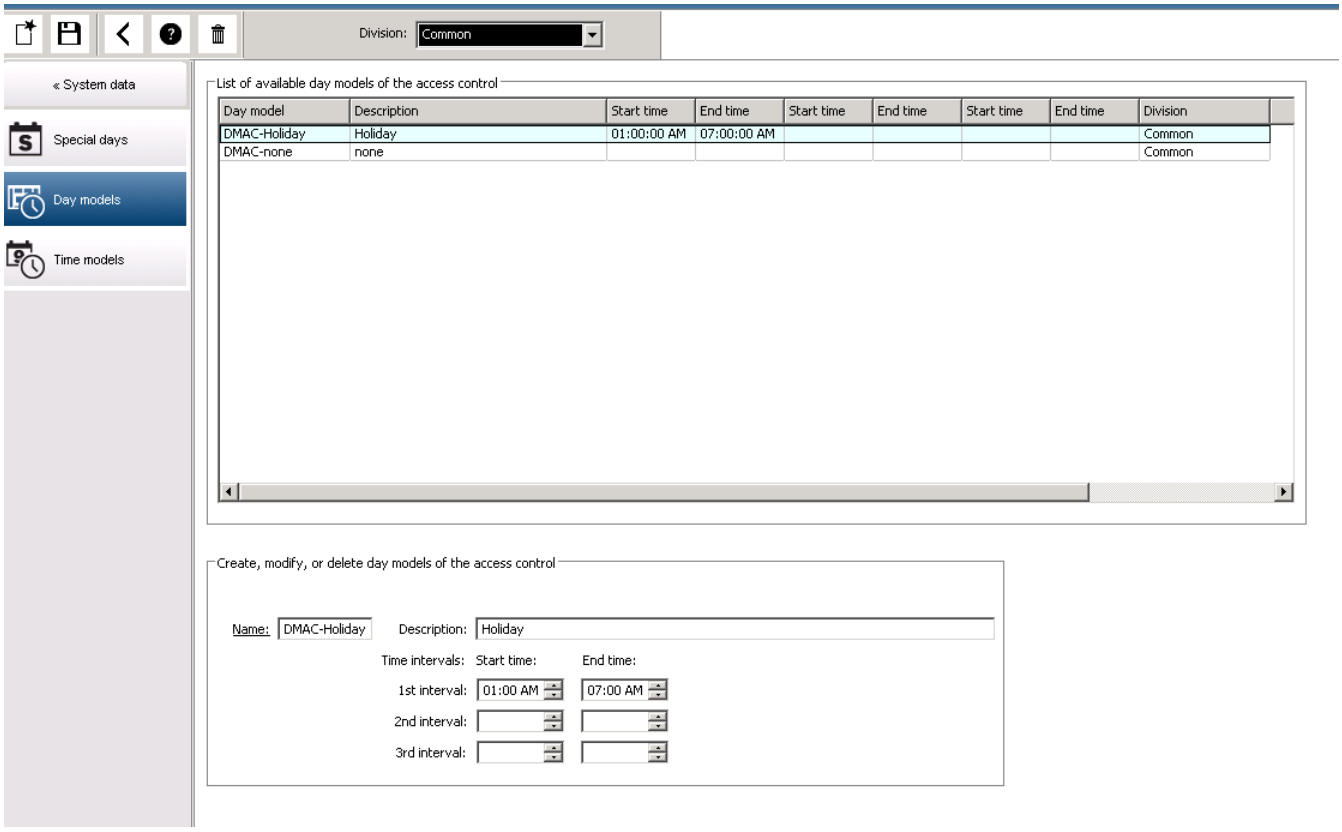
Dni świąteczne, które zależą od Świąt Wielkanocnych, nie są określane za pomocą konkretnej daty, ale poprzez liczbę dni dzielących je od Niedzieli Wielkanocnej. Data Niedzieli Wielkanocnej w bieżącym roku jest podana w polu **Data w tym roku**, a oddalenie od tej daty wprowadza się lub wybiera w polu **Dni do dodania**. Maksymalna liczba dni wynosi 188, więc dodając je lub odejmując, można zdefiniować każdy dzień roku.
Inne dane, np. **dzień tygodnia**, w który przypada dzień świąteczny, są opcjonalne. Należy pamiętać, że lista dni tygodnia jest uzależniona od ustawień regionalnych systemu operacyjnego. Prowadzi to nieuchronnie do wyświetlania danych w różnych językach, jeśli wersja językowa systemu kontroli dostępu odbiega od wersji językowej systemu operacyjnego.

Przypisanie **okresu ważności** również jest opcjonalne. Jeśli nie określono czasu trwania, zgodnie z domyślnymi ustawieniami okres ważności jest nieograniczony od daty wprowadzenia dnia świątecznego.
Można też wyznaczyć **priorytet**. Może on mieć wartość od 1 do 100, a określa, który dzień świąteczny powinien zostać użyty. Jeśli dwa święta przypadają w tym samym dniu, obowiązuje to o wyższym priorytecie. W przypadku równego priorytetu kwestia, którego święta użyć, pozostaje nierozstrzygnięta.
Dni świąteczne o priorytecie „0” są nieaktywne i nie będą używane.
W oknie dialogowym **Modele czasowe** podane są tylko aktywne dni świąteczne, czyli o priorytecie większym od 0.

Uwaga!
Model czasowy strefy „Wspólne” może zawierać tylko dni świąteczne przypisane do tej strefy.
Model czasowy konkretnej strefy „A” może zawierać tylko dni świąteczne przypisane do tej strefy.
Nie można mieszać ze sobą dni świątecznych należących do różnych stref, tzn. w każdej strefie można używać tylko dni świątecznych, które zostały do niej przypisane w ramach danego modelu czasowego.

5.2 Definiowanie modeli dziennych

Modele dzienne określają harmonogram każdego dnia. Mogą zawierać maksymalnie trzy przedziały czasu.
Po otwarciu tego okna dialogowego wyświetlane są wszystkie istniejące już modele czasowe.



W tym oknie dialogowym można wprowadzać i zmieniać nazwy modeli, opisy i przedziały czasu. Kliknięcie ikony  umożliwia skonfigurowanie nowego modelu.
Pory rozpoczęcia i zakończenia przedziałów czasu podaje się w godzinach i minutach. Gdy nadejdzie wyznaczona pora, przedział czasu jest odpowiednio uaktywniany lub dezaktywowany. W celu wyraźniejszego przedstawiania tych pór jako ograniczników są one wyświetlane w okienku listy razem z sekundami (zawsze 00). Przykładowo uprawnienie w modelu czasowym, który zawiera przedział czasu 8:00–15:30, umożliwia dostęp od 8:00 do 15:30, ale blokuje dostęp już o 15:30:01.
Pory rozpoczęcia i zakończenia podlegają sprawdzaniu pod względem logicznym podczas wpisywania, aby np. pora rozpoczęcia była zawsze wcześniejsza od pory zakończenia.
Jedną z konsekwencji jest to, że żaden przedział czasu nie może zawierać północy, tylko musi zostać podzielony o tej godzinie:

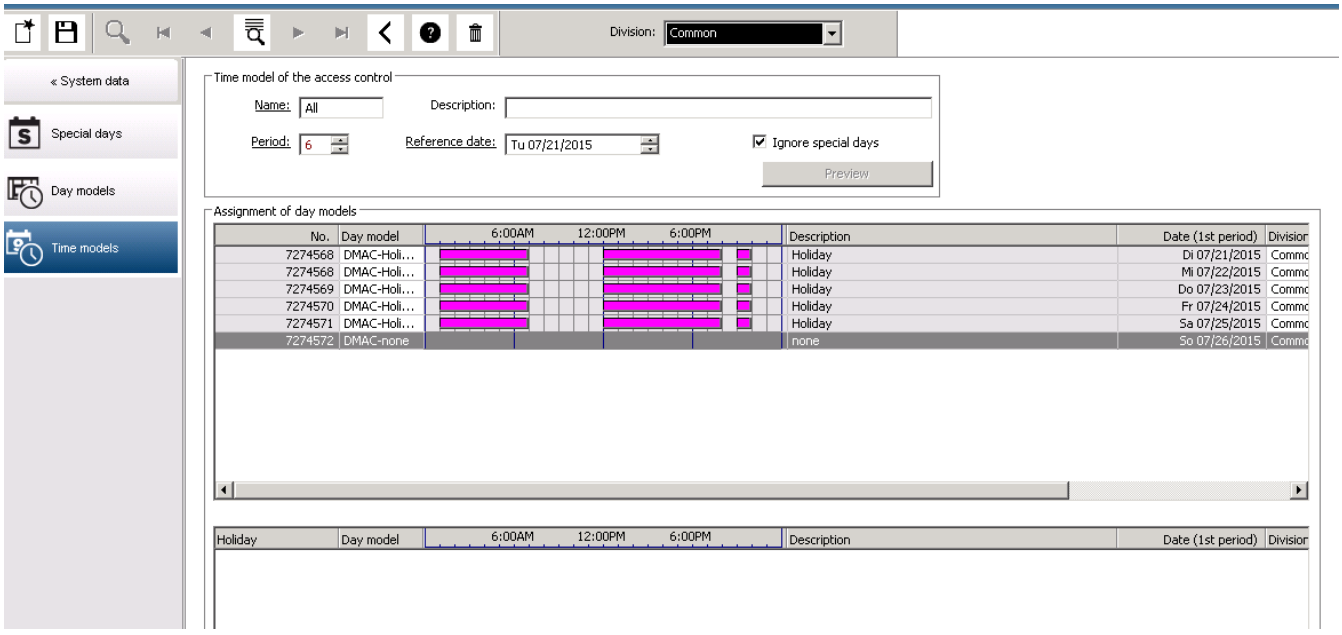
1. przedział czasu	od:	...	do:	24:00
Następny przedział czasu	od:	24:00	do:	...

Z wyjątkiem północy (24:00) ograniczniki przedziałów czasu tego samego modelu czasowego nie mogą się na siebie nakładać. Uwaga: wyklucza to możliwość wprowadzenia tej samej godziny i minuty dla zakończenia jednego przedziału czasu i rozpoczęcia kolejnego.
Wyjątek: 24-godzinny przedział czasu ma jednak porę rozpoczęcia i zakończenia o 24:00.

Uwaga!
Wskazówka: przedziały czasu można sprawdzać, wyświetlając je w oknie dialogowym Modele czasowe. Najpierw należy utworzyć model dzienny zawierający te przedziały czasu (Dane systemowe > Kalendarz > Modele dzienne). Następnie należy przypisać ten model dzienny do testowego modelu czasowego o 1-dniowym okresie trwania (Dane systemowe > Kalendarz > Modele czasowe). Przedziały czasu zostaną przedstawione na wykresie słupkowym.
Należy opuścić okno dialogowe Modele czasowe bez zapisywania zmian.

Model dzienny można usunąć, tylko jeśli nie został jeszcze przypisany do żadnego dnia specjalnego ani nie jest używany przez żaden model czasowy.

5.3 Definiowanie modeli czasowych



Utworzone modele czasowe można wybierać z listy wyszukiwania, a ich szczegóły pojawiają się w polach dialogowych. Wszelkie modyfikacje wprowadza się bezpośrednio w tym widoku w sposób analogiczny do tworzenia nowych modeli czasowych.

Jeśli maska jest pusta, modele czasowe można tworzyć od zera. W tym celu należy wprowadzić **nazwę** i liczbę dni trwania **okresu** oraz wybrać datę początkową lub **datę odniesienia**. Po potwierdzeniu tych danych (klawiszem **Enter**) pojawi się poniżej lista w polu dialogowym **Przypisywanie modeli dziennych**. Liczba wierszy na tej liście odpowiada określonej powyżej liczbie dni, a kolumny zawierają już numer porządkowy i daty okresu, zaczynające się od wybranej daty początkowej.

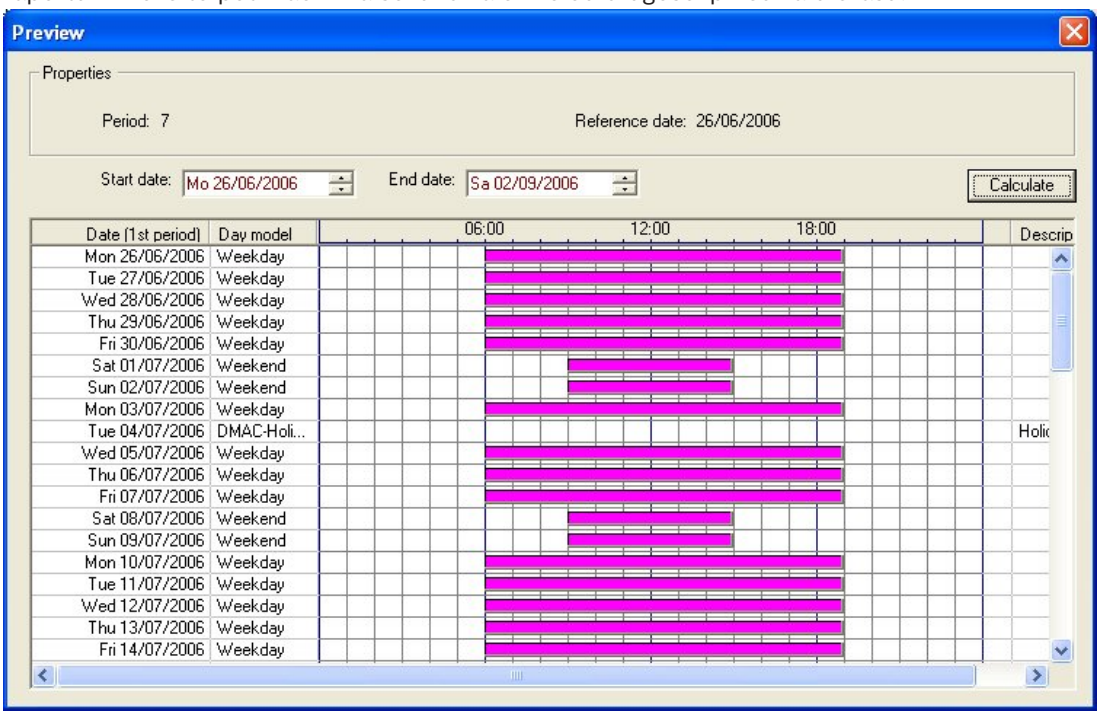
Na tej liście użytkownik może zmieniać lub wstawiać tylko pozycje w kolumnie **„Nazwa”**. Jak już wspomniano, pozycje w kolumnach **„Nr”** i **„Data”** wynikają z deklaracji w nagłówku okna dialogowego. Kolumna **„Opis”** jest wypełniana przez system po wybraniu modelu dziennego z użyciem objaśnień wprowadzonych w jego oknie dialogowym.

Dwukrotne kliknięcie danego wiersza w kolumnie **Model dzienny** powoduje uaktywnienie pola listy wyboru. Z listy można wybrać jeden z utworzonych modeli dziennych. W ten sposób można przypisywać konkretny model dzienny poszczególnym dniom okresu. Po przejściu przez użytkownika do innego wiersza obecny opis wybranego modelu dziennego jest wskazywany przez system w kolumnie **Opis**.

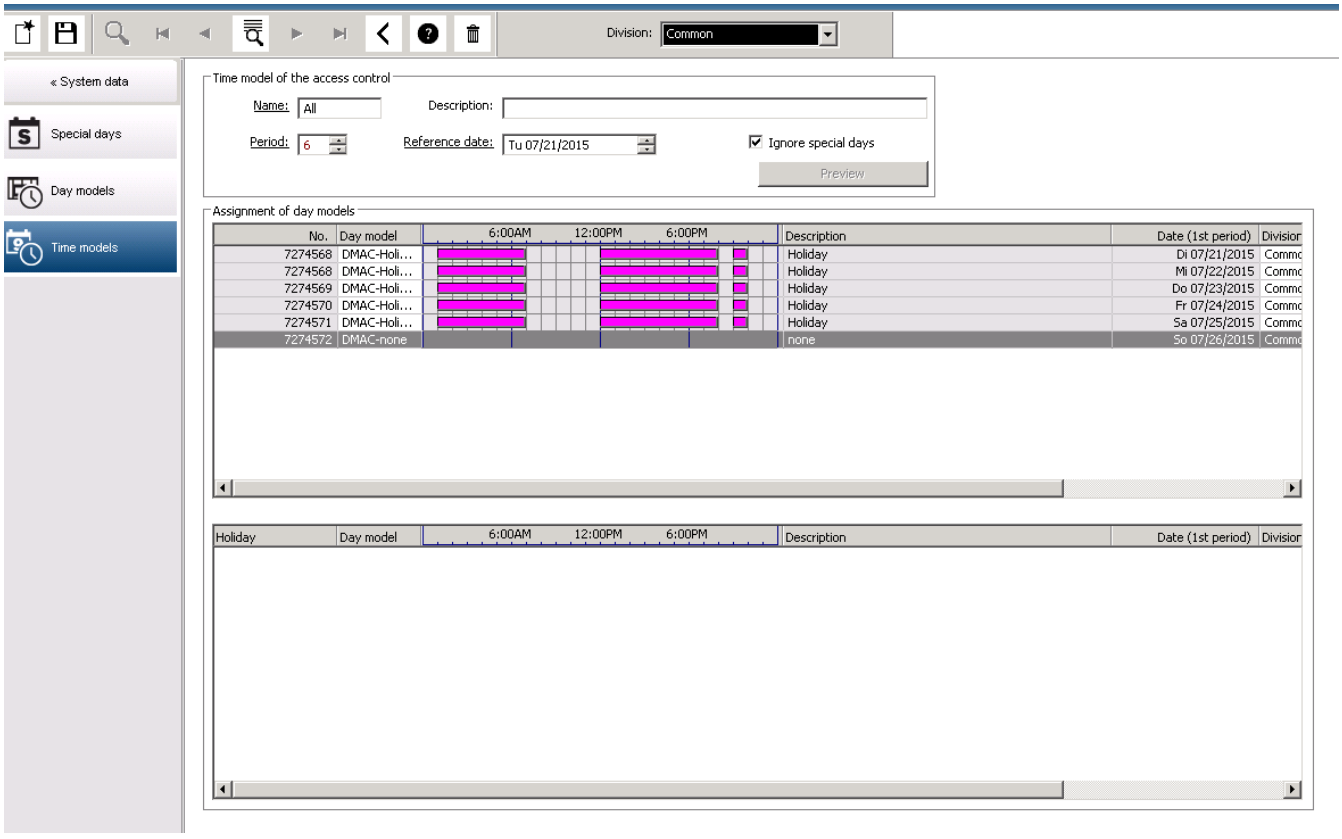
Wstępnie zdefiniowane **dni świąteczne** z odpowiednimi modelami dziennymi są wyświetlane w dolnym polu listy, aby umożliwiać łatwe poruszanie się po modelu i jego sprawdzanie. W przypadku wybranego lub nowo utworzonego modelu czasowego można zmieniać przypisanie modeli dziennych do określonych dni świątecznych. Jednak zmiany te będą mieć zastosowanie tylko do tego konkretnego modelu czasowego. Ogólne zmiany, które mają obowiązywać w przypadku wszystkich istniejących już i przyszłych modeli, można wprowadzać tylko w oknie dialogowym Wakacje. Zgodnie z tymi ustawieniami dniom tygodnia przypisywane są następnie modele dzienne z uwzględnieniem dni świątecznych.

Zgodnie z tymi ustawieniami dniom tygodnia przypisywane są modele dzienne z uwzględnieniem dni specjalnych. Aby umożliwić szybkie sprawdzanie, czy modele dzienne zostały prawidłowo użyte i przypisane — zwłaszcza w odniesieniu do dni świątecznych — udostępniono w tym oknie dialogowym funkcję **podglądu**, która podaje przydział dni w wybranych okresach.

I wreszcie, po kliknięciu przycisku **Podgląd** pojawia się osobne okno dialogowe, w którym można wyznaczyć okres obejmujący maksymalnie 90 dni, łącznie z dniami świątecznymi. Po kliknięciu przycisku **Oblicz** następuje wygenerowanie i wyświetlenie widocznego poniżej raportu – może to potrwać kilka sekund zależnie od długości przedziału czasu.



Przy ustawieniu domyślnym dni specjalne są stosowane w modelach czasowych zgodnie z ich definicjami. Jeśli jednak okaże się, że na podglądzie nie uwzględniono dni specjalnych, może to być spowodowane wybraniem opcji **Ignoruj dni specjalne**. Jednocześnie usuwane są pozycje na dwóch dolnych listach, przez co użytkownik orientuje się natychmiast, że dni specjalne i klasy dzienne nie mają zastosowania w tym modelu.


Division:
Common
« System data
Special days
Day models
Time models
Time model of the access control
Name:
All
Description:
Period:
6
Reference date:
Tu 07/21/2015
Ignore special days
Preview
Assignment of day models
No.
Day model
6:00AM
12:00PM
6:00PM
Description
Date (1st period)
Division
7274568 DMAC-Holi... Holiday Di 07/21/2015 Commc
7274568 DMAC-Holi... Holiday Mi 07/22/2015 Commc
7274569 DMAC-Holi... Holiday Do 07/23/2015 Commc
7274570 DMAC-Holi... Holiday Fr 07/24/2015 Commc
7274571 DMAC-Holi... Holiday Sa 07/25/2015 Commc
7274572 DMAC-none none So 07/26/2015 Commc
Holiday
Day model
6:00AM
12:00PM
6:00PM
Description
Date (1st period)
Division

6 Konfigurowanie stref

Wstęp

Opcjonalnie do systemu można dokupić licencję na wspólną kontrolę dostępu do obiektu. Taka licencja umożliwia nadzorowanie niezależnych jednostek nazywanych **dywizjami**. Operatorom systemu można przypisać jedną lub więcej dywizji. Operatorzy widzą wtedy tylko osoby, urządzenia i wejścia znajdujące się w tych dywizjach.
W razie braku licencji na funkcję **Dywizje** wszystkie obiekty zarządzane przez system należą do jednej dywizji o nazwie **Wspólna**.

Wymagania wstępne

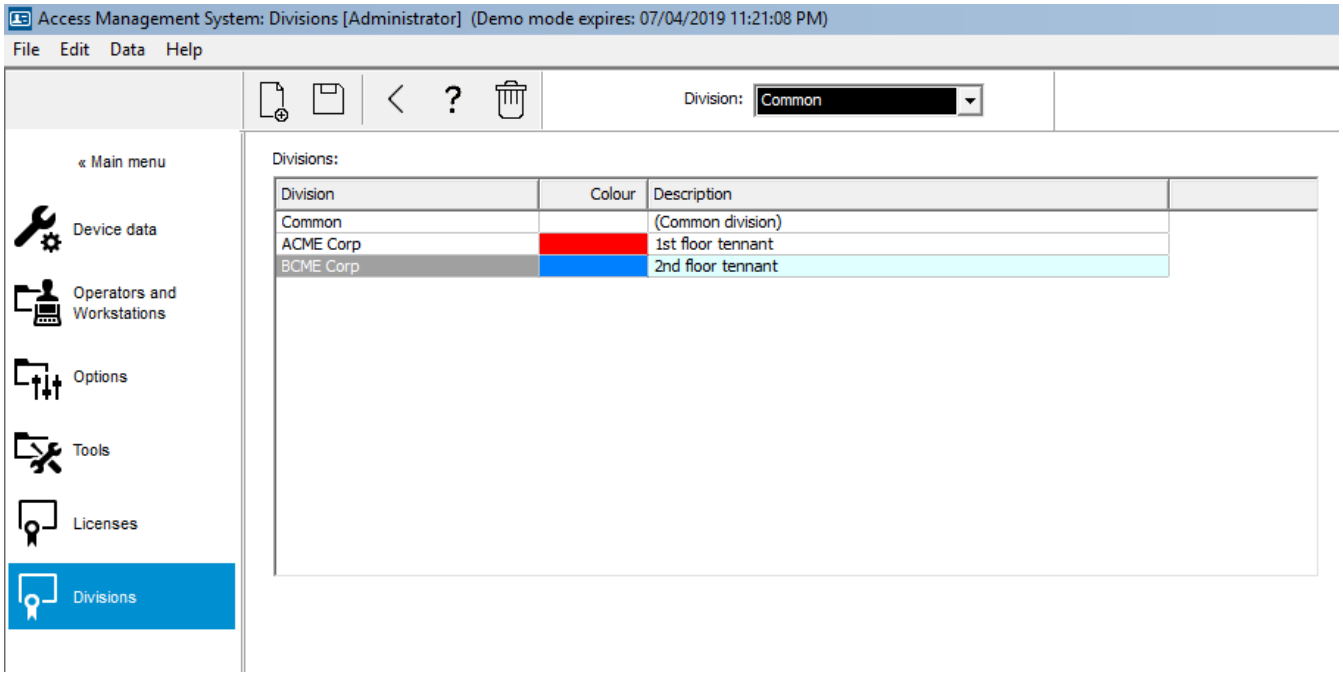
– Wykupienie licencji na funkcję Dywizji dla posiadanej instalacji.

Ścieżka w oknie dialogowym

– Menu główne > **Konfiguracja** > **Strefy**

Procedura

1. Na pasku narzędzi kliknij przycisk .
   – Zostanie utworzona nowa strefa z domyślną nazwą.
2. Zastąp domyślną nazwę i (opcjonalnie) wprowadź opis, który może się przydać innym operatorom.
3. Kliknij kolumnę **Kolor** i przypisz kolor, który ułatwi odróżnianie zasobów strefy w interfejsie użytkownika.
4. Kliknij przycisk , aby zapisać ustawienia.



6.1 Przypisywanie stref do urządzeń

Przypisywanie stref do urządzeń w edytorze urządzeń

Ścieżka w oknie dialogowym

Menu główne > **Konfiguracja** > **Dane urządzenia**

Wymagania wstępne

– Wykupiono licencję na funkcję stref i funkcja działa
– Utworzono co najmniej jedną strefę

Procedura

1. W drzewie urządzeń zaznacz urządzenie, któremu chcesz przypisać strefę.
   – W głównym panelu okna dialogowego pojawi się edytor urządzeń.
2. Na liście Strefy zaznacz nową strefę urządzenia.
   – Nowa strefa pojawi się w polu listy.
3. Kliknij przycisk  (Zapisz), aby zapisać wprowadzone zmiany.

Uwaga!
Wszystkie komponenty wejścia muszą należeć do jednej strefy
System pozwoli na zapisanie wejścia dopiero wtedy, gdy jego wszystkie komponenty będą należały do tej samej strefy.

6.2 Przypisywanie stref do operatorów

Przypisywanie stref do operatorów w oknie dialogowym **Uprawnienia użytkownika**

Ścieżka w oknie dialogowym

Menu główne > **Konfiguracja** > **Operatorzy i stacje robocze > Uprawnienia użytkownika**

Wymagania wstępne

– Wykupiono licencję na funkcję stref i funkcja działa
– Utworzono co najmniej jedną strefę
– W systemie utworzono co najmniej jednego operatora

Procedura

1. W oknie dialogowym **Prawa użytkownika** zaznacz zestaw danych osobowych operatora, któremu ma zostać przypisana strefa.
2. Na karcie **Strefy** za pomocą przycisków strzałek przenieś strefy z listy **Dostępne strefy** do listy **Przypisane strefy** dla tego operatora.
3. Kliknij przycisk  (Zapisz), aby zapisać wprowadzone zmiany.

7 Konfigurowanie adresów IP

Lokalne kontrolery dostępu w sieci wymagają spójnego schematu adresów IP, aby móc uczestniczyć w systemie kontroli dostępu. Narzędzie **AccessIPConfig** znajduje kontrolery w sieci oraz zapewnia wygodny interfejs do centralnego administrowania ich adresami i innymi opcjami sieciowymi.

Wymagania wstępne

– Lokalne kontrolery dostępu są włączone i podłączone do sieci.
– Istnieje uporządkowany schemat adresów IP kontrolerów i ich haseł, jeśli jest to wymagane.

Ścieżka w oknie dialogowym

Menu główne > **Konfiguracja** > **Narzędzia**

Procedura

1. Postępuj zgodnie ze ścieżką w oknie dialogowym podaną wyżej i kliknij opcję **Konfiguracja AMC i urządzeń do obsługi odcisków palców** . Otworzy się narzędzie **AccessIPConfig**.
2. Kliknij opcję **Skanuj w poszukiwaniu AMC** . Zostaną wyświetlone lokalne kontrolery dostępu, których można używać w sieci, każdy z następującymi parametrami:
   – **Adres MAC** : Adres sprzętowy kontrolera. Uwaga: to **nie** jest adres głównego kontrolera dostępu, a zbieżność nazw wynika wyłącznie z przypadku.
   – **Zapisano adres IP**:
   – **Numer portu**: Wartość domyślna to `10001`
   – **DHCP**: Wartością jest **Tak** tylko wtedy, gdy na kontrolerze skonfigurowano otrzymywanie adresu IP z usługi DHCP
   – **Bieżący adres IP**
   – **Numer seryjny**
   – Uwagi dodane przez zespół odpowiedzialny za konfigurację sieci
3. Kliknij dwukrotnie system AMC na liście, aby zmienić jego parametry w wyskakującym oknie. Alternatywnie zaznacz wiersz żądanego systemu AMC i kliknij przycisk **Ustaw IP...**Może być konieczne wprowadzenie hasła, jeśli zostało ono skonfigurowane dla urządzenia.
   Zmodyfikowane parametry zostaną zapisane, gdy tylko klikniesz przycisk OK w wyskakującym oknie.
4. Po zakończeniu konfigurowania parametrów IP kontrolerów kliknij kolejno opcje **Plik** > **Zakończ**, aby zamknąć narzędzie.
   Powrócisz do głównej aplikacji.

Aby uzyskać więcej szczegółowych informacji, kliknij przycisk **Pomoc** w narzędziu **AccessIPConfig**, a zostanie wyświetlony jego własny plik pomocy.

8 Korzystanie z edytora urządzeń

Wstęp

Edytor urządzeń (**DevEdit**) umożliwia dodawanie i usuwanie niewielkiej liczby wejść i urządzeń oraz dodawanie, modyfikowanie i usuwanie poszczególnych parametrów.
W przypadku importowania dużych, istniejących konfiguracji używaj funkcji **Konfiguracja importu/eksportu** dostępnej w ścieżce **Menu główne** > **Konfiguracja** > **Narzędzia**.

Edytor urządzeń oferuje widoki odpowiadające następującym edytowalnym hierarchiom:
- **Konfiguracja urządzeń**: urządzenia elektroniczne w systemie kontroli dostępu.
- **Stacje robocze**: komputery współpracujące w systemie kontroli dostępu.
- **Obszary**: fizyczne obszary, na jakie jest podzielony system kontroli dostępu.

Wymagania wstępne

System jest poprawnie zainstalowany, zaopatrzony w licencje i podłączony do sieci.

Ścieżka w oknie dialogowym

- **Menu główne** > **Konfiguracja** > **Dane urządzenia**

Korzystanie z paska narzędzi DevEdit

Przyciski paska narzędzi DevEdit mają podane funkcje niezależnie od tego, który widok jest aktywny (**Urządzenia**, **Stacje robocze** lub **Obszary**).

Przycisk	Skrót	Opis
	Ctrl+N	Tworzy nowy element pod wybranym węzłem. Alternatywnie kliknij węzeł prawym przyciskiem myszy, aby wywołać jego menu kontekstowe.
	Del	Usuwa zaznaczony element i wszystkie znajdujące się pod nim.
	Ctrl+Page Up	Pierwszy element w drzewie
	Ctrl -	Poprzedni element
	Ctrl +	Następny element
	Ctrl+Page Down	Ostatni element w drzewie
	Ctrl+A	Rozwija i zwija drzewo
	Ctrl+K	Odświeża dane przez ponowne załadowanie ich z bazy danych. **Wszystkie niezapisane zmiany są odrzucane.**
	Ctrl+S	Zapisuje bieżącą konfigurację
	Ctrl+F	Otwiera okno wyszukiwania

		Otwiera drzewo **Konfiguracja urządzeń**
		Otwiera drzewo **Stacje robocze**
		Otwiera drzewo **Obszary**

We wszystkich widokach narzędzia DevEdit należy zaczynać od katalogu głównego w drzewie, a następnie dodawać elementy za pomocą przycisków paska narzędzi, menu lub menu kontekstowego poszczególnych elementów (jego ono wywoływane kliknięciem prawego przycisku myszy). Aby dodać elementy podrzędne do drzewa, najpierw zaznacz element, pod którym elementy podrzędne powinny być wyświetlane.

Po zakończeniu dodawania elementów do drzewa kliknij przycisk **Zapisz**  , aby zapisać konfigurację.
Aby zamknąć narzędzie DevEdit, kliknij kolejno opcje **Plik** > **Zakończ**.

9 Konfigurowanie obszarów kontroli dostępu

Wprowadzenie do obszarów

Chronione budynki można dzielić na obszary. Obszary mogą mieć dowolną wielkość: obejmować jeden lub kilka budynków albo pojedyncze piętra czy nawet pomieszczenia.
Oto niektóre zastosowania obszarów:

- Lokalizacja poszczególnych osób w obrębie chronionego budynku.
- Szacowanie liczby osób znajdujących się na danym obszarze na wypadek ewakuacji lub sytuacji alarmowej.
- Ograniczanie liczby osób lub pojazdów na danym obszarze:
  Po osiągnięciu wyznaczonej wartości granicznej liczebności dalsze próby dostępu mogą być odrzucane do czasu opuszczenia obszaru przez jakieś osoby lub pojazdy.
- Wdrażanie kontroli kolejności dostępu i funkcji zapobiegającej przekazaniu karty niepowołanej osobie

System rozróżnia dwa typy obszarów z kontrolą dostępu

- Obszary dla osób
- Obszary dla pojazdów (parkingi)

Każdy obszar może mieć podobszary umożliwiające bardziej szczegółową kontrolę. Obszary dla osób mogą mieć do 3 poziomów zagnieżdżenia, a obszary parkingowe tylko 2: parking ogółem i strefy parkowania, w liczbie od 1 do 24.
Obszar domyślny, który istnieje we wszystkich instalacjach, nosi nazwę **Na zewnątrz**. Służy jako element nadrzędny dla wszystkich obszarów obu rodzajów — dla osób i parkingowych — zdefiniowanych przez użytkownika.

Aby obszar nadawał się do użytku, musi do niego prowadzić co najmniej jedno wejście.
W edytorze urządzeń **DevEdit** można przypisać każdemu wejściu obszaru lokalizacji i obszar docelowy. Gdy jakaś osoba skanuje kartę w czytniku przynależnym do wejścia, nowa lokalizacja tej osoby staje się obszarem docelowym tego wejścia.

Uwaga!
Kontrola kolejności dostępu i funkcja zapobiegająca przekazaniu karty niepowołanej osobie wymagają obecności czytników wejściowych i wyjściowych przy wejściach do obszarów.
W celu zapobiegania przypadkowemu lub umyślnemu „przemykaniu” przez wejście tuż za inną osobą bez skanowania swojej karty zdecydowanie zaleca się stosowanie wejść w postaci bramek obrotowych.

Procedura tworzenia obszarów

Wymagania wstępne

Jako operator systemu potrzebujesz autoryzacji na tworzenie obszarów od swojego administratora systemu.

Ścieżka w oknie dialogowym (AMS)

1. W menedżerze okien dialogowych AMS wybierz kolejno opcje **Menu główne** > **Konfiguracja** > **Dane urządzenia**.

2. Kliknij opcję Obszary  .
3. Wybierz węzeł **Na zewnątrz** lub jeden z jego elementów podrzędnych, a następnie na pasku narzędzi kliknij przycisk  . Alternatywnie kliknij prawym przyciskiem myszy element **Na zewnątrz** i dodaj obszar za pomocą menu kontekstowego.
   Wszystkie tworzone obszary początkowo otrzymują unikatową nazwę **Obszar** oraz dodatkowo przyrostek liczbowy.
4. W wyskakującym oknie wybierz typ obszaru, czyli **Obszar** dla osób lub **Parking** dla pojazdów.
   Zauważ, że tylko węzeł **Na zewnątrz** może mieć elementy podrzędne obu typów. Każdy podobszar tych elementów podrzędnych zawsze dziedziczy typ elementu nadrzędnego.
   - **Obszary** dla osób można zagnieżdżać na trzech poziomach. Dla każdego obszaru lub podobszaru można zdefiniować maksymalną liczebność.
   - **Parkingi** są wirtualnymi jednostkami składającymi się z co najmniej jednej **strefy parkowania**. Jeśli liczebność na parkingu nie musi być ograniczona przez system, wyświetlana jest wartość 0. W przeciwnym razie maksymalna liczba miejsc parkingowych w strefie wynosi 9999, a główny panel parkingu pokazuje sumę wszystkich miejsc parkingowych w jego wszystkich strefach.

Procedura edytowania obszarów

1. Kliknij obszar w hierarchii, aby go zaznaczyć.
2. W głównym panelu okna dialogowego zastąp jeden lub więcej poniższych atrybutów.

Nazwa	Domyślna nazwa, którą możesz zastąpić.
Opis	Opis obszaru w formacie tekstowym.
Maksymalna liczba osób/samochodów	Wartość domyślna 0 (zero) oznacza brak limitu. W przeciwnym razie wpisz liczbę całkowitą określającą maksymalną liczebność.

Uwagi:

– Obszaru nie można przenosić poprzez jego przeciągnięcie i upuszczenie w innej gałęzi hierarchii. W razie potrzeby usuń obszar i odtwórz go w innej gałęzi.

Procedura usuwania obszarów

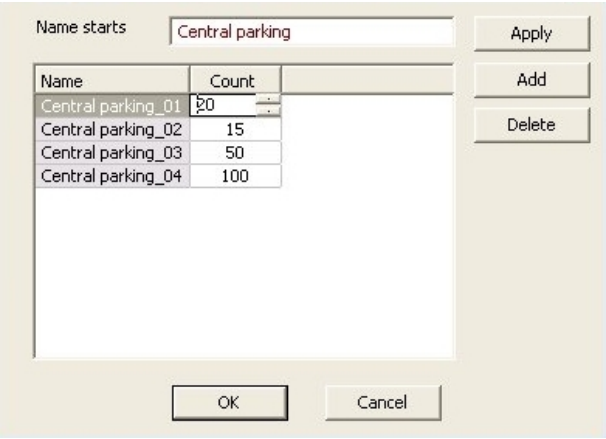
1. Kliknij obszar w hierarchii, aby go zaznaczyć.
2. Kliknij przycisk **Usuń**  lub kliknij prawym przyciskiem myszy i z menu kontekstowego wybierz polecenie usunięcia.

Uwaga: nie można usunąć obszaru, dopóki nie zostaną usunięte jego wszystkie elementy podrzędne.

9.1 Konfigurowanie obszarów dla pojazdów

Tworzenie obszarów dla pojazdów (parking, strefa parkowania)

Jeśli wybierzesz typ obszaru **Parking**, pojawi się wyskakujące okno.



1. W polu **Nazwa rozpoczyna się od** wprowadź nazwę, która będzie stanowiła rdzeń nazwy podobszarów parkingu, czyli inaczej **stref parkowania**.
   Używając przycisku **Dodaj**, można utworzyć maksymalnie 24 **strefy parkowania**. Każda będzie miała nazwę składającą się z rdzenia i dwucyfrowego sufiksu.
2. Jeśli system ma ograniczyć liczebność tych obszarów, wprowadź liczbę miejsc parkingowych w kolumnie **Liczba**. Jeśli nie jest wymagany żaden limit liczebności, wprowadź 0.

Uwaga: Maksymalna liczebność całego parkingu jest sumą tych wartości. Tylko strefy parkowania mogą zawierać miejsca parkingowe; **parking** jest tylko wirtualną jednostką składającą się z co najmniej jednej **strefy parkowania**. Maksymalna liczba miejsc parkingowych w każdej strefie to 9999.

Tworzenie wejść na parkingi

Podobnie jak w zwykłych obszarach, każdy parking musi mieć wejście. Odpowiedni model drzwi to **Parking 05c**.

Do monitorowania liczebności na parkingu są wymagane 2 wejścia z tym modelem drzwi podlegające temu samemu kontrolerowi: jedno do wchodzenia i jedno do wychodzenia.

Wymaganie wstępne

Utworzenie parkingu z co najmniej jedną strefą parkowania, jak opisano powyżej.

Ścieżka w oknie dialogowym

Menu główne > **Konfiguracja** > **Dane urządzenia**

Kliknij opcję **Kontrolery LAC/wejścia/urządzenia**  .

Procedura

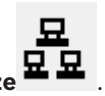
1. W hierarchii urządzeń utwórz kontroler AMC lub wybierz kontroler AMC, któremu nie podlegają żadne wejścia.
2. Kliknij prawym przyciskiem myszy kontroler AMC i wybierz polecenie **Nowe wejście**.
3. W wyskakującym oknie **Nowe wejście** wybierz model wejścia **Parking 05c** i dodaj czytnik przychodzących o typie zainstalowanym przy wejściu do parkingu.
4. Kliknij przycisk **OK**, aby zamknąć wyskakujące okno.
5. Zaznacz to nowo utworzone wejście w hierarchii urządzeń.
   – Zauważ, że system automatycznie oznaczył czytnik jako czytnik wejścia.
6. W głównym oknie edycji na karcie **Parking 05c** w menu rozwijanym **Obszar docelowy** zaznacz utworzony wcześniej parking.
7. Ponownie kliknij kontroler AMC prawym przyciskiem myszy i utwórz kolejne wejście typu **Parking 05c**, jak wyżej.
   – Zauważ, że tym razem można wybrać tylko czytnik wychodzących.

- Kliknij przycisk **OK**, aby zamknąć wyskakujące okno.

8. Zaznacz to drugie nowo utworzone wejście w hierarchii urządzeń.
   - Zauważ, że system automatycznie oznaczył drugi czytnik jako czytnik wyjścia.

10 Konfigurowanie operatorów i stacji roboczych

Wprowadzenie do uprawnień administracyjnych kontroli dostępu
Uprawnienia administracyjne w systemie kontroli dostępu określają, które okna dialogowe systemu można otwierać i które funkcje wykonywać.
Uprawnienia można przypisywać zarówno operatorom, jak i stacjom roboczym.
Uprawnienia stacji roboczej mogą tymczasowo ograniczać uprawnienia operatora, ponieważ operacje o znaczeniu krytycznym dla bezpieczeństwa powinny być wykonywane tylko ze stacji roboczych, które są szczególnie bezpieczne.
Uprawnienia są przydzielane operatorom i stacjom roboczym w pakietach zwanych **profilami**.
Każdy profil jest dostosowany do obowiązków jednego określonego typu operatora lub stacji roboczej.
Każdy operator lub stacja robocza może mieć wiele profili autoryzacji.

Ogólna procedura i ścieżki w oknach dialogowych
1. Utwórz stacje robocze w edytorze urządzeń:
   Konfiguracja > **Dane urządzenia** > **Stacje robocze**  .
2. Utwórz profile stacji roboczych w oknie dialogowym:
   Operatorzy i stacje robocze > **Profile stacji roboczej**.
3. Przypisz profile do stacji roboczych w oknie dialogowym:
   Operatorzy i stacje robocze > **Prawa stacji roboczej**.
4. Utwórz profile operatorów w oknie dialogowym:
   Operatorzy i stacje robocze > **Profile użytkownika**.
5. Przypisz profile do operatorów w oknie dialogowym:
   Operatorzy i stacje robocze > **Uprawnienia użytkownika**.

10.1 Tworzenie stacji roboczych

Stacje robocze to komputery, z których operatorzy obsługują system kontroli dostępu. Najpierw należy „utworzyć” stację roboczą, tzn. zarejestrować komputer w systemie kontroli dostępu.

Ścieżka w oknie dialogowym
Konfiguracja > **Dane urządzenia** > **Stacje robocze**

Procedura
1. Kliknij prawym przyciskiem myszy pozycję **DMS** i z menu kontekstowego wybierz polecenie **Nowy obiekt** lub kliknij przycisk ✚ na pasku narzędzi.
2. Wprowadź wartości parametrów:
   – Wartość pola **Nazwa** musi dokładnie odpowiadać nazwie komputera.
   – Pole **Opis** jest opcjonalne. Można go użyć na przykład do opisania funkcji i lokalizacji stacji roboczej.
   – **Logowanie za pomocą czytnika** Pozostaw to pole wyboru wyczyszczone, chyba że operatorzy mają się logować na tej stacji roboczej poprzez przyłożenie karty do czytnika rejestracji podłączonego do stacji. Szczegółowe informacje znajdują się w sekcji .

– **Automatyczne wylogowanie po:** Liczba sekund, po jakiej zalogowanie za pomocą czytnika rejestracji jest automatycznie kończone. Pozostawienie wartości 0 oznacza nieograniczoną ważność zalogowania.

10.2 Tworzenie profili stacji roboczych

Wprowadzenie do profili stacji roboczych

W zależności od swojej fizycznej lokalizacji stacja robocza kontroli dostępu powinna być starannie skonfigurowana pod kątem jej eksploatacji, na przykład:

– Którzy operatorzy mogą jej używać
– Jakie poświadczenia są niezbędne do jej używania
– Jakie zadania kontroli dostępu można na niej wykonywać

Profil stacji roboczej to zbiór uprawnień, które definiują następujące aspekty:

– Menu i okna dialogowe w menedżerze okien dialogowych, z których można korzystać na stacji roboczej.
– Które profile użytkowników musi posiadać operator, aby się logować na tej stacji roboczej.

Uwaga!
Profile stacji roboczej zastępują profile użytkowników
Operator może korzystać tylko z tych uprawnień ze swojego profilu, które należą również do profilu stacji roboczej komputera, na którym jest zalogowany. Jeśli profile stacji roboczej i operatora nie mają wspólnych uprawnień, użytkownik nie będzie mieć żadnych uprawnień na tej stacji roboczej.

Ścieżka w oknie dialogowym

Konfiguracja > **Operatorzy i stacje robocze** > **Profile stacji roboczej**

Tworzenie profilu stacji roboczej

1. Kliknij przycisk  , aby utworzyć nowy profil.
2. Wprowadź nazwę profilu w polu **Nazwa profilu** (obowiązkowe).
3. Wprowadź opis profilu w polu **Opis** (opcjonalnie, ale zalecane).
4. Kliknij przycisk  lub **Zastosuj**, aby zapisać zmiany.

Przypisywanie praw do wykonywania funkcji systemowych

1. Na liście **Funkcje** zaznacz funkcje, które mają być dostępne na tej stacji roboczej, kliknij je dwukrotnie i w kolumnie **Wykonaj** ustaw wartość `Yes`.
   – Podobnie upewnij się, że we wszystkich funkcjach, które mają być niedostępne, ustawiono wartość `No`.
2. Kliknij przycisk  lub **Zastosuj**, aby zapisać zmiany.

Przypisywanie profili użytkowników do profili stacji roboczych

W panelu **Profil użytkownika**:

Lista **Przypisane profile** zawiera wszystkie profile użytkowników upoważnione do logowania się na stacji roboczej przy użyciu tego profilu stacji roboczej.

Pole **Dostępne profile** zawiera wszystkie pozostałe profile. Nie są one jeszcze autoryzowane do logowania się na stacji roboczej przy użyciu tego profilu stacji roboczej.

1. Kliknij przyciski strzałek między listami, aby przenieść wybrane profile z jednej listy do drugiej.
2. Kliknij przycisk  lub **Zastosuj**, aby zapisać zmiany.

Uwaga!
Domyślne profile administratora dla użytkownika (**UP — administrator**) i stacji roboczej (**WP — administrator**) nie mogą być modyfikowane ani usuwane.
Profil **WP — administrator** jest nieodwołalnie związany z serwerową stacją roboczą.
Gwarantuje to, że istnieje co najmniej jeden użytkownik, który może się zalogować na serwerowej stacji roboczej.

10.3 Przypisywanie profili stacji roboczych

W tym oknie dialogowym można zarządzać przypisaniami profili stacji roboczych do stacji roboczych. Każda stacja robocza musi mieć co najmniej jeden profil stacji roboczej. Jeśli ma wiele profili, wszystkie uprawnienia z tych profili stosują się jednocześnie.

Ścieżka w oknie dialogowym
Konfiguracja > **Operatorzy i stacje robocze** > **Prawa stacji roboczej**

Procedura
Lista **Przypisane profile** zawiera wszystkie profile stacji roboczych, które już należą do tej stacji roboczej.
Lista **Dostępne profile** zawiera wszystkie profile stacji roboczych, które nie zostały jeszcze przypisane do tej stacji roboczej.

1. Na liście stacji roboczych zaznacz stację roboczą, którą chcesz skonfigurować.
2. Kliknij przyciski strzałek między listami **Przypisane** i **Dostępne**, aby przenieść wybrane profile z jednej listy do drugiej.
3. Kliknij przycisk  lub **Zastosuj**, aby zapisać zmiany.

Uwaga!
Domyślne profile administratora dla użytkownika (**UP — administrator**) i stacji roboczej (**WP — administrator**) nie mogą być modyfikowane ani usuwane.
Profil **WP — administrator** jest nieodwołalnie związany z serwerową stacją roboczą.
Gwarantuje to, że istnieje co najmniej jeden użytkownik, który może się zalogować na serwerowej stacji roboczej.

10.4 Tworzenie profili użytkowników (operatorów)

Wprowadzenie do profili użytkowników
Uwaga: W kontekście uprawnień użytkowników termin **Użytkownik** jest synonimem terminu **Operator**.
Profil użytkownika to zbiór uprawnień, które definiują następujące aspekty:
– Menu menedżera okien dialogowych i okna dialogowe widoczne dla operatora.
– Możliwości operatora w tych oknach dialogowych, czyli w praktyce prawa do wykonywania, zmiany, dodawania i usuwania elementów tych okien dialogowych.

Profile użytkowników powinny być starannie skonfigurowane, z uwzględnieniem doświadczenia, poświadczeń bezpieczeństwa i zakresu odpowiedzialności danej osoby:

Ścieżka w oknie dialogowym

Konfiguracja > **Operatorzy i stacje robocze** > **Profile użytkownika**

Procedura

1. Kliknij przycisk  , aby utworzyć nowy profil.
2. Wprowadź nazwę profilu w polu **Nazwa profilu** (obowiązkowe).
3. Wprowadź opis profilu w polu **Opis** (opcjonalnie, ale zalecane).
4. Kliknij przycisk  lub **Zastosuj**, aby zapisać zmiany.

Uwaga!

Wybieraj nazwy profili, które jasno i precyzyjnie opisują możliwości i ograniczenia profilu.

Dodawanie praw do edytowania i wykonywania funkcji systemowych

1. W panelu listy wybierz funkcje (pierwsza kolumna) i możliwości wewnątrz funkcji (**Wykonywanie**, **Zmiana**, **Dodawanie**, **Usuwanie**), które mają być dostępne w tym profilu. Kliknij dwukrotnie te elementy, aby przełączyć wartości ich ustawień na `Yes`.
   - Podobnie upewnij się, że we wszystkich funkcjach, które mają być niedostępne, ustawiono wartość `No`.
2. Kliknij przycisk  lub **Zastosuj**, aby zapisać zmiany.

10.5 Przypisywanie profili użytkowników (operatorów)

Uwaga: W kontekście uprawnień użytkowników termin **Użytkownik** jest synonimem terminu **Operator**.

Wymagania wstępne

- Operator, który ma otrzymać ten profil użytkownika, został zdefiniowany jako **Osoba** w systemie kontroli dostępu.
- Zdefiniowano odpowiedni profil użytkownika w systemie kontroli dostępu.
  - Pamiętaj, że zawsze istnieje możliwość przypisania profilu użytkownika z nieograniczonymi uprawnieniami **UP — administrator**, ale ta praktyka jest niezalecana ze względów bezpieczeństwa.

Ścieżka w oknie dialogowym

Konfiguracja > **Operatorzy i stacje robocze** > **Uprawnienia użytkownika**

Procedura

1. Załaduj zestaw danych osobowych wybranego użytkownika do okna dialogowego.
2. W razie potrzeby ogranicz ważność profilu użytkownika, wpisując daty w polach **Ważne od** i **Ważne do**.

Przypisywanie profili użytkowników do operatorów

W panelu **Profile użytkownika**:

Lista **Przypisane profile** zawiera wszystkie profile użytkowników, które przypisano temu użytkownikowi.

Pole **Dostępne profile** zawiera wszystkie profile dostępne do przypisania.

1. Kliknij przyciski strzałek między listami, aby przenieść wybrane profile z jednej listy do drugiej.
2. Zaznacz pole wyboru **Administrator globalny**, aby przyznać temu operatorowi prawa odczytu i zapisu wobec zestawów danych osobowych, w których włączono atrybut **Administrowane globalnie**. Domyślnie operator ma dostęp tylko do odczytu względem takich zestawów danych osobowych.
3. Kliknij przycisk , aby zapisać zmiany.

Przypisywanie operatorom praw używania interfejsów API
Przy odpowiedniej konfiguracji i zapewnieniu licencji kod źródłowy zewnętrznych programów może wywoływać funkcje systemu kontroli dostępu za pośrednictwem interfejsów programowania aplikacji, czyli API. Zewnętrzny program działa za pośrednictwem operatora proxy w systemie. Lista rozwijana **Korzystanie z API** kontroluje możliwości bieżącego operatora, jeśli jest on wykorzystywany jako operator proxy przez zewnętrzny kod źródłowy.
Konfiguracja > **Operatorzy i stacje robocze** > **Uprawnienia użytkownika**
– Zaznacz ustawienie na liście **Korzystanie z API**.
Dostępne opcje:

Brak dostępu	Interfejs API nie może korzystać z pośrednictwa operatora do wykonywania funkcji systemowych.
Tylko odczyt	Interfejs API może korzystać z pośrednictwa operatora do odczytywania danych systemowych, ale nie do ich dodawania, modyfikowania ani usuwania.
Nieograniczona	Interfejsu API może korzystać z pośrednictwa operatora do odczytywania, dodawania, modyfikowania i usuwania danych systemowych.

– Kliknij przycisk , aby zapisać zmiany.

10.6 Ustawianie haseł dla operatorów

Tu opisano, jak ustawić bezpieczne hasła dla siebie i innych użytkowników.

Wstęp
System wymaga co najmniej jednego operatora. Domyślny operator w nowej instalacji ma nazwę użytkownika **Administrator** i hasło **Administrator**. Pierwszym krokiem podczas konfigurowania systemu powinno być zawsze zalogowanie się przy użyciu tych poświadczeń i zmiana hasła **Administrator**, zgodnie z zasadami ustawiania haseł obowiązującymi w organizacji.
Następnie możesz dodać innych operatorów, zarówno uprzywilejowanych, jak i nieuprzywilejowanych.

Procedura zmiany własnego hasła
Wymagania wstępne
Jesteś użytkownikiem zalogowanym w menedżerze okien dialogowych.

Procedura
1. W menedżerze okien dialogowych wybierz menu: **Plik** > **Zmień hasło**.

2. W wyskakującym oknie wprowadź bieżące hasło, nowe hasło i ponownie nowe hasło, aby je potwierdzić.
3. Kliknij przycisk **Zmień**.

Ta procedura jest jedynym sposobem na zmianę hasła administratora.

Procedura zmiany haseł innych operatorów

Wymagania wstępne

Aby zmienić hasła innych użytkowników, zaloguj się w menedżerze okien dialogowych przy użyciu konta z uprawnieniami administratora.

Procedura

1. W głównym menu menedżera okien dialogowych wybierz kolejno opcje **Konfiguracja** > **Operatorzy i stacje robocze** > **Uprawnienia użytkownika**
2. W głównym panelu okna dialogowego za pomocą paska narzędzi wczytaj operatora, którego hasło chcesz zmienić.
3. Kliknij przycisk **Zmień hasło...**
4. W wyskakującym oknie wprowadź nowe hasło i ponownie nowe hasło, aby je potwierdzić.
5. W wyskakującym oknie wprowadź okres ważności nowego hasła — **Nieograniczona** lub liczbę dni.
   – W środowiskach produkcyjnych stanowczo zalecamy ustawienie okresu ważności.
6. Kliknij przycisk **OK**, aby zamknąć wyskakujące okno.

W głównym oknie dialogowym kliknij ikonę  , aby zapisać rekord użytkownika.

Zwróć uwagę, że selektory dat **Ważne od** i **Ważne do** pod przyciskiem **Zmień hasło...** dotyczą terminu ważności uprawnień użytkownika w tym oknie dialogowym, a nie hasła.

Więcej informacji

Zawsze ustawiaj hasła zgodnie z polityką haseł obowiązującą w organizacji. Aby uzyskać wskazówki dotyczące tworzenia takich zasad, możesz się na przykład zapoznać z wytycznymi Microsoft opublikowanymi tutaj:
https://www.microsoft.com/en-us/research/publication/password-guidance/

Odwołanie do tematu Tworzenie nowych użytkowników

11 Konfigurowanie kodów kart

Kodowanie kart kontroli dostępu daje gwarancję, że wszystkie dane kart są niepowtarzalne.

Ścieżka w oknie dialogowym
Menu główne > **Konfiguracja** > **Opcje** > **Konfiguracja kodowania kart**
Wprowadzanie liczb w oknie dialogowym
Aby uniknąć błędów w kodowaniu kart, wszystkie liczby można wprowadzać w formatach dziesiętnym lub szesnastkowym. Naciśnij przycisk radiowy **Szesnastkowy** lub **Dziesiętny** zgodnie z instrukcjami producenta karty. Wszelkie już wprowadzone wartości zostaną automatycznie przekonwertowane wewnętrznie.
Główny panel okna dialogowego jest podzielony na dwie grupy, które opisano bardziej szczegółowo poniżej:

- **Domyślne dane kodowania kart**
- **Sprawdź tylko wartości członkostwa**

Domyślne dane kodowania kart
W tej sekcji zdefiniuj wartości pól **Wersja**, **Kod kraju** i **Kod urządzenia**, które zostaną przypisane do numeru karty podczas rejestrowania karty w systemie.
Jeśli karta jest rejestrowana ręcznie na stacji roboczej operatora, pojawi się okno dialogowe z wartościami domyślnymi, które można dostosować dla każdej karty.

Nr kodowy kompletny (domyślnie)	Jest wprowadzany tylko kod urządzenia (szesnastkowy lub dziesiętny).  **Wprowadzanie danych kodowania:** Kod urządzenia jest podany przez producenta jako wartość dziesiętna 56720. Naciśnij przycisk radiowy **Dziesiętny** i wprowadź kod urządzenia. Kliknij przycisk Zastosuj, aby zapisać dane.
Nr kodowy podzielony	W polach Wersja, Kod kraju i Kod urządzenia należy wpisać wartości **dziesiętne**.  **Wprowadzanie danych kodowania:** Dane są podane przez producenta w formacie dziesiętnym: Wersja: 2 Kod kraju: 99 Kod urządzenia: 56720 Wprowadź dane w odpowiednich polach tekstowych.

	Kliknij przycisk Zastosuj, aby zapisać dane.

Uwagi dotyczące wprowadzania domyślnych danych kodowania:
Dane domyślne są przechowywane w rejestrze systemu operacyjnego, a każdy numer karty identyfikacyjnej jest dodawany w czasie kodowania. Dane rejestracyjne przybierają formę **8-cyfrowej wartości szesnastkowej**, w razie potrzeby z wiodącymi zerami.
Jeśli numer kodowy jest przesyłany całkowicie, system może go przekonwertować z wartości dziesiętnej na szesnastkową, dopełnić do 8 miejsc za pomocą wiodących zer, a następnie zapisać odpowiedni parametr systemu.

- Przykład:
  - Dane wejściowe: 56720
  - Konwersja: DD90
  - Zapis jako: 0000DD90

Jeśli numer kodowy jest przesyłany w częściach (jako podzielony), można to zrobić wyłącznie w formie **dziesiętnej**. Numer jest konwertowany na 10-cyfrową liczbę dziesiętną skonstruowaną w następujący sposób:

- Wersja: 2 cyfry
- Kod kraju: 2 cyfry
- Kod urządzenia: 6 cyfr
- Jeśli którejkolwiek z 10 cyfr nadal brakuje, jest dopełniana zerami wiodącymi.
  - Przykład: 0299056720

Ta 10-cyfrowa wartość dziesiętna jest konwertowana i przechowywana jako 8-cyfrowa wartość szesnastkowa.

- Przykład:
  - dziesiętna: 0299056720
  - szesnastkowa: 11D33E50

Uwaga!
W przypadku podzielonych numerów kodowych system sprawdza poprawność wartości szesnastkowych , aby zapobiec wprowadzeniu nieprawidłowych kodów krajów (powyżej 63 w wariancie szesnastkowym lub 99 w wariancie dziesiętnym) oraz nieprawidłowych kodów urządzeń (powyżej F423F w wariancie szesnastkowym lub powyżej 999 999 w wariancie dziesiętnym)

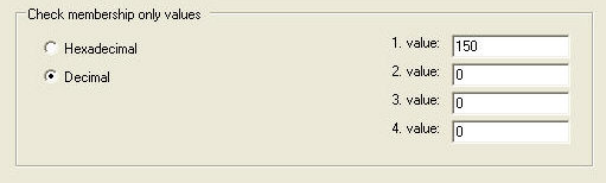
Uwaga!
Jeśli rejestracja karty następuje przez podłączony czytnik, to wartości domyślne są przypisywane automatycznie. Nie można zastąpić wartości domyślnych podczas odczytywania przez czytnik.
Aby było to możliwe, należy zmienić sposób przechwytywania danych na **Okno dialogowe**.

Ręczne wprowadzanie numeru karty odbywa się w formacie dziesiętnym.
Podczas zapisywania danych jest tworzona 10-cyfrowa wartość dziesiętna (z zerami wiodącymi), która następnie jest konwertowana na 8-cyfrową wartość szesnastkową. Ta wartość jest teraz przechowywana razem z domyślnymi danymi kodowymi jako 16-cyfrowy numer kodowy karty.

- Przykład:
  - Wprowadzony numer karty: 415
  - 10-cyfrowy numer: 0000000415
  - Przeliczenie na wartość szesnastkową: 0000019F
  - Połączenie z domyślnymi danymi kodowymi (patrz wyżej) i zapisanie jako numer kodowy karty identyfikacyjnej: 11D33E500000019F

Sprawdzanie tylko wartości członkostwa
Sprawdzenie członkostwa oznacza, że poświadczenie jest sprawdzane tylko w celu zweryfikowania przynależności do firmy lub organizacji, a nie w celu zidentyfikowania osoby. Dlatego nie należy stosować opcji **Tylko sprawdzanie członkostwa** do czytników umożliwiających dostęp do obszarów pilnie strzeżonych.

W tej grupie opcji można wprowadzić maksymalnie cztery kody firm lub klientów. Dane mogą być wprowadzane jako dziesiętne lub szesnastkowe, ale w rejestrze systemu operacyjnego są zapisywane jako wartości dziesiętne.



Wybierz czytnik w edytorze urządzeń DevEdit i aktywuj parametr czytnika **Sprawdzanie członkostwa**.
Tylko kody firm lub klientów w danych karty są odczytywane i weryfikowane względem przechowywanych wartości.

Uwaga!
Opcja **Sprawdzanie członkostwa** działa tylko dla definicji kart wstępnie skonfigurowanych w systemie (szare tło), a nie dla definicji niestandardowych.

12 Konfigurowanie kontrolerów

Wstęp

Kontrolery w systemie kontroli dostępu to wirtualne i fizyczne urządzenia, które wysyłają polecenia do urządzeń peryferyjnych przy wejściach (czytników i drzwi), a następnie zapytania z czytników i drzwi z powrotem do centralnego oprogramowania decyzyjnego.
Kontrolery przechowują kopie niektórych informacji o urządzeniach z centralnego oprogramowania i o posiadaczach kart, a przy odpowiedniej konfiguracji mogą podejmować decyzje w zakresie kontroli dostępu nawet w trakcie tymczasowego odizolowania od centralnego oprogramowania.
Oprogramowaniem decyzyjnym jest Data Management System.
Istnieją dwa rodzaje kontrolerów:

– Główne kontrolery dostępu, nazywane skrótowo MAC, oraz nadmiarowe rezerwowe odpowiedniki — RMAC.
– Lokalne kontrolery dostępu, nazywane skrótowo LAC lub AMC.

Kontrolery konfiguruje się w edytorze urządzeń DevEdit.

Ścieżka w oknie dialogowym do edytora urządzeń

Menu główne > **Konfiguracja** > **Dane urządzenia** > **Drzewo urządzeń** 

Korzystanie z edytora urządzeń DevEdit

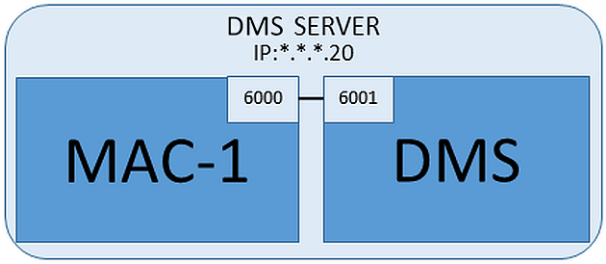
Podstawowe zasady używania edytora DevEdit opisano w tej sekcji **Korzystanie z edytora urządzeń** pod linkiem poniżej.

Patrz

– *Korzystanie z edytora urządzeń, Strona 21*

12.1 Konfigurowanie kontrolerów MAC i RMAC

12.1.1 Konfigurowanie kontrolera MAC na serwerze systemu DMS



W minimalnej konfiguracji systemu jest wymagany jeden kontroler MAC. W takim przypadku kontroler MAC może się znajdować na serwerze systemu DMS.

Procedura

Na serwerze systemu DMS otwórz edytor urządzeń i w drzewie urządzeń utwórz kontroler MAC, zgodnie z opisem w sekcji **Korzystanie z edytora urządzeń**.
Zaznacz kontroler MAC w edytorze urządzeń. Na karcie **MAC** podaj następujące wartości parametrów:

Parametr	Opis
Nazwa	Nazwa, która ma się pojawiać w drzewie urządzeń, na przykład MAC-1.

Parametr	Opis
Opis	Opcjonalny opis dla operatorów systemu.
Z RMAC (pole wyboru)	**<pozostaw puste>**
Port RMAC	**<pozostaw puste>**
Aktywny (pole wyboru)	**Wyczyść** to pole wyboru, aby tymczasowo zawiesić synchronizację w czasie rzeczywistym między tym kontrolerem MAC a systemem DMS. Przydaje się to po aktualizacji systemu DMS w większych instalacjach, ponieważ pozwala uniknąć ponownego uruchamiania wszystkich kontrolerów MAC równocześnie.
Ładowanie urządzeń (pole wyboru)	**Wyczyść** to pole wyboru, aby tymczasowo zawiesić synchronizację w czasie rzeczywistym między tym kontrolerem MAC a jego urządzeniami podrzędnymi. Skraca to czas potrzebny do otwarcia kontrolera MAC w edytorze urządzeń.
Adres IP	`Localhost 127.0.0.1`
Strefa czasowa	**WAŻNE:** Jest to strefa czasowa kontrolera MAC oraz jego wszystkich podległych kontrolerów AMC.
Strefa	(jeśli dotyczy) Strefa, do której należy kontroler MAC.

Ponieważ ten lokalny kontroler MAC nie ma nadmiarowego kontrolera MAC, do którego może awaryjnie przełączyć swoje zadania, nie trzeba dla niego uruchomić narzędzia MACInstaller. Po prostu pozostaw puste oba parametry kontrolera RMAC na karcie **MAC**.

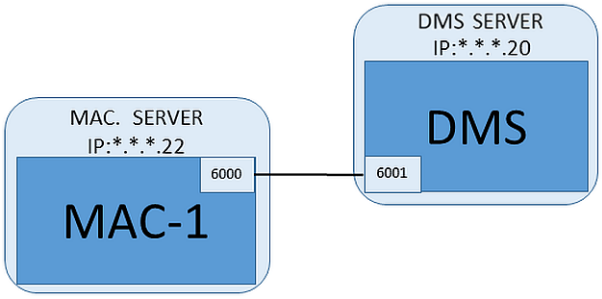
12.1.2 Przygotowywanie komputerów serwerów kontrolerów MAC do obsługi kontrolerów MAC i RMAC

W tej sekcji opisano sposób przygotowania komputerów do roli serwerów kontrolerów MAC. Domyślnie pierwszy kontroler MAC w systemie Access Engine działa na tym samym komputerze, co jego serwer zarządzania danymi (DMS), jednak w celu zwiększenia odporności na błędy zaleca się skonfigurowanie kontrolera MAC na oddzielnym komputerze, który może przejąć zadania kontroli dostępu w razie awarii komputera z systemem DMS.
Oddzielne komputery z kontrolerami MAC lub RMAC są nazywane serwerami kontrolerów MAC, niezależnie od tego, czy zawierają one kontrolery MAC, czy RMAC.
W celu zapewnienia funkcjonalności przełączania awaryjnego kontrolery MAC i RMAC **muszą** być zainstalowane na oddzielnych serwerach kontrolerów MAC.
Upewnij się, że są spełnione następujące warunki na wszystkich serwerach kontrolerów MAC w jednym środowisku:

1. Wszystkie serwery mają tę samą wersję tego samego systemu operacyjnego, co serwer systemu DMS, z najnowszymi aktualizacjami systemu Windows.
2. Użytkownik Administrator na wszystkich serwerach ma to samo hasło.
3. Jesteś użytkownikiem zalogowanym jako Administrator (w przypadku korzystania z narzędzia MSTSC używaj tylko sesji /Admin /Console).
4. Wyłącz używanie adresów IP V6. Uważnie spisz adres IP V4 każdego serwera.

5. Włącz obsługę platformy .NET 3.5 na wszystkich komputerach w środowisku.
   Uwaga: W systemie Windows 7 jest to osobno instalowany składnik. W systemach operacyjnych Windows 10 i Windows Server jest to włączana funkcja.
6. Uruchom ponownie komputer.

12.1.3 Konfigurowanie kontrolera MAC na jego własnym serwerze



– Komputer serwera kontrolera MAC został przygotowany w sposób opisany w sekcji .

1. Na serwerze systemu DMS dezaktywuj kontroler MAC, usuwając zaznaczenia z pól wyboru **Aktywuj** i **Ładowanie urządzeń** dla tego kontrolera MAC w edytorze urządzeń.
2. Na serwerze kontrolera MAC zatrzymaj proces kontrolera MAC przy użyciu programu Windows `services.msc`.
3. Uruchom program `MACInstaller.exe`.
   – W przypadku modułu ACE znajduje się on na nośniku instalacyjnym systemu BIS w folderze `\AddOns\ACE\MultiMAC\MACInstaller` (patrz poniżej sekcja Korzystanie z narzędzia MACInstaller).
   –
4. Przejdź przez kolejne ekrany narzędzia, podając wartości w poniższych parametrach.

Numer ekranu	Parametr	Opis
1	**Folder docelowy**	Lokalny katalog, w którym ma zostać zainstalowany kontroler MAC. Pozostawiaj wartość domyślną, o ile to tylko możliwe.
2	**Serwer**	Nazwa lub adres IP serwera, na którym działa system DMS.
2	**Port (dla systemu DMS)**	Port na serwerze systemu DMS, na którym będzie odbierana komunikacja z kontrolera MAC**.** Użyj wartości 6001 dla pierwszego kontrolera MAC w systemie DMS i zwiększaj ją o 1 dla każdego następnego kontrolera MAC.
2	**Numer (numer kontrolera MAC w systemie)**	Ustaw wartość 1 dla tego i wszystkich kontrolerów MAC (w przeciwieństwie do kontrolerów RMAC)**.**

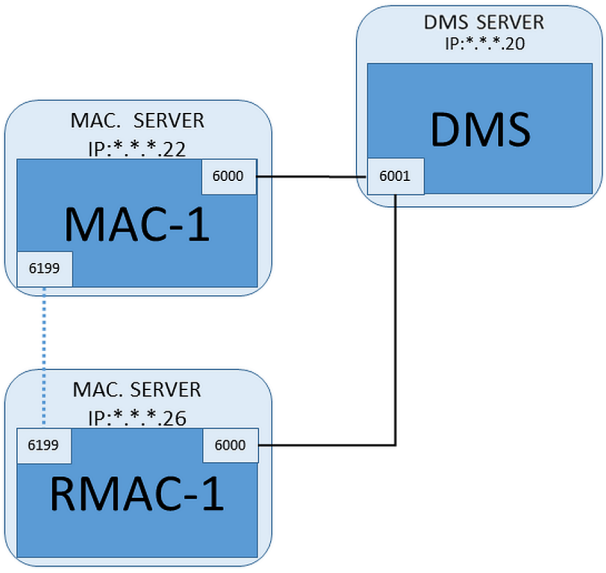
Numer ekranu	Parametr	Opis
2	**Bliźniak (nazwa lub adres IP partnerskiego kontrolera MAC)**	Pozostaw to pole puste, jeśli ten kontroler MAC nie będzie miał żadnego odpowiadającego mu kontrolera RMAC.
2	**Tylko konfiguruj** (przycisk radiowy)	Nie zaznaczaj tej opcji, ponieważ nie konfigurujesz kontrolera MAC na głównym serwerze logowania do systemu DMS.
2	**Aktualizuj oprogramowanie** (przycisk radiowy)	Zaznacz tę opcję, ponieważ konfigurujesz kontroler MAC na jego własnym komputerze (serwerze kontrolera MAC), a nie na głównym serwerze logowania do systemu DMS.

5. Po wykonaniu wszystkich czynności w narzędziu uruchom ponownie serwer kontrolera MAC lub — alternatywnie — uruchom proces kontrolera MAC na serwerze kontrolera MAC za pomocą programu Windows `services.msc`.
6. Na serwerze systemu DMS zaznacz kontroler MAC w edytorze urządzeń.
7. Na karcie **MAC** podaj wartości następujących parametrów:

Parametr	Opis
Nazwa	Nazwa, która ma się pojawiać w drzewie urządzeń, na przykład MAC-1.
Opis	Opcjonalny opis dla operatorów modułu ACE.
Z RMAC (pole wyboru)	**<pozostaw puste>**
Port RMAC	**<pozostaw puste>**
Aktywny (pole wyboru)	Teraz zaznacz to pole wyboru.
Ładowanie urządzeń (pole wyboru)	Teraz zaznacz to pole wyboru.
Adres IP	Adres IP komputera serwera kontrolera MAC.
Strefa czasowa	**WAŻNE:** Jest to strefa czasowa kontrolera MAC oraz jego wszystkich podległych kontrolerów AMC.
Strefa	(jeśli dotyczy) Strefa ACE, do której należy kontroler MAC.

12.1.4 Dodawanie kontrolerów RMAC do kontrolerów MAC

Uwaga!
Kontrolery RMAC można dodawać do zwykłych kontrolerów MAC dopiero wtedy, gdy kontrolery MAC zostaną zainstalowane i będą działały poprawnie.
W przeciwnym razie można utrudnić lub uniemożliwić replikację danych.



– Kontroler MAC dla tego kontrolera RMAC został zainstalowany zgodnie z opisem w poprzednich sekcjach i działa poprawnie.
– Komputer serwera kontrolera MAC dla kontrolera RMAC został przygotowany w sposób opisany w sekcji .

Kontrolery MAC mogą działać w układzie bliźniaczym z nadmiarowymi kontrolerami MAC (RMAC) w celu zapewnienia możliwości przełączania awaryjnego, czyli zwiększenia odporności systemu kontroli dostępu na błędy. W tym przypadku dane kontroli dostępu są automatycznie replikowane między oboma kontrolerami. Jeśli którykolwiek kontroler w parze ulegnie awarii, drugi przejmie sterowanie podległymi lokalnymi kontrolerami dostępu.

Na serwerze systemu DMS w przeglądarce konfiguracji

1. W edytorze urządzeń zaznacz kontroler MAC, dla którego chcesz dodać kontroler RMAC.
2. Na karcie **MAC** zmień wartości następujących parametrów:

Parametr	Opis
Z RMAC (pole wyboru)	**Wyczyść** to pole wyboru, dopóki nie zainstalujesz odnośnego kontrolera RMAC na nadmiarowym serwerze przełączania awaryjnego
Aktywny (pole wyboru)	**Wyczyść** to pole wyboru, aby tymczasowo zawiesić synchronizację w czasie rzeczywistym między tym kontrolerem MAC a systemem DMS. Przydaje się to po aktualizacji systemu DMS w większych instalacjach, ponieważ pozwala uniknąć ponownego uruchamiania wszystkich kontrolerów MAC równocześnie.
Ładowanie urządzeń (pole wyboru)	**Wyczyść** to pole wyboru, aby tymczasowo zawiesić synchronizację w czasie rzeczywistym między tym kontrolerem MAC a jego urządzeniami podrzędnymi. Skraca to czas potrzebny do otwarcia kontrolera MAC w edytorze urządzeń.

3. Klika przycisk **Zastosuj**.
4. Pozostaw edytor urządzeń otwarty, ponieważ za chwilę do niego wrócisz.

Na serwerze kontrolera MAC dla kontrolera MAC

Aby zmienić konfigurację kontrolera MAC w celu przygotowania go do współpracy z kontrolerem RMAC, wykonaj następujące czynności.

– Na wcześniej przygotowanym komputerze serwera kontrolera MAC uruchom narzędzie MACInstaller (patrz Korzystanie z narzędzia MACInstaller) i ustaw następujące parametry:
  – **Serwer**: Nazwa lub adres IP komputera serwera systemu DMS.
  – **Port**: `6001`
  – **Numer**: `1` (wszystkie kontrolery MAC mają numer 1).
  – **Bliźniak**: Adres IP komputera, na którym będzie działał kontroler RMAC.
  – **Aktualizuj oprogramowanie**: Zaznacz tę opcję podczas konfigurowania serwera komputera MAC, a nie serwera systemu DMS.

Na serwerze kontrolera MAC dla kontrolera RMAC

Aby skonfigurować kontroler RMAC, należy wykonać następujące czynności:

– Na osobnym i wcześniej przygotowanym komputerze serwera kontrolera MAC uruchom narzędzie MACInstaller (patrz Korzystanie z narzędzia MACInstaller) i ustaw następujące parametry:
  – **Serwer**: Nazwa lub adres IP komputera serwera systemu DMS.
  – **Port**: `6001` (tak samo, jak dla kontrolera MAC).
  – **Numer**: `2` (wszystkie kontrolery RMAC mają numer 2).
  – **Bliźniak**: Adres IP komputera, na którym działa bliźniaczy kontroler MAC.
  – **Aktualizuj oprogramowanie**: Zaznacz tę opcję podczas konfigurowania serwera komputera MAC, a nie serwera systemu DMS.

Powrót do edytora urządzeń na serwerze systemu DMS

1. **WAŻNE:** Upewnij się, że kontrolery MAC i RMAC są uruchomione na swoich odnośnych komputerach i widoczne dla siebie w sieci.
2. Na karcie **MAC** zmień wartości parametrów w następujący sposób:

Parametr	Opis
Z RMAC (pole wyboru)	**Zaznaczone** Nowa karta zatytułowana **RMAC** pojawia się obok karty **MAC**.
Port RMAC	`6199` (domyślna wartość statyczna) Wszystkie kontrolery MAC i RMAC używają tego portu do sprawdzania, czy ich urządzenia partnerskie działają i są dostępne**.**
Aktywny (pole wyboru)	**Zaznaczone** Umożliwia synchronizację między tym kontrolerem MAC a jego urządzeniami podrzędnymi.
Ładowanie urządzeń (pole wyboru)	**Zaznaczone** Skraca to czas potrzebny do otwarcia kontrolera MAC w edytorze urządzeń.

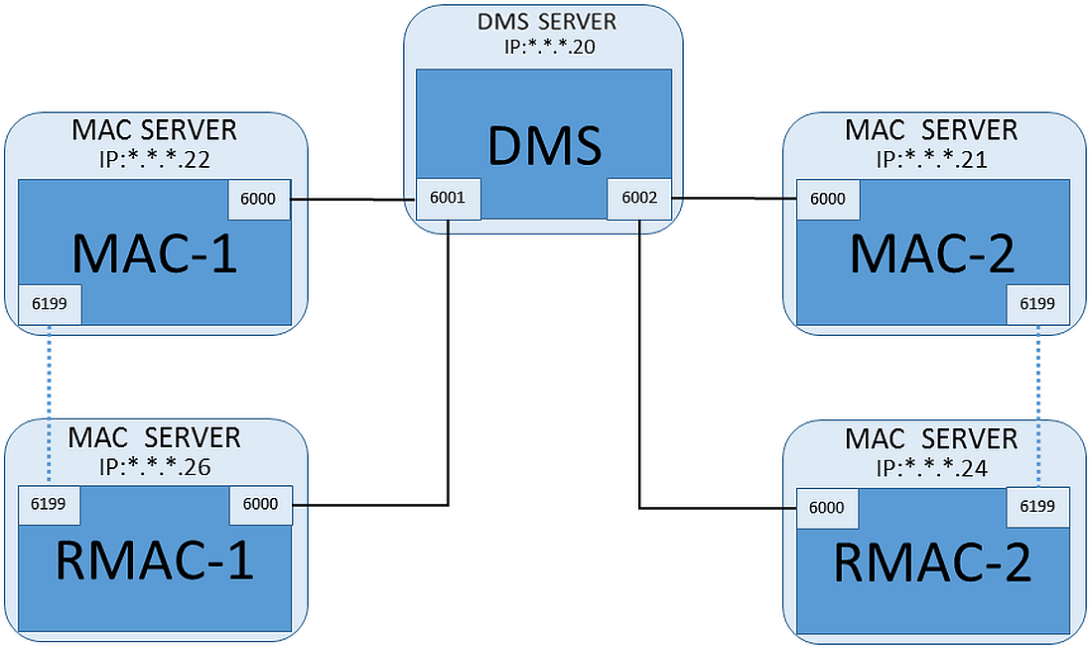
3. Na karcie **RMAC** podaj wartości następujących parametrów:

Parametr	Opis
Nazwa	Nazwa, która ma się pojawiać w drzewie urządzeń. Na przykład jeżeli odnośny kontroler MAC nosi nazwę MAC-01, to ten kontroler RMAC może mieć nazwę RMAC-01.

Parametr	Opis
Opis	Opcjonalna dokumentacja dla operatorów modułów ACE.
Adres IP	Adres IP kontrolera RMAC.
Port MAC	`6199` (domyślna wartość statyczna) Wszystkie kontrolery MAC i RMAC używają tego portu do sprawdzania, czy ich urządzenia partnerskie działają i są dostępne**.**

12.1.5 Dodawanie kolejnych par kontrolerów MAC/RMAC

Zależnie od liczby kontrolowanych wejść i wymaganego stopnia odporności na awarie do konfiguracji systemu można dodać dużą liczbę par kontrolerów MAC/RMAC. Dokładną liczbę par obsługiwaną przez daną wersję oprogramowania można znaleźć w odnośnej karcie katalogowej.



Dla każdej dodatkowej pary kontrolerów MAC/RMAC...

1. Przygotuj oddzielne komputery dla kontrolerów MAC i RMAC, zgodnie z opisem w sekcji .
2. Skonfiguruj kontroler MAC zgodnie z opisem w sekcji .
3. Skonfiguruj kontrolery RMAC dla kontrolera MAC zgodnie z opisem w sekcji .

Zauważ, że każda para kontrolerów MAC/RMAC wysyłane dane do innego portu na serwerze systemu DMS. Dlatego w parametrze **Port (dla systemu DMS)** w narzędziu `MACInstaller.exe` użyj następujących wartości:

- `6001` dla obu komputerów w pierwszej parze kontrolerów MAC/RMAC
- `6002` dla obu komputerów w drugiej parze kontrolerów MAC/RMAC
- itd.

W edytorze urządzeń zawsze można używać portu `6199` dla parametrów **Port MAC** i **Port RMAC**. Ten numer portu jest zarezerwowany dla uzgadniania wzajemnej komunikacji wewnątrz każdej pary kontrolerów MAC/RMAC, wskutek czego każdy kontroler dowiaduje się, czy urządzenie partnerskie jest dostępne, czy nie.

Uwaga!
Ponowne aktywowanie kontrolerów MAC po aktualizacji systemu
Uaktualnienie systemu powoduje domyślnie dezaktywację kontrolerów MAC i podległych im kontrolerów AMC. Pamiętaj, aby aktywować je ponownie w przeglądarce konfiguracji, zaznaczając odpowiednie pola wyboru w edytorze urządzeń.

12.1.6 Korzystanie z narzędzia MACInstaller

`MACInstaller.exe` to standardowe narzędzie służące do konfigurowania i zmiany konfiguracji kontrolerów MAC i RMAC na ich własnych komputerach (serwerach kontrolerów MAC). Zbiera wartości parametrów dla kontrolerów MAC lub RMAC oraz dokonuje niezbędnych zmian w rejestrze systemu Windows.

Uwaga!
Ponieważ narzędzie wprowadza zmiany w rejestrze systemu Windows, w celu zmiany konfiguracji każdego działającego procesu kontrolera MAC trzeba go najpierw zatrzymać.

Narzędzie MACInstaller znajduje się na nośniku instalacyjnym systemu BIS w następującej ścieżce:
`\BIS_<version>\AddOns\ACE\MultiMAC\MACInstaller.exe`
W szeregu ekranów użytkownicy wpisują wartości dla poniższych parametrów.

Numer ekranu	Parametr	Opis
1	**Folder docelowy**	Lokalny katalog, w którym ma zostać zainstalowany kontroler MAC.
2	**Serwer**	Nazwa lub adres IP serwera, na którym działa system DMS.
2	**Port (dla systemu DMS)**	Numer portu serwera systemu DMS, który będzie używany do obsługi komunikację między kontrolerem MAC a serwerem DMS. **Patrz szczegółowe informacje poniżej.**
2	**Numer (numer kontrolera MAC w systemie)**	Ustaw wartość 1 dla wszystkich oryginalnych kontrolerów MAC. Ustaw wartość 2 dla wszystkich nadmiarowych kontrolerów MAC przełączania awaryjnego (RMAC).
2	**Bliźniak (nazwa lub adres IP partnerskiego kontrolera MAC)**	Adres IP komputera, na którym ma działać nadmiarowy partner przełączania awaryjnego dla tego serwera kontrolera MAC. Jeśli nie ma takiego urządzenia, pozostaw to pole puste.

Numer ekranu	Parametr	Opis
2	**Tylko konfiguruj** (przycisk radiowy)	Zaznacz tę opcję, jeśli zmieniasz konfigurację kontrolera MAC na głównym serwerze logowania do systemu DMS. **Patrz szczegółowe informacje poniżej.**
2	**Aktualizuj oprogramowanie** (przycisk radiowy)	Zaznacz tę opcję, jeśli instalujesz lub rekonfigurujesz kontroler MAC na jego własnym komputerze (serwerze kontrolera MAC), a nie na głównym serwerze logowania do systemu DMS. **Patrz szczegółowe informacje poniżej.**

Numery portów mają następujący schemat numeracji:
– W systemie niehierarchicznym, w którym istnieje tylko jeden serwer systemu DMS, każdy kontroler MAC i jego odpowiedni kontroler RMAC wysyłają dane z tego samego portu, zwykle o numerze 6000. System DMS może się komunikować tylko z jedną parą kontrolerów MAC/RMAC na raz.
– System DMS odbiera sygnały z pierwszego kontrolera MAC lub pary kontrolerów MAC/RMAC na porcie 6001, z drugiego kontrolera MAC lub pary kontrolerów MAC/RMAC na porcie 6002, i tak dalej.

Uwaga!
Port odbiorczy systemu DMS w systemach hierarchicznych
Zauważyć, że schemat numerowania portów odbiorczych systemu DMS jest inny w systemach hierarchicznych. Więcej informacji zawiera temat .

Ten parametr ma na celu odróżnianie oryginalnych kontrolerów MAC od kontrolerów RMAC:
– Wszystkie oryginalne kontrolery MAC mają numer 1.
– Wszystkie nadmiarowe kontrolery MAC przełączania awaryjnego (RMAC) mają numer 2.

Zaznacz tę opcję, aby zmienić konfigurację istniejącego kontrolera MAC na głównym serwerze systemu DMS, w szczególności w celu poinformowania go o nowo zainstalowanym kontrolerze RMAC na innym komputerze.
W takim przypadku w parametrze **Bliźniak** wprowadź adres IP lub nazwę hosta kontrolera RMAC.

Zaznacz tę opcję na komputerze innym niż główny serwer systemu DMS, aby zainstalować kontroler RMAC lub zmienić jego konfigurację.
W takim przypadku w parametrze **Bliźniak** wprowadź adres IP lub nazwę hosta bliźniaczego kontrolera MAC kontrolera RMAC.

12.2 Konfigurowanie kontrolerów LAC

Tworzenie lokalnego kontrolera dostępu AMC
Modułowe kontrolery dostępu (Access Modular Controller, AMC) są urządzeniami podrzędnymi głównych kontrolerów dostępu (Main Access Controller, MAC) w edytorze urządzeń.

Aby utworzyć kontroler AMC:

1. W edytorze urządzeń kliknij prawym przyciskiem myszy kontroler MAC i z menu kontekstowego wybierz polecenie **Nowy obiekt**
   lub
2. Kliknij przycisk ✚.
3. W wyświetlonym oknie dialogowym wybierz jeden z następujących typów kontrolerów AMC:

AMC 4W (domyślny) z czterema interfejsami czytników Wiegand umożliwiającymi podłączenie maksymalnie 4 czytników

AMC 4R4 z czterema interfejsami czytników RS485 umożliwiającymi podłączenie maksymalnie 8 czytników

Wynik: W hierarchii w edytorze urządzeń zostanie utworzona nowa pozycja kontrolera AMC wybranego typu.

AMC2 4W	**A**ccess **M**odular **C**ontroller (modułowy kontroler dostępu) z czterema czytnikami Wiegand.	Można skonfigurować maksymalnie cztery czytniki Wiegand w celu podłączenia maksymalnie czterech wejść. Kontroler obsługuje maksymalnie osiem sygnałów wejściowych i osiem wyjściowych. W razie potrzeby moduły rozszerzeń mogą zapewnić obsługę dodatkowych 48 sygnałów wejściowych i wyjściowych.
AMC2 4R4	**A**ccess **M**odular **C**ontroller (modułowy kontroler dostępu) z czterema interfejsami czytników RS485	Można skonfigurować maksymalnie osiem czytników RS485 w celu podłączenia maksymalnie ośmiu wejść. Kontroler obsługuje maksymalnie osiem sygnałów wejściowych i osiem wyjściowych. W razie potrzeby moduły rozszerzeń mogą zapewnić obsługę dodatkowych 48 sygnałów wejściowych i wyjściowych.
AMC2 8I-8O-EXT	Moduł rozszerzeń do kontrolera AMC z ośmioma sygnałami wejściowymi i wyjściowymi	Pozwala dodać obsługę większej liczby sygnałów. Do jednego kontrolera AMC można podłączyć maksymalnie trzy moduły rozszerzeń.
AMC2 16I-16O-EXT	Moduł rozszerzeń do kontrolera AMC z szesnastoma sygnałami wejściowymi i wyjściowymi	

AMC2 8I-8O-4W	Moduł rozszerzeń do kontrolera AMC Wiegand z ośmioma sygnałami wejściowymi i wyjściowymi	

Aktywacja/dezaktywacja kontrolerów

Od razu po utworzeniu nowy kontroler ma zaznaczoną następującą opcję (pole wyboru): **Komunikacja z hostem włączona**.

Powoduje ona otwarcie połączenia sieciowego między kontrolerem MAC a innymi kontrolerami, tak aby wszelkie zmienione lub rozszerzone dane konfiguracyjne były automatycznie rozpowszechniane do kontrolerów.

Podczas tworzenia wielu kontrolerów i ich urządzeń zależnych (wejścia, drzwi, czytniki, moduły rozszerzeń) wyłącz tę opcję, aby zmniejszyć obciążenie sieci i tym samym poprawić szybkość działania całego środowiska. W edytorze urządzeń urządzenia zostaną wtedy oznaczone szarymi ikonami.

WAŻNE: Pamiętaj o ponownym włączeniu tej opcji po zakończeniu konfigurowania urządzeń. Dzięki temu kontrolery będą na bieżąco aktualizowane o wszelkie zmiany konfiguracyjne dokonane na innych poziomach.

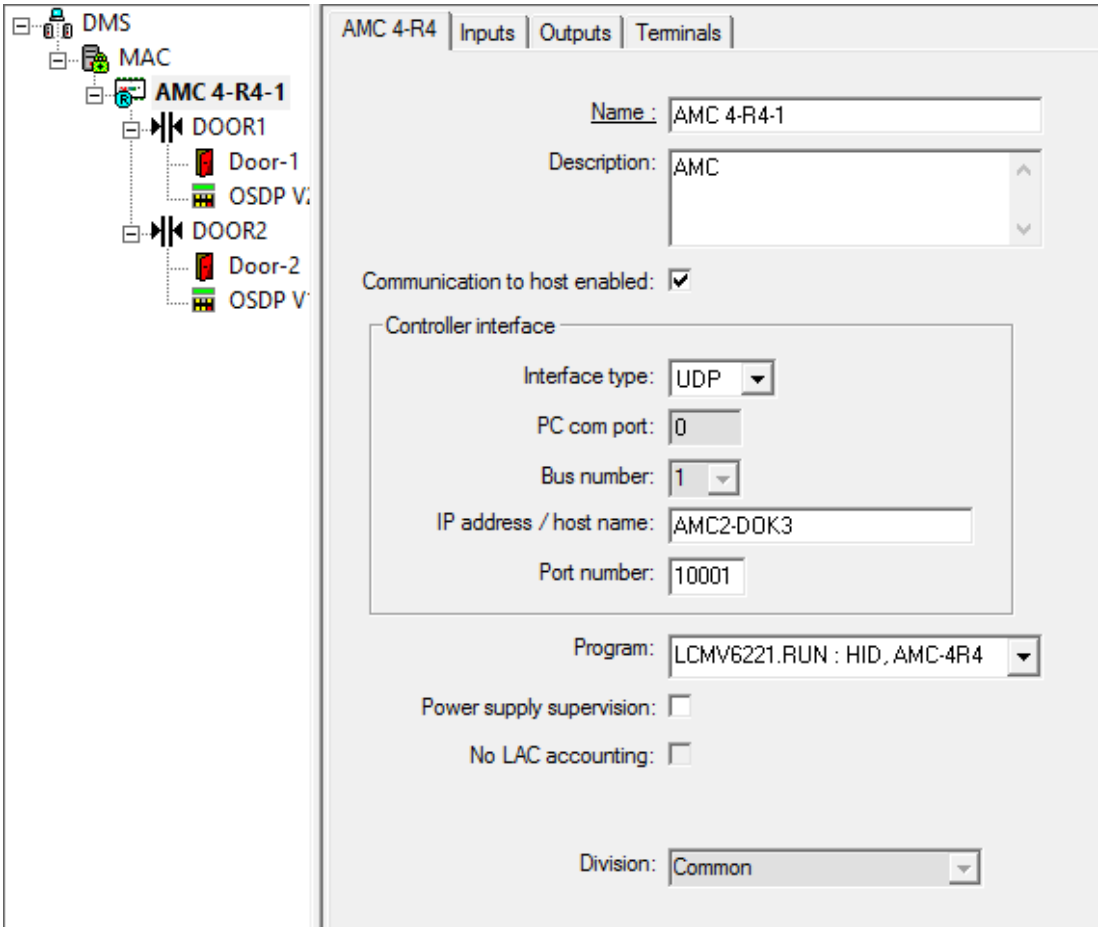
Mieszanie typów kontrolerów w jednej instalacji

Zazwyczaj systemy kontroli dostępu wyposaża się tylko w jeden typ kontrolerów i czytników. Uaktualnienia oprogramowania i rozrastające się instalacje mogą powodować konieczność uzupełniania istniejących składników sprzętowych o nowe. Możliwe są nawet konfiguracje łączące warianty RS485 (AMC 4R4) z wariantami Wiegand (AMC 4W), pod warunkiem przestrzegania następujących wymogów:

– Czytniki RS485 wysyłają „telegram”, który zawiera numer kodowy jako przeczytany.
– Czytniki Wiegand przesyłają swoje dane w taki sposób, że muszą one zostać odkodowane z pomocą definicji karty identyfikacyjnej, tak aby zachować numer kodowy we właściwej formie.
– Środowisko z kontrolerami mieszanymi może funkcjonować tylko wtedy, gdy oba numery kodowe są zbudowane tak samo.

12.2.1 Parametry i ustawienia kontrolera AMC

Ogólne parametry kontrolera AMC



Konfigurowanie parametrów kontrolera AMC

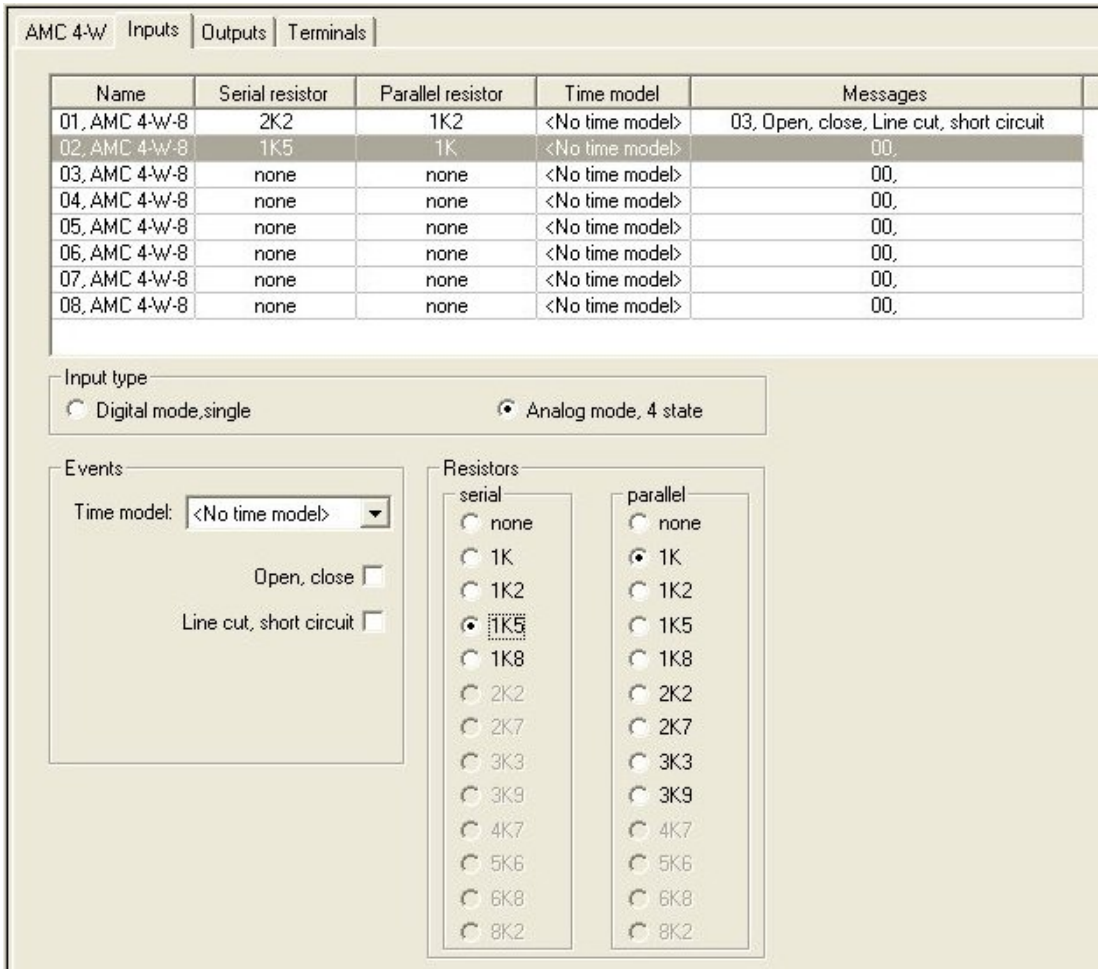
Parametr	Możliwe wartości	Opis
Nazwa kontrolera	Alfanumeryczne z ograniczeniami: 1–16 cyfr	Aparat generowania identyfikatorów (domyślnie) gwarantuje unikatowość nazw, ale można je indywidualnie zastępować. W przypadku ręcznego zastępowania użytkownik musi sam zagwarantować niepowtarzalność identyfikatorów. Dlatego zalecamy, aby w połączeniach sieciowych z serwerami DHCP używać nazw sieciowych.
Opis kontrolera	alfanumeryczne: 0–255 cyfr	Ten tekst jest wyświetlany w gałęzi serwera OPC.
Komunikacja z hostem włączona	0 = nieaktywne (pole wyboru jest wyczyszczone) 1 = aktywne (pole wyboru jest zaznaczone)	Wartość domyślna = aktywna To pole wyboru pokazuje aktualne ustawienie i może również służyć do jego zmiany. Status połączenia z hostem jest wskazywany przez następujące ikony w Eksploratorze: Wariant kontrolera: aktywne nieaktywne

		AMC2 4W   AMC2 4R4   Dezaktywacja pozwala utworzyć i skonfigurować urządzenia, które zostaną włączone do systemu kontroli dostępu w późniejszym terminie. Urządzenia nie powinny być aktywowane, a zatem dodawane do bazy danych hosta, dopóki nie będą potrzebne. Zmniejsza to również liczbę niepotrzebnych operacji sondowania urządzeń przez hosta.  Ze względów bezpieczeństwa po aktualizacji oprogramowania wszystkie kontrolery są ustawiane w trybie offline (pole wyboru jest wyczyszczone). Gwarantuje to, że instalacja będzie działać na starym oprogramowaniu, a uruchomienie nowego oprogramowania może się odbywać krok po kroku. Dołączaj nowe kontrolery do instalacji stopniowo, zaznaczając ich pola wyboru.
Interfejs kontrolera		
Typ interfejsu	COM UDP	COM, jeżeli połączenie z kontrolerem AMC odbywa się przez jeden z portów COM kontrolera MAC. UDP (User Datagram Protocol, protokół datagramów użytkownika), jeżeli połączenie odbywa się za pośrednictwem sieci. W przypadku wybrania tego typu połączenia można konfigurować parametry „nazwa hosta” i „port sterowany zdalnie”. 

		Przy interfejsie typu „UDP” w kontrolerze AMC należy **koniecznie** ustawić przełącznik DIP „5” na ON. Ponadto zaleca się ustawienie przełącznika „1” na ON.
Port COM komputera	liczbowe: z portami COM: 1–256 z portami UDP: 1–65535	Liczba portów COM, na których ten kontroler AMC łączy się z kontrolerem MAC. W przypadku połączeń ethernetowych za pośrednictwem konwerterów są generowane wirtualne porty COM i wyświetlane w tym miejscu. W przypadku typu „UDP” wprowadź port, przez który kontroler MAC będzie odbierał informacje z kontrolera AMC. Jeśli jest on nieznany, pole może pozostać puste, a wolny port zostanie wybrany automatycznie.
Numer magistrali	liczbowe: 1–8	Używając karty interfejsu AMC-MUX, można skonfigurować do 8 kontrolerów na jednym porcie COM. W takich przypadkach należy wprowadzić unikatowy adres każdego kontrolera AMC wynikający z ustawień jego przełączników DIP. **Uwaga:** Przełącznik 5 można zignorować, ponieważ do adresowania są wykorzystywane tylko pierwsze 4 przełączniki. W połączeniach przez UDP użyj ustawienia domyślnego (0).
Adres IP/nazwa hosta	Nazwa sieciowa lub adres IP kontrolera AMC	To pole danych wejściowych można ustawić tylko wtedy, gdy jako typ portu wybrano **UDP**. Jeśli adresy IP są przydzielane przez usługę DHCP, należy podać nazwę sieciową kontrolera AMC, tak aby kontroler AMC udało się odnaleźć po ponownym uruchomieniu nawet w razie zmiany adresu IP. W sieciach bez serwera DHCP należy podać adres IP.
Port UDP	liczbowe: 1–10001 — z domyślną konfiguracją	To pole danych wejściowych jest aktywowane tylko wtedy, gdy jako typ portu wybrano **UDP**. To jest port kontrolera AMC, na którym będą odbierane komunikaty z kontrolera MAC.
Inne parametry		

Program	alfanumeryczne	Nazwa pliku programu, który ma być wczytywany do kontrolera AMC. Dostępne programy znajdują się w katalogu BIN kontrolera MAC i można je wybierać z listy. Dla wygody są również wyświetlane protokół i opis. Ten parametr jest ustawiany automatycznie wraz z wczytywaniem programów i zależnie od podłączonych czytników, a w razie niezgodności czytnik/programu parametr jest nadpisywany.
Nadzorowanie zasilania	0 = nieaktywna (pole wyboru jest wyczyszczone) 1 = aktywna (pole wyboru jest zaznaczone)	Nadzór nad napięciem zasilającym. W razie spadku napięcia zasilającego zasilania jest generowany komunikat informacyjny. Na potrzeby generowania komunikatu funkcja nadzoru zakłada obecności zasilacza UPS. 0 = brak nadzoru 1 = nadzór aktywny
Brak ewidencjonowania LAC	0 = nieaktywna (pole wyboru jest wyczyszczone) 1 = aktywna (pole wyboru jest zaznaczone)	Zaznacz to pole wyboru dla urządzeń AMC, które wspólnie zapewniają dostęp do parkingów, przy czym tylko nadrzędny kontroler MAC ewidencjonuje liczbę jednostek wchodzących i wychodzących. **Zwróć uwagę**, że jeśli ta opcja zostanie zaznaczona, a kontroler AMC znajdzie się w trybie offline, kontroler nie będzie w stanie zapobiec dostępowi do przepełnionych obszarów, ponieważ nie zna pełnej liczebności.
Strefa	Wartość domyślna „Wspólna”	To jest pole informacyjne przeznaczone tylko do odczytu. „Strefy” to sposób podziału instalacji kontroli dostępu między wiele autonomicznych jednostek utworzonych i zarządzanych w programie BIS Manager.

Konfigurowanie wejść kontrolera AMC



To okno dialogowe jest podzielone na cztery panele:
- Lista wejść według nazwy
- Typy wejść
- Zdarzenia, które będą sygnalizowane przez wejścia
- Typy rezystorów używane w trybie analogowym

Parametry wejść

Parametry wejść kontrolera AMC opisano w poniższej tabeli:

Nazwa kolumny	Opis
Nazwa	Numeracja wejść (od 01 do 08) oraz nazwa odnośnego kontrolera AMC lub karty AMC-EXT.
Rezystor szeregowy	Wyświetlanie ustawionej wartości rezystora dla rezystora szeregowego. „brak” lub „---” = tryb cyfrowy
Rezystor równoległy	Wyświetlanie ustawionej wartości rezystora dla rezystora równoległego. „brak” lub „---” = tryb cyfrowy
Model czasowy	Nazwa wybranego modelu czasowego.

Komunikaty	Numer ewidencyjny i oznaczenie komunikatu, który zostanie wygenerowany. 00 = brak komunikatu 01 = jeśli zostały aktywowane wydarzenia **Otwórz**, **zamknij** 02 = jeśli zostały aktywowane wydarzenia **Przecięcie linii**, **zwarcie** 03 = jeśli zostały aktywowane oba rodzaje zdarzeń
Przypisane	W przypadku używania modelu wejścia 15 jest wyświetlana nazwa sygnału z przełącznika DIP.

Używając podczas klikania klawiszy Ctrl i Shift, można zaznaczyć kilka wejść jednocześnie. Wszelkie zmienione wartości zostaną powielone do wszystkich wybranych wejść.

Zdarzenia i modele czasowe

Zależnie od trybu działania są wykrywane i zgłaszane następujące stany drzwi: **Otwórz**, **Zamknięte**, **Przecięcie linii** i **Zwarcie**.

Zaznacz ich odpowiednie pola wyboru, aby umożliwić kontrolerowi AMC przekazywanie tych stanów jako zdarzeń do całego systemu.

Wybierz opcję **Model czasowy** z listy rozwijanej o tej samej nazwie, aby ograniczyć przesyłanie informacji o zdarzeniach do czasów określonych przez model. Na przykład zdarzenie **Otwórz** może być istotne tylko poza normalnymi godzinami pracy.

Typ wejścia

Rezystory mogą pracować w **trybie cyfrowym** lub **trybie analogowym (4 stany)**.

Ustawienie domyślne to **Tryb cyfrowy**: są wykrywane tylko stany drzwi **otwórz** i **zamknij**.

W trybie analogowym dodatkowo są wykrywane stany przewodów **Przecięcie linii** i **Zwarcie**.

Drzwi otwarte	suma wartości rezystorów szeregowych (R_S) i równoległych (R_P): $R_S + R_P$
Drzwi zamknięte	wartości rezystorów szeregowych: R_S
Przerwa w obwodzie	suma wartości rezystorów szeregowych (R_S) i równoległych (R_P) dąży do nieskończoności
Zwarcie w obwodzie	suma wartości rezystorów szeregowych (R_S) i równoległych (R_P) wynosi zero

Rezystory

W **trybie cyfrowym**, który jest domyślny, rezystory otrzymują wartość „brak” lub „---”.

W **trybie analogowym** wartości rezystorów szeregowych i równoległych można zmieniać, naciskając odpowiednie przyciski radiowe.

brak, 1K, 1K2, 1K5, 1K8, 2K2, 2K7, 3K3, 3K9, 4K7, 5K6, 6K8, 8K2 (podziałka 100 omów)

W zależności od wybranej wartości rezystora dla drugiego rezystora są dostępne tylko ograniczone zakresy.

Poniższe tabele pokazują w lewej kolumnie wybrane wartości, a w prawej kolumnie dostępne zakresy drugiego rezystora.

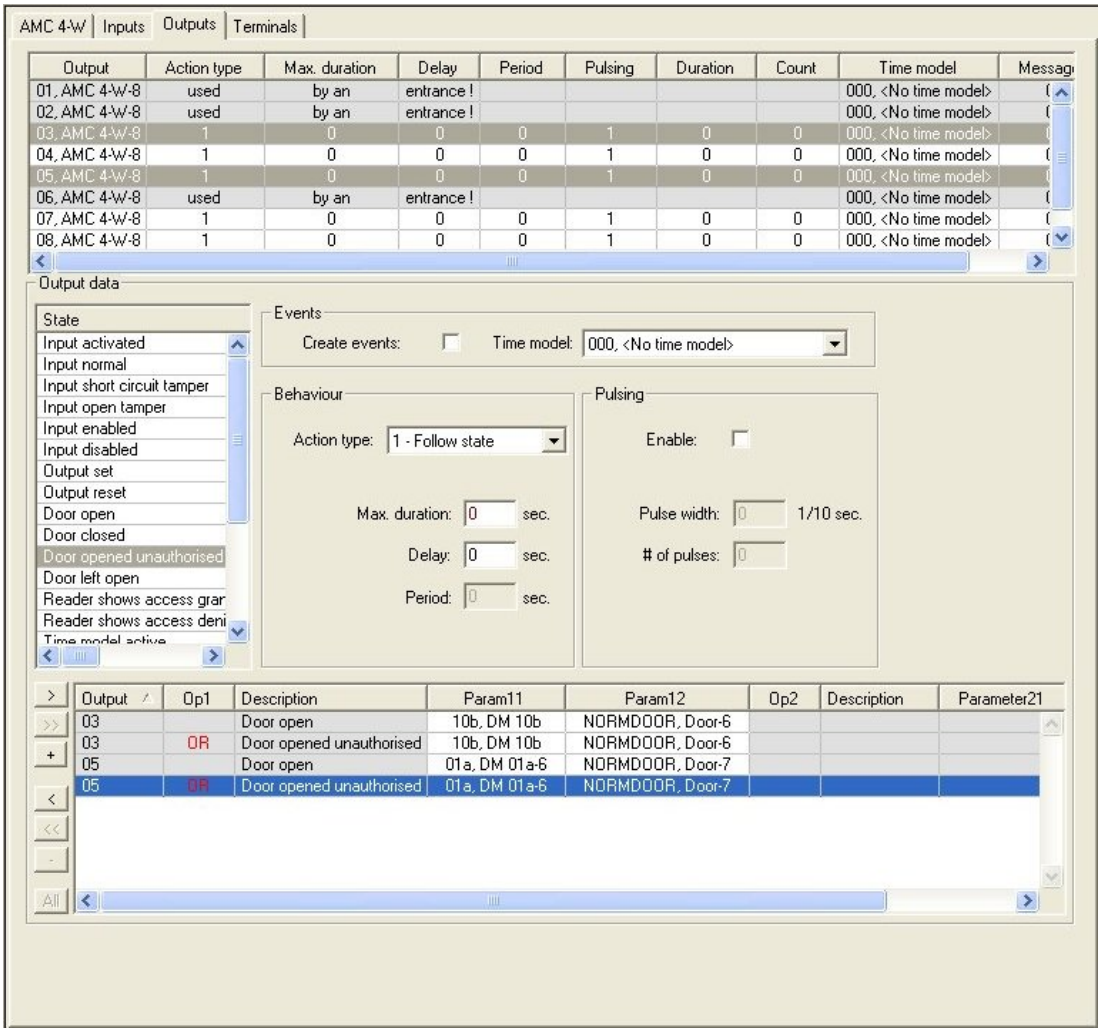
Szeregowy	**Zakres**		**Równoległy**	**Zakres**
„brak” lub „---”	Od 1K do 8K2		„brak” lub „---”	Od 1K do 8K2
1K	Od 1K do 2K2		1K	Od 1K do 1K8
1K2	Od 1K do 2K7		1K2	Od 1K do 2K7

1K5	Od 1K do 3K9		1K5	Od 1K do 3K3
1K8	Od 1K do 6K8		1K8	Od 1K do 3K9
2K2	Od 1K2 do 8K2		2K2	Od 1K do 4K7
2K7	Od 1K2 do 8K2		2K7	Od 1K2 do 5K6
3K3	Od 1K5 do 8K2		3K3	Od 1K5 do 6K8
3K9	Od 1K8 do 8K2		3K9	Od 1K5 do 8K2
4K7	Od 2K2 do 8K2		4K7	Od 1K8 do 8K2
5K6	Od 2K7 do 8K2		5K6	Od 1K8 do 8K2
6K8	Od 3K3 do 8K2		6K8	Od 1K8 do 8K2
8K2	Od 3K9 do 8K2		8K2	Od 2K2 do 8K2

Konfigurowanie wyjść kontrolera AMC — przegląd

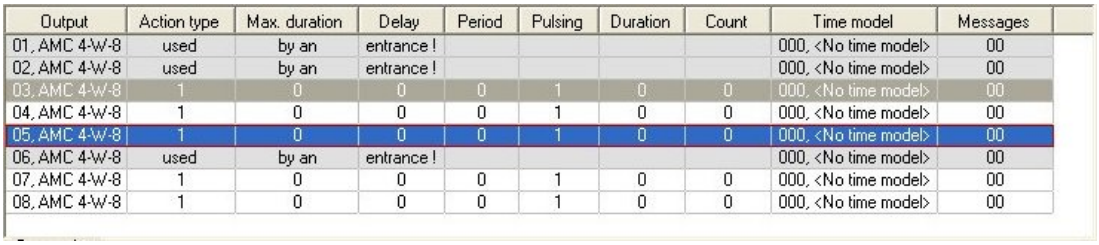
W tym oknie dialogowym można konfigurować poszczególne wyjścia kontrolera AMC lub karty AMC-EXT. Składa się ono z trzech głównych obszarów:

- Pole listy z przeglądem parametru ustawionego dla każdego wyjścia
- Opcje konfiguracyjne wyjść wybranych na liście
- Definicja warunków włączania wyjść



Wybieranie wyjść kontrolera AMC w tabeli

Aby skonfigurować styki wyjść, najpierw wybierz odpowiedni wiersz w górnej tabeli. W razie potrzeby używaj klawiszy Ctrl i Shift, aby zaznaczyć kilka wierszy. Zmiany wprowadzone w dolnej części okna będą miały wpływ tylko na wybrane wyjścia.



Output	Action type	Max. duration	Delay	Period	Pulsing	Duration	Count	Time model	Messages
01, AMC 4-W-8	used	by an	entrance !					000, <No time model>	00
02, AMC 4-W-8	used	by an	entrance !					000, <No time model>	00
03, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00
04, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00
05, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00
06, AMC 4-W-8	used	by an	entrance !					000, <No time model>	00
07, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00
08, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00

Wiersze, w których wyjścia zostały już przypisane przez model drzwi lub w inny sposób, są oznaczone kolorem jasnoszarym z informacją „**używane przez wejście!**”. Takich wyjść nie można dalej konfigurować.

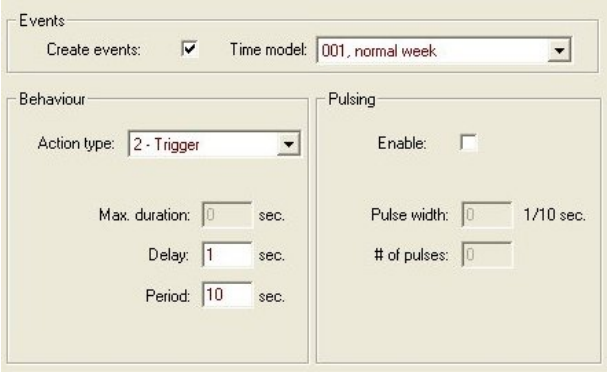
Wiersze zaznaczone przez Ciebie są w kolorze ciemnoszarym.

Parametry wyjść kontrolera AMC

Nazwa kolumny	**Opis**
Wyjście	bieżąca numeracja wyjść na odnośnym kontrolerze AMC lub karcie AMC-EXT Od 01 do 08 dla AMC i AMC_IO08 od 01 do 16 dla AMC_IO16
Typ czynności	oznaczenie wybranego typu czynności 1 = śledzenie stanu 2 = wyzwalanie 3 = naprzemiennie
Maks. czas trwania	długość sygnału w sekundach [1–9999; 0 = zawsze, jeśli drugi komunikat się nie pojawia] — tylko dla typu czynności „1”
Opóźnienie	opóźnienie w sekundach, po jakim sygnał jest podawany [0–9999] — tylko dla typów czynności „1” i „2”
Okres	okres w sekundach, przez jaki sygnał jest podawany — tylko dla typu czynności „2”
Impulsy	aktywacja impulsu — w przeciwnym razie sygnał jest podawany stale
Czas trwania	długość impulsu
Liczba	liczba impulsów na sekundę
Model czasowy	nazwa wybranego modelu czasowego
Komunikaty	oznaczenie działania w komunikacie 00 = brak komunikatu 03 = zdarzenia są zgłaszane
Przypisane	W przypadku używania modelu wejścia 15 jest wyświetlana nazwa sygnału z przełącznika DOP.

Wyjścia: Zdarzenia, Działanie, Impulsy

Wszystkie wpisy z listy powyżej są generowane za pomocą pól wyboru i pól danych wejściowych w oknie dialogowym w obszarach **Zdarzenia**, **Działanie** i **Impulsy**. Zaznaczenie pozycji na liście spowoduje podświetlenie odpowiednich ustawień w tych obszarach. Dotyczy to również zaznaczenia równocześnie kilku pozycji na liście, pod warunkiem, że parametry wszystkich zaznaczonych wyjść są takie same. Zmiany wartości parametrów są powielane do wszystkich wpisów zaznaczonych na liście.



Zaznacz pole wyboru **Utwórz zdarzenia**, jeśli chcesz wysyłać komunikat o aktywowaniu wyjścia. Jeśli komunikaty mają być wysyłane tylko w szczególnych okresach, np. nocą lub w weekendy, przypisz odpowiedni **model czasowy**.

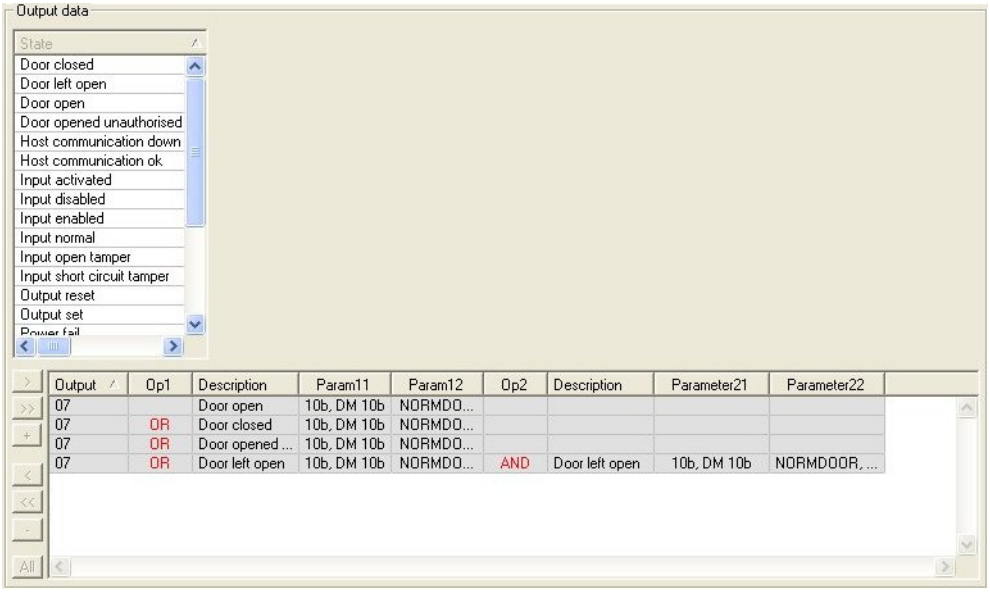
Dla poszczególnych typów czynności można ustawiać następujące parametry:

Typ czynności	**Maks. czas trwania**	**Opóźnienie**	**Okres**	**Pulsowanie/ Włącz**	**Szerokość impulsu**	**Liczba impulsów**
Śledzenie stanu	0 = zawsze 1 - 9999	0 - 9999	nie	tak	1 - 9999	Brak
Wyzwalanie	nie	0 - 9999	0–9999 jeśli pulsowanie **nie** jest włączone	tak wyłącza okres	1 - 9999	1 - 9999
Naprzemienie	nie	nie	nie	tak	1 - 9999	nie

Dane wyjściowe kontrolera AMC

Dolna część okna dialogowego **Wyjścia** zawiera:

– Pole listy ze **stanami** dostępnymi dla wybranych wyjść.
– Tabelę z wyjściami oraz skonfigurowanymi stanami, które mają je wyzwalać.



Konfigurowanie stanów wyzwalania wyjść

Wyjścia wybrane powyżej można skonfigurować w taki sposób, aby były inicjowane przez poszczególne stany lub logiczne kombinacje stanów.

– Zaznacz jedno lub kilka wyjść w górnym polu listy.
– Wybierz stan z listy **Stan**.
– Jeśli istnieje kilka urządzeń lub instalacji obsługujących wybrany stan, które mogą przekazywać informację o tym stanie, przycisk » jest aktywowany w dodatku do przycisku ›.

  Kliknij przycisk › (lub kliknij dwukrotne pole stanu), aby dla każdego wybranego wyjścia utworzyć pozycję jego statusu na pierwszym urządzeniu (na przykład „Kontroler AMC, pierwsze wejście”) i w instalacji (na przykład „Pierwszy sygnał, pierwsze drzwi”).

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2

  Kliknięcie przycisku » spowoduje przesłanie wybranego statusu do listy i połączenie go ze skrótem OR dla każdego zainstalowanego urządzenia (na przykład dla wszystkich kontrolerów AMC przy wejściach).

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 02, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 03, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 04, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 05, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 06, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 07, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 08, AMC 4-W-2

– Do jednego skrótu OR można przypisać kilka stanów.

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Door open	06a, Timemgm	<< !!! >>

Możliwe są również skróty z operatorem AND:

– Musi już być przypisany status. Do niego jest dodawany warunek poprzez wybranie w dowolnej kolumnie.
– Następnie wybiera się inny status i łączy z zaznaczonym statusem, klikając przycisk .

Exit	Operand1	Description	Param11	Param12	Operand2	Description	Parameter21	Parameter22
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2				
04	OR	Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2				
04	OR	Door open	06a, Timemgm	<< !!! >>	AND	Door opened unauthorised	06a, Timemgm	<< !!! >>

Uwaga!
Każdemu wyjściu można przypisać maks. 128 skrótów OR.
W przypadku każdego przypisanego warunku można utworzyć **jeden** skrót AND.

Po przypisaniu statusu do urządzenia lub instalacji można go przypisać również do wszystkich innych istniejących urządzeń i instalacji.

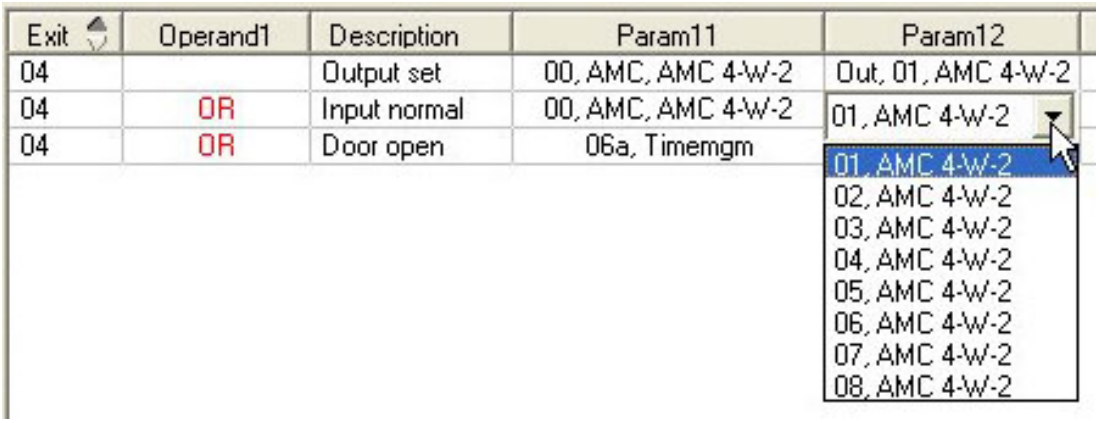
– Zaznacz przypisaną pozycję w dowolnej kolumnie.
– Następnie kliknij przycisk All, a ten status zostanie utworzony dla wszystkich istniejących urządzeń i instalacji.

Modyfikowanie parametrów wyjść

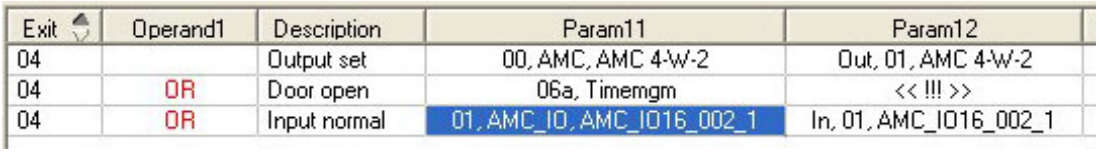
Pozycje list można zmieniać.
Jeżeli istnieje kilka urządzeń lub instalacji, w których przypisany status może zaistnieć, zawsze się ustawia pierwsze urządzenia i instalacje danego typu.
W kolumnach **Param11** i **Param21** (ze skrótami AND) są wyświetlane urządzenia (na przykład „Kontroler AMC, wejście”). Kolumny **Param12** i **Param22** zawierają wpisy instalacji specjalnych (na przykład „Sygnał wejściowy, drzwi, czytnik”).
Jeśli istnieje kilka urządzeń (na przykład kart we/wy) lub instalacji (na przykład dodatkowe sygnały i czytniki), wskaźnik myszy zmienia się podczas wskazywania kolumny.

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Door open	06a, Timemgm	<< !!! >>

Dwukrotne kliknięcie pozycji w kolumnie powoduje dodanie przycisku z listą rozwijaną prawidłowych wpisów dla parametru.



Zmiana wartości wpisów w kolumnach **Param11** i **Param21** powoduje aktualizację wpisów w kolumnach **Param12** i **Param22**:



Uwaga!
Jest to możliwe tylko w przypadku kolumn **Param11**, **Param12**, **Param21** i **Param22**.
Jeśli nie ma innych opcji (na przykład dlatego, że skonfigurowano tylko jedno wejście), wskaźnik myszy nie zmieni się i wszystkie pola będą szare. Dwukrotne kliknięcie tej pozycji zostanie zinterpretowane jako polecenie usunięcia i pojawi się pole komunikatu do weryfikacji operacji usuwania.

Usuwanie stanów wyzwalających wyjścia
Zaznaczone przypisania można usunąć, klikając przycisk „**<**” (lub dwukrotnym kliknięciem pozycji na liście). W polu komunikatu będzie widać monit o potwierdzenie zamiaru usunięcia.

Jeśli z wynikiem skojarzono kilka różnych stanów, można usunąć je wszystkie razem w następujący sposób:
- Zaznacz pierwszy wpis na liście (ten, który nie ma wartości w kolumnie **Op1**), a następnie kliknij przycisk „**<<**”.
- Alternatywnie kliknij dwukrotnie pierwszy wpis.
  - Pojawi się wyskakujące okno. Potwierdź lub anuluj zamiar usunięcia.
  - Jeśli potwierdzisz usunięcie, w drugim wyskakującym oknie zobaczysz pytanie, czy chcesz usunąć wszystkie powiązane wpisy (odpowiedź **Tak**), czy tylko wybraną pozycję (odpowiedź **Nie**).

Aby usunąć dodatkowe stany dookreślające pierwszy stan za pomocą operatora AND w kolumnie **Op2**, kliknij w dowolnym miejscu wiersza, a następnie kliknij przycisk „minus”, który jest aktywny tylko wtedy, gdy w tym wierszu znajduje się dookreślający stan z operatorem AND.

Opisy stanów
Poniższa tabela zawiera przegląd wszystkich stanów dostępnych do wyboru, ich liczbowych oznaczeń typów i opisów.
Pole listy **Stan** również zawiera te parametry — są one widoczne po przewinięciu listy w prawo.

Stan	Typ	Opis

Wejście zostało aktywowane	1	Lokalne wejście
Wejście normalne	2	Lokalne wejście
Sabotaż zwarcia wejścia	3	Skonfigurowano lokalne wejście z rezystorem
Sabotażowe otwarcie wejścia	4	Skonfigurowano lokalne wejście z rezystorem
Wejście włączono	5	Aktywacja lokalnego wejścia przez model czasowy
Wejście wyłączono	6	Dezaktywacja lokalnego wejścia przez model czasowy
Ustawienie wyjścia	7	Lokalne wyjście, wyjście niebieżące
Resetowanie wyjścia	8	Lokalne wejście, wejście niebieżące
Drzwi otwarte	9	GID wejścia, numer drzwi
Drzwi zamknięte	10	GID wejścia, numer drzwi
Nieautoryzowane otwarcie drzwi	11	GID wejścia, numer drzwi, zmiana otwartych drzwi (9)
Drzwi pozostawione otwarte	12	GID wejścia, numer drzwi
Czytnik pokazuje uprawnienia dostępu	13	Adres czytnika
Czytnik pokazuje odmowę dostępu	14	Adres czytnika
Model czasowy aktywny	15	Skonfigurowany model czasowy
Czytnik układu antysabotażowego	16	Adres czytnika
Układ antysabotażowy AMC	17	---
Moduł we/wy układu antysabotażowego	18	---
Awaria zasilania	19	dotyczy tylko AMC zasilanych z baterii
Zasilanie włączone	20	dotyczy tylko AMC zasilanych z baterii
Komunikacja z hostem OK	21	---
Komunikacja z hostem nie działa	22	---
Komunikaty czytnika	23	(szczegóły zależą od aktualnej wersji oprogramowania)
Komunikaty LAC	24	(szczegóły zależą od aktualnej wersji oprogramowania)

Konfigurowanie wyjść

Poza przypisywaniem sygnałów za pomocą modeli drzwi lub indywidualnego przypisania można definiować warunki dla nieprzydzielonych jeszcze wyjść. Po wystąpieniu tych warunków następuje uaktywnienie wyjścia zgodnie z ustawionym parametrem.

Musisz zdecydować, co będzie przełączane na wyjściu. W przeciwieństwie do sygnałów, które można powiązać z konkretnym modelem drzwi, drzwiami i czytnikami, w tym przypadku można zastosować sygnały wszystkich urządzeń i instalacji podłączonych do kontrolera AMC.

Jeżeli na przykład sygnał optyczny, sygnał akustyczny lub komunikat do modułu UGM ma być wyzwalany przez sygnały wejściowe **Sabotaż zwarcia wejścia** i **Nieautoryzowane otwarcie drzwi**, to wejście lub wejścia, które mogą być brane pod uwagę, są przypisane do odpowiedniego wyjścia docelowego.
Przykład, w którym wybrano tylko jeden styk w każdym przypadku:

Exit	Operand1	Description	Param11	Param12
04		Input short cir...	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Door opened ...	06a, Timemgm	<< !!! >>

Przykład ze wszystkimi stykami:

Exit	Operand1	Description	Param11	Param12
04		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 08, AMC 4-W-2
04	OR	Door opened unauthorised	06a, Timemgm	---
04	OR	Door opened unauthorised	03a, Entrance B:B	REVDOOR, Revolving Door

Przykład z wybranymi stykami:
Dla każdego styku jest tworzony jeden wpis poprzez kliknięcie przycisku » lub usunięcie niepotrzebnych styków po przypisaniu wszystkich styków:

Exit	Operand1	Description	Param11	Param12
04		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
04	OR	Door opened unauthorised	06a, Timemgm	---
04	OR	Door opened unauthorised	03a, Entrance B:B	REVDOOR, Revolving Door

Te same warunki można zastosować do kilku wyjść, jeśli na przykład oprócz sygnału optycznego jest również potrzebny sygnał akustyczny, a dodatkowo powinien być wysyłany komunikat do modułu UGM:

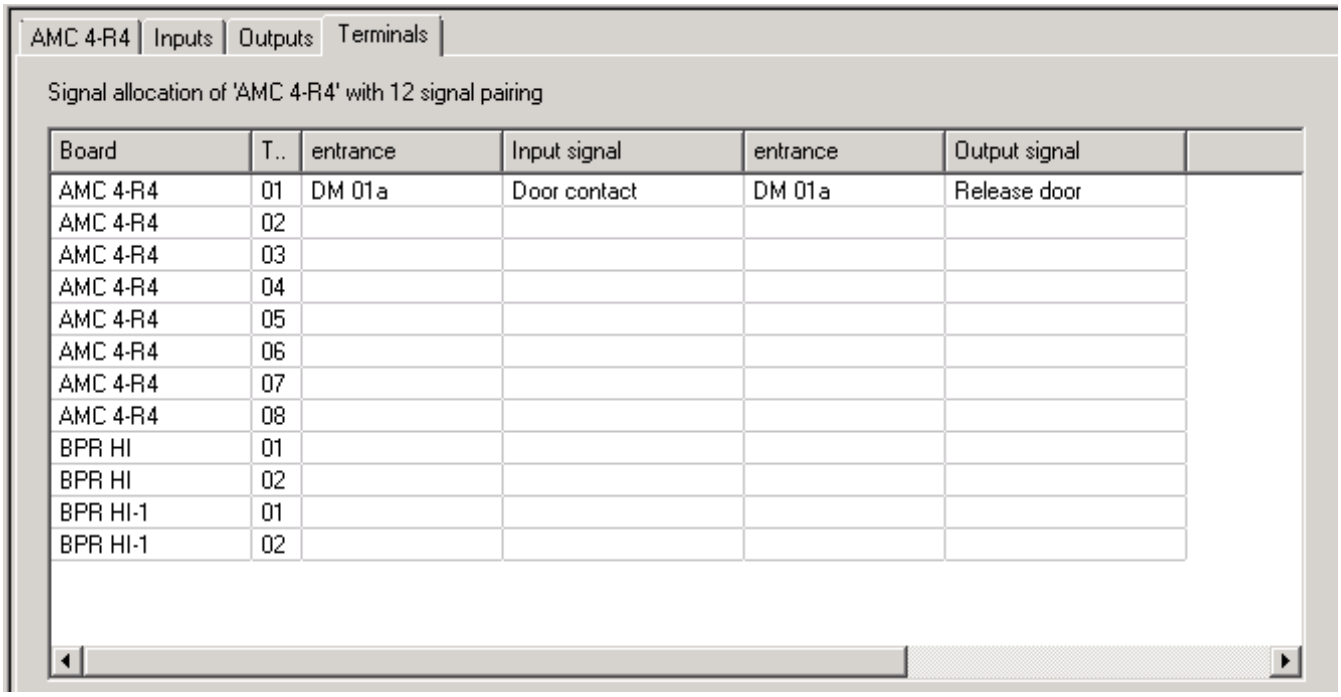
Exit	Operand1	Description	Param11	Param12
04		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 08, AMC 4-W-2
04	OR	Door opened unauthorised	06a, Timemgm	<< !!! >>
04	OR	Door opened unauthorised	03a, Entrance B:B	REVDOOR, Revolving Door
06		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 08, AMC 4-W-2
06	OR	Door opened unauthorised	06a, Timemgm	<< !!! >>
07		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2

Lista wszystkich istniejących stanów z wartościami domyślnymi dla parametrów 11/21 i 12/22:

Description	Param11	Param12
Input activated	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input open tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input enabled	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input disabled	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
Output reset	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
Door open	06a, Timemgm	<< !!! >>
Door closed	06a, Timemgm	<< !!! >>
Door opened unauthorised	06a, Timemgm	<< !!! >>
Door left open	06a, Timemgm	<< !!! >>
Reader shows access granted	---	TM-Reader IN
Reader shows access denied	---	TM-Reader IN
Time model active	---	000, <No time model>
Tamper reader	---	TM-Reader IN
Tamper AMC	---	---
Tamper I/O board	---	00, AMC, AMC 4-W-2
Power fail	---	---
Power good	---	---
Host communication ok	---	---
Host communication down	---	---

Definiowanie sygnałów na karcie Terminale

Karta **Terminale** zawiera listę przypisań styków w kontrolerze AMC lub na karcie AMC-EXT. Po utworzeniu wejść przypisania sygnałów są oznaczane zgodnie z wybranym modelem drzwi. Nie można wprowadzać modyfikacji na karcie **Terminale** kontrolera ani modułów rozszerzeń. Edycja jest możliwa tylko na karcie Terminali na stronie wejścia. Z tego powodu ustawienia terminalu są wyświetlane na szarym tle. Wejścia wyświetlane na czerwono wskazują konfiguracje sygnałów odpowiednich wyjść.



Board	T..	entrance	Input signal	entrance	Output signal
AMC 4-R4	01	DM 01a	Door contact	DM 01a	Release door
AMC 4-R4	02				
AMC 4-R4	03				
AMC 4-R4	04				
AMC 4-R4	05				
AMC 4-R4	06				
AMC 4-R4	07				
AMC 4-R4	08				
BPR HI	01				
BPR HI	02				
BPR HI-1	01				
BPR HI-1	02				

13 Konfigurowanie wejść

13.1 Wejścia — wprowadzenie

Określenie wejście oznacza cały mechanizm kontroli dostępu w punkcie wejścia:
Elementy wejścia:

- Czytniki dostępowe — od 1 do 4.
- Pewna forma bariery, na przykład drzwi, bramka obrotowa, śluza osobowa lub szlaban.
- Procedura dostępu zdefiniowana przez wstępnie skonfigurowane sekwencje sygnałów elektronicznych przekazywanych między elementami sprzętowymi.

Model drzwi to szablon określonego rodzaju wejścia. Opisuje istniejące elementy drzwi (liczba i typ czytników, typ drzwi lub bariery itp.) oraz wymusza określony proces kontroli dostępu z sekwencjami wstępnie zdefiniowanych sygnałów.
Modele drzwi znacznie ułatwiają konfigurowanie systemu kontroli dostępu.

Model drzwi 1	Proste lub zwykłe drzwi
Model drzwi 3	Kontrolowana bramka obrotowa do wchodzenia i wychodzenia
Model drzwi 5	Wjazd na parking lub wyjazd z niego
Model drzwi 6	Czytniki dla osób wchodzących/wychodzących do rejestracji czasu i udziału
Model drzwi 7	Sterowanie windą
Model drzwi 9	Szlaban i brama rolowana
Drzwi model 10	Proste drzwi z funkcją uzbrojenia/rozbrojenia systemu sygnalizacji włamania (SSW)
Model drzwi 14	Proste drzwi z funkcją uzbrojenia/rozbrojenia systemu SSW i specjalnymi uprawnieniami dostępu
Model drzwi 15	Niezależne sygnały wejściowe i wyjściowe

- Modele drzwi 1, 3, 5, 9 i 10 zawierają opcję dla dodatkowych czytników kart po stronie wchodzenia lub wychodzenia.
- Lokalny kontroler dostępu używany w modelu drzwi 05 (parking) lub 07 (winda) nie może być współdzielony z innym modelem drzwi.
- Gdy wejście zostanie skonfigurowane z modelem drzwi i zapisane, nie można zmienić modelu drzwi na inny. Jeśli jest wymagany inny model drzwi, należy usunąć wejście i skonfigurować je od nowa.

Niektóre modele drzwi mają warianty (a, b, c, r) o następujących cechach:

a	czytniki przychodzących **i** wychodzących
b	czytnik wchodzących i przycisk dla wychodzących
c	czytnik dla wchodzących **LUB** wychodzących (nie oba — to byłby wariant **a**)
r	(Tylko model drzwi 1) Jeden czytnik wyłącznie w celu rejestracji osób w miejscu zbiórki, na przykład w przypadku ewakuacji. W tym modelu drzwi nie ma żadnej fizycznej bariery.

Przycisk **OK** kończący konfigurowanie staje się aktywny dopiero po wprowadzeniu wszystkich obowiązkowych wartości. Na przykład modele drzwi wariantu (a) wymagają czytników dla osób wchodzących **i** wychodzących. Wpisy można zapisać dopiero po wybraniu typów dla obu czytników.

13.2 Tworzenie wejść

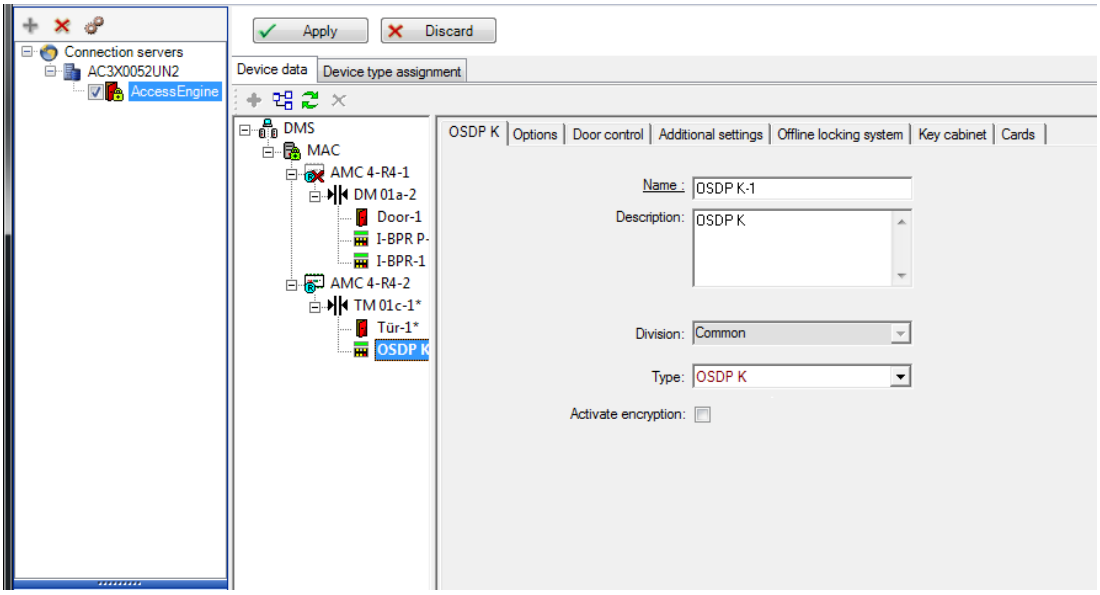
Lista czytników wyświetlanych do wyboru będzie dostosowana do wybranego typu kontrolera.

– Dla kontrolerów typu **AMC 4W** są dostępne tylko czytniki Wiegand, z klawiaturą lub bez.
– Dla kontrolerów typu **AMC 4R4** są dostępne czytniki podane w tabeli poniżej. Nie mieszaj protokołów na tym samym kontrolerze.

Nazwa czytnika	Protokół Wiegand	Protokół BPR	Protokół I-BPR	Protokół HID
WIE1	X			
WIE1K (z klawiaturą)	X			
BPR MF		X		
BPR MF z klawiaturą		X		
BPR LE		X		
BPR LE z klawiaturą		X		
BPR HI		X		
BPR HI z klawiaturą		X		
TA40 LE		X		
TB30 LE		X		
TB15 HI1		X		
INTUS 1600			X	
I-BPR			X	
I-BPR K (z klawiaturą)			X	
DT 7020			X	
OSDP				X
OSDP K (z klawiaturą)				X
OSDP KD (z klawiaturą i wyświetlaczem)				X
HADP				X
HADP K (z klawiaturą)				X
HADP KD (z klawiaturą i wyświetlaczem)				X
RKL 55 (z klawiaturą i ekranem LCD)				X
RK40 (z klawiaturą)				X

R40				X
R30				X
R15				X

W przypadku **czytnika OSDP** okno dialogowe wygląda następująco:



Dostępne są następujące typy czytników OSDP:

OSDP	Standardowy czytnik OSDP
OSDP z klawiaturą	Czytnik OSDP z klawiaturą
OSDP klaw.+wyśw.	Czytnik OSDP z klawiaturą i wyświetlaczem

Przetestowano następujące czytniki OSDP:

OSDPv1 — tryb niezabezpieczony	LECTUS duo 3000 C — MIFARE classic LECTUS duo 3000 CK — MIFARE classic LECTUS duo 3000 E — MIFARE Desfire EV1 LECTUS duo 3000 EK — MIFARE Desfire EV1
OSDPv2 — tryby niezabezpieczony i zabezpieczony	LECTUS secure 2000 RO LECTUS secure 4000 RO LECTUS secure 5000 RO

Uwaga!

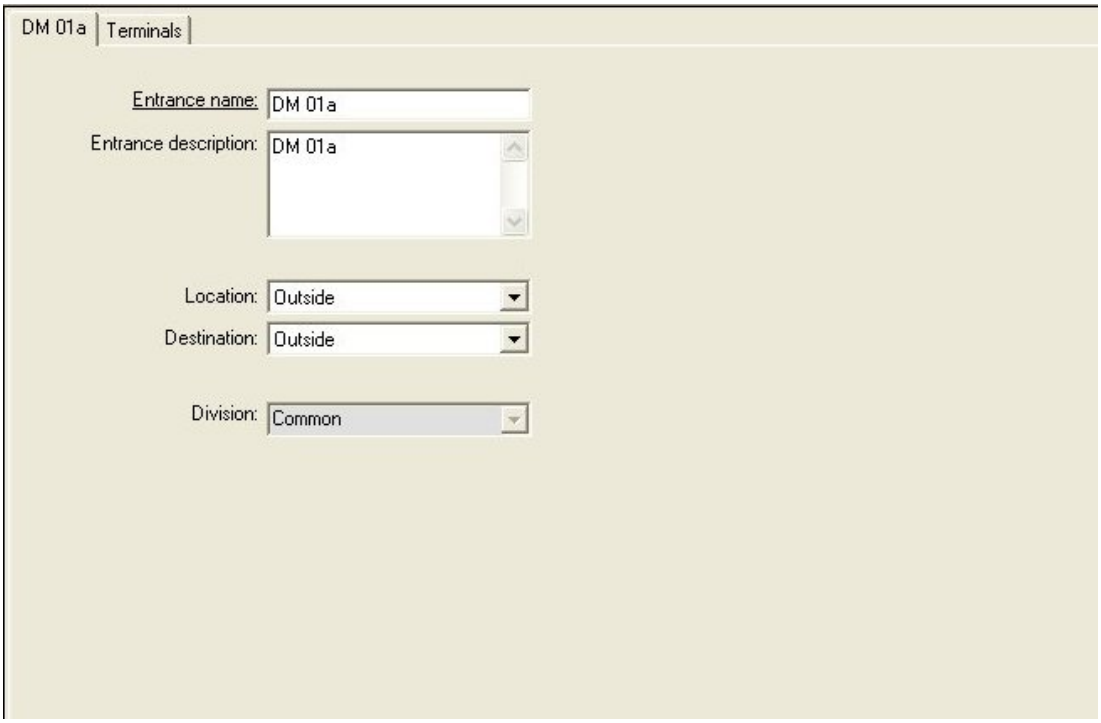
Uwagi dotyczące czytników OSDP

Nie mieszaj produktów z różnych rodzin, np **LECTUS duo** i **LECTUS secure**, na tej samej magistrali czytników OSDP.

W celu szyfrowanej transmisji danych do czytnika OSDP jest generowany i wykorzystywany klucz klienta. Upewnij się, że system ma poprawną kopię zapasową.

Trzymaj klucze w bezpiecznym miejscu. Utraconych kluczy nie można odzyskać, w takich przypadkach trzeba resetować czytnik do ustawień fabrycznych.

Ze względów bezpieczeństwa nie mieszaj trybów szyfrowanych i nieszyfrowanych na tej samej magistrali czytników OSDP.



Parametr	Możliwe wartości	Opis
Nazwa wejścia	Alfanumeryczne, od 1 do 16 znaków	Okno dialogowe generuje unikatową nazwę wejścia, ale w razie potrzeby może ją zastąpić operator konfigurujący wejście.
Opis wejścia	Alfanumeryczne, od 0 do 255 znaków	Dowolny tekst opisowy do wyświetlenia w systemie.
Lokalizacja	Dowolny zdefiniowany obszar (inny niż parking)	Nazwany obszar (zgodnie z definicją w systemie), w którym znajduje się czytnik. Ta informacja służy do kontroli kolejności dostępu: jeśli osoba próbuje użyć tego czytnika, ale obecna lokalizacja tej osoby (śledzona przez system) różni się od lokalizacji czytnika, to czytnik odmówi tej osobie dostępu.
Obszar docelowy	Dowolny zdefiniowany obszar (inny niż parking)	Nazwany obszar, zgodnie z definicją w systemie, do którego czytnik umożliwia dostęp. Ta informacja służy do kontroli kolejności dostępu: jeśli osoba użyje tego czytnika, jej lokalizacja zostanie zaktualizowana o wartość z pola **Obszar docelowy**.

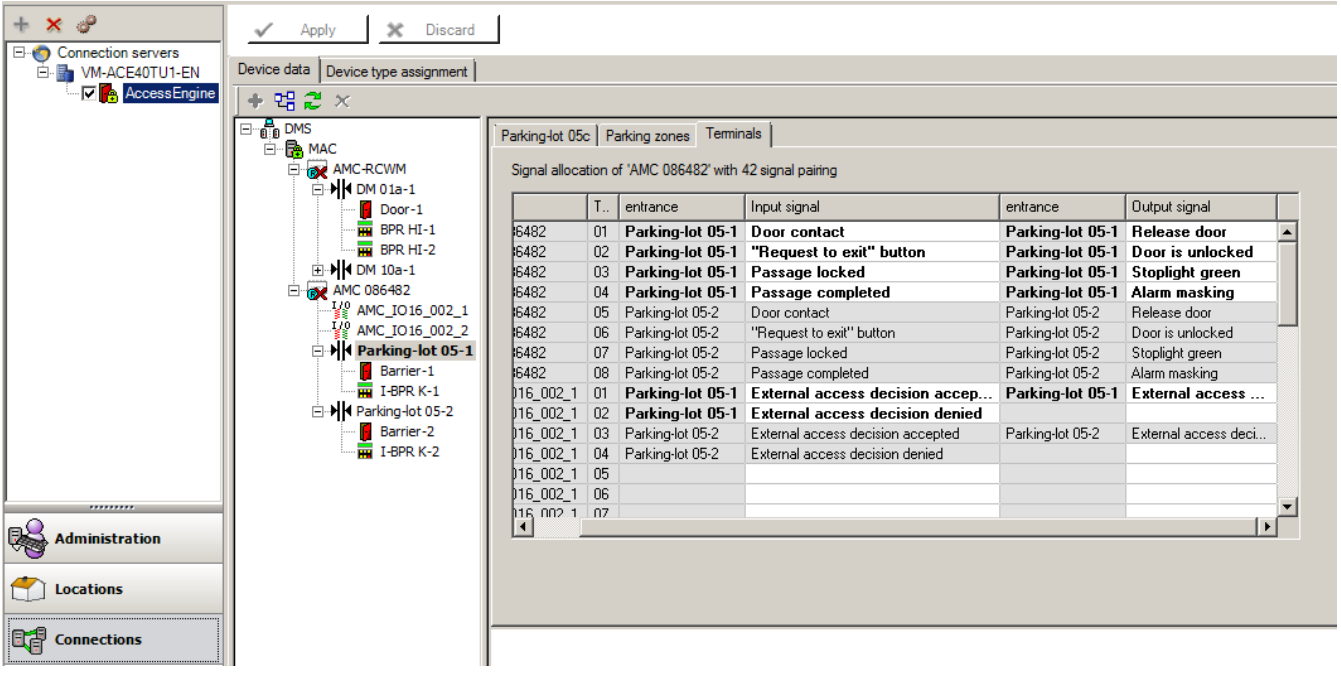
Czas oczekiwania na zewnętrzną decyzję o dostępie	Liczba dziesiątych części sekundy	Czas, przez jaki kontroler dostępu czeka na decyzję z systemu kontroli dostępu. zanim podejmie własną decyzję.
Strefa	Pole tylko do odczytu	Zdefiniowana strefa, do której należy czytnik. Strefą domyślną jest **Wspólna**.
Opóźnienie urządzenia alarmowego (tylko dla modeli wejść 10 i 14)	100 - 9999	Przedział czasu, w którym automat do otwierania drzwi może być aktywowany bez wywoływania alarmu. Jest to parametr czytnika, który należy ustawić, po czym jest on wysyłany do czytników. Jednostką tego parametru jest jedna dziesiąta (1/10) sekundy.
Uzbrajanie obszaru (tylko dla modelu wejścia 14)	Jedna litera: od A do Z	Wejścia grupy urządzeń w systemie sygnalizacji włamania (SSW) będą aktywowane razem wskutek aktywacji czytników w obszarze.

13.3 Dodatkowe kontrole we/wy

Dodatkowe kontrole we/wy mogą na przykład pomagać w identyfikowaniu gości przy użyciu systemu automatycznego rozpoznawania tablic rejestracyjnych (ANPR).
Kontroler AMC otrzymuje 1 sygnał wejściowy przez swój styk we/wy:

– Gość autoryzowany przez dodatkową kontrolę we/wy

Kontroler AMC uniemożliwia dostęp w przypadku sygnału „Nie autoryzowano”.



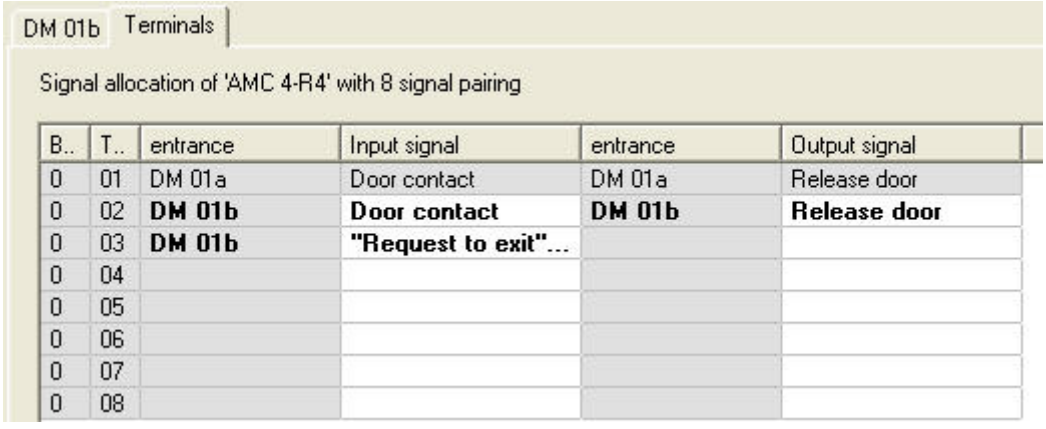
Stan karty	**Sygnał = 1: autoryzacja przez ANPR**	**Sygnał = 0: brak autoryzacji przez ANPR**

Karta autoryzowana	Dostęp	Zdarzenie „Nieprawidłowy numer pojazdu”
Karta na czarnej liście	Nie autoryzowano — czarna lista	Nie autoryzowano — czarna lista
Upłynął okres ważności karty	Nie autoryzowano — wygaśnięcie	Nie autoryzowano — wygaśnięcie
Karta nieautoryzowana dla tego czytnika	Nie autoryzowano	Nie autoryzowano

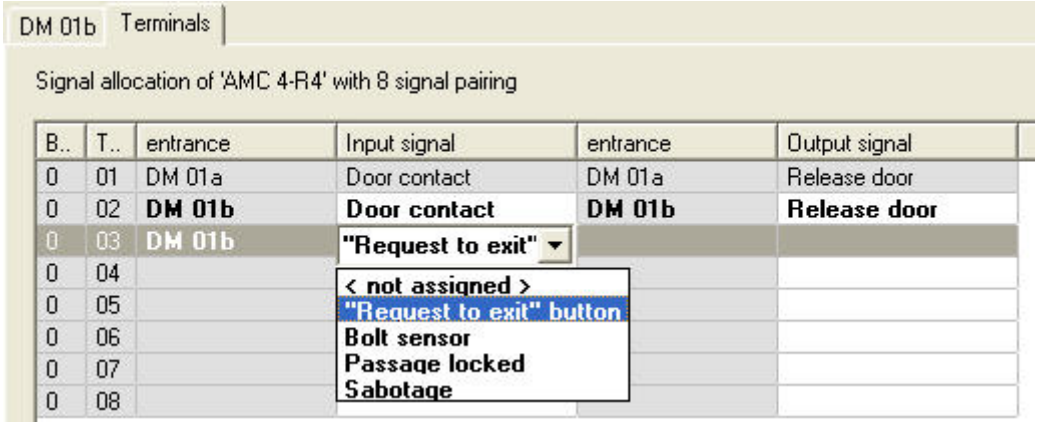
Istnieje możliwość ręcznego otwarcia bariery, nawet jeśli gość nie został rozpoznany.
Na potrzeby obsługi tej funkcjonalności do styków wejścia/wyjścia kontrolera AMC podłącza się przełącznik.
Kontroler AMC ustawia sygnał wyjściowy **Dodatkowa kontrola aktywna** przed analizą sygnału wejściowego.
Podczas rejestracji nowego gościa informacje z tablicy rejestracyjnej muszą zostać wprowadzone przez operatora w systemach BIS (na potrzeby raportów) i ANPR (w celu sprawdzenia).
System ANPR rozpozna zarejestrowany pojazd w swojej bazie danych.

13.4 Konfigurowanie terminali kontrolerów AMC

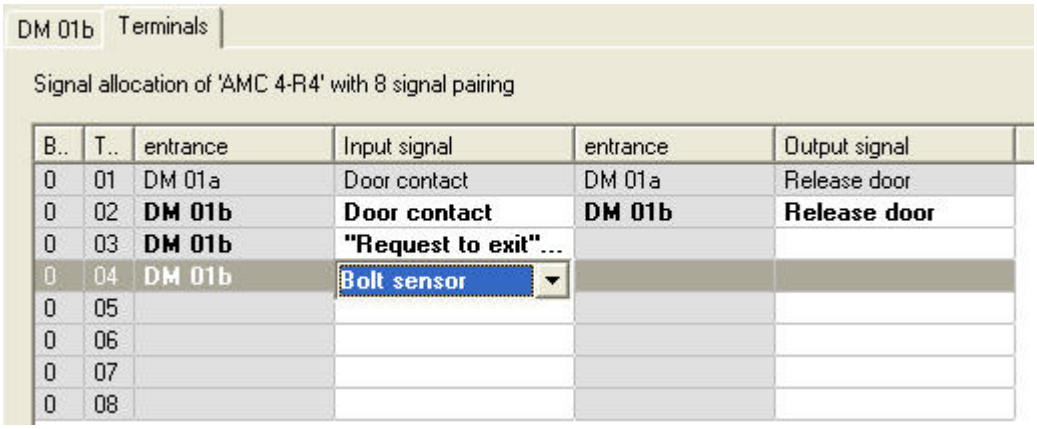
Pod względem zawartości i struktury ta karta jest identyczna z kartą **Terminale** w ustawieniach kontrolera AMC.



Tutaj jednak można zmienić przypisania sygnałów do wybranego modelu wejścia. Dwukrotne kliknięcie w kolumnie **Sygnał wyjściowy** lub **Sygnał wejściowy** spowoduje otwarcie pól kombi.



Podobnie można utworzyć dodatkowe sygnały dla odnośnego wejścia. Dwukrotne kliknięcie pustego wiersza spowoduje wyświetlenie odpowiedniego pola kombi:



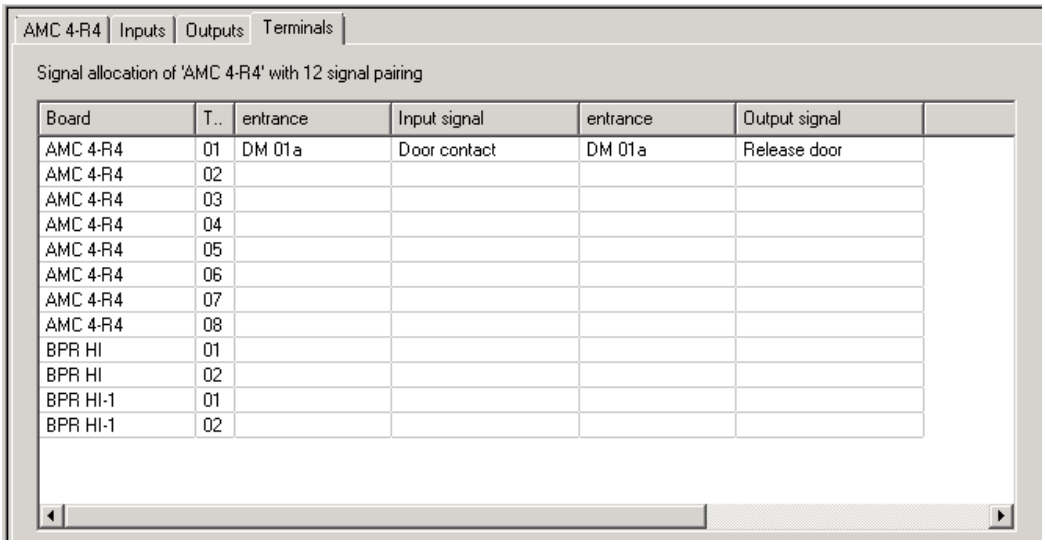
Przypisania sygnałów nieodpowiednie dla edytowanego wejścia są tylko do odczytu i mają szare tło. Można je edytować tylko po wybraniu odpowiedniego wejścia.
Podobne szare tło i blady kolor pierwszego planu są ustawiane dla wyjść, których parametry skonfigurowano karcie **Wyjścia** w ustawieniach kontrolera AMC.

Uwaga!
Pola kombi nie są całkowicie zależne od kontekstu, dlatego można wybrać sygnały, które nie będą działać w warunkach realnych. Jeśli dodasz lub usuniesz sygnały na karcie **Terminale**, przetestuj je, aby uzyskać pewność, że są logicznie i fizycznie zgodne z wejściem.

Przypisywanie terminala
Dla każdego kontrolera AMC i każdego wejścia karta **Terminal** zawiera listę wszystkich 8 sygnałów kontrolera AMC w 8 osobnych wierszach. Nieużywane sygnały są oznaczone na biało, a używane na niebiesko.
Lista ma następującą strukturę:

- **Moduł**: numer modułu rozszerzeń Wiegand kontrolera AMC (0) lub modułu rozszerzeń we/wy (od 1 do 3)
- **Terminal**: numer styku w kontrolerze AMC (od 01 do 08) lub w module rozszerzeń Wiegand (od 09 do 16)
- **Wejście**: nazwa wejścia
- **Sygnał wyjściowy**: nazwa sygnału wyjściowego
- **Wejście**: nazwa wejścia
- **Sygnał wejściowy**: nazwa sygnału wejściowego

–



Board	T..	entrance	Input signal	entrance	Output signal
AMC 4-R4	01	DM 01a	Door contact	DM 01a	Release door
AMC 4-R4	02				
AMC 4-R4	03				
AMC 4-R4	04				
AMC 4-R4	05				
AMC 4-R4	06				
AMC 4-R4	07				
AMC 4-R4	08				
BPR HI	01				
BPR HI	02				
BPR HI-1	01				
BPR HI-1	02				

Zmiana przypisania sygnału

Na kartach terminali w ustawieniach kontrolerów przypisania poszczególnych sygnałów są tylko wyświetlane (wyłącznie do odczytu). Natomiast na kartach terminali odpowiednich wejść można zmieniać wartości lub pozycje sygnałów.

Dwukrotne kliknięcie wpisu, który ma zostać zmodyfikowany, w kolumnie **Sygnał wyjściowy** lub **Sygnał wejściowy** uaktywnia listę rozwijaną umożliwiającą wybranie innej wartości sygnału dla modelu wejścia. Jeśli wybierzesz opcję **Nie przypisano**, sygnał zostanie zwolniony i można go użyć w innych wejściach.

W ten sposób można nie tylko zmieniać sygnały, ale także przypisać sygnały do innych styków w celu optymalizacji wykorzystania dostępnego napięcia. Wszystkie wolne lub zwolnione styki można później wykorzystywać na nowe sygnały albo jako nowe pozycje dla istniejących sygnałów.

Uwaga!

Zasadniczo wszystkie sygnały wejściowe i wyjściowe można wybierać dowolnie, ale nie wszystkie wybory mają sens we wszystkich modelach drzwi. Na przykład nie ma sensu przypisywać sygnałów systemu SSW do modelu drzwi (np. 01 lub 03), który nie obsługuje systemu SSW. Więcej szczegółów znajduje się w tabeli w rozdziale Przypisywanie sygnałów do modeli drzwi.

Przypisywanie sygnałów do modeli drzwi

Aby uniknąć ustawiania nieprawidłowych parametrów za pomocą menu rozwijanych służących do przypisywania sygnałów do modeli drzwi, menu oferują tylko sygnały zgodne z wybranym modelem drzwi.

Tabela sygnałów wejściowych

Sygnały wejściowe	Opis
Czujnik drzwi	
Przycisk żądania wyjścia	Przycisk otwarcia drzwi.
Czujnik rygla	Służy wyłącznie do przekazywania komunikatów. Nie zapewnia funkcji sterowania.

Wejście zablokowane	Służy do tymczasowego blokowania przeciwnych drzwi w śluzach. Umożliwia także blokowanie na dłuższy czas.
Sabotaż	Sygnał sabotażu z kontrolera zewnętrznego.
Bramka obrotowa w pozycji normalnej	Bramka obrotowa jest zamknięta.
Przejście zakończone	Przejście zostało z powodzeniem zakończone. Jest to impuls z kontrolera zewnętrznego.
System sygnalizacji włamania gotowy do uzbrojenia	Zostanie użyty przez system sygnalizacji włamania, jeśli wszystkie czujki znajdują się w spoczynku i system może zostać uzbrojony.
System sygnalizacji włamania jest uzbrojony	System sygnalizacji włamania jest uzbrojony.
Przycisk żądania uzbrojenia systemu sygnalizacji włamania	Przycisk uzbrajania systemu sygnalizacji włamania.
Włączenie otwarcia lokalnego	Sygnał zostanie użyty, jeśli układ drzwi otworzy drzwi bez udziału kontrolera AMC. Kontroler AMC nie wyśle komunikatu o włamaniu, lecz o „lokalnym otwarciu drzwi”.
Zewnętrzne decyzje o dostępie — zaakceptowano	Sygnał jest ustawiany, jeśli zewnętrzny system zaakceptuje dostęp
Zewnętrzne decyzje o dostępie — odmowa	Sygnał jest ustawiany, jeśli zewnętrzny system zaakceptuje dostęp

Tabela sygnałów wyjściowych

Sygnały wyjściowe	**Opis**
Automat do otwierania drzwi	
Śluza: blokada przeciwnych drzwi	Zamyka drzwi z przeciwnej strony śluzy osobowej. Ten sygnał jest wysyłany podczas otwierania drzwi.
Wyciszenie alarmu	...do systemu sygnalizacji włamania. Zostanie użyty, kiedy drzwi są otwarte, aby uniknąć utworzenia przez system sygnalizacji włamania komunikatu o włamaniu.
Zielony wskaźnik	Zielony wskaźnik świeci, kiedy drzwi są otwarte.
Drzwi są otwarte zbyt długo	Impuls trwający 3 s. Jeśli drzwi są otwarte zbyt długo.
Aktywacja kamery	Kamera zostanie włączona na początku przejścia.

Bramka obrotowa otwarta dla przechodzenia do wewnątrz	
Bramka obrotowa otwarta dla przechodzenia na zewnątrz	
Drzwi są otwarte na stałe	Sygnał do odblokowania drzwi na dłuższy czas.
Uzbrojenie systemu sygnalizacji włamania	Sygnał do uzbrojenia systemu SSW.
Rozbrojenie systemu sygnalizacji włamania	Sygnał do rozbrojenia systemu SSW.
Zewnętrzne decyzje o dostępie — aktywowano	Sygnał musi być ustawiony, aby aktywować zewnętrzny system dostępu.

Tabela mapowań modeli drzwi na sygnały wejściowe i wyjściowe

W poniższej tabeli wymieniono istotne przypisania sygnałów i modeli drzwi.

Model drzwi	**Opis**	**Sygnały wejściowe**	**Sygnały wyjściowe**
01	Proste drzwi z czytnikiem wejścia i wyjścia Czytniki do rejestracji czasu i obecność Funkcjonalność zewnętrznej decyzji o dostępie	- Czujnik drzwi - Przycisk żądania wyjścia - Czujnik rygla - Wejście zablokowane - Sabotaż - Włączenie otwarcia lokalnego - Zewnętrzne decyzje o dostępie — zaakceptowano - Zewnętrzne decyzje o dostępie — odmowa	- Automat do otwierania drzwi - Śluza: blokada przeciwnych drzwi - Wyciszenie alarmu - Zielony wskaźnik - Aktywacja kamery - Drzwi są otwarte zbyt długo - Zewnętrzne decyzje o dostępie — aktywowano
03	Drzwi obrotowe z czytnikiem wejścia i wyjścia Czytniki do rejestracji czasu i obecność Funkcjonalność zewnętrznej decyzji o dostępie	- Bramka obrotowa w pozycji spoczynkowej - Przycisk żądania wyjścia - Wejście zablokowane - Sabotaż - Zewnętrzne decyzje o dostępie — zaakceptowano - Zewnętrzne decyzje o dostępie — odmowa	- Śluza: blokada przeciwnych drzwi - Bramka obrotowa otwarta dla przechodzenia do wewnątrz - Bramka obrotowa otwarta dla przechodzenia na zewnątrz - Wyciszenie alarmu - Aktywacja kamery - Drzwi są otwarte zbyt długo - Zewnętrzne decyzje o dostępie — aktywowano

05	Wjazd na parking lub wyjazd z niego — maksymalnie 24 strefy parkowania Czytniki do rejestracji czasu i obecność Funkcjonalność zewnętrznej decyzji o dostępie	- Czujnik drzwi - Przycisk żądania wyjścia - Wejście zablokowane - Przejście zakończone - Zewnętrzne decyzje o dostępie — zaakceptowano - Zewnętrzne decyzje o dostępie — odmowa	- Automat do otwierania drzwi - Wyciszenie alarmu - Zielony wskaźnik - Drzwi są otwarte zbyt długo - Drzwi są otwarte na stałe - Zewnętrzne decyzje o dostępie — aktywowano
06	Czytniki do rejestracji czasu i obecność		
07	Winda — maksymalnie 56 pięter		
09	Czytnik i przycisk na wjeździe lub wyjeździe pojazdów Czytniki do rejestracji czasu i obecność Funkcjonalność zewnętrznej decyzji o dostępie	- Czujnik drzwi - Przycisk żądania wyjścia - Wejście zablokowane - Przejście zakończone - Zewnętrzne decyzje o dostępie — zaakceptowano - Zewnętrzne decyzje o dostępie — odmowa	- Automat do otwierania drzwi - Wyciszenie alarmu - Zielony wskaźnik - Drzwi są otwarte zbyt długo - Drzwi są otwarte na stałe - Zewnętrzne decyzje o dostępie — aktywowano
10	Proste drzwi z czytnikiem wejścia i wyjścia oraz funkcją uzbrojenia/ rozbrojenia systemu sygnalizacji włamania Czytniki do rejestracji czasu i obecność Funkcjonalność zewnętrznej decyzji o dostępie	- Czujnik drzwi - Przycisk żądania wyjścia - System sygnalizacji włamania gotowy do uzbrojenia - System sygnalizacji włamania jest uzbrojony - Sabotaż - Żądanie uzbrojenia systemu sygnalizacji włamania - Zewnętrzne decyzje o dostępie — zaakceptowano - Zewnętrzne decyzje o dostępie — odmowa	- Automat do otwierania drzwi - Aktywacja kamery - Uzbrojenie systemu sygnalizacji włamania - Rozbrojenie systemu sygnalizacji włamania - Drzwi są otwarte zbyt długo - Zewnętrzne decyzje o dostępie — aktywowano
14	Proste drzwi z czytnikiem wejścia i wyjścia oraz funkcją uzbrojenia/ rozbrojenia systemu sygnalizacji włamania	- Czujnik drzwi - Przycisk żądania wyjścia - System sygnalizacji włamania gotowy do uzbrojenia - System sygnalizacji włamania jest uzbrojony - Sabotaż - Żądanie uzbrojenia systemu sygnalizacji włamania	- Automat do otwierania drzwi - Aktywacja kamery - Uzbrojenie systemu sygnalizacji włamania - Drzwi są otwarte zbyt długo

	Czytniki do rejestracji czasu i obecność		
15	Styki cyfrowe		

Przypisywanie sygnałów do czytników

Czytniki szeregowe (tj. czytniki podłączone do kontrolera AMC2 4R4) i czytniki OSDP można rozszerzyć o lokalne sygnały we/wy. W ten sposób można udostępnić dodatkowe sygnały oraz skrócić ścieżki elektryczne do styków drzwi.

Po utworzeniu czytnika szeregowego na karcie **Terminale** w ustawieniach odpowiedniego wejścia pojawiają się dwa sygnały wejściowe i dwa sygnały wyjściowe dla każdego czytnika pod kontrolerem oraz (jeśli występują) sygnały modułu rozszerzeń.

Uwaga!

Te wpisy na liście są tworzone dla każdego czytnika szeregowego, niezależnie od tego, czy ma on lokalne wejścia/wyjścia, czy nie.

Inaczej niż w kontrolerach i modułach rozszerzeń, tych lokalnych sygnałów czytnika nie można przypisywać do funkcji ani konfigurować dla nich parametrów. Nie są one również wyświetlane na kartach **Sygnał wejściowy** i **Sygnał wyjściowy** ani nie można ich stosować do wind (np. w celu przekroczenia limitu 56 pięter). Z tego powodu najlepiej nadają się do bezpośredniego sterowania drzwiami (np. zatrzaśnięcie lub zwolnienie drzwi). Przynoszą jednak tę korzyść, że zwalniają sygnały kontrolera dla bardziej skomplikowanych funkcji parametryzowanych.

Edytowanie sygnałów

Po utworzeniu wejścia na karcie **Terminale** w ustawieniach odpowiedniego wejścia pojawiają się dwa sygnały wejściowe i dwa sygnały wyjściowe dla każdego czytnika pod kontrolerem. W kolumnie Moduł jest wyświetlana nazwa czytnika. Standardowe sygnały wejścia są domyślnie przypisywane do pierwszych wolnych sygnałów kontrolera. Aby przenieść te sygnały do własnych sygnałów czytnika, najpierw trzeba je usunąć z ich pierwotnych pozycji. Aby to zrobić, wybierz pozycję listy **<Nie przypisano>**.

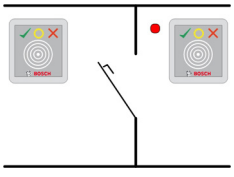
Kliknij dwukrotnie kolumnę **Sygnał wejściowy** lub **Sygnał wyjściowy** w ustawieniach czytnika. Zostanie wyświetlona lista możliwych sygnałów dla wybranego modelu drzwi, co umożliwi zmianę pozycji sygnału. Podobnie jak wszystkie inne sygnały, można je oglądać na karcie **Terminale** w ustawieniach kontrolera, ale nie da się ich tam edytować.

Uwaga!

Nie istnieje możliwość monitorowania statusów sygnałów czytnika.
Można ich używać tylko w drzwiach, do których jest przypisany czytnik.

13.5 Predefiniowane sygnały dla modeli drzwi

Model wejścia 01



Warianty modelu:

01a	Pojedyncze drzwi z czytnikiem wejścia **i** wyjścia
01b	Pojedyncze drzwi z czytnikiem wejścia i przyciskiem otwierania drzwi
01c	Pojedyncze drzwi z czytnikiem wejścia **lub** wyjścia

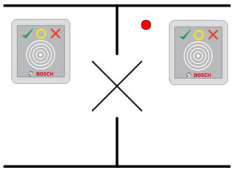
Możliwe sygnały:

Sygnały wejściowe	**Sygnały wyjściowe**
Czujnik drzwi	Automat do otwierania drzwi
Przycisk żądania wyjścia	Śluza: blokada przeciwnych drzwi
Sabotaż	Zielony wskaźnik
Włączenie otwarcia lokalnego	Aktywacja kamery
	Drzwi są otwarte zbyt długo

Uwaga!
Funkcję przechodzenia wyłącznie pojedynczo, w tym zwłaszcza blokadę dla kierunku przeciwnego, można konfigurować za pomocą parametrów wyłącznie w modelu drzwi 03.

Wyciszenie alarmu jest skuteczne tylko wówczas, gdy czas wyciszenia przed otwarciem drzwi jest większy od 0.
Ten model wejścia nadaje się również do przejazdów dla samochodów, jednak wtedy jest zalecany montaż dodatkowego czytnika do obsługi z samochodów osobowych i ciężarowych.

Model wejścia 03



Warianty modelu:

03a	Kontrolowana bramka obrotowa z czytnikiem wejścia **i** wyjścia
03b	Kontrolowana bramka obrotowa z czytnikiem wejścia i przyciskiem otwierania
03c	Kontrolowana bramka obrotowa z czytnikiem wejścia **lub** wyjścia

Możliwe sygnały:

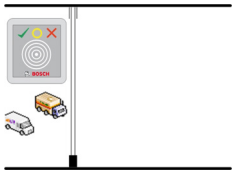
Sygnał wejściowy	**Sygnały wyjściowe**
Bramka obrotowa w pozycji normalnej	Bramka obrotowa otwarta dla przechodzenia do wewnątrz

Przycisk żądania wyjścia	Bramka obrotowa otwarta dla przechodzenia na zewnątrz
Sabotaż	Wejście zablokowane
	Aktywacja kamery
	Drzwi są otwarte zbyt długo
Dodatkowe sygnały wykorzystujące opcję **śluza osobowa**:	
Wejście zablokowane	Śluza: blokada przeciwnych drzwi
	Wyciszenie alarmu

Uwagi dotyczące konfigurowania śluz osobowych:
Gdy bramka obrotowa znajduje się w normalnym położeniu, są włączane pierwsze sygnały wejściowe wszystkich podłączonych czytników. Jeśli zostanie przedstawiona karta, a właściciel ma uprawnienia dostępu przez to wejście, wówczas:
– Jeżeli karty użyto w czytniku wejścia, pierwszy sygnał wyjściowy jest ustawiany w czytniku wejścia na czas trwania aktywacji.
– Jeżeli karty użyto w czytniku wyjścia, drugi sygnał wyjściowy jest ustawiany w czytniku wyjścia na czas trwania aktywacji.

Po naciśnięciu przycisku żądania wyjścia (REX) są ustawiane drugi sygnał wejściowy i drugi sygnał wyjściowy. W tym czasie drzwi obrotowych można używać w ich normalnym kierunku.

Model wejścia 05c



Wariant modelu:

05c	Czytnik wjazdu na parking **lub** wyjazdu z parkingu

Możliwe sygnały w tym modelu wejścia:

Sygnały wejściowe	**Sygnały wyjściowe**
Czujnik drzwi	Automat do otwierania drzwi
Przycisk żądania wyjścia	Drzwi są otwarte na stałe
Wejście zablokowane	Zielony wskaźnik
Przejście zakończone	Wyciszenie alarmu
	Drzwi są otwarte zbyt długo

Wejście na parking i wyjście z parkingu muszą być skonfigurowane na tym samym kontrolerze. Jeśli sterowanie dostępem do parkingu przypisano kontrolerowi, wówczas ten kontroler nie może zarządzać żadnymi innymi modelami drzwi. Wjazdowi na parking można przypisać tylko czytnik wejścia (bez czytnika wyjścia). Po przypisaniu wejścia ponowne wybranie modelu

drzwi umożliwi tylko zdefiniowanie czytnika wyjścia. Na każdym parkingu można zdefiniować maksymalnie 24 podobszary, z których jeden musi być uwzględniony w autoryzacji karty, aby karta działała.

Model wejścia 06


Warianty modelu

06a	Czytnik wejścia **i** wyjścia do rejestracji czasu i obecności
06c	Czytnik wejścia **lub** wyjścia do rejestracji czasu i obecności

Czytniki utworzone z tym modelem drzwi nie kontrolują dostępu, ale są wykorzystywane wyłącznie do rejestrowania czasu i obecności. Nie sterują drzwiami, a jedynie przekazują dane z karty do systemu zarządzania czasem i obecnością.
W konsekwencji nie są definiowane żadne sygnały. Te czytniki są zwykle instalowane wewnątrz już kontrolowanego obszaru.

Uwaga!
Aby można było tworzyć prawidłowe pary rezerwacji (czas wejścia + czas wyjścia) w systemie zarządzania czasem i obecnością, trzeba skonfigurować parametry na dwóch oddzielnych czytnikach z modelem drzwi 06: jednym do rejestrowania wejść i jednym do rejestrowania wyjść.

Używaj wariantu **a**, gdy wejście i wyjście nie są oddzielne. Używaj wariantu **c**, jeśli wejście i wyjście są od siebie fizycznie odległe lub jeśli nie można podłączyć czytników do tego samego kontrolera. Upewnij się, że jeden czytnik jest zdefiniowany do rejestrowania ruchu wchodzącego, a drugi dla ruchu wychodzącego.
Podobnie jak w każdym innym wejściu trzeba utworzyć i przypisać autoryzacje. W module Access Engine na karcie **Zarządzanie czasem** w oknach dialogowych **Uprawnienia dostępu** i **Uprawnienia obszarowe/czasowe** znajduje się lista wszystkich zdefiniowanych czytników czasu i obecności. Aktywuj co najmniej jeden czytnik w kierunku wchodzenia i jeden w kierunku wychodzenia. Autoryzacje czytników czasu i obecności można przypisywać wraz z innymi uprawnieniami dostępu lub oddzielnie.
Jeśli dla danego kierunku ruchu istnieje więcej niż jeden czytnik czasu i obecności, można przypisać określonych posiadaczy kart do określonych czytników. Wtedy czytnik będzie rejestrował i zapisywał tylko czasy obecności przypisanych i autoryzowanych użytkowników.

Uwaga!
Na zachowanie czytników czasu i obecności mają również wpływ inne funkcje kontroli dostępu. Dlatego czarne listy, modele czasowe i daty ważności również mogą blokować rejestrowanie czasów dostępu na czytniku czasu i obecności.

Zarejestrowane czasy wejścia i wyjścia są przechowywane w katalogu `C:\MgtS \AccessEngine\AC\TAExchange` w pliku tekstowym `TAccExc_EXP.tx`t, który następnie jest eksportowany do systemu zarządzania czasem i obecnością.
Dane rejestrowania są przesyłane w następującym formacie:
`ddMMyyyy;hhmm[s];Direction [0,1]; AbsenceReason; Personnel-Nr.`

d=dzień, M=miesiąc, y=rok, h=godzina, m=minuta, s=czas letni, 0=ruch wychodzący, 1=ruch przychodzący
Plik eksportu nie jest sortowany według osób, ale zawiera wszystkie rejestracje w porządku chronologicznym, w jakim zdarzenia odbierał moduł administracyjny. Separatorem pól w tym pliku jest średnik.

Warianty modelu wejścia 07

Warianty modelu:

07a	Winda obsługująca maksymalnie 56 pięter
07b	Winda obsługująca maksymalnie 56 pięter

Model wejścia 07a
Sygnały:

Sygnał wejściowy	**Sygnały wyjściowe**
	Zwolnienie <nazwa piętra>
	Jeden sygnał wyjściowy dla każdego zdefiniowanego piętra, maksymalnie 56.

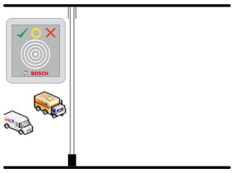
Po przywołaniu windy właściciel karty może wybrać tylko te piętra, dla których jego karta jest autoryzowana.
Modeli drzwi z windą nie można łączyć z innymi modelami drzwi na tym samym kontrolerze. Używając modułu rozszerzeń, dla każdej windy skonfigurowanej w kontrolerze AMC można zdefiniować nawet 56 pięter. Autoryzacje karty muszą obejmować samą windę i co najmniej jedno piętro.

Model wejścia 07c
Sygnały:

Sygnał wejściowy	**Sygnał wyjściowy**
Klawisz wejścia <nazwa piętra>	Zwolnienie <nazwa piętra>
Dla każdego zdefiniowanego piętra istnieją wpisy wejścia i wyjścia — maksymalnie 56.	

Po przywołaniu windy i naciśnięciu przycisku wyboru piętra (stąd konieczność sygnałów wejściowych) następuje sprawdzenie autoryzacji karty w celu ustalenia, czy uwzględniają one wybrane piętro.
Ponadto w tym modelu drzwi można zdefiniować traktowanie dowolnych pięter jako mających **dostęp publiczny**. Na takim piętrze nie będzie dokonywana kontrola autoryzacji i każda osoba może dojechać do niego windą. Sam dostęp publiczny może być regulowany przez **model czasowy**, który ogranicza swobodę dostępu do wybranych godzin w określonych dniach. Poza tymi godzinami kontrole autoryzacji będą przeprowadzane w zwykły sposób.
Modeli drzwi z windą nie można łączyć z innymi modelami drzwi na tym samym kontrolerze. Używając modułu rozszerzeń, dla każdej windy skonfigurowanej w kontrolerze AMC można zdefiniować nawet 56 pięter. Autoryzacje karty muszą obejmować samą windę i co najmniej jedno piętro.

Model wejścia 09

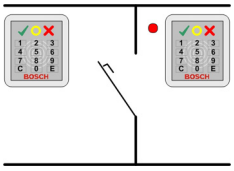


Możliwe sygnały:

Sygnały wejściowe	Sygnały wyjściowe
Czujnik drzwi	Automat do otwierania drzwi
Przycisk żądania wyjścia	Drzwi są otwarte na długo
Wejście zablokowane	Sygnalizator świetlny ma kolor zielony
Przejście zakończone	Wyciszenie alarmu
	Drzwi są otwarte zbyt długo

W przypadku sterowania barierą zakłada się obecność mechanizmu kontroli bazowej (SPS). W odróżnieniu od **model drzwi 5c** to wejście i wyjście można skonfigurować w różnych kontrolerach AMC. Ponadto nie ma podobszarów, istnieje tylko ogólna autoryzacja wobec obszaru parkingu.

Model wejścia 10



Warianty modelu:

10a	Pojedyncze drzwi z czytnikiem wejścia **i** wyjścia **oraz** funkcją uzbrojenia/rozbrojenia systemu sygnalizacji włamania (SSW)
10b	Pojedyncze drzwi z wejściem, przycisk REX (żądanie wyjścia) oraz funkcją uzbrojenia/rozbrojenia systemu sygnalizacji włamania
10e	Pojedyncze drzwi z czytnikiem wejścia, przyciskiem REX oraz zdecentralizowaną funkcją uzbrojenia/rozbrojenia systemu sygnalizacji włamania

Możliwe sygnały:

Sygnały wejściowe	Sygnały wyjściowe
Czujnik drzwi	Automat do otwierania drzwi
System sygnalizacji włamania jest uzbrojony	Uzbrojenie systemu sygnalizacji włamania
System sygnalizacji włamania gotowy do uzbrojenia	Rozbrojenie systemu sygnalizacji włamania [tylko model drzwi 10e]
Przycisk żądania wyjścia	Aktywacja kamery

Czujnik rygla	Drzwi są otwarte zbyt długo
Sabotaż	
Przycisk żądania uzbrojenia systemu sygnalizacji włamania	

Uwaga!
Ten model drzwi wymaga czytników z klawiaturą. Posiadacze kart muszą wpisać **kody PIN** w celu uzbrojenia/rozbrojenia systemu SSW.

W zależności od zainstalowanych czytników są wymagane różne procedury.
Czytniki I-BPR: (np. DELTA 1010, INTUS 1600)
W celu uzbrojenia naciśnij klawisz **7** i potwierdź klawiszem Enter (#). Następnie przedstaw kartę, wprowadź kod PIN i ponownie potwierdź klawiszem Enter (#).
W celu rozbrojenia przystaw kartę, wprowadź kod PIN i potwierdź klawiszem Enter (#).

Czytnik BPR: (w tym Wiegand)
W celu uzbrojenia naciśnij 7, przyłóż kartę i wprowadź kod PIN. Nie trzeba potwierdzać klawiszem Enter.
W celu rozbrojenia przyłóż kartę i wpisz kod PIN. Rozbrojenie i zwolnienie drzwi następują jednocześnie.

Funkcje specjalne modelu drzwi 10e:
W modelach drzwi 10a i 10b każde wejście ma swój własny obszar strzeżony, natomiast w przypadku modelu 10e wejścia można grupować w jednostki. Każdy czytnik w tej grupie jest w stanie uzbroić lub rozbroić całą jednostkę. Do zresetowania statusu ustawionego przez którykolwiek czytnik w grupie jest wymagany sygnał wyjściowy **Rozbrojenie systemu sygnalizacji włamania**.
Sygnały:
- Modele drzwi 10a i 10b:
  - - Uzbrojenie jest wyzwalane przez ciągły sygnał.
  - - Rozbrojenie jest wyzwalane przez przerwanie ciągłego sygnału.
- Model drzwi 10e:
  - - Uzbrojenie i rozbrojenie jest wyzwalane impulsem sygnału trwającym 1 sekundę.

[Używając przekaźnika bistabilnego, można sterować systemem SSW z wielu drzwi. W tym celu sygnały ze wszystkich drzwi wymagają operacji OR na przekaźniku. Sygnały **System sygnalizacji włamania uzbrojony** i **System sygnalizacji włamania gotowy do uzbrojenia** muszą zostać zreplikowane do wszystkich drzwi w grupie.]

13.6 Wejścia specjalne

13.6.1 Windy (model drzwi 07)

Uwagi ogólne o windach (model wejścia 07)
Wind nie można łączyć z innymi modelami drzwi na tym samym kontrolerze AMC.
Wind nie można używać z opcjami czytnika **Dostęp grupy** ani **Potrzebny parkingowy**.
W jednym kontrolerze AMC można zdefiniować do 8 pięter. Moduł rozszerzeń kontrolera AMC oferuje 8 lub 16 dodatkowych wyjść.

W efekcie używając maksymalnej liczby największych modułów rozszerzeń, można skonfigurować do 56 pięter z czytnikami RS485 oraz 64 piętra z czytnikami Wiegand, jeżeli dodatkowo zostanie użyta specjalna karta rozszerzeń Wiegand.

Różnice między modelami wejść 07a i 07c

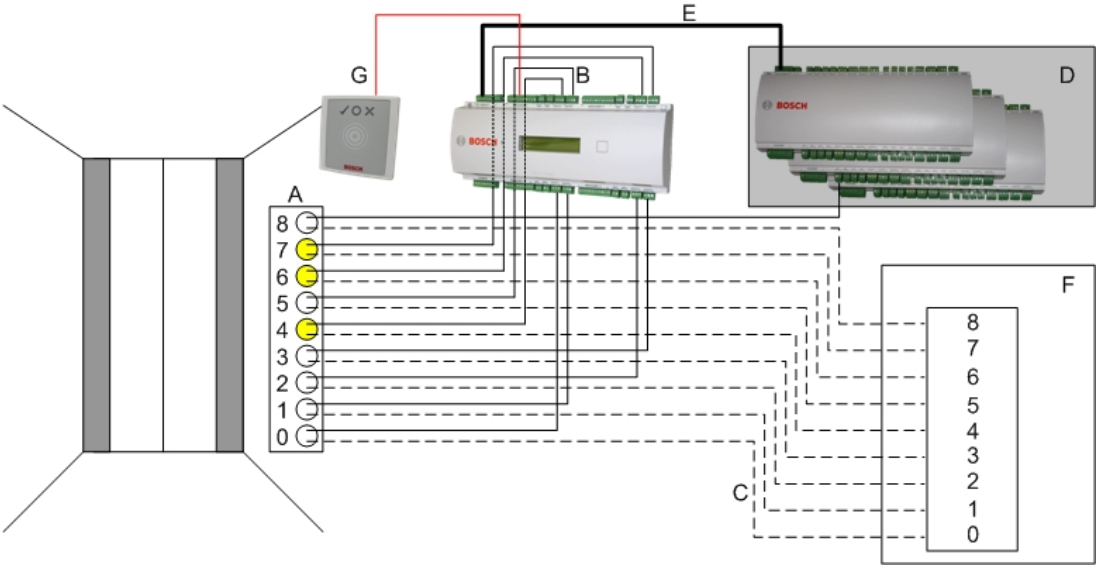
W oknach dialogowych uprawnień dostępu w systemie Access Engine można przypisać określone piętra do autoryzacji osoby.

Jeśli windę utworzono przy użyciu modelu wejścia **07a**, to posiadacz karty okazuje kartę identyfikacyjną, a piętra, wobec których ma pozwolenie, stają się dostępne.

W modelu wejścia **07c** system sprawdza autoryzację do wybranego piętra po wybraniu go przez osobę. Piętra oznaczone jako **publiczne** są dostępne dla wszystkich osób, niezależnie od posiadanych uprawnień. Za pomocą modelu czasowego funkcję dostępu publicznego można ograniczyć do wybranego okresu. Poza tym okresem na wybranym piętrze będzie sprawdzana autoryzacja.

Schemat okablowania wind:

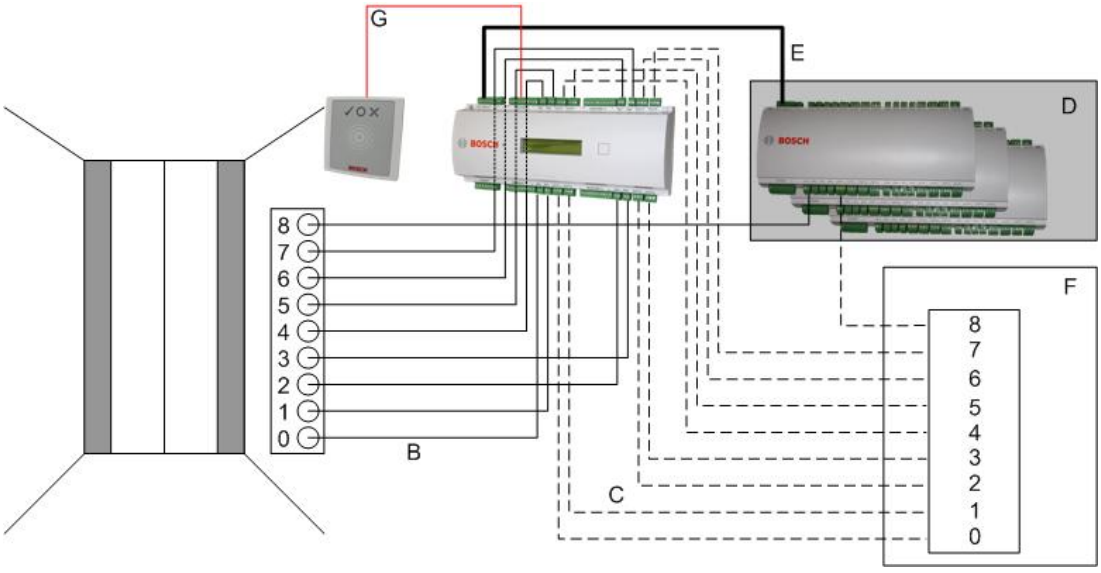
Poniższa ilustracja przedstawia schemat połączeń windy w modelu drzwi 07a.



Legenda:

- A = Klawiatura windy
- B = (linia ciągła) Sygnały wyjściowe kontrolera AMC
- C = (linia przerywana) Połączenie z opcjami sterowania windą
- D = Do kontrolera AMC można podłączyć nawet trzy karty we/wy, jeśli osiem własnych wejść i wyjść kontrolera nie wystarcza.
- E = Przesyłanie danych i zasilania z kontrolera AMC do kart we/wy
- F = Selektor pięter w windzie
- G = Czytnik. Dla każdej windy można skonfigurować dwa czytniki.

Poniższa ilustracja przedstawia schemat połączeń windy w modelu drzwi 07c.



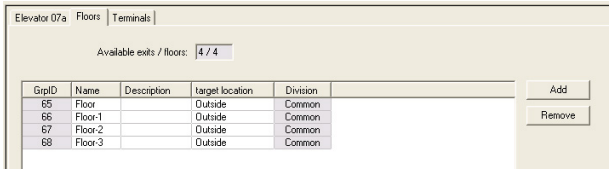
Legenda:

- B = (linia ciągła) Sygnały wyjściowe kontrolera AMC
- C = (linia przerywana) Połączenie z opcjami sterowania windą
- D = Do kontrolera AMC można podłączyć nawet trzy karty we/wy, jeśli osiem własnych wejść i wyjść kontrolera nie wystarcza.
- E = Przesyłanie danych i zasilania z kontrolera AMC do kart we/wy
- F = Selektor pięter w windzie
- G = Czytnik. Dla każdej windy można skonfigurować dwa czytniki.

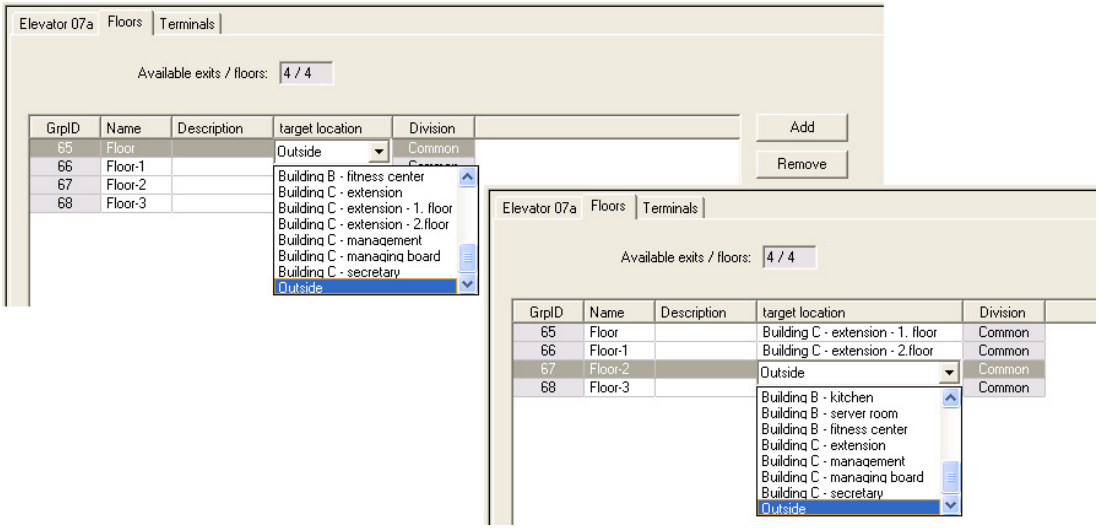
Podobnie jak parkingi, windy mają parametr **Publiczny.** Ten parametr można ustawić dla każdego piętra indywidualnie. Po aktywowaniu parametru **Publiczny** nie są sprawdzane uprawnienia dostępu, więc każdy posiadacz karty w windzie może wybrać piętro.
W razie potrzeby ustaw model czasowy dla modelu wejścia: poza zdefiniowanymi przedziałami czasu autoryzacje będą sprawdzane.

Piętra dla modelu wejścia 07

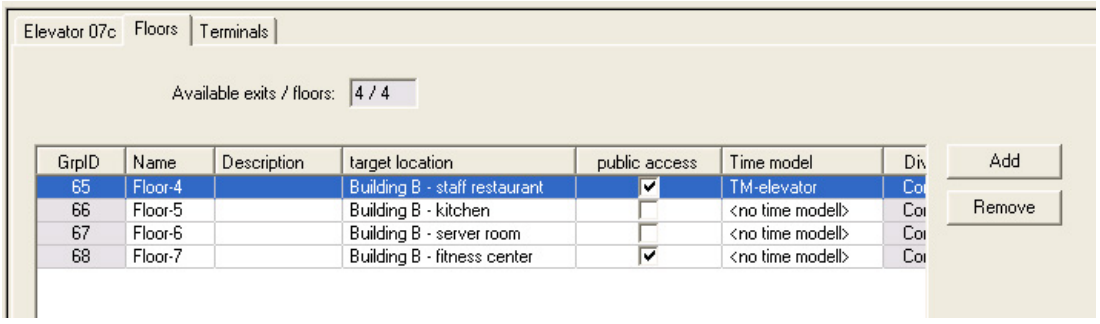
Na karcie **Piętra** za pomocą przycisków **Dodaj** i **Usuń** można dodawać i usuwać piętra obsługiwane przez windę.



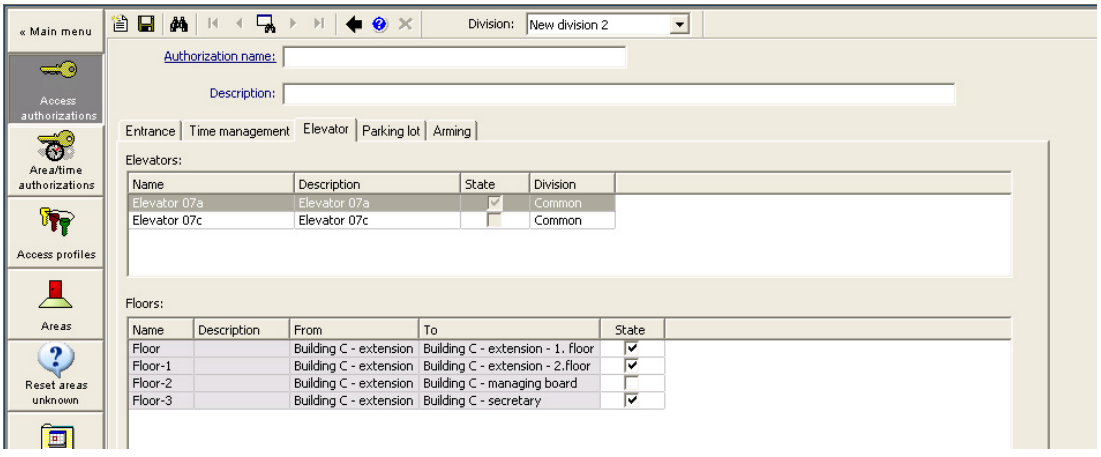
Lokalizacjami docelowymi piętra mogą być dowolne **obszary**, z wyjątkiem parkingów i stref parkowania.
Każdemu piętru można przypisać tylko jeden obszar. W związku z tym wybór obszarów dostępnych w polach kombi zmniejsza się po każdym przypisaniu, co zapobiega niezamierzonemu dublowaniu przypisań.



Podczas korzystania z modelu wejścia 07a można ustawić publiczny charakter poszczególnych pięter, zaznaczając pole wyboru **Dostęp publiczny**. W takim przypadku nie ma kontroli autoryzacji. Za pomocą dodatkowego przypisania **modelu czasowego** można jednak ograniczyć dostęp, przyznając go tylko w predefiniowanych okresach.



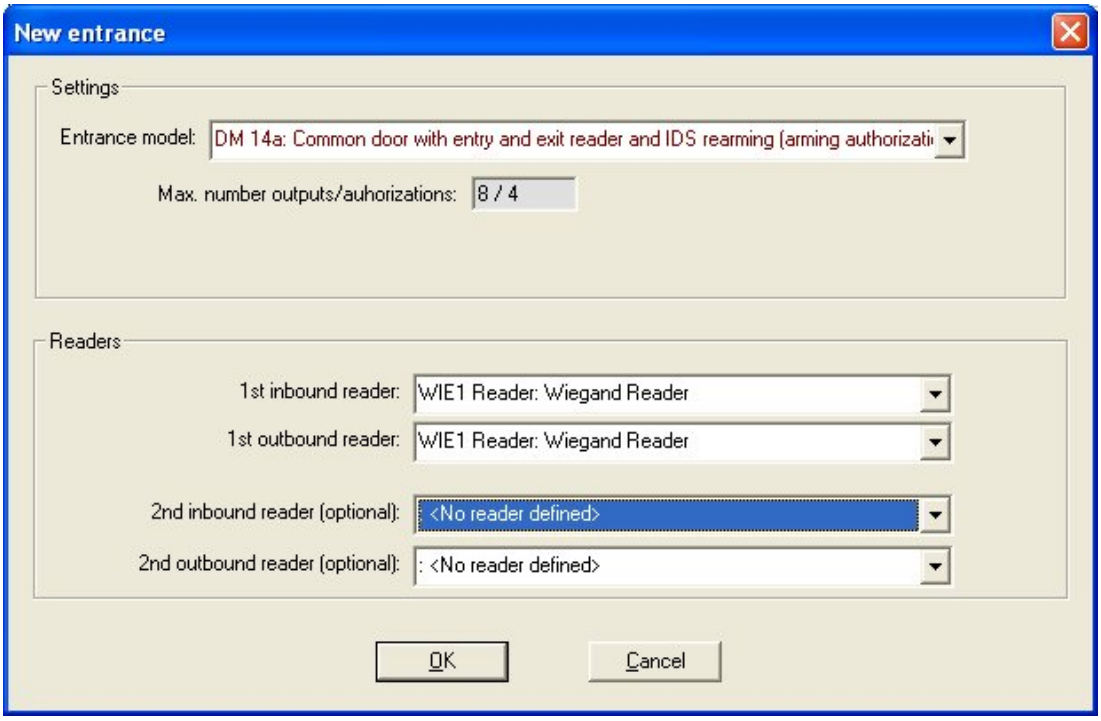
Na karcie **Winda** nad górnym polem listy w oknach dialogowych modułu Access Engine **Uprawnienia dostępu** i **Uprawnienia obszarowe/czasowe** zaznacz najpierw wymaganą windę, a następnie pod spodem piętra, do których ma dostęp posiadacz karty.



13.6.2 Modele drzwi z alarmami antywłamaniowymi (model drzwi 14)

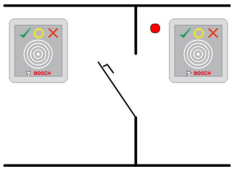
Uzbrajanie i rozbrajanie systemów wykrywania włamań – model drzwi 14

W przeciwieństwie do modelu wejścia 10 model drzwi 14 pozwala na uzbrajanie i rozbrajanie.



Obszar zazbrajania jest oznaczony wielką literą na pierwszej stronie wejścia. Przypisanie wejścia do obszaru zazbrajania sprawia, że uzbrojenie na jednym czytniku zostanie rozpowszechnione do wszystkich wejść w tym obszarze.

Model wejścia 14



Warianty modelu:

14a	Pojedyncze drzwi z czytnikiem wejścia i wyjścia oraz funkcją uzbrojenia/rozbrojenia systemu sygnalizacji włamania
14b	Pojedyncze drzwi z czytnikiem wejścia, przyciskiem otwierania drzwi oraz funkcją uzbrojenia/rozbrojenia systemu sygnalizacji włamania

Możliwe sygnały:

Sygnały wejściowe	**Sygnały wyjściowe**
Czujnik drzwi	Automat do otwierania drzwi
System sygnalizacji włamania jest uzbrojony	Uzbrojenie systemu sygnalizacji włamania
System sygnalizacji włamania gotowy do uzbrojenia	Aktywacja kamery
Przycisk żądania wyjścia	Drzwi są otwarte zbyt długo
Czujnik rygla	
Sabotaż	

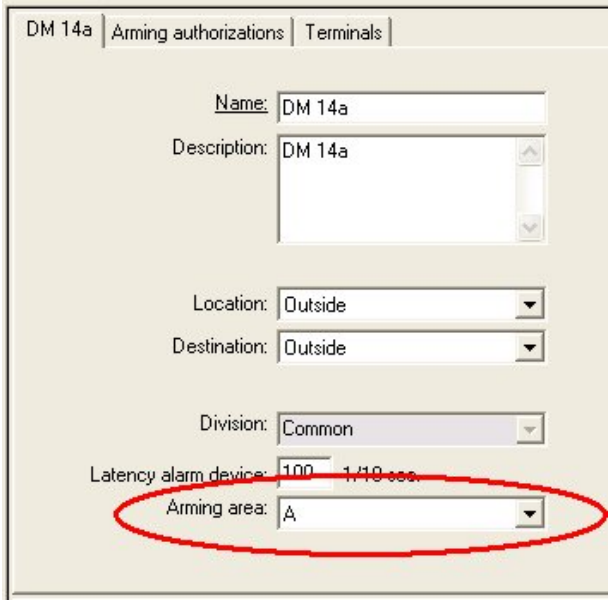
Przycisk żądania uzbrojenia systemu sygnalizacji włamania	

W modelu drzwi 14 można tworzyć obszary strzeżone, w których system systemów sygnalizacji włamania (SSW) będzie uzbrajany z dowolnego czytnika w obszarze. W takim przypadku sygnały **System sygnalizacji włamania uzbrojony** i **System sygnalizacji włamania gotowy do uzbrojenia** należy replikować przy każdym wejściu.
W przeciwieństwie do modelu 10 w modelu drzwi 14 można stosować czytniki z klawiaturą lub bez. Kolejną różnicą jest przypisywanie uprawnień do uzbrajania/rozbrajania. Tylko posiadacze kart z odpowiednimi uprawnieniami mogą uzbrajać/rozbrajać.
W przypadku czytników z klawiaturą uzbrajanie i rozbrajanie odbywa się tak, jak w modelu drzwi 10.
W czytnikach bez klawiatury uzbrojenie nie odbywa się przez wprowadzenie kodu PIN, ale za pomocą przełącznika umieszczonego w pobliżu czytnika, który ma taką samą funkcję, jak przycisk 7 w czytnikach z klawiaturami. Po użyciu tego przełącznika status urządzenia alarmowego jest wyświetlany przez kolorowe diody LED czytnika:
– Nieuzbrojony = naprzemienne miganie światła zielonego i czerwonego
– Uzbrojony = stałe światło czerwone

W celu uzbrojenia przyłóż prawidłowo autoryzowaną kartę.
W celu rozbrojenia użyj przełącznika i przystaw prawidłowo autoryzowaną kartę.
Odblokowanie drzwi nie odbywa się automatycznie po rozbrojeniu, ale wymaga ponownego przedstawienia karty.

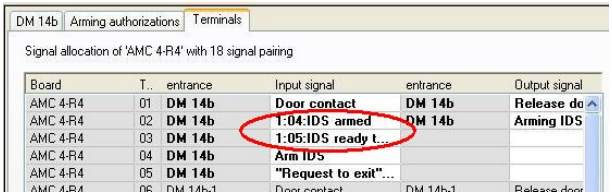
Autoryzacje do uzbrojenia w modelu drzwi 14

Pierwsza zakładka okna dialogowego wejścia 14 zawiera dodatkowy parametr do tworzenia obszarów zazbrajania. Kilka wejść modelu 14 może się odwoływać do tego samego obszaru zazbrajania, tak aby każdy czytnik w tym obszarze mógł uzbroić lub rozbroić system sygnalizacji włamania (SSW).

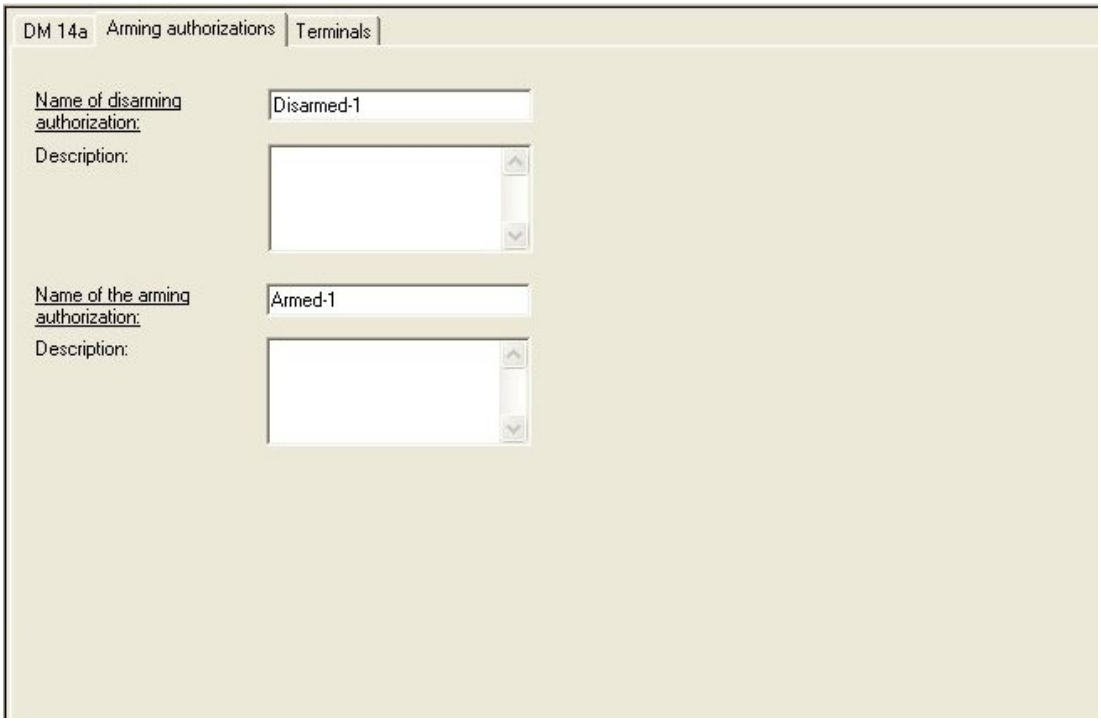


W tym przypadku sygnały **System sygnalizacji włamania uzbrojony** i **System sygnalizacji włamania gotowy do uzbrojenia** należy zreplikować na stykach wejściowych innych wejść.
Gdy dla tego samego obszaru zazbrajania będzie tworzony drugi model wejścia, edytor

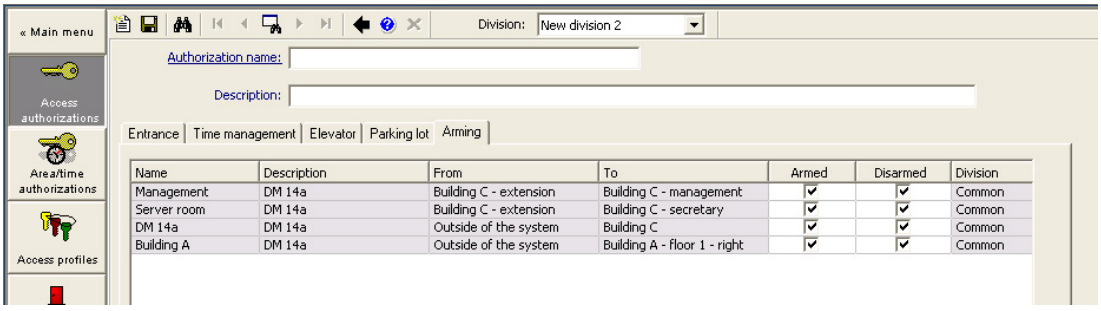
urządzeń wykona replikację automatycznie. Opis sygnału drugich drzwi zostanie poszerzony o numer odpowiedniego sygnału z modelu pierwszego wejścia, np. 1:04 [= czwarty sygnał na karcie 1].



Po utworzeniu wystąpienia modelu wejścia 14 pojawi się dodatkowa karta **Uprawnienia uzbrajania** z listą autoryzacji wygenerowanych wskutek utworzenia instancji. Użytkownik może swobodnie wybierać nazwy dla uprawnień do uzbrajania/ rozbrajania.



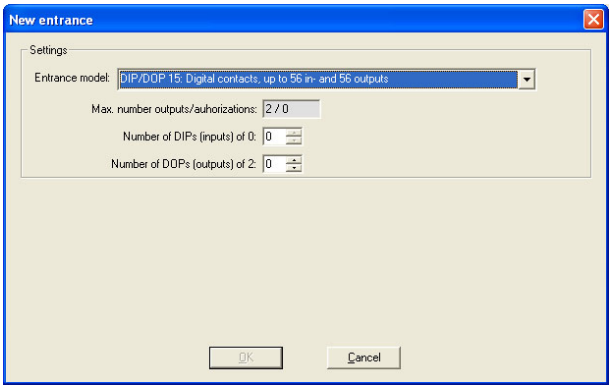
Podczas tworzenia zestawienia autoryzacji wszystkie utworzone wystąpienia modelu wejścia 14 są wyszczególnione na karcie **Uzbrojenie** w oknach dialogowych **Uprawnieniami dostępu** i **Uprawnienia obszarowe/czasowe**. Uprawnienia do uzbrajania i rozbrajania można przypisywać osobno.



13.6.3 Przełączniki DIP i DOP (model drzwi 15)

Tworzenie wejścia o modelu 15:

Ten model wejścia oferuje niezależne sygnały wejściowe i wyjściowe.



Jeśli wszystkie interfejsy czytnika zostaną zajęte, tylko ten model wejścia staje się dostępny. Można go konfigurować, dopóki występują co najmniej dwa wolne sygnały.
Tego modelu wejścia nie można przypisywać do kontrolerów AMC połączonych z windami (model 07) lub parkingami (model 05c).

Model wejścia 15

Możliwe sygnały: Te domyślne nazwy można zastąpić.

Sygnał wejściowy	Sygnał wyjściowy
DIP	DOP
DIP-1	DOP-1
...	...
DIP-63	DOP-63

W odróżnieniu od innych modeli drzwi model wejścia 15 służy on do zarządzania wejściami i wyjściami kontrolera, które są nadal wolne. Udostępnia je w całym systemie jako wejścia ogólne i wyjścia beznapięciowe.
W odróżnieniu od styków wejściowych w innych modelach drzwi te w modelu wejścia 15 można przeglądać indywidualnie w interfejsie użytkownika systemu BIS.

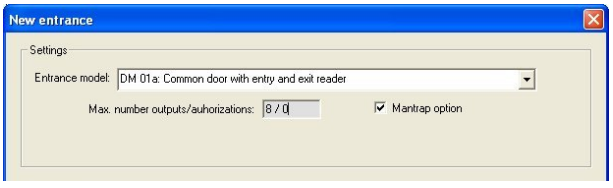
Przywracanie ustawień przełączników DOP po ponownym uruchomieniu

Po restarcie kontrolera MAC lub AMC standardowo następuje reset wartości stanów podległych im przełączników DOP do wartości domyślnej 0 (zero).
Aby mieć pewność, że ponowne uruchomienie zawsze będzie powodować reset przełącznika DOP do ostatniego stanu przypisanego ręcznie, zaznacz przełącznik DOP w drzewie urządzeń, a następnie w głównym oknie zaznacz pole wyboru **Zachowaj stan**.

13.6.4 Modele drzwi ze śluzami osobowymi

Tworzenie śluzy osobowej

Modele wejść 01 i 03 mogą być używane jako „śluzy osobowe” wymuszające pojedyncze przechodzenie posiadaczy kart. Użyj pola wyboru **Opcja śluzy**, aby udostępnić niezbędne dodatkowe sygnały.



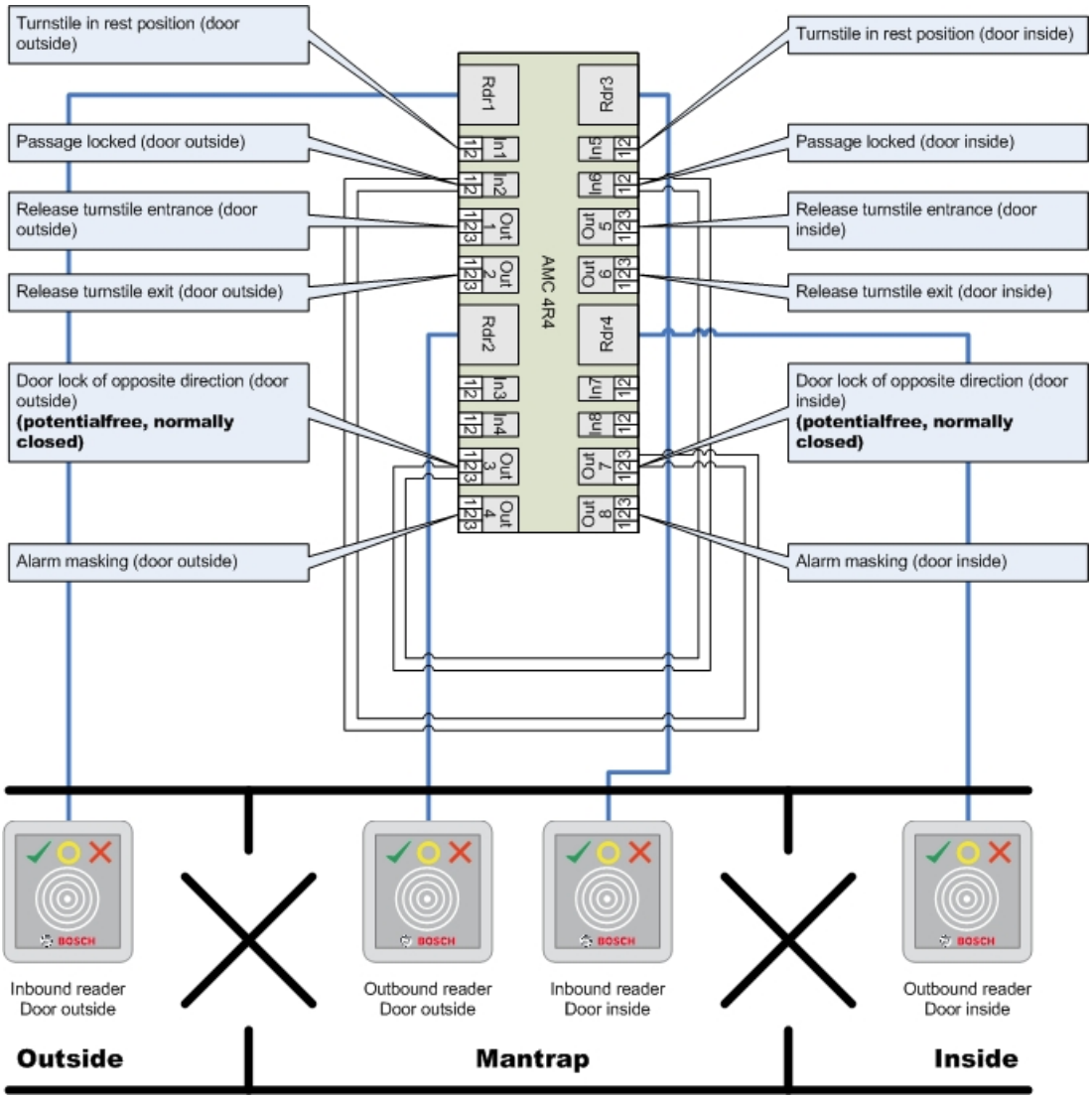
Można dowolnie łączyć wszystkie modele 01 i 03, z tym że trzeba ustawić tę opcję na obu wejściach tworzących śluzę.

Oprócz typowych przypisań sygnałów jak w innych modelach drzwi opcja śluzy osobowej wymaga przypisania dodatkowych sygnałów.

Przykład: śluza osobowa na jednym kontrolerze

Bramki obrotowe są najpowszechniejszym sposobem kontroli dostępu pojedynczych osób posiadających identyfikatory. Dlatego w poniższym przykładzie użyjemy modelu drzwi 3a (kontrolowana bramka obrotowa z czytnikiem wejścia i wyjścia).

Konfiguracja śluzy osobowej z dwoma bramkami obrotowymi (model drzwi 03a):



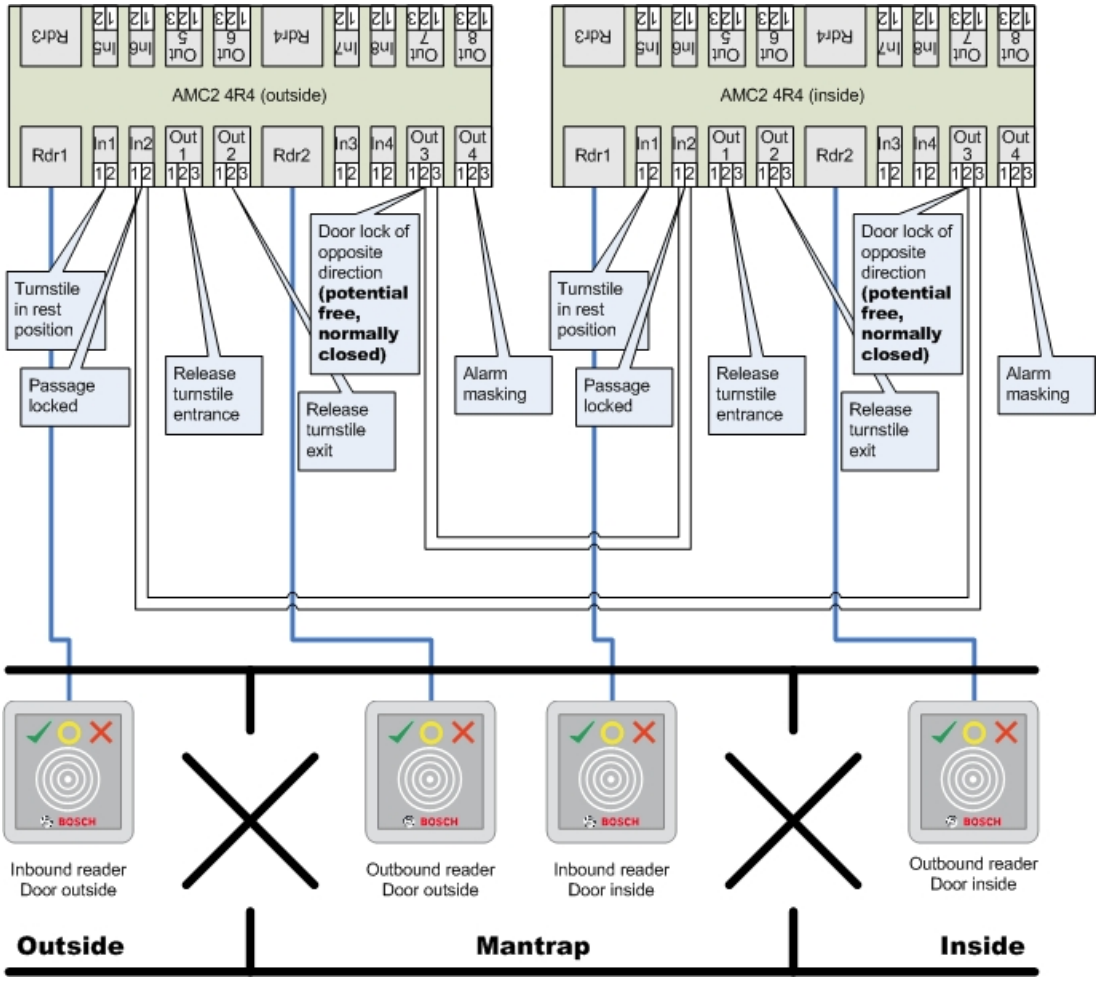
Połączenia do blokady drzwi dla kierunku przeciwnego zapewniają, że w danym momencie można otworzyć tylko jedną bramkę obrotową.

Uwaga!

Sygnały wyjściowe (Wyjście) 3 i 7 należy ustawić jako beznapięciowe (tryb bezprądowy). Sygnał „blokada drzwi dla kierunku przeciwnego” jest aktywna przy ustawieniu 0. Należy go zastosować do wyjść 3 i 7, które są stykami rozwiernymi.

Przykład: śluza osobowa na dwóch kontrolerach

Konfiguracja śluzy osobowej z dwiema bramkami obrotowymi (model wejścia 03a), których obsługa podzielona jest między dwa kontrolery:

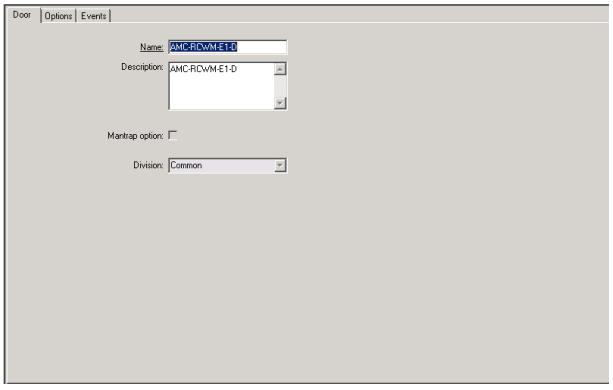


Połączenia do blokady drzwi dla kierunku przeciwnego zapewniają, że w danym momencie można otworzyć tylko jedną bramkę obrotową.

Uwaga!
Sygnał wyjściowy (Wyjście) 3 należy ustawić jako beznapięciowy (tryb bezprądowy).
Sygnał „blokada drzwi dla kierunku przeciwnego" jest aktywna przy ustawieniu 0. Należy go zastosować do wyjścia 3, które jest stykiem rozwiernym.

13.7 Drzwi

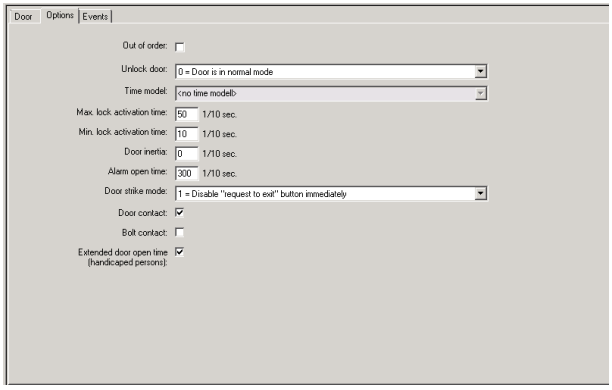
Konfigurowanie drzwi: Parametry ogólne



Rysunek 13.1:

Parametr	Możliwe wartości	Opis
Nazwa	Alfanumeryczne, do 16 znaków	Wygenerowaną wartość domyślną można opcjonalnie zastąpić unikatową nazwą.
Opis	Alfanumeryczne, do 255 znaków	
Strefa	Strefą domyślną jest „Wspólna”	To jest pole tylko do odczytu. Przypisań do stref dokonuje się w edytorze urządzeń DevEdit dla każdych drzwi w hierarchii urządzeń.
Tylko w przypadku modeli drzwi 01 i 03, jeśli skonfigurowano śluzę osobową:		
Opcja śluzy	0 = nieaktywne (pole wyboru jest wyczyszczone) 1 = aktywne (pole wyboru jest zaznaczone)	Istnieje śluza osobowa zawierająca kombinację drzwi modelu 01 lub 03. Opcję śluzy należy aktywować dla **obojga** drzwi. Drzwi będą również wymagały specjalnego fizycznego okablowania.

Konfigurowanie drzwi: Opcje

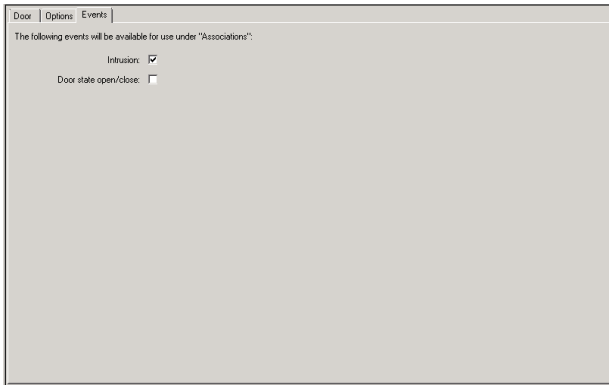


Parametr	Możliwe wartości	Uwagi
Obsługa ręczna	0 = pole wyboru jest wyczyszczone. 1 = pole wyboru jest zaznaczone.	0 = drzwi są w trybie normalnym (domyślnie), to znaczy podlegają kontroli dostępu w ramach całego systemu. 1 = drzwi są wykluczone z systemu kontroli dostępu. Drzwi nie są kontrolowane i nie generują komunikatów. Można je zablokować lub odblokować tylko ręcznie. Wszystkie pozostałe parametry tych drzwi są wyłączone. Ten parametr należy ustawić oddzielnie dla drzwi i czytnika.
Odblokuj drzwi	0 = drzwi w trybie normalnym 1 = drzwi są niezablokowane	0 = tryb normalny (domyślnie) — drzwi zostaną zablokowane lub odblokowane w zależności od uprawnień dostępu w poświadczeniach.

	2 = drzwi są odblokowane w zależności od modeli czasowego 3 = po pierwszym przejściu drzwi są otwarte w zależności od modelu czasowego 5 = drzwi są zablokowane na długo 6 = drzwi są zablokowane w zależności od modelu czasowego	1 = odblokowanie na dłuższy czas — kontrola dostępu jest zawieszona na ten czas. 2 = odblokowanie na czas określony przez model czasowy. Kontrola dostępu jest zawieszona w tym okresie. 3 = zablokowane tak długo, jak model czasowy jest aktywny, dopóki pierwsza osoba nie uzyska dostępu — następnie otwierane na tak długo, jak model czasu jest aktywny. 5 = zablokowane do momentu ręcznego odblokowania. 6 = zablokowane tak długo, jak model czasowy jest aktywny — brak kontroli drzwi, nie można z nich korzystać w czasie, gdy model czasowy jest aktywny.
Model czasowy	Jeden z dostępnych modeli czasowych	Model czasowy dla czasów otwarcia drzwi. W przypadku wybrania modelu drzwi 2, 3, 4, 6 lub 7 pojawia się pole listy z modelami czasowymi. Wybór modelu czasowego jest konieczny.
Maks. czas aktywacji blokady	0 - 9999	Czas trwania aktywacji automatu do otwierania drzwi, w wielokrotności 1/10 sekundy — domyślnie: 50 dla drzwi, 10 dla drzwi obrotowych (03) i 200 dla barier (05c lub 09c).
Min. czas aktywacji blokady	0 - 9999	Minimalny czas trwania aktywacji automatu do otwierania drzwi, w wielokrotności 1/10 sekundy. Zamki elektromagnetyczne potrzebują nieco czasu na rozmagnesowanie — domyślnie: 10.
Bezwładność drzwi	0 - 9999	Po upływie czasu aktywacji drzwi mogą zostać otwarte w tym przedziale czasu stanowiącym wielokrotność 1/10 sekundy bez wywoływania alarmu. Drzwi hydrauliczne potrzebują nieco czasu na skumulowanie ciśnienia — domyślnie: 0.
Czas otwarcia alarmu	0 - 9999	Jeśli po tym czasie stanowiącym wielokrotność 1/10 sekundy drzwi pozostaną otwarte, zostanie wyświetlony komunikat (drzwi otwarte zbyt długo) — domyślnie: 300. 0 = brak limitu czasu, brak komunikatu
Tryb zamka drzwi	Wpis w polu listy	0 = przycisk REX (żądanie wyjścia) wyłączony po czasie aktywacji 1 = przycisk REX (żądanie wyjścia) jest natychmiast wyłączany (= domyślnie)

Kontaktron drzwiowy	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	0 = drzwi nie mają styku w ramie 1 = drzwi mają styk w ramie. Zamknięcie styku zwykle oznacza, że drzwi są zamknięte. (= domyślnie)
Styk rygla	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	0 = drzwi nie mają styku rygla (= domyślnie) 1 = drzwi mają styk rygla. Otwarcie lub zamknięcie drzwi powoduje generowanie komunikatu.
Rozszerzony czas otwierania drzwi (dla osób niepełnosprawnych)	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	0 = czas aktywacji blokady jest normalny. 1 = czas aktywacji blokady jest wydłużony o współczynnik określony w ogólnosystemowym parametrze EXTIMFAC. Ma to dać osobom niepełnosprawnym więcej czasu na przejście przez drzwi. (= domyślnie)

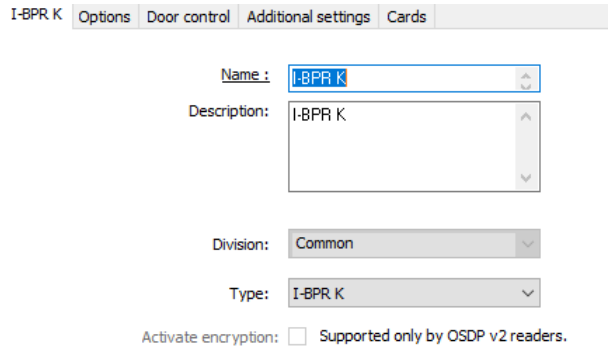
Konfigurowanie drzwi: Zdarzenia



Parametr	**Możliwe wartości**	**Uwagi**
Włamanie	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	0 = brak komunikatu o włamaniu. To ustawienie jest przydatne, gdy drzwi można swobodnie otwierać od środka. 1 = Po nieautoryzowanym otwarciu zostanie zainicjowany komunikat. Kolejny komunikat będzie wskazywał zamknięcie. (domyślnie)
Stan drzwi otwarte/ zamknięte	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	0 = nie jest wysyłany komunikat „drzwi otwarte” (domyślnie) 1 = po otwarciu lub zamknięciu jest wysyłany komunikat.

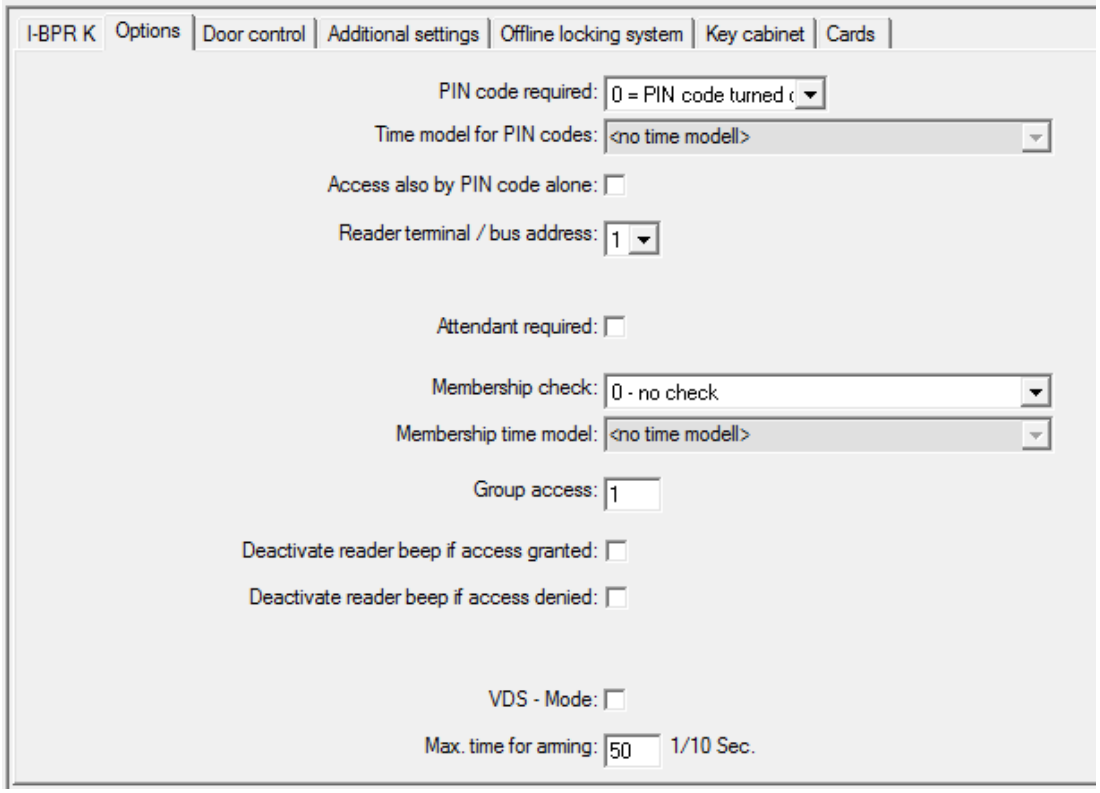
13.8 Czytniki

Konfigurowanie czytnika: Parametry ogólne



Parametr	Możliwe wartości	Opis
Nazwa czytnika	alfanumeryczne, od 1 do 16 znaków	Wartość domyślną można zastąpić unikatową nazwą.
Opis czytnika	Alfanumeryczne, od 0 do 255 znaków	Tekstowy opis.
Strefa	Strefą domyślną jest „Wspólna”	Opcja działa tylko w przypadkach, gdy istnieją licencje na strefy i są używane.
Typ	alfanumeryczne, od 1 do 16 znaków	Typ czytnika lub grupy czytników

Konfigurowanie czytnika: Opcje



Parametr	Możliwe wartości	Opis
Wymagany kod PIN	0 = kod PIN wyłączony — nie trzeba go wpisywać (domyślnie) 1 = kod PIN włączony — zawsze trzeba go wpisać 2 = kod PIN kontrolowany przez model czasowy — trzeba wpisać tylko w okresach poza modelem czasowym	To pole jest aktywne tylko wtedy, gdy do czytnika podłączono urządzenie wejściowe. Należy pamiętać, że kontrole ustawień na karcie, np. jej autoryzacje i kolejność dostępu (jeśli włączono tę funkcję), mają pierwszeństwo przed kontrolą poprawności kodu PIN.
Model czasowy do kodów PIN	Jeden z dostępnych modeli czasowych	Wybór modelu czasu w tym polu jest obowiązkowy, jeśli w parametrze **Wymagany kod PIN** ustawiono wartość 2.
Dostęp także z samym kodem PIN	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	Określa, czy ten czytnik może również zezwalać na dostęp na podstawie samego kodu PIN, czyli bez karty, jeśli system kontroli dostępu jest tak skonfigurowany. Patrz .
Terminal czytnika/ adres magistrali	1 - 4	Kontroler AMC 4W: numerowanie odpowiada interfejsom Wiegand. Kontroler AMC 4R4: numerowanie odpowiada adresom zworek czytnika.
Potrzebny parkingowy	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	0 = gość nie potrzebuje opiekuna (domyślnie) 1 = również opiekun musi korzystać z czytnika
Sprawdzanie członkostwa	Wpis w polu listy	**Zauważ**, że opcja Sprawdzanie członkostwa działa tylko dla definicji kart wstępnie skonfigurowanych w systemie (szare tło), a nie dla definicji niestandardowych. **0 — bez sprawdzania** Sprawdzanie członkostwa jest wyłączone, ale karta jest sprawdzana pod kątem autoryzacji jak zwykle (domyślnie). **1 — kontrola** Karta jest sprawdzana tylko pod kątem identyfikatora firmy, czyli członkostwa w systemie.

		2 — w zależności od modelu czasowego Karta jest sprawdzana pod kątem identyfikatora firmy (członkostwa), ale tylko w okresie określonym w modelu czasowym członkostwa.
Model czasowy członkostwa	Jeden z dostępnych modeli czasowych	Model czasowy włącza/wyłącza sprawdzanie członkostwa. Wybór modelu czasowego jest obowiązkowy, jeśli w ustawieniu **Sprawdzanie członkostwa** zaznaczono opcję 2.
Dostęp grupy	1 - 10	**Czytniki z klawiaturą:** Minimalna liczba ważnych kart, które należy przystawić do czytnika kart, aby drzwi zostały otwarte. Grupa może zawierać więcej kart, niż określa ta liczba. W takim przypadku klawisz ENTER/# służy do sygnalizowania, że grupa jest kompletna. Wtedy drzwi zostaną otwarte. **Czytniki bez klawiatury:** Dokładna liczba ważnych kart, które należy przystawić do czytnika kart, aby drzwi zostały otwarte. Wartość domyślna to 1.
Wyłącz buzzer czytnika, gdy udzielono dostępu	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	W przypadku aktywowania tej opcji (1) czytnik milczy, jeśli autoryzowany użytkownik uzyska dostęp.
Wyłącz buzzer czytnika, gdy nie udzielono dostępu	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	W przypadku aktywowania tej opcji (1) czytnik milczy, gdy nieuprawnionemu użytkownikowi zostanie odmówiony dostęp.
 Działanie funkcji „Wyłącz buzzer czytnika” zależy od oprogramowania układowego czytnika. Oprogramowanie układowe niektórych czytników może nie obsługiwać tej funkcji.		
Tryb VDS	0 = nieaktywny (pole wyboru jest wyczyszczone)	W przypadku aktywowania tej opcji (1) sygnalizacja czytnika jest wyłączona.

	1 = aktywny (pole wyboru jest zaznaczone)	
Maks. czas uzbrajania	1–100 [1/sec]	Maksymalny czas na informację zwrotną z centrali alarmowej, że uzbrajanie zostało zakończone.

Tryb pracy i sieci

Ta karta jest wyświetlana tylko dla czytników biometrycznych połączonych w sieć.

Szablony to zapisane wzorce. Mogą to być dane kart lub dane biometryczne.

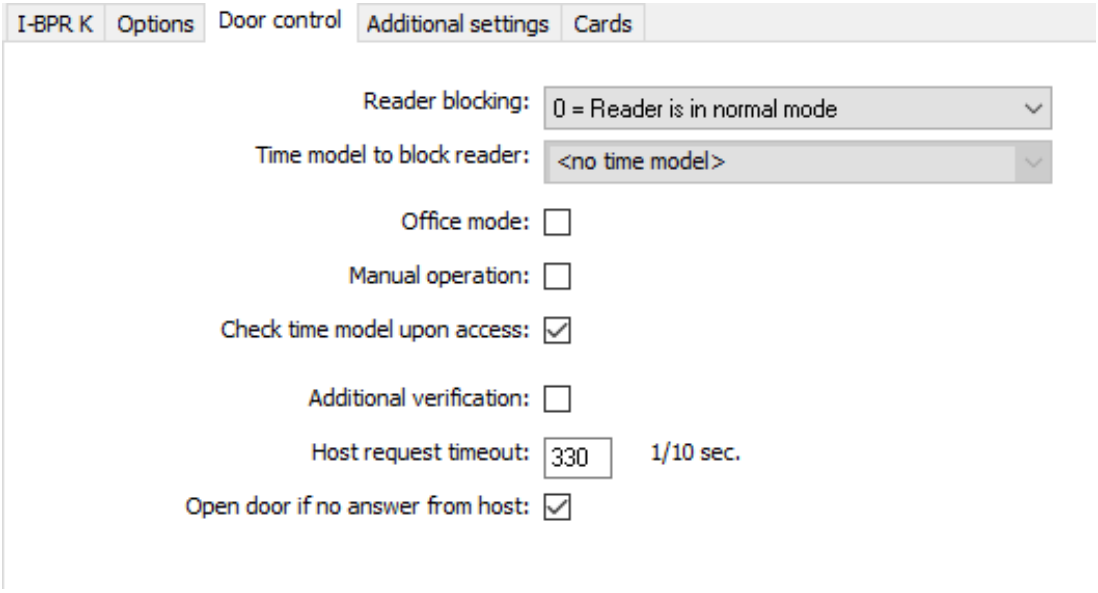
Szablony mogą być przechowywane w urządzeniach nad czytnikiem w drzewie urządzeń oraz w samym czytniku. Dane w czytniku są okresowo aktualizowane przez znajdujące się nad nim urządzenie.

W czytniku można określić, że podczas podejmowania decyzji o dostępie ma używać swoich własnych szablonów lub szablonów z urządzeń nad nim.

Parametr	**Opis**
Adres IP:	Adres IP tego sieciowego czytnika
Port:	Domyślny port to `51211`
Szablony na serwerze	
Tylko karta	Czytnik odczytuje tylko dane karty. Uwierzytelnia je na podstawie danych z całego systemu.
Karta i odcisk palca	Czytnik odczytuje zarówno dane karty, jak i dane daktyloskopijne. Uwierzytelnia je na podstawie danych z całego systemu.
Szablony na urządzeniu	
Weryfikacja zależna od osoby	Czytnik pozwala, aby ustawienia indywidualnego posiadacza karty decydowały o tym, którego **trybu identyfikacji** będzie używał. Istnieją następujące opcje wykorzystywania danych osobowych: – Tylko odcisk palca – Tylko karta – Karta i odcisk palca Zostały one opisane w dalszej części tej tabeli.
Tylko odcisk palca	Czytnik odczytuje tylko dane odcisków palców. Uwierzytelnia je na podstawie własnych przechowywanych danych.
Tylko karta	Czytnik odczytuje tylko dane karty. Uwierzytelnia je na podstawie własnych przechowywanych danych.
Karta i odcisk palca	Czytnik odczytuje zarówno dane karty, jak i dane daktyloskopijne. Uwierzytelnia je na podstawie własnych przechowywanych danych.

Parametr	Opis
Karta lub odcisk palca	Czytnik odczytuje dane karty lub dane daktyloskopijne, w zależności od tego, które posiadacz karty przedstawi jako pierwsze. Uwierzytelnia je na podstawie własnych przechowywanych danych.

Konfigurowanie czytnika: Kontrola drzwi

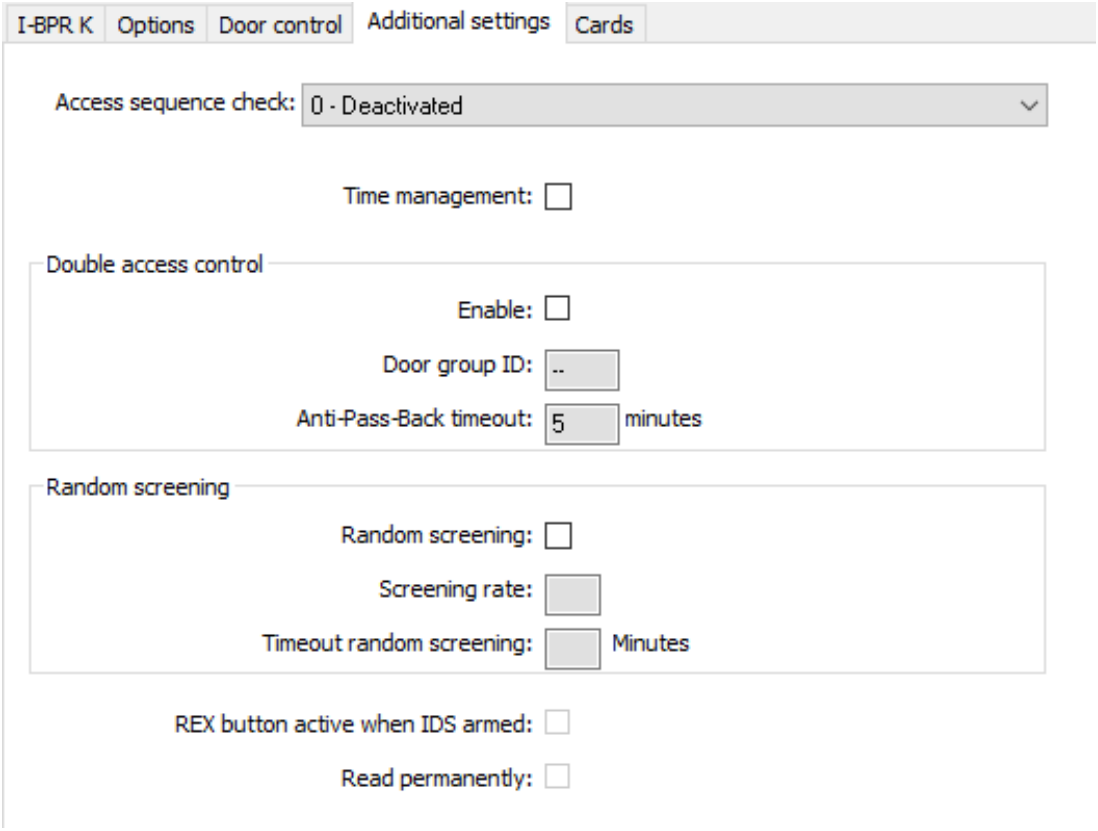


Parametr	Możliwe wartości	Uwagi
Blokowanie czytnika	Wpis w polu listy	0 = Czytnik w trybie normalnym — bez blokady (= domyślnie) 1 = Czytnik jest trwale zablokowany 2 = Czytnik jest zablokowany w zależności od modelu czasowego — blokada zgodnie z modelem czasowym ustawionym w parametrze *Model czasowy blokowania czytnika*
Model czasowy blokowania czytnika	Jeden z modeli czasowych zdefiniowanych w systemie.	Blokuje czytnik zgodnie z wybranym modelem czasowym.
Tryb biurowy	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	Umożliwia używanie tego czytnika w trybie biurowym.
Obsługa ręczna	0 = nieaktywny (pole wyboru jest wyczyszczone)	0 = czytnik w trybie normalnym (= domyślnie)

	1 = aktywny (pole wyboru jest zaznaczone)	1 = czytnik jest skutecznie usunięty z systemu kontroli dostępu, czyli „nieczynny"". Nie odbiera żadnych poleceń. Wszystkie pozostałe parametry tego czytnika są wyłączone. Parametr należy ustawić niezależnie dla czytnika i drzwi.
Sprawdź modele czasowe podczas dostępu	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	0 = Modele czasowe nie będą sprawdzane. Nie ma czasowego ograniczenia dostępu. 1 = Jeśli posiadacz karty ma przypisany model czasowy — bezpośrednio lub w formie uprawnień obszarowych/czasowych, model czasowy będzie sprawdzany. (= domyślnie)
Dodatkowa weryfikacja	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	0 = weryfikacja hosta nie jest wymagana 1 = wymagana jest weryfikacja hosta (domyślnie) (**WAŻNE**: Aktywacja tej opcji jest wymagana na potrzeby dodatkowej weryfikacji wideo przez operatora systemu BVMS lub BIS)
Limit czasu żądania hosta	0 = nieaktywne	0 = kontroler AMC działa bez funkcji weryfikacji hosta (nie używa opcji *Zmiana obszaru* ani *Liczenie osób*). Ta kontrola jest aktywna tylko wtedy, gdy włączono opcje Weryfikacja hosta (0) i *Otwórz drzwi, gdy brak odpowiedzi z hosta* (1). Od 1 do 9999 = korzystanie z czytnika wymaga zapytania do systemu BIS. Odpowiedź na zapytanie musi zostać udzielona w określonym przedziale czasu. Jeśli czas upłynie, kontroler AMC sprawdza parametr **Otwórz drzwi, gdy brak odpowiedzi z hosta** i sam podejmuje decyzję. Wartości są wielokrotnością 1/10 sekundy. (Domyślne = 30).
Otwórz drzwi, gdy brak odpowiedzi z hosta	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	Ta kontrola jest aktywna tylko po ustawieniu parametru **Weryfikacja hosta**. 0 = nie otwiera drzwi, jeśli jest wymagana decyzja hosta, ale nie można jej uzyskać (działanie w trybie offline). 1 = otwiera drzwi po upływie limitu czasu, jeśli kontroler AMC może je zwolnić. (= domyślnie)

Sprawdź kredytowanie biletów za parking	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	Po włączeniu tej opcji (1) system sprawdza liczbę punktów, którymi można płacić za parking.
Sprawdź przedłużone parkowanie	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	Po włączeniu tej opcji (1) system sprawdza, czy parkowanie nie trwało za długo.

Konfigurowanie czytnika: Ustawienia dodatkowe

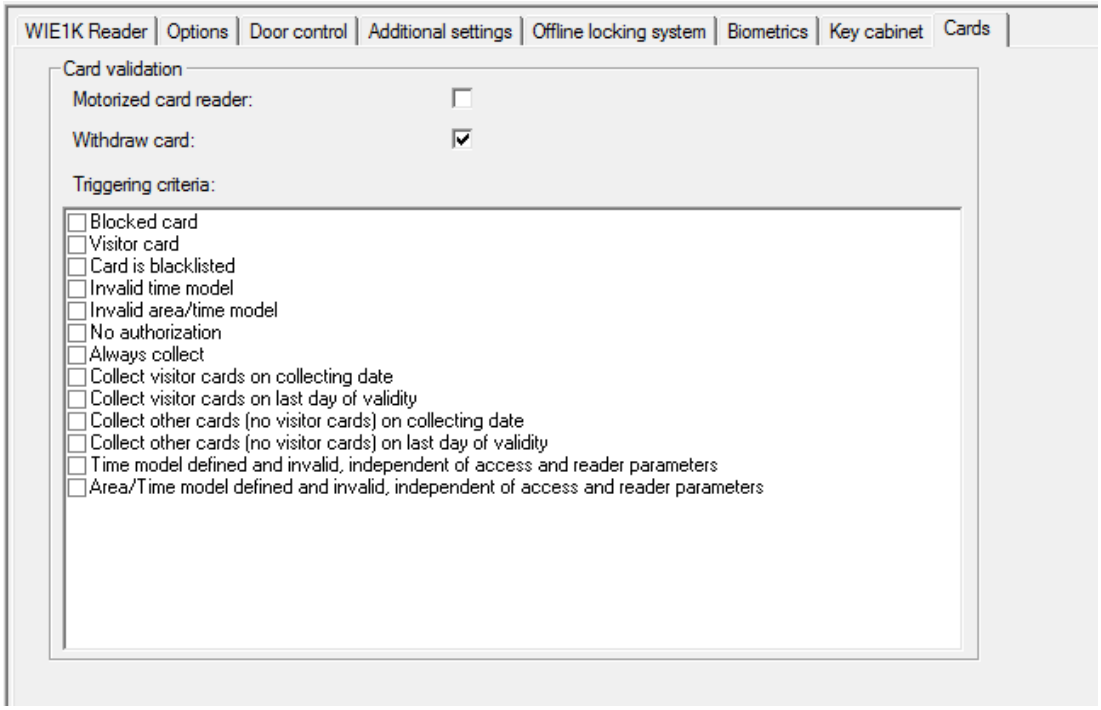


Parametr	**Możliwe wartości**	**Uwagi**
Sekwencyjna kontrola dostępu	0 — nieaktywne 1 — aktywny; dezaktywowanie przy awarii LAC 2 — aktywny; pozostaw aktywny przy awarii LAC	0 = czytnik nie bierze udziału w sprawdzaniu kolejności dostępu (= domyślnie) Aktywowana funkcja kontroli kolejności może realizować następujące warianty obsługi osób z ustawionym statusem NIEZNANE: 1 = Pierwszy odczyt karty zostanie wyłączony bez sprawdzania lokalizacji. Wszystkie kontrolery muszą być online.

	3 — aktywne; użycie ścisłego sprawdzania sekwencyjnego nawet w przypadku usterki LAC (uwaga: aktualizuj lokalizację osoby ręcznie)	2 = Pierwsze odczyt karty zostanie wyłączony bez sprawdzania lokalizacji. 3 = Sprawdzanie lokalizacji zostanie wyłączone dla każdego odczytu karty podczas awarii kontrolera LAC.
 Na platformie BIS znajduje się polecenie do kontrolerów MAC, które aktywuje lub dezaktywuje cały mechanizm sprawdzania kolejności dostępu. Aby wyłączyć kontrolę kolejności dostępu przez określony czas, podaje się wartość w minutach, maksymalnie 2880 (= 48 godzin). Ustawienie wartości „0” całkowicie dezaktywuje funkcję kontrolę kolejności dostępu. **Uwaga:** To polecenie może modyfikować funkcję sprawdzanie kolejności dostępu tylko dla czytników, w których ustawiono parametr **Włącz monitorowanie sekwencji dostępu**. Nie wyłącza/włącza sprawdzania kolejności dostępu na *wszystkich* czytnikach.		
Zarządzanie czasem	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	Po włączeniu tej opcji (1) proces systemu ACE zbiera dane dla systemu zarządzania czasem i obecnością.
Podwójna kontrola dostępu (kontrola w funkcji zapobiegającej przekazaniu karty niepowołanej osobie)		
Włącz	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	0 = bez podwójnej kontroli dostępu (= domyślnie) 1 = z podwójną kontrolą dostępu W przedziale czasowym ustalonym przez parametr **Czas trwania** nie można użyć tej samej karty na tym czytniku i innych czytnikach w grupie. Jeśli ten parametr jest aktywny, należy podawać identyfikator grupy drzwi, nawet jeśli używany jest tylko jeden czytnik.
Identyfikator grupy drzwi	Listy A–Z i a–z oraz znak „-” 2 znaki	Czytniki można grupować za pomocą identyfikatora grupy drzwi. Przyłożenie karty do jednego czytnika zablokuje możliwość następnych rejestracji na wszystkich pozostałych czytnikach w grupie drzwi (domyślnie = **--**) aż do upływu limitu czasu.

Czas oczekiwania blokady podwójnego wejścia	1 - 120	Po upływie tego czasu na czytniku można użyć tej samej karty. Z chwilą użycia karty w czytniku poza grupą blokada zostanie zniesiona. Wartości to minuty — domyślnie = 5.
Losowa kontrola	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	0 = bez losowej kontroli 1 = losowa kontrola w oparciu o współczynnik uniemożliwi dostęp, dopóki nie zostanie wyłączona w oknie dialogowym **Blokowanie**.
Odsetek kontroli	1 - 100	Procent zdarzeń losowej kontroli używanych do rozszerzonego sprawdzenia. Opcja dostępna tylko po włączeniu funkcji losowej kontroli.
Losowa kontrola limitu czasu	1 - 120	W ustalonym czasie użytkownik podlega kontroli losowej. Wartości to minuty — domyślnie = 5.
Przycisk REX aktywny po uzbrojeniu IDS	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	Dotyczy tylko modeli drzwi **10** i **14**: przyciski REX są domyślnie wyłączone po włączeniu systemu SSW. To uniemożliwiłoby wyjście z monitorowanego obszaru. Nowy parametr czytnika włącza przycisk REX nawet po uzbrojeniu systemu SSW. Ten parametr należy również ustawić w przypadku używania czytnika zamiast przycisku.
Odczyt na stałe	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	Czytnik jest odczytywany nieprzerwanie, jeśli zainstalowano na nim odpowiednie oprogramowanie układowe producenta.

Konfigurowanie czytnika: Karty



Parametr	Możliwe wartości	Uwagi
Mechaniczny czytnik kart	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	Zaznacz to pole wyboru, jeśli jest używany mechaniczny czytnik kart
Wycofaj kartę	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	W przypadku mechanicznego czytnika kart wycofanie oznacza fizyczne wyciągnięcie karty. W przypadku innych czytników kart wycofanie oznacza unieważnienie karty przez system.
Kryteria wyzwalania	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	Wybierz z tej listy wszelkie kryteria, które powinny wywoływać czynność **Wycofaj kartę** .

Uwaga!
Mechaniczne czytniki kart mogą współpracować tylko z czytnikami IBPR.

13.8.1 Konfigurowanie losowej kontroli

Losowa kontrola to popularna metoda zwiększania bezpieczeństwa obiektu poprzez losowe wybieranie personelu w celu poddania go dodatkowej kontroli.

Wymagania wstępne:

- Wejście powinno mieć postać śluzy lub bramki obrotowej, aby uniemożliwiać „przemykanie” tuż za inną osobą bez pokazywania swojego identyfikatora.
- Czytnik kart musi być obecny dla co najmniej jednego kierunku przejścia.
- W czytnikach musi być skonfigurowana normalna kontrola dostępu.
- Osobno dla każdego czytnika można skonfigurować układ losujący.
- W bezpośrednim sąsiedztwie powinna znajdować się stacja robocza służąca do zwalniania wszelkich blokad nakładanych przez system.

Procedura

1. Znajdź żądany czytnik w edytorze urządzeń DevEdit.
2. Na karcie **Ustawienia** zaznacz pole wyboru **Losowa kontrola**.
3. W polu **Procent kontroli** wprowadź odsetek osób, które mają być kontrolowane.
4. Zapisz wprowadzone ustawienia.

13.9 Dostęp z użyciem samego kodu PIN

Informacje wstępne

Czytniki wyposażone w klawiaturę można skonfigurować w taki sposób, aby zezwalały na dostęp po podaniu samego kodu PIN.
Po dostosowaniu czytników do takiego działania operator systemu BIS może przypisywać poszczególne kody PIN wybranym pracownikom. W efekcie otrzymują oni „karty wirtualne”, na których zapisany jest tylko kod. Nosi on nazwę kodu identyfikacyjnego PIN. W przeciwieństwie do tego kod weryfikacyjny PIN to kod PIN używany w połączeniu z kartą, więc zapewniający wyższy poziom bezpieczeństwa.

Operator można ręcznie wprowadzać kody PIN dla pracowników lub przydzielać im kody PIN wygenerowane przez system.
Należy pamiętać, że ten sam pracownik może kontynuować dostęp, korzystając z dowolnych przydzielonych mu kart fizycznych.

Wymaganie wstępne w zakresie uprawnień operatorów

Posiadacz karty może otrzymać prawo dostępu za pomocą samego kodu PIN tylko od operatorów posiadających specjalne uprawnienia do przydzielania wirtualnych kart. Aby nadać operatorowi takie uprawnienie, wykonaj następujące czynności.

1. Przejdź do menu głównego > **Konfiguracja** > **Operatorzy i stacje robocze** > **Profile użytkownika**.
2. Zaznacz profil użytkownika, który ma otrzymać autoryzację:
   Wprowadź go w polu tekstowym **Nazwa profilu** lub znajdź za pomocą funkcji wyszukiwania.
3. Na liście okien dialogowych kliknij komórkę zawierającą pozycję **Karty** **.**W dolnej części głównego okna pojawi się okno wyskakujące **Funkcje specjalne**.
4. W panelu Funkcje specjalne zaznacz pole wyboru **Przypisz wirtualne karty (PIN)**.
5. Kliknij przycisk  lub **Zastosuj**, aby zapisać zmiany.

Ustawienie długości kodu identyfikacyjnego PIN dla wszystkich typów czytników
Długość kodów PIN wprowadzanych ręcznie lub generowanych przez system jest regulowana przez parametr ustawiany w konfiguracji systemu.
– Menu główne > **Konfiguracja** > **Opcje** > **Kody PIN** > **Długość kodu PIN**

Konfigurowanie funkcji dostępu z użyciem samego kodu PIN w czytniku
1. Przejdź do menu głównego > **Konfiguracja** > **Dane urządzenia** > drzewo **Stacje robocze**  .
2. W panelu **Stacja robocza** wybierz stację roboczą, do której czytnik jest fizycznie podłączony.
3. Kliknij stację roboczą prawym przyciskiem myszy i dodaj czytnik typu **Wprowadzanie kodu PIN w oknie dialogowym** lub **Generowanie kodu PIN w oknie dialogowym**.
4. Wybierz czytnik w panelu **Stacje robocze**.
   Na prawo od panelu **Stacje robocze** pojawi się panel niestandardowej konfiguracji czytnika.
5. Sprawdź, czy lista rozwijana **Domyślny sposób użycia karty** zawiera domyślną wartość **Wirtualna karta. Użyj kodu PIN jako karty**.
6. Kliknij przycisk  lub **Zastosuj**, aby zapisać zmiany.
7. W edytorze urządzeń DevEdit przejdź do drzewa **Konfiguracja urządzeń**  .
8. Wybierz czytnik przy wejściu, w którym chcesz skonfigurować dostęp za pomocą samego kodu PIN.
9. Na karcie **Opcje** zaznacz pole wyboru **Dostęp także z samym kodem PIN**.
10. Kliknij przycisk  lub **Zastosuj**, aby zapisać zmiany.

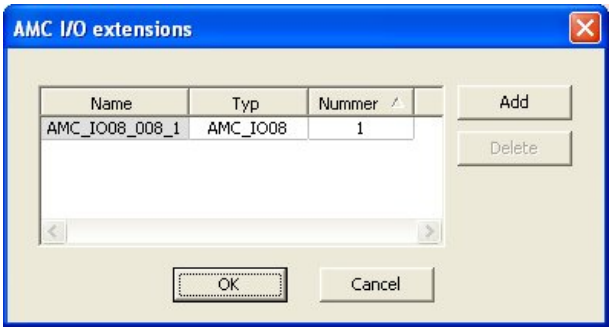
13.10 Moduły rozszerzeń kontrolera AMC

Tworzenie obiektu AMC-I/O-EXT (modułu rozszerzeń we/wy)
Moduły (karty) rozszerzeń dostarczają dodatkowe sygnały wejściowe i wyjściowe, jeśli osiem styków w kontrolerze AMC nie wystarcza do podłączenia niezbędnych sygnałów (na przykład gdy są używane windy).
Te moduły są fizycznie podłączone do kontrolerów AMC i mogą być instalowane tylko pod odnośnymi kontrolerami AMC w edytorze urządzeń. W eksploratorze jest wybierany odpowiedni wpis kontrolera AMC potrzeby do utworzenia obiektu karty AMC-EXT, a w menu kontekstowym **Nowy obiekt** jest wybierany wpis **Nowy moduł rozszerzeń**.

Uwaga!

Kliknięcie przycisku **+**  na pasku narzędzi edytora urządzeń powoduje utworzenie tylko nowego wejścia. Moduły rozszerzeń można wybierać za pomocą menu kontekstowego.

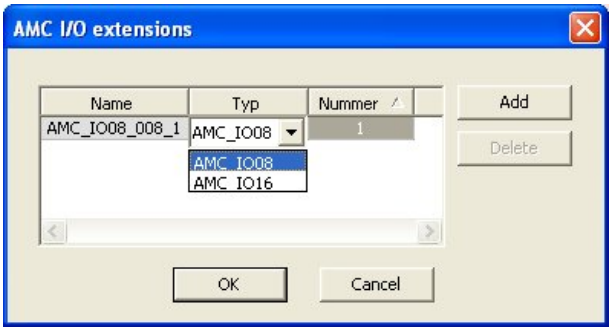
Pojawi się okno dialogowe wyboru kart rozszerzeń.



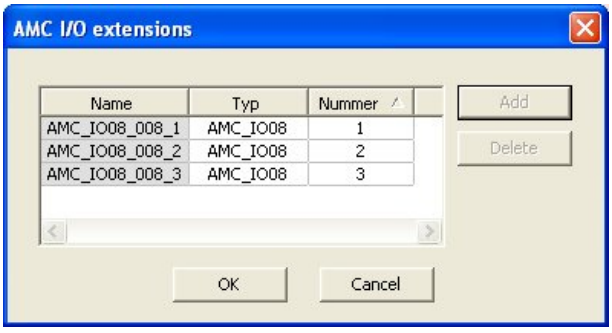
Moduły AMC-EXT są dostępne w dwóch wariantach:

- AMC_IO08: z 8 wejściami i 8 wyjściami
- AMC_IO16: z 16 wejściami i 16 wyjściami
- AMC_4W: z 8 wejściami i 8 wyjściami

Okno dialogowe wyboru zawiera wpis z modułem AMC_IO08. Klikając dwukrotnie pole listy w kolumnie **Typ**, możesz również umieścić kartę AMC_IO16.



Do jednego kontrolera AMC można podłączyć maksymalnie trzy moduły rozszerzeń. Istnieje możliwość łączenia dwóch wariantów. Kliknij przycisk **Dodaj**, aby utworzyć więcej wpisów na liście. Dzięki temu wszystkie pozycje w kolumnach można dostosować.



Karty rozszerzeń są numerowane 1, 2 lub 3 w trakcie tworzenia. Numeracja sygnałów zaczyna się w każdym module od 01. Numer sygnału w połączeniu z numerem karty zapewnia unikatową identyfikację. Sygnały kart rozszerzeń można również zobaczyć w kontrolerze AMC, któremu podlegają.
W efekcie razem z sygnałami wejściowymi i wyjściowymi kontrolera AMC można uzyskać do 56 par sygnałów.
Moduły rozszerzeń można dodawać w razie potrzeby indywidualnie lub w późniejszym terminie, łącznie nie więcej niż 3 na każdy kontroler AMC.

Tworzenie obiektu AMC2 4W-EXT

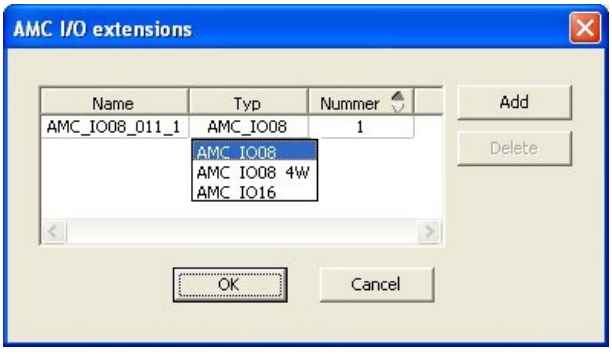
Istnieje możliwość konfigurowania specjalnych modułów rozszerzeń (AMC2 4W-EXT) dla kontrolerów z interfejsami czytników Wiegand (AMC2 4W). Moduły te oferują dodatkowe 4 złącza na czytniki Wiegand, a także po 8 styków wejściowych i wyjściowych. W ten sposób maksymalną liczbę czytników i drzwi możliwych do podłączenia do kontrolera AMC2 4W można podwoić do 8.

Uwaga!
Moduł AMC2 4W-EXT nie może funkcjonować jako samodzielny kontroler, ale tylko jako rozszerzenie kontrolera AMC2-4W. Drzwi są kontrolowane, a decyzje w zakresie kontroli dostępu są podejmowane tylko przez kontroler AMC2 4W.

Karta rozszerzeń AMC2 4W-EXT może być używana tylko w połączeniu z kontrolerem AMC2 4W. Ponieważ moduł ma tylko interfejsy do czytników Wiegand, nie może współpracować z kontrolerem AMC2 4R4.
Podobnie jak moduły rozszerzeń we/wy (AMC2 8I-8O-EXT i AMC2 16I-16O-EXT), kartę AMC2 4W-EXT podłącza się przez interfejs modułów rozszerzeń umieszczony w kontrolerze AMC2 4W. Moduł nie ma własnej pamięci ani wyświetlacza i jest sterowany całkowicie przez kontroler AMC2 4W.
Do każdego kontrolera AMC2-4W można podłączyć jedną kartę rozszerzeń AMC2 4W-EXT i maksymalnie trzy karty rozszerzeń we/wy.
Aby utworzyć obiekt modułu AMC2 4W-EXT w systemie, kliknij prawym przyciskiem myszy żądany nadrzędny kontroler AMC2 4W w eksploratorze, a następnie z menu kontekstowego wybierz kolejno opcje **Nowy obiekt** > **Nowy moduł rozszerzeń**.

Uwaga!
Przycisk ✚ na pasku narzędzi edytora danych urządzenia służy wyłącznie dodawaniu wejść. Karty rozszerzeń można dodawać tylko za pośrednictwem menu kontekstowego.

Pojawi się to samo okno dialogowe wyboru, jak przy tworzeniu rozszerzeń we/wy, z tym że lista urządzeń podłączonych do kontrolera AMC2 4W zawiera dodatkowy element AMC_IO08_4W.



Pozycję listy AMC2 4W można dodać tylko raz, natomiast w przypadku kart rozszerzeń we/wy można ich dodać aż trzy.
Przycisk **Dodaj** dodaje nowe wpisy na liście. W przypadku kontrolera AMC2 4W maksymalna liczba to 4, przy czym czwarta pozycja jest tworzona dla modułu AMC2 4W-EXT.

Karty rozszerzeń są numerowane w kolejności tworzenia 1, 2 i 3. Moduł AMC2 4W-EXT otrzymuje numer 0 (zero). Numeracja sygnałów modułu AMC2 4W-EXT jest kontynuacją numerowania z kontrolera, czyli od 09 do 16, podczas gdy dla każdej karty we/wy numeracja zaczyna się od 01. Sygnały wszystkich modułów rozszerzeń są również wyświetlane na karcie odnośnego kontrolera AMC2 4W.
W efekcie razem z sygnałami wejściowymi i wyjściowymi kontrolera AMC 4W można uzyskać do 64 par sygnałów.

Modyfikowanie i usuwanie modułów rozszerzeń
Pierwsza karta zawiera następujące elementy sterujące do konfigurowania kart rozszerzeń.

Parametr	Możliwe wartości	Opis
Nazwa modułu	Alfanumeryczne z ograniczeniami: 1–16 cyfr	Domyślny identyfikator gwarantuje unikatowość nazwy, ale można go zastąpić ręcznie. Upewnij się, że identyfikator jest niepowtarzalny. W połączeniach sieciowych z serwerami DHCP powinna być używana nazwa sieciowa.
Opis modułu	alfanumeryczne: 0–255 cyfr	Ten tekst jest wyświetlany w gałęzi serwera OPC.
Numer modułu	1 - 3	Numer modułu podłączonego do kontrolera AMC. Tylko pole wyświetlania.
Zasilanie	0 = nieaktywne (pole wyboru jest zaznaczone) 1 = aktywna (pole wyboru jest zaznaczone)	Nadzór nad napięciem zasilającym. W razie awarii napięcia na końcu opóźnienia jest generowany komunikat. Na potrzeby generowania komunikatu funkcja nadzoru zakłada obecności zasilacza USV. 0 = brak nadzoru 1 = nadzór aktywny
Strefa	Wartość domyślna „Wspólna”	To pole tylko do odczytu ma zastosowanie tylko w przypadku, gdy istnieją licencje na strefy i są używane.

Karty Wejścia, Wyjścia i Ustawienia sygnałów mają taki sam układ i funkcjonalność, jak odpowiadające im karty w interfejsie kontrolerów.

Usuwanie modułów rozszerzeń
Moduł rozszerzeń można usunąć tylko wtedy, gdy żaden z jego interfejsów nie jest zajęty. Aby przycisk usuwania  i opcja menu kontekstowego **Usuń obiekt** stały się dostępne, należy najpierw skonfigurować odnośne sygnały na innej karcie.

AMC2 4W-EXT
Ponieważ czytników podłączonych do kart rozszerzeń nie można usuwać ani rekonfigurować pojedynczo, trzeba je usuwać wraz z odpowiadającymi im wejściami. Dopiero wtedy można usunąć sam moduł AMC2 4W-EXT.

14 Niestandardowe pola na dane osobowe

Wstęp

Pola danych personelu można dostosowywać na wiele sposobów:

- Czy mają być **widoczne**, tzn. czy będą wyświetlane w ogóle w aplikacji klienckiej ACE
- Czy są **wymagane**, tzn. czy rekord danych można zapisać bez prawidłowych danych w polu
- Czy znajdujące się w nich wartości muszą być **unikatowe** w systemie
- Jakie typy danych zawierają (tekst, data i godzina, liczba całkowita itp.)
- Gdzie (na której karcie, w której kolumnie i w którym wierszu) w aplikacji klienckiej ACE będą wyświetlane
- Jak duże będą te pola
- Czy i gdzie dane będą wykorzystywane w standardowych raportach

Oczywiście nadal można definiować całkowicie nowe pola danych ze wszystkimi wymienionymi tu atrybutami.

14.1 Wyświetlanie podglądu i edytowanie pól niestandardowych

Ścieżka w oknie dialogowym

- Menu główne > **Konfiguracja** > **Opcje** > **Pola niestandardowe**

Główne okno jest podzielone na dwie karty

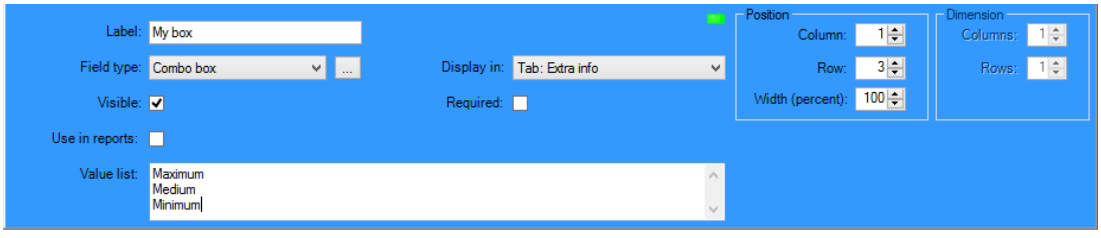
Przegląd Ta karta i jej podkarty (**Adres, Kontakt, Dodatkowe dane osobowe, Dodatkowe dane firmy, Uwagi, Kontrola kart** i **Dodatkowa informacja**) są tylko do odczytu i przedstawiają w przybliżeniu widok WYSIWYG tego, które dane będą wyświetlane na których kartach w aplikacji klienckiej ACE.

Szczegóły Ta karta zawiera listę edytorów, po jednym dla każdego pola danych predefiniowanego lub zdefiniowanego przez użytkownika.

Edytowanie istniejących pól danych

Na karcie **Pola niestandardowe** > **Szczegóły** każde pole danych — predefiniowane lub definiowane przez użytkownika — ma własne okno edytora, w którym można modyfikować jego atrybuty.

Kliknij edytor pola, które chcesz zmodyfikować. Aktywny edytor zostanie podświetlony.



W tabeli poniżej omówiono edytowalne atrybuty niestandardowych pól.

Podpis na etykiecie	Opis
Etykieta	**Etykieta** jest etykietą pola danych wyświetlana w aplikacji klienckiej. Jej wartość można dowolnie zastępować, aby odzwierciedlić terminologię używaną w obiekcie.

Podpis na etykiecie	Opis
Typ pola	**Typ pola** określa typ danych i wskazuje formant okna dialogowego, którego operator będzie używał do wprowadzania wpisów w aplikacji klienckiej. W każdym typie pola działa mechanizm sprawdzanie zgodności wprowadzanych wartości, tak aby zagwarantować poprawność dat, godzin i długości tekstu oraz przestrzeganie ograniczeń liczbowych. – **Pole tekstowe** – Kliknij przycisk wielokropka obok pola, aby określić dozwoloną liczbę znaków. – **Pole wyboru** – **Pole daty** – **Godzina** – **Pole daty i godziny** – **Pole kombi** – Wprowadź poprawne wartości dla pola kombi w polu tekstowym. Oddziel wartości przecinkami lub znakami powrotu karetki. – **Liczbowe dane wejściowe** – W polach pokręteł określ wartości minimalne i maksymalne dla wpisywanych danych liczbowych. – **Kontrola budynku 1** i **Kontrola budynku 2** – Są to specjalne elementy sterujące, którym można tutaj zmienić podpisy (w polu **Etykieta**) oraz połączyć z poleceniami w interfejsie użytkownika aplikacji klienckiej. W ten sposób można udzielać określonym użytkownikom — za pośrednictwem ich kart — pozwolenia na wykonywania specjalnych operacji w obiekcie. Przykładami takich operacji są włączanie reflektorów lub sterowanie specjalnym wyposażeniem.
Widoczne	Wyczyść to pole wyboru, aby zapobiec wyświetlaniu pola danych w aplikacji klienckiej.
Unikalne	Zaznacz to pole wyboru, aby odrzucać zawartość pola danych, która nie jest niepowtarzalna. Na przykład numery personalne powinny być unikatowe u wszystkich pracowników.
	Zielone światło oznacza, że pole danych **nie** jest obecnie używane w bazie danych. Czerwone światło oznacza, że pole danych jest obecnie używane w bazie danych.
Wyświetlaj w	Na tej liście rozwijanej można wybrać kartę aplikacji klienckiej, na której pole danych ma być wyświetlane.
Wymagane	Zaznacz to pole wyboru, aby pole danych było obowiązkowe. Na przykład nazwisko jest wymagane w każdym zestawie danych osobowych. Bez nazwiska nie można zapisać rekordu danych. Zauważ, że edytor nie pozwoli użyć pola wyboru **Widoczne** w celu ustawienia wymaganego pola danych jako niewidocznego. Aby ułatwić sobie korzystanie z aplikacji klienckiej, najlepiej umieścić wszystkie wymagane pola na pierwszej karcie.

Podpis na etykiecie	Opis
Pozycja	Za pomocą pól pokręteł **Kolumna** i **Wiersz** określ położenie pola danych na karcie, której nazwa figuruje na liście rozwijanej **Wyświetlaj w**. Zauważ, że edytor nie pozwoli wybrać pozycji, która jest już używana, ani nałożyć pola na istniejące pola danych. Za pomocą polu pokrętła **Szerokość (procent)** ustaw rozmiar niektórych skalowalnych elementów sterujących, takich jak pola tekstowe. Wartość 100% oznacza, że formant wypełni całe miejsce, który nie jest jeszcze zajęte przez etykietę pola danych.
Wymiary	W polach pokręteł **Kolumna** i **Wiersz** określ liczbę kolumn i wierszy, jakie mają zostać zajęte na karcie, której nazwa figuruje na liście rozwijanej **Wyświetlaj w**. Zauważ, że edytor nie pozwoli wejść na istniejące pola danych.

Tworzenie i edytowanie nowych pól danych

Na karcie **Pola niestandardowe** > **Szczegóły** każde pole danych — predefiniowane lub definiowane przez użytkownika — ma własny panel edytora, w którym można modyfikować jego atrybuty.

Kliknij przycisk **Nowe pole**, aby utworzyć nowe niestandardowe pole z jego własnym edytorem. Aktywny panel edytora zostanie podświetlony.

Edytor ma te same elementy sterujące do edytowania istniejących pól danych, jak w tabeli powyżej, oraz dwie dodatkowe opcje:

Użyj w raportach (pole wyboru)	Zaznacz to pole wyboru, aby nowe pole danych było wyświetlane w standardowych raportach.
Numer sekwencji (pole pokrętła)	Numer kolejny decyduje o kolumnie, którą pole danych będzie zajmować w standardowych raportach.

Uwaga!
Obecnie narzędzia **Projektant identyfikatorów** i **Raporty** obsługują tylko numery kolejne od 1 do 10.

14.2 Reguły dotyczące pól danych

- Umiejscowienie pól danych
  - Każde pole może występować tylko raz na każdej karcie.
  - Każde niestandardowe pole może się znajdować na dowolnej wybieralnej karcie.
  - Pola można przenosić do innych kart, zmieniając wpis na liście rozwijanej **Wyświetlaj w**.
- Etykieta może zawierać dowolny tekst o maksymalnej długości 20 znaków.
- Niestandardowe pola tekstowe mogą zawierać dowolny tekst o maksymalnej długości 2000 znaków.
- Każde pole może można ustawić jako wymagane, ale jego pole wyboru **Widoczne** musi być zaznaczone.

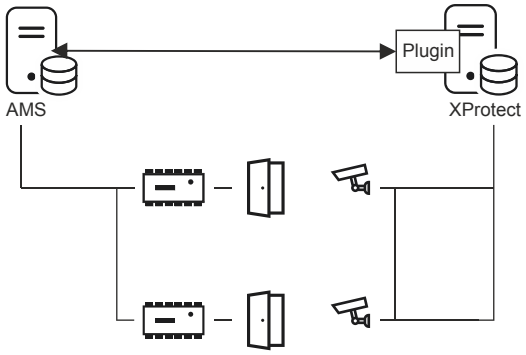
Uwaga!
Ważne zalecenia przed rozpoczęciem użytkowania w środowisku produkcyjnym
Uzgodnij i sfinalizuj wybór typów pól oraz ich wykorzystania, zanim zaczniesz w nich umieszczać dane osób:
Każde pole danych wejściowych jest przypisane do określonego pola bazy danych, dzięki czemu dane mogą być umieszczane zarówno ręcznie, jak i przez generatory raportów. Po zapisaniu rekordów danych z pól niestandardowych w bazie danych nie można już ich przenosić ani zmieniać bez ryzyka utraty danych.

15 Konfigurowanie obsługi systemu AMS w systemie Milestone XProtect

Wstęp

W tym rozdziale opisano, jak w systemie Milestone XProtect skonfigurować używanie funkcji kontroli dostępu zawartych w systemie AMS.

Wtyczka dołączona w systemie AMS, ale instalowana na serwerze systemu XProtect, wysyła zdarzenia i polecenia do systemu AMS, a następnie wyniki przesyła z powrotem do systemu XProtect.



Konfiguracja jest podzielona na 3 etapy, które opisano w sekcjach poniżej:

– Instalowanie publicznego certyfikatu systemu AMS na serwerze systemu XProtect.
– Instalowanie wtyczki systemu AMS na serwerze systemu XProtect.
– Konfigurowanie systemu AMS wewnątrz aplikacji XProtect.

Wymagania wstępne

– System AMS jest zainstalowany i wykupiono na niego licencję.
– Wykupiono licencję na system XProtect i jest on zainstalowany na tym samym lub własnym komputerze.
– Istnieje połączenie sieciowe między oboma systemami.

Instalowanie publicznego certyfikatu systemu AMS na serwerze systemu XProtect

Należy pamiętać, że ta procedura jest wymagana tylko wtedy, gdy serwer AMS działa na innym komputerze.

1. Skopiuj plik certyfikatu z serwera systemu AMS
   `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System \Certificates\Access Management System Internal CA.cer`
   do serwera systemu XProtect.
2. Na serwerze systemu XProtect kliknij dwukrotnie plik certyfikatu.
   Zostanie otwarty Kreator certyfikatów.
3. Kliknij przycisk **Zainstaluj certyfikat...**
   Zostanie otwarty Kreator importu.
4. W ustawieniu **Lokalizacja przechowywania** zaznacz opcję **Komputer lokalny** i kliknij przycisk **Dalej**.
5. Zaznacz opcję **Umieść wszystkie certyfikaty...**
6. Kliknij przycisk **Przeglądaj...**
7. Zaznacz opcję **Zaufane główne urzędy certyfikacji** i kliknij przycisk **OK**.
8. Kliknij przycisk **Dalej>**.

9. Przejrzyj podsumowanie ustawień i kliknij przycisk **Zakończ**.

Instalowanie wtyczki systemu AMS na serwerze systemu XProtect

1. Skopiuj plik instalacyjny
   `AMS XProtect Plugin Setup.exe`
   z nośnika instalacyjnego systemu AMS do serwera systemu XProtect.
2. Uruchom plik na serwerze systemu XProtect.
   Zostanie otwarty Kreator instalacji.
3. W kreatorze instalacji upewnij się, że dodatek AMS XProtect jest zaznaczony do instalacji, i kliknij przycisk **Dalej**.
   Zostanie wyświetlona Umowa licencyjna z użytkownikiem końcowym. Jeśli chcesz kontynuować, kliknij przycisk **Akceptuj**, aby zaakceptować umowę.
4. W kreatorze zostanie wyświetlona domyślna ścieżka instalacji dodatku. Kliknij przycisk **Dalej**, aby zaakceptować ścieżkę domyślną, lub przycisk **Przeglądaj**, aby ją zmienić, a następnie kliknij przycisk **Dalej**.
   Kreator potwierdzi, że zamierza zainstalować wtyczkę AMS XProtect.
5. Kliknij przycisk **Instalacja**.
6. Poczekaj na potwierdzenie ukończenia instalacji i kliknij przycisk **Zakończ**.
7. Uruchom ponownie usługę systemu Windows o nazwie **Milestone XProtect Event Server**.

Konfigurowanie systemu AMS wewnątrz aplikacji XProtect

1. W aplikacji zarządzania systemem XProtect wybierz kolejno opcje **Advanced Configuration** (Zaawansowana konfiguracja) > **Access Control** (Kontrola dostępu).
2. Kliknij prawym przyciskiem myszy pozycję **Access Control** (Kontrola dostępu) i wybierz polecenie **Create new...**
   (Utwórz nowy). Zostanie otwarty kreator dodatku.
3. W kreatorze dodatku wprowadź następujące informacje:
   - **Nazwa**: Opis tej integracji systemów AMS i XProtect, który ją odróżni od innych integracji tego samego systemu XProtect.
   - **Wtyczka integracji**: `AMS - XProtect Plugin` (ta nazwa będzie wyświetlana na liście rozwijanej po pomyślnym zainstalowaniu wtyczki)
   - **Punkt końcowy wykrywania interfejsu API AMS**: `https://<hostname of the AMS system>:44347/`
     , gdzie `44347` jest domyślnym portem wybieranym podczas instalowania interfejsu API systemu AMS.
   - **Nazwa operatora**: Nazwa użytkownika wykorzystywana przez operatora systemu AMS mającego co najmniej uprawnienia do obsługi drzwi, do których zostaną przypisane kamery objęte systemem XProtect.
   - **Hasło operatora**: Hasło tego operatora systemu AMS.
4. Kliknij przycisk **Dalej**
   . Wtyczka systemu AMS nawiąże połączenie ze wskazanym serwerem systemu AMS i pokaże listę wykrytych przez siebie elementów kontroli dostępu (drzwi, jednostki, serwery, zdarzenia, polecenia i stany).
5. Gdy pasek postępu dojdzie do końca, kliknij przycisk **Dalej**
   .Zostanie otwarta strona kreatora **Przypisz kamery**.
6. Aby skojarzyć kamery z drzwiami, przeciągnij kamery z listy **Kamery** do punktów dostępu na liście **Drzwi**.

7. Po zakończeniu kliknij przycisk **Dalej**.
   System XProtect zapisze konfigurację i potwierdzi pomyślne wykonanie tej operacji.

16 Konfigurowanie funkcji zarządzania poziomem zagrożenia

Wstęp

Celem zarządzania poziomem zagrożenia jest skuteczne reagowanie na sytuacje awaryjne poprzez natychmiastowe wprowadzenie zmian w zachowaniu wejść w całym obszarze dotkniętym problemem.

16.1 Pojęcia związane z zarządzaniem poziomem zagrożenia

- **Zagrożenie** jest to sytuacja krytyczna, która wymaga natychmiastowej i równoczesnej reakcji na niektórych lub wszystkich wejściach w systemie kontroli dostępu.
- **Poziom zagrożenia** to reakcja systemu na przewidywaną sytuację. Każdy poziom zagrożenia trzeba starannie skonfigurować, tak aby każde wejście nadzorowane przez kontroler MAC wiedziało, jak reagować.
  Poziomy zagrożenia są w pełni konfigurowalne. Na przykład typowe poziomy wysokiego zagrożenia można skonfigurować w następujący sposób:
  - **Blokada globalna**: może wchodzić tylko personel służb ratowniczych, mający przypisane wysokie poziomy bezpieczeństwa.
  - **Blokada lokalna**: wszystkie drzwi są zablokowane. Prawo wejścia i wyjścia mają tylko osoby z poświadczeniami nie niższymi niż poziom bezpieczeństwa ustawiony w systemie.
  - **Ewakuacja**: wszystkie drzwi wyjściowe są odblokowane. Drzwi kierunkowe (np. bramki obrotowe i śluzy osobowe) pozwalają tylko na wyjście.
- Typowe poziomy niskiego zagrożenia można skonfigurować w następujący sposób:
  - **Wydarzenie sportowe**: drzwi do sektorów sportowych są odblokowane, a do wszystkich innych sektorów zablokowane.
  - **Wywiadówka**: dostępne są tylko wybrane sale lekcyjne i główne wejście.
- **Alert zagrożenia** to alarm wyzwalający poziom zagrożenia. Odpowiednio uprawnione osoby mogą inicjować alert zagrożenia jedną czynnością, np. w interfejsie operatora, sygnałem sprzętowym (np. przyciskiem) lub przykładając specjalną kartę alarmową do dowolnego czytnika.
- **Poziom bezpieczeństwa** to atrybut **profili ochrony** posiadaczy kart i czytników, wyrażony liczbą całkowitą z zakresu 0..100. Każdy poziom zagrożenia ustawia wyznaczone poziomy bezpieczeństwa w czytnikach podlegających konkretnemu głównemu kontrolerowi dostępu (MAC). Następnie te czytniki przyznają dostęp tylko poświadczeniom osób mających poziom bezpieczeństwa nie niższy niż ustawiony w profilu ochrony danego czytnika.
- **Profil ochrony** to zbiór atrybutów, które można przypisać do **typu osoby** (**Profil ochrony osoby**), drzwi (**Profil ochrony drzwi**) lub czytnika (**Profil ochrony czytnika**). Profile ochrony decydują o następujących zachowaniach w zakresie kontroli dostępu:
  - **Poziom bezpieczeństwa** (w rozumieniu opisanym powyżej) dla typu osoby, drzwi lub czytnika.
  - **Odsetek kontroli**. Procentowe prawdopodobieństwo, że ten typ osoby lub czytnika spowoduje zainicjowanie losowej kontroli.

16.2 Przegląd procesu konfiguracji

Funkcja zarządzania poziomem zagrożenia wymaga wykonania następujących czynności konfiguracyjnych, które opisano szczegółowo po tych informacjach ogólnych.

1. W edytorze urządzeń
   - Definiowanie poziomów zagrożenia

- Definiowanie profili ochrony drzwi
- Definiowanie profili ochrony czytników
- Przypisywanie profili ochrony drzwi do wejść

2. W oknach dialogowych danych systemowych
   - Definiowanie profili ochrony osób
   - Przypisywanie profili ochrony osób do typów osób
3. W oknach dialogowych danych osobowych
   - Przypisywanie typów osób do osób
   - Przypisywanie typów osób do grup osób

Po pomyślnym skonfigurowaniu funkcji zarządzania poziomami zagrożeń można z aplikacji Map View monitorować i kontrolować alarmy oraz stany urządzeń objętych kontrolerem MAC. Szczegółowe informacje na ten temat można znaleźć w pomocy ekranowej aplikacji Map View.

16.3 Czynności konfiguracyjne w edytorze urządzeń

W tej sekcji opisano czynności konfiguracyjne, które są wymagane w edytorze urządzeń.

16.3.1 Tworzenie poziomu zagrożenia

W tej sekcji opisano, jak tworzyć poziomy zagrożenia z przeznaczeniem do używania w obiekcie. Można utworzyć maksymalnie 15.

Ścieżka w oknie dialogowym

- **Menu główne** > **Konfiguracja** > **Dane urządzenia**

Procedura

1. Kliknij podkartę **Poziomy zagrożenia**.
   - Pojawi się tabela Poziomy zagrożenia. Może ona zawierać maksymalnie 15 poziomów zagrożenia, każdy z nazwą, opisem i polem wyboru służącym do aktywowania poziomu zagrożenia po jego skonfigurowaniu.
2. Kliknij wiersz o treści **Wprowadź nazwę poziomu zagrożenia**.
3. Wprowadź nazwę, która będzie mieć znaczenie dla operatorów systemu.
4. (Opcjonalnie) W kolumnie **Opis** opisz dokładniej, jak wejścia będą się zachowywać po uaktywnieniu poziomu zagrożenia.
5. Na tym etapie **nie** zaznaczaj pola wyboru **Aktywny**. Najpierw należy wykonać pozostałe czynności konfiguracyjne dla tego poziomu zagrożenia, jak opisano w poniższych sekcjach.
6. Kliknij przycisk  (Zapisz), aby zapisać nowy poziom zagrożenia.

16.3.2 Tworzenie profilu ochrony drzwi

W tej sekcji opisano sposób tworzenia profili ochrony dla różnych typów drzwi oraz definiowania stanu, do którego wszystkie drzwi w tym profilu zostaną przełączone po uaktywnieniu poziomu zagrożenia.

Ścieżka w oknie dialogowym

- **Menu główne** > **Konfiguracja** > **Dane urządzenia**

Wymagania wstępne

- Zdefiniowany co najmniej jeden poziom zagrożenia
- Skonfigurowane co najmniej jedno wejście w drzewie urządzeń

Procedura

1. Kliknij podkartę **Profile ochrony drzwi**.
   – Główne okno dialogowe dzieli się na 2 panele: **Wybór** i **Profil ochrony drzwi** (nazwa domyślna).
2. Kliknij przycisk **Nowy**.
   – Zostanie utworzony nowy profil ochrony drzwi z domyślną nazwą.
   – Tabela **Poziom zagrożenia** znajdująca się w panelu **Profil ochrony drzwi** jest wypełniana poziomami zagrożenia, które zostały już utworzone, oraz dla każdego poziomu wartością **niezdefiniowane** w kolumnie **Stan**.
3. W panelu **Profil ochrony drzwi** wprowadź nazwę typu drzwi, do którego zostanie przypisany ten profil.
   – Nazwa nowego profilu pojawi się w panelu **Wybór**. W razie potrzeby profil można usunąć z konfiguracji, klikając przycisk **Usuń** w tym panelu.
4. (Opcjonalnie) Wprowadź opis profilu, aby pomóc operatorom prawidłowo przypisać profil.
5. Jeśli ten profil ma być przypisany do drzwi kierunkowych (np. do bramki obrotowej lub śluzy osobowej), zaznacz pole wyboru **Bramka obrotowa**.
   – Spowoduje to udostępnienie dodatkowych opcji docelowego stanu drzwi na różnych poziomach zagrożenia, np. opcji zezwalania na wejście, wyjście lub obie te czynności.
6. W tabeli **Poziom zagrożenia** w kolumnie **Stan** dla każdego poziomu zagrożenia dla wszystkich drzwi w profilu wybierz stan docelowy, który ma być ustawiany po zaistnieniu poziomu zagrożenia.
7. Kliknij przycisk  (Zapisz), aby zapisać zmiany.

Powtórz tę procedurę, aby utworzyć tyle profili ochrony drzwi, ile istnieje typów drzwi w konfiguracji. Popularne typy drzwi:
– Główne drzwi publiczne
– Wyjście ewakuacyjne na zewnątrz
– Dostęp do klas
– Publiczny dostęp do areny sportowej

16.3.3 Tworzenie profilu ochrony czytnika

W tej sekcji opisano sposób tworzenia profili ochrony dla różnych typów czytników. Profile ochrony czytników określają następujące atrybuty czytników **dla każdego poziomu zagrożenia**:
– Minimalny poziom bezpieczeństwa wymagany w poświadczeniu, aby przyznać mu dostęp do czytnika.
– Odsetek kontroli, czyli procent posiadaczy kart, którzy będą losowo wybierani do przeprowadzenia dodatkowej kontroli bezpieczeństwa.
   – **Uwaga**: częstotliwość kontroli ustawiona w profilu ochrony czytnika zastępuje częstotliwość kontroli ustawioną w samym czytniku.

Ścieżka w oknie dialogowym

– **Menu główne** > **Konfiguracja** > **Dane urządzenia**

Wymagania wstępne

– Zdefiniowany co najmniej jeden poziom zagrożenia
– Skonfigurowane co najmniej jedno wejście w drzewie urządzeń

Procedura

1. Kliknij podkartę **Profile ochrony czytników**.
   – Główne okno dialogowe dzieli się na 2 panele: **Wybór** i **Profil ochrony czytnika** (nazwa domyślna).
2. Kliknij przycisk **Nowy**.
   – Zostanie utworzony nowy profil ochrony czytnika z domyślną nazwą.
   – Tabela **Poziom zagrożenia** znajdująca się w panelu **Profil ochrony czytnika** jest wypełniana poziomami zagrożenia, które zostały już utworzone, oraz dla każdego poziomu domyślną wartością **0** w kolumnach **Poziom bezpieczeństwa** i **Odsetek kontroli**.
3. W panelu **Profil ochrony czytnika** wprowadź nazwę typu czytnika, do którego zostanie przypisany ten profil.
   – Nazwa nowego profilu pojawi się w panelu **Wybór**. W razie potrzeby profil można usunąć z konfiguracji, klikając przycisk **Usuń** w tym panelu.
4. (Opcjonalnie) Wprowadź opis profilu, aby pomóc operatorom prawidłowo przypisać profil.
5. W tabeli **Poziom zagrożenia** w kolumnie **Poziom bezpieczeństwa** dla każdego poziomu zagrożenia wybierz minimalny poziom bezpieczeństwa (liczba całkowita z zakresu 0..100), który musi posiadać operator, aby mógł użyć czytnika objętego tym profilem po zaistnieniu poziomu zagrożenia.
6. W tabeli **Poziom zagrożenia** w kolumnie **Odsetek kontroli** dla każdego poziomu zagrożenia wybierz procent posiadaczy kart, którzy będą losowo wybierani przez czytnik do przeprowadzenia dodatkowej kontroli bezpieczeństwa po zaistnieniu poziomu zagrożenia.
7. Kliknij przycisk  (Zapisz), aby zapisać zmiany.

16.3.4 Przypisywanie profili ochrony drzwi i czytników do wejść

W tej sekcji opisano sposób przypisywania profili ochrony drzwi i czytników do drzwi i czytników przy określonych wejściach.
Pierwsza podprocedura służy zidentyfikowaniu i wyfiltrowaniu zbioru wejść, którym mają zostać przypisane profile, a druga podprocedura służy wykonaniu przypisań.
Ponadto dla konkretnych wejść można wyświetlić podgląd stanów, poziomów bezpieczeństwa i odsetka kontroli w postaci, w jakiej byłyby one ustawiane przez różne zdefiniowane poziomy zagrożenia.

Ścieżka w oknie dialogowym

– **Menu główne** > **Konfiguracja** > **Dane urządzenia**

Wymagania wstępne

– Zdefiniowany co najmniej jeden poziom zagrożenia
– Skonfigurowane co najmniej jedno wejście w drzewie urządzeń

Procedura

1. W drzewie urządzeń kliknij pozycję **DMS** (katalog główny drzewa urządzeń).
2. W głównym panelu okna dialogowego kliknij kartę **Zarządzanie poziomem zagrożenia**.
   – Główny panel okna dialogowego zawiera kilka podkart.

Podprocedura 1: Wybieranie wejść do przypisania

1. Kliknij podkartę **Wejścia**.
   – Główne okno dialogowe dzieli się na 2 panele: **Warunki filtrowania** oraz tabelę wszystkich wejść, które dotychczas utworzono w systemie.

2. (Opcjonalnie) W panelu **Warunki filtrowania** wprowadź kryteria ograniczające zbiór wejść wyświetlanych w tabeli w dolnej połowie okna dialogowego. Na przykład:
   – Zaznacz lub wyczyść pola wyboru **Czytniki wchodzących**, **Czytniki wychodzących** i/lub **Drzwi** określające, czy mają być wyświetlane te elementy.
   – Wprowadź ciągi znaków, które muszą się znaleźć w nazwach wejść, obszarów, nazwach profili lub nazwach czytników wszystkich wejść wymienionych w tabeli.
   – Zaznacz lub wyczyść pole wyboru określające, czy w tabeli powinny być wyświetlane również drzwi i czytniki, które jeszcze nie zostały skonfigurowane.
3. Kliknij przycisk **Zastosuj filtr**, aby wyfiltrować listę wejść, lub przycisk **Resetuj filtr**, aby przywrócić domyślne wartości formantów filtrowania.

Podprocedura 2: Przypisywanie profili ochrony do wybranych wejść

Warunek wstępny: Wejścia, którym mają zostać przypisane profile, zostały zidentyfikowane i są wyświetlane w tabeli w dolnej połowie okna dialogowego.

Należy pamiętać, że każde wejście składa się zazwyczaj z drzwi lub bariery oraz jednego lub więcej czytników kart. Jednak w niektórych specjalistycznych typach wejść, takich jak **Miejsce (punkt) zbiórki**, te elementy mogą nie występować.

1. W kolumnie **Profil ochrony drzwi lub czytnika** kliknij komórkę odpowiadającą drzwiom lub czytnikowi, któremu chcesz przypisać profil.
2. Z listy rozwijanej komórki wybierz profil ochrony drzwi lub czytnika.

(Opcjonalnie) Wyświetlanie podglądu zachowań drzwi i czytników na różnych poziomach zagrożenia

Kolumny po prawej stronie tabeli są tylko do odczytu. Pokazują one, jaki zostałby ustawiony stan blokady (**Tryb**) oraz parametry **Poziom bezpieczeństwa** i **Odsetek kontroli** dla drzwi i czytników w tabeli, gdyby doszło do aktywowania poziomu zagrożenia wybranego na liście **Wybierz poziom zagrożenia, aby uzyskać szczegółowe informacje**.

Warunek wstępny: Wejścia, dla których ma zostać wyświetlony podgląd, zostały zidentyfikowane i są wyświetlane w tabeli w dolnej połowie okna dialogowego.

- ▸ Na liście **Wybierz poziom zagrożenia, aby uzyskać szczegółowe informacje** zaznacz poziom zagrożenia, którego podgląd chcesz wyświetlić.
- ✓ W tabeli zostanie wyświetlony stan blokady (**Tryb**) dla drzwi oraz wartości parametrów **Poziom bezpieczeństwa** i **Odsetek kontroli** dla czytników takie, jakie zostałyby ustawione po zaistnieniu określonego poziomu zagrożenia.

16.3.5 Przypisywanie poziomu zagrożenia do sygnału sprzętowego

W tej sekcji opisano sposób przypisywania wejściowego sygnału sprzętowego mającego wyzwalać lub anulować alert zagrożenia.

Ścieżka w oknie dialogowym

– **Menu główne** > **Konfiguracja** > **Dane urządzenia**

Wymagania wstępne

– Zdefiniowany co najmniej jeden poziom zagrożenia
– Skonfigurowane co najmniej jedno wejście w drzewie urządzeń

Procedura

1. W drzewie urządzeń zaznacz **wejście** pod kontrolerem AMC, którego sygnały wejściowe chcesz przypisać.
2. W głównym oknie dialogowym kliknij kartę **Terminale**.
   – Zostanie wyświetlona tabela wejść i sygnałów.

3. W wierszu sygnału, który chcesz przypisać, kliknij komórkę w kolumnie **Sygnał wejściowy**.
   – Na liście rozwijanej znajduje się polecenie **Poziom zagrożenia: wyłącz** oraz polecenie **Poziom zagrożenia:** <name> dla każdego zdefiniowanego wcześniej poziomu zagrożenia.
   – Polecenie **Poziom zagrożenia: wyłącz** powoduje anulowanie każdego obecnie aktywnego poziomu zagrożenia.
4. Przypisz polecenia do żądanych sygnałów wejściowych.
5. Kliknij przycisk  (Zapisz), aby zapisać zmiany.

Uwaga!
Ograniczenie dotyczące modelu drzwi 15
Obecnie poziom zagrożenia nie może być inicjowany w modelu drzwi 15 (DIP/DOP).

16.4 Czynności konfiguracyjne w oknach dialogowych danych systemowych

W tej sekcji opisano sposób tworzenia **profili ochrony osób** i przypisywania ich do **typów osób**.

16.4.1 Tworzenie profilu ochrony osoby

Ścieżka w oknie dialogowym

– **Menu główne** > **Dane systemowe** > **Profil ochrony osoby**

Wymagania wstępne

Profile ochrony osób należy wcześniej starannie zaplanować i określić ich specyfikacje, ponieważ będą mieć one istotne konsekwencje dla funkcjonowania systemu w krytycznych sytuacjach.

Procedura

1. Jeśli w oknie dialogowym znajdują się już dane, kliknij przycisk  (Nowy), aby je usunąć.
2. Nadaj nowemu profilowi nazwę w polu tekstowym Nazwa profilu bezpieczeństwa:
3. (Opcjonalnie) Wprowadź opis profilu, aby pomóc operatorom prawidłowo przypisać profil.
4. W polu **Poziom bezpieczeństwa** wprowadź liczbę całkowitą z przedziału od 0 do 100.
   – Przyjmując, że posiadacz karty jest uprawniony do korzystania z wejścia, wartość 100 wystarcza do uzyskania dostępu przez dowolny czytnik, nawet jeśli jego poziom bezpieczeństwa również jest obecnie ustawiony na 100.
   – W przeciwnym razie poziom bezpieczeństwa w profilu ochrony osoby posiadacza karty musi być taki sam lub wyższy niż poziom bezpieczeństwa ustawiony obecnie w czytniku.
5. W polu **Odsetek kontroli** wprowadź liczbę całkowitą z przedziału od 0 do 100.
   – **Uwaga**: Odsetek kontroli w profilu osoby jest drugorzędny w stosunku do profilu czytnika. W poniższej tabeli opisano zależności między odsetkami kontroli w obu profilach.
6. Kliknij przycisk  (Zapisz), aby zapisać zmiany.

Relacja między odsetkami kontroli w profilach ochrony osób i czytników

Odsetek kontroli (%) w profilu ochrony czytnika R	Odsetek kontroli (%) w profilu ochrony osoby P	Osoba wybrana do dodatkowych kontroli bezpieczeństwa?
0	Dowolny	**Nie**
100	Dowolny	**Tak**
1..99	0	**Nie**
1..99	100	**Tak**
1..99	1..99	**Być może** Prawdopodobieństwo = MAX(R,P)

16.4.2 Przypisywanie profilu ochrony osoby do typu osoby

Ścieżka w oknie dialogowym

- **Menu główne** > **Dane systemowe** > **Typ osoby**
- **Aplikacja kliencka ACE** > **Dane systemowe** > **Typ osoby**

Procedura

Uwaga: Z powodów historycznych pojęcie **Identyfikator pracownika** jest synonimem pojęcia **Typ osoby**.

1. W tabeli **Predefiniowane identyfikatory pracowników** lub **Zdefiniowane przez użytkownika identyfikatory pracowników** zaznacz komórkę w kolumnie **Nazwa profilu bezpieczeństwa** odpowiadającej żądanemu typowi osoby.
2. Z listy rozwijanej wybierz profil ochrony osoby.
   - Powtórz tę procedurę dla wszystkich typów osób, które wymagają profilu ochrony osoby.
3. Kliknij przycisk  (Zapisz), aby zapisać dokonane przypisania.

16.5 Czynności konfiguracyjne w oknach dialogowych danych osobowych

W tej sekcji opisano, jak nowe rekordy **osób** tworzone w systemie otrzymują **profile ochrony osoby** za pośrednictwem **typu osoby**.

Ścieżki w oknie dialogowym

- **Menu główne** > **Dane osobowe** > **Osoby**
- **Menu główne** > **Dane osobowe** > **Grupa osób**

Uwaga: Z powodów historycznych pojęcie **Identyfikator pracownika** jest synonimem pojęcia **Typ osoby**.

Procedura

Wszystkie rekordy **osób** tworzone w systemie muszą mieć zdefiniowany **typ osoby**.

1. Upewnij się, że operatorzy systemu przypisują wyłącznie takie **typy osoby**, które zostały połączone z **profilem ochrony osoby** w oknie dialogowym **Menu główne** > **Dane systemowe** > **Typ osoby**.
2. Aby uzyskać szczegółowe informacje na temat łączenia z **profilami ochrony osób** i tworzenia rekordów **osób**, kliknij poniższe łącza.

Patrz

- *Przypisywanie profilu ochrony osoby do typu osoby, Strona 122*
- *Tworzenie danych osobowych i zarządzanie nimi, Strona 124*

17 Tworzenie danych osobowych i zarządzanie nimi

Ścieżka w oknie dialogowym

Menu główne > **Dane osobowe** > <podokna dialogowe>

Ogólna procedura

1. W podoknie dialogowym **Osoby** wprowadź dane identyfikacyjne osoby.
2. W podoknie dialogowym **Karty**:
   - przypisz profile dostępu lub indywidualne uprawnienia dostępu.
   - w razie potrzeby przypisz model czasowy.
   - przypisz kartę,
3. W podoknie dialogowym **Kod PIN**: w razie potrzeby przypisz kod PIN.
4. W podoknie dialogowym **Drukowanie kart identyfikacyjnych** wydrukuj kartę.

W przypadku **gości** procedura wygląda następująco:

- Wprowadź dane osobowe w oknie dialogowym **Goście** wyświetlanym poprzez menu **Goście** i w razie potrzeby przydziel eskortę (opiekuna).

Uwaga!

Kart identyfikacyjnych i uprawnień dostępu nie trzeba przypisywać równocześnie. Dlatego możliwe jest przydzielanie kart identyfikacyjnych osobom nie mającym przypisanych uprawnień dostępu i odwrotnie. Jednak w obu przypadkach osoby te spotkają się z odmową dostępu.

Proces skanowania kart

Kiedy karty są skanowane w czytniku, czytnik przeprowadza szereg kontroli:

- Czy karta jest ważna i zarejestrowana w systemie?
- Czy posiadacz karty ma obecnie zablokowany dostęp (jest wyłączony w systemie)?
- Czy posiadacz karty ma uprawnienie dostępu do przekroczenia wejścia w tę stronę?
- Czy uprawnienie dostępu jest ograniczone pod względem obszarowym lub czasowym? Jeśli tak, to czy czas skanowania mieści się w okresach wyznaczonych przez model czasowy?
- Czy uprawnienie dostępu jest aktywne, tzn. nie **wygasło** ani nie jest **zablokowane** (wyłączone)?
- Czy posiadacz karty podlega modelowi czasowemu? Jeśli tak, czy czas skanowania mieści się w wyznaczonym przedziale?
  Warunek wstępny: Na danym czytniku muszą być włączone kontrole modelu czasowego.
- Czy posiadacz karty znajduje się we właściwym miejscu zgodnie z ustawieniami funkcji Monitorowanie sekwencji dostępu?
  Warunek wstępny: Na czytniku musi być włączona funkcja Monitorowanie sekwencji dostępu.
- Czy dla obszaru docelowego tego czytnika została wyznaczona maksymalna liczba osób i czy została ona już osiągnięta?
- W przypadku używania funkcji Monitorowanie sekwencji dostępu, w tym funkcji zapobiegającej przekazaniu karty niepowołanej osobie: Czy ta karta jest skanowana w czytniku przed upływem czasu blokowania ustawionego przez funkcję zapobiegającą przekazaniu karty niepowołanej osobie (blokady podwójnego wejścia)?
- Czy wymagany jest dodatkowy kod PIN? **Warunek wstępny**: Czytnik jest wyposażony w klawiaturę.
- Jeśli jest aktywny poziom zagrożenia: Czy **profil ochrony osoby** posiadacza karty ma ustawiony **poziom bezpieczeństwa** co najmniej równy poziomowi bezpieczeństwa czytnika objętego tym poziomem zagrożenia?

17.1 Osoby

Dane osób, w przypadku których zostało zaznaczone pole wyboru **Administered globally (Administrowane globalnie)** mogą być edytowane tylko przez operatorów posiadających dodatkowe uprawnienie **Global Administrator (Administrator globalny)**. Jest ono przyznawane w oknie dialogowym operatora w przeglądarce konfiguracji BIS.
Chronione dane:

- Wszystkie dane w oknie dialogowym **Persons (Osoby)** z wyjątkiem karty **Remarks (Uwagi)** oraz dodatkowych, specjalnie zdefiniowanych pól z informacjami na karcie **Extra Info (Dodatkowa informacja)**.
- Wszystkie dane w oknie dialogowym **Cards (Karty)**.
- Wszystkie dane w oknie dialogowym **PIN Code (Kod PIN)**.

Pozostałe dane tych osób mogą być edytowane przez każdego operatora.

W poniższej tabeli znajdują się główne rodzaje danych, które mogą być rejestrowane. Prawie wszystkie pola są opcjonalne. Pola obowiązkowe są wyraźnie oznaczone podkreślonymi etykietami w interfejsie użytkownika.

Karta	Nazwa pola
Nagłówek okna dialogowego	Nazwa
	Imię
	Nazwisko panieńskie
	Numer personalny
	Data urodzenia
	Identyfikator pracownika (inaczej „Typ osoby”)
	Płeć
	Firma
	Tytuł
	Nr karty identyfikacyjnej
	Nr prawa jazdy
Adres	Kod pocztowy
	Street, no. (Ulica/nr)
	Country, state (Kraj, województwo)
	Nationality (Narodowość)
Contact (Kontakt)	Phone other (Telefon inny)
	Telefon firmy
	Nr faksu firmy
	Telefon komórkowy
	Telefon
	E-mail

	Web page address (Adres strony sieci web)
Additional Person Data (Dodatkowe dane osobowe)	Patronymic (Imię odojcowskie)
	Birthplace (Miejsce urodzenia)
	Marital status (Stan cywilny)
	Official identity card (Służbowa karta identyfikacyjna)
	Identity card no. (Nr karty identyfikacyjnej)
	Ważne do
	Wzrost
Additional Company Data (Dodatkowe dane firmy)	Department (Dział)
	Location (Lokalizacja)
	Cost center (Centrum kosztów)
	Job title (Stanowisko)
	Attendant (Parkingowy)
	Reason for visit (Powód wizyty)
	Rermarks (Uwagi)
Rermarks (Uwagi)	(Dostępne jest pole, w którym można wpisywać notatki i uwagi na temat danej osoby).
Extra Info (Dodatkowa informacja)	10 pól definiowanych przez użytkownika
Podpis	Rejestrowanie, ponowne rejestrowanie i usuwanie podpisów
Odciski palców	Rejestrowanie, ponowne rejestrowanie, usuwanie i testowanie odcisków palców jako poświadczeń biometrycznych. Przypisywanie odcisków palców do sygnału zagrożenia.

17.1.1 Opcje kontroli kart/budynków

17.1.2 Dodatkowa informacja: Rejestrowanie informacji zdefiniowanych przez użytkownika

Karta **Dodatkowa informacja** służy do definiowania dodatkowych pól, których nie ma na innych kartach. W przypadku niezdefiniowania dodatkowych pól karta pozostaje pusta.

17.1.3 Rejestrowanie podpisów

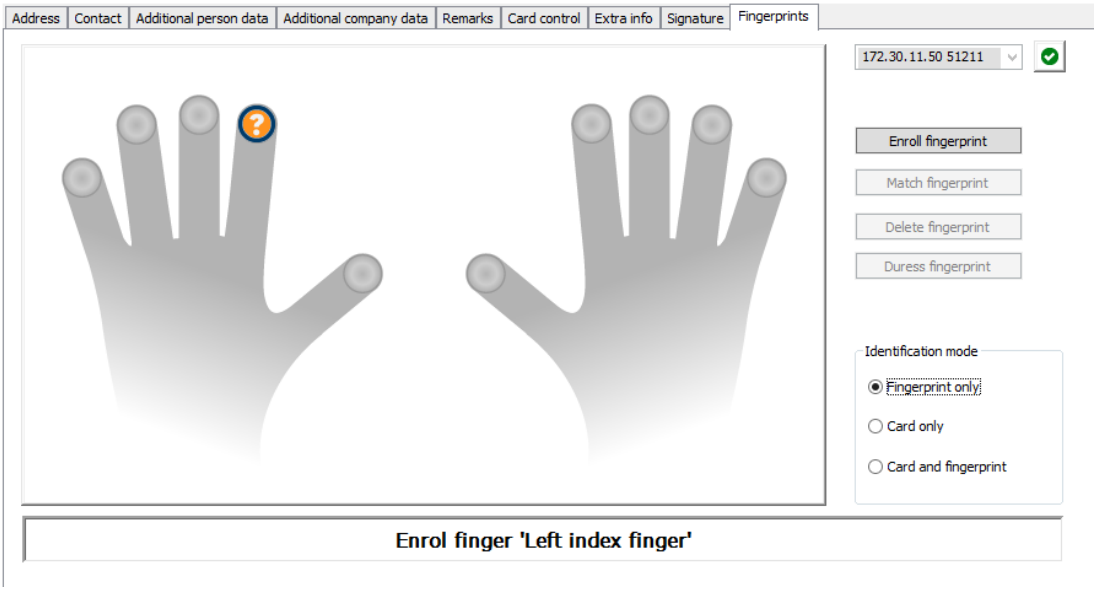
Urządzenie firmy Signotec do przechwytywania podpisów musi być podłączone i skonfigurowane w systemie. W razie wątpliwości należy skontaktować się z administratorem systemu.

1. Kliknij kartę **Podpis**.
2. Kliknij przycisk **Zarejestruj podpis**, aby zarejestrować nowy podpis.
3. Złóż podpis bezpośrednio na płytce za pomocą specjalnego rysika.
4. Kliknij przycisk zaznaczenia na płytce, aby potwierdzić.
   Nowy podpis zostanie wyświetlony na ekranie (ewentualnie kliknij podpis, aby powiększyć widok).

Powiązane procedury:

– Kliknij przycisk **Zarejestruj podpis**, aby zastąpić istniejący podpis.
– Kliknij przycisk **Usuń podpis**, aby usunąć dotychczasowy podpis.

17.1.4 Rejestracja odcisku palca



Wymagania wstępne

– Aby umożliwić biometryczną kontrolę dostępu, co najmniej jeden czytnik linii papilarnych musi być skonfigurowany przy wejściach.
– WAŻNE: Te czytniki okresowo otrzymują z serwerów i przechowują dane kart i odcisków palców. Ustawienia danego czytnika ostatecznie decydują, które poświadczenia są akceptowane. Zastępują one wszelkie ustawienia dokonane tutaj dla danej osoby.
– Aby używać odcisków palców jako weryfikacji (lub alternatywy dla) uwierzytelniania na podstawie karty, wszyscy posiadacze kart muszą mieć zeskanowane odciski palców.
– Rejestrowana osoba znajduje się przed czytnikiem linii papilarnych, który jest podłączony i skonfigurowany dla stacji roboczej.
– Będąc operatorem, komunikujesz się bezpośrednio z rejestrowaną osobą, której odciski palca chcesz pobrać i wykorzystywać jako dane biometryczne służące do uzyskania dostępu.
– Użytkownik wie, jak ułożyć palec na używanym czytniku w celu dokładnego pobrania odcisku.

Procedura rejestracji odcisku palca w celu uzyskania dostępu

1. Przejdź do okna dialogowego odcisków palców: **Dane osobowe** > **Osoby** > karta: **Odciski palców** i utwórz lub znajdź rejestrowaną osobę w bazie danych.
2. Zapytaj rejestrowaną osobę, którego palca będzie chciała używać do uwierzytelnienia się w czytniku.
3. Wybierz odpowiedni palec z rysunku ręki.
   Wynik: koniec palca jest oznaczony znakiem zapytania.
4. Kliknij przycisk **Enroll fingerprint (Zarejestruj odcisk palca)**.

5. Poinstruuj rejestrowaną osobę, jak ułożyć palec w celu poprawnego odczytu danych biometrycznych.
   Przykładowe instrukcje można przeczytać w oknie dialogowym poniżej rysunku rąk, ale procedury mogą się nieznacznie różnić w zależności od czytnika.
6. Jeśli odcisk palca zostanie pomyślnie zarejestrowany, system wyświetli okno z potwierdzeniem.
7. Wybierz **Tryb identyfikacji** — określa, jakich poświadczeń czytnik linii papilarnych będzie wymagać, gdy zarejestrowana osoba zażąda dostępu. Należy pamiętać, że ustawiony tu tryb identyfikacji będzie działać tylko wtedy, gdy wybrano parametr czytnika **Weryfikacja zależna od osoby**.
   Dostępne są następujące opcje:
   - **Tylko odcisk palca** — używany jest tylko skaner odcisku palca w czytniku
   - **Tylko karta** — używany jest tylko skaner karty w czytniku
   - **Karta i odcisk palca** — używane są oba skanery w czytniku. Zarejestrowana osoba, aby uzyskać dostęp, musi przedstawić na czytniku zarówno wybrany palec, jak i kartę.
8. Kliknij przycisk  (Zapisz), aby zapisać odcisk palca i tryb identyfikacji rejestrowanej osoby.

Uwaga!
Ustawienia czytnika zastępują ustawienia osoby
Należy pamiętać, że tryb identyfikacji wybrany w oknie dialogowym Odcisk palca działa jedynie jeśli sam czytnik linii papilarnych jest skonfigurowany z opcją **Weryfikacja zależna od osoby** w edytorze urządzeń. W razie wątpliwości należy skontaktować się z administratorem systemu.

Procedura rejestracji odcisku palca na potrzeby sygnału zagrożenia
Wymagania wstępne:
- Został już zarejestrowany i zapisany co najmniej jeden odcisk palca rejestrowanej osoby.
- Czytnik odcisku palca jest online. W trybie offline czytnik nie może wysłać sygnału zagrożenia do systemu.

1. Poproś rejestrowaną osobę, aby wybrała palec, którego będzie używać do wywołania sygnału zagrożenia, tj., w razie gdyby ktoś nieupoważniony zmusił ją do użycia czytnika odcisków palców.
2. Wykonaj dla drugiego palca procedurę rejestracji odcisku palca opisaną powyżej.
3. Po pomyślnym zarejestrowaniu drugiego odcisku palca, wybierz go na rysunku dłoni i kliknij przycisk **Palec sygnału zagrożenia**.
   Wybrany palec sygnału zagrożenia jest oznaczony wykrzyknikiem na rysunku dłoni.

Jeśli zarejestrowana osoba korzysta z czytnika odcisku palca pod przymusem, używając w takim wypadku wybranego palca, i czytnik nie jest offline, to system wyśle operatorowi tę informację za pomocą wyskakującego okienka.

Procedura testowania zapisanych odcisków palców

1. Na rysunku dłoni wybierz odcisk palca, który chcesz przetestować.
2. Poinstruuj zarejestrowaną osobę, aby umieściła palec na czytniku.

3. Kliknij przycisk **Match fingerprint (Dopasuj odcisk palca)**.
   Wynik: wyskakujące okienko będzie zawierało informację, czy zapisany odcisk palca odpowiada odciskowi podanemu w czytniku. Pamiętaj, że może być konieczne powtórzenie tej procedury, aby ograniczyć prawdopodobieństwo występowania fałszywych alarmów.

Procedura usuwania zapisanych odcisków palców

1. Na rysunku dłoni wybierz odcisk palca, który chcesz usunąć.
2. Klika przycisk **Delete fingerprint (Usuń odcisk palca)**.
3. Zaczekaj na potwierdzenie usunięcia.

17.2 Firmy

– To okno dialogowe służy do tworzenia nowych firm oraz modyfikowania i usuwania istniejących już danych firmy.
– Nazwę i krótką nazwę firmy trzeba obowiązkowo wprowadzić. Krótka nazwa musi być unikatowa.
– Jeśli podanie firmy w oknie dialogowym **Osoby** jest obowiązkowe, najpierw utwórz firmę, a dopiero potem utwórz dla niej zestawy danych osobowych.
– Nie można usuwać firm z systemu, jeśli nadal mają przypisane zestawy danych osobowych.

17.3 Karty: Tworzenie oraz przypisywanie poświadczeń i uprawnień

To okno dialogowe służy do przypisywania **kart**, **uprawnień dostępu** lub pakietów uprawnień dostępu nazywanych **profilami dostępu** do zestawów danych osobowych.
Uprawnienia i profile dostępu przypisuje się do osób, a nie do kart.
Nowe karty przypisywane do osoby otrzymują uprawnienia dostępu już przypisane tej osobie.

Uwaga: Używanie profili dostępu do łączenia uprawnień w pakiety
Dla spójności i wygody uprawnienia dostępu nie są przypisywane pojedynczo, ale zazwyczaj łączone w **profile dostępu** i przypisywane w ten sposób.
– Menu główne: **> Dane systemowe** > **Profile dostępu**

Lista kart
W oknie dialogowym Karty wyświetlana jest lista kart należących do wybranej osoby. Niektóre z atrybutów widocznych na tej liście:
– Typ użycia karty.
– Flaga wskazująca, czy karty można używać w skonfigurowanym systemie blokowania offline.
– Nie ma znaczenia, czy karta została zablokowana po kilkukrotnym podanku błędnego kodu PIN. Ten stan jest szczególnie zaznaczony.
– Data utworzenia karty
– Data ważności (pobrania) karty.
  Uwaga: jeśli używany jest mechaniczny czytnik kart, może on fizycznie zatrzymać wygasłą kartę. W każdym innym przypadku karta jest po prostu unieważniana.
– Data ostatniego wydrukowania karty oraz liczba wydrukowanych kart.
– Szczegóły danych kodowania.

Opcja **Administrowane globalnie**
Dane osób, które mają wybrane ustawienie **Administrowane globalnie** (pole wyboru obok ramki ze zdjęciem), mogą być edytowane przez operatorów posiadających dodatkowe uprawnienie **Administrator globalny**.
Poniższe dane są tylko do odczytu dla operatorów, którzy nie mają tego prawa:
– Wszystkie dane w oknie dialogowym **Osoby** z wyjątkiem kart **Uwagi i Dodatkowa informacja** oraz pól niestandardowych.
– Wszystkie dane w oknie dialogowym **Karty**.
– Wszystkie dane w oknie dialogowym **Kod PIN**.

To uprawnienie **Administrator globalny** można przypisać w następującym polu wyboru:
– Menu główne: **Konfiguracja** > **Operatorzy i stacje robocze** > **Uprawnienia użytkownika** > pole wyboru: **Administrator globalny**.

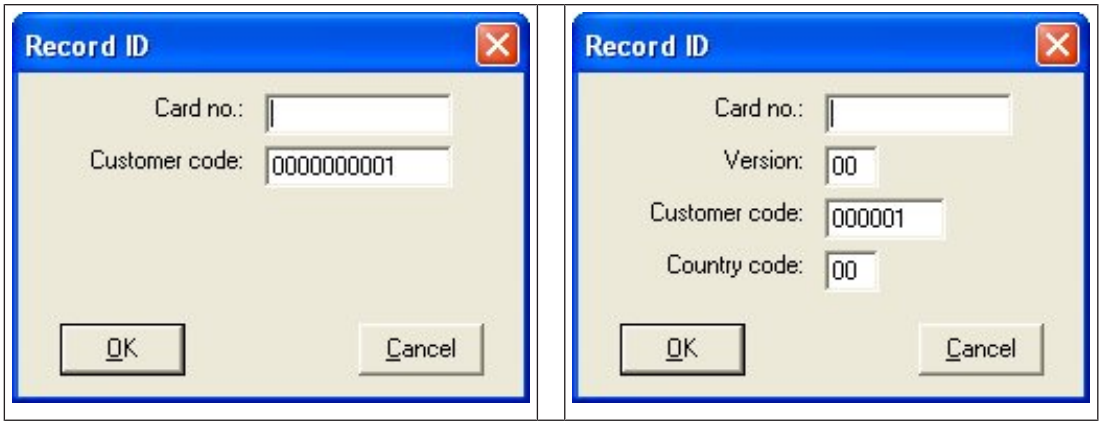
17.3.1 Przypisywanie kart do osób

Wstęp
Osoby objęte kontrolą dostępu muszą mieć kartę lub inne elektroniczne narzędzie do poświadczania tożsamości przypisane do danego posiadacza w oknie dialogowym Karty. Numery kart mogą być przypisywane ręcznie lub automatycznie za pomocą czytnika rejestracji.

Ścieżka w oknie dialogowym
Menu główne > **Dane osobowe** > **Karty**

Wymaganie wstępne
Załadowano zestaw danych osobowych, któremu ma zostać przypisana karta w nagłówku okna dialogowego **Karty**.

Ręczne wprowadzanie danych karty
Przycisk **Karta rejestrująca** służy do przydzielania karty identyfikacyjnej osobie. Po jego kliknięciu pojawia się maska okna dialogowego **Rejestracja identyfikatora**. Zostanie wyświetlone jedno z dwóch okien dialogowych wprowadzania danych zależnie od wybranego typu karty oraz używanych kontrolerów i czytników.



Numer wydrukowany na karcie identyfikacyjnej wpisuje się ręcznie — numery kart są automatycznie uzupełniane o zera, aby zawsze zawierały 12 cyfr. W przypadku niektórych systemów po utracie karty identyfikacyjnej nie jest przypisywany nowy numer. Zamiast tego

wystawiana jest karta o tym samym numerze identyfikacyjnym, ale o wyższym numerze wersji. Kody kraju i klienta są podawane przez wytwórcę, a należy je wprowadzić w pliku rejestracyjnym systemu.
Jeśli karta nie jest jeszcze używana w systemie, jej numer zostanie przypisany osobie. Powodzenie tej operacji potwierdza odpowiedni komunikat.

Korzystanie z czytnika rejestracji

Wymaganie wstępne

Czytnik rejestracji został podłączony do stacji roboczej, na której pracujesz.

Procedura rejestracji

1. Kliknij przycisk po prawej stronie przycisku **Karta rejestrująca** i wybierz skonfigurowany czytnik rejestracji.
2. Kliknij przycisk **Karta rejestrująca** i postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.
3. Zależnie od typu czytnika można wprowadzić szczegóły karty w oknie dialogowym lub odczytać dane z karty, przykładając ją do czytnika.

Procedura zmiany kart

1. Zaznacz kartę na liście.
2. Kliknij przycisk **Zmień kartę**.
3. Zmodyfikuj dane karty w wyskakującym oknie i kliknij przycisk OK, aby je zapisać.

Usuwanie kart

1. Zaznacz kartę na liście.
2. Kliknij przycisk **Usuń kartę**, aby usunąć przypisanie danej osoby do karty.

Uwaga: W przypadku usunięcia ostatniej karty stan posiadacza zmieni się na **Niezarejestrowany** (czerwona etykieta na pasku zadań obok pozycji **Zarejestrowany**). Odtąd ta osoba nie będzie już poddawana kontroli dostępu.

17.3.2 Karta Uprawnienia

Przypisywanie uprawnień w pakiecie jako profili dostępu

Najwygodniejszym i najbardziej elastycznym sposobem przydzielania uprawnień posiadaczom kart jest najpierw zebranie uprawnień ich w profile dostępu, a następnie przypisanie całego profilu.

– Opis tworzenia profili dostępu znajduje się w rozdziale *Tworzenie profili dostępu, Strona 145*.
– Aby przypisać profil dostępu posiadaczowi karty, wybierz zdefiniowany profil z listy **Profil dostępu:**.

Bezpośrednie przypisywanie uprawnień dostępu

Na karcie **Uprawnienia**:
Wszystkie uprawnienia dostępu, które zostały już przypisane danej osobie, pojawiają się na liście po lewej stronie.
Wszystkie uprawnienia dostępu, które są dostępne do przypisania, pojawiają się na liście po prawej stronie.
Zaznacz elementy, a następnie kliknij przyciski między listami, aby przenieść elementy z jednej listy do drugiej.

< przypisuje wybrany element.

 cofa przypisanie wybranego elementu.

 przypisuje wszystkie dostępne elementy.

 cofa przypisanie wszystkich przypisanych elementów.

Opcja: **Zachowaj przypisane uprawnienia**
Efekt przypisania profilu dostępu do osoby zależy od stanu pola wyboru **Zachowaj przypisane uprawnienia**:

– Jeśli nie jest ono zaznaczone, wszelkie dokonane wcześniej wybory i wszystkie przypisane już uprawnienia dostępu zostają **zastąpione** po przypisaniu profilu.
– Jeśli jest ono zaznaczone, uprawnienia z profilu zostają **dodane** do przyznanych już uprawnień.

Ograniczanie czasu obowiązywania uprawnień
Za pomocą pól daty **Ważne od:** i **Ważne do:** można godziny czas rozpoczęcia i zakończenia obowiązywania autoryzacji oraz profili. Jeśli nie ustawisz żadnych wartości, autoryzacja wchodzi w życie natychmiast i obowiązuje bezterminowo.

Kliknij przycisk  , aby otworzyć okno dialogowe pozwalające określić czas obowiązywania poszczególnych uprawnień.

Wyświetlanie wejść objętych autoryzacją
Kliknij prawym przyciskiem myszy uprawnienie na dowolnej liście, a zostanie wyświetlona lista wejść, z którymi autoryzacja jest powiązana.

17.3.3 Karta Inne dane: Zwolnienia i uprawnienia specjalne

Przypisywanie modelu czasowego:
Korzystając z pola listy **Model czasowy**, można wyznaczyć posiadaczowi karty godziny dostępu, czyli okres, w którym uprawnienia zapewnią mu dostęp.

Wykluczanie osób z losowej kontroli
Za pomocą pola wyboru **Excluded from random screening (Wykluczono z losowej kontroli)** można wykluczyć te osoby z losowych kontroli przy wejściu i wyjściu.

Wykluczanie osób z kontroli kodu PIN
Za pomocą pola wyboru **Disable PIN code check (Wyłącz sprawdzanie kodów PIN)** można zwolnić wybrane osoby z obowiązku podawania kodu PIN poza godzinami pracy.

Uwaga!
Wykluczenie z kontroli kodu PIN wpływa na cały system.
Na przykład ze względu na to, że kody PIN tych osób nie są sprawdzane, nie będą one mogły uzbrajać ani rozbrajać alarmów przy wejściach, w których zastosowano model drzwi 10.

Rozszerzony czas otwierania drzwi
Zaznaczenie pola wyboru **Extended door opening time (Rozszerzony czas otwierania drzwi)** daje osobom niepełnosprawnym trzy razy więcej czasu na przedostanie się przez drzwi zanim pojawi się komunikat **Door open too long (Drzwi są otwarte zbyt długo)**.
Monitoring trasy

Trasa oznacza ścisłą sekwencję czytników zdefiniowaną w menu aplikacji klienckiej: okno dialogowe **Monitoring trasy** > **Definiowanie tras**.
Aby przypisać trasę do posiadacza karty, należy zaznaczyć pole wyboru **Monitoring trasy**, a następnie wybrać zdefiniowaną trasę z listy rozwijanej. Jeśli nie zdefiniowano żadnej trasy, pole wyboru będzie nieaktywne.
Gdy **Tour (Trasa)** jest przypisana do posiadacza karty, staje się aktywna po zeskanowaniu przez niego karty w czytniku, który jest pierwszy w sekwencji. Następnie musi on użyć wszystkich kolejnych czytników w sekwencji aż do końca trasy. Zazwyczaj służy to do wymuszenia ścisłej sekwencji dostępu w środowiskach sterylnych lub wymagających najwyższego stopnia bezpieczeństwa.
Pozwolenie na odblokowanie drzwi
Zaznacz to pole wyboru, aby umożliwić posiadaczowi karty odblokowywanie drzwi przez dłuższy czas. Patrz **Tryb Biuro**.

17.3.4 Osoby upoważnione do ustawiania trybu Biuro

Wstęp
Tryb biuro oznacza zawieszenie kontroli dostępu przy wejściu w godzinach pracy biura lub danego zakładu. Wejście pozostaną otwarte w tych godzinach, aby zezwalały na nieutrudniony dostęp publiczny. Poza tymi godzinami obowiązuje Tryb normalny, oznacza to, że dostęp jest przyznawany tylko osobom, których ważne uprawnienia zostaną rozpoznane w czytniku.
Tryb Biuro jest typowo wymagany w placówkach handlowych, edukacyjnych i medycznych.

Wymagania wstępne
Dla trybu Biuro muszą być spełnione następujące warunki:
W konfiguracji (w drzewie urządzeń)
– Musi być skonfigurowane jedno lub więcej wejść z przedłużonym okresem odblokowania.
– Przy wejściu należy użyć co najmniej jeden czytnik z klawiaturą.

W aplikacji klienckiej (okno dialogowe Osoby)
– Jeden lub więcej użytkowników musi mieć uprawnienia do włączenia i wyłączenia trybu biurowego.
– Ich karty muszą być ważne i muszą umożliwiać dostęp poza godzinami pracy w trybie biurowym.

Procedury autoryzacji osoby upoważnionej do włączania trybu Biuro
Procedura w przypadku poszczególnych posiadaczy kart
1. Przejdź do opcji: **Dane osobowe** > **Karty** > karta: **Inne dane**, aby utworzyć lub znaleźć podanego posiadacza karty w bazie danych.
2. Zaznacz pole wyboru **Pozwolenie na odblokowanie drzwi**.
3. Kliknij ikonę dyskietki  , aby zapisać dane posiadacza karty.

Procedura w przypadku grup użytkowników
1. Przejdź do opcji: **Dane osobowe** > **Grupa osób** i użyj kryteriów filtrowania, aby utworzyć listę posiadaczy kart w oknie Lista.
2. Z listy rozwijanej **Pole do zmiany** wybierz **Odblokowanie drzwi**
3. Zaznacz pole wyboru **Odblokowanie drzwi**.
4. Kliknij przycisk **Zastosuj zmiany**, aby zapisać dane tych posiadaczy kart.

Poinstruuj posiadacza karty, jak włączyć i wyłączyć tryb Biuro

Aby włączyć lub wyłączyć tryb Biuro na wejściu, posiadacz karty musi nacisnąć cyfrę 3na klawiaturze, a następnie wczytać na czytniku specjalną kartę z uprawnieniami.

Wejście pozostanie otwarte do czasu, aż upoważniony posiadacz karty ponownie naciśnie na klawiaturze 3i wczyta kartę.

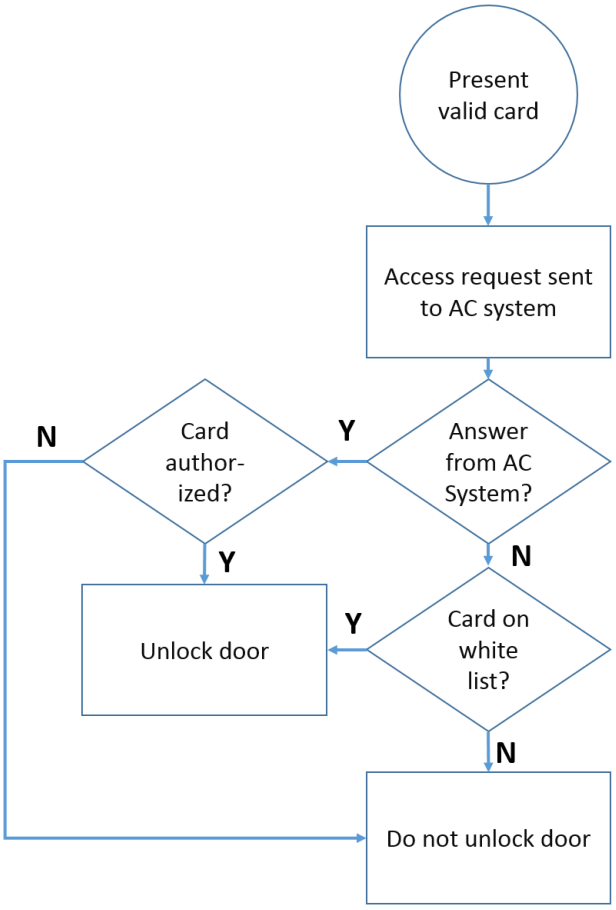
Należy pamiętać, że ochrona może w taki sam sposób wyłączyć tryb Biuro bez specjalnego pozwolenia, używając karty pracownika ochrony.

17.3.5 Karta SmartIntego

System blokowania SmartIntego

Wstęp

Czytnik kart SmartIntego próbuje najpierw zezwolić na dostęp za pośrednictwem głównego systemu kontroli dostępu. Jeśli połączenie nie powiedzie się, czytnik przeszukuje zapisaną w nim „białą listę”, poszukując numer tej karty.



Uprawnienia dostępu systemu SmartIntego są przydzielane w taki sam sposób jak wszystkie inne uprawnienia dostępu.

Wymagania wstępne

– System blokowania SimonsVoss SmartIntego został skonfigurowany w ramach istniejącego systemu kontroli dostępu. Zobacz instrukcje w podręczniku konfiguracji.
– Posiadacze kart używają kart MIFARE Classic lub MIFARE Desfire.
System SmartIntego używa numeru seryjnego karty (CSN).

Procedura przypisywania

Następująca procedura opisuje sposób dodawania numeru karty do białej listy systemu SmartIntego dodatkowo do wszystkich uprawnień przypisanych już przez główny system kontroli dostępu.

Białe listy są zapisywane lokalnie przy drzwiach systemu SmartIntego, dzięki czemu czytnik może udzielić dostępu posiadaczowi karty z numerem zapisanym na białej liści również wtedy, gdy połączenie ze sterownikiem MAC jest przerwane.

Dodania i usunięcia z białej listy są transmitowane do systemu SmartIntego po zapisaniu danych posiadacza karty i przywróceniu połączenia.

1. W głównym menu aplikacji klienckiej AMS wybierz kolejno opcje **Dane osobowe** > **Karty**.
2. Wybierz osobę, której chcesz udzielić uprawnień SmartIntego.
3. Kliknij kartę **SmartIntego.**
4. Dokonaj przypisań:
   - Wszystkie uprawnienia dostępu, które zostały już przypisane danej osobie, pojawiają się na liście po lewej stronie.
   - Wszystkie uprawnienia dostępu, które są dostępne do przypisania, pojawiają się na liście po prawej stronie.

Zaznacz elementy, a następnie kliknij przyciski między listami, aby przenieść elementy z jednej listy do drugiej.

 przypisuje wybrany element.

 cofa przypisanie wybranego elementu.

 przypisuje wszystkie dostępne elementy.

 cofa przypisanie wszystkich przypisanych elementów.

17.3.6 Tworzenie karty alarmowej

W tej sekcji opisano sposób tworzenia karty alarmowej, której można użyć do wyzwalania poziomu zagrożenia.

Wstęp

Karta alarmowa to karta, która po przyłożeniu do czytnika inicjuje konkretny poziom zagrożenia. Poziomu zagrożenia nie można anulować kartą alarmową, a jedynie w oprogramowaniu kontroli dostępu.

Wymagania wstępne

- W systemie jest zainstalowany czytnik dialogowy umożliwiający zapisywanie danych na karcie.
- W systemie zdefiniowano co najmniej jeden poziom zagrożenia.

Ścieżka w oknie dialogowym

Menu główne > **Dane osobowe** > **Karty** > **Karta alarmowa**

Procedura

1. Wczytaj rekordu osoby, której zostanie przypisana karta alarmowa.
2. Na karcie Karta alarmowa kliknij przycisk Karta rejestrująca.
   - Pojawi się wyskakujące okno **Wybierz poziom zagrożenia**.
3. W wyskakującym oknie wybierz żądany poziom zagrożenia i kliknij przycisk **OK**.
   - Pojawi się wyskakujące okno **Rejestrowanie identyfikatora karty identyfikacyjnej**.

4. Wprowadź typowe dane karty odpowiednie dla instalacji w obiekcie, a następnie kliknij przycisk **OK**.
   – Zarejestrowana karta alarmowa pojawi się na liście na karcie **Karta alarmowa**.

17.4 Tymczasowe karty

Karta tymczasowa jest tymczasowym zamiennikiem karty, która została zgubiona przez zwykłego posiadacza karty. Jest to duplikat zawierający wszystkie autoryzacje i ograniczenia oryginału, w tym prawa do przechodzenia przez drzwi autonomiczne.
Aby zapobiec nadużyciom, system może opcjonalnie zablokować jedną lub wszystkie inne karty posiadacza karty na czas określony lub do momentu odblokowania ręcznego.
W efekcie karty tymczasowe **nie nadają się** na karty dla gości.

Wymagania wstępne
– Operator ma dostęp do czytnika rejestracji skonfigurowanego na jego stacji roboczej.
– Jest dostępna odpowiednia fizyczna karta do rejestracji w systemie w roli karty tymczasowej.
– Odbiorca karty tymczasowej ma już co najmniej jedną inną kartę.

Menu główne > **Dane osobowe** > **Karty**

Procedura: Przydzielanie tymczasowych kart
1. Załaduj wymagany zestaw danych osobowych do okna dialogowego **Karty**.
2. Na liście kart zaznacz kartę lub karty, które wymagają tymczasowych zamienników.
3. Kliknij przycisk **Zmień kartę**.
4. W wyskakującym oknie **Zmień kartę** zaznacz opcję **Tymczasowa karta**.
5. Na liście **Okres** zaznacz jedną z opcji:
   – **Dziś**
   – **Dziś i jutro**
   – **Wprowadź liczbę dni**
6. W przypadku ostatniej opcji wpisz w polu liczbę całkowitą określającą liczbę dni.
   Pamiętaj, że we wszystkich trzech przypadkach **okres** zawsze kończy się o północy danego dnia.
7. W razie potrzeby zaznacz pole wyboru **Dezaktywuj wszystkie karty teraz**.
   – Po wybraniu tej opcji wszystkie karty należące do tego posiadacza zostaną zablokowane.
   – Jeśli pole wyboru jest wyczyszczone, będzie blokowana tylko karta wybrana powyżej.
8. W razie potrzeby zaznacz pole wyboru **Aktywuj karty automatycznie po czasie**.
   – Zablokowane karty zostaną odblokowane automatycznie po upływie **okresu** określonego powyżej.
9. Umieść tymczasową kartę w czytniku rejestracji.
10. Kliknij przycisk **OK**
    .Identyfikator karty zostanie rejestrowany przez czytnik rejestracji.
    – Na liście kart tymczasowa karta będzie wyświetlana jako aktywna ✔, wraz z okresem ważności i danymi kodowymi.
    – Pozostałe karty będą wyświetlane jako zablokowane ✘, w zależności od ustawienia dokonanego powyżej: **Dezaktywuj wszystkie karty teraz**.
11. (Opcjonalnie) Na liście kart kliknij dla karty tymczasowej kolumnę **Data zbierania** i ustaw datę jej odebrania od posiadacza karty.
    Wartość domyślna to **Nigdy**.

Procedura: Usuwanie kart tymczasowych

Po znalezieniu zgubionej oryginalnej karty usuń tymczasową kartę w następujący sposób:

1. Załaduj wymagany zestaw danych osobowych do okna dialogowego **Karty**.
2. Na liście kart zaznacz kartę tymczasową.
3. Kliknij przycisk **Usuń kartę**
   .Karta tymczasowa zostanie usunięta z listy, a zastępowane przez nią karty natychmiast odblokowane.

Procedura: Usuwanie tymczasowych blokad kart

Jeśli blokowanie oryginalnej karty nie jest już potrzebne, usuń blokadę w następujący sposób:

1. Przejdź do okna dialogowego **Blokowanie** i wybierz kolejno opcje **Dane osobowe** > **Blokowanie**.
2. Na liście kart zaznacz kartę osobistą oznaczoną jako zablokowaną w kolumnie **Blokady**.
3. Kliknij przycisk **Zwolnij tymczasową blokadę**
   .Zauważ, że rekord na liście **Blokowanie** pozostał. Lista zawiera tylko historię wszystkich blokad — przeszłych i obecnych — aktualnego zestawu danych osobowych.

Uwagi na temat kart tymczasowych

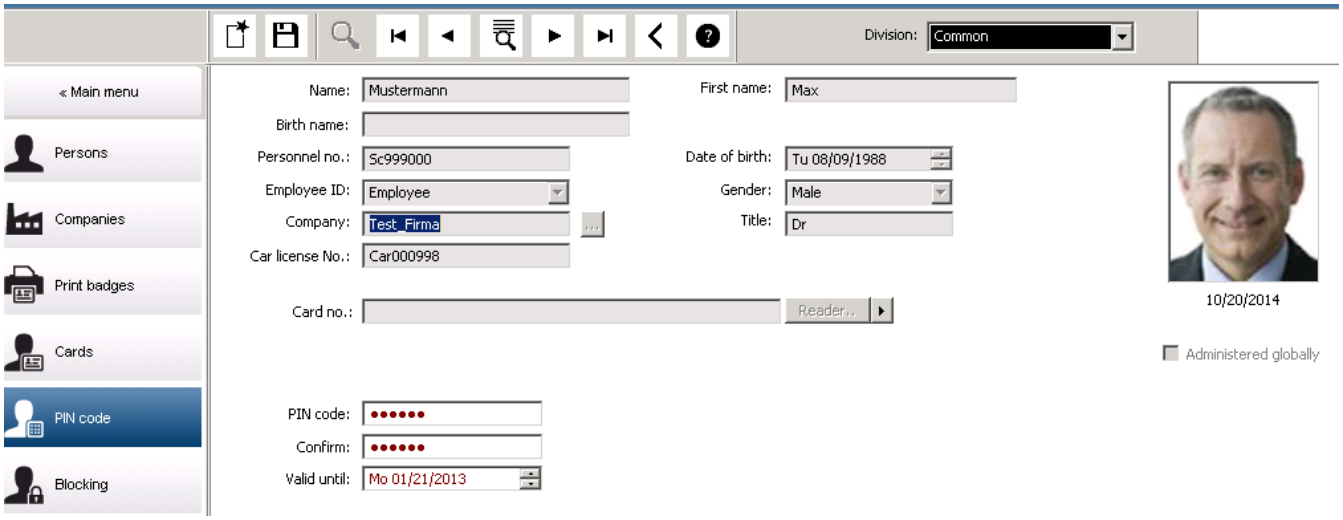
- System nie pozwala na zastępowanie kart tymczasowych innymi kartami tymczasowymi.
- System nie pozwala, aby karta osobista miała więcej niż jedną kartę tymczasową na zamianę.
- Aby zobaczyć szybkie podsumowanie wszystkich kart posiadanych przez osobę, umieść kursor myszy nad małym panelem najbardziej z lewej strony (podpisanym **Zarejestrowane**) na pasku stanu w głównym oknie dialogowym.

17.5 Kody PIN dla personelu

Okno dialogowe: Kod PIN

W celu dostępu do stref o wyższych wymaganiach w zakresie bezpieczeństwa samo uprawienie dostępu może okazać się niewystarczające. Trzeba dodatkowo wprowadzić kod PIN. Każda osoba lub karta identyfikacyjna może mieć przypisany kod PIN, który jest ważny na wszystkich obszarach. System zapobiega używaniu bardzo prostych kodów (np. 123456 lub palindromów typu 127721). W oknie dialogowym można ograniczać termin ważności i wyznaczać go oddzielnie dla każdej osoby.
Jeśli kod PIN jest zablokowany lub wygasł, próba dostępu do obszaru wymagającego podania kodu spotka się z odmową, nawet jeśli karta identyfikacyjna zachowuje nadal ważność na pozostałych obszarach.

W przypadku wprowadzenia nieprawidłowego kodu trzy razy z rzędu (jest to ustawienie domyślne, które można zmieniać w zakresie 1–99) karta zostaje zablokowana, tzn. próby dostępu będą odrzucane na wszystkich obszarach. Zablokowaną w ten sposób kartę można odblokować tylko w oknie dialogowym Blokowanie.



Wprowadź kod PIN w polu **Kod PIN**, po czym potwierdź go, wpisując ponownie. Długość kodu PIN (w zakresie 4–9 cyfr, domyślnie 6) jest ustalana przez administratora systemu.

Uwaga!
Sposób wprowadzania kodu PIN przez posiadaczy kart zależy od rodzaju czytników skonfigurowanych w systemie. Na przykład:
W czytnikach RS485 należy wpisać: **4 #** `<the PIN>`
W czytnikach Wiegand i innych należy wpisać: `<the PIN>` **#**
Posiadacze kart powinni zostać poinformowani, jak mają wprowadzać kod PIN. W razie wątpliwości należy skontaktować się z administratorem systemu.

Kod PIN do uzbrajania systemów sygnalizacji włamania (SSW)
Należy wprowadzić kod PIN o długości od 4 do 8 cyfr (domyślnie 6 — tyle samo, co w przypadku weryfikacyjnego kodu PIN). Ten kod PIN będzie służyć do uzbrajania systemu sygnalizacji włamania (IDS).
Wyświetlanie tych pól można konfigurować. Powyższe ustawienie jest dostępne tylko po włączeniu opcji **oddzielny kod IDS PIN**.
– Menu główne > **Konfiguracja** > **Opcje** > **Kody PIN**
W razie potrzeby należy wybrać termin ważności.
Jeśli pola do wprowadzania kodu PIN systemu sygnalizacji włamania są niedostępne, można uzbrajać i rozbrajać ten system również przy użyciu weryfikacyjnego kodu PIN. Jeśli jednak pola te są widoczne w oknie dialogowym, można stosować tylko kod PIN przeznaczony do uzbrajania systemu sygnalizacji włamania.
Ustawienie domyślne: pola wprowadzania kodu PIN służącego do uzbrajania są niewidoczne.

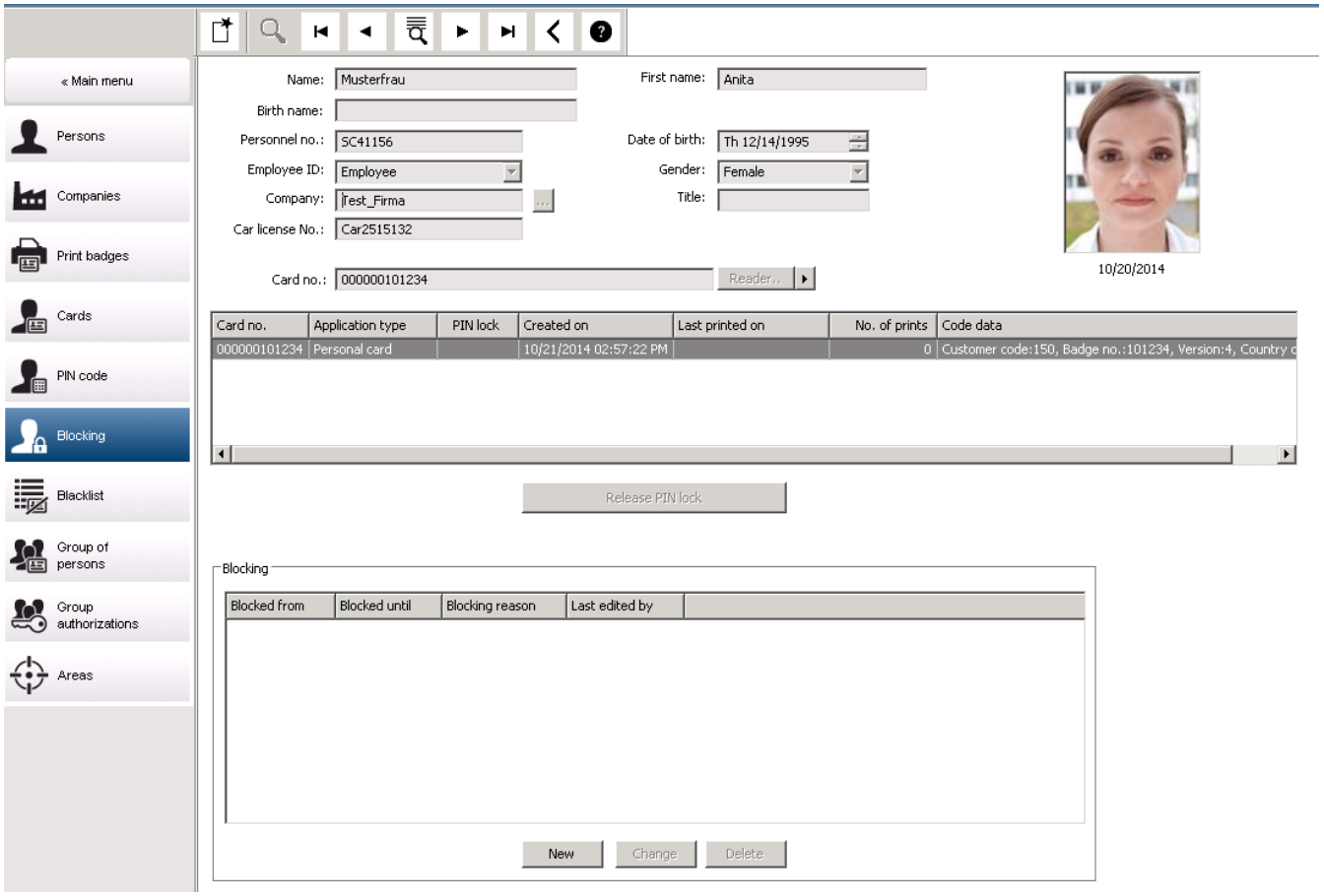
Kody PIN alarmu (zagrożenia)
W sytuacji zagrożenia można uruchomić cichy alarm za pomocą specjalnego kodu PIN. Ponieważ cichy alarm musi pozostać niezauważony przez napastnika, dlatego dostęp jest przyznawany, ale operatorzy systemu otrzymują ostrzeżenie o niebezpieczeństwie.
Dostępne są dwie odmiany, które są aktywne równolegle, a osoba znajdująca się w sytuacji zagrożenia może wybrać dowolną z nich:
– Wpisanie kodu PIN w odwrotnej kolejności (321321 zamiast 123123).

– Zwiększanie kodu PIN o 1 (na przykład: 123124 zamiast 123123). Uwaga: jeśli ostatnią cyfrą kodu PIN jest 9, to kod alarmu zagrożenia zostanie zmieniony z 123129 na 123130.

17.6 Blokowanie dostępu personelowi

Okno dialogowe: Blokowanie

W pewnych okolicznościach trzeba tymczasowo zabronić osobie dostępu lub usunąć blokadę nałożoną przez kontroler MAC, np. z powodu trzykrotnego wprowadzenia z rzędu nieprawidłowego kodu PIN albo w celu przeprowadzenia losowej kontroli.
Zablokowanie oznacza, że osoba ma całkowity zakaz dostępu, niezależnie od podanych poświadczeń.



1. Zaznacz osobę w zwykły sposób.
2. W panelu Blokowanie kliknij przycisk **Nowy**, aby utworzyć blokadę dla aktualnie wybranej osoby.
3. W wyskakującym oknie dialogowym wprowadź dodatkowe informacje:
   – **Zablokowane od / do**: (jeśli nie określono godziny zakończenia, osoba jest blokowana do czasu ręcznego zniesienia blokady)
   – **Rodzaj blokady:**
   – **Przyczyna blokowania:** (dla rekordu osoby, jeśli rodzajem blokady jest `Manual`)
4. W wyskakującym oknie kliknij przycisk **Zapisz**, aby zapisać blokadę.

– W razie potrzeby zaznacz blokadę na liście i kliknij przycisk **Zmień** lub **Usuń**, aby zmienić lub usunąć blokadę.

Jeśli w polu rodzaju blokady wybrano opcję **Blokowanie ręczne**, wypełnij pole **Przyczyna blokowania** w rekordzie osoby.

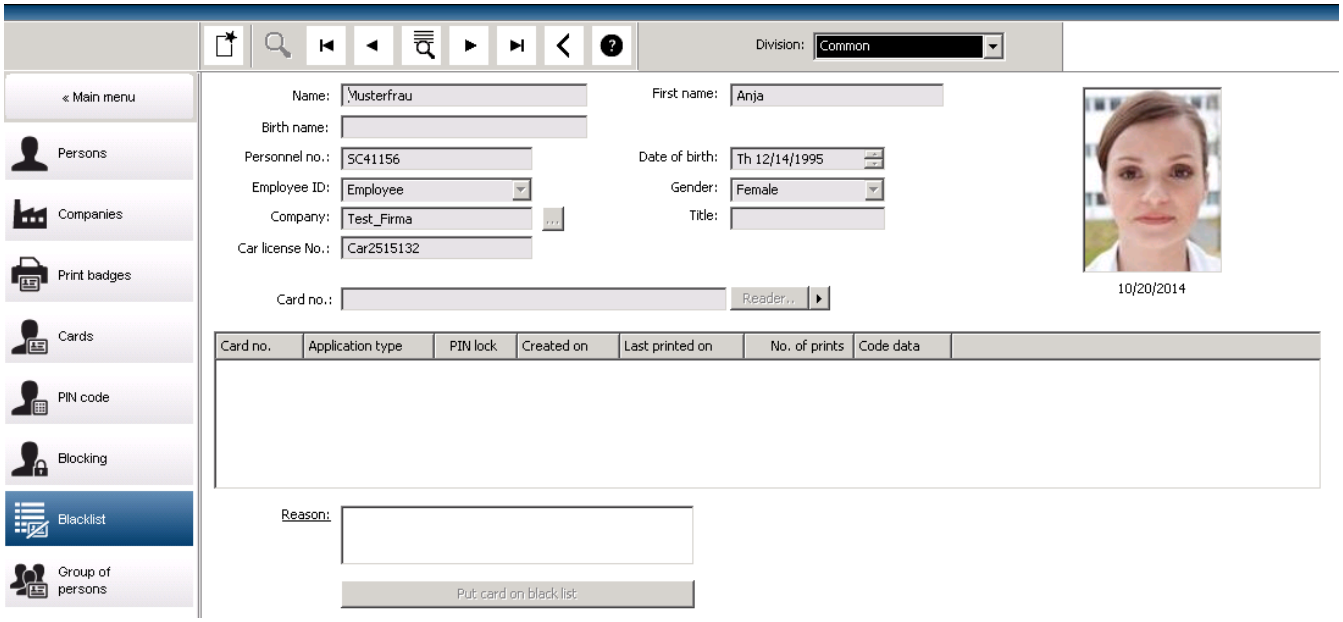
Uwaga!
Blokada odnosi się do osoby, a nie do określonego poświadczenia. Nie można więc anulować ani unieważnić blokady poprzez przydzielenie nowej karty identyfikacyjnej.

17.7 Karty wymienione na czarnej liście

Okno dialogowe: Czarna lista
Wszystkie karty, które już nigdy nie powinny być używane, ponieważ np. je skradziono lub zgubiono, są wprowadzane w tabeli czarnej listy.
Pamiętaj, że na czarnej liście są umieszczane poświadczenia, a nie osoby.

Uwaga!
Proces ten jest nieodwracalny. Kart znajdujących się na czarnej liście nie można nigdy odblokować i trzeba je zastąpić.

Karty z czarnej listy nie zapewniają dostępu. Wręcz przeciwnie — próba ich użycia jest rejestrowana w pliku dziennika i wywołuje alarm.



Menu główne > **Dane osobowe** > **Czarna lista**

1. Wybierz osobę, której karta identyfikacyjna ma trafić na czarną listę.
2. Jeśli ten posiadacz ma przypisaną więcej niż jedną kartę, należy wybrać odpowiednią z nich na liście **Nr karty identyfikacyjnej**.
3. W polu wprowadzania danych **Powód** określ przyczynę umieszczenia tej karty na czarnej liście.

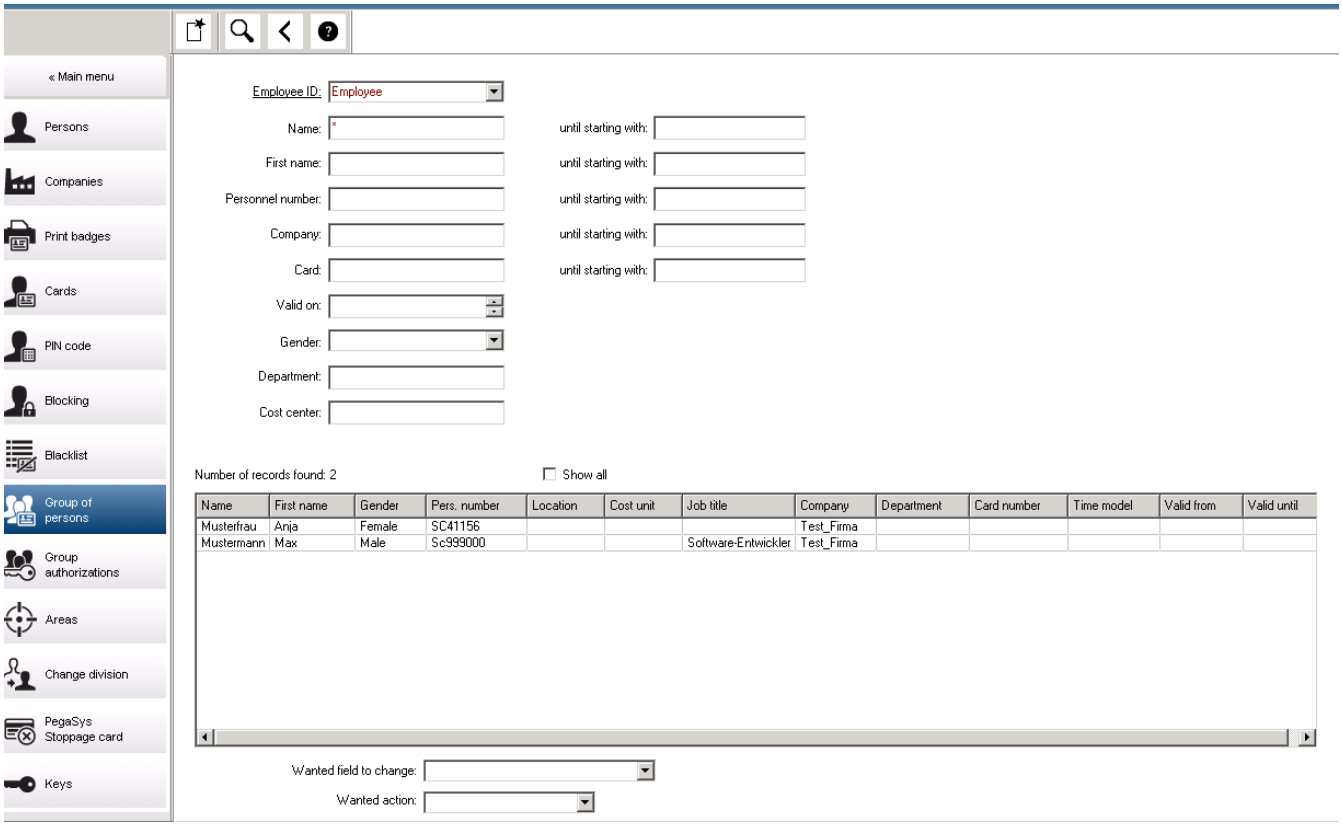
4. Kliknij przycisk **Umieść kartę na czarnej liście**.
5. W wyświetlonym oknie potwierdź umieszczenie na czarnej liście.

Karta trafia na czarną listę ze skutkiem natychmiastowym.

Uwaga!
Umieszczanie na czarnej liście dotyczy kart, a **nie** ich posiadaczy.
Należące do tej samej osoby karty, które nie znajdują się na czarnej liście, nie są blokowane.

17.8 Edytowanie wielu osób jednocześnie

Grupa osób



Kolejne okno dialogowe służy do wybierania grupy osób, w odniesieniu do której można wprowadzać modyfikacje. Aby zachować kontrolę nad wybraną grupą osób, pierwsze dziesięć osób jest wyświetlanych z nazwiskami i rzeczywistymi danymi z bazy danych (rzeczywiste dane: jeśli jako dział wybrano „ST-AC”, wyświetlane będą np. pozycje „ST-ACS” i „ST-ACX”). Ponadto wyświetlana jest liczba osób należących do wybranej grupy.
Po wybraniu grupy osób dostępne są do wyboru następujące pozycje:

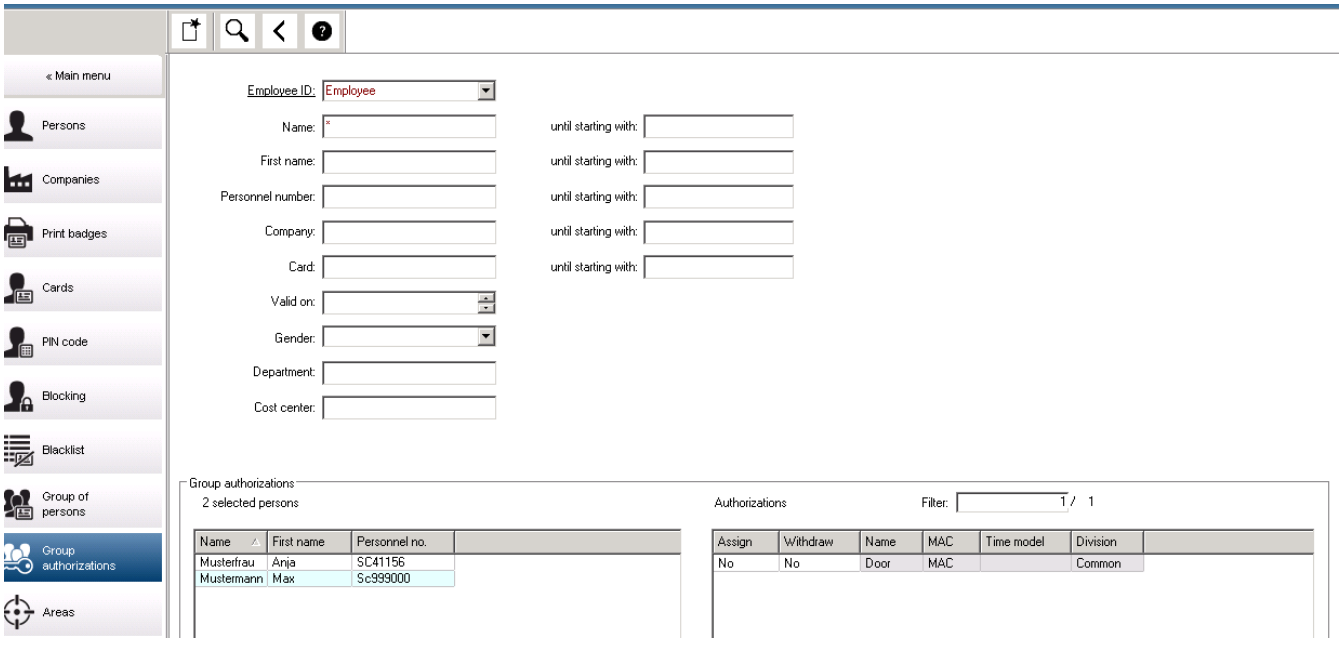
- Identyfikator pracownika
- Nazwa
- Imię
- Numer personalny
- Firma
- Karta
- Ważne w dniu

– Płeć
– Department (Dział)
– Jednostka kosztów
– Zarezerwowane pola, o ile je zdefiniowano

Następnie można wybierać spośród opcji modyfikacji:
– Pole do zmiany
– Żądana akcja
– Stara wartość
– Nowa wartość

Modyfikowane wartości wprowadza się w polach odpowiednio **Stara wartość** i **Nowa wartość**. Po kliknięciu przycisku **Zastosuj zmiany** i udzieleniu odpowiedzi twierdzącej na pytanie zabezpieczające **zastosować zmiany do wszystkich wybranych osób?** nastąpi wykonanie wybranego działania. W trakcie jego realizacji nie można korzystać z tego okna dialogowego. Działania wyzwalane przez pola od *1 do *4 będą z reguły trwać dłużej niż w przypadku pozostałych pól (czyli nieoznaczonych gwiazdką), a ponadto nie można w nich stosować niektórych modyfikacji. Nie można np. porównywać pól wprowadzania danych **Żądana akcja** i **Nowa wartość**, ponieważ nie są one obejmowane przez standardowy system. Pola **Stara wartość** i **Nowa wartość** również mogą ulegać zmianom.

Grupa uprawnień



Element menu **[Grupa uprawnień]** obsługuje następujące kryteria wyszukiwania:
– Identyfikator pracownika
– Nazwa
– Imię
– Numer personalny
– Firma
– Karta
– Ważne w dniu

- Płeć
- Department (Dział)
- Jednostka kosztów
- Zarezerwowane pola, o ile je zdefiniowano

Następnie w dolnej części okna dialogowego pojawia się lista wszystkich wybranych osób (z nazwiskiem, imieniem i numerem personalnym). Wszystkie uprawnienia są podane na liście w prawym dolnym rogu razem z opisem uprawnienia, modelem czasowym oraz kolumnami **[Przypisz]** i **[Wycofaj]**. Gdy pojawia się lista uprawnień, bieżące uprawnienia są niewidoczne, a w kolumnach **[Przypisz]** i **[Wycofaj]** znajduje się ustawienie wstępne „Nie”. Można teraz przypisywać poszczególne uprawnienia, klikając dwukrotnie pole w jednej z kolumn. Spowoduje to zmianę ustawienia „Nie” na „Tak” lub odwrotnie. Kliknięcie przycisku Wykonaj powoduje zmianę wszystkich uprawnień mających ustawienie „Tak” — zostają one przypisane lub wycofane w przypadku wszystkich wybranych osób. Pozostałe uprawnienia tych osób nie zostaną zmienione, ponieważ zwykle wybrane osoby nie mają całkiem identycznych uprawnień.

18 Definiowanie uprawnień i profili dostępu

18.1 Tworzenie uprawnień dostępu

Ścieżka w oknie dialogowym

Menu główne > **Dane systemowe** > **Uprawnienia**

Procedura

1. Wyczyść zawartość pól wprowadzania danych, klikając na pasku narzędzi przycisk **Nowy**  .

   Alternatywnie kliknij przycisk **Kopiuj**  , aby utworzyć nową autoryzację na podstawie istniejącej.
2. Nadaj uprawnieniu niepowtarzalną nazwę.
3. (Opcjonalnie) Wprowadź opis.
4. (Opcjonalnie) Wybierz model czasowy mający rządzić tym uprawnieniem.
5. (Opcjonalnie) Z listy wybierz **limit nieaktywności**.
   Jest to okres wynoszący od 14 do 365 dni. Jeśli posiadacz tej autoryzacji nie skorzysta z niej w podanym czasie, straci ją. Za każdym razem, gdy posiadacz użyje uprawnienia, licznik czasu uruchamia się ponownie od zera.
6. (Obowiązkowe) Przypisz co najmniej jedno **wejście**.
   Istniejące wejścia są wyszczególnione na różnych kartach, w zależności od ich modeli drzwi.
   (Standardowe) **Wejście**, **Zarządzanie czasem**, **Winda**, **Parking**, **Uzbrajanie systemu sygnalizacji włamania**.
   Wybierz poszczególne wejścia z list na różnych kartach, jak opisano poniżej.
   Alternatywnie użyj przycisków **Przypisz wszystkie** i **Usuń wszystkie** na poszczególnych kartach.
   - na karcie **Wejście** wybierz wejście, zaznaczając jedno lub oba pola wyboru **W** lub **Wyjście**
   - na karcie **Zarządzanie czasem** (dla czytelników rejestrujących czas i obecność) zaznacz jedno lub oba pola wyboru **W** lub **Wyjście**
   - na karcie **Winda** zaznacz poszczególne piętra
   - na karcie **Parking** zaznacz parking i strefę parkowania
   - na karcie **Uzbrajanie systemu sygnalizacji włamania** zaznacz opcję **Uzbrojony** lub **Rozbrojone**
7. Wybierz odpowiedni kontroler MAC z listy.
8. Kliknij przycisk Zapisz  , aby zapisać autoryzację.

Uwaga!

Późniejsze zmiany uprawnień wpłyną na obecnych posiadaczy, chyba że profil rządzący uprawnieniami zostanie zablokowany.

Przykład: Jeśli limit nieaktywności wynoszący 60 dni zostanie skrócony do 14 dni, autoryzację utracą wszystkie osoby, które jej nie wykorzystały w ciągu ostatnich 14 dni.

Wyjątek: Jeśli autoryzacja jest częścią profilu dostępu **zblokowanego** z identyfikatorem pracownika (typem osoby), to limity nieaktywności w uprawnieniu nie mają wpływu na tego typu osoby. Blokady profili można ustawić za pomocą następującego pola wyboru.

Menu główne > **Dane systemowe** > **Typy osób** > tabela: **Predefiniowane identyfikatory pracowników** > pole wyboru: **Profil zablokowany**

18.2 Tworzenie profili dostępu

Uwaga: Używanie profili dostępu do łączenia uprawnień w pakiety
Dla spójności i wygody uprawnienia dostępu nie są przypisywane pojedynczo, ale zazwyczaj łączone w **profile dostępu** i przypisywane w ten sposób.

– Menu główne: **> Dane systemowe** > **Profile dostępu**

Wymagania wstępne
Uprawnienia dostępu zostały już zdefiniowane w systemie.

Procedura

1. Wyczyść zawartość pól wprowadzania danych, klikając na pasku narzędzi przycisk **Nowy**  .
   Alternatywnie kliknij przycisk **Kopiuj**  , aby utworzyć nowy profil na podstawie istniejącego.
2. Nadaj profilowi unikatową nazwę.
3. (Opcjonalnie) Wprowadź opis.
4. (Opcjonalnie) Zaznacz to pole wyboru **Profil gościa**, aby ograniczyć ten profil do osób odwiedzających.
5. (Opcjonalnie) Ustaw wartość w polu **Standardowy czas trwania ważności**.
   – Jeśli nie ustawisz żadnej wartości, profil będzie przypisany bezterminowo.
   – W przypadku ustawienia wartości będzie ona używana do obliczania daty ważności każdego późniejszego przypisania profilu.
6. (Obowiązkowe) Przypisz co najmniej jedno **uprawnienie**:
   Uprawnienia dostępne do przypisania są wymienione po prawej stronie.
   Uprawnienia, które zostały już przypisane, są wymienione po lewej stronie.
   Zaznacz elementy, a następnie kliknij przyciski między listami, aby przenieść elementy z jednej listy do drugiej.
   –  przypisuje wybrany element.
   –  cofa przypisanie wybranego elementu.
7. Kliknij przycisk Zapisz  , aby zapisać profil.

19 Zarządzanie gośćmi

Goście mają specjalny status w systemie kontroli dostępu, a informacje o nich nie są przechowywane z pozostałymi danymi osobowymi. Z tego powodu dane gości tworzy się i modyfikuje w osobnych oknach dialogowych.

19.1 Dane gościa

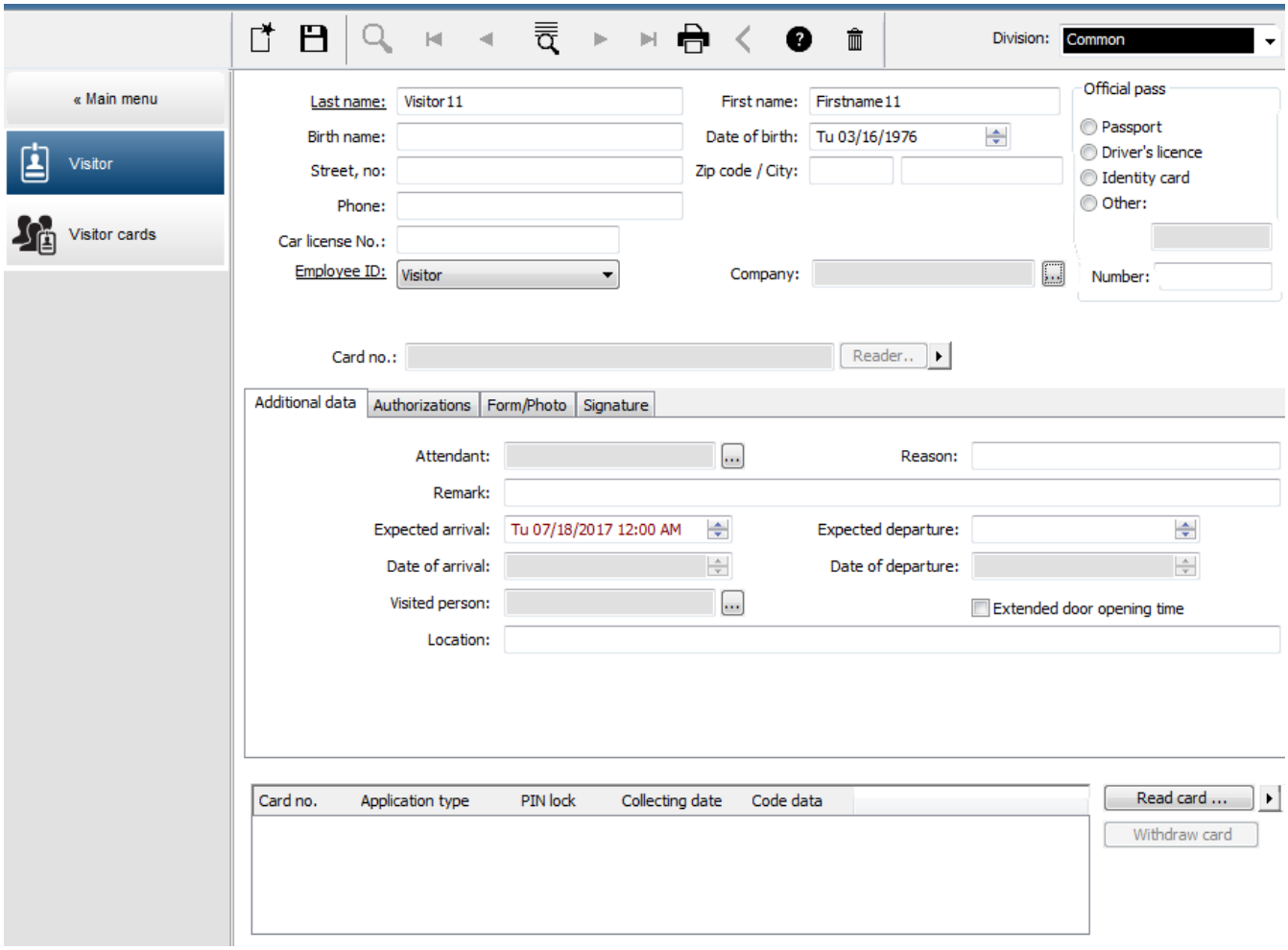
Wstęp

System obsługuje szybkie i łatwe zarządzanie danymi gości. Dzięki temu dane gości, którzy są już znani, można wprowadzać i uzupełniać o uprawnienia dostępu jeszcze przed ich przybyciem. Gdy gość dotrze na miejsce, pozostanie tylko przydzielenie mu karty. Na zakończenie wizyty, gdy następuje zwrot karty, powiązanie między kartą identyfikacyjną a osobą zostaje usunięte, a uprawnienia są automatycznie wycofywane.
Jeśli użytkownik nie usunie danych gościa, system wykona to automatycznie po upływie wyznaczonego czasu (wartość domyślna to 6 miesięcy) od chwili ostatniego zwrotu karty identyfikacyjnej.
Do zarządzania zewnętrznymi gośćmi służą dwa okna dialogowe.

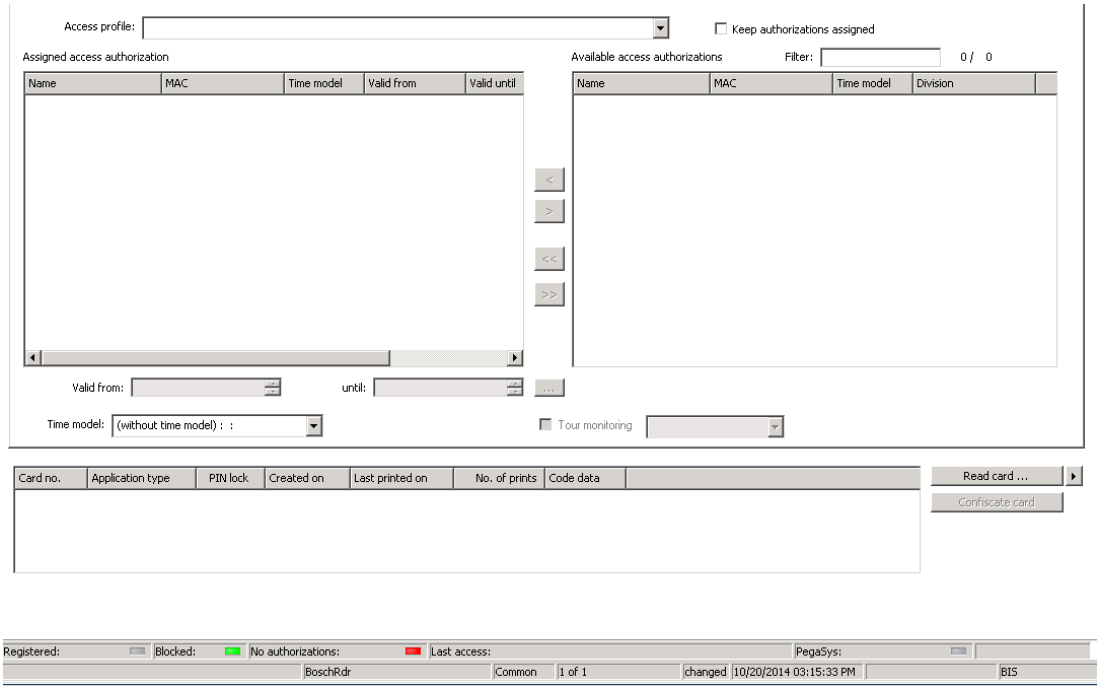
– Okno dialogowe **Goście** jest przeznaczone do wprowadzania danych gości i ich uprawnień dostępu.
– W oknie dialogowym **Karty gości** przeprowadza się rejestrowanie i usuwanie kart gości.

Okno dialogowe: Goście

Goście mają zupełnie odrębny status niż inne osoby i dlatego ich dane są przetwarzane w osobnym oknie dialogowym. Osób oznaczonych jako **gość** nie można tworzyć w oknie dialogowym **Osoby** ani też nie można rejestrować dla nich kart identyfikacyjnych w służącym do tego oknie dialogowym.
W oknie dialogowym **Goście** brakuje m.in. pola wprowadzania danych **Identyfikator pracownika**. W bazie danych znajduje się odrębna tabela dla gości, więc osoby tworzone w omawianym tu oknie dialogowym są automatycznie identyfikowane jako goście. Oznacza to, że nie można w nim tworzyć żadnych innych osób poza gośćmi. W związku z tym wybory dokonywane w tym oknie dialogowym odnoszą się wyłącznie do odpowiadającej mu tabeli w bazie danych. W przeciwieństwie do tego wszystkie osoby zarejestrowane w systemie można wybierać w pozostałych oknach dialogowych danych osobowych, ale nie zawsze możliwe jest korzystanie z tych okien w przypadku gości (dotyczy to np. okna dialogowego **Karty**).
O ile tylko znane są pełne lub częściowe dane gościa, można je wprowadzać do systemu jeszcze przed jego przybyciem. Ogranicza to do minimum czas oczekiwania w przypadku gości, których dane zostały już zarejestrowane.



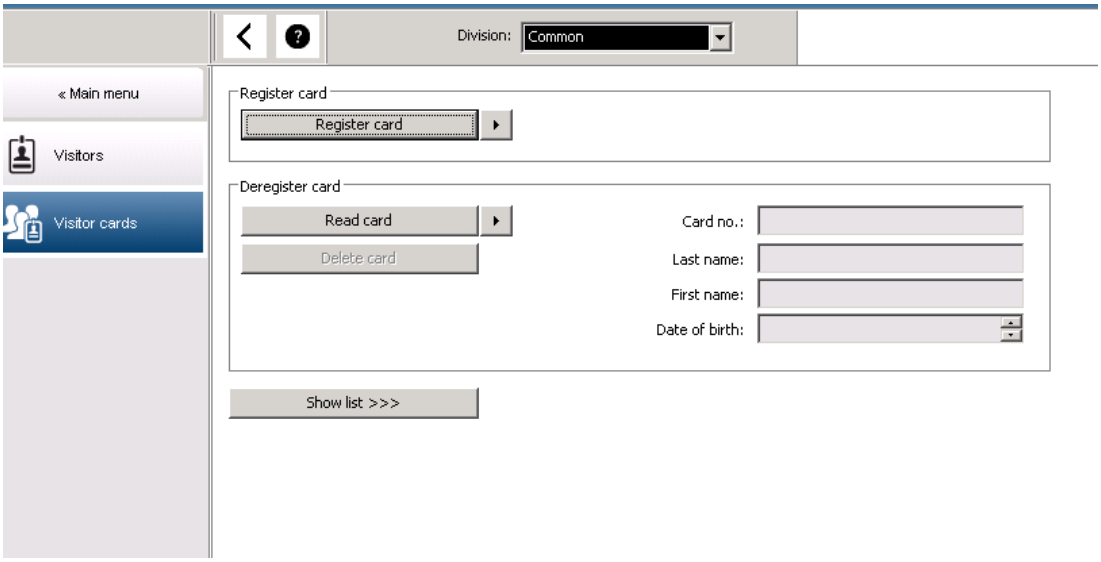
W poniższych polach wprowadzania danych **Powód**, **Lokalizacja** i **Uwaga** można wpisać odpowiednio: powód wizyty, lokalizację, która zostanie odwiedzona, oraz uwagę dotyczącą pobytu.
W przypadku wypełnienia pól **Spodziewane wejście** i **Spodziewane wyjście** dane te pojawią się również w polach **ważne od** i **ważne do**.
Odpowiednie daty są wprowadzane przez system w polach **Data wejścia** i **Data wyjścia**, gdy dane gościa są przypisywane do karty identyfikacyjnej gościa i z niej wycofywane.
Podobnie jak w oknie dialogowym **Karty**, można też przypisywać gościom przedłużony czas otwarcia drzwi, aby ułatwić dostęp np. osobom niepełnosprawnym.



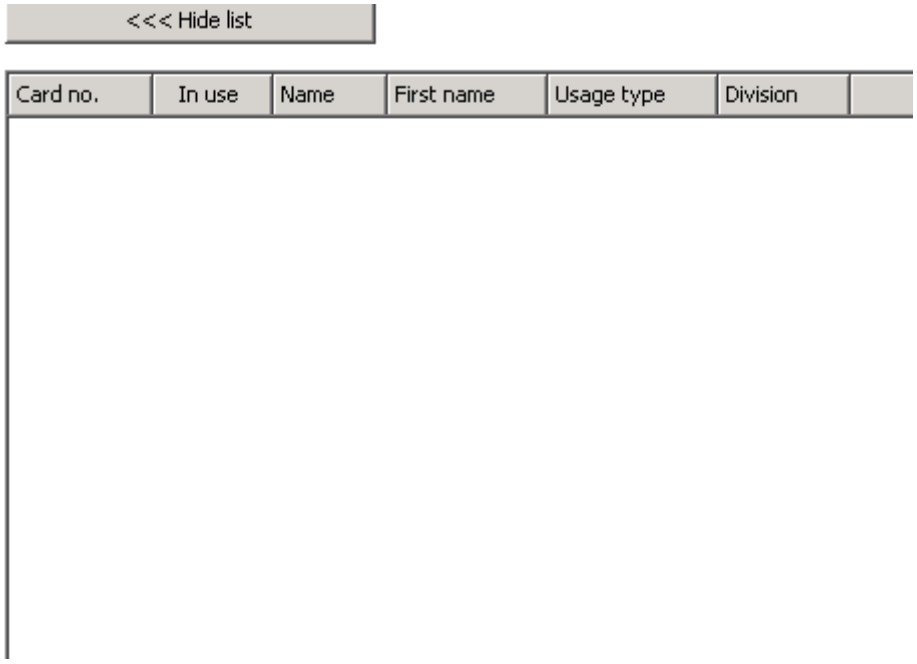
W polu dialogowym **Przypisz autoryzację** można na liście wyboru o tej samej nazwie wybrać jeden z istniejących już profili gości albo zaznaczać poszczególne uprawnienia dostępu na liście **Dostępne uprawnienia dostępu** po prawej stronie i przenosić je na listę **Przypisane uprawnienia dostępu** po lewej stronie.
W tym oknie dialogowym można wybierać tylko profile dostępu oznaczone jako profile gości. Dlatego należy unikać przyznawania gościom dostępu do specjalnych obszarów poprzez nadawanie im ogólnych uprawnień.
Poszczególnym uprawnieniom dostępu można też wyznaczać termin ważności.
Jeśli odczyt karty wykazuje błąd, można również ręcznie wprowadzić numer karty identyfikacyjnej. Jako data wejścia zapisywana jest wtedy bieżąca data.
Po zakończeniu wizyty gość zwraca swoją kartę identyfikacyjną. Po odczytaniu karty identyfikacyjnej w czytniku kart lub ręcznym wprowadzeniu jej numeru wybierana jest powiązana z nią osoba, a na ekranie pojawiają się jej dane.
Operator potwierdza zwrot karty. Powiązanie karty identyfikacyjnej z gościem zostaje usunięte kliknięciem przycisku **Konfiskuj kartę**. Data i godzina tej operacji jest zapisywana jako data wyjścia.

Okno dialogowe: Karty gości
Niektóre karty w systemie są zarezerwowane jako karty gości. Zwykle karta gościa jest przydzielana przybywającemu gościowi i zwracana, gdy gość opuszcza teren. Wtedy może zostać ponownie użyta. Aby takie karty można było przydzielać gościom, należy je wcześniej zarejestrować jako karty gości w tym oknie dialogowym.

Uwaga!
Z zasady na kartach identyfikacyjnych gości nie umieszcza się imienia i nazwiska ani zdjęcia, dzięki czemu można ich używać wielokrotnie.



Aby zarezerwować kartę, należy kliknąć przycisk **Zarejestruj kartę identyfikacyjną**. Następnie stosuje się opisaną już procedurę wprowadzania danych (patrz sekcje **Osoby** i **Karty identyfikacyjne** w podrozdziale **Dane osobowe**), aby wykryć kartę identyfikacyjną na podstawie jej numeru. Umożliwia to systemowi rozpoznanie karty jako karty identyfikacyjnej gościa, dzięki czemu można jej używać w granicach zastosowań wyznaczanych przez poniższe okna dialogowe.



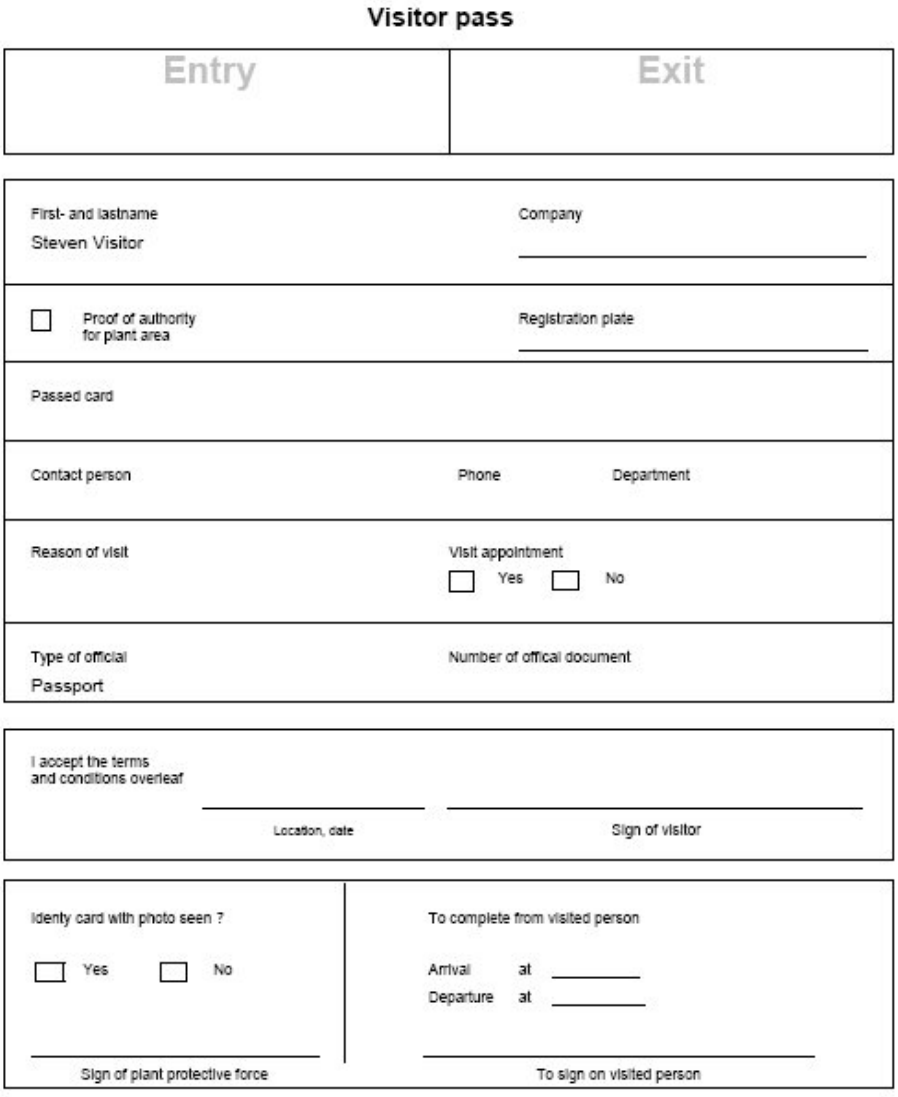
Aby przyspieszyć przydzielanie kart identyfikacyjnych gości, zaleca się zeskanowanie wszystkich istniejących już kart identyfikacyjnych, co umożliwi przydzielanie ich gościom w kolejnym oknie dialogowym.

Na zakończenie wizyty gość zwraca swoją kartę identyfikacyjną. Po zeskanowaniu karty identyfikacyjnej w czytniku kart lub ręcznym wprowadzeniu jej numeru wybierana jest osoba, której ją przydzielono, a na ekranie pojawiają się dane tej osoby. [Informacje na temat ręcznego wprowadzania numeru karty identyfikacyjnej i przełączania się na użycie czytników można znaleźć w podrozdziałach **Okno dialogowe: Karty** i **Okno dialogowe: Goście**].

Użytkownik potwierdza zwrot karty identyfikacyjnej. Powiązanie karty identyfikacyjnej z danymi osobowymi gościa zostaje usunięte po kliknięciu odpowiedniego przycisku. Bieżąca data jest zapisywana jako data wyjścia.

Drukowanie formularza gościa

Na pasku narzędzi okna dialogowego **Goście** znajduje się dodatkowy przycisk  służący do drukowania certyfikatu gościa. Osoba przyjmująca gościa może użyć takiego certyfikatu m.in. do potwierdzenia, czy i kiedy jej gość przybył i opuścił teren.



Visitor pass

Entry	Exit

First- and lastname
Steven Visitor

Company

☐ Proof of authority for plant area

Registration plate

Passed card

Contact person | Phone | Department

Reason of visit

Visit appointment ☐ Yes ☐ No

Type of official
Passport

Number of offical document

I accept the terms and conditions overleaf

Location, date

Sign of visitor

Identy card with photo seen ?

☐ Yes ☐ No

Sign of plant protective force

To complete from visited person

Arrival at _____
Departure at _____

To sign on visited person

19.2 Spóźniony gość

W widoku **Spóźniony gość** klient może sprawdzać, gdzie na terenie firmy znajdują się goście i czy przypadkiem nie przekroczyli spodziewanego czasu wyjścia.
Uprawnieni użytkownicy systemu BIS powinni mieć na ekranie startowym umieszczone łącze do wyświetlania tej strony internetowej.

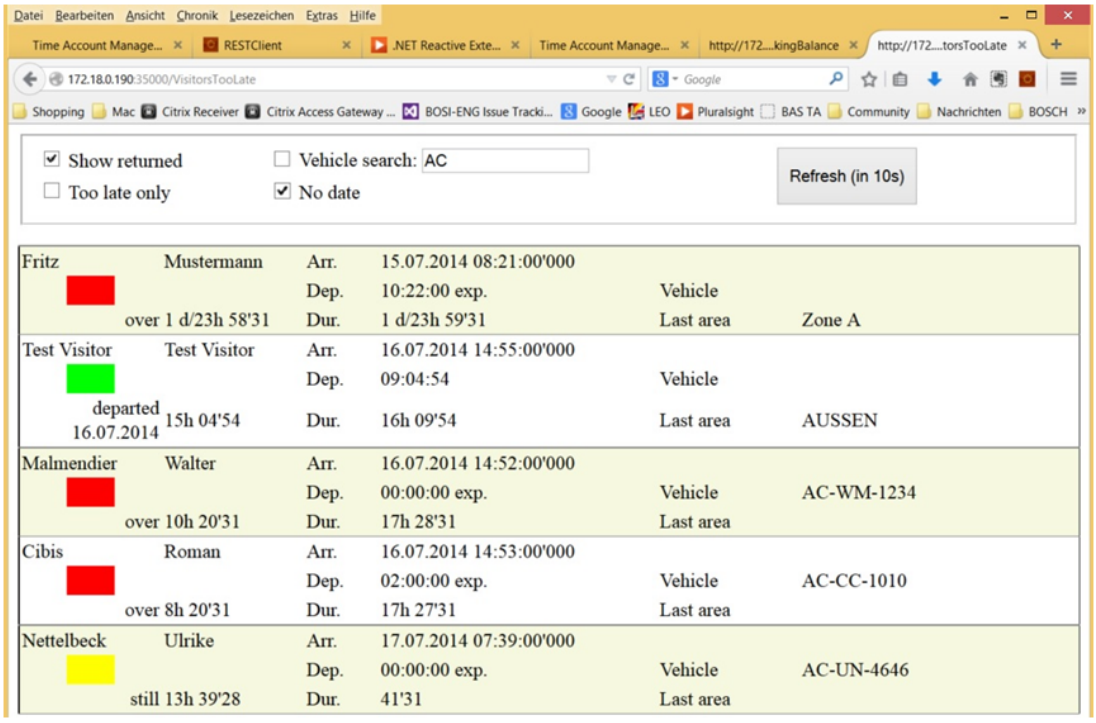
Możliwe jest ponadto skonfigurowanie w systemie BIS wyzwalacza urządzenia DMS, który będzie wywoływać alarm w przypadku pojawienia się komunikatu Spóźniony gość. Spowoduje to wyświetlenie użytkownikowi strony internetowej zawierającej wyłącznie dane odpowiedniej osoby z ostatnim znanym miejscem jej pobytu.
[patrz zrzut ekranu ze stroną internetową]

Zdarzenia powodujące pojawienie się komunikatu Spóźniony gość:
Kiedy kartę przydziela się gościowi, operator systemu wprowadza oczekiwany czas wyjścia. Po zakończeniu wizyty gość zwraca kartę w recepcji, gdzie operator ją dezaktywuje.
Alternatywnie czytnikiem wyjścia dla gości może być czytnik kart samochodowych z ustawioną opcją zatrzymywania kart wyjeżdżających osób.
Jeżeli gość nie odda karty przed ustaloną wcześniej godziną wyjścia, to bez względu na fakt, czy wciąż znajduje się na terenie obiektu, system wygeneruje komunikat **Spóźniony gość**.
Ta kontrola nieterminowego oddania kart jest wykonywana w regularnych odstępach czasu (np. co minutę). Komunikat **Spóźniony gość** będzie wysyłany przy każdej kontroli do momentu, aż gość zwróci kartę. Odstęp czasu można określić w rejestrze serwera w ustawieniu `HKLM\Software\Micos\SPS\Default\VLDP\Interval`.

Uwaga!
Generowanie komunikatu można wyłączyć w rejestrze serwera w ustawieniu `HKLM\Software\Micos\SPS\Default\VLDP\Active`.

Ta funkcja umożliwia klientowi wykrywanie gości, którzy nie spotkali wyznaczonego przedstawiciela lub nie zgłosili się w określonym czasie w recepcji przy wyjściu po odbyciu spotkania z przedstawicielem.
Sprawdzeniu podlegają następujące kwestie:
- na którym obszarze po raz ostatni użyto przydzielonego gościowi identyfikatora dostępu do budynku,
- czy gość zwrócił identyfikator dostępu do budynku,
- czy gość zwrócił identyfikator pojazdu (jeśli dotyczy danego przypadku).

Generowane są raporty **Spóźniony gość** i **Spóźniony pojazd**.
Jeśli identyfikator nie zostanie zwrócony, jego bieżący obszar może znaleźć się w raporcie „Spóźniony gość”.
Stan gościa jest sygnalizowany na stronie internetowej za pomocą kolorowych pasków:
- **Zielony**: gość zwrócił wszystkie karty dostępu.
- **Żółty:** wizyta jeszcze się nie zakończyła, a jej spodziewany czas jeszcze nie minął.
- **Czerwony:** wizyta jeszcze się nie zakończyła, ale jej spodziewany czas już minął, tzn. **Spóźniony gość**.



Zawartość tej strony jest automatycznie odświeżana co 30 sekund. Czas odświeżania można określać na samej stronie. Ponadto widok operatora można modyfikować za pomocą filtrów **Pokaż zwrócone**, **Tylko spóźnieni** i **Wyszukiwanie pojazdu**.

20 Zarządzanie parkingami

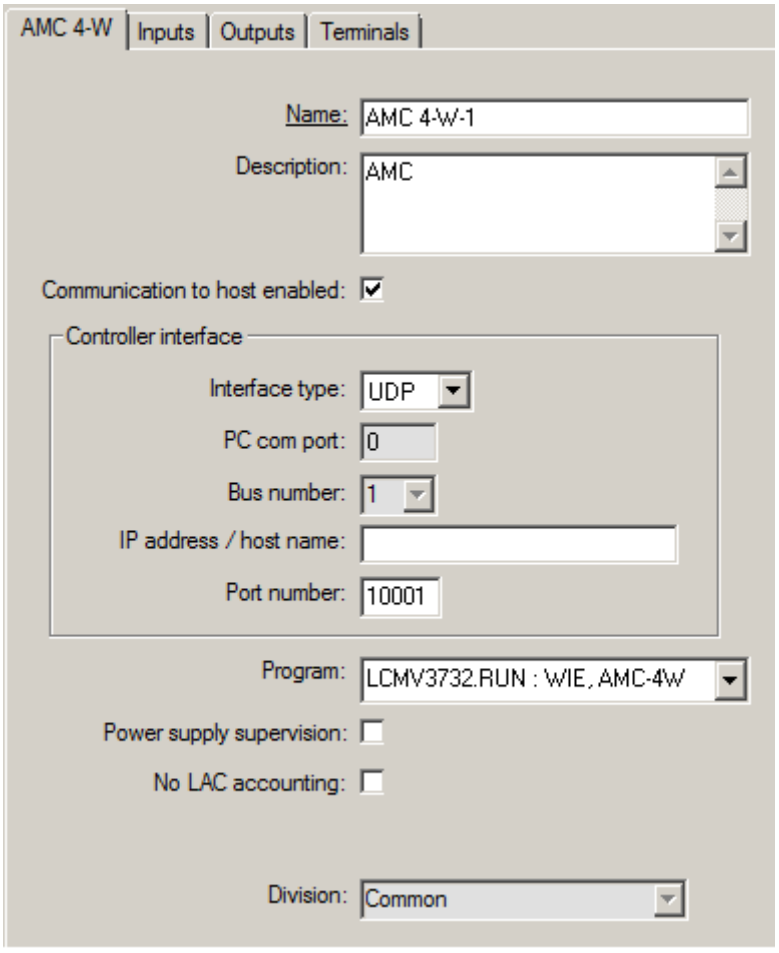
20.1 Uprawnienia do kilku stref parkingowych

Na niektórych parkingach znajdują się strefy dla kierowców pełnosprawnych i niepełnosprawnych. W takim przypadku obowiązują następujące reguły:

– Właściciele biletów sezonowych mogą wjechać na parking, tylko jeśli są nadal wolne miejsca parkingowe dla osób pełnosprawnych.
– Osoby niepełnosprawne mogą wjechać na parking, tylko jeśli są nadal wolne miejsca parkingowe dla osób pełnosprawnych lub niepełnosprawnych.

Uwaga!
Zakłada się więc, że właściciele biletów będą przestrzegać tych reguł. Oznacza to w szczególności, że:
Osoby pełnosprawne nie będą parkować na miejscach parkingowych przeznaczonych dla osób niepełnosprawnych.
Osoby niepełnosprawne będą korzystać z miejsc parkingowych przeznaczonych dla osób niepełnosprawnych, o ile są dostępne.

Osoba, która ma wiele uprawnień, może korzystać z obu rodzajów miejsca parkingowych niezależnie od tego, czy jest niepełnosprawna. Modułowy kontroler dostępu (AMC) próbuje umożliwić wjazd danej osobie zgodnie ze skonfigurowaną kolejnością stref parkingowych. Jeśli jedna strefa jest pełna, rozpoczyna wyszukiwanie kolejnej uprawnionej strefy z wolnymi miejscami parkingowymi.
Zliczanie pojazdów w głównym kontrolerze dostępu i w modułowych kontrolerach dostępu:
1) Jeden modułowy kontroler dostępu nadzoruje wszystkie wjazdy na parking i wyjazdy z niego:
=> Modułowy kontroler dostępu samodzielnie zlicza pojazdy, a po przełączeniu w tryb online jego wskazania mogą być korygowane przez główny kontroler dostępu.
2) Wjazdy na jeden parking i wyjazdy z niego są podzielone między różne modułowe kontrolery dostępu:
=> W przypadku działania w trybie online główny kontroler dostępu przejmuje zliczanie pojazdów od modułowych kontrolerów dostępu. Podczas pracy w trybie offline modułowe kontrolery dostępu zezwalają na wjazd i wyjazd (jeśli są odpowiednio skonfigurowane), ale nie zliczają pojazdów.
Jeśli jeden parking nadzoruje wiele modułowych kontrolerów dostępu, należy zaznaczyć w ich konfiguracji pole wyboru **Brak ewidencjonowania przez AMC**.



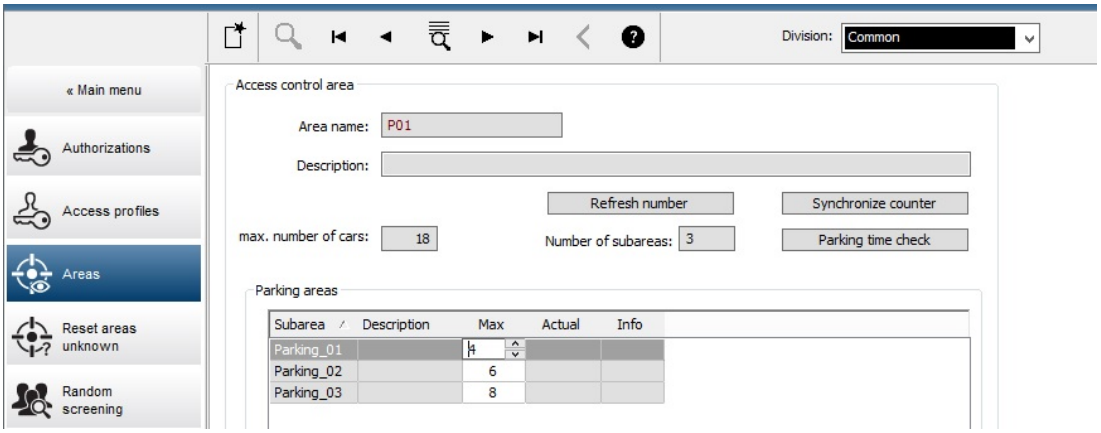
20.2 Parking dla pojazdów — informacje ogólne

20.3 Rozszerzone zarządzanie parkingami

Operator może dostosować liczbę miejsc parkingowych na obszarze parkingowym, aby uwzględnić pojazdy o niestandardowych rozmiarach, np.:

- Samochody ciężarowe
- Dostęp dla osób niepełnosprawnych
- Motocykle

1. Wybierz obszar parkingu
2. W panelu **Obszary parkingu** skoryguj wartość w kolumnie **Maks.** odpowiednio do nowej liczby miejsc parkingowych dla danego obszaru.



Menu główne > **Dane systemowe** > **Obszary**

21 Zarządzanie trasami dozorowymi i patrolami

Wprowadzenie do tras dozorowych

Trasa dozorowa prowadzi dookoła obiektu pomiędzy czytnikami kart, w których **pracownicy ochrony** muszą przedstawić specjalną kartę pracownika ochrony, by zarejestrować fizyczne sprawdzenie czytnika.

Karty pracowników ochrony nie otwierają przejść i służą wyłącznie do monitorowania. Aby otworzyć przejście, pracownik ochrony musi mieć dodatkowo kartę dostępu.

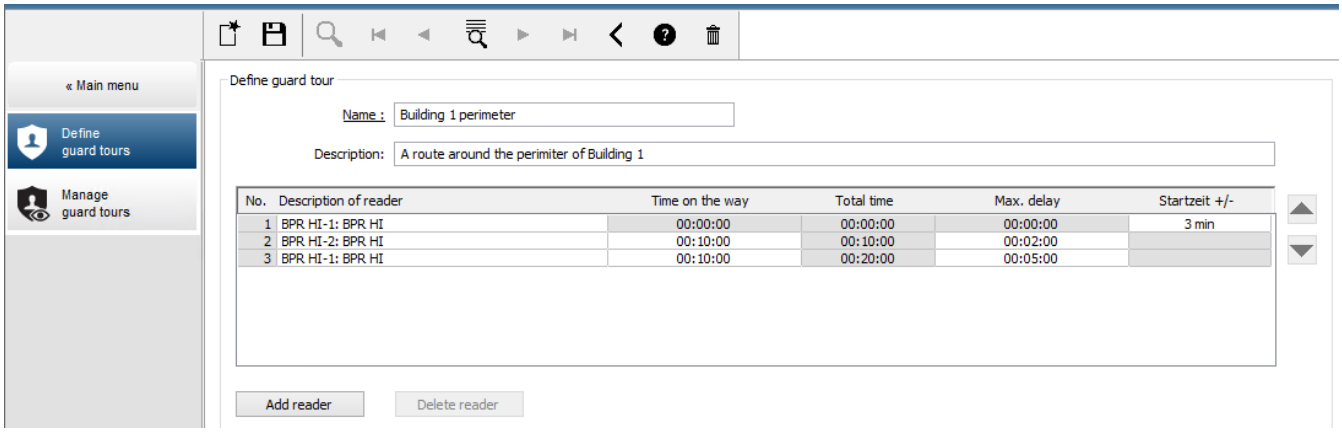
Trasa dozorowa składa się z serii czytników i przybliżonego czasu przejścia między nimi. Określone są również maksymalne dopuszczalne opóźnienie między czytnikami oraz odchylenie (+/-) od czasu rozpoczęcia trasy. Odchylenia wykraczające poza zdefiniowane wartości mogą uruchamiać alarmy i są rejestrowane w **Patrolach**.

Wprowadzenie do patroli

Patrol to trasa dozorowa z określoną datą i godziną. Każdy patrol jest tworzony i rejestrowany jako niepowtarzalna pozycja w systemie do celów ewentualnego dochodzenia.

21.1 Definiowanie tras dozorowych

Wybierz kolejno opcje **Trasy dozorowe** > **Definiowanie tras dozorowych**



– W polu tekstowym **Nazwa** wprowadź nazwę trasy dozorowanej.
– W polu tekstowym **Opis** wprowadź szczegółowy opis trasy (opcjonalnie).

Dodawanie czytników do trasy dozorowej:

1. Kliknij przycisk **Dodaj czytnik**.
   W tabeli tworzony jest wiersz.
2. W kolumnie **Description of reader (Opis czytnika)** wybierz czytnik z listy rozwijanej.
3. Wprowadź wartości dopuszczalnych odchyleń:
   – Jeśli jest to pierwszy czytnik w sekwencji, w polu **Start time +/- (Czas rozpoczęcia +/-)** wprowadź, o ile minut wcześniej lub później może się rozpocząć patrol na danej trasie dozorowej.
   – Jeśli to **nie** jest pierwszy czytnik w sekwencji, w polu **Time on the way (Czas w drodze)** wprowadź czas (hh:mm:ss) potrzebny pracownikowi ochrony do przejścia między poprzednim a tym czytnikiem.
   Łączny czas trasy, wyłączając opóźnienia, jest zsumowany w kolumnie **Total time (Łączny czas)**.

4. W polu **Max. delay (Maksymalne opóźnienie)** wprowadź maksymalną ilość dodatkowego **czasu w drodze**, który może upłynąć bez oznaczenia patrolu jako **Delayed (Opóźniony)**.
5. Dodaj tyle czytników, ile trzeba. Uwaga: niektóre czytniki mogą występować kilka razy, jeśli trasa dozorowa przechodzi przez nie klika razy lub wraca do nich.

– Aby usunąć czytnik z sekwencji, zaznacz wiersz i kliknij przycisk **Delete reader (Usuń czytnik)**.
– Aby zmienić pozycję czytnika w sekwencji, zaznacz wiersz i kliknij przycisk  w górę lub w dół.

21.2 Zarządzanie patrolami

Wybierz kolejno opcje **Trasy dozorowe** > **Zarządzanie trasami dozorowymi**.

Planowanie nowego patrolu

Aby zaplanować nowy patrol na danej trasie dozorowej:

1. Upewnij się, że masz odpowiednią kartę pracownika ochrony dla danego patrolu oraz dostęp do skonfigurowanego czytnika kart dostępowych lub bezpośrednio podłączonego czytnika administracyjnego.
2. W kolumnie **Guard tours (Trasy dozorowe)** wybierz jedną ze zdefiniowanych tras dozorowych.
3. Kliknij przycisk **New patrol... (Nowy patrol...)**.
   Pojawi się nowe okno wyboru.
4. W razie potrzeby zmień w nim trasę dozorową, wybierając ją z listy rozwijanej.
5. Jeśli patrol ma mieć wstępnie ustaloną godzinę rozpoczęcia, zaznacz pole wyboru **Set start time: (Ustaw czas rozpoczęcia:)**
   – Wprowadź datę i godzinę rozpoczęcia.
   – W razie potrzeby kliknij pole obrotowe **Start time +/- (Czas rozpoczęcia +/-)**, aby dostosować tolerancję późniejszego lub wcześniejszego rozpoczęcia.
6. Kliknij prawą strzałkę i wybierz czytnik, który ma zostać użyty do zarejestrowania karty pracownika ochrony. Uwaga: czytnik musi być już skonfigurowany w systemie, aby były dostępny do wybrania.
7. Kliknij zielony przycisk plusa, aby rozpocząć odczyt karty pracownika ochrony, zbliż kartę do czytnika i wykonuj instrukcje wyświetlane na ekranie.
   Karta pracownika ochrony zostanie zarejestrowana do użycia podczas patrolu.
8. Powtórz poprzedni krok, aby zarejestrować alternatywne karty pracowników ochrony. Uwaga: pierwsza karta patrolu musi być używana we wszystkich czytnikach do końca trasy.
9. Kliknij **OK**. Wybrana trasa dozorowa zostanie oznaczona na liście jako **planowana**.

Śledzenie patrolu

Wszystkie planowane i aktywne patrole są przenoszone na górę listy. Gdy jest kilka zaplanowanych lub aktywnych patroli, wybrany patrol jest oznaczony czerwoną ramką. Kliknij ramkę, aby uzyskać więcej informacji.

Patrol rozpoczyna się po odczytaniu karty pracownika ochrony przez pierwszy czytnik należący do trasy dozorowej. Ta karta musi być używana na całym patrolu, nawet jeśli zdefiniowano dla niego alternatywne karty.

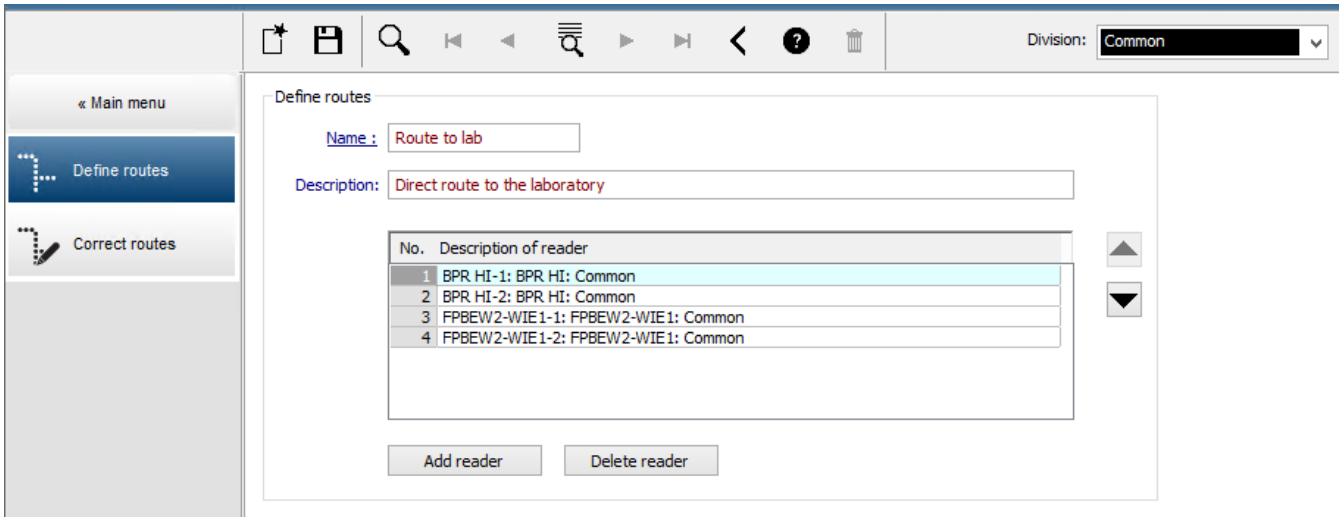
Stan patrolu zmienia się na **Active (Aktywny)**.

Każdy czytnik, do którego dociera pracownik ochrony, otrzymuje zielony znacznik –✔. Zaplanowane i rzeczywiste czasy między czytnikami w aktualnie zaznaczonym patrolu są wyświetlane w dolnej połowie okna dialogowego.
Każdy czytnik, do którego pracownik ochrony dociera później od zaplanowanego czasu plus **Max. delay (Maksymalne opóźnienie)** otrzymuje czerwony znacznik –⊘. Patrol jest oznaczany jako **Opóźniony**.
W takim przypadku pracownik ochrony wywołuje operatora, aby potwierdzić, że nie ma problemu. Następnie operator klika przycisk **Wznów patrol**. Na czytniku pojawi się zielony znacznik wyboru z dodatkową literą „c” –✔c. Pracownik ochrony może teraz kontynuować patrol od następnego czytnika.
Jeśli w aktywnym patrolu wystąpi nieprzewidziane ale nieszkodliwe opóźnienie, pracownik ochrony może zadzwonić do operatora, aby zmienić harmonogram. Należy w tym celu wprowadzić opóźnienie w polu obrotowym **Opóźnienie (min)** i potwierdzić przyciskiem **Zastosuj**.
Jeśli nie można zakończyć patrolu zgodnie z harmonogramem, operator może go przerwać przyciskiem **Przerwij**. **Stan** patrolu zmienia się na **Przerwany** i spada na liście poniżej zaplanowanych i aktywnych tras dozorowych.

21.3 Monitoring trasy (wcześniej Kontrola ścieżki)

Wstęp
Trasa to wstępnie zdefiniowana sekwencja czytników, którą można przypisywać do osób zdefiniowanych w systemie kontroli dostępu w celu kierowania ich ruchem na terenie obiektu niezależnie od uprawnień.
Zazwyczaj służy to do wymuszenia ścisłej sekwencji dostępu w środowiskach sterylnych lub wymagających najwyższego stopnia bezpieczeństwa.

Definiowanie tras
1. W menu głównym wybierz kolejno opcje **Monitoring trasy** > **Definiowanie tras**.
2. Wprowadź nazwę trasy (maks. 16 znaków).
3. Wprowadź szczegółowy opis (opcjonalnie)
4. Tak samo jak w przypadku tras dozorowych kliknij przycisk **Add reader (Dodaj czytnik)**, aby utworzyć sekwencję czytników. Za pomocą strzałek możesz zmienić pozycję czytnika w sekwencji, a jeśli chcesz któryś usunąć, użyj przycisku **Delete reader (Usuń czytnik)**.



Przypisywanie trasy do osoby

Aby przypisać trasę do osoby:

1. W menu głównym kliknij kolejno opcje **Dane osobowe** > **Karty**.
2. Załaduj zestaw danych osobowych osoby, którą chcesz przypisać.
3. Na karcie **Inne dane** zaznacz pole wyboru **Monitoring trasy**.
4. Z listy rozwijanej obok wybierz zdefiniowaną trasę (więcej informacji na temat definiowania trasy znajdziesz w poprzednim rozdziale).
5. Zapisz dane osobowe.

Uaktywnienie trasy następuje, gdy osoba przypisana użyje pierwszego czytnika leżącego na trasie. Pozostał czytniki na trasie muszą teraz zostać użyte w odpowiedniej kolejności, tj. tylko następny czytnik w sekwencji pozwoli użytkownikowi przejść danej. Po przejściu całej trasy osoba może używać dowolnych innych czytników mieszczących się w obrębie jej uprawnień.

Poprawianie i monitorowanie tras

1. W menu głównym wybierz kolejno opcje **Monitoring trasy** > **Popraw trasy**.
2. Załaduj zestaw danych osobowych osoby przypisanej do trasy.
3. Aby znaleźć osobę na trasie, kliknij przycisk **Określ lokalizację**.
4. Użyte czytniki są oznaczane na liście zielonym znacznikiem ✔.
5. Aby zresetować lub poprawić lokalizację osoby na trasie, kliknij przycisk **Ustaw lokalizację**.

22 Losowa kontrola osób

Procedura losowej kontroli

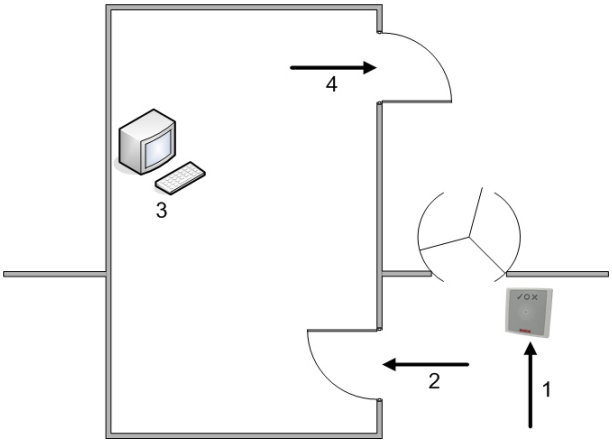
1. Posiadacz karty przykłada ją do czytnika, w którym skonfigurowano losową kontrolę.
   Uwaga
   Wybór losowy obejmuje tylko osoby uprawnione do przechodzenia przez wejście w wyznaczonym kierunku. Sprawdzanie uprawnień odbywa się przed losową kontrolą, więc wszystkie nieupoważnione osoby zostaną natychmiast zatrzymane i nie będą objęte procedurą wyboru.
2. Jeśli układ losujący wybierze daną osobę do kontroli, jej karta zostanie zablokowana w całym systemie.
   - To zdarzenie jest rejestrowane w dzienniku zdarzeń systemu.
   - Do okna dialogowego **Blokowanie** trafia wpis o nieograniczonym czasie trwania, oznaczony etykietą **Losowa kontrola**. [Poniższy rysunek – numer 1]
   - Na pasku stanu w oknach dialogowych danych osobowych w pakiecie Access Engine wyświetlane są „kontrolki” oznaczające stany Zablokowane (czerwona) i Losowa kontrola (migająca fioletowa).

Uwaga!
Osoby, którym ustawiono parametr **Wykluczono z losowej kontroli** (na karcie **Inne dane** w oknie dialogowym **Karty**), nie są uwzględniane w ramach procedury kontroli.

3. Losowo wybrana osoba jest zapraszana na dodatkowe czynności sprawdzające w oddzielnym pomieszczeniu pracowników ochrony.
4. Po wykonaniu tych czynności sprawdzających pracownik ochrony resetuje blokadę w oknie dialogowym **Blokowanie** w następujący sposób:
   - Wybiera odpowiednią blokadę na liście **Blokowanie**.
   - Klika przycisk **Usuń**.
   - Potwierdza usunięcie, klikając przycisk **Tak**.

Osoba poddana losowej kontroli może teraz ponownie używać swojej karty we wszystkich czytnikach, do korzystania z których ma uprawnienia.

Przykładowy układ pomieszczenia do losowej kontroli



1 = Przyłożenie karty — kontrola — blokada w całym systemie
2 = Posiadacz karty wchodzi do pomieszczenia pracowników ochrony
3 = Następuje przeszukanie posiadacza karty, a następnie usunięcie blokady z jego karty w odpowiednim oknie dialogowym.

4 = Posiadacz karty opuszcza pomieszczenie pracowników ochrony bez ponownego przykładania karty do czytnika.

Uwaga!
Procent kontroli jest osiągany łącznie w przedziale czasu. Na przykład przy 10-procentowej losowej kontroli nadal istnieje możliwość (1 na 100, czyli 1/10 x 1/10), że zostaną wybrane dwie kolejne osoby.

23 Korzystanie z przeglądarki zdarzeń

Wstęp

Przeglądarka zdarzeń umożliwia odpowiednio upoważnionym operatorom badanie zdarzeń zarejestrowanych przez system oraz tworzenie raportów drukowanych lub wyświetlanych na ekranie.

Aby pobrać i wyświetlić żądane rekordy z bazy danych dziennika zdarzeń, ustaw kryteria filtrowania i kliknij przycisk **Odśwież** .

Kryteria filtrowania można ustawiać na różne sposoby:

Relatywne Wybieranie zdarzeń dotyczących obecnego czasu.

Interwał Wybieranie zdarzeń w dowolnie definiowalnym przedziale czasu.

Łącznie Wybieranie zdarzeń niezależnie od czasu ich wystąpienia.

Wymagania wstępne

Jesteś użytkownikiem zalogowanym w menedżerze okien dialogowych.

Ścieżka w oknie dialogowym

Menu główne menedżera okien dialogowych > **Raporty** > **Przeglądarka zdarzeń**

23.1 Ustawianie kryteriów filtrowania dla czasu względem teraźniejszości

1. W obszarze **Przedział czasu** zaznacz przycisk radiowy **Relatywne**.
2. W polu **Wyszukaj w ostatniej** ustaw liczbę jednostek czasu, w granicach której ma być prowadzone wyszukiwanie, oraz wybierz jednostki, które mają być używane, na przykład tygodnie, dni, godziny, minuty lub sekundy.
3. W menu **Typy zdarzeń** wybierz kategorię zdarzeń, która ma być przeszukiwana, a następnie typy zdarzeń, które Cię interesują.
4. W menu **Maksymalna liczba** ogranicz liczbę zdarzeń, która ma zostać przekazana do przeglądarka zdarzeń. Ze względu na wydajność **nie** zaleca się pozostawiania wartości **(Nieograniczona)**.
5. W razie potrzeby określ inne kryteria filtrowania:
   - Nazwisko
   - Imię
   - Numer personalny
   - Nr karty
   - Użytkownik (czyli operator systemu)
   - Dane kodowania
   - Nazwa urządzenia
   - Nazwa obszaru

- Kliknij przycisk **Odśwież** , aby rozpocząć zbieranie informacji o zdarzeniach, a potem w razie potrzeby przycisk **Anuluj**, aby zatrzymać operację.
- Kliknij przycisk , aby zapisać wyniki, lub przycisk , aby je wydrukować.
- Kliknij przycisk , aby wyczyścić wyniki w przygotowaniu na nowe wyszukiwanie.

23.2 Ustawianie kryteriów filtrowania według przedziału czasu

1. W obszarze **Przedział czasu** zaznacz przycisk radiowy **Interwał**.
2. W selektorach dat **Od czasu, Czas do** zdefiniuj początek i koniec okresu, w którym chcesz szukać zdarzeń.
3. W menu **Typy zdarzeń** wybierz kategorię zdarzeń, która ma być przeszukiwana, a następnie typy zdarzeń, które Cię interesują.
4. W menu **Maksymalna liczba** ogranicz liczbę zdarzeń, która ma zostać przekazana do przeglądarka zdarzeń. Ze względu na wydajność **nie** zaleca się pozostawiania wartości **(Nieograniczona)**.
5. W razie potrzeby określ inne kryteria filtrowania:
   - Nazwisko
   - Imię
   - Numer personalny
   - Nr karty
   - Użytkownik (czyli operator systemu)
   - Dane kodowania
   - Nazwa urządzenia
   - Nazwa obszaru

- Kliknij przycisk **Odśwież**  , aby rozpocząć zbieranie informacji o zdarzeniach, a potem w razie potrzeby przycisk **Anuluj**, aby zatrzymać operację.
- Kliknij przycisk  , aby zapisać wyniki, lub przycisk  , aby je wydrukować.
- Kliknij przycisk  , aby wyczyścić wyniki w przygotowaniu na nowe wyszukiwanie.

23.3 Ustawianie kryteriów filtrowania niezależnie od czasu

1. W obszarze **Przedział czasu** zaznacz przycisk radiowy **Łącznie**.
2. W menu **Typy zdarzeń** wybierz kategorię zdarzeń, która ma być przeszukiwana, a następnie typy zdarzeń, które Cię interesują.
3. W menu **Maksymalna liczba** ogranicz liczbę zdarzeń, która ma zostać przekazana do przeglądarka zdarzeń. Ze względu na wydajność **nie** zaleca się pozostawiania wartości **(Nieograniczona)**.
4. W razie potrzeby określ inne kryteria filtrowania:
   - Nazwisko
   - Imię
   - Numer personalny
   - Nr karty
   - Użytkownik (czyli operator systemu)
   - Dane kodowania
   - Nazwa urządzenia
   - Nazwa obszaru

- Kliknij przycisk **Odśwież**  , aby rozpocząć zbieranie informacji o zdarzeniach, a potem w razie potrzeby przycisk **Anuluj**, aby zatrzymać operację.

– Kliknij przycisk  , aby zapisać wyniki, lub przycisk  , aby je wydrukować.

– Kliknij przycisk  , aby wyczyścić wyniki w przygotowaniu na nowe wyszukiwanie.

24 Używanie raportów

W tej sekcji opisano zbiór funkcji raportów, których można używać do filtrowania danych dziennika systemu i dziennika zdarzeń oraz do ich przedstawienia w czytelnych formatach.

Ścieżka w oknie dialogowym

Menu główne > **Raporty**.

Korzystanie z paska narzędzi raportów

Kliknij przycisk  , aby wyświetlić podgląd przed drukowaniem.

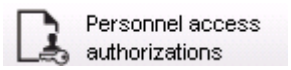
W oknie podglądu znajduje się specjalny pasek narzędzi:

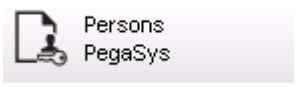
- Kliknij przycisk ✕, aby wyjść z okna podglądu bez drukowania.
- Za pomocą przycisków strzałek ⏮ ◀ 2 of 17 ▶ ⏭ na pasku narzędzi podglądu można przeglądać w przód i w tył oraz wybierać pojedyncze strony po ich numerach.
- Kliknij przycisk  , aby natychmiast rozpocząć drukowanie na domyślnej drukarce.
- Kliknij przycisk  , aby wydrukować za pośrednictwem okna dialogowego Ustawienia drukowania, w którym można skonfigurować więcej opcji drukowania.
- Kliknij przycisk  , aby wyeksportować raport do wybranego formatu pliku, w tym PDF, RTF lub Excel.
- Liczby po prawej stronie paska narzędzi reprezentują:
  - Łączną liczbę istniejących wpisów bazy danych, które odpowiadają kryteriom filtru.
  - Procent tych wpisów bazy danych, które są wyświetlane w podglądzie.

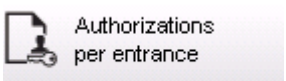
24.1 Raporty: dane główne

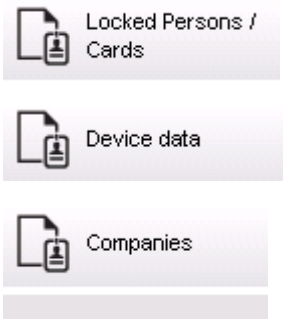
Omówienie raportów — dane główne

Do raportów danych głównych należą wszystkie raporty dotyczące osób, gości, kart i ich uprawnień dostępu. Ponadto wyświetlane mogą być w nich dane o urządzeniach i firmach.









Raport: Dane osobowe
Przy tworzeniu raportów można stosować dwa filtry.
Filtr osób: Tutaj operator filtruje na podstawie typowych pól w zestawie danych osobowych.
Filtr kart dostępu: W tym miejscu operator może filtrować na podstawie numerów kart, zakresów numerów, statusu i statusu blokowania.

Raport: Goście
Można tu tworzyć raporty o gościach w analogiczny sposób jak w przypadku raportów z danymi osobowymi. Możliwy jest przy tym dostęp do wszystkich utworzonych danych gości, tzn. można wybierać nawet gości, którzy jeszcze wprawdzie nie dotarli na miejsce, ale zostali już zarejestrowani w systemie.

Raport: Uprawnienia dostępu personelu
Ten raport zapewnia wgląd w zarejestrowane w systemie uprawnienia dostępu oraz wskazuje osoby, którym je przyznano.
Można stosować filtry związane z danymi osobowymi i poszczególnymi uprawnieniami:
- Dane osobowe: nazwisko, imię, numer personalny.
- Termin ważności wszystkich uprawnień.
- Nazwa uprawnienia obejmującego dane wejście.
- Nazwa modelu czasowego — jeśli występuje.
- Kierunek wejścia.
- Termin ważności uprawnień specjalnych.

Raport: Czarna lista
W tym oknie dialogowym można wydrukować listę zawierającą wszystkie lub wybrane karty identyfikacyjne, które z różnych powodów zostały umieszczone na czarnej liście.

Raport: Osoby zablokowane/karty
To okno dialogowe służy do tworzenia raportów zawierających wszystkie zablokowane osoby. Za pomocą dat można wyszukiwać blokady istniejące w określonych przedziałach czasu.

Raport: Dane urządzenia
To okno dialogowe może służyć do tworzenia raportów na podstawie danych urządzenia, np. jego nazwy lub typu.

Raport: Firmy
Okno dialogowe raportu Firmy umożliwia przedstawianie danych firm w formie listy.

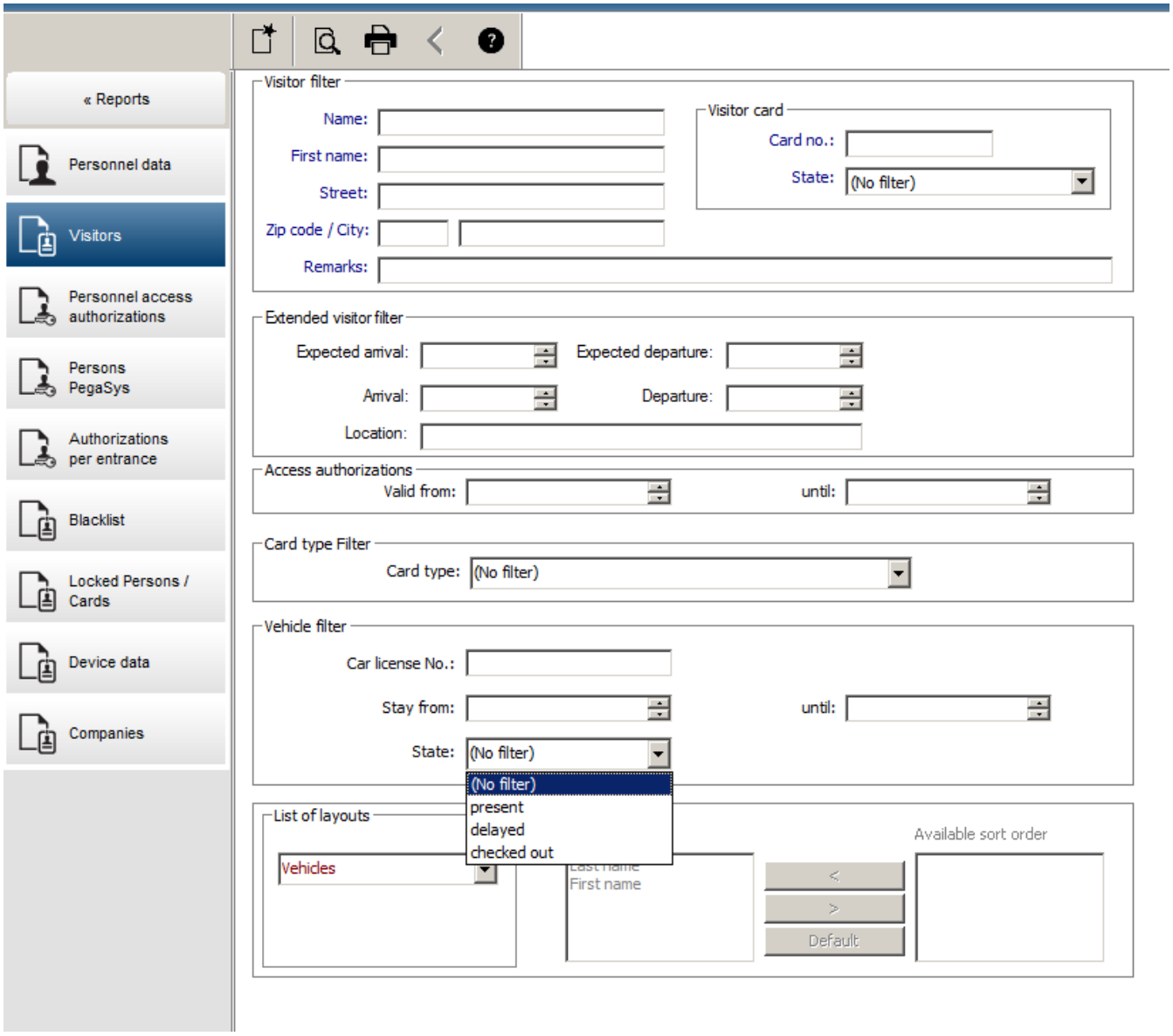
Używając gwiazdek, można na przykład wyszukać firmy, których nazwy zaczynają się określoną literą.

24.1.1 Raportowanie o pojazdach

W oknie dialogowym **Raporty > Goście** można wybrać z listy układów pozycję **Pojazdy**. Po jej wybraniu zostaje uaktywniony obszar dialogowy **Filtr pojazdów**, w którym można odfiltrowywać pojazdy i ich stan.

Stan jest podawany w następujący sposób:

- Obecne: wizyta jeszcze się nie zakończyła, a jej spodziewany czas jeszcze nie minął.
- Opóźnione: wizyta jeszcze się nie zakończyła, ale jej spodziewany czas już minął.
- Wyewidencjonowane: gość zwrócił wszystkie karty dostępu.

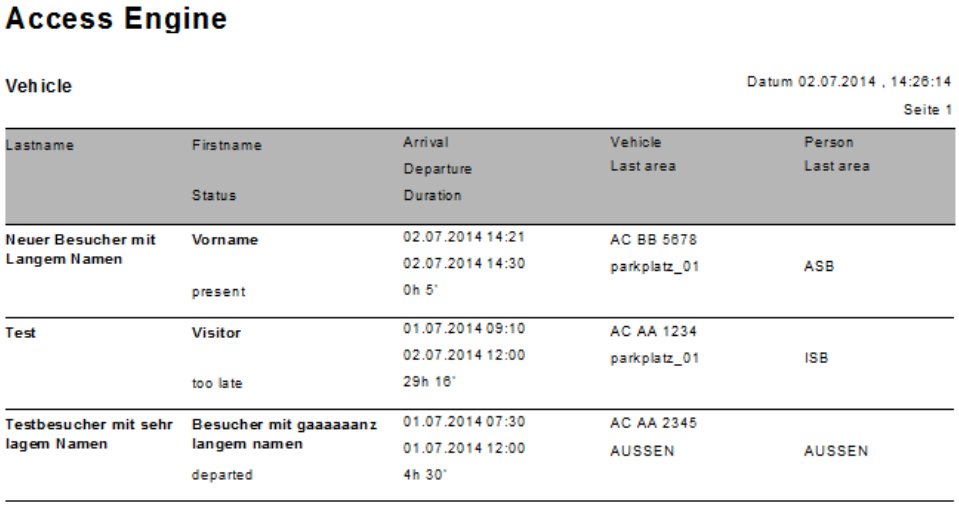


Raport dotyczący pojazdów jest dostępny tylko w przypadku gości, ponieważ takie parametry jak spodziewana data wejścia, spodziewana data wyjścia, data wejścia i data wyjścia odnoszą się wyłącznie do gości, a znajdują w tabeli bazy danych **Goście**.

Raport ten zawiera tylko listę numerów rejestracyjnych pojazdów, które są przechowywane w tabeli bazy danych **Osoby**. Jeśli więc numer rejestracyjny pojazdu uległ zmianie, raport będzie podawać nieprawidłowe dane.

Czas trwania jest obliczany w następujący sposób:

– jeśli gość został już wyewidencjonowany, wyświetlana jest różnica między wejściem a wyjściem w minutach;
– jeśli gość nie został jeszcze wyewidencjonowany, wyświetlany jest czas, jaki upłynął do tej pory od wejścia gościa.



Access Engine

Vehicle

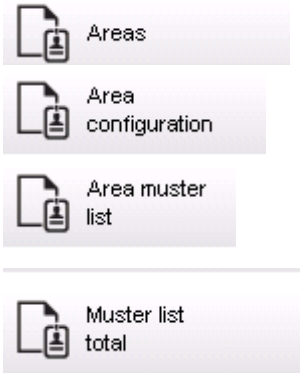
Datum 02.07.2014 , 14:26:14
Seite 1

Lastname	Firstname Status	Arrival Departure Duration	Vehicle Last area	Person Last area
Neuer Besucher mit Langem Namen	**Vorname** present	02.07.2014 14:21 02.07.2014 14:30 0h 5'	AC BB 5678 parkplatz_01	ASB
Test	**Visitor** too late	01.07.2014 09:10 02.07.2014 12:00 29h 16'	AC AA 1234 parkplatz_01	ISB
Testbesucher mit sehr lagem Namen	**Besucher mit gaaaaaanz langem namen** departed	01.07.2014 07:30 01.07.2014 12:00 4h 30'	AC AA 2345 AUSSEN	AUSSEN

24.2 Raporty: dane systemowe

Raporty — dane systemowe

W odróżnieniu od danych głównych dane systemowe to informacje, które są przypisane do systemu i niezwiązane z osobą, identyfikatorem czy też firmą. Bardziej szczegółowe objaśnienie tych raportów znajduje się poniżej.



Raport: Obszary

To okno dialogowe służy do przedstawiania lokalizacji w formie raportu. Znajduje się tu tylko jeden filtr obszarów, który umożliwia wybór różnych budynków i innych stref.

Dany obszar wybiera się, klikając go lewym przyciskiem myszy. Przed wydrukowaniem raportu (za pomocą przycisku **Drukuj**) użytkownik może go wyświetlić na ekranie, klikając przycisk **Podgląd**.

Dostępne są dwa układy.

	Standardowy	Osoby obecne w lokalizacji — brak parkingów

	Obłożenie parkingu	Osoby obecne w lokalizacji – tylko parkingi

Aby umożliwić sprawdzanie, czy wyświetlane zestawy danych są aktualne, podawane są również ostatnie skanowania kart na wybranych obszarach.
Dzięki temu można w przypadku różnorodnych zdarzeń dysponować wiarygodnymi informacjami na temat miejsc pobytu poszczególnych osób.

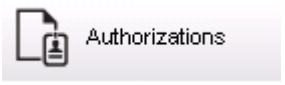
Raport: Konfiguracja obszarów
Wyznaczone obszary i ich podobszary z parkingami oznaczonymi flagami oraz maksymalna liczba osób lub pojazdów.

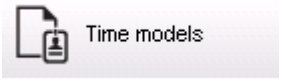
Raport: Lista obecności na obszarze
Lista osób na danym obszarze może być przedstawiana nie tylko zgodnie z czystymi danymi numerycznymi, ale również według nazwiska.
Dzięki godzinom skanowania na poszczególnych obszarach raporty zawierają także dane czasowe dotyczące każdej osoby.

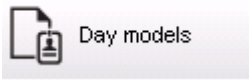
Raport: Lista obecności ogółem
Listy obecności odpowiadają z reguły oknu dialogowemu raportu **Obszary**. Udostępniają one też jednak listy dotyczące konkretnych stref, dzięki czemu uzyskuje się liczbę osób, które według systemu kontroli znajdują się aktualnie na danym obszarze.

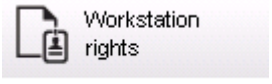
24.3 Raporty: uprawnienia

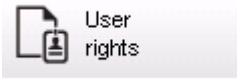
Przegląd
Korzystając z tej pozycji menu, można uzyskać wgląd w różne uprawnienia przyznane w odpowiednich oknach dialogowych:

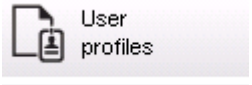












Raport: Uprawnienia
To okno dialogowe służy do wyświetlania uprawnień dostępu zdefiniowanych w systemie. Podane są w nim wejścia należące do poszczególnych uprawnień dostępu. Widoczna jest też nazwa wybranego modelu czasowego. Dodatkowo w raporcie tym wyświetlana jest liczba osób, którym przyznano uprawnienia.

Raport: Modele czasowe
Ten raport służy do wyświetlania wybranych modeli czasowych zdefiniowanych w systemie. Widoczne są w nim wszystkie dane związane z modelem oraz liczba osób, do których jest on przypisany.

Raport: Modele dzienne
W tym raporcie widoczne są wszystkie zdefiniowane modele dzienne razem z ich nazwami, opisami i zawartymi w nich przedziałami czasu.

Raport: Prawa stacji roboczej
To okno dialogowe służy do wyświetlania uprawnień stacji roboczych przypisanych w systemie stacjom roboczym.

Raport: Profile stacji roboczej
To okno dialogowe służy do wyświetlania zdefiniowanych w systemie profili stacji roboczych. Zapewnia to czytelny wgląd w operacje, jakie są możliwe na poszczególnych stacjach roboczych.

Raport: Uprawnienia użytkownika
To okno dialogowe służy do wyświetlania zdefiniowanych w systemie profili użytkowników przypisanych użytkownikom.

Raport: Profile użytkownika
To okno dialogowe służy do wyświetlania okien dialogowych i uprawnień do okien dialogowych przypisanych do profili użytkowników, które są zdefiniowane w systemie.

25 Używanie funkcji zarządzania poziomami zagrożenia

W tej sekcji opisano różne sposoby wywoływania poziomu zagrożenia i anulowania go. Informacje ogólne można znaleźć w sekcji *Konfigurowanie funkcji zarządzania poziomem zagrożenia, Strona 116*.

Wstęp

Poziom zagrożenia jest uaktywniany przez alert zagrożenia. Alert zagrożenia może być inicjowany na jeden z następujących sposobów:

- Polecenie w interfejsie użytkownika oprogramowania
- Sygnał wejściowy zdefiniowany w lokalnym kontrolerze dostępu, np. przyciskiem
- Przeciągnięcie karty alarmowej przez czytnik

Należy pamiętać, że alerty zagrożenia mogą być anulowane przez polecenie interfejsu użytkownika lub sygnał sprzętowy, ale nie przez kartę alarmową.

Patrz

- *Konfigurowanie funkcji zarządzania poziomem zagrożenia, Strona 116*

25.1 Wyzwalanie i anulowanie alertu zagrożenia za pomocą polecenia interfejsu użytkownika

W tej sekcji opisano sposób inicjowania alertu zagrożenia w aplikacji AMS Map View.

Ścieżka w oknie dialogowym

- AMS Map View >  (drzewo urządzeń)

Wymagania wstępne

- Zdefiniowany co najmniej jeden poziom zagrożenia
- Co najmniej jeden poziom zagrożenia został w edytorze urządzeń oznaczony jako aktywny.
- Operator aplikacji Map View i systemu AMS (czyli Ty) ma niezbędne uprawnienia:
  - do obsługi poziomów zagrożenia
  - do wyświetlania kontrolerów MAC w strefie, w której ma zostać zainicjowany alert zagrożenia

Procedura wyzwalania alertu zagrożenia

1. W aplikacji AMS Map View w drzewie urządzeń kliknij prawym przyciskiem myszy urządzenie MAC, na którym ma zostać wywołany alert zagrożenia.
   - Zostanie wyświetlone menu kontekstowe zawierające polecenia, które masz prawo wykonywać na tym kontrolerze MAC.
   - Jeśli żaden poziom zagrożenia nie jest jeszcze aktywny, w menu zobaczysz jeden lub więcej elementów podpisanych **Włącz poziom zagrożenia** „<name>”, gdzie <name> to nazwa poziomu zagrożenia zdefiniowanego w edytorze urządzeń.
2. Zaznacz poziom zagrożenia, który chcesz zainicjować.
   - Poziom zagrożenia zostanie uaktywniony.

Procedura anulowania alertu zagrożenia

Warunek wstępny: poziom zagrożenia jest już aktywny.

1. W aplikacji AMS Map View w drzewie urządzeń kliknij prawym przyciskiem myszy urządzenie MAC, na którym ma zostać anulowany alert zagrożenia.

– Zostanie wyświetlone menu kontekstowe zawierające polecenia, które masz prawo wykonywać na tym kontrolerze MAC.

2. Kliknij opcję **Wyłącz poziom zagrożenia** widoczną w menu kontekstowym.
   – Aktualnie aktywny poziom zagrożenia zostanie wyłączony.

25.2 Wyzwalanie alertu zagrożenia przez sygnał sprzętowy

W tej sekcji opisano, jak wysłać wejściowy sygnał sprzętowy w celu wywołania alertu zagrożenia.

Wymagania wstępne

– Zdefiniowany co najmniej jeden poziom zagrożenia
– Skonfigurowane co najmniej jedno wejście w drzewie urządzeń
– Na kontrolerze AMC zdefiniowano sygnały sprzętowe, a do odpowiedniego terminala tego kontrolera AMC podłączono urządzenie, które wyśle sygnał. W razie potrzeby kliknij łącze na końcu tej sekcji, aby się dowiedzieć, jak skonfigurować sygnał wejściowy, lub skontaktuj się z administratorem systemu.

Procedura

Aktywuj urządzenie, zazwyczaj przycisk lub przełącznik sprzętowy, który jest podłączone do kontrolera AMC.
Aby anulować alert zagrożenia, aktywuj urządzenie wysyłające sygnał wejściowy zdefiniowany jako **Poziom zagrożenia: wyłącz**.

Patrz

– *Przypisywanie poziomu zagrożenia do sygnału sprzętowego, Strona 120*

25.3 Wyzwalanie alertu zagrożenia za pomocą karty alarmowej

W tej sekcji opisano sposób wywoływania alertu zagrożenia za pomocą karty alarmowej.

Wymagania wstępne

– Zdefiniowany co najmniej jeden poziom zagrożenia
– Skonfigurowane co najmniej jedno wejście w drzewie urządzeń
– Utworzono kartę alarmową dla konkretnego posiadacza karty. W razie potrzeby kliknij łącze na końcu tej sekcji, aby się dowiedzieć, jak utworzyć kartę alarmową, lub skontaktuj się z administratorem systemu.

Procedura

1. Posiadacz karty przykłada swoją specjalną kartę alarmową do dowolnego czynnika **innego niż czytnik odcisku palca** istniejącego w obiekcie.
   – Zostanie uaktywniony poziom zagrożenia zdefiniowany dla tej karty.
2. Po wygaśnięciu zagrożenia anuluj poziom zagrożenia za pomocą polecenia interfejsu użytkownika lub przełącznika sprzętowego. Nie ma technicznej możliwości anulowania poziomu zagrożenia za pomocą karty alarmowej.

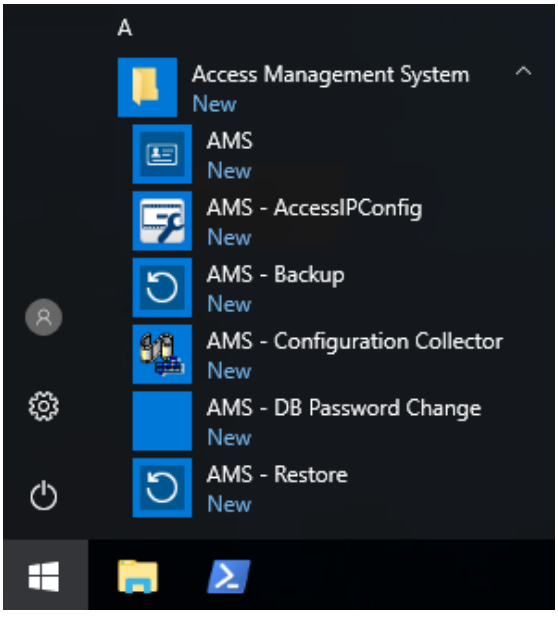
Patrz

– *Tworzenie karty alarmowej, Strona 135*

26 Tworzenie kopii zapasowych i ich przywracanie

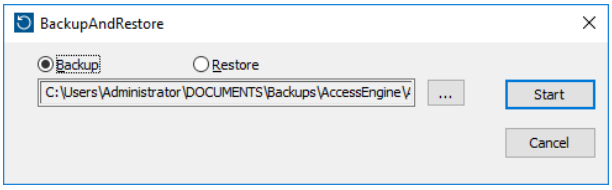
Funkcja **Tworzenie kopii zapasowych i ich przywracanie** umożliwia zrekonstruowanie instalacji na innym komputerze, jeśli oryginalny komputer ulegnie awarii.
Funkcję **Tworzenie kopii zapasowych i ich przywracanie** można uruchomić tylko na komputerze, na którym jest zainstalowany serwer systemu AMS. Dla wygody są tworzone dwa skróty:

- **AMS — Kopia zapasowa** do tworzenia kopii zapasowej
- **AMS — Przywracanie** do przywracania kopii zapasowej:

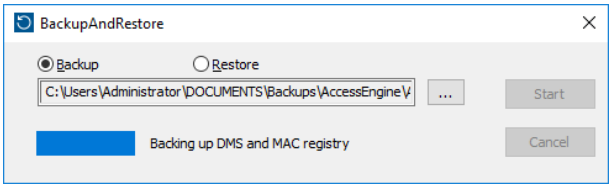


26.1 Procedura tworzenia kopii zapasowej

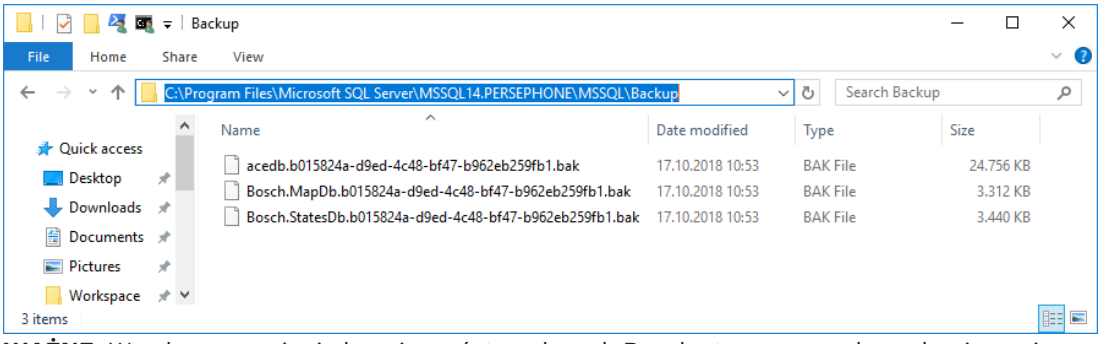
1. Kliknij skrót **AMS — Kopia zapasowa**.
   Spowoduje to uruchomienie narzędzie **Tworzenie kopii zapasowych i ich przywracanie**:



2. Wprowadź ścieżkę, w której ma zostać zapisany plik GZIP.
3. Kliknij przycisk **Rozpocznij**, aby rozpocząć tworzenie kopii zapasowej.
   Zostanie wyświetlony pasek postępu.
   Po zakończeniu procesu zostanie utworzony plik GZIP.



Lokalizacja kopii zapasowej bazy danych zależy od wersji programu SQL Server i nazwy instancji bazy danych.
Na przykład jeśli nazwa instancji bazy danych SQL w systemie AMS to „PERSEPHONE”, kopia zapasowa będzie się znajdować w ścieżce:



WAŻNE: W celu zapewnienia bezpieczeństwa danych Bosch stanowczo zaleca skopiowanie tego folderu i pliku GZIP do bezpiecznej, odległej lokalizacji. Nie pozostawiaj jedynej kopii zapasowej na komputerze serwera systemu DMS.

Uwaga!
Dziennik zdarzeń jest zapisywany w następującej domyślnej ścieżce (instalator mógł wybrać inną ścieżkę):
`C:\Program Files (x86)\Access Management System\Access Engine\AC\LgfLog\`

26.2 Procedura przywracania

Wymagania wstępne

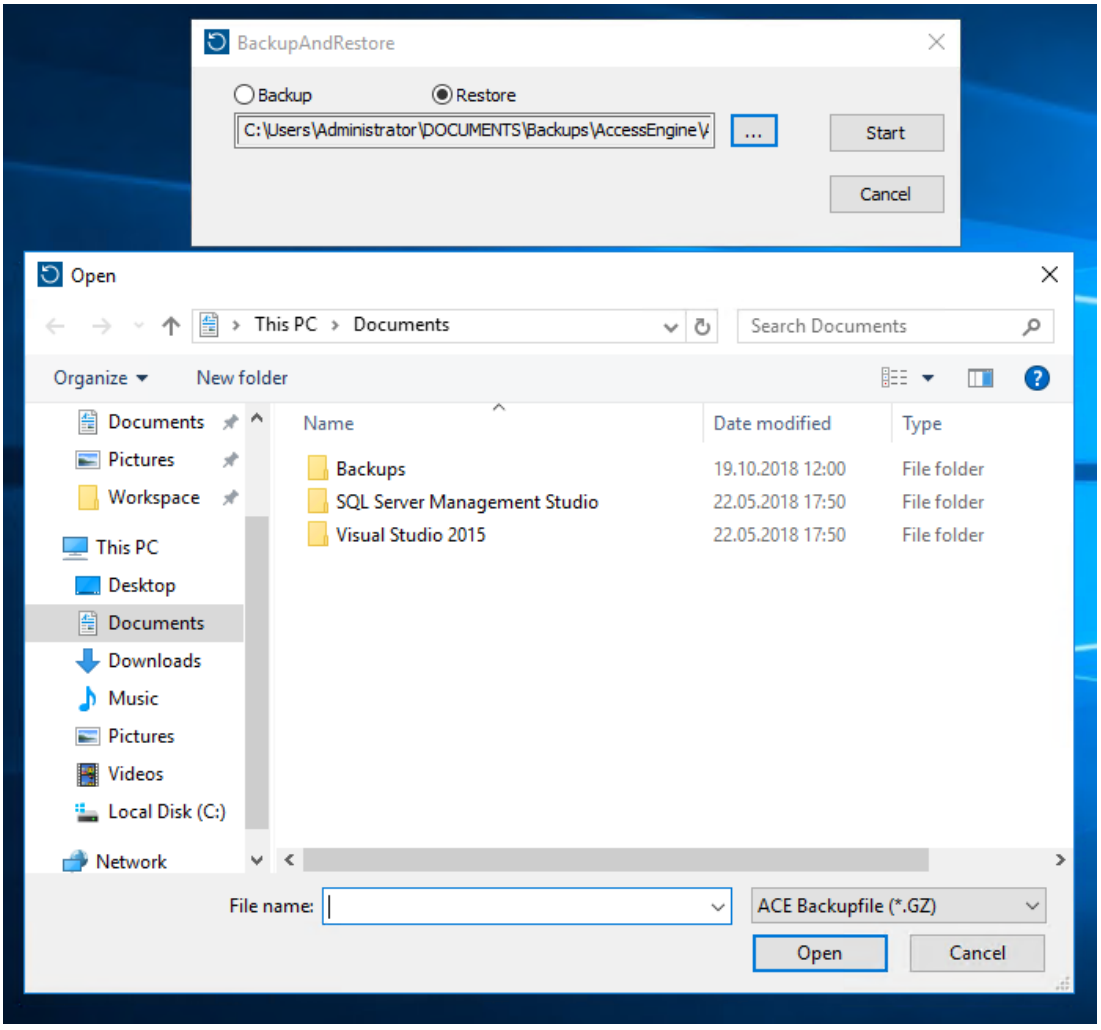
- Plik GZIP utworzony przez narzędzie **Tworzenie kopii zapasowych i ich przywracanie**.
- Dane kopii zapasowej utworzone przez program SQL Server w folderze kopii zapasowej programu SQL Server.
- Konto w programie SQL z uprawnieniami **sysadmin**, takie jak `sa`.

Uwagi na temat komputera docelowego

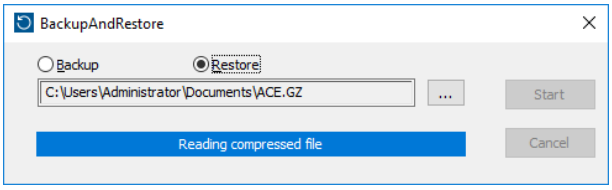
- Aby można było uruchomić przywróconą konfigurację, komputer docelowy (na którym przywracasz kopię zapasową) musi mieć co najmniej takie same licencje, jak istniejące na komputerze, na którym wykonano kopię zapasową.
- Wszystkie urządzenia klienckie komputera docelowego będą wymagały certyfikatów wygenerowanych przez instalację na komputerze docelowym, a nie na oryginalnym komputerze.
  Instalowanie certyfikatów klientów jest omówione w podręczniku instalacji.

Procedura

1. W programie AMS kliknij kolejno opcje **Plik** > **Zakończ**, aby zatrzymać wszystkie uruchomione usługi.
2. Po zakończeniu działania programu uruchom aplikację systemu Windows **Usługi** i sprawdź, czy wszystkie usługi systemów `Access Engine` i `Access Management System` zostały zatrzymane.
3. Kliknij przycisk Start w systemie Windows > **AMS — Przywracanie**.
4. Kliknij przycisk **[...]**, poszukaj pliku kopii zapasowej GZIP i go zaznacz.



5. Kliknij przycisk **Rozpocznij**, aby rozpocząć proces przywracania.
6. Wprowadź poświadczenia logowania **użytkownika sysadmin programu SQL**.
   Rozpocznie się proces przywracania.



7. Po zakończeniu procesu przywracania uruchom aplikację systemu Windows **Usługi** i sprawdź, czy wszystkie usługi systemów `Access Engine` i `Access Management System` zostały ponownie uruchomione.
   Jeśli nie, zrestartuj je ręcznie.
8. Na pulpicie uruchom aplikację **AMS Map View**.
9. W aplikacji Map View odszukaj kontroler MAC i kliknij go prawym przyciskiem myszy.
10. Wybierz opcję **Zimny start MAC**, aby ponownie zsynchronizować dane kopii zapasowej z bieżącymi danymi systemowymi.

Słowniczek

1. MAC (pierwszy kontroler MAC)

Główny kontroler MAC (Master Access Controller) w systemie BIS Access Engine (ACE) lub Access Manager (AMS). Może się znajdować na tym samym komputerze, co system DMS, ale może być również zainstalowany — podobnie jak dodatkowy kontroler MAC — na oddzielnym komputerze nazywanym serwerem kontrolera MAC.

Alert zagrożenia

Alarm wyzwalający poziom zagrożenia. Odpowiednio uprawnione osoby mogą inicjować alert zagrożenia jedną czynnością, np. w interfejsie operatora, sygnałem sprzętowym (np. przyciskiem) lub przykładając specjalną kartę alarmową do dowolnego czytnika.

Automatyczne rozpoznawanie tablic rejestracyjnych (ANPR)

Wykorzystanie technologii wideo do odczytywania i przetwarzania numerów tablic rejestracyjnych, zazwyczaj pojazdów drogowych.

Biała lista (SmartIntego)

Biała lista to lista numerów kart przechowywanych lokalnie na czytnikach kart w systemie blokowania SmartIntego. Jeśli sterownik MAC czytnika jest w trybie offline, czytnik udziela dostępu kartom, których numery są w jego lokalnej białej liście.

Data Management System (DMS)

Nadrzędny procesu zarządzania danymi kontroli dostępu w systemie Access Engine. System DMS dostarcza dane do kontrolerów MAC, które z kolei dostarczają dane do kontrolerów AMC.

Data Management System (DMS)

Nadrzędny procesu zarządzania danymi kontroli dostępu w systemie Access Engine. System DMS dostarcza dane do kontrolerów MAC, które z kolei dostarczają dane do kontrolerów AMC.

Funkcja zapobiegająca przekazaniu karty osobie niepowołanej/podwójnemu przejściu

Prosta forma monitorowania sekwencji dostępu, w której posiadacz karty nie może wejść do obszaru dwa razy w określonym przedziale czasu, chyba że w międzyczasie zeskanowano kartę na wyjściu z tego obszaru. Funkcja zapobiegająca podwójnemu przejściu zniechęca osobę do przekazania swoich poświadczeń nieuprawnionej osobie znajdującej się przed wejściem.

IDS (SSW)

System sygnalizacji włamania, nazywany również jako systemem alarmu włamaniowego.

Kod identyfikacyjny PIN

Osobisty numer identyfikacyjny (ang. Personal Identification Number, PIN), który jest jedynym poświadczeniem niezbędnym do uzyskania dostępu.

Kod weryfikacyjny PIN

Osobisty numer identyfikacyjny używany w połączeniu z poświadczeniem fizycznym w celu zapewnienia wyższego poziomu bezpieczeństwa.

Lokalny kontroler dostępu (LAC)

Urządzenie sprzętowe, które wysyła polecenia dostępu do peryferyjnych urządzeń kontroli dostępu, takich jak czytniki i zamki, oraz przetwarza żądania z tych urządzeń dla całościowego systemu kontroli dostępu. Najpopularniejszym kontrolerem LAC jest modułowy kontroler dostępu, czyli AMC.

MAC (główny kontroler dostępu)

W systemach kontroli dostępu program serwerowy, który koordynuje i kontroluje lokalne kontrolery dostępu, zwykle AMC (modułowe kontrolery dostępu).

Miejsce (punkt) zbiórki

Wyznaczony obszar, do którego zgodnie z instrukcjami ludzie się kierują i tam mają czekać na ewakuację z budynku.

Model drzwi

Zapisany szablon oprogramowania określonego typu wejścia. Modele drzwi ułatwiają definiowanie wejść w systemach kontroli dostępu.

Monitorowanie sekwencji dostępu

Śledzenie osoby lub pojazdu przemieszczającego się z jednego zdefiniowanego obszaru do innego poprzez rejestrowanie każdego skanu karty identyfikacyjnej i przyznawanie dostępu tylko z obszarów, w których karta została już zeskanowana.

przemykanie

Obchodzenie systemu kontroli dostępu poprzez podążanie bardzo blisko za uprawnionym posiadaczem karty bez okazywania własnych danych uwierzytelniających na wejściu.

RMAC

Nadmiarowy główny kontroler dostępu (MAC), który jest synchronizowanym bliźniakiem istniejącego kontrolera MAC i przejmuje zarządzanie jego danymi, jeśli pierwszy kontroler MAC ulegnie awarii lub zostanie rozłączony.

Serwer kontrolera MAC

Sprzęt: Komputer w sieci systemu Access Engine, oddzielony od serwera systemu DMS, na którym działa kontroler MAC lub RMAC.

SmartIntego

Cyfrowy system blokowania w technologii Simons Voss. System SmartIntego jest zintegrowany z niektórymi systemami kontroli dostępu firmy Bosch.

Tryb biuro

Zawieszenie kontroli dostępu przy wejściu w godzinach pracy biura.

Tryb normalny

W przeciwieństwie do trybu Biuro w trybie normalnym udziela się dostępu tylko osobom, które zaprezentują w czytniku prawidłowe poświadczenia.

Wejście

Określenie „wejście” oznacza cały mechanizm kontroli dostępu w punkcie wejścia. Obejmuje czytniki, pewną formę blokowanej bariery oraz procedurę dostępu zdefiniowaną przez sekwencje sygnałów elektronicznych przekazywanych między elementami sprzętowymi.

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com