Access Management System V5.2

Konfiguracja i obsługa

pl Software manual

Spis treści

1 Zabezpieczenia

Użyj najnowszego oprogramowania

Przed pierwszym rozpoczęciem obsługi urządzenia należy upewnić się, że jest instalowana najnowsza dostępna wersja oprogramowania. Aby zapewnić spójność działania, zgodność, wydajność i bezpieczeństwo, oprogramowanie należy regularnie aktualizować przez cały okres eksploatacji urządzenia. Należy postępować zgodnie z instrukcjami podanymi w dokumentacji produktu w zakresie aktualizacji oprogramowania.

Więcej informacji można znaleźć w następujących miejscach:

– Informacje ogólne: https://www.boschsecurity.com/xc/en/support/product-security/
– Forum bezpieczeństwa, czyli lista rozpoznanych zagrożenia i proponowanych rozwiązań: https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

Firma Bosch nie ponosi odpowiedzialności za szkody spowodowane korzystaniem ze starej wersji oprogramowania.

2 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]

3 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.

4 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.

5 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.

Uaktywnianie licencji

Ścieżka dostępu

– Menedżer okien dialogowych systemu AMS > **Menu główne** > **Konfiguracja** > **Licencje**

1. Kliknij przycisk **Menedżer licencji**
   Zostanie otwarty kreator **Menedżer licencji**.
2. Kliknij przycisk **Zapisz**, a następnie zapisz informacje o systemie do pliku.
3. Kliknij przycisk **Kontynuuj**.
4. Zaloguj się na platformie Remote Portal remote.boschsecurity.com przy użyciu swoich firmowych poświadczeń.
5. Wybierz produkt, na których chcesz uzyskać licencję, po czym postępuj zgodnie z instrukcjami wyświetlanymi w portalu, aby wygenerować i pobrać plik licencji.
6. Wróć do okna **Menedżer licencji**.
7. Kliknij przycisk **Kontynuuj**.
8. Kliknij przycisk **Import**, odszukaj pobrany plik licencji, po czym dodaj go do swojego systemu.
9. Kliknij przycisk **Finish (Zakończ)**.

Uwaga!
Jeżeli w trakcie procesu zostaną wyświetlone jakiekolwiek komunikaty o błędach, skontaktuj się z działem pomocy technicznej Bosch.

Uwaga!
Skutki zmian dotyczących sprzętu i oprogramowania
Zmiany sprzętowe serwera mogą unieważnić Twoją licencję i spowodować, że oprogramowanie przestanie działać. Zanim wprowadzisz zmiany ma serwerze, skontaktuj się z pomocą techniczną.

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.

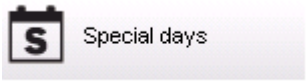
1. Zaloguj się do programu Access Manager.
2. Wybierz kolejno opcje **Konfiguracja** > **Licencje**.
3. Kliknij przycisk **Aktywuj tryb demonstracyjny**.
4. Sprawdź, czy funkcje są wyświetlane w oknie dialogowym **Licencje**.

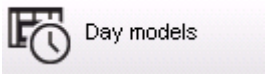
Tryb demonstracyjny jest aktywowany na 5 godzin. Czas do końca aktywności trybu jest wyświetlany w górnej części okna dialogowego **Licencje** oraz na paskach tytułu większości okien dialogowych.

6 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.

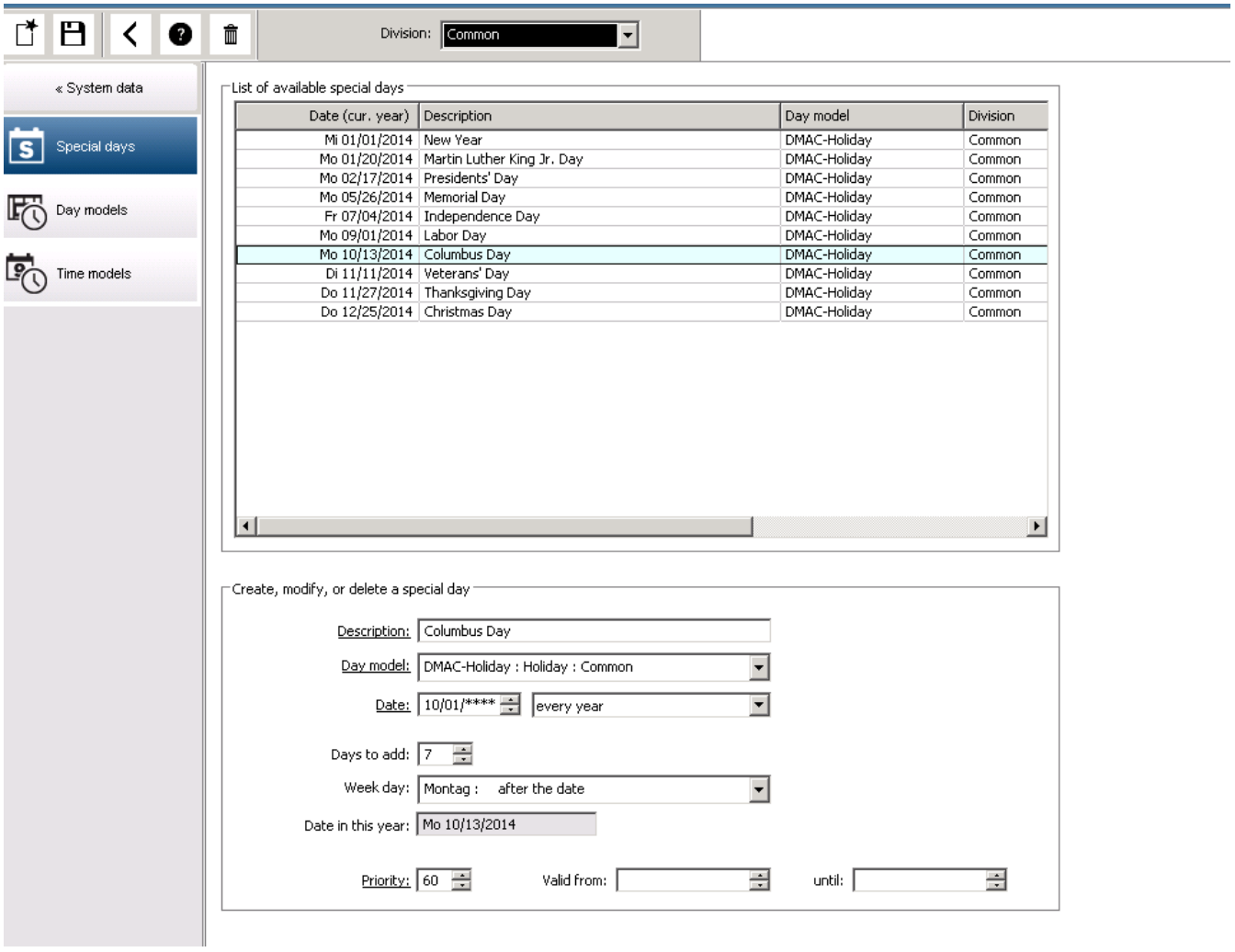
1. Zdefiniuj **dni specjalne** kalendarza dla swojej lokalizacji.
2. Zdefiniuj **modele dzienne**, które opisują aktywne i nieaktywne okresy w każdym typie dnia. Na przykład model dnia dla święta państwowego będzie się różnił od modelu dla zwykłego dnia roboczego. Na rodzaj i liczbę potrzebnych modeli 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.





6.1 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	**.**.****

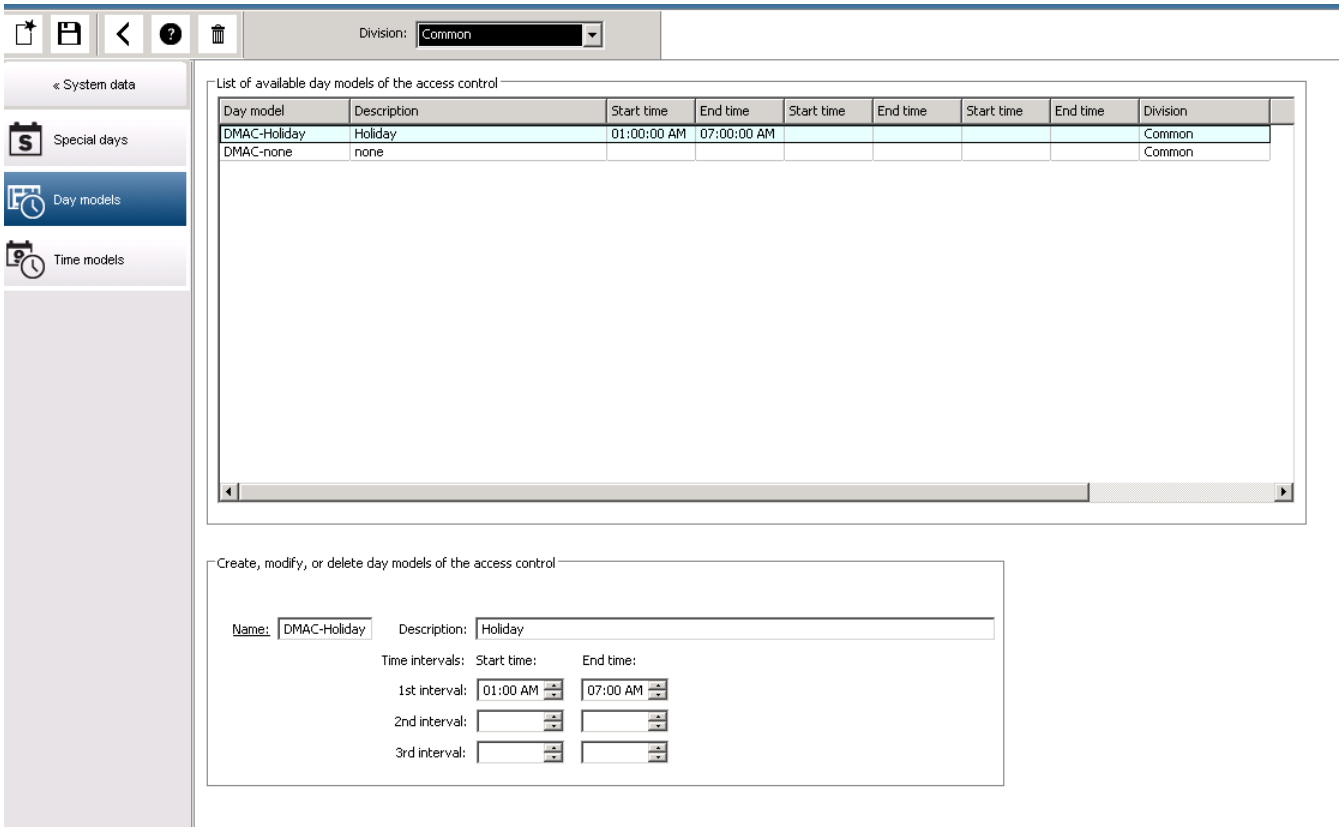
Dni świąteczne, które zależą od Świąt Wielkanocnych, nie są określane za pomocą konkretnej daty, ale poprzez liczbę dni dzielących je od Niedzieli Wielkanocnej. Data Niedzieli Wielkanocnej w bieżącym roku jest podana w polu **Data w tym roku**, a oddalenie od tej daty wprowadza się lub wybiera w polu **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.

6.2 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:

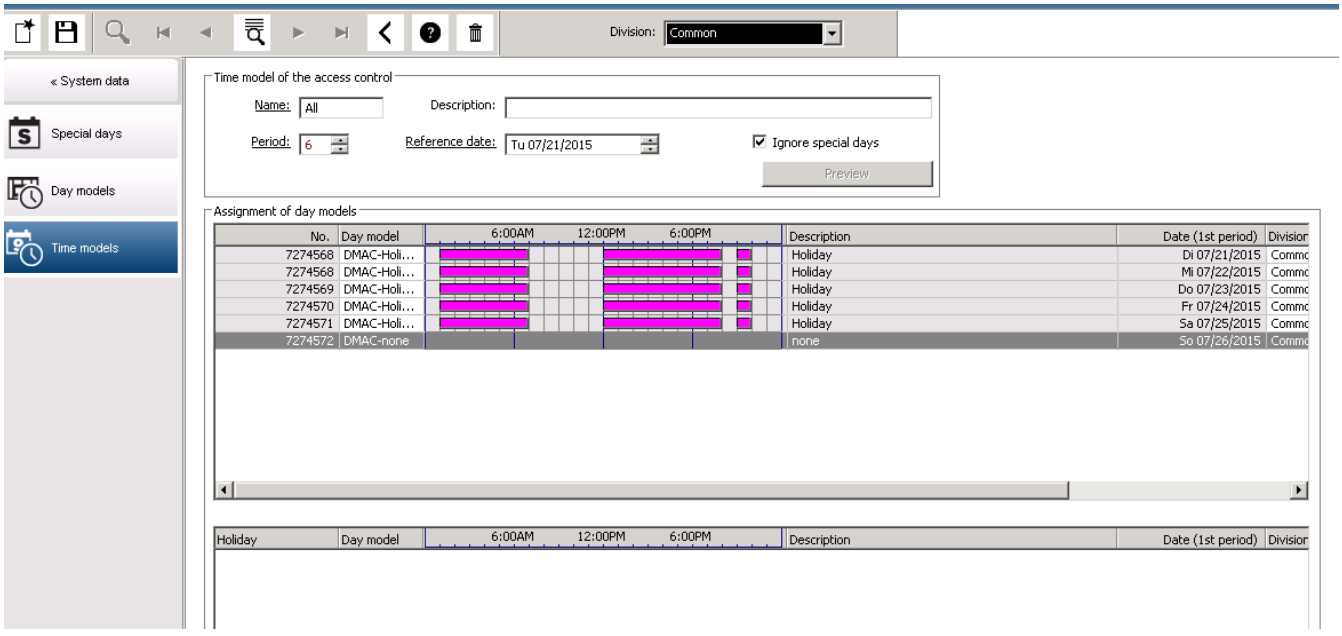
1. przedział czasu	od:	...	do:	24:00
Następny przedział czasu	od:	24:00	do:	...

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.

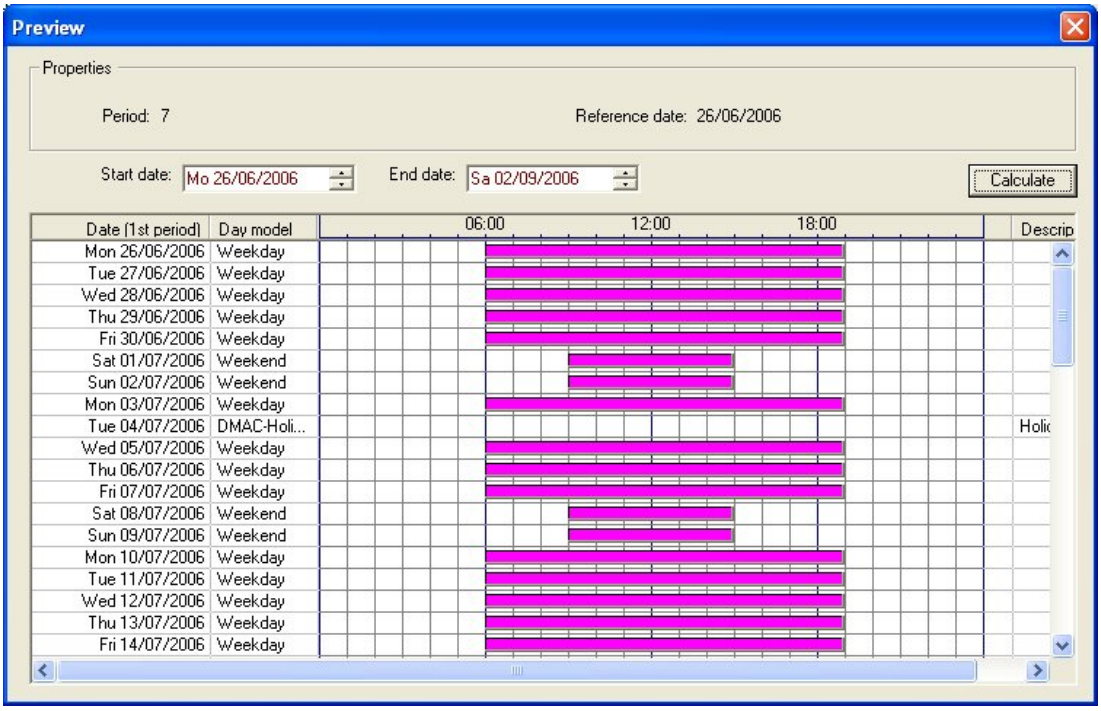
Model dzienny można usunąć, tylko jeśli nie został jeszcze przypisany do żadnego dnia specjalnego ani nie jest używany przez żaden model czasowy.

6.3 Definiowanie modeli czasowych

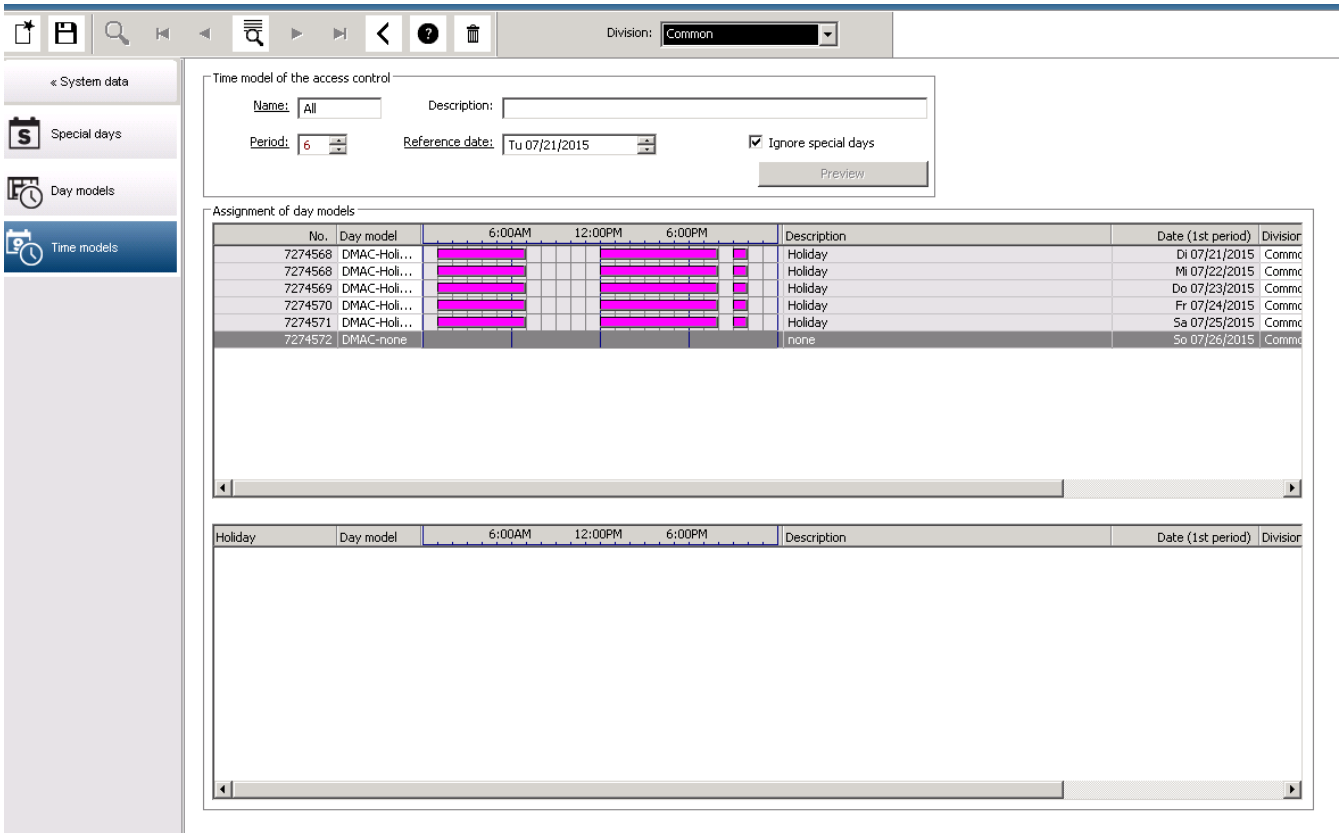


Utworzone modele czasowe można wybierać z listy wyszukiwania, a ich szczegóły pojawiają się w polach dialogowych. Wszelkie modyfikacje wprowadza się bezpośrednio w tym widoku w sposób analogiczny do tworzenia nowych modeli czasowych.
Jeśli maska jest pusta, modele czasowe można tworzyć od zera. W tym 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)
7274568 DMAC-Holi... Holiday Di 07/21/2015
7274568 DMAC-Holi... Holiday Mi 07/22/2015
7274569 DMAC-Holi... Holiday Do 07/23/2015
7274570 DMAC-Holi... Holiday Fr 07/24/2015
7274571 DMAC-Holi... Holiday Sa 07/25/2015
7274572 DMAC-none none So 07/26/2015
Holiday
Day model
6:00AM
12:00PM
6:00PM
Description
Date (1st period)

7 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

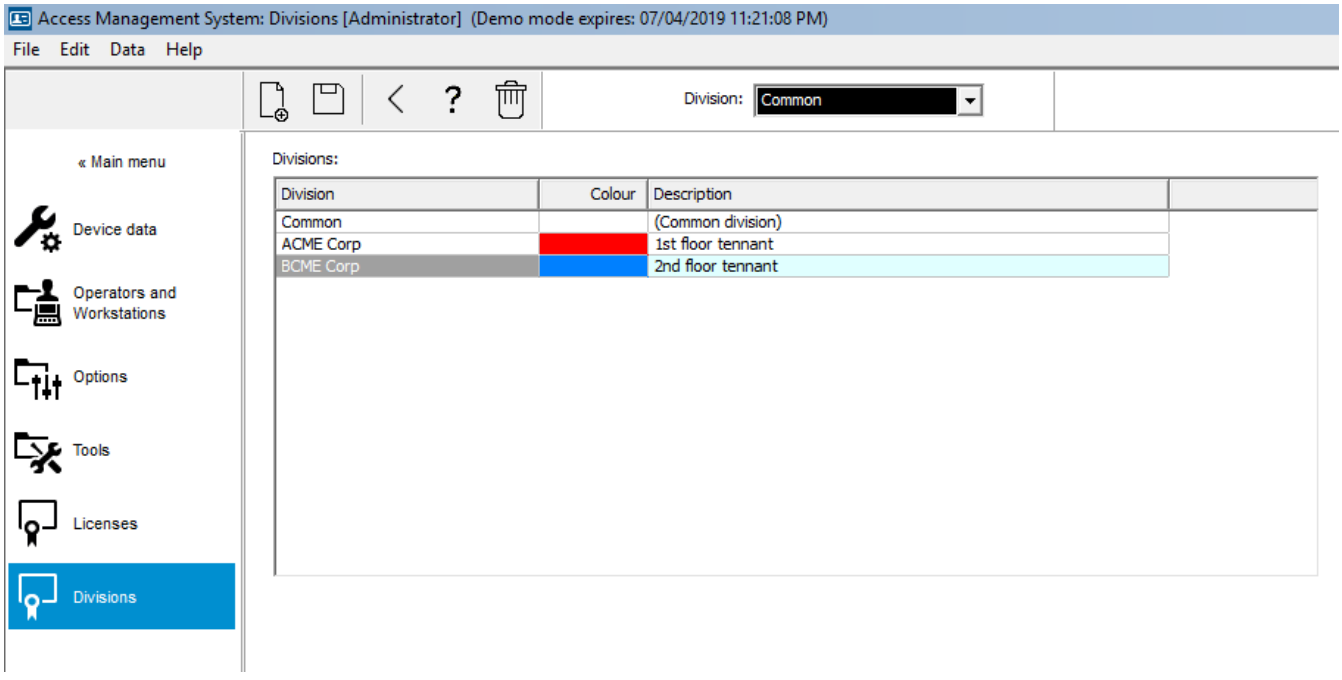
– Wykupienie licencji na funkcję Dywizji dla posiadanej instalacji.

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.



7.1 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.

7.2 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.

8 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.

9 Korzystanie z edytora urządzeń

Wstęp

Edytor urządzeń to narzędzie do dodawania, usuwania lub modyfikowania wejść i urządzeń. Edytor urządzeń udostępnia 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 edytora urządzeń

Przyciski paska narzędzi edytora urządzeń mają następujące 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 urządzeń należy zaczynać od katalogu głównego w drzewie, a następnie dodawać elementy za pomocą przycisków paska narzędzi, menu lub menu kontekstowego poszczególnych elementów (jest ono wywoływane kliknięciem prawego przycisku myszy). Aby dodać elementy podrzędne do urządzenia, najpierw zaznacz urządzenie nadrzędne, pod którym elementy podrzędne powinny być wyświetlane.

Kopiowanie i wklejanie urządzeń AMC

Kopiowanie urządzeń AMC z jednej części drzewa do innej:

1. Kliknij prawym przyciskiem myszy urządzenie AMC i wybierz z menu kontekstowego polecenie **Kopiuj**.
2. Kliknij prawym przyciskiem myszy odpowiednie urządzenie nadrzędne w dowolnym miejscu drzewa i wybierz w menu kontekstowym polecenie **Wklej**.
   - Urządzenie jest kopiowane z urządzeniami podrzędnymi i ustawieniami do nowej lokalizacji.
   - Parametry urządzeń, takie jak **adres IP** i **Nazwa**, które muszą być unikatowe, **nie są** kopiowane.
3. Wprowadź niepowtarzalne wartości tych parametrów urządzeń, które tego wymagają. Dopóki tego nie zrobisz, nie można zapisać drzewa urządzeń.

Zapisywanie swojej pracy

Po zakończeniu dodawania i modyfikacji elementów w drzewie kliknij przycisk **Zapisz**  , aby zapisać konfigurację.

Aby zamknąć edytor urządzeń, kliknij **Plik** > **Zakończ**.

9.1 Tryby konfiguracji i zastępowanie

Tryb konfiguracji jest domyślnym stanem urządzeń kontroli dostępu w edytorze urządzeń. W trybie konfiguracji uprawniony użytkownik posiadający konto AMS lub BIS ACE może wprowadzać zmiany w urządzeniach w edytorze urządzeń, a ACS natychmiast stosuje te zmiany w urządzeniach podrzędnych.

Operator może **zastąpić** tryb konfiguracji, wysyłając polecenia bezpośrednio do urządzeń kontroli dostępu spoza edytora urządzeń. Jest to typowy przykład sytuacji, gdy operator obsługuje przychodzące komunikaty i alarmy. Zanim operator wyśle polecenie **Restore configuration (Przywróć konfigurację)**, w urządzeniu pozostaje włączony Tryb pracy .

Jeśli osoba korzystająca z konfiguracji wybierze w edytorze urządzenie w trybie pracy, na stronie głównej właściwości urządzenia zostanie wyświetlone powiadomienie:

To urządzenie nie jest w trybie konfiguracji.

Użytkownik może wprowadzać i zapisywać zmiany w konfiguracji, ale zmiany te są buforowane i nie obowiązują do momentu zakończenia trybu alarmowego i przywrócenia trybu konfiguracji.

10 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

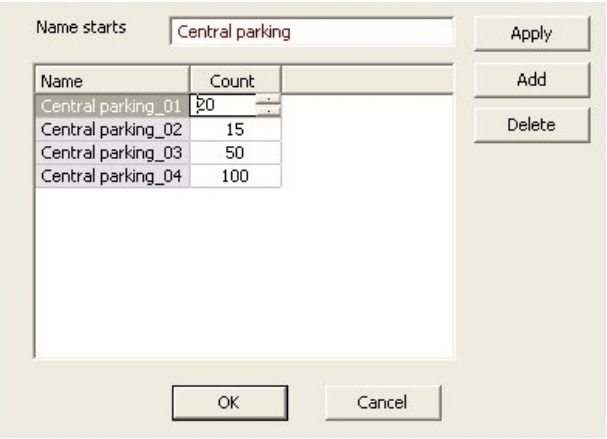
1. Kliknij obszar w hierarchii, aby go zaznaczyć.
2. Kliknij przycisk **Usuń**  lub kliknij prawym przyciskiem myszy i z menu kontekstowego wybierz polecenie usunięcia.

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

10.1 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.

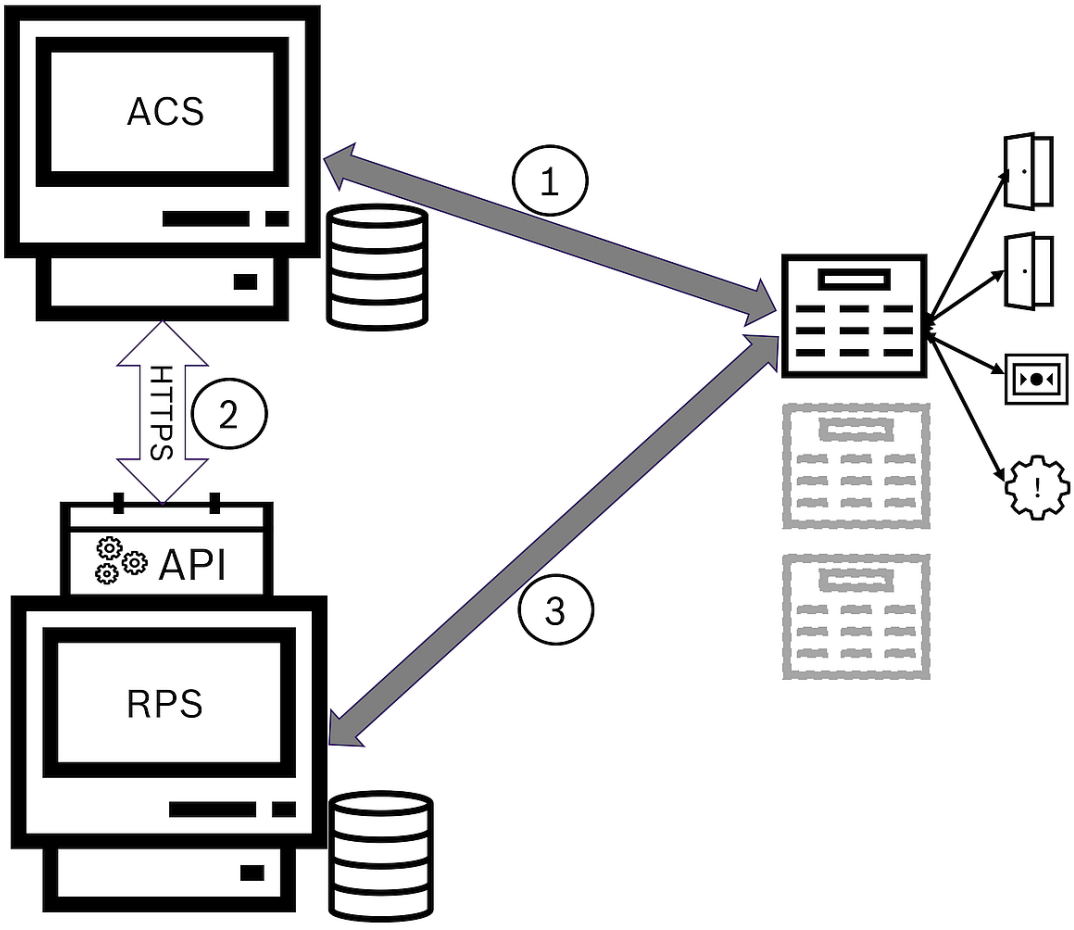
11 Konfigurowanie obszarów i central alarmowych włamania

Wstęp

System kontroli dostępu uczestniczy w zarządzaniu i eksploatacji central alarmowych sygnalizacji włamania firmy Bosch. Szczegółowe informacje o modelach, które obsługuje, można znaleźć w arkuszu danych systemu kontroli dostępu. System kontroli dostępu daje szczególne uprawnienia administrowania centralami alarmowymi sygnalizacji włamania **użytkownikom**. Użytkownicy stanowią podzbiór posiadaczy kart identyfikacyjnych ogólnego systemu kontroli dostępu. Administratorzy systemu kontroli dostępu przyznają tym posiadaczom kart specjalne uprawnienia do obsługi central alarmowych sygnalizacji włamania poprzez menedżera okien dialogowych ACE.

Centrale alarmowe sygnalizacji włamania są skonfigurowane i aktualizowane tak jak poprzednio za pośrednictwem odpowiedniego oprogramowania do zdalnego programowania (RPS). ACE umożliwia ciągły odczyt danych z oprogramowaniu RPS i wyświetla dostępne centrale alarmowe.

ACE zawiera okna dialogowe służące do tworzenia i przypisywania profili upoważnień oraz do zarządzania użytkownikami central alarmowych w oprogramowaniu RPS.



Rysunek 11.1: Uproszczona topologia zintegrowanego systemu kontroli dostępu i sygnalizacji włamania

ACS	Główny system kontroli dostępu: AMS lub BIS-ACE
API	Interfejs programowania aplikacji

RPS	Remote Programming System: aplikacja do sterowania centralami alarmowymi sygnalizacji włamania
1	ACS do centrali: wysyłanie poleceń do centrali alarmowej. Centrala do ACS: zdarzenia z punktów włamania.
2	ACS do RPS: dane posiadaczy kart
3	RPS do centrali: ustawienia konfiguracyjne

Wymagania wstępne

- Oprogramowanie RPS dla obsługiwanych central alarmowych sygnalizacji włamania Bosch jest instalowane na osobnym komputerze połączonym siecią z serwerem systemu ACE, a **nie** na samym serwerze systemu ACE. Odpowiednie instrukcje można znaleźć w instrukcji instalacji oprogramowaniu RPS.
- Oprogramowanie RPS zostało skonfigurowane z centralami alarmowymi sygnalizacji włamania, które będą elementami systemu kontroli dostępu ACE. Instrukcje można znaleźć w podręczniku użytkownika oprogramowaniu RPS lub w pomocy online.
- W celu zapewnienia automatycznej synchronizacji zegary na panelach znajdują się w przedziale 100 dni zegara na serwerze ACE.
- Protokół Trybu 2 jest ustawiony na wszystkich centralach w grupie.
- Karty z jedną z następujących standardowych definicji:
  - HID 37 BIT -> Włamanie 37 BIT z kodem urządzenia/lokalizacji 32767 lub niższym.
  - HID 26 BIT- > Włamanie 26 BIT
  - EM 26 BIT- > Włamanie 26 BIT

Przegląd

Proces konfiguracji składa się z następujących etapów, które opisano w poniższych sekcjach w tym rozdziale:

1. Instalowanie interfejsu API oprogramowania sygnalizacji włamania RPS na komputerze z oprogramowaniem RPS
2. Podłączenie systemu kontroli dostępu do central alarmowych sygnalizacji włamania.
   - Definiowanie połączenia z interfejsem API oprogramowaniu RPS.
   - Konfigurowanie połączeń centrali alarmowej.
3. Tworzenie profili uprawnień do centrali określających dostępne funkcje podłączonych central.
4. Przydzielanie profili upoważnień posiadaczom kart identyfikacyjnych.
   - W ten sposób posiadacz karty staje się operatorem central alarmowych sygnalizacji włamania.

11.1 Instalowanie interfejsu API oprogramowania sygnalizacji włamania RPS na komputerze z oprogramowaniem RPS

Interfejs API oprogramowania sygnalizacji włamania RPS pełni rolę kanału komunikacyjnego między aplikacjami AMS i RPS zainstalowanymi na osobnych komputerach. Najpierw należy zainstalować interfejs API na komputerze z oprogramowaniem RPS, a następnie na komputerze z oprogramowaniem AMS zainstalować certyfikaty wygenerowane przez program instalacyjny.

Procedura

1. Uruchom plik konfiguracyjny interfejsu API oprogramowaniu RPS zgodnie z instrukcjami w jego dokumentacji.

– Program instalacyjny i jego dokumentacja znajdują się na nośniku instalacyjnym oprogramowania AMS:
  `AddOns\Intrusion-RPS-API\Bosch_RPS_API_Setup_v*.exe`
  `AddOns\Intrusion-RPS-API\RPS-API_Application_note_v*.pdf`
– Program instalacyjny generuje 2 certyfikaty i zapisuje je na komputerze oprogramowaniu RPS:
  `%AppData%\Roaming\Bosch_RPS_API\BoschRpsAPI.cer`
  `%AppData%\Roaming\Bosch_RPS_API\BoschRpsAPI.pfx` (wymaga ustawienia hasła)

2. Skopiuj pliki certyfikatów do komputera z oprogramowaniem AMS.
3. Na komputerze z oprogramowaniem AMS zainstaluj certyfikaty w folderach **Lokalizacja przechowywania**: `Local Machine`, **Magazyn certyfikatów**: `Trusted Root Certification Authority`.

11.2 Podłączenie systemu kontroli dostępu do central alarmowych sygnalizacji włamania

Wstęp

W tej sekcji opisano sposób wyświetlania centrali alarmowych sygnalizacji włamania i udostępniania ich do sterowania przez aplikację ACE client. System kontroli dostępu łączy się przez interfejs API z oprogramowaniem RPS w tej samej sieci. Korzystając z pośrednictwa interfejsu API, prowadzi stale aktualizowaną wewnętrzną listę zgodnych dostępnych central alarmowych sygnalizacji włamania.
Aby program AMS łączył się z centralami alarmowymi sygnalizacji włamania, trzeba w nim wykonać dwie czynności:
– Krok 1: Definiowanie połączenia z interfejsem API oprogramowaniu RPS
– Krok 2: Konfigurowanie połączeń centrali alarmowej

Ścieżka w oknie dialogowym

– menu główne > **Konfiguracja** > **Centrale** i podokna dialogowe

11.2.1 Krok 1: Definiowanie połączenia z interfejsem API oprogramowaniu RPS

Krok 1 ma na celu udostępnienie adresu komputera z programem RPS oraz informacji o logowaniu do systemu kontroli dostępu.

Ścieżka w oknie dialogowym

Menu główne > **Konfiguracja** > **Centrale > konfiguracja interfejsu API oprogramowania RPS**

Procedura

1. Wprowadź następujące informacje:

Informacje	Opis
Nazwa hosta / adres IP	Adres HTTPS komputera, na którym działa oprogramowaniu RPS, oraz numer portu, przez który komunikuje się oprogramowanie RPS. Nie można użyć nazwy `localhost`. Domyślnym portem jest `9000`.
Nazwa użytkownika	Nazwa użytkownika będącego administratorem interfejsu RPS API.
Hasło	Hasło użytkownika będącego administratorem RPS.

2. Kliknij przycisk **Sprawdź połączenie**, aby upewnić się, że oprogramowaniu RPS działa, oraz że nazwa użytkownika i hasło są prawidłowe.
3. Kliknij przycisk  (Zapisz), aby zapisać zmiany.

11.2.2 Krok 2: Konfigurowanie połączeń centrali alarmowej

Krok 2 służy do konfigurowania zakresu kontroli, którą system kontroli dostępu ma odnośnie do poszczególnych central alarmowych w sieci.

Ścieżka w oknie dialogowym

Menu główne > **Konfiguracja** > **Centrale alarmowe > Administrowanie centralą**

W oknie dialogowym znajduje się lista zgodnych central alarmowych sygnalizacji włamania, które interfejs API oprogramowania RPS przypisał do systemu ACE.

Lista jest okresowo aktualizowana w tle. Po otworzeniu okna dialogowego od czasu do czasu klikaj  w celu wymuszenia natychmiastowej ręcznej aktualizacji.

Lista jest przeznaczona tylko do odczytu, z wyjątkiem elementów sterujących opisanych w poniższej sekcji.

Procedura

1. Zaznacz centralę na liście
2. Za pomocą elementów sterujących widocznych poniżej określ, jakie operacje może wykonywać system kontroli dostępu w wybranej centrali alarmowej sygnalizacji włamania.

Kolumna listy **Administrowanie użytkownikami**	Zaznacz pole wyboru, aby zapewnić się, że użytkownicy centrali alarmowej sygnalizacji włamania wymienieni w tym wierszu są administrowani przez system kontroli dostępu, a **nie** przez centralę alarmową. **WAŻNE**: to ustawienie powoduje zastąpienie wszystkich użytkowników central utworzonych lokalnie w RPS.
Lista kolumn **Map View**	Zaznaczenie tego pola wyboru powoduje umożliwienie wydawania poleceń i sterowanie tą centralą przez aplikację ACE client.
Ustawienia ikony w kolumnie  **Dane dostępu**.	Jeżeli zaznaczono pole wyboru w kolumnie **Map View**, kliknij ikonę, a następnie wpisz – adres IP – numer portu (domyślnie 7700) – kod dostępu do konkretnej centrali. Kod dostępu jest ustawiany w oprogramowaniu RPS.
Przycisk: **Usuń wybraną centralę**	Po usunięciu centrali w oprogramowaniu do zdalnego programowania jest ona wyświetlana na liście ze statusem **Usunięte**. Wybierz centralę, a następnie kliknij ten przycisk w celu jej całkowitego usunięcia z bazy danych.

11.3 Tworzenie profili upoważnień do centrali

Wstęp

W tej sekcji opisano sposób tworzenia profili upoważnień do centrali.

Profil upoważnień do centrali alarmowej to dostosowany zestaw uprawnień do obsługi wybranych central alarmowych sygnalizacji włamania. Administrator systemu ACE może utworzyć wiele profili uprawnień do centrali dla różnych zakresów obowiązków różnych grup posiadaczy kart.

Ścieżka w oknie dialogowym

– Menu główne > **Dane systemowe** > **Autoryzacja Profil upoważnień do central alarmowych**

Procedura

1. Kliknij przycisk  , aby utworzyć nowy profil.
2. (obowiązkowo) Nadaj profilowi unikatową nazwę.
3. (opcjonalnie) Wprowadź dowolnie wybrany opis centrali
4. Pod listą **Przypisane centrale** kliknij przycisk **Dodaj...**, aby dodać jedną lub więcej central z wyświetlanej listy central dostępnych w sieci.
   Wybierz jedną lub więcej central i kliknij przycisk **Usuń**, aby je usunąć z listy.
5. Na liście **Przypisane centrale** kliknij centralę, aby ją zaznaczyć.
   – W okienku **Upoważnienia** pojawi się lista zawierająca wszystkie obszary włamania, które należą do wybranej centrali.
6. Na liście **Upoważnienia** w kolumnie **Poziom upoważnień** wybierz poziom uprawnień dla poszczególnych obszarów włamania przypisanych do tej centrali, które mają być objęte tym profilem
   – Poziomy upoważnień są definiowane i utrzymywane w oprogramowaniu do zdalnego programowania. Można je również dostosowywać. Przed przypisaniem go do profilu należy poznać definicję poziomu uprawnień w oprogramowaniu do zdalnego programowania.
   – Domyślnie **L1** jest najwyższym poziomem upoważnień, a **L2**, **L3** itd. są coraz bardziej ograniczone.
   – Jeśli to pole jest puste, użytkownik o tym profilu **nie** będzie miał żadnych upoważnień w obszarze wybranej centrali.
7. Powtórz ten proces w przypadku wszystkich obszarów włamania dostępnych centralach, które obejmuje ten profil.
8. (opcjonalnie) Na liście **Grupa użytkowników** wybierz grupę użytkowników centrali, aby ograniczyć upoważnienia do określonych okresów czasu.
   – Grupy użytkowników można definiować i obsługiwać w oprogramowaniu do zdalnego programowania. Można je również dostosowywać. Przed przypisaniem grupy użytkowników do profilu upewnij się, że znasz definicję grupy użytkowników w oprogramowaniu do zdalnego programowania.
9. Kliknij przycisk  (Zapisz), aby zapisać zmiany.

11.4 Przydzielanie profili upoważnień posiadaczom kart identyfikacyjnych

Wstęp

W tej sekcji opisano sposób przypisywania różnych profili upoważnień do central alarmowych różnym typom lub grupom posiadaczy kart identyfikacyjnych.

Wymaganie wstępne
W systemie kontroli dostępu zdefiniowano co najmniej jeden profil upoważnienia do centrali.

Ścieżka w oknie dialogowym
Menu główne > **Osoby** > **Karty**

Procedura
1. W zwykły sposób znajdź i wybierz żądanego posiadacza karty z bazy danych.
2. Kliknij kartę **Włamanie**.
3. Na karcie **Włamanie** zaznacz pole wyboru **Użytkownik centrali.**
4. (obowiązkowo) W polu **Kod dostępu** wpisz kod, za pomocą którego posiadacz karty będzie obsługiwać centrale alarmowe sygnalizacji włamania.
   – W razie potrzeby użyj przycisku, aby wygenerować nieużywany nowy kod dostępu.
5. Na liście **Karta identyfikacyjna** wybierz jedno z poświadczeń kontroli dostępu przypisanych do tego posiadacza karty.
6. (opcjonalnie) W polu **Numer pilota** wprowadź numer, który jest wydrukowany na pilocie zdalnego sterowania centralą alarmową używanym przez tego operatora.
7. Na liście **Język** wybierz język, w którym posiadacz karty preferuje dostęp do okien dialogowych centrali.
8. Jeśli posiadacz karty ma korzystać z aplikacji Bosch na smartfon do obsługi central alarmowych, zaznacz pole wyboru **Dostęp zdalny**.
9. Na liście **Profil upoważnień** wybierz odpowiedni profil uprawnień do centrali dla posiadacza karty.
10. Kliknij przycisk  (Zapisz), aby zapisać zmiany.
    – Ten profil uprawnień do centrali, ze wszystkimi jego centralami i uprawnieniami, zostanie przypisany do posiadacza karty. W ten sposób posiadacz karty staje się operatorem central alarmowych sygnalizacji włamania.

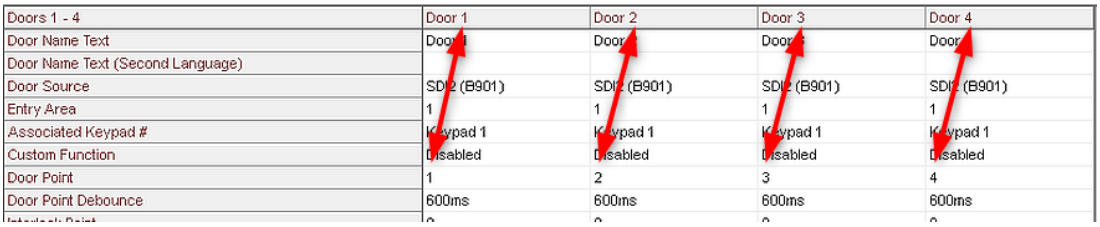
Należy zwrócić uwagę, że w tym oknie dialogowym można też użyć pól danych z przyciskiem  , aby znaleźć posiadaczy kart w bazie danych.

11.5 Kontrolowanie drzwi za pomocą modułów B901 w centralach alarmowych sygnalizacji włamania

W oprogramowaniu AMS w wersji 4.0.1 i nowszych modułami interfejsu kontroli dostępu B901 można sterować za pomocą aplikacji AMS Map View.
B901 to prosty kontroler drzwi, który administrator systemu podłącza do central alarmowych sygnalizacji włamania Bosch. W celu ustanowienia połączenia między odnośną centralą alarmową sygnalizacji włamania a systemem AMS należy skorzystać z procedur opisanych w poprzednich punktach.
Modułu B901 nie konfiguruje się w edytorze urządzeń.
Moduł B901 może blokować/odblokowywać zamki drzwi, zabezpieczać/odbezpieczać drzwi oraz przełączać stan drzwi, ale przekazuje jedynie ograniczone informacje o stanie do systemu kontroli dostępu. Na przykład nie informuje, czy drzwi zostały fizycznie otwarte, a nie jedynie odblokowane.

Podobnie jak się do dzieje w przypadku wszystkich innych urządzeń sygnalizacji włamania, aby umożliwić wysyłanie poleceń do modułu B901 z aplikacji AMS Map View, należy w aplikacji Map View włączyć obsługę odnośnej centrali. Służy do tego okno dialogowe programu AMS:
Menu główne > **Konfiguracja** > **Centrale alarmowe > Administrowanie centralą**.

Rejestrator przeciągnięć kartą w aplikacji Map View a drzwi z modułem B901
Aby aplikacja **Rejestrator przeciągnięć kartą** dostępna wewnątrz aplikacji AMS Map View otrzymywała poprawne informacje, identyfikatory drzwi wyposażonych w kontroler B901 muszą być takie same, jak identyfikatory punktów drzwiowych. Innymi słowy drzwi 1 muszą być przypisane do punktu drzwiowego 1, drzwi 2 do punktu drzwiowego 2 itd.



Doors 1 - 4	Door 1	Door 2	Door 3	Door 4
Door Name Text	Door 1	Door 2	Door 3	Door 4
Door Name Text (Second Language)				
Door Source	SDI2 (B901)	SDI2 (B901)	SDI2 (B901)	SDI2 (B901)
Entry Area	1	1	1	1
Associated Keypad #	Keypad 1	Keypad 1	Keypad 1	Keypad 1
Custom Function	Disabled	Disabled	Disabled	Disabled
Door Point	1	2	3	4
Door Point Debounce	600ms	600ms	600ms	600ms

Przypisań tych należy dokonać w ustawieniach kontrolera drzwi B901 w narzędziu RPS używanym do konfigurowania central alarmowych sygnalizacji włamania i kontrolerów.

12 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**.

12.1 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 czasie braku aktywności:** Liczba sekund, po jakiej sesja zalogowania za pomocą czytnika rejestracji jest automatycznie kończona. Pozostawienie wartości `0` oznacza nieograniczoną ważność zalogowania.

12.2 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.

12.3 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.

12.4 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.

12.5 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.

12.6 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.
Przy pierwszym logowaniu po zakończeniu instalacji system wymaga zmiany 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.

Należy zwrócić 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/

13 Konfigurowanie kart

13.1 Definicja karty

To okno dialogowe służy do aktywowania, dezaktywowania, modyfikowania i dodawania definicji kart wykorzystywanych przez system kontroli dostępu.

Ścieżka w oknie dialogowym

– Menu główne AMS > **Konfiguracja** > **Opcje** > **Definicja karty**

System jest dostarczany z zestawem wstępnie zdefiniowanych typów kart. Wstępnie zdefiniowane typy kart są wyświetlane na szarym tle w tabeli **Dostępne typy kart** i nie można ich modyfikować. Można je przenosić tylko między tabelami **Aktywne typy kart** i **Dostępne typy kart**.

13.1.1 Tworzenie i modyfikacja

Kliknij przycisk ✚ (zielony +) nad polem listy po prawej stronie, aby utworzyć nową pozycję na liście. W przeciwieństwie do wstępnie zdefiniowanych typów kart nowo tworzone typy można swobodnie edytować. Kliknij dwukrotnie pola **Nazwa**, **Opis** i **Liczba bitów**, aby je edytować.

Nazwa może zawierać maksymalnie 80 znaków, a opis 255. Liczba bitów jest ograniczona do 64 (w przypadku wprowadzenia większej wartości spowoduje to przywrócenie wartości maksymalnej po wyjściu z tego pola).

Uwaga!

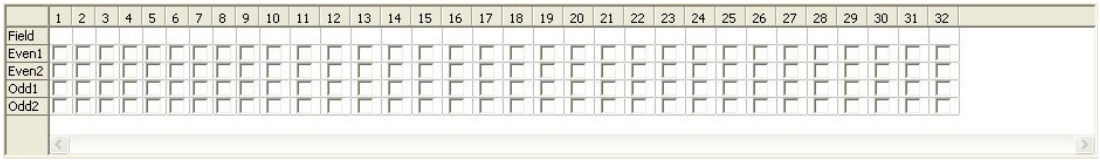
Długość w bitach służy do rozróżniania definicji Wiegand. Dlatego każda nowa definicja musi mieć określoną unikatową długość bitową, która nie została jeszcze użyta w istniejących definicjach.

- Aby zmodyfikować bit danych, kliknij dwukrotnie odpowiednie pole. Aby go usunąć, należy najpierw wybrać bit danych, a następnie kliknąć przycisk ✕ (czerwona litera x).

Uwaga!

Można zmieniać lub usuwać tylko typy kart utworzone przez użytkownika.

Po wybraniu pojedynczego typu karty (na listach po lewej lub po prawej) jego kodowanie jest wyświetlane w dolnej części okna dialogowego. Bity danych wyświetlane są w 5 wierszach i w tylu kolumnach ile bitów zawiera definicja.



Każda kolumna wiersza **Pole** może mieć etykietę określającą sposób interpretacji części kodu. Dostępne są następujące etykiety:

F	Funkcja: oznacza część kodu powiązaną z funkcją	

C	Numer: część kodu zawierająca indywidualny numer karty	
E1	Parzyste 1: bit wyrównania pierwszej maski parzystości	Podanie tych wartości uaktywnia pole wyboru odpowiadające podanemu wierszowi.
E2	Parzyste 2: bit wyrównania drugiej maski parzystości	
O1	Nieparzyste 1: bit wyrównania pierwszej maski parowania nieparzystości	
O2	Nieparzyste 2: bit wyrównania drugiej maski nieparzystości	
1	Stałe wartości bitu w kodzie	
0		

W przypadku etykiet E1, E2, O1 i O2 wystarczy zaznaczyć pole wyboru w odpowiednim wierszu. Pole wyboru wiersza **Pole** zostanie odpowiednio oznaczone.
Wyjaśnienie:
Wysyłany przez czytnik w momencie prezentacji karty identyfikacyjnej sygnał ma postać szeregu zer i jedynek. W przypadku każdego typu karty długość tego sygnału (tzn. liczba bitów) jest określona dokładnie.
Oprócz rzeczywistych danych użytkownika, które są zapisywane jako dane kodowe, sygnał zawiera również dane sterujące, aby umożliwić identyfikację sygnału jako sygnału karty i sprawdzanie prawidłowości transmisji.
Na ogół stałe zera i ich ustawienia są przydatne do identyfikowania typu sygnału.
Bity parzystości, które muszą dać wartość zero (parzystość) lub jeden (nieparzystość) jako sumę kontrolną w wybranych bitach sygnału, służą do weryfikacji prawidłowości transmisji. Kontrolery można skonfigurować tak, aby obliczały jedną lub dwie sumy kontrolne cyfr dla parzystości i jedną lub dwie sumy kontrolne cyfr dla nieparzystości.
Na liście w poszczególnych wierszach można dla sumy kontrolnej parzystości (Parzyste1, Parzyste2, Nieparzyste1 i Nieparzyste 2) zaznaczyć bity, które mają zostać włączone do sumy kontrolnej. W górnym wierszu (Pole) dla każdej sumy kontrolnej definiowany jest bit w celu wyrównania sumy kontrolnej zgodnie z typem parzystości. Jeśli opcja parzystości nie jest używana, odpowiednia wiersz po prostu pozostaje pusty.

13.1.2 Aktywacja/dezaktywacja definicji kart

Można równocześnie uaktywnić maksymalnie 8 definicji kart. Definicje, które mają być uaktywnione muszą zostać przeniesione do listy po lewej stronie z **Aktywne typy kart**. W tym celu należy wybrać jedną lub więcej definicji po prawej stronie, a następnie kliknąć przycisk strzałki w lewo (**<**).
Jednocześnie można przenieść nie więcej niż cztery definicje. Po czterech definicjach wszystkie następne zostaną odrzucone. Aby dodać więcej definicji do **Aktywne typy kart**, należy usunąć jedną lub więcej spośród tych, które są wyświetlane, zaznaczając je i przenosząc na prawą stronę za pomocą przycisku (**>**), co spowoduje ich dezaktywację.

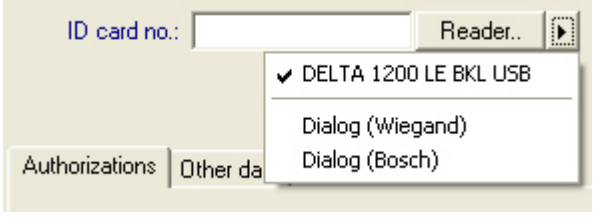
Uwaga!
Aby korzystać z czytników za pomocą protokołów L-Bus lub BG900, należy aktywować czytnik kart identyfikacyjnych typu **Czytnik szeregowy**. Spowoduje to wyświetlenie w menedżerze okien dialogowych systemu kontroli dostępu okna **Bosch** do ręcznego wprowadzania danych.

13.1.3 Tworzenie danych karty w menedżerze okien dialogowych

Ręczne wprowadzanie danych
W przypadku kart Wiegand i Bosch stosowane są inne metody wprowadzania danych.
W przypadku wszystkich definicji Wiegand (HID 26, HID 35, HID 37 i 32 bit CSN) Wiegand **okno dialogowe (Wiegand)** umożliwia wprowadzenie **kodu klienta** i **numeru karty**.
W przypadku czytników szeregowych okno dialogowe **(Bosch)** zawiera dodatkowe pola dla **wersji** i **kodu kraju**.

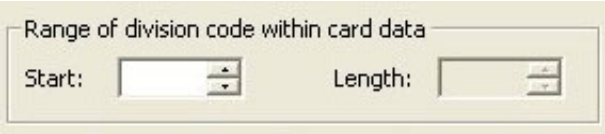
Wprowadzanie danych za pomocą czytnika rejestrującego
W uzupełnieniu do ręcznego wprowadzania danych każda stacja robocza może być wyposażona w czytnik służący do zbierania danych karty. Użyj czytnika z listy w następującym oknie dialogowym:
– Menu główne AMS > **Konfiguracja** > **Opcje** > **Czytnik kart**
Jeśli wybrany czytnik jest czytnikiem wejścia dla kart Wiegand, wszystkie aktywne typy kart Wiegand zostaną umieszczone na liście wraz z czytnikiem
– Menu główne AMS > **Dane osobowe** > **Karty** > przycisk czytnika > ▶ (strzałka w prawo)
Aby zapewnić prawidłowe zapisanie kodowania kart, należy wybrać jeden z tych typów kart. Oznacza to, że samego czytnika nie można wybierać bezpośrednio, ale tylko pośrednio poprzez wybór definicji Wiegand.
Jeśli wymagany typ karty nie jest wyświetlany na liście rozwijanej, należy ją uaktywnić w oknie dialogowym Definicja karty.
– Menu główne AMS > **Konfiguracja** > **Opcje** > **Definicja karty**

Można bezpośrednio wybierać z listy czytniki rejestracji HITAG, LEGIC i MIFARE.



Definicja karty dla stref (funkcja wielu stref)
W przypadku posiadania licencji obsługi stref pozwalającej na zarządzanie wieloma podmiotami (tzw. strefami) w pomieszczeniach objętych kontrolą dostępu można skonfigurować obszar kodu na karcie, który umożliwia operatorowi rozróżnianie kart w

różnych strefach. Aby określić położenie bitu **startowego** i **długość** kodowania strefy na kartach, należy użyć pól opcjonalnych (tylko w przypadku, gdy funkcja stref jest licencjonowana).



13.2 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
Wprowadzanie liczb w oknie dialogowym
Dla wygody można wprowadzać liczby w formacie dziesiętnym lub szesnastkowym. Wybierz przycisk radiowy **Szesnastkowy** lub **Dziesiętny** zgodnie z formatem określonym przez producenta karty.
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 pola te nie są udostępnione do zapisu, to nie mają zastosowania do żadnej z aktywnych definicji kart. W przypadku kodu Bosch wszystkie pola są udostępnione do zapisu.
Jeśli karta jest rejestrowana ręcznie na stacji roboczej operatora, pojawi się okno dialogowe z wartościami domyślnymi, które można dostosować dla każdej karty.

Wprowadzanie danych kodowania:
Jeśli dane są podawane przez producenta jako wartości dziesiętne, wybierz przycisk radiowy Dziesiętne i wprowadź podane wartości, np.:
Wersja: 2
Kod kraju: 99
Kod urządzenia: 56720
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)

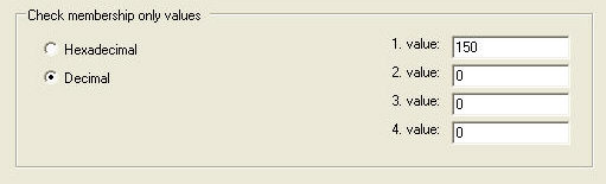
Uwaga!
Jeśli rejestracja karty następuje przez podłączony czytnik, to wartości domyślne są przypisywane automatycznie. Nie można zastąpić wartości domyślnych podczas odczytywania przez czytnik.
Aby było to możliwe, należy zmienić sposób przechwytywania danych na **Okno dialogowe**.

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.

14 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

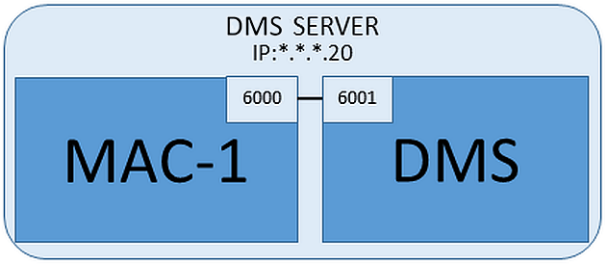
Podstawowe zasady używania edytora DevEdit opisano w tej sekcji **Korzystanie z edytora urządzeń** pod linkiem poniżej.

Patrz

- *Korzystanie z edytora urządzeń, Strona 24*

14.1 Konfigurowanie kontrolerów MAC i RMAC

14.1.1 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**.

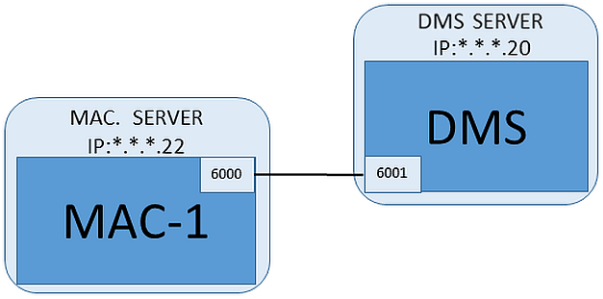
14.1.2 Przygotowywanie komputerów serwerów kontrolerów MAC do obsługi kontrolerów MAC i RMAC

W tej sekcji opisano sposób przygotowania komputerów do roli serwerów kontrolerów MAC. Domyślnie pierwszy kontroler MAC w systemie kontroli dostępu 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. Obecnie systemy operacyjne wszystkich serwerów MAC muszą być obsługiwane przez Microsoft i mieć zainstalowane najnowsze aktualizacje.
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 systemach operacyjnych Windows 10 i Windows Server jest to włączana funkcja.
6. Uruchom ponownie komputer.

14.1.3 Konfigurowanie kontrolera MAC na jego własnym serwerze



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

1. Na komputerze będącym serwerem systemu DMS przejdź do edytora urządzeń,
   – Kliknij MAC prawym przyciskiem myszy i wybierz **Wyłącz wszystkie LAC**.
   – Wyłącz MAC, usuwając zaznaczenia pól wyboru **Aktywuj** i **Ładowanie urządzeń** dla tego kontrolera MAC.
2. Na komputerze serwera kontrolera MAC za pomocą programu systemu Windows `services.msc`
   – wyłącz usługę MAC **AUTO_MAC2**
   – Ustaw **Typ uruchomienia** tej usługi Mac jako **Ręczny**.
3. Uruchom program `MACInstaller.exe`.
   – W przypadku modułu AMS znajduje się on na nośniku instalacyjnym systemu AMS w folderze `\AddOns\MultiMAC\MACInstaller` (patrz poniżej sekcja Korzystanie z narzędzia MACInstaller).
4. Przejdź przez kolejne ekrany narzędzia, podając wartości w poniższych parametrach.

Numer ekranu	Parametr	Opis
3	**Folder docelowy**	Lokalny katalog, w którym ma zostać zainstalowany kontroler MAC. Pozostawiaj wartość domyślną, o ile to tylko możliwe.
4	**Serwer**	Nazwa lub adres IP serwera, na którym działa system DMS.
4	**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.

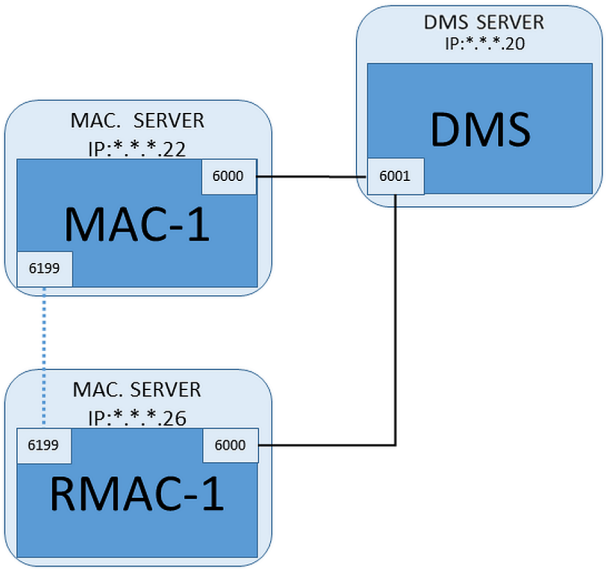
Numer ekranu	Parametr	Opis
4	**Numer (numer kontrolera MAC w systemie)**	Ustaw wartość 1 dla tego i wszystkich kontrolerów MAC (w przeciwieństwie do kontrolerów RMAC)**.**
4	**Bliźniak (nazwa lub adres IP partnerskiego kontrolera MAC)**	Pozostaw to pole puste, jeśli ten kontroler MAC nie będzie miał żadnego odpowiadającego mu kontrolera RMAC.

5. Na serwerze systemu DMS zaznacz kontroler MAC w edytorze urządzeń.
6. 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 systemu.
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**, do której należy kontroler MAC.

14.1.4 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 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.

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:

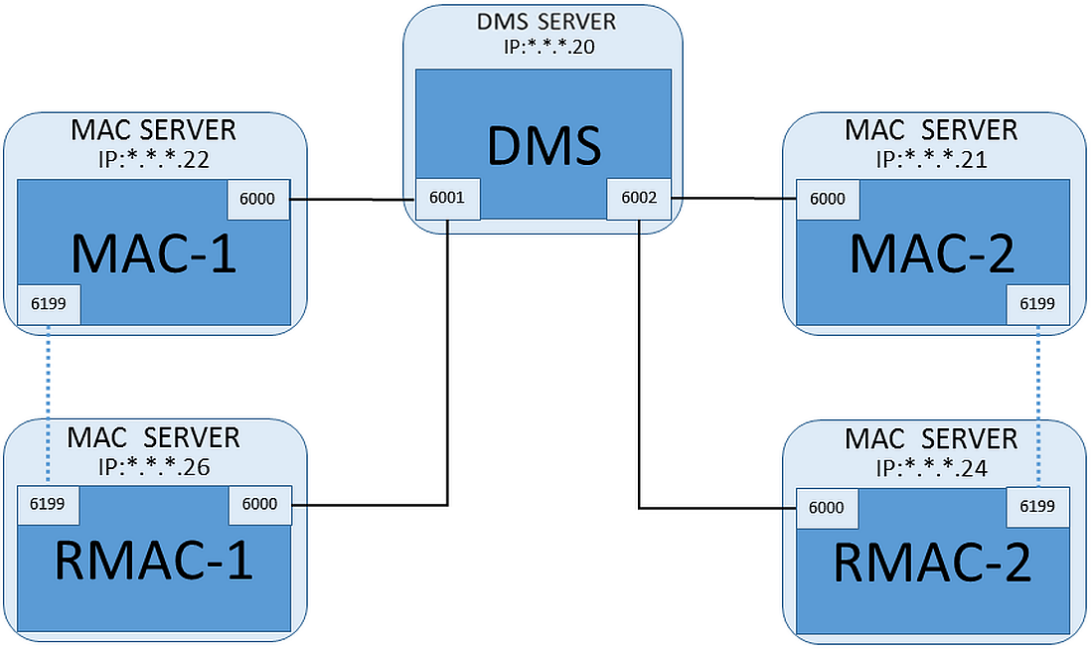
Parametr	Opis
Nazwa	Nazwa, która ma się pojawiać w drzewie urządzeń. Na przykład jeżeli odnośny kontroler MAC nosi nazwę MAC-01, to ten kontroler RMAC może mieć nazwę RMAC-01.
Opis	Opcjonalna dokumentacja dla operatorów kontroli dostępu.
Adres IP	Adres IP kontrolera RMAC.
Port MAC	`6199` (domyślna wartość statyczna) Wszystkie kontrolery MAC i RMAC używają tego portu do sprawdzania, czy ich urządzenia partnerskie działają i są dostępne**.**

Patrz

– *Korzystanie z narzędzia MACInstaller, Strona 56*

14.1.5 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.

14.1.6 Korzystanie z narzędzia MACInstaller

`MACInstaller.exe` to standardowe narzędzie do instalowania 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 w następującej ścieżce:

– `\AddOns\MultiMAC\MACInstaller.exe`

W szeregu ekranów użytkownicy wpisują wartości dla poniższych parametrów.

Numer ekranu	Parametr	Opis
3	**Folder docelowy**	Lokalny katalog, w którym ma zostać zainstalowany kontroler MAC.
4	**Serwer**	Nazwa lub adres IP serwera, na którym działa system DMS.
4	**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.**
4	**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).
4	**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.

Parametr: Port (port do DMS)

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.

Parametr: Numer (numer kontrolera MAC w systemie)

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.

Parametr: Tylko konfiguruj (przycisk radiowy)
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.

Parametr: Aktualizuj oprogramowanie (przycisk radiowy)
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.

14.2 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

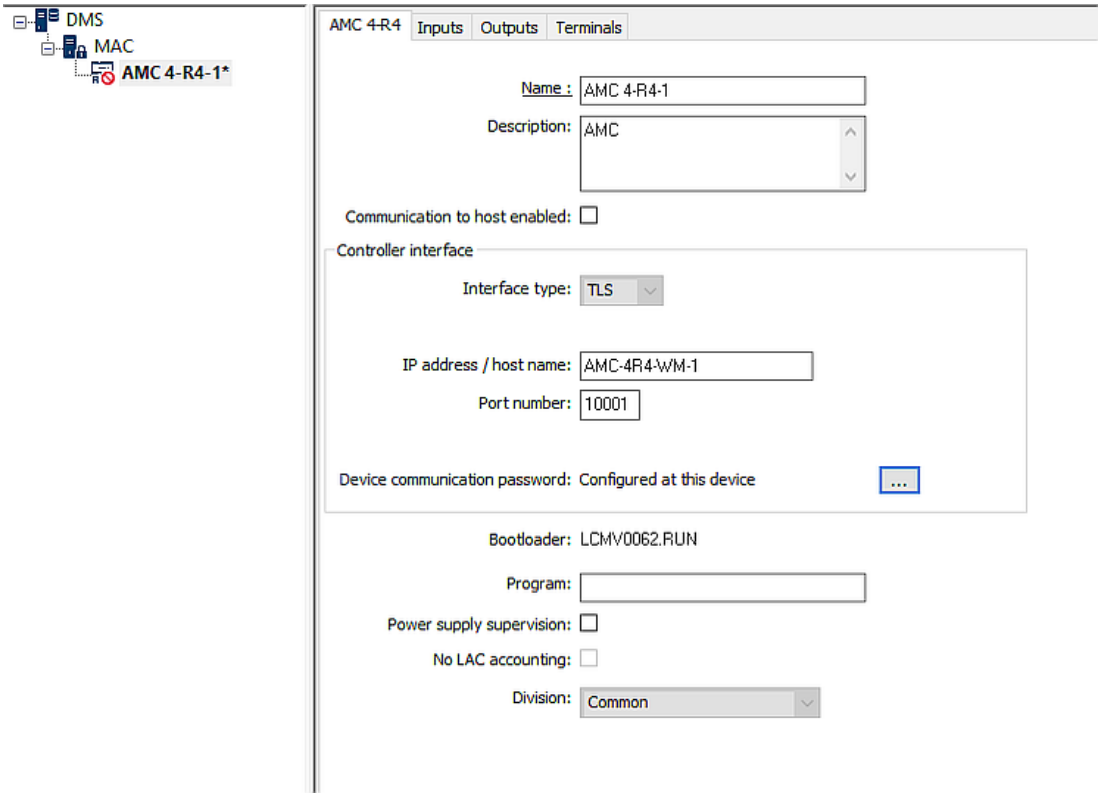
Zazwyczaj systemy kontroli dostępu wyposaża się tylko w jeden typ kontrolerów i czytników. Uaktualnienia oprogramowania i rozrastające się instalacje mogą powodować konieczność uzupełniania istniejących składników sprzętowych o nowe. Możliwe są nawet konfiguracje łączące warianty RS485 (AMC 4R4) z wariantami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

14.2.1 Parametry i ustawienia kontrolera AMC

Ogólne parametry kontrolera AMC



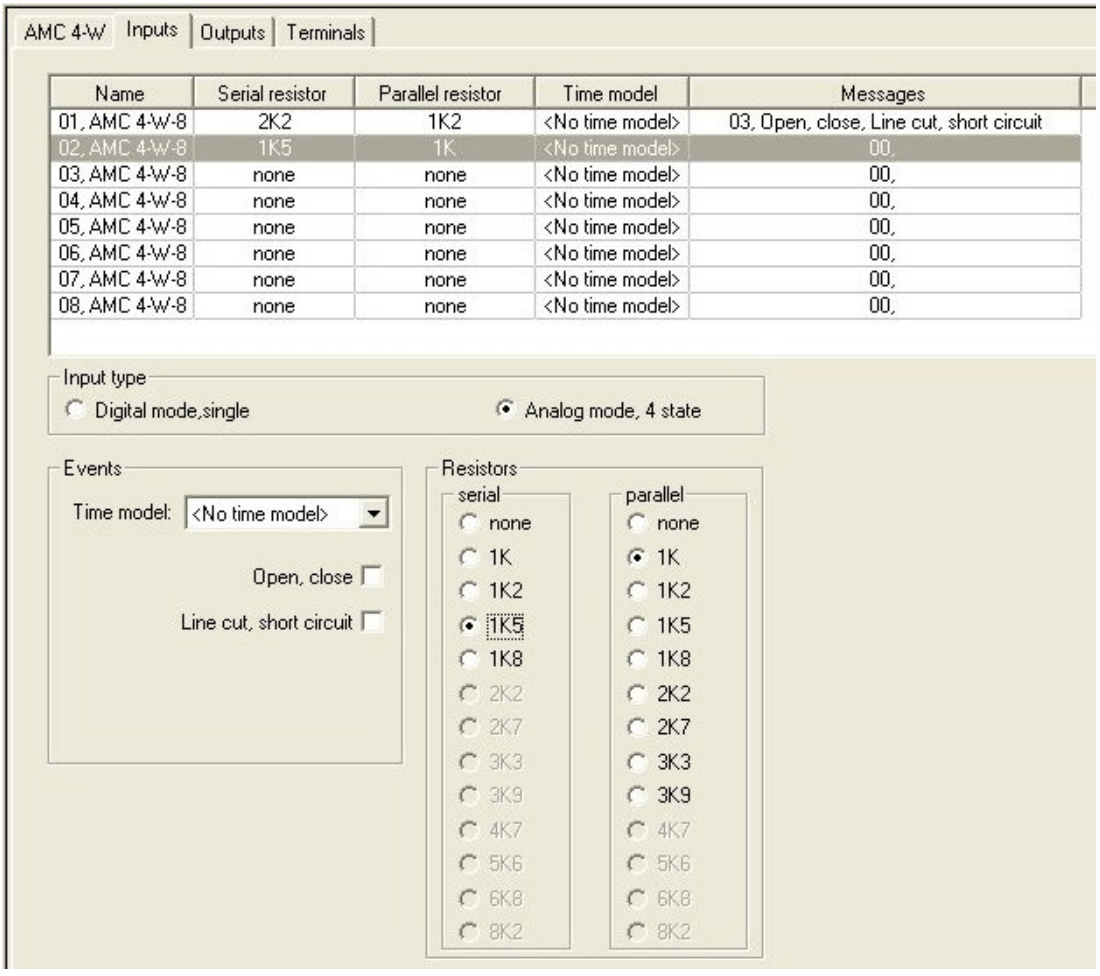
Konfigurowanie parametrów kontrolera AMC

Parametr	Możliwe wartości	Opis
Nazwa kontrolera	Alfanumeryczne z ograniczeniami: 1–16 cyfr	Generowanie identyfikatora (wykonywane domyślnie) gwarantuje niepowtarzalne nazwy, ale użytkownicy mogą je zastąpić. W przypadku zastępowania nazwy należy upewnić się, że identyfikatory są niepowtarzalne.
Opis kontrolera	alfanumeryczne: 0–255 cyfr	Dowolny tekst.
Komunikacja z hostem włączona	0 = wyłączone (pole wyboru nie jest zaznaczone) 1 = włączone (pole wyboru jest zaznaczone)	Domyślne = włączone Ikony nakładki na kontrolerach w drzewie urządzeń oznaczają stan połączenia z hostem (włączone/wyłączone).

		Wyczyszczenie pola wyboru powoduje tymczasowe włączenie trybu offline AMS, aby można było przeprowadzić ponowną konfigurację i wykonać testy. Zaktualizowanie systemu kontroli dostępu do nowej wersji powoduje automatyczne usunięcie zaznaczenia pól wyboru dla wszystkich kontrolerów. Zaznacz i usuń zaznaczenia pól wyboru AMC, aby przetestować je pojedynczo w zaktualizowanym oprogramowaniu.
		Zaznacz to pole wyboru, używając edytora urządzeń do ustawiania DCP (hasła komunikacji urządzenia) w kontrolerze AMC podczas „odgórnej” implementacji DTLS. Zostanie na 15 minut wyświetlone okno do propagowania DCP do AMC. Usuń zaznaczenie, a następnie zaznacz pole wyboru, by ponownie włączyć okno czasowe.
Interfejs kontrolera		
Typ interfejsu	UDP TLS	UDP (= user datagram protocol, protokół datagramów użytkownika), gdy połączenie jest nawiązywane przez się i jeszcze nie ustawiono DCP (device communication password, hasła komunikacji urządzenia) w kontrolerze AMC. TLS (= transport layer security, zabezpieczenie warstwy transportu): po ustawieniu DCP dla AMC komunikacja z MAC odbywa się poprzez DTLS i korzysta z wyższego poziomu zabezpieczeń. W przypadku UDP i TLS należy upewnić się, że przełączniki DIP 1 i 5 na AMC są włączone.
Adres IP/nazwa hosta	Nazwa sieciowa lub adres IP kontrolera AMC	To pole tekstowe jest aktywne tylko po wybraniu **UDP** jako typu portu. 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 przypadku sieci bez protokołu DHCP należy wprowadzić adres IP.
Numer portu	numeryczny: 10001 (domyślnie)	To jest port kontrolera AMC, na którym będą odbierane komunikaty z kontrolera MAC.
Inne parametry		
Program	Alfanumeryczny	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	Wartością domyślną jest „Wspólna”	Ma to znaczenie tylko wtedy, gdy funkcja **Strefy** jest licencjonowana.

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.

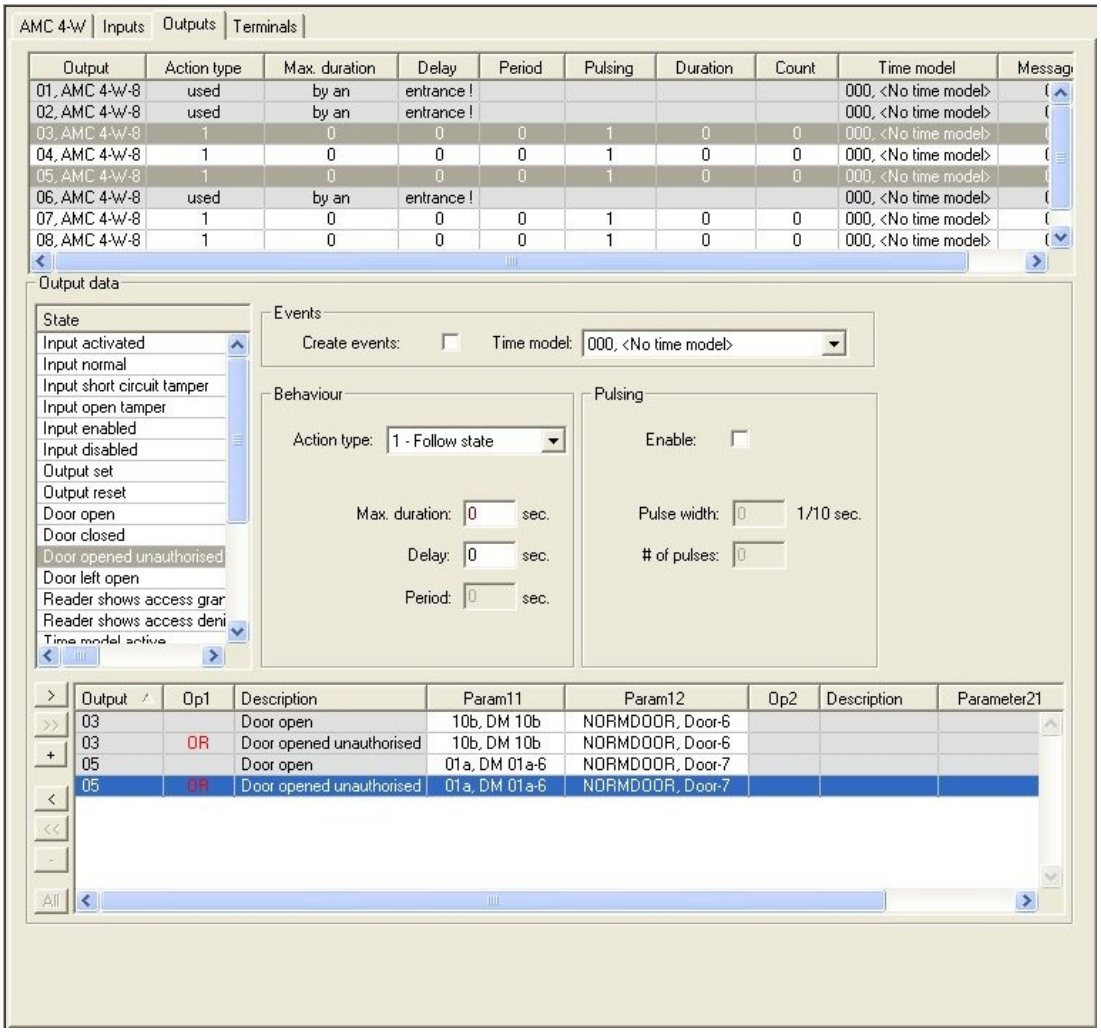
Szeregowy	**Zakres**		**Równoległy**	**Zakres**
„brak” lub „---”	Od 1K do 8K2		„brak” lub „---”	Od 1K do 8K2
1K	Od 1K do 2K2		1K	Od 1K do 1K8
1K2	Od 1K do 2K7		1K2	Od 1K do 2K7

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

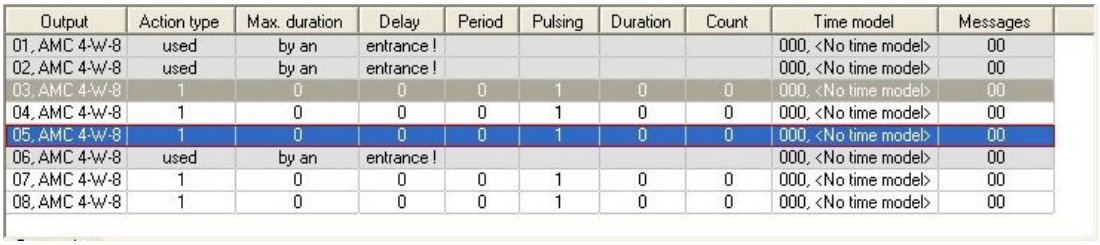
W tym oknie dialogowym można konfigurować poszczególne wyjścia kontrolera AMC lub karty AMC-EXT. Składa się ono z trzech głównych obszarów:

- 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.

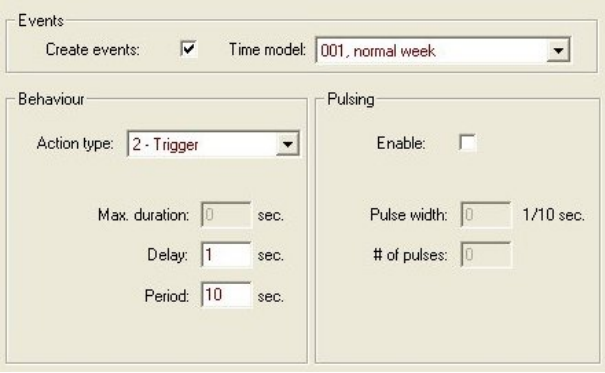
Wiersze zaznaczone przez Ciebie są w kolorze ciemnoszarym.

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**.

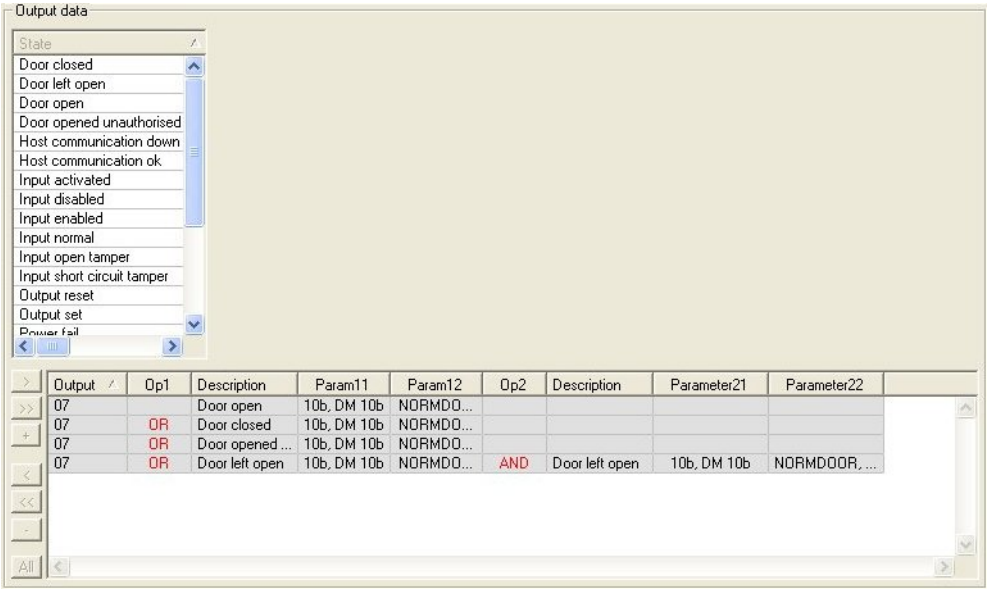
Dla poszczególnych typów czynności można ustawiać następujące parametry:

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
Naprzemiennie	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 wyzwalania wyjść przez określone stany

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

– Zaznacz jedno lub więcej 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 wejście z tym stanem 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 z logicznym operatorem LUB 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 stan. Do niego jest dodawany warunek poprzez wybranie w dowolnej kolumnie.
– Następnie wybiera się inny stan 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 warunków LUB.
Każdy warunek może zawierać tylko **jeden** warunek I.

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

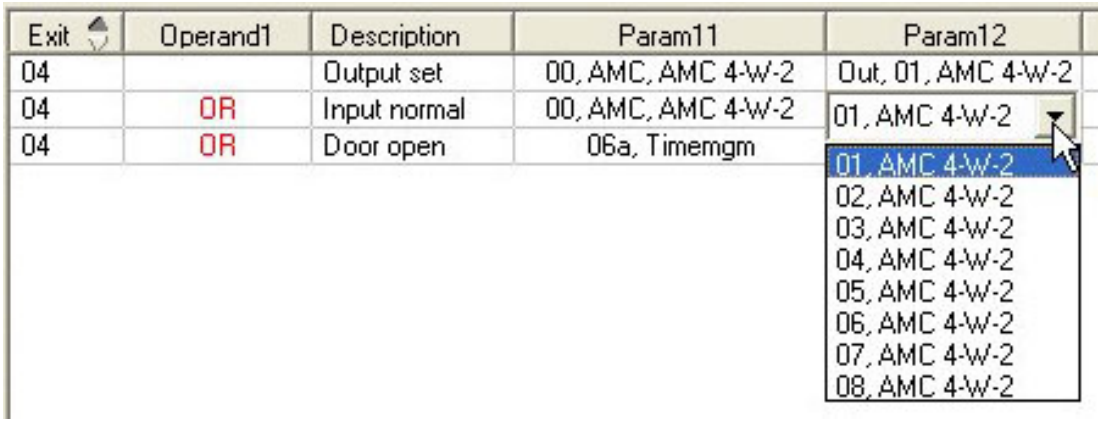
– Zaznacz przypisaną pozycję w dowolnej kolumnie.
– Następnie kliknij przycisk All, a ten status zostanie utworzony dla wszystkich istniejących urządzeń i instalacji.

Modyfikowanie parametrów wyjść

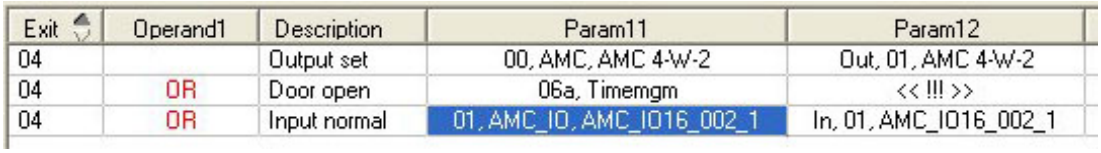
Wiersze na liście można modyfikować
Jeżeli istnieje kilka urządzeń lub instalacji, w których przypisany status może zaistnieć, zawsze się ustawia pierwsze urządzenia i instalacje danego typu.
W kolumnach **Param11** i **Param21** (ze skrótami AND) są wyświetlane urządzenia (na przykład „Kontroler AMC, 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 wyłączono	5	Dezaktywacja lokalnego wejścia przez model czasowy
Wejście włączono	6	Aktywacja 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	---
Komunikat z czytnika	23	Adres czytnika
Komunikat z LAC	24	Numer modułu
Kontrola karty	25	Adres czytnika, funkcja kontrolna karty.

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 urządzenia zewnętrznego 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 jednocześnie wysyłany komunikat do urządzenia zewnętrznego:

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

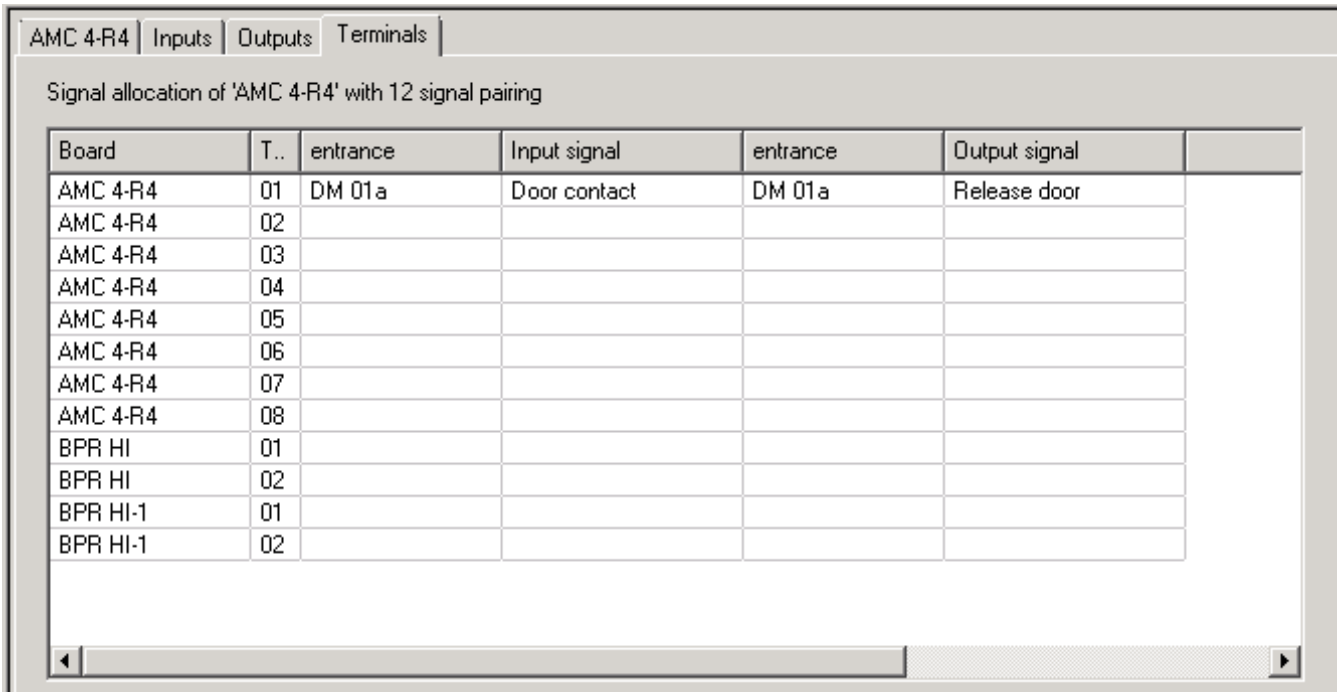
Lista wszystkich istniejących stanów z wartościami domyślnymi dla parametrów 11/21 i 12/22:

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				

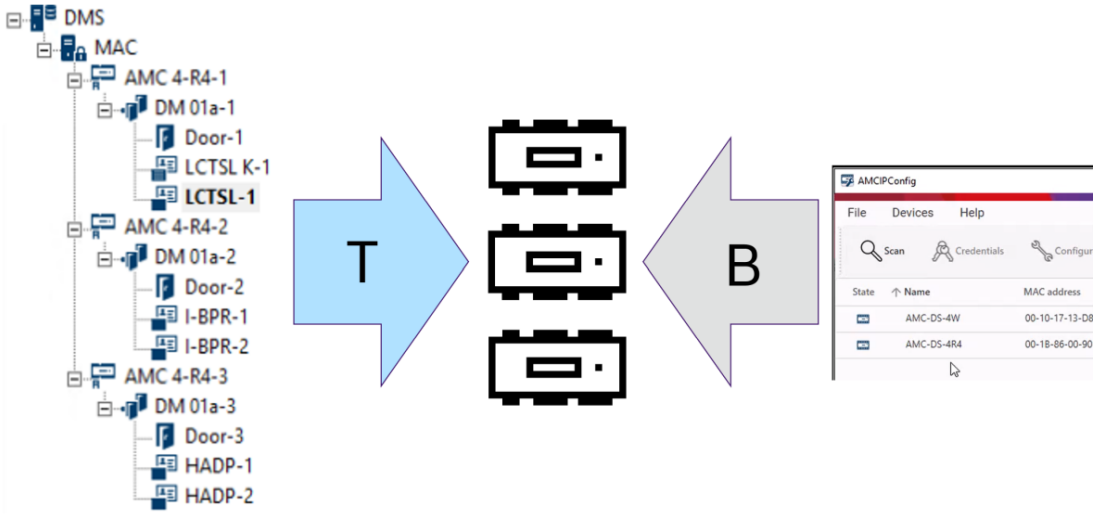
15 Konfigurowanie DTLS do bezpiecznej komunikacji

Wstęp

System kontroli dostępu (ACS) oferuje komunikację między urządzeniami na bardzo wysokim poziomie bezpieczeństwa dzięki zastosowaniu DTLS. Możliwe są dwa główne sposoby wdrażania komunikacji DTLS między urządzeniami w ACS:

Wdrożenie odgórne (T) wykonywane w edytorze urządzeń w ACS.

Wdrożenie oddolne (B) realizowane głównie za pomocą narzędzia AMCIPConfig , ale edytor urządzeń jest konieczny do zakończenia procesu.



- (T) Wdrożenie odgórne może być wykonane w edytorze urządzeń na dwa sposoby:
  - Za pomocą hasła do komunikacji z pojedynczym urządzeniem (DCP) na poziomie DMS dla wszystkich AMC,
  - Używanie kilku DCP dla różnych gałęzi drzewa urządzeń, począwszy od odpowiednich MAC lub AMC.
- (B) Wdrożenie odgórne można też zainicjować na dwa różne sposoby za pomocą narzędzia AMCIPConfig:
  - Za pomocą klucza sprzętowego AMC
  - Za pomocą losowego klucza LCD

Uwaga!

Wdrożenie oddolne wciąż wymaga konfiguracji DCP w edytorze urządzeń.

Wdrożenie odgórne pozwala skonfigurować DCP w urządzeniu AMC. Trzeba jednak ustawić taką samą wartość DCP w tym samym AMC również w edytorze urządzeń, aby umożliwić pełną komunikację DTLS między MAC i AMC.

Podsumowanie opcji wdrażania DTLS

	Krótki opis	Zalety	Wady
Od góry	Administrator systemu wprowadza silne hasło w **edytorze urządzeń**. Na podstawie tego hasła system generuje **klucz główny**, który jest propagowany odgórnie w	Szybkie, proste, wdrażanie.	W trakcie propagowania klucza głównego do kontrolerów drzwi AMC strumienie danych wysyłane i

	Krótki opis	Zalety	Wady
	całym drzewie urządzeń kontroli dostępu, od DMS przez MAC aż po kontrolery drzwi AMC. Do całego drzewa urządzeń można ustawić jedno hasło lub różne hasła do różnych gałęzi drzewa.		odbierane przez urządzenia nie są chronione przez DTLS.
Od dołu z użyciem klucza sprzętowego AMC	Administrator systemu używa narzędzia **AMC IPConfig** do wdrożenia protokołu DTLS na poziomie kontrolerów drzwi AMC.	Większe zróżnicowanie i elastyczność wdrożeń. Metoda ta pozwala uniknąć największej wady wdrażania odgórnego, jaką jest sporadyczne przekazywanie klucza głównego bez zabezpieczenia. Wymaga to jednak zabezpieczenia połączenia z narzędzia AMCIPConfig do kontrolera AMC podczas ustawiania DCP.	W trakcie konfigurowania DCP w AMC przez narzędzie IPConfig należy zapewnić bezpieczną komunikację za pomocą innych środków. Można na przykład podłączyć kontroler AMC bezpośrednio do komputera, na którym uruchomione jest narzędzie IPConfig. DCP skonfigurowane w narzędziu IPConfig muszą być również skonfigurowane na tych samych kontrolerach AMC za pomocą edytora urządzeń.
Metoda konfiguracji od dołu za pomocą losowego klucza LCD		Większe zróżnicowanie i elastyczność wdrożeń. Ta metoda zapewnia najwyższe bezpieczeństwo, ponieważ klucz LCD nie jest w ogóle przesyłany przez sieć, więc poświadczenia są chronione przez cały czas.	Bardziej skomplikowane i czasochłonne wdrażanie. Losowy klucz LCD składający się z 27 symboli należy przesłać do narzędzia IP Config w inny sposób niż przez sieć.
Szczegóły i instrukcje znajdują się w kolejnych częściach tego rozdziału.			

Terminologia DTLS

DCP (hasło do komunikacji z urządzeniem)	Pojedyncze silne hasło, na podstawie którego ACS generuje wewnętrzny klucz główny. Hasło musi być bezpieczne, ponieważ nie jest przechowywane w systemie ACS.
Klucz główny	Kod generowany przez system z poziomu DCP, używany do zabezpieczania urządzeń kontroli dostępu. Klucz główny nigdy nie jest widoczny dla żadnego użytkownika.
Losowy klucz LCD	Tymczasowy kod alfanumeryczny generowany na nowo przez kontroler AMC przy każdym uruchomieniu. Klucz może być wyświetlany na ekranie ciekłokrystalicznym (LCD) kontrolera AMC i może być wymagany przez oprogramowanie narzędziowe do uwierzytelniania komunikacji w sieci.
Klucz sprzętowy AMC .	Wewnętrzny kod uwierzytelniający generowany przez kontroler AMC na podstawie określonych parametrów sprzętowych. Nie jest on widoczny dla użytkownika.

15.1 Wdrażanie DTLS od góry

Wymagania wstępne

– AMS 4.0 lub BIS-ACE 4.9.1 lub nowszy.
– Drzewo urządzeń kontroli dostępu z DMS do AMC jest skonfigurowane fizycznie i podłączone do sieci, ale AMC nie są włączone. Jeśli opcja jest włączona, oznacza to, że pola wyboru kontrolerów AMC **Komunikacja z hostem włączona** są zaznaczone.
– DTLS nie został jeszcze skonfigurowany w kontrolerach AMC za pomocą jednej z metod konfiguracji od dołu za pomocą narzędzia IPConfig.

Procedura: Jeden DCP dla wszystkich

1. W systemie ACS otwórz edytor urządzeń

– Menu główne AMS > **Konfiguracja** > **Dane urządzenia** > **Drzewo urządzeń** 
– Zostanie wyświetlone okno dialogowe z prośbą o wprowadzenie silnego hasła komunikacji z urządzeniem (DCP).

2. Aby ustawić pojedyncze DCP do wszystkich AMC w drzewie urządzeń, należy wprowadzić i potwierdzić silne hasło zgodnie z lokalnymi zasadami dotyczącymi haseł.
– W oknie dialogowym wyświetlana jest informacja zwrotna o sile hasła na podstawie entropii hasła .
3. Zanotuj hasło, ponieważ nie jest ono przechowywane w systemie ACS.
4. Kliknij przycisk **OK**, aby zamknąć okno dialogowe.

Procedura alternatywna: wiele DCP do różnych gałęzi drzewa urządzeń

1. W systemie ACS otwórz edytor urządzeń

– Menu główne AMS > **Konfiguracja** > **Dane urządzenia** > **Drzewo urządzeń** 
– Zostanie wyświetlone okno dialogowe z prośbą o wprowadzenie silnego hasła komunikacji z urządzeniem (DCP).
2. Kliknij przycisk **Anuluj**, aby ustawić różne DCP w różnych gałęziach drzewa urządzeń (MAC i AMC).
– W podręcznym oknie dialogowym zostanie wyświetlona informacja, ile kontrolerów AMC w systemie nie posiada jeszcze DCP.
– W edytorze urządzeń zostanie otwarte drzewo urządzeń.
3. Rozwiń drzewo urządzeń, aby wybrać MAC lub AMC, do którego chcesz ustawić DCP.
– Jeśli ustawisz DCP na poziomie MAC, zostanie ono ustawione we wszystkich podrzędnych AMC danego MAC.
– Jeśli ustawisz DCP na poziomie AMC, zostanie ono ustawione tylko dla tego AMC.
4. Kliknij przycisk wielokropka ... obok pola tekstowego **Hasło do komunikacji z urządzeniem:**
5. Wprowadź i potwierdź silne hasło zgodnie z lokalnymi zasadami dotyczącymi haseł.
6. Zanotuj dokładnie hasło i gałąź, której ono dotyczy, ponieważ nie jest ono przechowywane w ACS.
7. Powtórz tę procedurę dla każdego MAC lub AMC, dla których chcesz ustawić oddzielne DCP.
8. Kliknij przycisk **OK**, aby zamknąć okno dialogowe.

Wynik wdrożenia od góry

ACS używa jednego lub kilku DCP do wygenerowania kluczy wewnętrznych dla wszystkich AMC poniżej wybranego DMS lub MAC.

Nie trzeba powtarzać tej procedury, o ile nie zmieniono DCP w jednym lub kilku urządzeniach AMC za pomocą narzędzia AMC IPConfig (patrz wdrażanie od dołu). W takim przypadku należy natychmiast ustawić to samo DCP od góry na tych samych AMC w edytorze urządzeń.

Jeśli później dodasz urządzenia w drzewie urządzeń podrzędne względem DMS i MAC, które mają już DCP, to nowe urządzenia automatycznie przejmą to samo DCP od urządzeń nadrzędnych.

16 Konfigurowanie wejść

16.1 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
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.

16.2 Tworzenie wejść

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

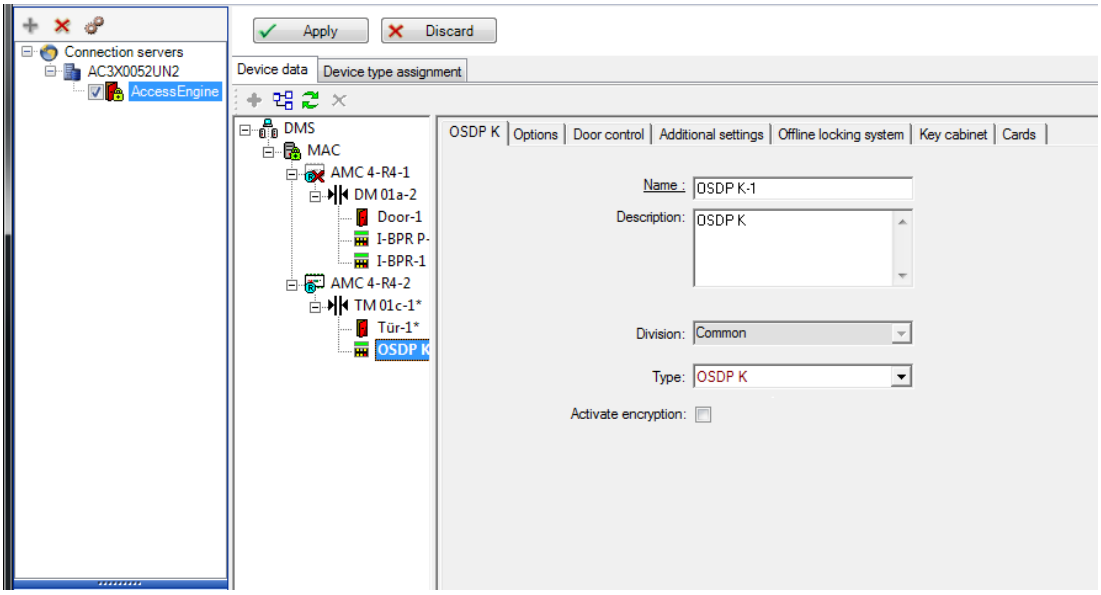
- Dla kontrolerów typu **AMC 4W** są dostępne tylko czytniki Wiegand, z klawiaturą lub bez.
- Dla kontrolerów typu **AMC 4R4** są dostępne czytniki podane w tabeli poniżej. Nie mieszaj protokołów na tym samym kontrolerze.

Nazwa czytnika	Protokół Wiegand	Protokół BPR(*)	Protokół I-BPR	Protokół HADP	Protokół OSDP
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			
TB15 HI1		X			
TB30 LE		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 LCD)				X	

RK40 (z klawiaturą)				X	
R15				X	
R30				X	
R40				X	
RK40				X	
RKL55				X	

(*) Protokół BPR został wycofany i jest on uwzględniony tu, tylko ze względu na kompatybilności.

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



Bezpieczna komunikacja z OSDP

Domyślnie pole wyboru **Uaktywnij szyfrowanie** nie jest zaznaczone. Zaznacz je, aby używać czytników z obsługą **bezpiecznego kanału OSDPv2**.

Jeśli później wyłączysz szyfrowanie poprzez usunięcie zaznaczenia tego pola wyboru, zresetuj sprzęt czytnika zgodnie z instrukcjami producenta.

Aby zapewnić dodatkowe zabezpieczenie, każda próba wymiany skonfigurowanego modułu czytnika OSDP na inny moduł czytnika OSDP wyzwala alarm w systemie kontroli dostępu. Operator może potwierdzić alarm w urządzeniu klienckim i jednocześnie zaakceptować wymianę.

Komunikat alarmowy: **Odmowa wymiany czytnika OSDP**

Polecenie: **Zezwalaj na wymianę czytnika OSDP**

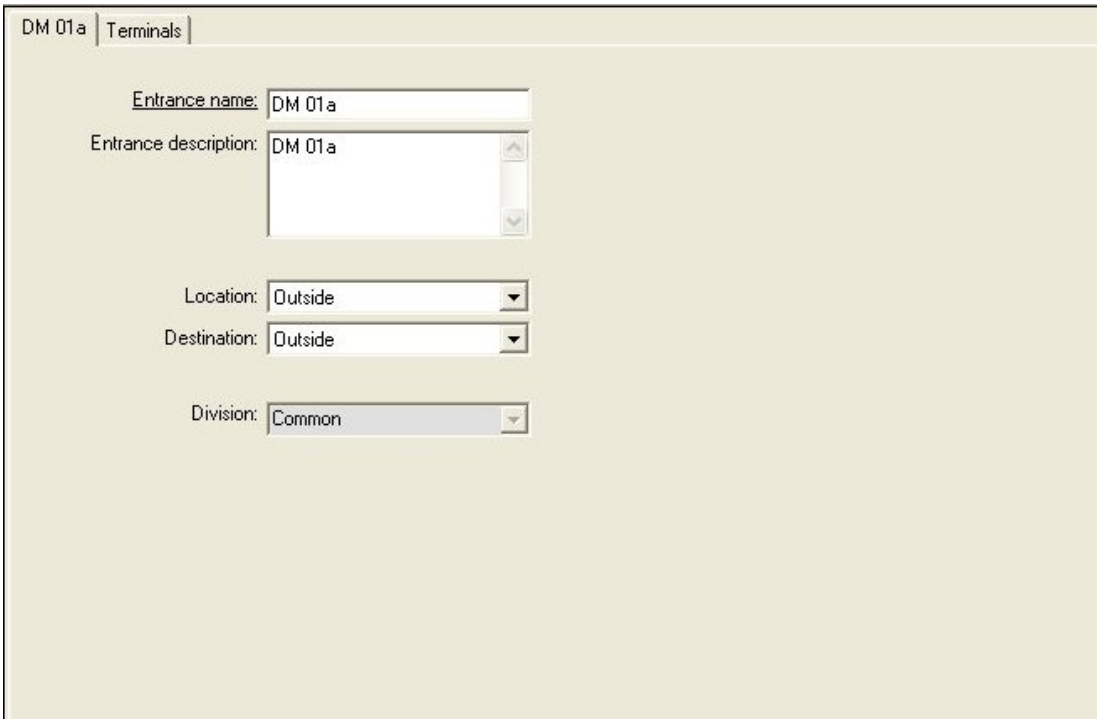
Dostępne są następujące typy czytników OSDP:

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.
Jeżeli dezaktywujesz szyfrowanie poprzez usunięcie zaznaczenia pola wyboru na karcie OSDP czytnika w edytorze urządzeń, musisz zresetować sprzęt czytnika zgodnie z instrukcją producenta.

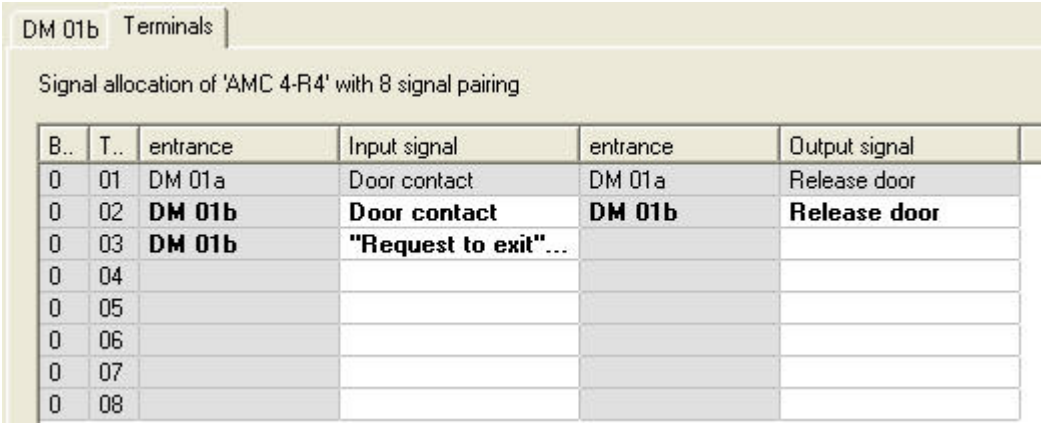


Parametr	Możliwe wartości	Opis

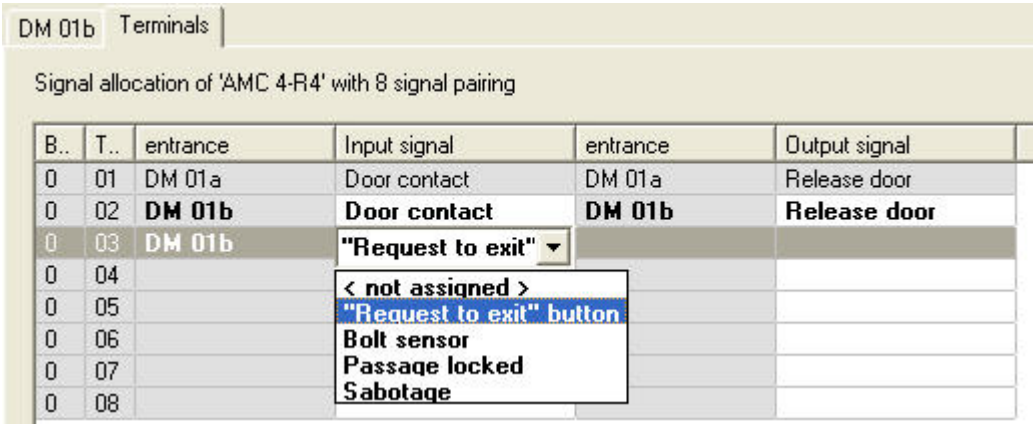
Nazwa wejścia	Alfanumeryczne, od 1 do 16 znaków	Okno dialogowe generuje unikatową nazwę wejścia, ale w razie potrzeby może ją zastąpić operator konfigurujący wejście.
Opis wejścia	Alfanumeryczne, od 0 do 255 znaków	Dowolny tekst opisowy do wyświetlenia w systemie.
Lokalizacja	Dowolny zdefiniowany obszar (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 od zewnętrznego systemu lub urządzenia podłączonego do jednego z wejść.
Strefa	Zdefiniowana strefa, do której należy czytnik. Wartością domyślną jest **Wspólna**	Ma to znaczenie tylko wtedy, gdy funkcja **Strefy** jest licencjonowana.
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.

16.3 Konfigurowanie terminali kontrolerów AMC

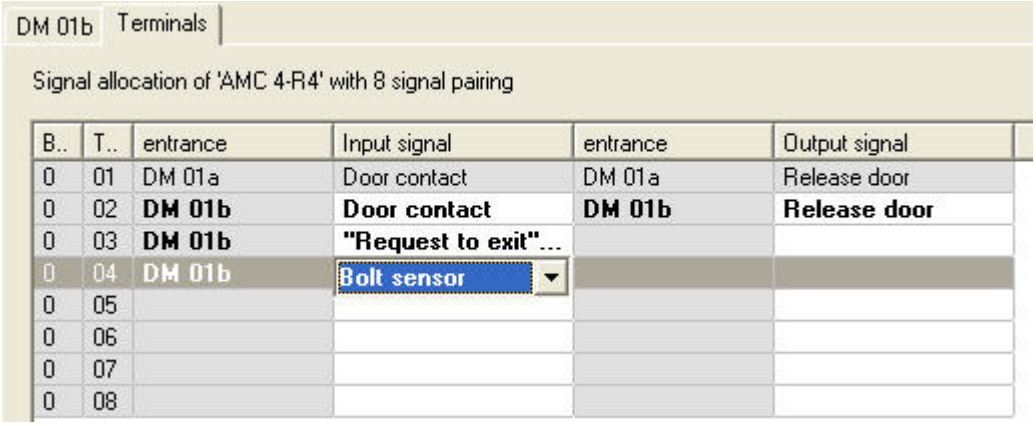
Pod względem zawartości i struktury ta karta jest identyczna z kartą **Terminale** w ustawieniach kontrolera AMC.



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:



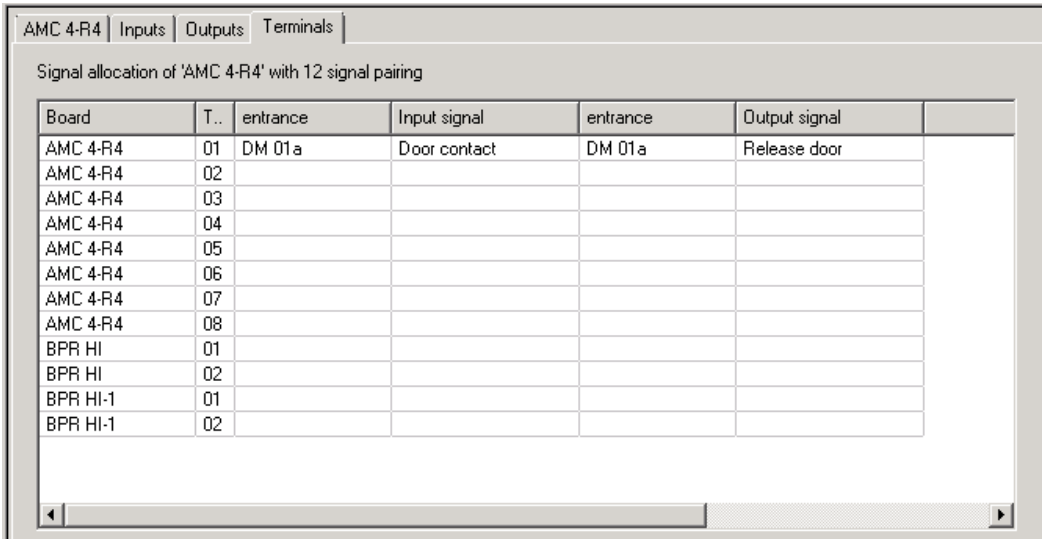
Przypisania sygnałów nieodpowiednie dla edytowanego wejścia są tylko do odczytu i mają szare tło. Można je edytować tylko po wybraniu odpowiedniego wejścia.
Podobne szare tło i blady kolor pierwszego planu są ustawiane dla wyjść, których parametry skonfigurowano karcie **Wyjścia** w ustawieniach kontrolera 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
Kontaktron drzwiowy	
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.
Układ antysabotażowy	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.
Wycisz alarm nieautoryzowanego otwarcia	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 nie zaakceptuje dostępu

Tabela sygnałów wyjściowych

Sygnały wyjściowe	Opis
Zwolnienie 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.
Światło stopu zielone	Zielony wskaźnik świeci, kiedy drzwi są otwarte.
Upłynął maksymalny czas otwarcia drzwi lub Naruszona ochrona drzwi	Jeżeli drzwi są przytrzymywane w pozycji otwarcia lub otwarte zbyt długo
Nawiązywanie połączenia z kamerą	Kamera zostanie włączona na początku przejścia.
Zwolnienie wejścia bramki obrotowej	
Zwolnienie wyjścia bramki obrotowej	
Drzwi są niezablokowane	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	- Kontaktron drzwiowy - Przycisk żądania wyjścia - Czujnik rygla - Wejście zablokowane	- Zwolnienie drzwi - Śluza: blokada przeciwnych drzwi - Wyciszenie alarmu

	Czytniki do rejestracji czasu i obecność Funkcjonalność zewnętrznej decyzji o dostępie	- Układ antysabotażowy - Włączenie otwarcia lokalnego - Zewnętrzne decyzje o dostępie — zaakceptowano - Zewnętrzne decyzje o dostępie — odmowa	- Światło stopu zielone - Nawiązywanie połączenia z kamerą - Upłynął maksymalny czas otwarcia drzwi lub Naruszona ochrona drzwi - 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 - Układ antysabotażowy - Zewnętrzne decyzje o dostępie — zaakceptowano - Zewnętrzne decyzje o dostępie — odmowa	- Śluza: blokada przeciwnych drzwi - Zwolnienie wejścia bramki obrotowej - Zwolnienie wyjścia bramki obrotowej - Wyciszenie alarmu - Nawiązywanie połączenia z kamerą - Upłynął maksymalny czas otwarcia drzwi lub - Naruszona ochrona drzwi - 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	- Kontaktron drzwiowy - Przycisk żądania wyjścia - Wejście zablokowane - Przejście zakończone - Zewnętrzne decyzje o dostępie — zaakceptowano - Zewnętrzne decyzje o dostępie — odmowa	- Zwolnienie drzwi - Wyciszenie alarmu - Światło stopu zielone - Upłynął maksymalny czas otwarcia drzwi lub - Naruszona ochrona drzwi - Drzwi są niezablokowane - 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	- Kontaktron drzwiowy - Przycisk żądania wyjścia - Wejście zablokowane - Przejście zakończone - Zewnętrzne decyzje o dostępie — zaakceptowano - Zewnętrzne decyzje o dostępie — odmowa	- Zwolnienie drzwi - Wyciszenie alarmu - Światło stopu zielone - Upłynął maksymalny czas otwarcia drzwi lub - Naruszona ochrona drzwi - Drzwi są niezablokowane - 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	- Kontaktron drzwiowy - Przycisk żądania wyjścia - System sygnalizacji włamania gotowy do uzbrojenia - System sygnalizacji włamania jest uzbrojony - Układ antysabotażowy - Żądanie uzbrojenia systemu sygnalizacji włamania - Zewnętrzne decyzje o dostępie — zaakceptowano - Zewnętrzne decyzje o dostępie — odmowa	- Zwolnienie drzwi - Nawiązywanie połączenia z kamerą - Uzbrojenie systemu sygnalizacji włamania - Rozbrojenie systemu sygnalizacji włamania - Upłynął maksymalny czas otwarcia drzwi lub - Naruszona ochrona drzwi - Zewnętrzne decyzje o dostępie — aktywowano
14	Proste drzwi z czytnikiem wejścia i wyjścia oraz funkcją uzbrojenia/ rozbrojenia systemu sygnalizacji włamania Czytniki do rejestracji czasu i obecność	- Kontaktron drzwiowy - Przycisk żądania wyjścia - System sygnalizacji włamania gotowy do uzbrojenia - System sygnalizacji włamania jest uzbrojony - Układ antysabotażowy - Żądanie uzbrojenia systemu sygnalizacji włamania	- Zwolnienie drzwi - Nawiązywanie połączenia z kamerą - Uzbrojenie systemu sygnalizacji włamania - Upłynął maksymalny czas otwarcia drzwi lub - Naruszona ochrona drzwi
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.

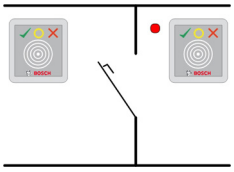
Edytowanie sygnałów

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.

16.4 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

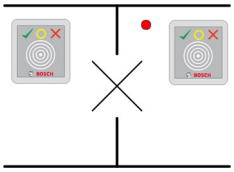
Możliwe sygnały:

Sygnały wejściowe	**Sygnały wyjściowe**
Kontaktron drzwiowy	Zwolnienie drzwi
Przycisk żądania wyjścia	Śluza: blokada przeciwnych drzwi
Układ antysabotażowy	Światło stopu zielone
Wycisz alarm nieautoryzowanego otwarcia	Nawiązywanie połączenia z kamerą
	Upłynął maksymalny czas otwarcia drzwi lub Naruszona ochrona drzwi

Uwaga!
Funkcje 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

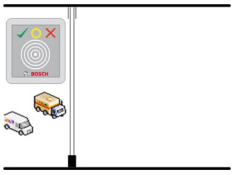
Możliwe sygnały:

Sygnał wejściowy	**Sygnały wyjściowe**
Bramka obrotowa w pozycji normalnej	Zwolnienie wejścia bramki obrotowej
Przycisk żądania wyjścia	Zwolnienie wyjścia bramki obrotowej
Układ antysabotażowy	Wejście zablokowane
Wycisz alarm nieautoryzowanego otwarcia	Nawiązywanie połączenia z kamerą
	Upłynął maksymalny czas otwarcia drzwi lub Naruszona ochrona drzwi
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**
Kontaktron drzwiowy	Zwolnienie drzwi
Przycisk żądania wyjścia	Drzwi są niezablokowane
Wejście zablokowane	Światło stopu zielone
Przejście zakończone	Wyciszenie alarmu
	Upłynął maksymalny czas otwarcia drzwi lub Naruszona ochrona drzwi

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 dla tego modelu drzwi nie kontrolują drzwi ani barier, ale tylko przesyłają dalej dane karty do systemu zarządzania czasem i obecnością Czytniki te są zwykle usytuowane w miejscach, do których dostęp został już sprawdzony.
Dlatego nie określono żadnych sygnałów.

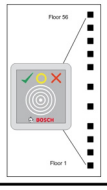
Uwaga!
Aby można było tworzyć prawidłowe pary rezerwacji (czas wejścia + czas wyjścia) w systemie zarządzania czasem i obecnością, trzeba skonfigurować parametry na dwóch oddzielnych czytnikach z modelem drzwi 06: jednym do rejestrowania wejść i jednym do rejestrowania wyjść.

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. 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
`<SW_installation_folder>\AccessEngine\AC\TAExchange\`
w pliku tekstowym `TAccExc_EXP.txt`, 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 zawiera wszystkie rejestracje w kolejności chronologicznej ich otrzymywania. Separatorem pól w tym pliku jest średnik.

Warianty modelu wejścia 07



Warianty modelu:

07a	Winda obsługująca maksymalnie 56 pięter
07c	Winda z maks. 56 pięter i model czasowy

Model wejścia 07a
Sygnały:

Sygnał wejściowy	**Sygnały wyjściowe**

	Zwolnienie <nazwa piętra>
	Jeden sygnał wyjściowy dla każdego zdefiniowanego piętra, maksymalnie 56.

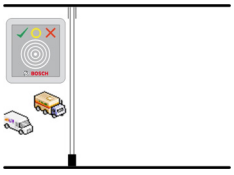
Po przywołaniu windy właściciel karty może wybrać tylko te piętra, dla których jego karta jest autoryzowana.
Modeli drzwi z windą nie można łączyć z innymi modelami drzwi na tym samym kontrolerze. Używając modułu rozszerzeń, dla każdej windy skonfigurowanej w kontrolerze AMC można zdefiniować nawet 56 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

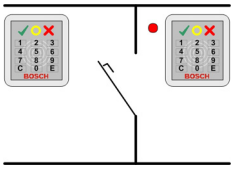


Możliwe sygnały:

Sygnały wejściowe	**Sygnały wyjściowe**
Kontaktron drzwiowy	Zwolnienie drzwi
Przycisk żądania wyjścia	Drzwi są otwarte na długo
Wejście zablokowane	Sygnalizator świetlny ma kolor zielony
Przejście zakończone	Wyciszenie alarmu
	Upłynął maksymalny czas otwarcia drzwi lub Naruszona ochrona drzwi

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**
Kontaktron drzwiowy	Zwolnienie 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	Nawiązywanie połączenia z kamerą
Czujnik rygla	Upłynął maksymalny czas otwarcia drzwi lub Naruszona ochrona drzwi
Układ antysabotażowy	
Wycisz alarm nieautoryzowanego otwarcia	
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 szeregowe (w tym I-BPR, HADP i OSDP)

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 (#).

Czytniki Wiegand (w tym protokół szeregowy BPR)
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.]

Wejścia specjalne
Modele do ochrony wejścia wyposażone w funkcje specjalne, takie jak:
- Windy
- Wykrywanie włamania
- Uniwersalne przełączniki cyfrowe lub binarne
- Śluzy

są opisane w odnośnym rozdziale poświęconym wejściom specjalnym.

Patrz
- *Wejścia specjalne, Strona 96*

16.5 Wejścia specjalne

16.5.1 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

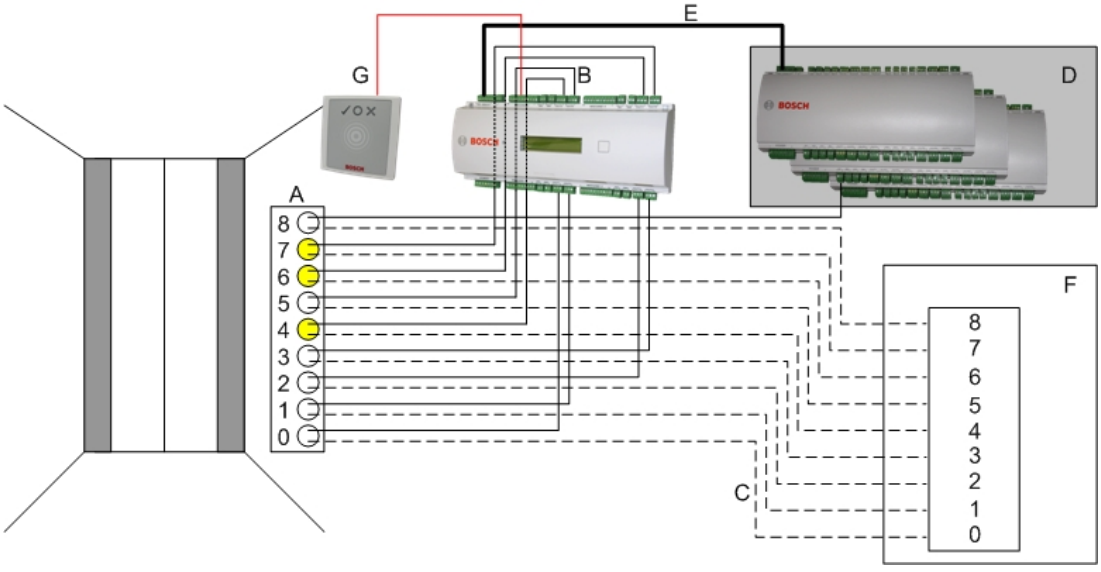
W oknach dialogowych uprawnień dostępu w systemie można przypisać określone piętra do autoryzacji osoby.

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:

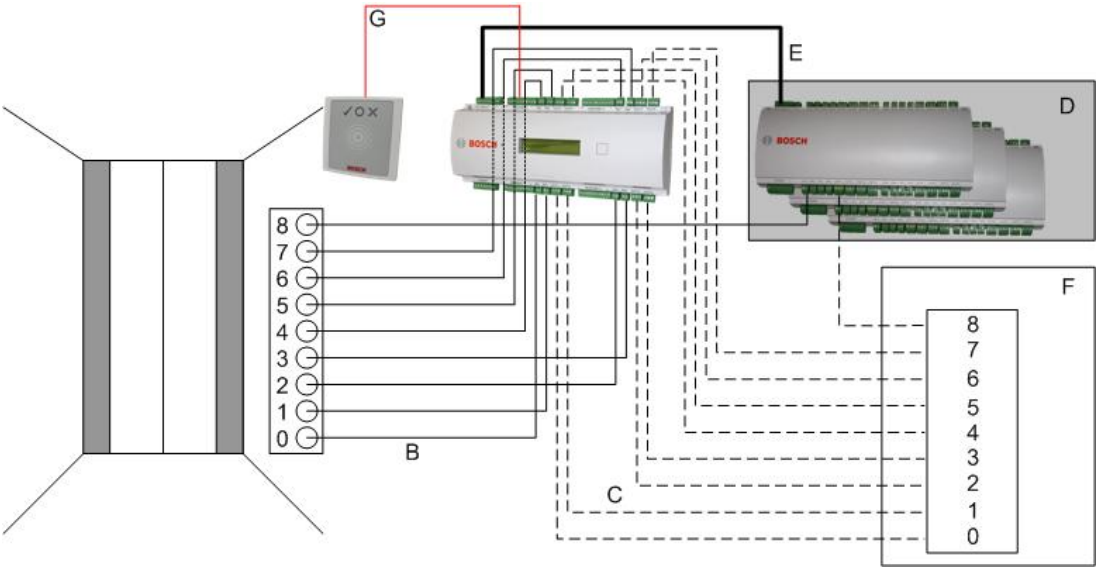
Poniższa ilustracja przedstawia schemat połączeń windy w modelu drzwi 07a.



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.



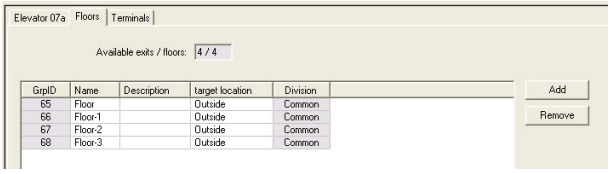
Legenda:

- 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.

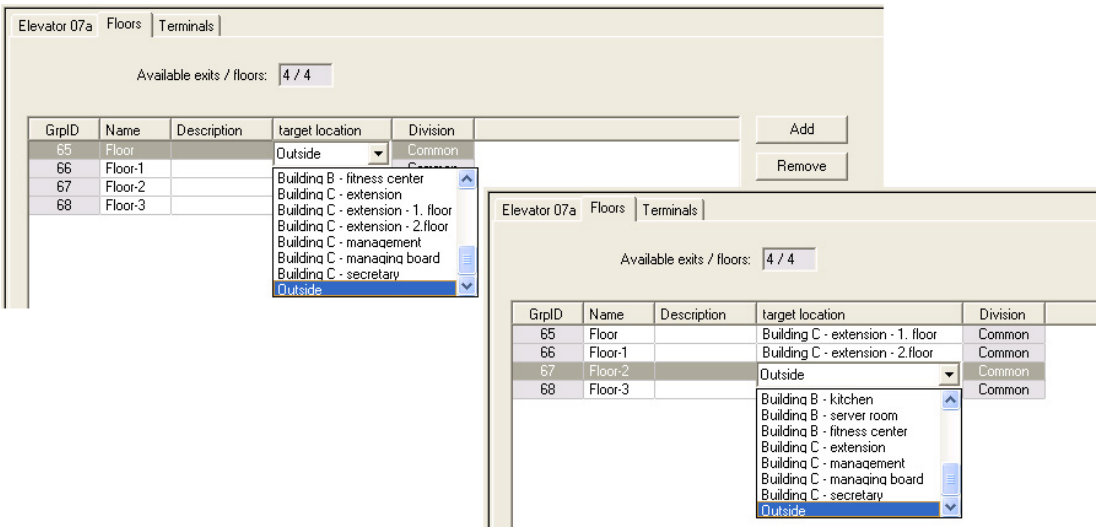
Podobnie jak parkingi, windy mają parametr **Publiczny.** Ten parametr można ustawić dla każdego piętra indywidualnie. Po aktywowaniu parametru **Publiczny** nie są sprawdzane uprawnienia dostępu, więc każdy posiadacz karty w windzie może wybrać piętro.
W razie potrzeby ustaw model czasowy dla modelu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

Piętra dla modelu wejścia 07

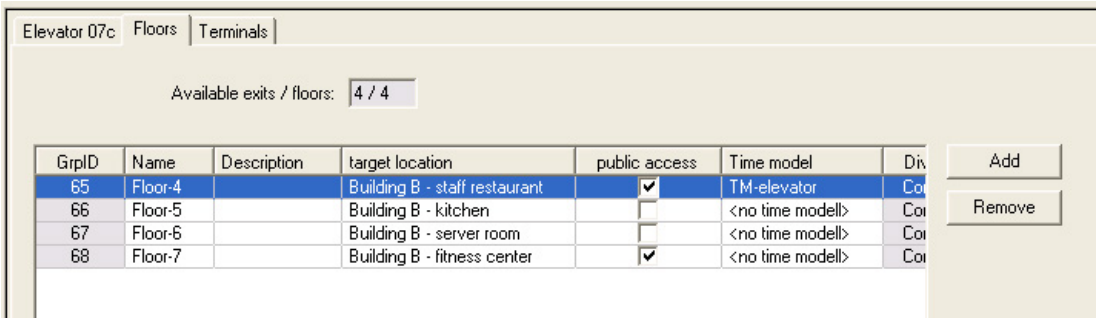
Na karcie **Piętra** za pomocą przycisków **Dodaj** i **Usuń** można dodawać i usuwać piętra obsługiwane przez windę.



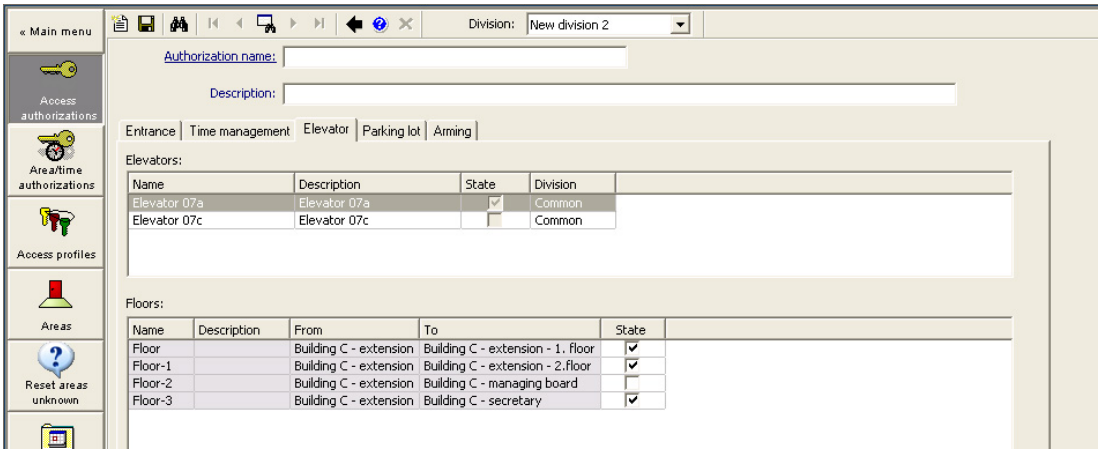
Lokalizacjami docelowymi piętra mogą być dowolne **obszary**, z wyjątkiem parkingów i stref parkowania.
Każdemu piętru można przypisać tylko jeden obszar. W związku z tym wybór obszarów dostępnych w polach kombi zmniejsza się po każdym przypisaniu, co zapobiega niezamierzonemu dublowaniu przypisań.



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 **Uprawnienia dostępu** i **Uprawnienia obszarowe/czasowe** zaznacz najpierw wymaganą windę, a następnie pod spodem piętra, do których ma dostęp posiadacz karty.



16.5.2 Modele drzwi z alarmami antywłamaniowymi (model drzwi 14)

Wstęp

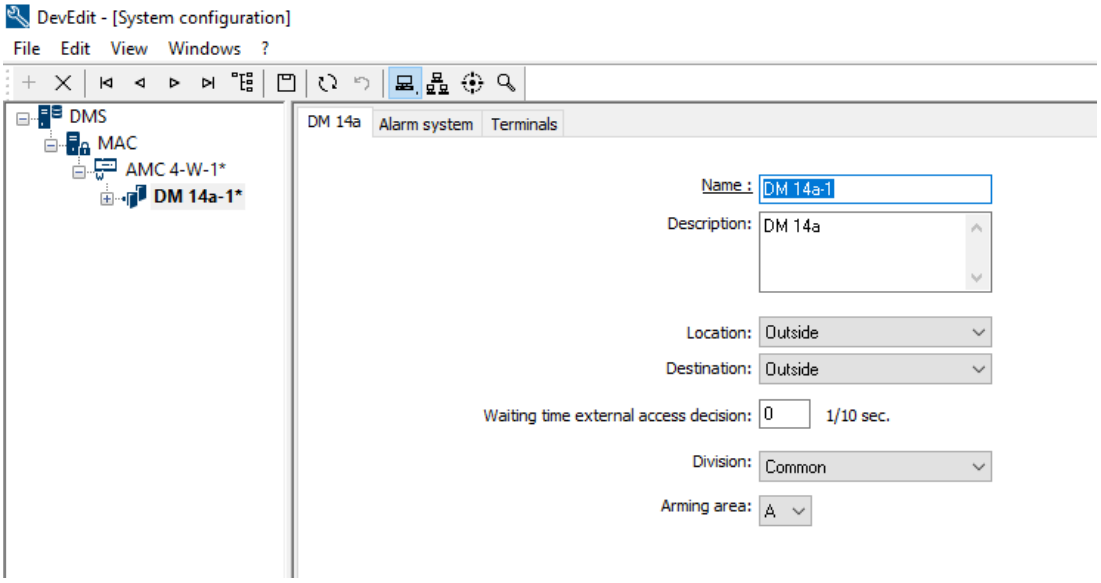
W przeciwieństwie do modelu wejść 10 (DM10) model **DM14** umożliwia uzbrojenie lub rozbrojenie alarmu systemu sygnalizacji włamania dla konkretnego obszaru uzbrojenia. Można też skonfigurować wejście DM14, aby przyznać dostęp posiadaczowi karty, o ile posiadacz karty ma wszystkie inne wymagane uprawnienia dostępu.
W ramach procedury konfiguracji DM14 w edytorze urządzeń i menedżerze okien dialogowych wykonywane są następujące zadania:

1. Ustawianie parametrów ogólnych identyfikujących wejście i jego obszar uzbrojenia.
2. Ustawianie określonych parametrów w celu określenia dokładnej procedury rozbrojenia obszaru.
3. Definiowanie właściwych sygnałów wejściowych i wyjściowych systemu sygnalizacji włamania dla poszczególnych styków kontrolera drzwi wejściowych.
4. Określanie uprawnień uzbrajania/rozbrajania w uprawnieniach dostępu tych posiadaczy kart, którzy mają korzystać z wejść typu DM 14.

Te zadania są opisane w poniższych sekcjach.

Parametry ogólne

Na pierwszej karcie **DM14a** lub **DM14b** ustaw następujące parametry.

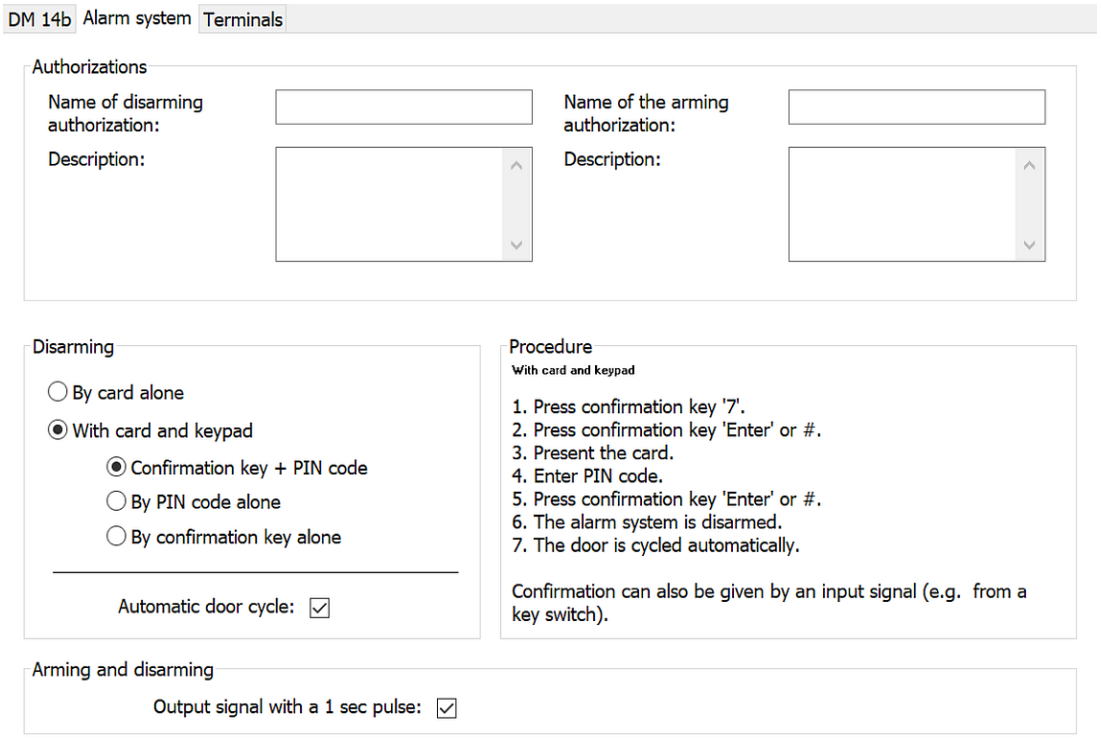


Parametr	Typ wartości	Opis
Nazwa	Dowolny tekst	Nazwa wejścia.
Opis	Dowolny tekst, opcjonalnie	Opis wejścia.

Parametr	Typ wartości	Opis
Lokalizacja	Lista zdefiniowanych obszarów, jeśli używane	Obszar dostępu, w którym znajduje się wejście.
Obszar docelowy	Lista zdefiniowanych obszarów, jeśli używane	Obszar dostępu, do którego prowadzi wejście.
Strefa	Lista zdefiniowanych stref, jeśli używane	Strefa lub najemca w systemie kontroli dostępu, do którego należy wejście.
Czas oczekiwania na zewnętrzną decyzję o dostępie	W dziesiątkach sekund	Jeśli do styków AMC połączony jest zewnętrzny system, który podejmuje decyzje dotyczące dostępu w jego imieniu, parametr ten ogranicza czas oczekiwania na odpowiedź z systemu zewnętrznego. Uwaga: decyzja dotycząca dostępu wymaga spełnienia **wszystkich** warunków zdefiniowanych w systemie kontroli dostępu, np. uprawnień dostępu, modeli czasowych i stref (jeśli są używane). Wartość domyślna wynosi 0, co oznacza, że parametr jest ignorowany.
Uzbrajanie obszaru	Lista wielkich liter A... Z	Litery umożliwiająca grupowanie wejść DM14 w Obszary uzbrojenia.

Parametry systemu alarmowego

Na drugiej karcie **System alarmowy** ustaw następujące parametry. Parametry te kontrolują uwierzytelnianie i procedurę rozbrojenia systemu sygnalizacji włamani, a rozbrojenia wpływa na wszystkie wejścia w obrębie tego samego obszaru uzbrojenia, zgodnie z definicją na pierwszej karcie.



Parametr	Typ wartości	Opis
Okienko Uprawnienia		
Nazwa uprawnienia rozbrojenia	Dowolny tekst	Nazwa, która ma być wyświetlana w protokołach i raportach, gdy posiadacz karty rozbroi system sygnalizacji włamania na tym wejściu.
Nazwa autoryzacji uzbrajania	Dowolny tekst	Nazwa, która ma być wyświetlana w protokołach i raportach, gdy posiadacz karty uzbroi system sygnalizacji włamania na tym wejściu.
Opis (jedna dla każdego uprawnienia)	Dowolny tekst, opcjonalnie	Opisy uprawnień do uzbrajania
Okienko rozbrojenia		
Tylko za pomocą karty	Przycisk radiowy	Wybierz tę opcję, aby zezwolić na rozbrojenie systemu sygnalizacji włamania przez przyłożenie karty do czytnika bez potrzeby uwierzytelniania.
Z kartą i klawiaturą	Przycisk radiowy	Zaznacz tę opcję, aby umożliwić rozbrojenie systemu przez przyłożenie karty do czytnika, a następnie dodatkowe uwierzytelnienie za pomocą klawiatury czytnika. Dokładne wymagania procedury uwierzytelniania i rozbrajania są określane przez następujące parametry podrzędne:

Parametr	Typ wartości	Opis
Klucz potwierdzenia + kod PIN	Przycisk radiowy	Posiadacze kart muszą się uwierzytelniać za pomocą karty, klucza potwierdzającego i kodu PIN.
Tylko za pomocą kodu PIN	Przycisk radiowy	Posiadacze kart muszą się uwierzytelniać za pomocą karty i kodu PIN.
Tylko za pomocą klucza potwierdzenia	Przycisk radiowy	Posiadacze kart muszą się uwierzytelniać za pomocą karty i klucza potwierdzającego.
Automatyczny cykl drzwi	Pole wyboru	Zaznacz to pole wyboru, jeśli chcesz ponownie uaktywnić blokadę drzwi przy rozbrojeniu, aby umożliwić posiadaczowi karty rozbrojenie i wejście jednocześnie. **Uwaga:** blokada zostanie powtórzona tylko wtedy, gdy posiadacz karty ma również uprawnienia dostępu do tych drzwi.
Okienko procedury		
W zależności od parametrów określonych w okienku **Rozbrajania** w tym okienku jest pokazana standardowa procedura rozbrojenia systemu sygnalizacji włamania. Poinformuj o tej procedurze wszystkich posiadaczy kart, którzy będą korzystać z wejść typu DM14 w tym obszarze uzbrojenia.		
Okienko uzbrajania i rozbrajania		
Sygnał wyjściowy z impulsem 1 s	Pole wyboru	Zaznacz to pole wyboru, jeśli korzystasz z centrali alarmowej sygnalizacji włamania **Bosch, seria B lub G**. Efektem jest wysłanie pojedynczego sygnału, który przełącza stan uzbrojenia wejść w obszarze włamania, a nie ustawia sygnał na wartość stałą 1 (uzbrój) lub 0 (rozbrój).

Styki kontrolera drzwi

W celu możliwości uzbrajania i rozbrajania wejść z drzwiami typu DM14, należy określić sygnały wejściowe i wyjściowe systemu sygnalizacji włamania, które mają być używane na stykach kontrolera drzwi.

Ten krok jest wymagany raz dla każdego kontrolera, który obsługuje wejścia typu DM14. Wszystkie kolejne wejścia DM14 zdefiniowane na tym samym kontrolerze i jego modułach rozszerzeń odziedziczą sygnały z udostępnionego kontrolera.

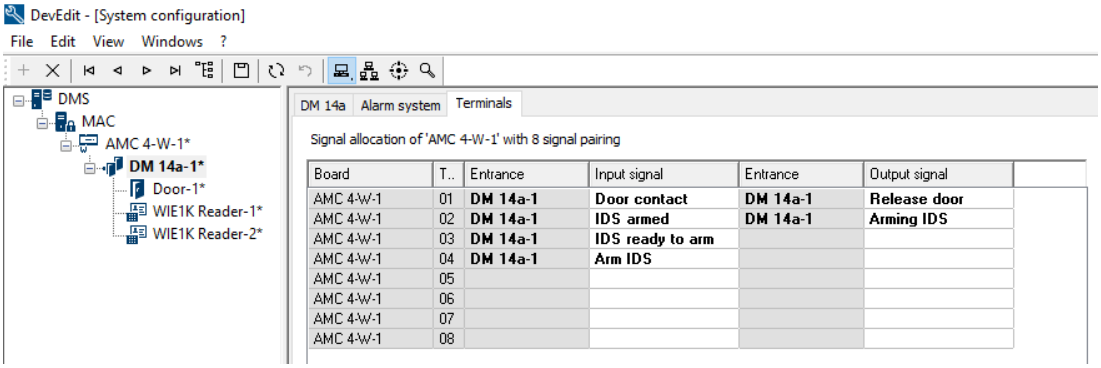
Domyślne sygnały są opisane w poniższej tabeli.

Sygnał	Wejście/ wyjście	Opis
System sygnalizacji włamania uzbrojony)	Wejście	Dla tego obszaru system sygnalizacji włamania jest uzbrojony.
System sygnalizacji włamania gotowy do uzbrojenia	Wejście	Żadne punkty systemu sygnalizacji włamania nie są w stanie usterki (otwarcia lub braku gotowości).
Uzbrojenie systemu sygnalizacji włamania	Wejście	Żądania uzbrojenia systemu sygnalizacji włamania.
Przycisk „Żądanie wyjścia” (REX)	Wejście	
Czujnik rygla	Wejście	Czujnik monitoruje rygiel drzwi.
Układ antysabotażowy	Wejście	Wykryto sabotaż.
Wycisz alarm nieautoryzowanego otwarcia	Wejście	Wyciszanie alarmu przez skonfigurowaną liczbę dodatkowych sekund, jeżeli czujka ruchu wysłała sygnał REX. Więcej informacji znajduje się w omówieniu funkcji Wyciszenie po REX.
Zwolnienie drzwi	Wyjście	Przełączanie mechanizmu drzwi do stanu odblokowania, aby umożliwić dostęp, i z powrotem do stanu zablokowania.
Uzbrajanie systemu sygnalizacji włamania	Wyjście	Uzbrojenie lub rozbrojenie systemu sygnalizacji włamania zależnie od jego bieżącego stanu (przełączanie pomiędzy oboma stanami).
Nawiązywanie połączenia z kamerą	Wyjście	Aktywacja kamery podłączonej do wejścia.
Upłynął maksymalny czas otwarcia drzwi lub **Naruszona ochrona drzwi**	Wyjście	Drzwi są przytrzymywane w stanie otwarcia lub system podejrzewa naruszenie ochrony przy drzwiach.

Procedura przypisywania sygnałów do styków

1. Otwórz trzecią kartę, **Styki**.

– Styki kontrolera drzwi tego wejścia oraz wszystkie jego płyty rozszerzeń są wyświetlane w tabeli.



2. Wybierz wiersz odpowiadający stykowi, którego chcesz używać dla sygnału wejściowego.
3. W odpowiednim polu w kolumnie **Sygnał wejściowy** wybierz żądany sygnał z listy rozwijanej. Należy pamiętać, że na liście pojawiają się tylko dotychczas nieprzypisane sygnały.
4. Powtórz powyższe czynności, aby dodać inne sygnały wejściowe wymagane w przypadku tego wejścia.
5. Powtarzaj tę procedurę, aby dodać do kolumny **Sygnał wyjściowy** wszystkie wymagane sygnały wyjściowe.

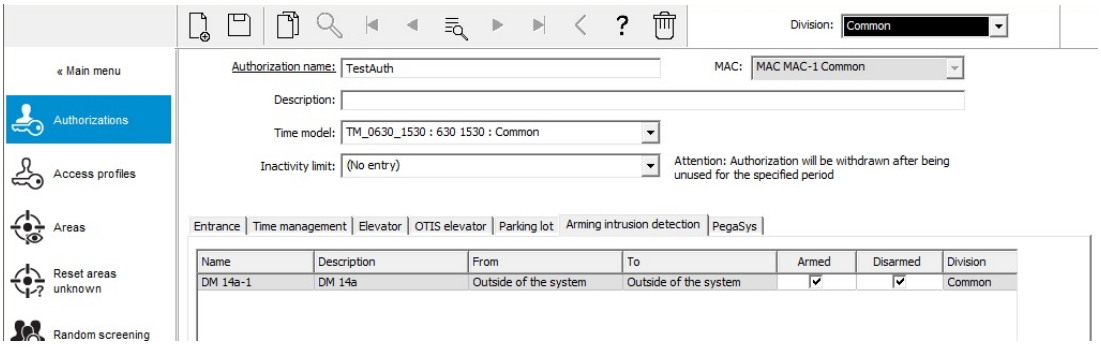
Definiowanie uprawnień do uzbrajania i rozbrajania wejść typu DM14

Po utworzeniu w edytorze urządzeń wejścia DM14, będzie ono dostępne do objęcia uprawnieniami dostępu.

1. W menedżerze okien dialogowych przejdź do:

– Menu główne > **Dane systemowe** > **Uprawnienia** > karta: **Uzbrojenia wykrywania włamania**

2. Wczytaj istniejące uprawnienia dostępu do okna dialogowego lub kliknij przycisk (Nowe), aby utworzyć nowe uprawnienie.
3. Zlokalizuj na liście odpowiednie wejście DM14 i zaznacz pola wyboru **Uzbrojone** i/lub **Rozbrojone**.



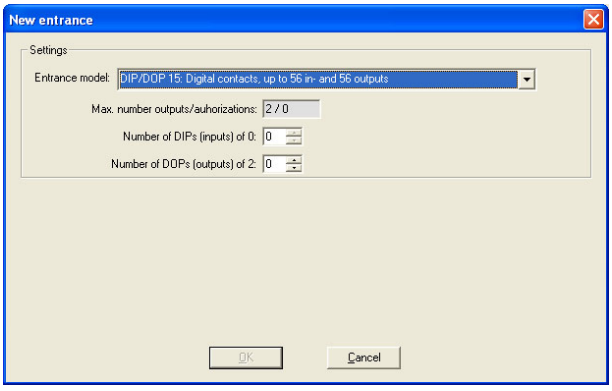
4. Kliknij przycisk (Zapisz), aby zapisać uprawnienie dostępu z wybranymi opcjami.

5. Przypisz to uprawnienie dostępu tym posiadaczom kart, którzy mają korzystać z wejść typu DM 14.

16.5.3 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 edytorze urządzenia.

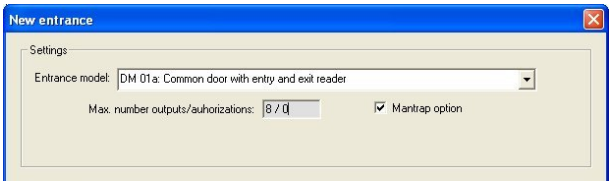
Przywracanie ustawień przełączników DOP po ponownym uruchomieniu

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**.

16.5.4 Modele drzwi ze śluzami osobowymi

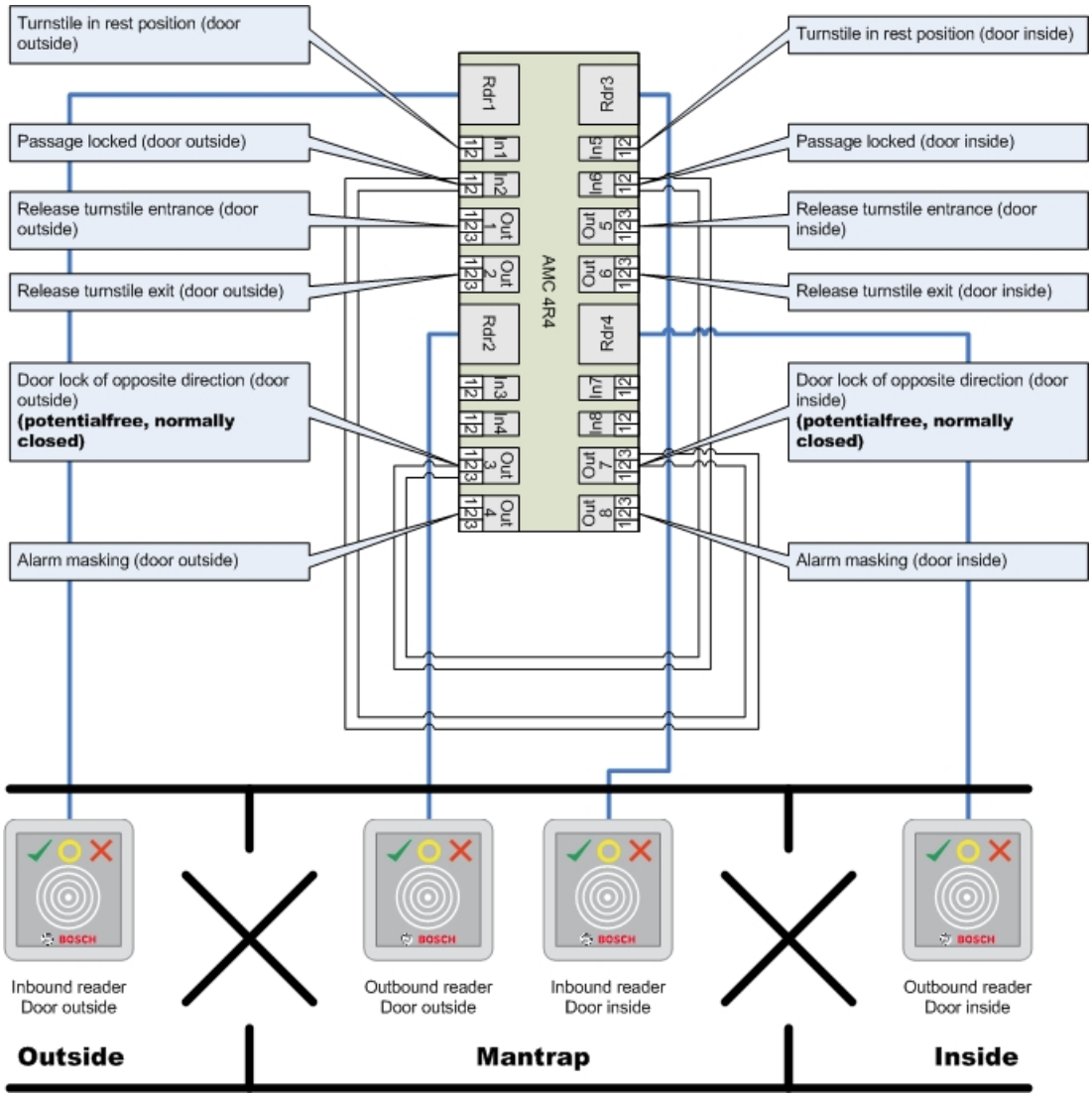
Tworzenie śluzy osobowej

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.

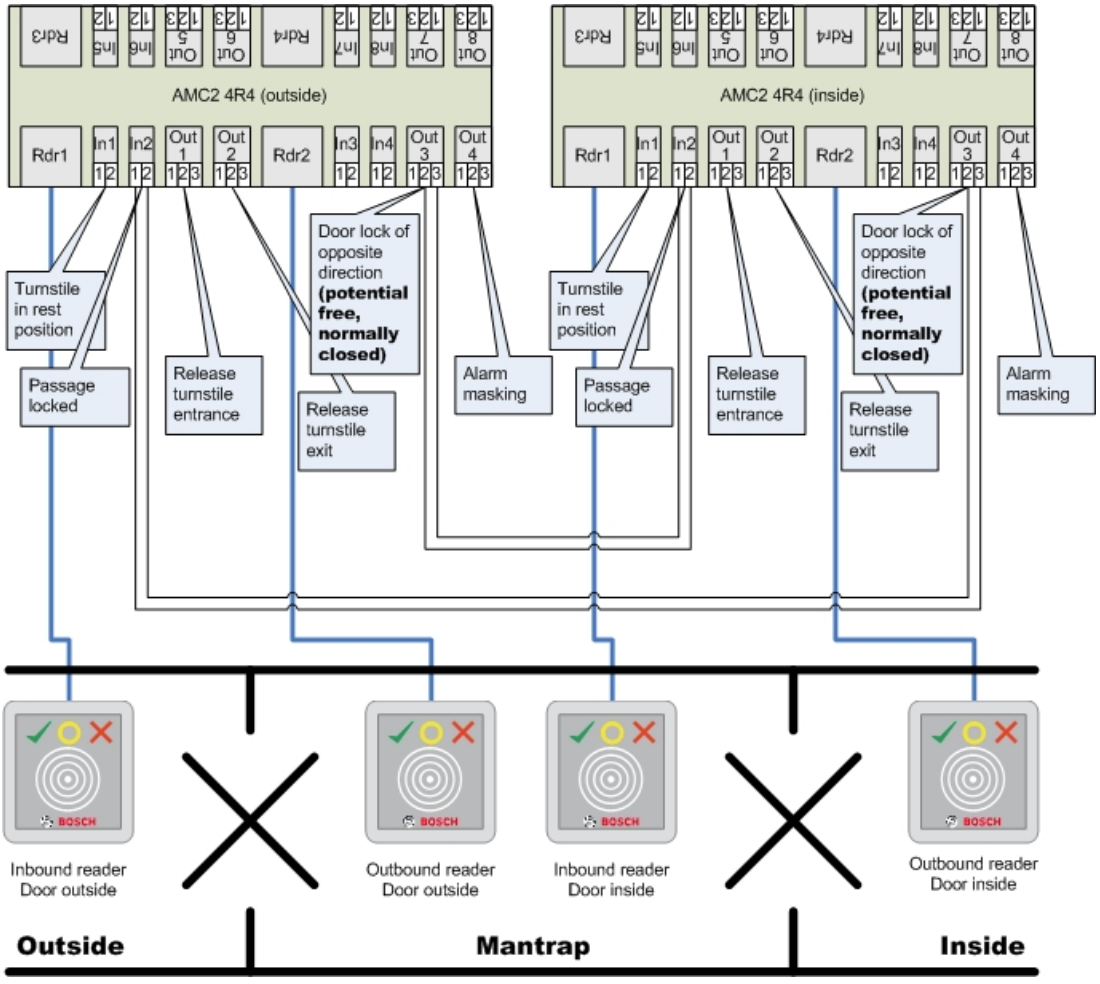
Przykład: śluza osobowa na jednym kontrolerze
Bramki obrotowe są najpowszechniejszym sposobem kontroli dostępu pojedynczych osób posiadających identyfikatory. Dlatego w poniższym przykładzie użyjemy modelu drzwi 3a (kontrolowana bramka obrotowa z czytnikiem wejścia i wyjścia).
Konfiguracja śluzy osobowej 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.

16.6 Drzwi

Karta: drzwi

Parametr	Możliwe wartości	Opis
Nazwisko	Alfanumeryczne, do 16 znaków	Wygenerowaną wartość domyślną można opcjonalnie zastąpić unikatową nazwą.

Opis	Alfanumeryczne, do 255 znaków	
Strefa	Strefą domyślną jest „Wspólna”	Ma to znaczenie tylko wtedy, gdy funkcja **Strefy** jest licencjonowana.
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.

Karta: Opcje

Parametr	**Możliwe wartości**	**Uwagi**
Generuj komunikat o otwarciu/zamknięciu	0 = pole wyboru jest wyczyszczone. 1 = pole wyboru jest zaznaczone.	0 = brak generowania komunikatu po otwarciu (ustawienie pod kątem względem futryny) ani zamknięciu (pełne zatrzaśnięcie wewnątrz futryny) drzwi. 1 = odpowiednie komunikaty są generowane w dzienniku zdarzeń.
Ustawiono ręczne sterowanie drzwiami	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.
Tryb drzwi	0 = drzwi w trybie normalnym 1 = drzwi są niezablokowane 2 = drzwi są odblokowane w zależności od modeli czasowego 3 = po pierwszym przejściu drzwi są otwarte w zależności od modelu czasowego	0 = tryb normalny (domyślnie) — drzwi zostaną zablokowane lub odblokowane w zależności od uprawnień dostępu w poświadczeniach. 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 = drzwi są zablokowane na długo 6 = drzwi są zablokowane w zależności od modelu czasowego	5 = zablokowane (wykluczone z systemu kontroli dostępu) do momentu ręcznego odblokowania. 6 = zablokowane (wykluczone z systemu kontroli dostępu) 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.
Maksymalny czas trwania impulsu do zamka drzwi:	0 - 9999	Maksymalny czas trwania sygnału odblokowania. Jednostka 1/10 s. Wartości domyślne: 50 dla drzwi, 10 dla drzwi obrotowych (model drzwi 03) oraz 200 dla barier (modele drzwi 05c i 09c).
Minimalny czas trwania impulsu do zamka drzwi:	0 - 9999	Minimalny czas trwania sygnału odblokowania wyrażony wielokrotnością 1/10 s. Domyślnie: 10.
Początkowe wyciszenie alarmu	0 - 9999	Dodatkowe wyciszenie alarmu **przed** impulsem do zatrzasku drzwi. (`$PARAMETER_WAITEMA`) Na wypadek bardzo rzadkich sytuacji, gdy zamek drzwi reaguje wolniej niż alarm sygnalizacji włamania, można ustawić tymczasowe wyciszenie alarmu, zanim do drzwi zostanie wysłany sygnał odblokowania. Jednostka: 1/10 s. Domyślnie: 0. Wartość 20, czyli 2 s, zazwyczaj wystarcza nawet dla bardzo powolnych drzwi.
Końcowe wyciszenie alarmu	0 - 9999	Dodatkowe wyciszenie alarmu **po** impulsie do zatrzasku drzwi. (`$PARAMETER_OPENINRT`) Gdy impuls do zamka drzwi (sygnał odblokowania) dotrze do odbiornika, drzwi można otworzyć w tym przedziale czasu bez wywoływania alarmu. Jednostka: 1/10 s. Domyślnie: 0.
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)

Czujnik w futrynie jest obecny	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)
Czujnik rygla jest obecny	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	0 (domyślnie) = drzwi nie mają czujnika rygla 1 = drzwi mają czujnik rygla. Zaryglowanie lub odryglowanie drzwi powoduje generowanie komunikatu.
Rozszerzony czas otwierania drzwi (dla osób niepełnosprawnych)	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	0 = sygnał odblokowania ma standardowy czas trwania ustawiony w sekcji **Drzwi** w parametrze „Maks. czas aktywacji blokady”, czyli czas trwania impulsu wysyłanego do zamka drzwi. 1 (domyślnie) = czas trwania sygnału odblokowania jest mnożony przez współczynnik ustawiany w sekcji **MAC** w parametrze „**Współczynnik czasu dla osób niepełnosprawnych**” (karta: **Globalne ustawienia dostępu**). Wartość 0 w tym parametrze w obszarze MAC powoduje wyłączenie funkcji przedłużonego otwarcia drzwi.

Karta: Ochrona drzwi

Parametr	**Możliwe wartości**	**Uwagi**
Generuj komunikat o zdarzeniu „Drzwi otwarto siłą”	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 = (domyślnie) po nieautoryzowanym otwarciu zostanie wysłany komunikat, a po zamknięciu drzwi kolejny komunikat.
Generuj komunikat o zdarzeniu „Drzwi przytrzymane w pozycji otwarcia” po:	0 - 9999	Jeśli drzwi pozostają otwarte przez ten czas, zostanie wysłany komunikat ostrzegający, że drzwi były zbyt długo otwarte. Jednostka: 1/10 s. Domyślnie: 300. 0 = brak limitu czasu, brak komunikatu.
Przedłużenie wyciszenia alarmu o zdarzeniu „Drzwi otwarto siłą”	0 - 9999	Używany w funkcji „Wyciszenie po REX”: Jednostka = 1/10 s. Domyślne = 0. Jeżeli po sygnale REX z czujki ruchu drzwi zostaną ponownie zamknięte w tym przedziale czasu, typowy komunikat

		`Unauthorized opening of door N` zostanie zastąpiony komunikatem `Door N opened (in alarm suppression mode)` gdzie N to numer drzwi.
Generuj lokalny alarm o zdarzeniu „Drzwi otwarto siłą”	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (pole wyboru jest zaznaczone)	Warunek wstępny: pole wyboru **Generuj komunikat o zdarzeniu „Drzwi otwarto siłą”** w tym oknie dialogowym jest zaznaczone (patrz wyżej). 0 = (domyślnie) czytniki podłączone do tych drzwi nie powodują emitowania lokalnego alarmu dźwiękowego. 1 = czytniki podłączone do tych drzwi powodują emitowanie lokalnego alarmu dźwiękowego w razie siłowego otwarcia drzwi.
Generuj lokalny alarm o zdarzeniu „Drzwi przytrzymane w pozycji otwarcia” po:	0 - 9999	Jeśli drzwi pozostają otwarte przez ten czas, czytniki podłączone do tych drzwi powodują emitowanie lokalnego alarmu dźwiękowego. Jednostka: 1/10 s. 0 = (domyślnie) brak lokalnego alarmu.

16.6.1 Wyciszenie po REX

Wstęp

W wejściach, gdzie nie występuje ryzyko ręcznego otwarcia drzwi od środka, często przycisk REX służący do odblokowywania drzwi jest zastępowany czujką ruchu. W tym typowym scenariuszu system ACS umożliwia proste wydłużenie czasu trwania sygnału REX wysyłanego z czujki ruchu, równocześnie wyciszając (zawieszając) alarm `Door forced open` .
Ta funkcja jest nazywana „Wyciszenie po REX”.
Gdy funkcja jest włączona, posiadacze kart wychodzący przez drzwi w czasie trwania wyciszenia spowodują wygenerowanie komunikatu o zdarzeniu `Door N opened (in alarm suppression mode)`, a nie zdarzeniu `Unauthorized opening of door N`.

Uwaga!
Funkcja wyciszenia po REX w połączeniu z uzbrojonymi systemami detektorów włamania
Funkcja Wyciszenie po REX zawiesza emitowanie alarmów na czas określony w parametrze: Edytor urządzeń > ... > **Drzwi** > karta: **Ochrona drzwi** > **Przedłużenie wyciszenia alarmu o zdarzeniu „Drzwi otwarto siłą”**
bez względu na fakt, czy drzwi są obecnie uzbrojone w ramach działania systemu alarmu włamaniowego.

Wymagania wstępne

– Skonfigurowane drzwi następującego typu: 01a, 01b, 01c, 03a, 03b, 03c, 10a, 10b, 10e, 14a, 14b

– Na potrzeby odblokowywania fizyczne drzwi są wyposażone w czujkę ruchu a nie przycisk REX. Ustaw czas trwania sygnału wysyłanego z czujki ruchu na co najmniej 1 sekundę.

Ścieżka w oknie dialogowym

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

Procedura

1. W edytorze urządzeń przejdź do odpowiedniego wejścia (bezpośredni węzeł podrzędny kontrolera drzwi).
2. W ustawieniach wejścia na karcie **Styki** utwórz nowy sygnał wejściowy o następującym typie:
   `Suppress alarm from unauthorized opening`
3. Kliknij przycisk  (Zapisz), aby zapisać zmiany.
4. Zaznacz drzwi należące do interesującego Cię wejścia
5. W ustawieniach drzwi na karcie **Ochrona drzwi** ustaw wartość w parametrze **Przedłużenie wyciszenia alarmu o zdarzeniu „Drzwi otwarto siłą”**

– Ta wartość jest podawana w dziesiątych częściach sekundy.
– Wartość domyślna to `0`. Oznacza to, że wyciszenie alarmu nie jest przedłużane, kiedy posiadacz karty opuści obszar nadzorowany przez czujkę ruchu.

6. Kliknij przycisk  (Zapisz), aby zapisać zmiany.

16.6.2 Konfigurowanie emitowania lokalnych alarmów przez drzwi

Wstęp

Dla stanów drzwi wymienionych poniżej system ACS może emitować alarmy ze wszystkich czytników podłączonych do drzwi.

Stan	Reakcja lokalnego alarmu
Drzwi otwarto siłą	Alarm rozlega się przez 17 sekund lub do momentu zamknięcia drzwi.
Drzwi przytrzymane w pozycji otwarcia	Alarm rozlega się do momentu zamknięcia drzwi.

Wymagania wstępne

– Czytniki używają protokołu OSDP lub Wiegand
– W czytnikach zamontowano brzęczyki alarmowe i mają one elektryczne połączenie z kontrolerem drzwi.
– Kontroler AMC ma oprogramowanie układowe w wersji 02.38 lub nowszej.

Następujące typy czytników **nie** są obsługiwane:

– Czytniki IDEMIA
– Czytniki Suprema z protokołem Wiegand
– Czytniki LBUS
– Czytniki BG900

Ścieżka w oknie dialogowym

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

Procedura dla zdarzeń Drzwi otwarto siłą

1. W drzewie urządzeń zaznacz drzwi, które chcesz skonfigurować.
2. W ustawieniach drzwi na karcie **Ochrona drzwi** zaznacz pole wyboru **Generuj komunikat o zdarzeniu „Drzwi otwarto siłą”**
3. Zaznacz pole wyboru **Generuj lokalny alarm o zdarzeniu „Drzwi otwarto siłą”** Wartość domyślna wynosi `0` (pole wyboru jest wyczyszczone). Oznacza to, że domyślnie nie jest emitowany żaden lokalny alarm.
4. Kliknij przycisk  (Zapisz), aby zapisać zmiany.

Procedura dla zdarzeń Drzwi przytrzymane w pozycji otwarcia

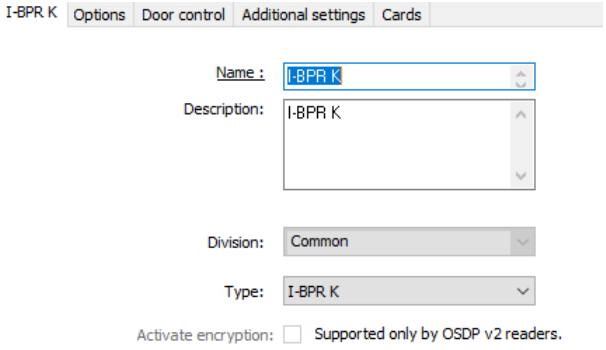
1. W drzewie urządzeń zaznacz drzwi, które chcesz skonfigurować.
2. W ustawieniach drzwi na karcie **Ochrona drzwi** określ niezerową wartość w polu **Generuj lokalny alarm o zdarzeniu „Drzwi przytrzymane w pozycji otwarcia” po:**

– Ta wartość jest podawana w dziesiątych częściach sekundy.
– Wartość domyślna to `0`. Oznacza to, że domyślnie nie jest emitowany żaden lokalny alarm.

3. Kliknij przycisk  (Zapisz), aby zapisać zmiany.

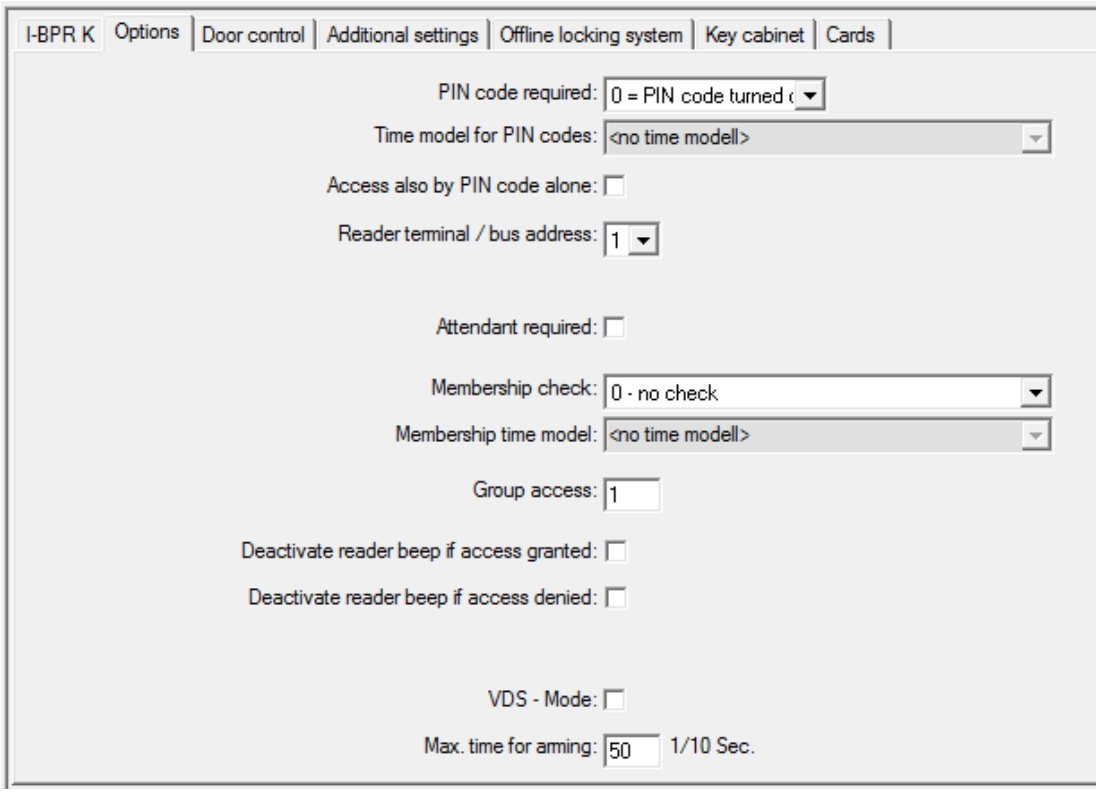
16.7 Czytniki

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.
Wymagany opiekun	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	Sprawdzanie członkostwa jest zazwyczaj stosowane we wczesnych fazach, zanim system kontroli dostępu zostanie oddany do użytku. W tym przypadku dostęp jest przyznawany w oparciu o ogólny identyfikator firmy, a nie unikatowy identyfikator osobisty. **Ważne**: sprawdzanie członkostwa działa tylko z fizycznymi poświadczeniami, w których definicje kart są określone w systemie (szare **tło**), a nie z niestandardowymi definicjami lub poświadczeniami biometrycznymi. **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) 1 = aktywny (pole wyboru jest zaznaczone)	W przypadku aktywowania tej opcji (1) sygnalizacja czytnika jest wyłączona.
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.

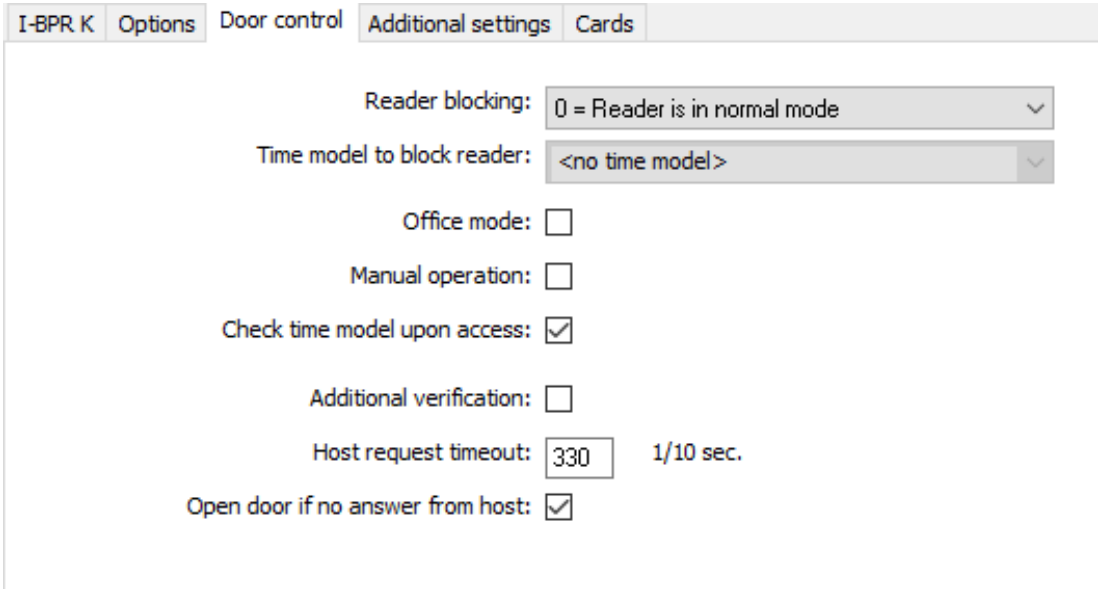
Szablony to zapisane wzorce. Mogą to być dane kart lub dane biometryczne.

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.
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.

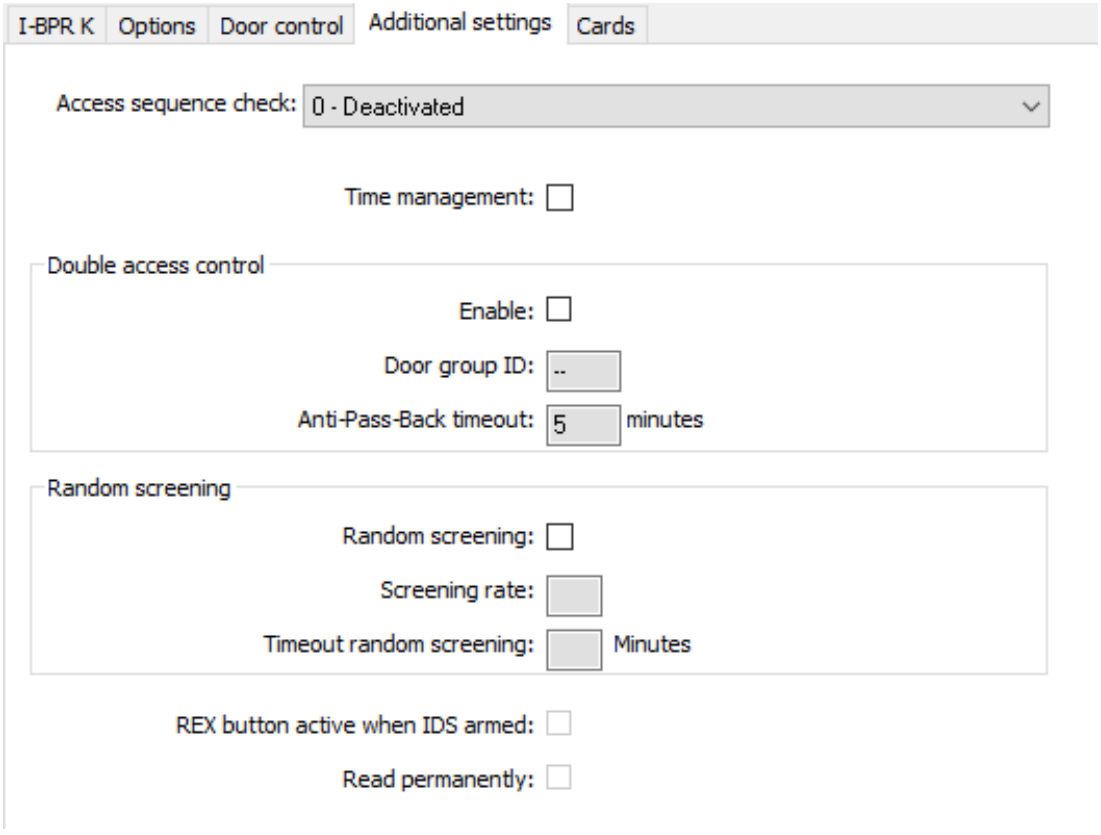
Konfigurowanie czytnika: Kontrola drzwi



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 temu czytnikowi ustawienie dla wejścia atrybutu Tryb biurowy. Czytnik musi być wyposażony w klawiaturę. Gdy ten parametr jest aktywowany, odpowiednio uprawniony posiadacz karty może włączać i wyłączać tryb biurowy poprzez naciśnięcie klawisza 3, a następnie przyłożenie swojej karty. Patrz *Osoby upoważnione do ustawiania trybu Biuro, Strona 205*.
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 systemu kontroli dostępu firmy Bosch).
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). 1 do 9999 x 1/10 sekundy. (Domyślnie 330 tzn. 33 sekundy). Czytnik żąda potwierdzenia z systemu kontroli dostępu. Jeśli potwierdzenie nie zostanie odebrane w tym czasie, system AMC sprawdza parametr **Otwórz drzwi, gdy brak odpowiedzi z hosta** i odpowiednio udzieli lub odmówi dostępu.
Otwórz drzwi, gdy brak odpowiedzi z hosta	0 = nieaktywny (pole wyboru jest wyczyszczone) 1 = aktywny (domyślnie) (pole wyboru jest zaznaczone)	Ta kontrola jest aktywna tylko po ustawieniu parametru **Weryfikacja hosta**. 0 = nie otwiera drzwi, jeśli przed upływem limitu czasu brak będzie potwierdzenia z systemu hosta. 1 (domyślnie) = powoduje otwarcie drzwi po upływie limitu czasu, jeśli przed upływem limitu czasu brak będzie potwierdzenia z systemu hosta.

Konfigurowanie czytnika: Ustawienia dodatkowe

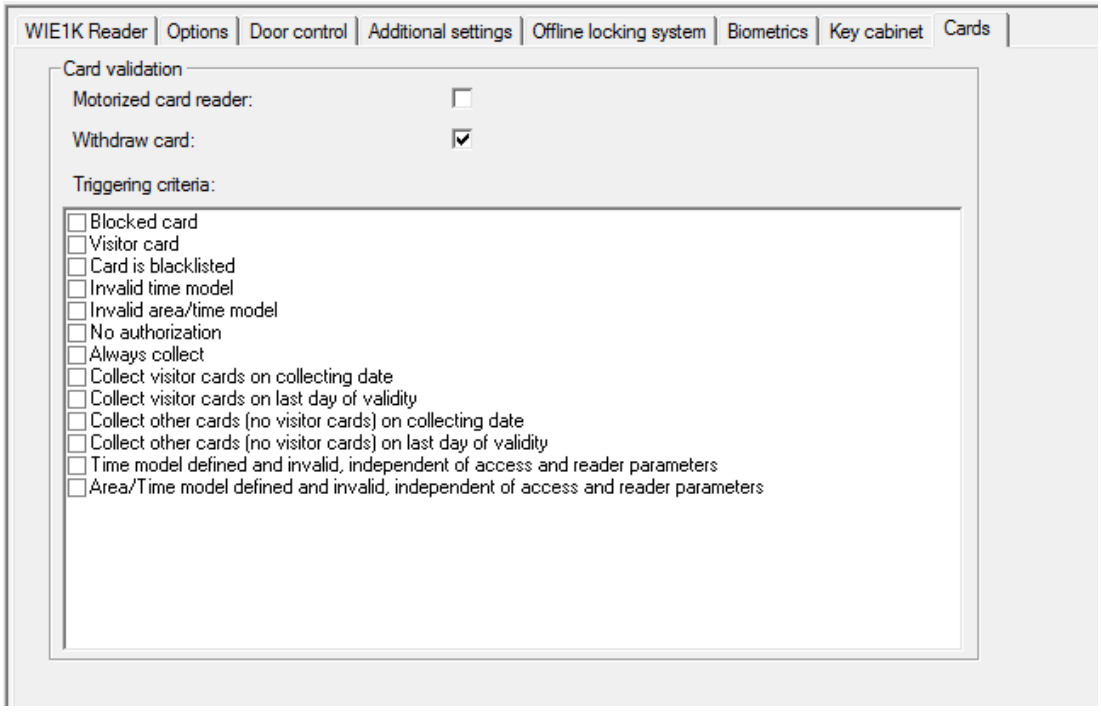


Parametr	Możliwe wartości	Uwagi
Sekwencyjna kontrola dostępu	0 — nieaktywne 1 — aktywny; dezaktywowanie przy awarii LAC 2 — aktywny; pozostaw aktywny przy awarii LAC 3 — aktywne; użycie ścisłego sprawdzania sekwencyjnego nawet w przypadku usterki LAC (uwaga: aktualizuj lokalizację osoby ręcznie)	0 = 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. 2 = Pierwsze odczyt karty zostanie wyłączony bez sprawdzania lokalizacji. 3 = Sprawdzanie lokalizacji zostanie wyłączone dla każdego odczytu karty podczas awarii kontrolera LAC.
Jest 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 wybraniu tego pola system kontroli dostępu gromadzi dane do 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.
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.

Patrz
– *Osoby upoważnione do ustawiania trybu Biuro, Strona 205*

16.7.1 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.

16.8 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 kontroli dostępu 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 obsługiwanych 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.

16.9 Moduły rozszerzeń kontrolera AMC

Tworzenie obiektu AMC-I/O-EXT (modułu rozszerzeń we/wy)

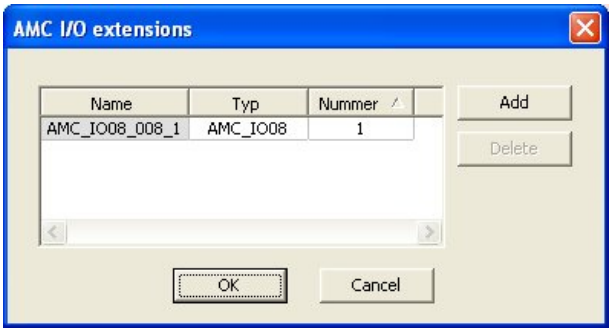
Moduły (karty) rozszerzeń dostarczają dodatkowe sygnały wejściowe i wyjściowe, jeśli osiem styków w kontrolerze AMC nie wystarcza do podłączenia niezbędnych sygnałów (na przykład gdy są używane windy).

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.

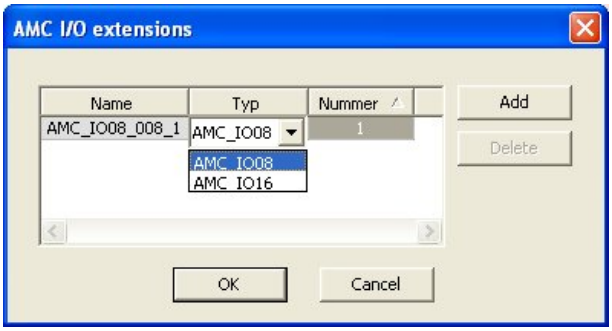
Pojawi się okno dialogowe wyboru kart rozszerzeń.



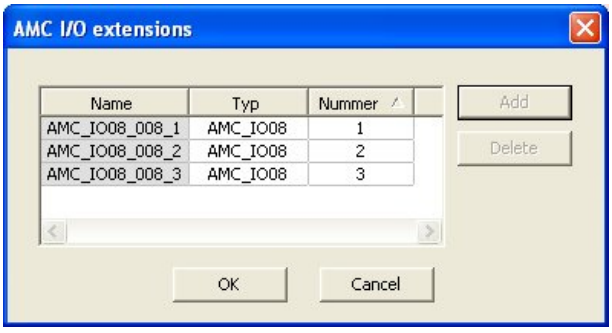
Moduły AMC-EXT są dostępne w dwóch wariantach:

- 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.

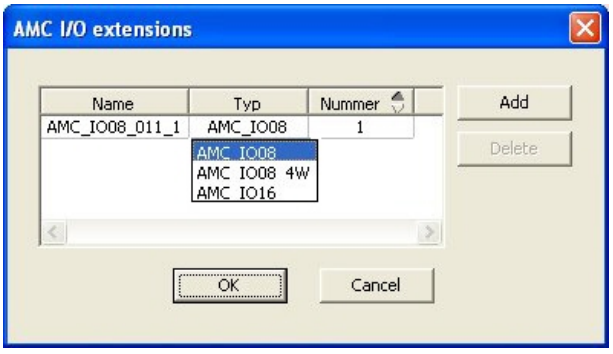
Uwaga!
Moduł AMC2 4W-EXT nie może funkcjonować jako samodzielny kontroler, ale tylko jako rozszerzenie kontrolera AMC2-4W. Drzwi są kontrolowane, a decyzje w zakresie kontroli dostępu są podejmowane tylko przez kontroler AMC2 4W.

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	Wartością domyślną jest **Wspólna**	Ma to znaczenie tylko wtedy, gdy funkcja **Strefy** jest licencjonowana.

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.

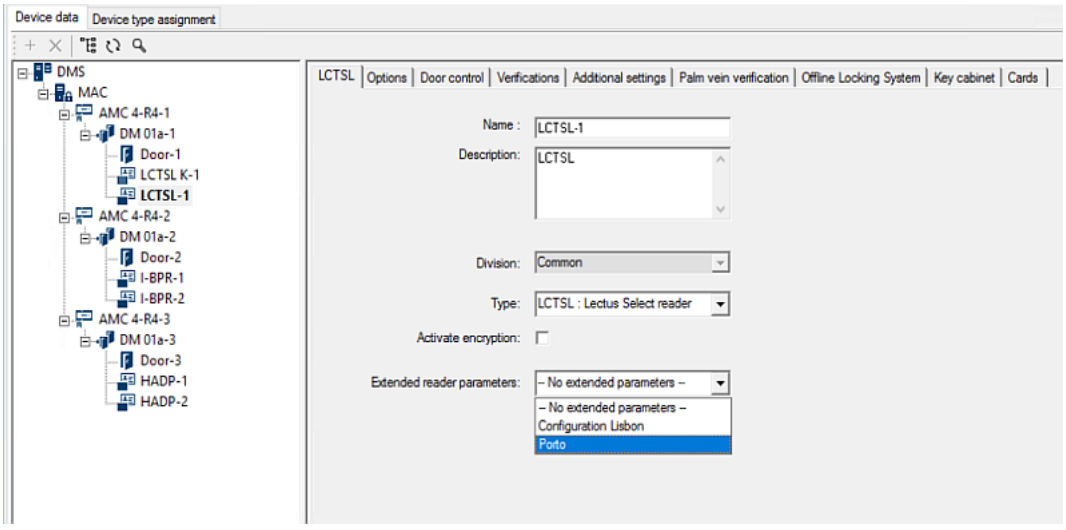
17 Niestandardowe konfiguracje czytników

17.1 Wstęp

Od wersji oprogramowania BIS 4.9 i AMS 4.0 systemy kontroli dostępu firmy Bosch umożliwiają stosowanie niestandardowych ustawień MIFARE DESFire. Możesz tworzyć zaszyfrowane pliki parametrów za pomocą narzędzia pomocniczego `Bosch.ReaderConfigTool.exe`. To narzędzie jest zawarte w ustawieniach oprogramowania BIS ACE 4.9, AMS 4.0 i późniejszych wersji i posiada własną dokumentację, w której znajduje się aktualna lista obsługiwanych czytników.
W dalszych częściach tej instrukcji opisano sposób użycia edytora urządzeń do zaimportowania zaszyfrowanego pliku parametrów i zastosowania go do dowolnego lub wszystkich obsługiwanych czytników w hierarchii urządzeń kontroli dostępu.

17.2 Właściwość czytnika: rozszerzone parametry czytnika

Dostępne zestawy rozszerzonych parametrów obsługiwanych czytników są wyświetlane na ich stronach właściwości w edytorze urządzeń pod etykietą **Rozszerzone parametry czytnika**.



Rysunek 17.1: Rozszerzone parametry czytnika

Domyślną wartością listy rozwijanej jest `No extended parameters`. Jest to jedyna dostępna wartość, chyba że zostaną zaimportowane dodatkowe zestawy parametrów.

Procedura

Aby zastosować zaimportowany zestaw parametrów do pojedynczego zgodnego czytnika:

1. W edytorze urządzeń wybierz czytnik w drzewie urządzeń
2. Wybierz pierwszą kartę właściwości
3. Wybierz wymagany zestaw parametrów z listy **Rozszerzone parametry czytnika**.
4. Kliknij przycisk **Zastosuj** lub 

17.3 Importowanie zestawu parametrów czytnika

Importowanie i usuwanie plików parametrów odbywa się tylko na poziomie DMS w hierarchii urządzeń.

Wymagania wstępne

Dostęp do zatwierdzonego pliku parametrów systemu kontroli dostępu. Domyślnie plik jest typu `.ReaderConfigSave`

Procedura

1. W edytorze urządzeń kliknij prawym przyciskiem myszy węzeł DMS i wybierz opcję **Importuj zestawy parametrów czytników** z menu kontekstowego.
   Pojawi się okno podręczne **Importowanie zestawu parametrów czytnika**.
2. Kliknij opcję **Plik** i znajdź plik z parametrami za pomocą eksploratora plików.
3. Po wyświetleniu monitu wprowadź hasło pliku parametrów.
   Jeśli hasło jest prawidłowe, w dolnej połowie okna dialogowego zostaną wyświetlone następujące informacje:

– Lista typów czytników, do których odnosi się dany zestaw parametrów.
– Nazwa zestawu parametrów. Możesz ją edytować w tym oknie dialogowym.
– Opis tekstowy, o ile został podany przez autora zestawu parametrów. W tym oknie dialogowym możesz dodać i edytować opis.

4. Kliknij przycisk **Importuj** w celu zaimportowania zestawu parametrów do ewentualnego wykorzystania w przyszłości przez system kontroli dostępu.

– Zestaw parametrów jest importowany i przechowywany w systemie kontroli dostępu.
– Zostanie on dodany do listy dostępnych zestawów parametrów w górnej części okna podręcznego.

5. Kliknij przycisk **Zakończ**, aby zamknąć okno podręczne **Importowanie zestawów parametrów czytnika**.

17.4 Stosowanie zestawu parametrów do czytników

Wstęp

Zestawy parametrów zaimportowane do systemu kontroli dostępu są przechowywane w celu ich późniejszego wykorzystania, ale nie są stosowane do czytników w systemie.
Zastosowanie zestawu parametrów jest dodatkowym krokiem, który można wykonać na różnych poziomach w hierarchii urządzeń:

– DMS
– Kontroler MAC
– AMC

Po zastosowaniu zestawu parametrów na poziomie DMS, MAC lub AMC, może on mieć zastosowanie tylko do czytników podrzędnych, do których został utworzony dany zestaw. Wszystkie pozostałe czytniki podrzędne pozostają bez zmian.

Wymagania wstępne

Pomyślnie zaimportowano zestaw parametrów czytnika.

Procedura

1. W edytorze urządzeń kliknij prawym przyciskiem myszy czytnik lub urządzenie (DMS, MAC lub AMC), których czytniki chcesz skonfigurować pomocą parametrów.
2. Z menu kontekstowego wybierz opcję **Zarządzaj zestawami parametrów czytnika**.
3. W górnym okienku listy (**Zestawy parametrów dla typów czytników**) wybierz zestaw parametrów, który chcesz zastosować.
   Obsługiwane czytniki znajdują się na liście w lewym dolnym okienku: **Czytniki skonfigurowane za pomocą tego zestawu parametrów**.
4. Na liście **Czytniki skonfigurowane za pomocą tego zestawu parametrów** zaznacz te czytniki, do których chcesz zastosować wybrany zestaw parametrów.

– Jeśli masz dużo czytników, użyj list rozwijanych, aby ograniczyć widok do podrzędnych czytników określonego MAC lub AMC.

5. Za pomocą przycisków strzałek można przenosić zaznaczone czytniki w okienku po prawej stronie **Wszystkie czytniki z wybranym zestawem parametrów**.

Uwaga!
Widok zgodnych czytników
Na liście znajdą się tylko te czytniki zgodne z danym zestawem parametrów. Jeśli zaznaczone zostanie pole wyboru **Pokaż wszystkie czytniki**, wówczas wyświetlone zostaną również czytniki z innymi zestawami parametrów. Są one pokazane na szarym tle, aby zaznaczyć je jako tylko do odczytu dla wybranego zestawu parametrów.

6. Kliknij przycisk **OK**, aby zamknąć wyskakujące okno.
7. W edytorze urządzeń kliknij przycisk **Zastosuj** lub
   Zestaw parametrów zostanie zastosowany do wszystkich czytników, które pozostawiono na liście **Wszystkie czytniki z wybranym zestawem parametrów** w oknie dialogowym.

17.5 Zarządzanie zestawami parametrów czytnika

Wstęp
Zastosowanie zestawów parametrów można zmieniać na różnych poziomach hierarchii urządzeń:
– DMS
– Kontroler MAC
– AMC
Zmiany na poziomie DMS, MAC lub AMC mogą dotyczyć tylko czytników podrzędnych, dla których utworzono zestaw. Wszystkie pozostałe czytniki podrzędne pozostają bez zmian.

Wymaganie wstępne
Pomyślnie zaimportowano zestaw parametrów czytnika.

Procedura
1. W edytorze urządzeń kliknij prawym przyciskiem myszy czytnik lub urządzenie (DMS, MAC lub AMC)
2. Z menu kontekstowego wybierz opcję **Zarządzaj zestawami parametrów czytnika**.
3. W górnym okienku listy **Zestawy parametrów do typów czytników** wybierz zestaw parametrów, który chcesz zastosować.
– Odpowiednie czytniki są wymienione w lewym dolnym okienku: **Czytniki skonfigurowane za pomocą tego zestawu parametrów**.
– Czytniki, do których zastosowano już dany plik parametrów, są wyświetlane w prawym dolnym okienku: **Wszystkie czytniki z wybranym zestawem parametrów**.
4. Zaznacz czytniki na obu listach. Za pomocą klawiszy strzałek można przenosić czytniki na listę po prawej stronie **Wszystkie czytniki z wybranym zestawem parametrów**.
– WAŻNE: Na końcu tej procedury dokładnie zanotuj wszystkie czytniki usunięte z listy.
5. Po wprowadzeniu zmian kliknij przycisk **OK**, aby zamknąć okno podręczne.
6. W edytorze urządzeń kliknij przycisk **Zastosuj** lub
– Zestaw parametrów jest stosowany do wszystkich czytników, które pozostawiono na liście **Wszystkie czytniki z wybranym zestawem parametrów.**
– Zestaw parametrów jest usuwany z czytników, które zostały usunięte z tej listy.
7. W przypadku wszystkich czytników z listy wykonaj jedną z następujących czynności:
– Przywróć domyślne ustawienia fabryczne, korzystając z przełączników sprzętowych DIP w czytniku.
– Zastosuj do nich inny zestaw parametrów.

Uwaga!
Usunięcie zestawu parametrów nie powoduje ponownego skonfigurowania czytników, które ich używały.
Usunięta konfiguracja czytnika pozostanie w czytnikach, które jej używały, do czasu zresetowania czytnika lub zastosowania innego zestawu parametrów.

17.6 Usuwanie zestawów parametrów czytnika

Importowanie i usuwanie plików parametrów odbywa się tylko na poziomie DMS w hierarchii urządzeń.

Wymagania wstępne
Co najmniej jeden plik parametrów został już zaimportowany do systemu kontroli dostępu.

Procedura
1. W edytorze urządzeń kliknij prawym przyciskiem myszy węzeł DMS i wybierz opcję **Usuń zestawy parametrów czytników** z menu kontekstowego.
   Pojawi się okno podręczne **Usuwanie zestawu parametrów czytnika**.
2. Na liście **Zestawy parametrów do typów czytników** wybierz zestaw parametrów, który chcesz usunąć.
– W prawym dolnym rogu okna podręcznego pojawi się lista wszystkich czytników, które aktualnie są skonfigurowane z wybranym zestawem parametrów.
– Uwaga: zanotuj te czytniki; po usunięciu zestawu parametrów będzie trzeba je zresetować lub skonfigurować ponownie. Szczegółowe informacje na ten temat znajdują się w ostatnim kroku tej procedury.
3. Kliknij przycisk **Usuń**
4. Kliknij przycisk **Zakończ**
5. W edytorze urządzeń kliknij przycisk **Zastosuj** lub 
6. Wykonaj jedną z poniższych czynności w odniesieniu do wszystkich czytników, które używały usuniętego zestawu parametrów:
– Przywróć domyślne ustawienia fabryczne, korzystając z przełączników sprzętowych DIP w czytniku.
– Zastosuj do nich inny zestaw parametrów.

Uwaga!
Usunięcie zestawu parametrów nie powoduje ponownego skonfigurowania czytników, które ich używały.
Usunięta konfiguracja czytnika pozostanie w czytnikach, które jej używały, do czasu zresetowania czytnika lub zastosowania innego zestawu parametrów.

18 Niestandardowe pola na dane osobowe

Wstęp

Pola danych personelu można dostosowywać na wiele sposobów:

- Czy mają być **widoczne**, tzn. czy będą w ogóle wyświetlane w aplikacji klienckiej
- 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 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.

18.1 Wyświetlanie podglądu i edytowanie pól niestandardowych

Ścieżka w oknie dialogowym

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

Główne okno jest podzielone na dwie karty

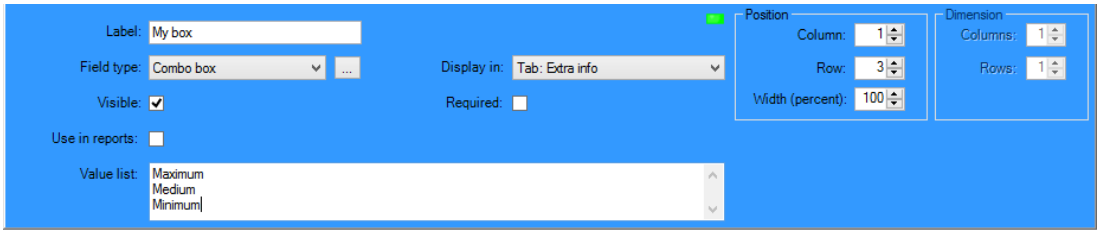
Przegląd Ta karta i jej podkarty (**Adres, Kontakt, Dodatkowe dane osobowe, Dodatkowe dane firmy, Uwagi, Kontrola kart** i **Dodatkowa informacja**) są tylko do odczytu i przedstawiają w przybliżeniu widok WYSIWYG tego, które dane będą wyświetlane na których kartach w aplikacji klienckiej.

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 pokrętełł 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 zapewnić unikatowość wartości wprowadzanych w tym polu. System odrzuca wtedy dane wejściowe o wartości, która została już zapisana dla tego pola w bazie danych. Np. numery personalne powinny być niepowtarzalne w stosunku do osób, a numery tablic rejestracyjnych w stosunku do pojazdów.
	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.

Podpis na etykiecie	Opis
	Aby ułatwić sobie korzystanie z aplikacji klienckiej, najlepiej umieścić wszystkie wymagane pola na pierwszej karcie.
Pozycja	Za pomocą pól pokrętеł **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 pokrętеł **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.

18.2 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.

19 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.

19.1 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.
- 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.

19.2 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.

19.3 Czynności konfiguracyjne w edytorze urządzeń

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

Uwaga!
Nie można zmodyfikować danych urządzenia w edytorze urządzeń, jeśli jest aktywny poziom zagrożenia.

19.3.1 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.

19.3.2 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 jest podzielone na 2 okienka: **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 bramki obrotowej, należy zaznaczyć 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

19.3.3 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 jest podzielone na 2 okienka: **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.

19.3.4 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.

19.3.5 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 DM 15
Obecnie poziom zagrożenia nie może być inicjowany w modelu drzwi 15 (DIP/DOP).

19.4 Czynności konfiguracyjne w oknach dialogowych danych systemowych

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

19.4.1 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)

19.4.2 Przypisywanie profilu ochrony osoby do typu osoby

Ścieżka w oknie dialogowym

- **Menu główne** > **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.

19.5 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

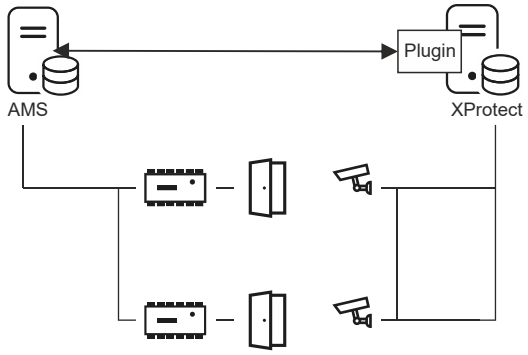
– *Przypisywanie profilu ochrony osoby do typu osoby, Strona 144*
– *Tworzenie danych osobowych i zarządzanie nimi, Strona 194*

20 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.

Uwaga!

Potencjalna niezgodność wtyczek pochodzących z różnych źródeł

Wtyczki systemu Milestone XProtect działają we wspólnym obszarze, tzn. nie są od siebie całkowicie odizolowane. W związku z tym mogą wystąpić błędy oprogramowania, jeżeli na jednym serwerze systemu XProtect zostanie uruchomionych wiele wtyczek używających różnych wersji środowiska .NET i mających różne obiekty zależne. BOSCH jest w stanie zagwarantować prawidłowe działanie wtyczki oprogramowania AMS tylko wtedy, gdy jest to jedyna zainstalowana wtyczka.

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.

21 Integrowanie systemu Otis Compass

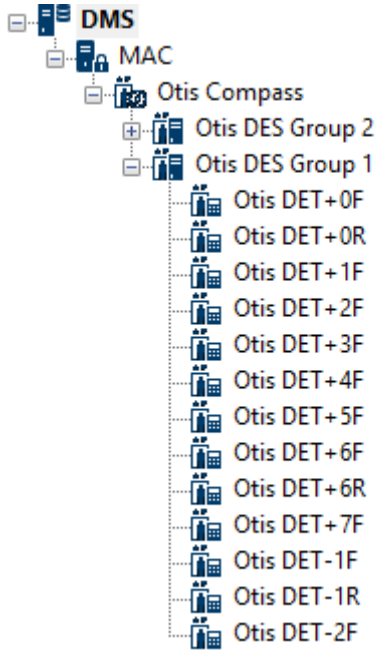
Wstęp

Compass to system zarządzania obszarami docelowymi firmy Otis Elevator Company. Jego zadaniem jest zarządzanie wieloma bankami wind i wysyłanie wind do pasażerów, by mogli sprawnie dotrzeć do celu. Aby wprowadzić niezbędne informacje, pasażer nie naciska już przycisków **Góra** lub **Dół**, lecz zgłasza destynację za pomocą czytnika kart, ekranu dotykowego lub terminalu z klawiaturą.

Integracja z systemami kontroli dostępu firmy Bosch zwiększa bezpieczeństwo. W oparciu o poświadczenia i modele czasowe pasażerowie są sprawnie przewożeni na piętra, na których mieszkają, i do innych obszarów docelowych, do których mają dostęp. System nie przyjmie próśb o piętra, których nie ma w profilu autoryzacji pasażera, lub w godzinach poza używanym modelem czasowym.

Topologia sprzętowa systemu Compass

Urządzenia w systemie Compass są konfigurowane od góry w hierarchii 3-warstwowej pod jednym adresem MAC w edytorze urządzeń.



Hierarchia powyżej zawiera następujące elementy:

System **Otis Compass** na dedykowanym adresie MAC

Jedna grupa windy zarządzana przez jeden system **DES**

Kilka terminali (**DET**), każdy z numerem piętra od -2 do +7 i literami F lub R oznaczającym odpowiednio przednich i tylnych drzwi.

Pierwsza warstwa: (Otis Compass)

System zarządzania obszarami docelowymi. Każdy system **Compass** może zarządzać maksymalnie 8 grupami wind (tzw. bankami wind).

Parametry: zasięg pięter,
adresy sieciowe,
numery portów i limity czasu.

Druga warstwa: (Otis DES/DER)

Maksymalnie 8 grup wind, każda zarządzana przez logiczny serwer wprowadzania obszaru docelowego (DES) składający się z 1 lub 2 urządzeń fizycznych.

Ponadto warstwa ta może zawierać maksymalnie 2 opcjonalne urządzenia do optymalizacji, tzw. urządzenia przekierowujące wprowadzanie obszaru docelowego (DER).

Parametry: 1 identyfikator grupy na grupę windy.
1 adres IP na urządzenie.
Tabelę pięter z drzwiami wind oraz to, czy są publicznie dostępne.

Trzecia warstwa: Otis DET

Terminale wejścia do obszaru docelowego (DET)

Parametry: 1 adres IP na terminal. Dostępne piętra z drzwiami windy na każdym terminalu.

Przegląd integracji w systemie kontroli dostępu

Administratorzy systemu kontroli dostępu integrują system Compass w następujące etapy, opisane szczegółowo w dalszej części rozdziału:

1. W edytorze urządzeń skonfiguruj sprzęt systemu Compass na jednym MAC.
2. Skonfiguruj dostosowane pola odpowiednio do posiadacza karty Otis, np. jako piętro domowe.
3. Utwórz profile autoryzacji do zarządzania dostępem do określonych obszarów docelowych windy.
4. Przypisz profile autoryzacji do odpowiednich posiadaczy kart

21.1 Konfigurowanie systemu Compass w edytorze urządzeń

W tej sekcji opisano kroki konfigurowania systemu Otis Comapss w edytorze urządzeń.

Ścieżka w oknie dialogowym

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

21.1.1 Warstwa 1: Konfigurowanie systemu Compass

Procedura dotycząca warstwy 1: Konfigurowanie systemu Compass

1. Wybierz odpowiedni MAC w widoku drzewa edytora urządzeń
2. Kliknij prawym przyciskiem myszy i wybierz **Nowy system Otis Compass**. Na stronie właściwości znajdują się 2 karty.
   – **Otis Compass**
   – **Piętra**
3. Na karcie **Otis Compass** najważniejsze parametru, które należy ustawić, to
   – **Nazwa** (nazwa, która powinna być wyświetlana w drzewie urządzeń)
   – **Adres IP MAC** (adres IP wywołania zwrotnego systemu Compass na osobnej karcie sieciowej, za pośrednictwem którego system Compass komunikuje się z MAC). **UWAGA:** to **nie** jest adres IP samego urządzenia MAC.
   – **Strefa** (tylko jeśli Strefy są licencjonowane i używane w instalacji)

Zostaw wartości domyślne pozostałych parametrów, chyba że specjalista pomocy technicznej poleci je zmienić. Zostały one zwięźle objaśnione w tabeli poniżej:

Parametr	**Wartość domyślna**	**Opis**
Adres grupy kontrolera MC	234.46.30.7	Adres IP grupy multiemisji
Port MC urządzenia DES/DER (zdalnego) Port MC urządzenia DES/DER (lokalnego)	48307 47307	Porty multiemisji
Port UDP urządzenia DES/DER (zdalnego)	46303 45303	Porty UDP urządzeń DES i DER

Parametr	**Wartość domyślna**	**Opis**
Port UDP urządzenia DES/DER (lokalnego)		
Port UDP urządzenia DET (zdalnego) Port UDP urządzenia DET (lokalnego)	45308 46308	Porty UDP urządzeń DET
Czas wygaśnięcia (TTL) multiemisji	5 sekund	
Interwał impulsu	1 sekunda	Ilość czasu między sygnałami impulsów. Sygnały te wskazują inne urządzenia „żywe”, tj. działa
Maksymalna liczba pominiętych impulsów	3	Liczba impulsów, które można pominąć, zanim urządzenie zostanie uznane za „martwe” (niedziałające)
Upływ limitu czasu komunikatu	1 sekunda	
Ponowne próby wysłania komunikatu	3	

1. Na karcie **Piętra** kliknij przycisk **Zmień zakres pięter**
2. Wprowadź numery najniższego i najwyższego piętra, które będą obsługiwane przez wszystkie banki wind w systemie Otis Compass.
   – Maksymalny zakres: od -127 do +127
3. Kliknij przycisk  (Zapisz), aby zapisać zmiany.

21.1.2 Warstwa 2: Grupy wind, urządzenia DES i DER

Procedura dotycząca warstwy 2: Konfigurowanie grup wind (urządzenia DES/DER)
Wstęp
DES (serwer wprowadzania obszaru docelowego) jest komputerem zarządzającym grupą windy. W razie potrzeby dwa fizyczne urządzenia DES z oddzielnymi adresami IP można połączyć w logicznym standardzie DES z możliwością pracy w trybie awaryjnym.
DER (urządzenie przekierowujące wprowadzanie obszaru docelowego) łączy grupy wind i umożliwia urządzeniom DET we wspólnym punkcie wejścia do budynku, np. w poczekalni, na przyjmowanie żądań obszarów docelowych na dowolnych piętrach budynku. DER nie może działać w trybie awaryjnym.

Tworzenie urządzeń DES w drzewie urządzeń:
1. W edytorze urządzeń wybierz odpowiedni system Otis Compass w widoku drzewa
2. Kliknij prawym przyciskiem myszy i wybierz opcję **Nowy Otis DES**. Na stronie właściwości znajdują się 2 karty:

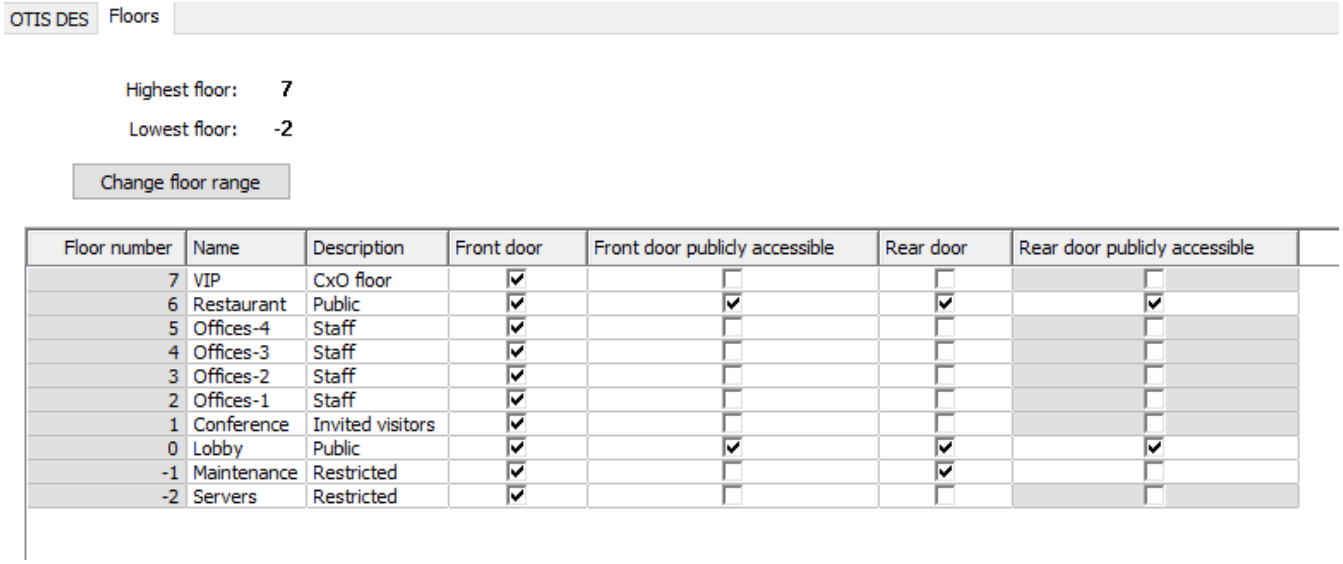
- **Otis DES**
- **Piętra**

3. Na karcie **Otis DES** ustaw następujące parametry:
   - **Nazwa**: nazwa, która powinna być widoczna w drzewie urządzeń.
     Użyj systematycznego schematu nazw, który ułatwi konfigurację urządzeń DES i DET na dalszych etapach.
   - **Opis:** (opcjonalnie) opis tekstowy urządzenia.
   - **Grupa:** liczba całkowita od 1 do 10**.** Każda grupa wind powinna mieć niepowtarzalny numer (zgodny z ich urządzeniami DES/DER) w danym systemie Otis Compass. Jeżeli użyjesz tego samego numeru **grupy** więcej niż raz, nie będzie można zapisać zmian wprowadzonych w urządzeniach.
   - **1. adres IP:** adres IP tego urządzenia DES.
   - **3. adres IP:** jeśli to urządzenie DES ma redundantne urządzenie bliźniacze, wprowadź jego adres w tym miejscu
   - **Strefa** (tylko jeśli Strefy są licencjonowane i używane w instalacji)

Na karcie **Piętra** piętra zdefiniowane w odniesieniu do warstwy 1 (system Compass) są przedstawiane w tabeli edytowalnych komórek.

Tworzenie urządzeń DER w drzewie urządzeń:
Urządzenia DER tworzy się niemal identycznie ja urządzenia DES z tą różnicą, że algorytm DER nie musi mieć żadnego urządzenia mogącego działać w trybie awaryjnym, więc **2. adres IP** nie ma żadnego parametru.

Przykładowa Grupa wind.
W poniższym przykładzie przedstawiono piętra grupy wind zawierających 10 pięter, z przednim/tylnymi drzwiami oraz dostępnymi publicznie poziomami parteru i 6. piętra.



Floor number	Name	Description	Front door	Front door publicly accessible	Rear door	Rear door publicly accessible
7	VIP	CxO floor	☑	☐	☐	☐
6	Restaurant	Public	☑	☑	☑	☑
5	Offices-4	Staff	☑	☐	☐	☐
4	Offices-3	Staff	☑	☐	☐	☐
3	Offices-2	Staff	☑	☐	☐	☐
2	Offices-1	Staff	☑	☐	☐	☐
1	Conference	Invited visitors	☑	☐	☐	☐
0	Lobby	Public	☑	☑	☑	☑
-1	Maintenance	Restricted	☑	☐	☑	☐
-2	Servers	Restricted	☑	☐	☐	☐

1. W kolumnie **Przednie drzwi** zaznacz pola wyboru wszystkich pięter, na których winda ma używać przednich drzwi.
2. W razie potrzeby zaznacz również pola wyboru w kolumnie **Tylne drzwi**.
3. W kolumnie **Przednie drzwi dostępne publicznie**, zaznacz pola wyboru tych pięter, które są dostępne dla wszystkich pasażerów windy bez ograniczeń.
4. W razie potrzeby zaznacz również pola wyboru w kolumnie **Tylne drzwi dostępne publicznie**.

5. (opcjonalnie) Kliknij na tej karcie opcję **Zmień zakres pięter**, aby bardziej ograniczyć zakres pięter ustawiony na poziomie systemu **Otis Compass**.
6. Zastąp nazwy domyślne w kolumnach **Nazwa**i **Opis** odpowiednimi nazwami kontekstowymi.
7. Kliknij przycisk  (Zapisz), aby zapisać zmiany.

21.1.3 Warstwa 3: Urządzenia DET

Procedura dotycząca warstwy 3: Konfigurowanie terminali (urządzeń DET)
Wstęp:
DET (znany również pod nazwą DEC, tj. komputer wprowadzania obszaru docelowego) odczytuje fizyczne poświadczenia lub kody PIN. DET może znajdować się na konkretnym piętrze za przednimi lub tylnymi drzwiami windy lub wewnątrz kabiny windy.

Tworzenie urządzeń DET w drzewie urządzeń:
1. W widoku drzewa edytora urządzeń wybierz odpowiednie urządzenie Otis DES/DER.
2. Kliknij prawym przyciskiem myszy i wybierz **Nowy terminal Otis Compass**.
   – Pojawi się okno podręczne **Utwórz terminale OTIS**
3. Wprowadź liczbę terminali do skonfigurowania na tym urządzeniu DES/DER.
4. Zaakceptuj wartości domyślne lub wprowadź nowe wartości początkowe czterech oktetów jego adresu IP.
   – Dla dowolnego oktetu, ale zazwyczaj dla czwartego, zaznacz pole wyboru **Automatyczny przyrost**, jeśli chcesz, aby system skonfigurował unikatowy adres IP dla każdego terminalu, zwiększając jego oktet.
5. Kliknij **OK**.
   – W drzewie urządzeń tworzona jest żądana liczba urządzeń DET.
   – Ich adresy IP są zwiększane zgodnie z konfiguracją w poprzednim kroku.

Konfigurowanie urządzeń DET
Na stronie właściwości każdego urządzenia DET znajdują się 2 karty:
– **Terminal Otis**
– **Piętra**
1. Na karcie **Terminal Otis** ustaw następujące parametry:
   – **Nazwa:** nazwa, która powinna być wyświetlana w drzewie urządzeń
   – **Opis** (opcjonalnie) opis tekstowy urządzenia.
   – **Adres IP** adres IP tego urządzenia DET
   – **Tryb operacyjny:** `1..4`
   określa, jak terminal żąda obszaru docelowego od pasażera windy i jak przekazuje żądania do urządzenia DES/DER w celu walidacji. Szczegółowe informacje można uzyskać w tabeli poniżej:

Tryb działania	Opis	Zachowanie
1	Domyślne piętro	(Domyślny tryb działania)

Tryb działania	Opis	Zachowanie
		Pasażer przedstawia swoje poświadczenie lub wpisuje kod PIN. Jeśli poświadczenie lub kod PIN są prawidłowe, a pasażer nie poda dalszych informacji, wówczas urządzenie DET wysyła do DES żądanie piętra domyślnego lub „domowego" pasażera. Jeśli pasażer wprowadzić inne piętro docelowe, wówczas urządzenie DET wysyła żądanie tego piętra do DES.
2	Dostęp do autoryzowanych pięter	Pasażer udostępnia swoje poświadczenie lub wpisuje kod PIN, a następnie wpisuje docelowe piętro. Urządzenie DET wysyła żądanie obszaru docelowego do DES. System kontroli dostępu przyznaje dostęp do żądanego obszaru docelowego lub nie przyznaje takiego dostępu.
3	Wprowadzenie piętra docelowego przez użytkownika	Pasażer wprowadza piętro docelowe. Jeśli obszar docelowy jest publicznie dostępny, urządzenie DET wysyła żądanie tego obszaru docelowego do DES. Jeżeli nie jest do obszar publicznie dostępny, urządzenie DET prosi pasażera o udostępnienie poświadczeń w celu weryfikacji.
4	Piętro domyślne lub wprowadzenie przez użytkownika piętra docelowego.	Pasażer przedstawia swoje poświadczenie lub wpisuje kod PIN. Jeśli poświadczenia lub kod PIN są prawidłowe, wówczas urządzenie DET wysyła od DES żądanie piętra domyślnego lub „domowego" pasażera. W wyznaczonym przedziale czasu pasażer może zastąpić wybór domyślnego piętra i wybrać inny obszar docelowy.

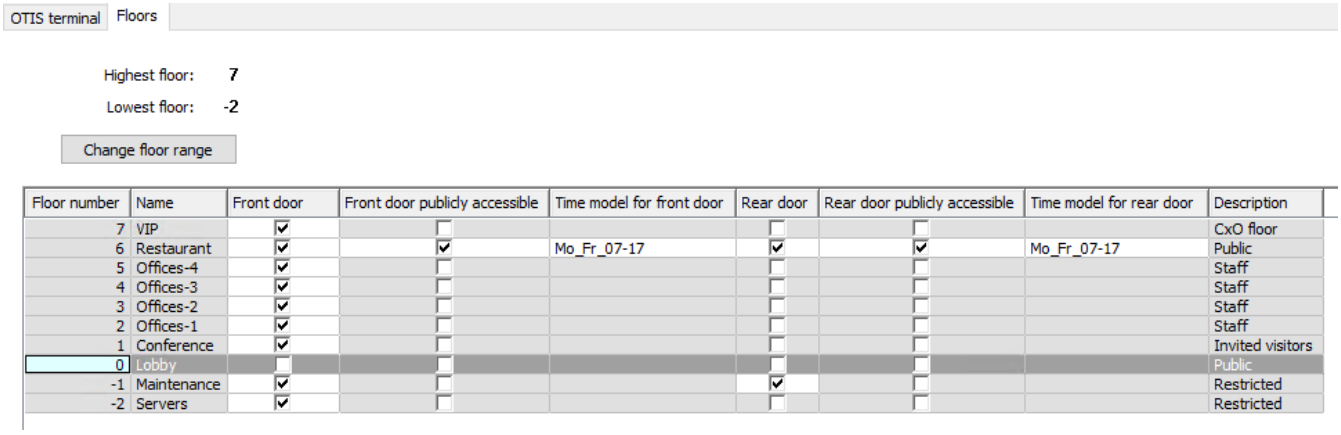
- **Rekordy audytu:** zaznacz to pole wyboru, aby rejestrować dane wprowadzane przez pasażerów na danym terminalu w dzienniku danych.
- **Kod PIN:** zaznacz to pole wyboru, aby zezwolić na używanie identyfikacyjnego kodu PIN na danym terminalu jako alternatywy poświadczeń fizycznych.
  Uwaga: do rejestracji kodów PIN, które mają być używane w terminalach Otis użyj czytników rejestracji typu **Okno dialogowe karty PIN (wprowadzanie)**.
- **Modele czasowe:** zaznacz to pole wyboru, aby zezwolić na używanie modeli czasowych w celu ograniczenia czasu, w jakim można używać danego terminalu.
- **Strefa** (tylko jeśli Strefy są licencjonowane i używane w instalacji)

Na karcie **Piętra** na stronie właściwości **terminalu Otis** piętra zdefiniowane w warstwie 2 (DES/DER), są przedstawiane jako tabela komórek edytowalnych.
Uwaga: Schemat nazewnictwa zdefiniowany w warstwie 2 powyżej powinien zapewniać odpowiednią orientację. W przeciwnym razie zalecamy zapisanie pracy i powrót do warstwy 2 w celu uzupełnienia schematu nazewnictwa.

1. Wybieraj kolejno poszczególne urządzenia DET, które zostały dopiero co utworzone w drzewie urządzeń, i otwórz kartę **Piętra**.
   – Zostanie wyświetlona tabela **Piętra**
2. W kolumnie **Przednie drzwi** zaznacz pola wyboru każdego piętra, które ma być osiągalne z aktualnego urządzenia DET.
3. W kolumnie **Przednie drzwi dostępne publicznie** zaznacz pole wyboru przy każdych drzwiach wejściowych, które mają być dostępne publicznie, czyli niewymagające wyraźnej autoryzacji.
4. (opcjonalnie) W kolumnie **Model czasowy przednich drzwi** wybierz model czasowy, aby ograniczyć publiczny dostęp do przednich drzwi na danym piętrze, jeśli jest to wymagane. Na przykład, piętro restauracji może być dostępne tylko w określonych godzinach.
5. W razie potrzeby powtórz wcześniejsze kroki w odniesieniu do kolumn **Tylne drzwi**, **Tylne drzwi publicznie dostępne** oraz **Model czasowy tylnych drzwi.**
6. Kliknij przycisk  (Zapisz), aby zapisać zmiany.

Przykład:

Na przykładzie poniżej pokazano piętra w 10-piętrowej grupie wind wraz z piętrami i drzwiami dostępnymi z przednich drzwi windy w holu. Dostęp do piętra restauracji, zarówno z przednich, jak i tylnych drzwi windy, jest ograniczony modelem czasowym.



Floor number	Name	Front door	Front door publicly accessible	Time model for front door	Rear door	Rear door publicly accessible	Time model for rear door	Description
7	VIP	☑	☐		☐	☐		CxO floor
6	Restaurant	☑	☑	Mo_Fr_07-17	☑	☑	Mo_Fr_07-17	Public
5	Offices-4	☑	☐		☐	☐		Staff
4	Offices-3	☑	☐		☐	☐		Staff
3	Offices-2	☑	☐		☐	☐		Staff
2	Offices-1	☑	☐		☐	☐		Staff
1	Conference	☑	☐		☐	☐		Invited visitors
0	Lobby	☐	☐		☐	☐		Public
-1	Maintenance	☑	☐		☑	☐		Restricted
-2	Servers	☑	☐		☐	☐		Restricted

21.2 Konfigurowanie pól niestandardowych dotyczących specyficznych dla Otis właściwości posiadacza

Wstęp

W tej sekcji opisano sposób tworzenia pól niestandardowych, w których operator może wprowadzić specyficzne dla Otis właściwości posiadacza karty, w szczególności jego „domowy” lub domyślny obszar docelowy. Ten obszar „domowy” musi być określony przez **trzy współrzędne**:

1. Grupa wind,
2. Piętro
3. Drzwi

Należy pamiętać, że podczas określania piętra domowego posiadacza karty w urządzeniu klienckim systemu kontroli dostępu operator musi wprowadzić dane w tej samej kolejności: grupa wind, piętro, drzwi. Dlatego trzy pola niestandardowe powinny być umieszczone w kolejności czytania, najlepiej od góry do dołu.

Kliknij przycisk **OK**, aby potwierdzić wszelkie wyskakujące przypomnienia o konieczności skonfigurowania wszystkich trzech współrzędnych.
Zdefiniuj 3 niezbędne pola niestandardowe oraz wszelkie wymagane specjalne opcje Otis, które mają być wyświetlane na karcie **Windy** w interfejsie urządzenia klienckiego kontroli dostępu.
Informacje ogólne na temat konfigurowania pól niestandardowych można znaleźć w pomocy konfiguracji ACE/AMS w sekcji **Niestandardowe pola na dane osobowe**

Ścieżka w oknie dialogowym
Menu główne > **Konfiguracja** > **Opcje** > **Pola niestandardowe**

Procedura
Na stronie właściwości **Pola niestandardowe** wybierz kartę **Windy**.
Pierwsza współrzędna: Grupa wind
1. Kliknij dwukrotnie w komórce na karcie i kliknij **Tak**, aby utworzyć nowe pole wprowadzania danych.
2. Z listy **Typ pola** wybierz opcję **Wybór Otis DES**.
3. W polu **Etykieta** wprowadź `Elevator Group`
4. Z listy **Wyświetlaj w** wybierz `Tab:Elevators`
5. W grupie **Pozycja** wybierz unikalną lokalizację na karcie **Windy**, w której to pole ma się pojawić.

Druga współrzędna: Piętro domowe
1. Kliknij przycisk **Nowe pole**, aby utworzyć nowe pola niestandardowe
2. Z listy **Typ pola** wybierz opcję **Piętro domowe**.
3. W polu **Etykieta** wprowadź `Home floor`
4. Z listy **Wyświetlaj w** wybierz `Tab:Elevators`
5. W grupie **Pozycja** wybierz unikalną lokalizację na karcie **Windy**, w której to pole ma się pojawić. Aby ułatwić zadanie operatorom systemu, pole to powinno znajdować się pod poprzednią współrzędną.

Trzecia współrzędna: Drzwi wyjściowe
1. Kliknij przycisk **Nowe pole**, aby utworzyć nowe pola niestandardowe
2. Z listy **Typ pola** wybierz opcję **Drzwi wyjściowe**.
3. W polu **Etykieta** wprowadź `Exit door`
4. Z listy **Wyświetlaj w** wybierz `Tab:Elevators`
5. W grupie **Pozycja** wybierz unikalną lokalizację na karcie **Windy**, w której to pole ma się pojawić. Aby ułatwić zadanie operatorom systemu, pole to powinno znajdować się pod poprzednią współrzędną.

Specjalne opcje Otis dla posiadaczy kart
Wstęp
Zgodnie ze standardową funkcjonalnością systemu Otis, dostępnych jest osiem opcji binarnych specyficznych dla Otis. Jeśli są zdefiniowane jako niestandardowe pola na karcie **Windy**, są wyświetlane jako pola wyboru na karcie **Dane windy** posiadaczy kart w oknie dialogowym **Osoby** (Menu główne > **Dane osobowe** > **Osoby**). Mogą być one następnie wybierane i usuwane przez operatorów systemu kontroli dostępu.
Skonfiguruj te opcje tylko zgodnie z instrukcjami przedstawiciela Otis.
Procedura
1. Kliknij przycisk **Nowe pole**, aby utworzyć nowe pola niestandardowe

2. Z listy **Typ pola** wybierz **Opcje Otis**.
3. W polu **Etykieta** wprowadź własną etykietę, np. `Otis flag 1` lub zgodnie z dokumentacją Otis.
4. Z listy **Wyświetlaj w** wybierz `Tab:Elevators`
5. Z listy **Typ funkcji** wybierz jedną z opcji: od `OTIS option 1` do `OTIS option 8`
6. W grupie **Pozycja** wybierz unikalną lokalizację na karcie **Windy**, w której to pole wyboru ma się pojawić.
7. Kliknij przycisk  (Zapisz), aby zapisać zmiany.

21.3 Tworzenie i konfigurowanie autoryzacji dla wind Otis

Wstęp

W tej części instrukcji opisano sposób włączania praw dostępu dla grup wind Otis, pięter i drzwi wind za pośrednictwem **autoryzacji**.

Autoryzacje są przypisywane bezpośrednio do posiadaczy kart lub częściej łączone z innymi autoryzacjami w **Profile dostępu**, które są następnie przypisywane do posiadaczy kart.

Wymagania wstępne

W edytorze urządzeń na kontrolerze MAC został zdefiniowany system Otis Compass. Jest on dostarczany wraz z grupą wind (której odpowiada jej DES) oraz kombinacjami drzwi i pięter (którym odpowiadają ich urządzenia DET).

Ścieżka w oknie dialogowym

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

Procedura

1. W polu **Nazwa autoryzacji** wprowadź nazwę istniejącego uprawnienia lub kliknij  (Nowy) w celu utworzenia nowego uprawnienia.
2. Na liście kontrolerów **MAC** wybierz nazwę kontrolera MAC, na którym został utworzony system Otis Compass.
3. Kliknij kartę **Winda OTIS**
4. Na liście **wind Otis** wybierz DES/DER dla grupy windy, którą chcesz dodać do uprawnienia (Uwaga: Autoryzacja może zawierać tylko jedno urządzenie DES/DER).
   – Piętra wybranej grupy wind są wyświetlane w okienku **Piętra**.
5. W kolumnach **Przednie drzwi** oraz **Tylne drzwi** okienka **Piętra** wybierz drzwi na piętrach, które chcesz uwzględnić w tym uprawnieniu.
   – Uwaga: piętra i drzwi, które **nie** zostały zaznaczone dla tej grupy wind na etapie definiowania w edytorze urządzeń, będą oznaczone kolorem szarym i nie będzie można ich wybrać w tym menu.
6. Można także kliknąć przyciski **Przypisz wszystkie piętra** i **Usuń wszystkie piętra**, aby jednocześnie wybrać lub wyczyścić wszystkie piętra i drzwi.
7. Kliknij  (**Zapisz**), aby zapisać uprawnienie.

22 Konfiguracja IDEMIA Universal BioBridge

W tej części znajduje się opis konfiguracji urządzeń biometrycznych IDEMIA pod kątem współpracy z systemami kontroli dostępu Bosch przy użyciu opcji **MorphoManager** i **BioBridge**.
W podsekcjach zostały opisane zadania konfiguracyjne, które należy wykonać w następujących obszarach:

- Systemy kontroli dostępu firmy Bosch
- MorphoManager
- Rejestracja klienta BioBridge w MorphoManager
- Adaptacje do potrzeb rozmaitych formatów i technologii kart

22.1 Konfiguracja BioBridge w systemie kontroli dostępu Bosch

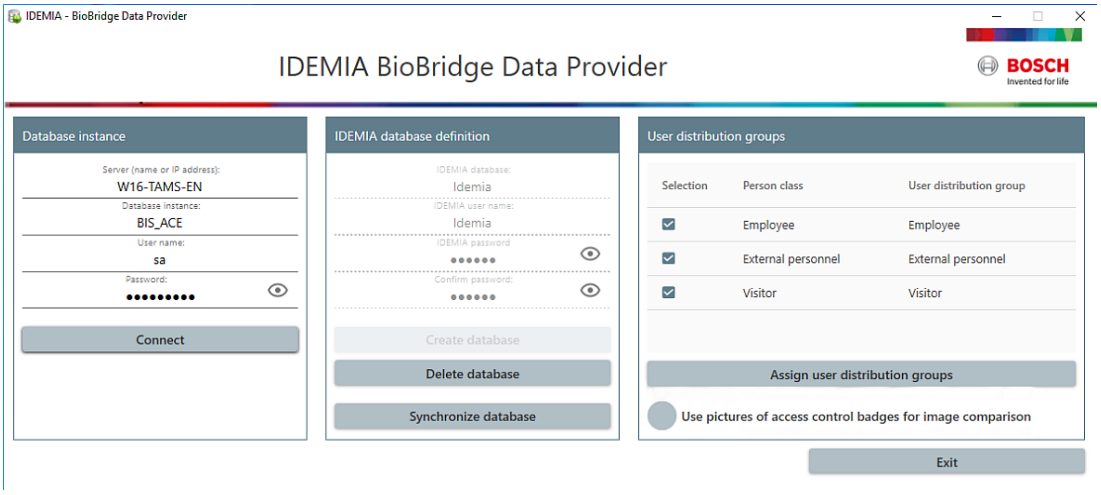
Czynności opisane poniżej są wykonywane w systemie ACS w celu utworzenia bazy danych łączącej urządzenia biometryczne IDEMIA z systemem kontroli dostępu Bosch. Baza danych mapuje między sobą następujące podmioty bazy danych:

- **Klasa osób** (Bosch) i
- **Grupa dystrybucji użytkownika** (IDEMIA).

Ścieżka w oknie dialogowym

- Menu główne AMS > **Konfiguracja** > **Narzędzia** > **Baza danych IDEMIA konfiguracji**

1. Kliknij opcję **Baza danych IDEMIA konfiguracji**
   Zostanie wyświetlone okno dialogowe **Dostawca danych IDEMIA BioBridge**.



2. W okienku **Instancja bazy danych** wprowadź następujące informacje:

- **Serwer**: Nazwa hosta lub adres IP komputera, na którym uruchomiona jest instancja bazy danych SQL Server systemu ACS. Może to być lokalna nazwa hosta, jeśli serwer SQL działa na komputerze lokalnym.
- **Instancja bazy danych**: wystąpienie bazy danych systemu ACS (domyślnie `ACE`).
- **Nazwa użytkownika**: nazwa konta administratora wystąpienia bazy danych systemu ACS (domyślnie: `sa`)
- **Hasło**: hasło konta administratora skonfigurowane podczas instalacji systemu ACS.

3. Kliknij przycisk **Połącz**, aby przetestować połączenie. Dopóki tego nie zrobisz, wszystkie inne formanty są wyłączone.

W okienku definicji bazy danych IDEMIA

Pierwsze dwa pola są tylko do odczytu:

– **Baza danych Idemia**: nazwa bazy danych łączącej dane systemów Bosch i IDEMIA.
– **Nazwa użytkownika w systemie Idemia**: nazwa użytkownika bazy danych, w imieniu którego oprogramowanie wykonuje polecenia w bazie danych.

1. Wprowadź i Potwierdź silne hasło dla **nazwy użytkownika systemu Idemia**.
2. Zapisz dokładnie hasło. Podanie tego hasła będzie wymagane do wykonania zadań konfiguracyjnych w przyszłości. W razie utraty hasła nie można go przywrócić.
3. Kliknij przycisk **Utwórz bazę danych**.
   Pomyślne utworzenie bazy danych zostanie potwierdzone wyświetleniem komunikatu. Kliknij **OK**.
4. Po pomyślnym zakończeniu testu kliknij przycisk **Zakończ** w celu zamknięcia okna dialogowego.

W okienku Grupy dystrybucji użytkownika

Grupy dystrybucyjne użytkowników są obiektami MorphoManager mapującymi użytkowników (posiadaczy poświadczeń) do grup czytników biometrycznych lub klientów MorphoManager. Mapujemy je do **klas osób** w systemach kontroli dostępu Bosch.

1. W kolumnie Wybierz zaznacz pola wyboru obok wszystkich **klas osób** ACE używanych przez Twoją instalację.
2. Dla każdego wybranego wiersza skopiuj nazwę Klasy osób do odpowiedniej komórki w kolumnie **Grupa dystrybucji użytkownika**.

– Należy pamiętać, że nazwy w polach **Klasa osób** i **Grupa dystrybucji użytkownika** muszą być dokładnie takie same.

3. Po zakończeniu mapowania kliknij przycisk **Przypisz grupę dystrybucji użytkownika**.

Dostarczanie zdjęć identyfikacyjnych dla systemu rozpoznawania twarzy VisionPass

Aby czytniki IDEMIA mogły wykonywać rozpoznawanie twarzy VisionPass przy użyciu zdjęć identyfikacyjnych posiadaczy kart z bazy danych ACE:

- Kliknij przycisk
  Używaj zdjęć kart identyfikacyjnych kontroli dostępu w celu porównywania obrazów i potwierdź to w wyskakującym oknie.
  Okno **dostawcy danych IDEMIA BioBridge** wyświetla informację o trwającej synchronizacji.
  Uwaga: w zależności od ilości danych obrazu transfer może trwać dłużej.

22.2 Wybór technologii i formatów kart

Wstęp

Jeśli zamierzasz używać kart w połączeniu z identyfikacją biometryczną, musisz utworzyć profil (lub „profil Wiegand”) w MorphoManager zawierający format (lub formaty) tych kart dostępu.

Poniższa tabela zawiera przegląd obsługiwanych formatów. Należy pamiętać, że w przypadku technologii MIFARE obsługiwana jest tylko identyfikacja CSN.

Card Family	HID Prox	HID Class	HID iClass Seos	MIFARE Classic	MIFARE DESFire EV0	MIFARE DESFire EV1
Card Variant	Prox	2k/2 16k/2 16k/16 32k(16k/2+16k/1) 32k(16k/16+16k/1)	Seos	1K 4-byte NUID 1k 7-byte UID 4k 4-byte NUID 4k 7byte UID	2k 4k 8k	2k 4k 8k

Rysunek 22.1: Obsługiwane karty IDEMIA

Procedura ogólna

1. W aplikacji MorphoManager przejdź do menu **Administracja** > **Profil Wiegand**
2. Kliknij przycisk **Dodaj**, aby utworzyć niestandardowy profil Wiegand
3. W odpowiednich oknach dialogowych wprowadź informacje o formatowaniu i technologii kart używane przez system
4. Aby użyć nowo zdefiniowanego profilu Wiegand w systemie, wprowadź jego nazwę w polu **Profil Wiegand** w następujących oknach dialogowych aplikacji MorphoManager:

– **Administracja > Profil urządzenia biometrycznego**
– **Administracja > Zasady dotyczące użytkownika**

Mifare Classic CSN

1. Dodaj element Wiegand `User CSN Element` i wprowadź następujące dane

– **Nazwa**: `CSN` (na przykład)
– **Długość** `32`
– **Tryb transformacji:** `Reversed`

2. **W obszarze Administracja > Profil urządzenia biometrycznego** na stronie **Ustawienia trybu wieloskładnikowego** zaznacz pole wyboru **MIFARE Classic**.

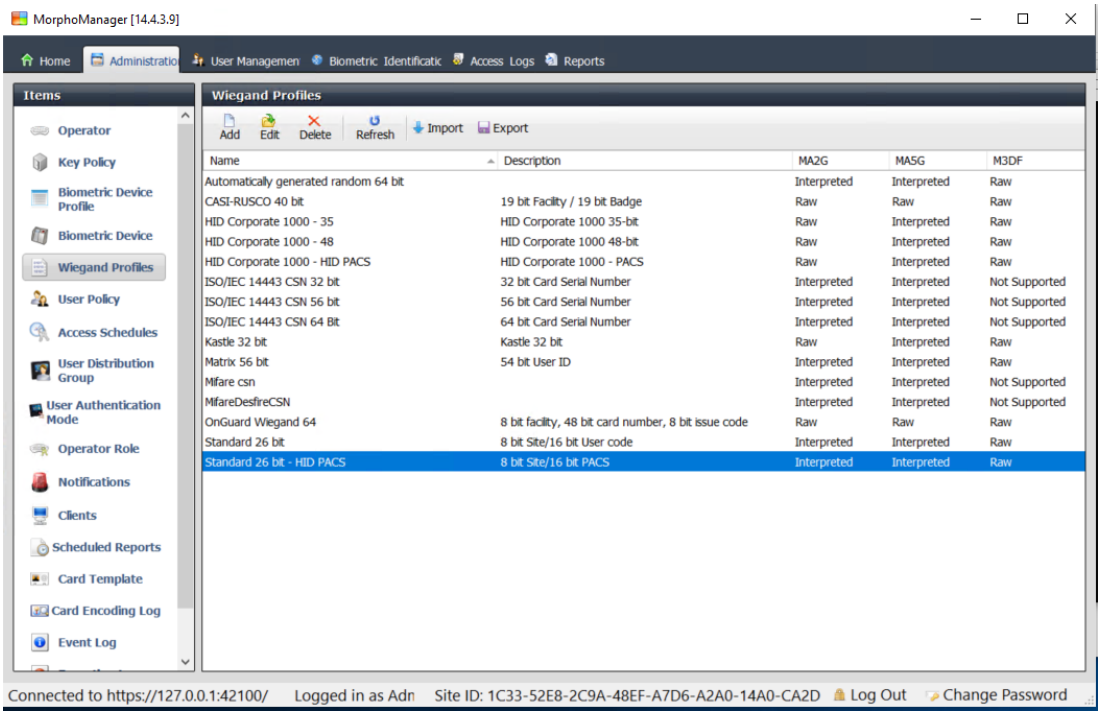
Mifare DESFire CSN

Konfiguracja jest identyczna jak w przypadku Mifare Classic z wyjątkiem następujących szczegółów:

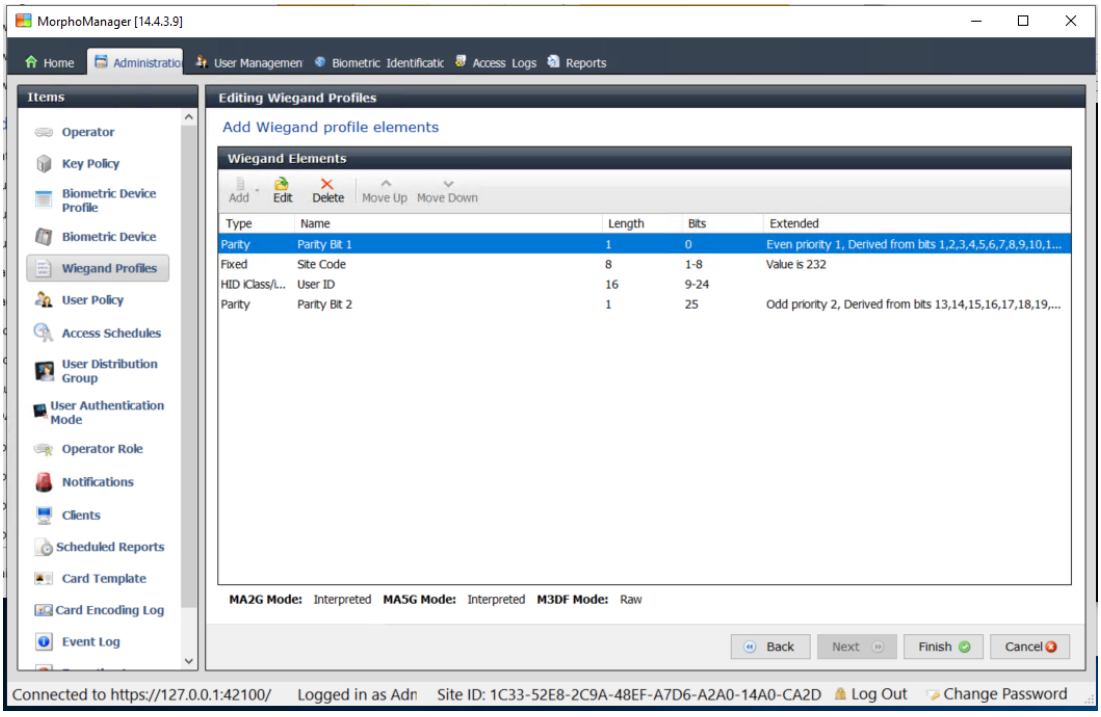
– **Długość:** `56`
– Dodaj **Element Wiegand Element CSN użytkownika**
  – Wprowadź nazwę w obszarze **Nazwa:**
  – Jako **Długość** wprowadź 56
  – Jak **Tryb transformacji:** wprowadź `Reversed`
– **W obszarze Administracja > Profil urządzenia biometrycznego** na stronie **Ustawienia trybu wieloskładnikowego** zaznacz pole wyboru **Mifare DESFire 3DES**.

iClass 26 BIT

1. Wybierz wstępnie zdefiniowany profil `Standard 26 bit-HID PACS`



2. Kliknij przycisk **Edytuj**
3. Kliknij przycisk **Dalej>**.



4. Kliknij przycisk **Edytuj**
5. Usuń wiersz `Fixed Facility Code`
6. Wybierz wiersz `HID iClass SEP User ID`
7. Kliknij przycisk **Edytuj**
8. Zmień długość identyfikatora użytkownika z `1..16` na `1..24`
9. **W obszarze Administracja > Profil urządzenia biometrycznego** na karcie Ustawienia urządzenia biometrycznego wybierz dla Profilu Wiegand wartość `Standard 26 BIT-HID-PACS`

10. **W obszarze Administracja > Profil urządzenia biometrycznego** na stronie **Ustawienia trybu wieloskładnikowego** zaznacz pole wyboru `HID iClass`
11. Klikaj Dalej, aż przejdziesz do strony **Parametry niestandardowe**
12. Kliknij przycisk **Dodaj**
13. Dodaj parametr niestandardowy (uwzględniający wielkość liter) `wiegand.site_code_propagation`
14. Ustaw jego wartość na `1`
15. Kliknij przycisk **Finish (Zakończ)**.
16. Wprowadź ten ukończony profil Wiegand w obszarze **Administracja > Zasady dotyczące użytkownika**

iClass 35 BIT

1. Wybierz wstępnie zdefiniowany profil`HID Corporate 1000 35 BIT`
2. Kliknij przycisk **Edytuj**
3. Kliknij przycisk **Dalej>**.
4. Wybierz i usuń linię elementu `Fixed Company ID`
5. Wybierz i usuń linię elementu `User Card ID Number`
6. Dodaj wiersz elementu `HID iClass/iClass SE PACS Data` i szczegóły elementu, po czym skonfiguruj następujące ustawienia:

– Nazwa: `Card ID Number`
– Długość: `32`
– **W obszarze Administracja > Profil urządzenia biometrycznego** na stronie **Ustawienia trybu wieloskładnikowego** zaznacz pole wyboru `HID iClass`
– Klikaj **Dalej**, aż przejdziesz do strony **Parametry niestandardowe**
– Kliknij przycisk **Dodaj**
– Dodaj parametr niestandardowy (uwzględniający wielkość liter) `wiegand.site_code_propagation`
– Ustaw jego wartość na `1`
– Kliknij przycisk **Finish (Zakończ)**.
– Wprowadź ten ukończony profil Wiegand w obszarze **Administracja > Zasady dotyczące użytkownika**

iClass 37 BIT

– **Administracja > Profil Wiegand**
– Kliknij **Dodaj nowy profil**
– **Długość** `37`

1. Dodaj parzystość elementów:

– **Nazwa**: (na przykład) `EvenParityBit 1`
– **Priorytet**: `1`
– **Długość**: `18`
– **Tryb**: `Even`
– **Podstawowe bity**: `1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18`
– Kliknij przycisk **Dalej>**.

2. Dodaj element `User HID iClass/iClass SE PACS Data` i jego szczegóły, po czym skonfiguruj następujące ustawienia:

– **Imię i nazwisko:** `UserID`
– **Długość**: `35`
– Kliknij przycisk **Dalej>**.

3. Dodaj parzystość elementów:

- **Nazwa**: (na przykład): `Parity Bits 2`
- **Priorytet**: `2`
- **Długość**: `19`
- **Tryb**: `Odd`
- **Podstawowe bity**: `19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37`
- Kliknij przycisk **Dalej>**.
- **W obszarze Administracja > Profil urządzenia biometrycznego** na stronie **Ustawienia trybu wieloskładnikowego** zaznacz pole wyboru `HID iClass`
- Klikaj **Dalej**, aż przejdziesz do strony **Parametry niestandardowe**
- Kliknij przycisk **Dodaj**
- Dodaj parametr niestandardowy (uwzględniający wielkość liter) `wiegand.site_code_propagation`
- Ustaw jego wartość na `1`
- Kliknij przycisk **Finish (Zakończ)**.
- Wprowadź ten ukończony profil Wiegand w obszarze **Administracja > Zasady dotyczące użytkownika**

iClass 48BIT

1. Wybierz wstępnie zdefiniowany profil`HID Corporate 1000 48 BIT`
2. Kliknij przycisk **Edytuj**
3. Kliknij przycisk **Dalej>**.
4. Wybierz i usuń linię elementu `Fixed Company ID`
5. Wybierz i usuń linię elementu `User Card ID Number`
6. Dodaj wiersz elementu `HID iClass/iClass SE PACS Data` i szczegóły elementu, po czym skonfiguruj następujące ustawienia:

- Nazwa: `User`
- Długość: `45`

7. **W obszarze Administracja > Profil urządzenia biometrycznego** na stronie **Ustawienia trybu wieloskładnikowego** zaznacz pole wyboru `HID iClass`
8. Klikaj **Dalej**, aż przejdziesz do strony **Parametry niestandardowe**
9. Kliknij przycisk **Dodaj**
10. Dodaj parametr niestandardowy (uwzględniający wielkość liter) `wiegand.site_code_propagation`

- Ustaw jego wartość na `1`

11. Kliknij przycisk **Finish (Zakończ)**.
12. Wprowadź ten ukończony profil Wiegand w obszarze **Administracja** > **Zasady dotyczące użytkownika**

HID Prox

1. Wybierz wstępnie zdefiniowany profil `Standard 26 BIT`
2. Kliknij przycisk **Edytuj**
3. Kliknij przycisk **Dalej>**.
4. Usuń wiersz `Fixed Facility Code`
5. Kliknij przycisk **Edytuj**
6. Zmień długość identyfikatora użytkownika z `1..16` na `1..24`
7. **W obszarze Administracja > Profil urządzenia biometrycznego** na karcie Ustawienia urządzenia biometrycznego wybierz dla Profilu Wiegand wartość `Standard 26 BIT`
8. **W obszarze Administracja > Profil urządzenia biometrycznego** na stronie **Ustawienia trybu wieloskładnikowego** zaznacz pola wyboru:

– **Biometria**
– **Karta zbliżeniowa**
9. Klikaj **Dalej**, aż przejdziesz do strony **Parametry niestandardowe**
10. Kliknij przycisk **Dodaj**
11. Dodaj parametr niestandardowy (uwzględniający wielkość liter)
`wiegand.site_code_propagation`
– Ustaw jego wartość na `1`
12. Kliknij przycisk **Finish (Zakończ)**.
13. Wprowadź ten ukończony profil Wiegand w obszarze **Administracja** > **Zasady dotyczące użytkownika**

22.3 Wybór trybu identyfikacji

Wstęp

Czytniki biometryczne mogą identyfikować posiadaczy poświadczeń na różne sposoby. Metody te są nazywane trybami identyfikacji lub trybami uwierzytelniania.

– Według **Kart lub Biometrii**, zależnie od tego, jakie poświadczenia zostaną okazane w kontakcie z czytnikiem
– Za pomocą **Karty i Biometrii**, tzn. użytkownik musi potwierdzić danymi biometrycznymi, że jest posiadaczem karty.
– Tylko **Biometria**

W tej części został przedstawiony sposób konfigurowania trybów w aplikacji MorphoManager.

Należy pamiętać, że wszędzie tam, gdzie w grę wchodzą dane uwierzytelniające karty, konieczne jest oczywiście utworzenie profilu dla odpowiedniej technologii i formatu karty.

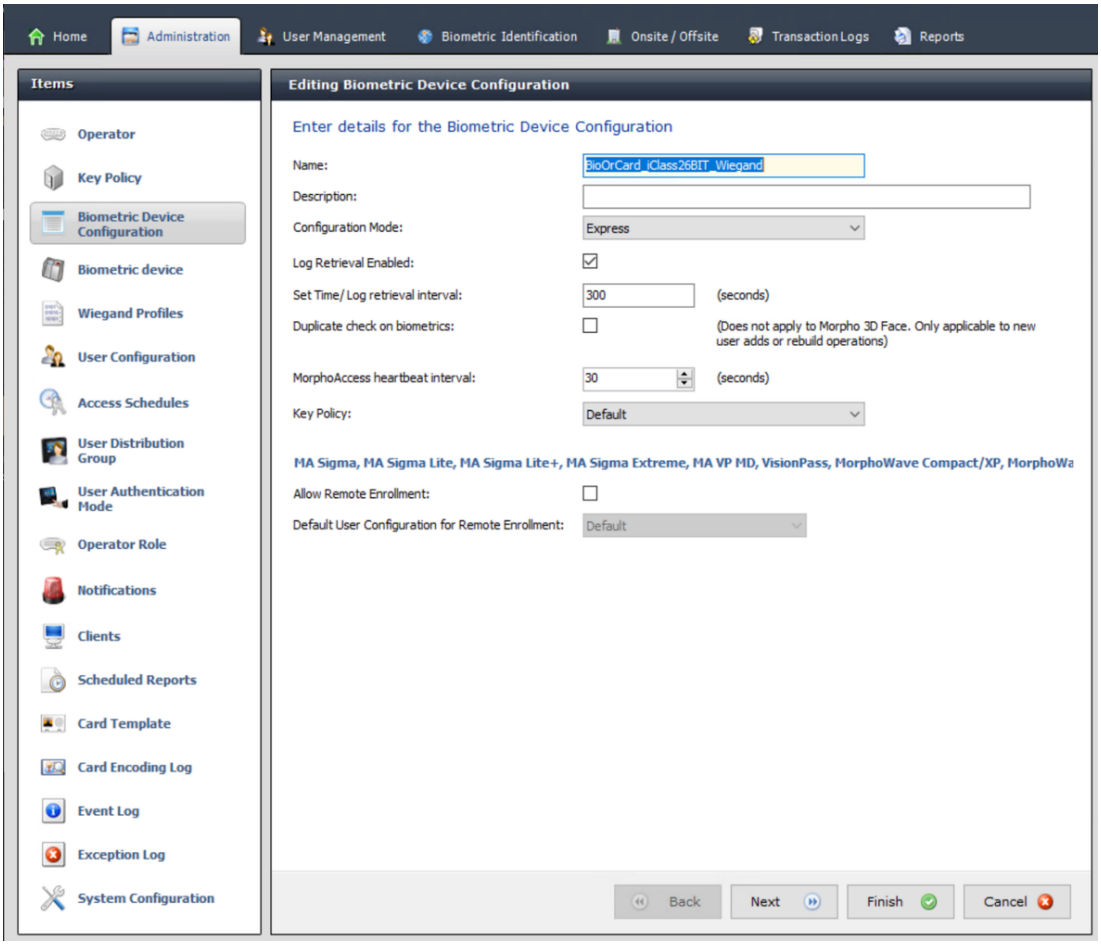
Ścieżka w oknie dialogowym

Na karcie **Administracja** w aplikacji MorphoManager

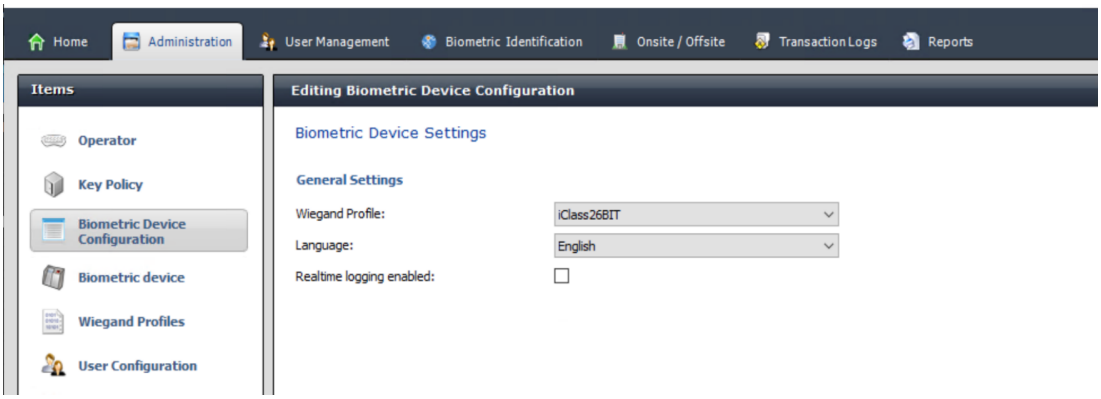
22.3.1 Karta lub Biometria

Ten niestandardowy tryb uwierzytelniania należy utworzyć w sytuacji, gdy użytkownicy mają się identyfikować za pomocą karty LUB poświadczeń biometrycznych.

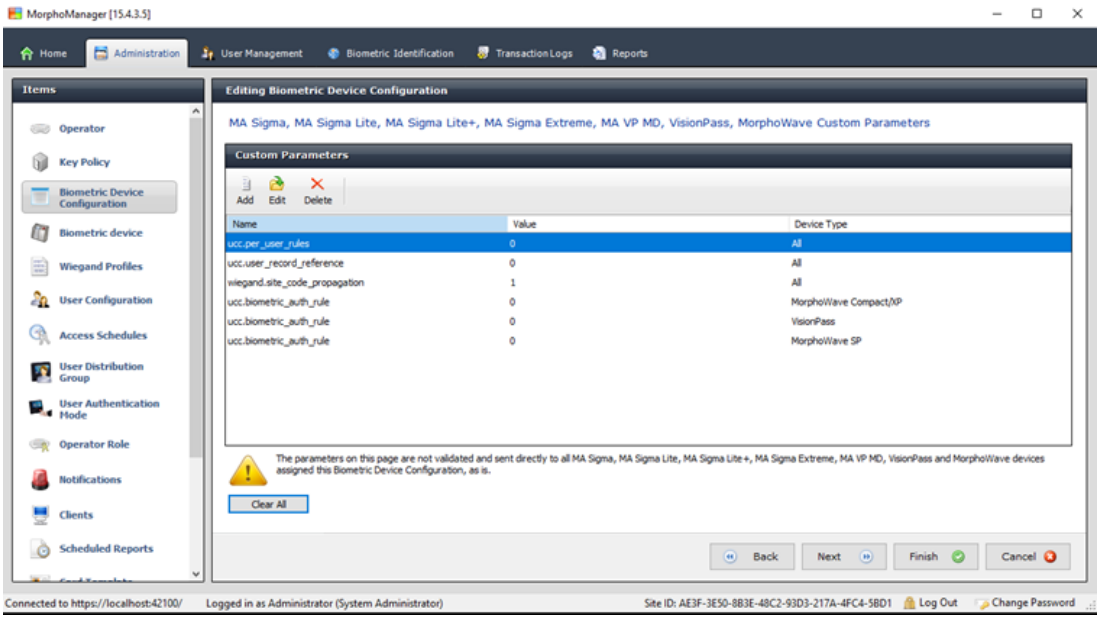
1. W aplikacji MorphoManager przejdź do menu **Administracja** > **Biometria** > **Konfiguracja urządzenia**
2. Nadaj nazwę tej konfiguracji urządzenia biometrycznego, np. `CardORBiometric`



3. Klikaj **Dalej**, aż przejdziesz do karty **Ustawienia urządzenia biometrycznego**



4. W przypadku **profilu Wiegand** wybierz ten sam profil, który został zdefiniowany dla urządzeń biometrycznych podczas konfigurowania BioBridge.
5. Klikaj przycisk **Dalej**, aż dotrzesz do okna dialogowego **Ustawienia progu rozpoznawania biometrycznego**.
6. W obszarze **Próg rozpoznawania biometrycznego** ustaw wartości na podstawie lokalnych warunków i dokumentacji oprogramowania MorphoManager. Wartość domyślna to `Recommended`.
7. Klikaj przycisk **Dalej**, aż dotrzesz do ekranu **Ustawienia trybu wieloskładnikowego**.
8. Zaznacz pole wyboru **Biometria** oraz pole wyboru technologii kart używanej przez daną instalację.
9. Klikaj **Dalej**, aż przejdziesz do ekranu **Parametry niestandardowe**



10. Dla każdego używanego urządzenia:
    Kliknij przycisk **Dodaj**, aby dodać dwa niestandardowe parametry.
    (Jeśli te dwa parametry są ustawione, czytnik przesyła dane karty bezpośrednio do AMC. Użytkownik nie musi być zarejestrowany na czytniku IDEMIA.)

– `ucc.per_user_rules`
– `ucc.user_record_reference`

11. Dla czytników WAVE i VisionPass dodaj jeszcze jeden parametr:

– `ucc.biometric_auth_rule=0`
– W tym przypadku w ustawieniu **Typ urządzenia** zaznacz wartość `MorphoWave Compact/XP`, `MorphoWave SP` lub `VisionPass`

12. Kliknij przycisk **Finish (Zakończ)**

Przypisz ten tryb uwierzytelniania do użytkowników

W systemie ACS każdemu docelowemu posiadaczowi karty należy przypisać prawidłowo zdefiniowaną kartę.

1. W aplikacji MorphoManager przejdź do menu **Administracja** > **Tryb uwierzytelniania użytkowników**
2. Skonfiguruj następujące atrybuty**:**

– W polu **Tryb** ustaw wartość `Enabled`
– Na liście **Lokalizacja szablonu** zaznacz wartość `Download to Device`
– Zaznacz pole wyboru **Zezwalaj na uruchamianie biometryczne**
– Zaznacz pole wyboru **Zezwól na uruchamianie przez bezdotykowe karty**
– Wyłącz opcję **Wymagaj dopasowania szablonu**

3. Wybierz kolejno opcje **Administracja** > **Konfiguracja użytkownika**
4. Kliknij przycisk **Dodaj**
5. W ustawieniu **Tryb uwierzytelniania użytkowników** zaznacz nazwę trybu utworzonego wyżej dla trybu Karta lub Biometria.
6. Kliknij przycisk **Finish (Zakończ)**

Patrz

– *Wybór technologii i formatów kart, Strona 159*

22.3.2 Karta ORAZ biometria

Wprowadź następujące ustawienia, jeśli użytkownicy mają używać karty ORAZ poświadczeń biometrycznych w celu weryfikacji, że są posiadaczami karty.

1. W aplikacji MorphoManager przejdź do menu **Administracja** > **Biometria** > **Konfiguracja urządzenia**
2. Klikaj **Dalej**, aż przejdziesz do karty **Ustawienia urządzenia biometrycznego**
3. W przypadku **profilu Wiegand** wybierz ten sam profil, który został zdefiniowany dla urządzeń biometrycznych podczas konfigurowania BioBridge.
4. Kliknij przycisk **Dalej**, aż dotrzesz do strony **Ustawienia trybu wieloskładnikowego**.
5. Zaznacz pole wyboru technologii karty, której używa Twoja instalacja.
6. Kliknij przycisk **Finish (Zakończ)**

Przypisz ten tryb uwierzytelniania do użytkowników

W systemie ACS każdemu docelowemu posiadaczowi karty należy przypisać prawidłowo zdefiniowaną kartę.

1. W aplikacji MorphoManager przejdź do menu **Administracja** > **Konfiguracja użytkownika**
2. W przypadku **trybu uwierzytelniania użytkownika** wybierz `Contactless Card ID + Biometric` z listy.
3. Kliknij przycisk **Zakończ**.

Patrz

– *Wybór technologii i formatów kart, Strona 159*

22.3.3 Tylko biometria

Jeśli użytkownicy mają się identyfikować wyłącznie na podstawie poświadczeń biometrycznych, należy wprowadzić następujące ustawienia.

1. W aplikacji MorphoManager przejdź do menu **Administracja** > **Biometria** > **Konfiguracja urządzenia**
2. Klikaj **Dalej**, aż przejdziesz do karty **Edytowanie konfiguracji urządzenia biometrycznego**
3. W przypadku **profilu Wiegand** wybierz ten sam profil, który został zdefiniowany dla urządzeń biometrycznych podczas konfigurowania BioBridge.
4. Kliknij przycisk **Dalej**, aż dotrzesz do strony **Ustawienia trybu wieloskładnikowego**.
5. W przypadku **trybu wieloskładnikowego** wybierz z listy opcję `Biometric only`.
6. Kliknij przycisk **Finish (Zakończ)**

Przypisz ten tryb uwierzytelniania do użytkowników

W systemie ACS każdemu docelowemu posiadaczowi karty należy przypisać prawidłowo zdefiniowaną kartę.

1. W aplikacji MorphoManager przejdź do menu **Administracja** > **Konfiguracja użytkownika**
2. W przypadku **trybu uwierzytelniania użytkownika** wybierz `Biometric(1:many)` z listy.
3. Kliknij przycisk **Zakończ**.

22.4 Konfiguracja BioBridge w MorphoManager

Wymagania wstępne

MorphoManager jest instalowany na serwerze MorphoManager w Twojej sieci. Zapoznaj się z Podręcznikiem instalacji MorphoManager i jego pomocą online.

Przegląd

Do korzystania z interfejsu BioBridge pomiędzy systemami kontroli dostępu firmy Bosch a Morphomanager konieczne jest skonfigurowanie następujących elementów w aplikacji MorphoManager:

- **Konfiguracja urządzeń biometrycznych**
- **Urządzenie biometryczne**
- **Profile Wiegand**
- **Konfiguracja użytkownika**
- **Grupa dystrybucji użytkownika**
- **Tryb uwierzytelniania użytkowników**
- **Konfiguracja systemu**

Trzeba także skonfigurować Open Database Connectivity (ODBC) do komunikacji pomiędzy Morphomanager BioBridge a bazą danych, z której korzysta wspólnie z systemem ACS. Wszystkie te zadania konfiguracyjne zostały opisane w poniższych sekcjach.

22.4.1 Konfiguracja urządzeń biometrycznych

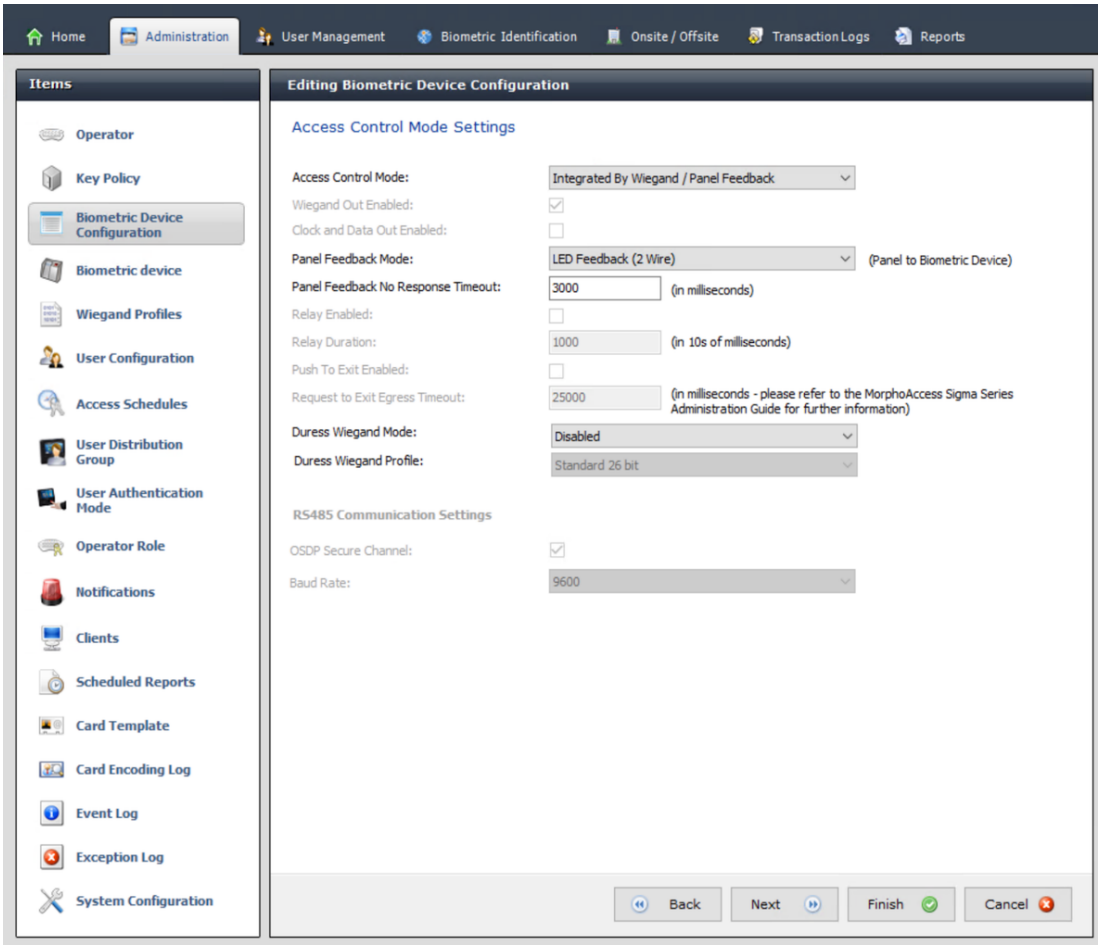
Konfiguracja urządzeń biometrycznych definiuje wspólne ustawienia i parametry dla jednego lub kilku urządzeń biometrycznych. W przypadku późniejszego dodawania urządzeń biometrycznych do systemu w sekcji **Urządzenie biometryczne** menu **Administracja**, zostanie do nich zastosowana konfiguracja urządzeń biometrycznych.
Poniższa procedura zakłada wdrożenie czytników biometrycznych firmy IDEMIA z dodatkową technologią odczytu kart.

Procedura:

1. W aplikacji MorphoManager przejdź do menu **Administracja** > **Konfiguracja urządzeń biometrycznych**.
2. Kliknij przycisk **Dodaj**, aby utworzyć nową konfigurację urządzeń biometrycznych.
3. Na następnym ekranie wprowadź nazwę profilu i opis (opcjonalnie). Jeśli nie korzystasz z pola Opis, zalecamy wybranie nazwy opisującej typ oraz tryby identyfikacyjne (biometria i/lub karta) grupy czytników.
4. Klikaj **Dalej**, aż przejdziesz do sekcji **Ustawienia urządzenia biometrycznego**

– Wybierz profil Wiegand utworzony wcześniej dla instalacji.

5. Klikaj **Dalej**, aż przejdziesz do strony **Ustawienia trybu kontroli dostępu**.



Na tym etapie procedury dla kontrolerów AMC Wiegand i OSDP różnią się. Postępuj według procedury poniżej odpowiadającej typowi kontrolera AMC:

Kontrolery Wiegand

1. Ustaw **Tryb kontroli dostępu** jako `Integrated by Wiegand`
2. Ustaw **Tryb informacji zwrotnych panelu** jako `LED Feedback (2 wire)`
3. Kliknij przycisk **Finish (Zakończ)**

Kontrolery OSDP

1. Ustaw **Tryb kontroli dostępu** jako `Integrated by OSDP`
2. Ustaw **Tryb informacji zwrotnych panelu** jako `LED Feedback (2 wire)`
3. Zaznacz pole wyboru **Bezpieczny kanał OSDP**
4. Ustaw szybkość transmisji `9600`
5. Więcej informacji można znaleźć w podrozdziale **Urządzenie biometryczne**
6. Kliknij przycisk **Zakończ**, aby zamknąć program MorphoManager.

Rozwiązywanie problemów z kluczami protokołu OSDP

Jeśli nie można ustanowić bezpiecznego połączenia z czytnikiem OSDP, spróbuj zresetować klucz podstawowy w następujący sposób:

1. Uruchom osobny program **MorphoBioToolBox (MBTB)**
2. W programie MorphoBioToolBox wybierz kolejno opcje **Ustawienia urządzenia** > **Resetuj**

3. Zaznacz klucz podstawowy protokołu OSDP
4. Kliknij przycisk **Resetuj klucze kryptograficzne**
5. Zamknij program MorphoBioToolBox

W bardziej złożonych przypadkach skontaktuj się z pomocą techniczną IDEMIA.

Patrz

– *Urządzenie biometryczne, Strona 170*

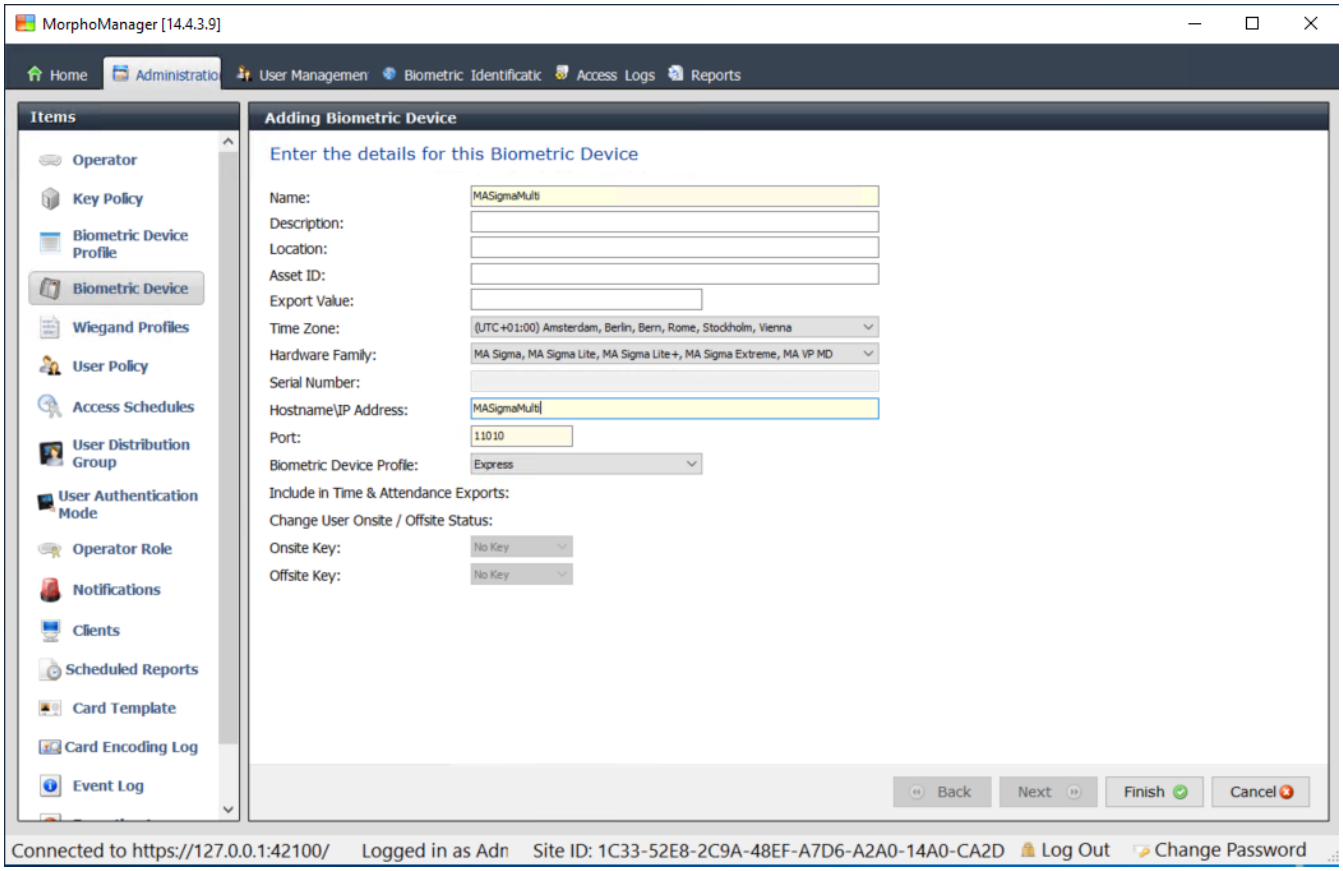
22.4.2 Urządzenie biometryczne

Urządzenia biometryczne sprawdzają, czy odczytywane przez nie poświadczenia biometryczne są zgodne z zapisami w bazie danych. Ponadto przechowują one dzienniki wszystkich przypadków użycia.

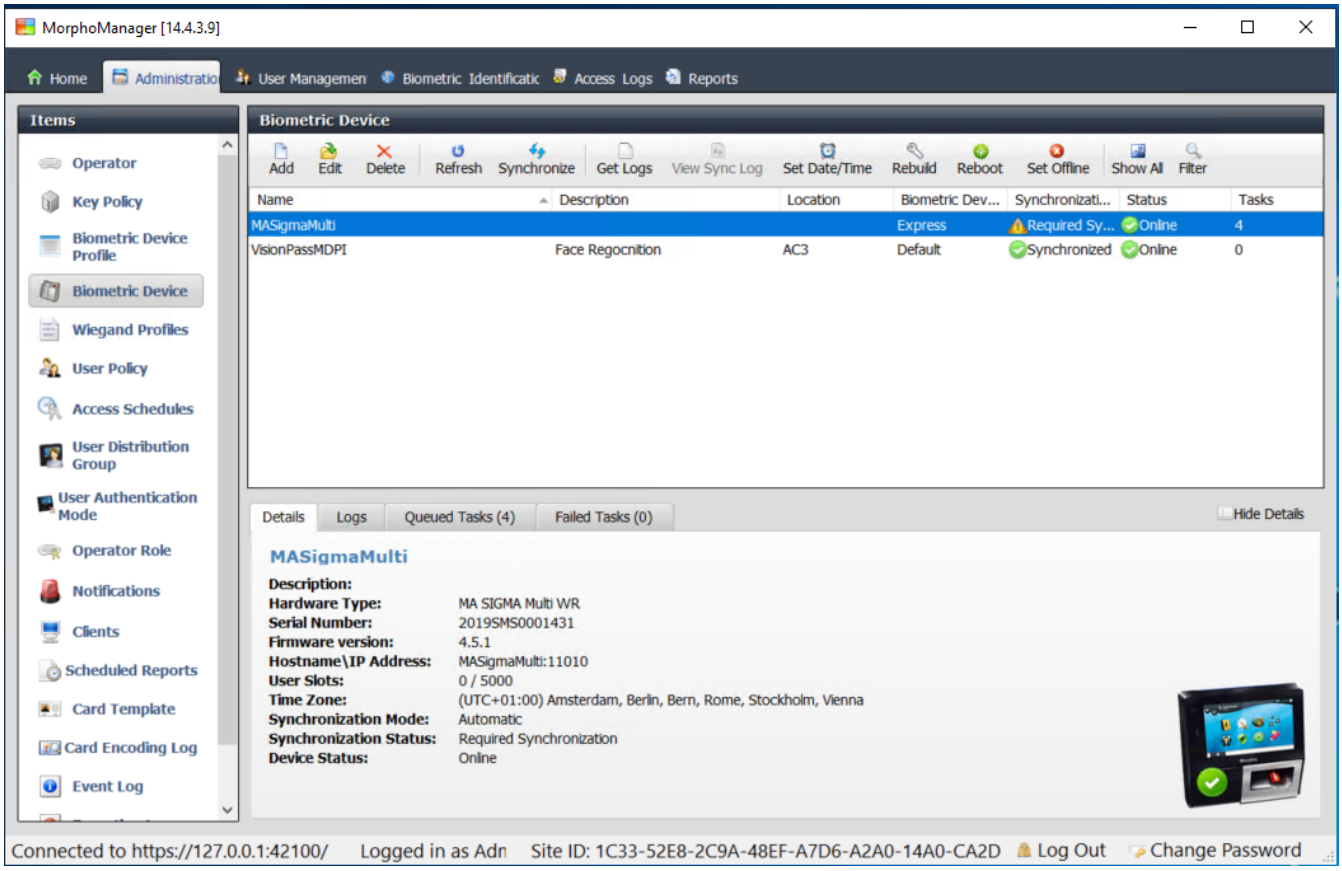
Procedura:

1. W aplikacji MorphoManager przejdź do menu **Administracja** > **Urządzenie biometryczne**.
2. Kliknij przycisk **Dodaj**, aby utworzyć nowe urządzenie biometryczne.
3. Wprowadź co najmniej podstawowe informacje o urządzeniu:

– (z listy) **Rodzina urządzeń**
– **Nazwa hosta / adres IP**
– (z listy) **Konfiguracja urządzeń biometrycznych** zdefiniowany wcześniej



4. Kliknij przycisk **Zakończ**
   W oknie dialogowym Urządzenie biometryczne znajduje się teraz lista urządzeń, które zostały już skonfigurowane:

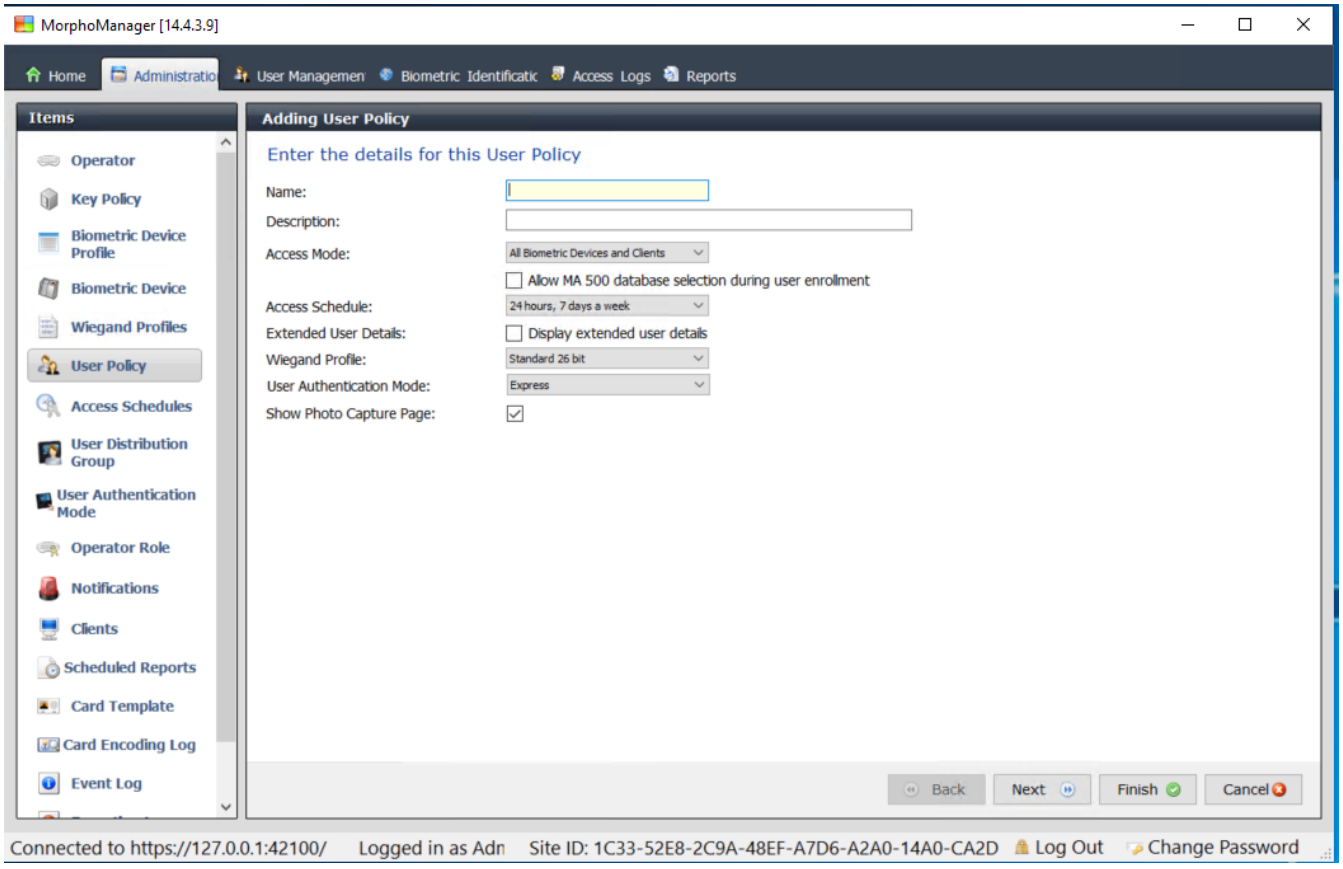


22.4.3 Konfiguracja użytkownika

Konfiguracje użytkowników to pakiety uprawnień dostępu przypisywane użytkownikom o tych samych wymaganiach dotyczących dostępu, tzn. które urządzenia biometryczne mogą być używane w jakich trybach i w jakim czasie.

Procedura:

1. W aplikacji MorphoManager przejdź do menu **Administracja** > **Konfiguracja użytkownika**
2. Kliknij przycisk **Dodaj** w celu utworzenia nowej konfiguracji użytkownika.



3. W okienku dialogowym **Dodawanie zasad dotyczących użytkownika** wprowadź następujące informacje:

- **Nazwa** Zasad dotyczących użytkownika i (opcjonalnie) opis
- **Tryb dostępu** `Per User`
- **Harmonogram dostępu**, który określa dni i godziny, w których dostęp jest dozwolony
- **Profil Wiegand** określony i używany na potrzeby **Profilu urządzenia biometrycznego**.
- **Tryb uwierzytelniania użytkownika**, który zależy od tego, jak użytkownicy będą korzystali z urządzeń (na podstawie odcisków palca, palca, twarzy, kart itp.). Szczegółowe informacje można znaleźć w podrozdziale **Wybór trybu identyfikacji**.

4. Kliknij przycisk **Finish (Zakończ)**

Domyślne Zasady dotyczące użytkownika będą miały Tryb uwierzytelniania użytkownika `(1: Many)`. Aby korzystać z innych trybów uwierzytelniania, trzeba utworzyć dodatkowe Zasady dotyczące użytkownika. Więcej informacji na temat różnych właściwości, które można przypisywać do Zasad dotyczących użytkownika, można znaleźć w instrukcji obsługi aplikacji MorphoManager.

Patrz

– *Wybór trybu identyfikacji, Strona 164*

22.4.4 Grupy dystrybucji użytkownika

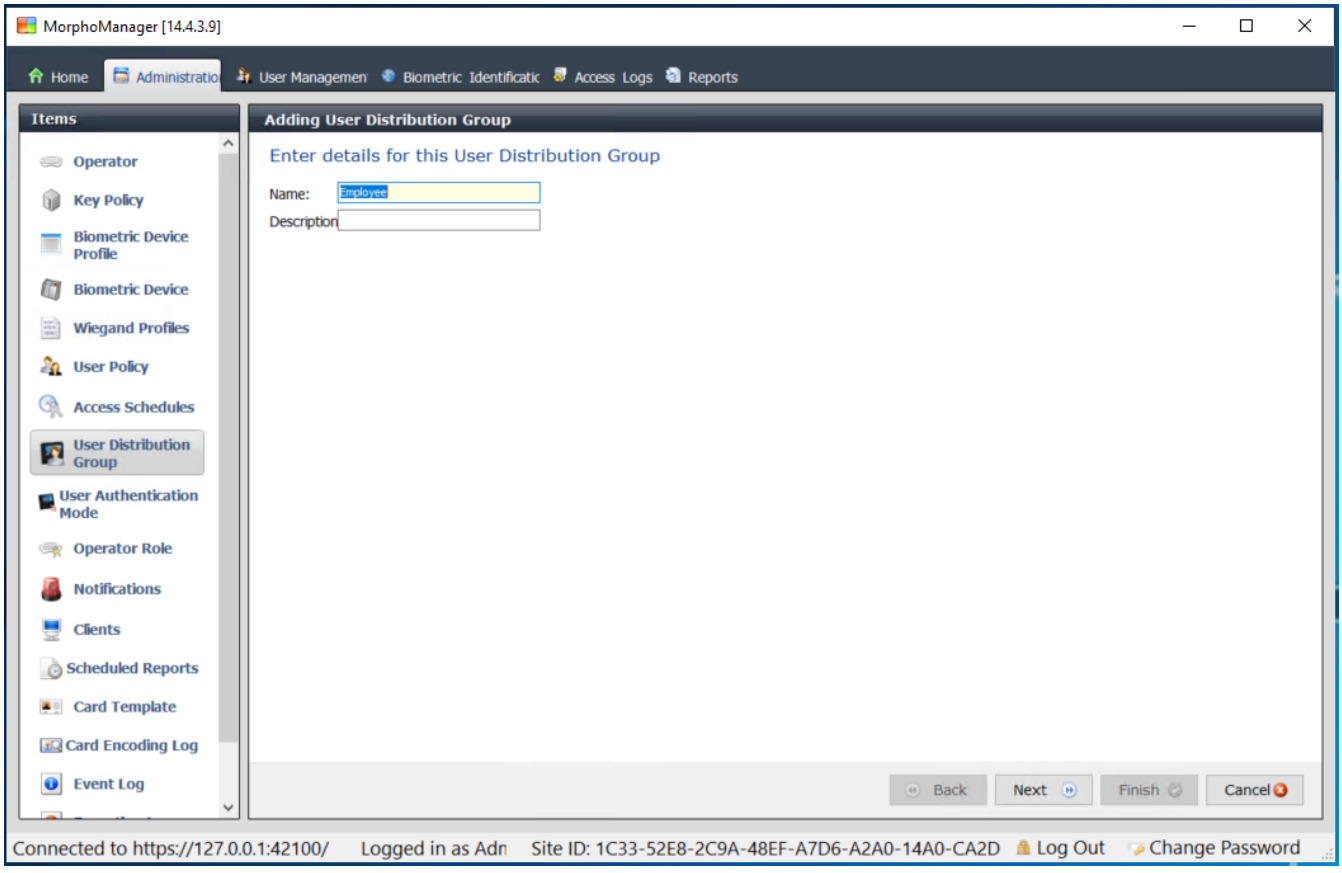
Grupy dystrybucji użytkownika mapują użytkowników do grup czytników biometrycznych lub klientów aplikacji MorphoManager.

Wymagania wstępne:

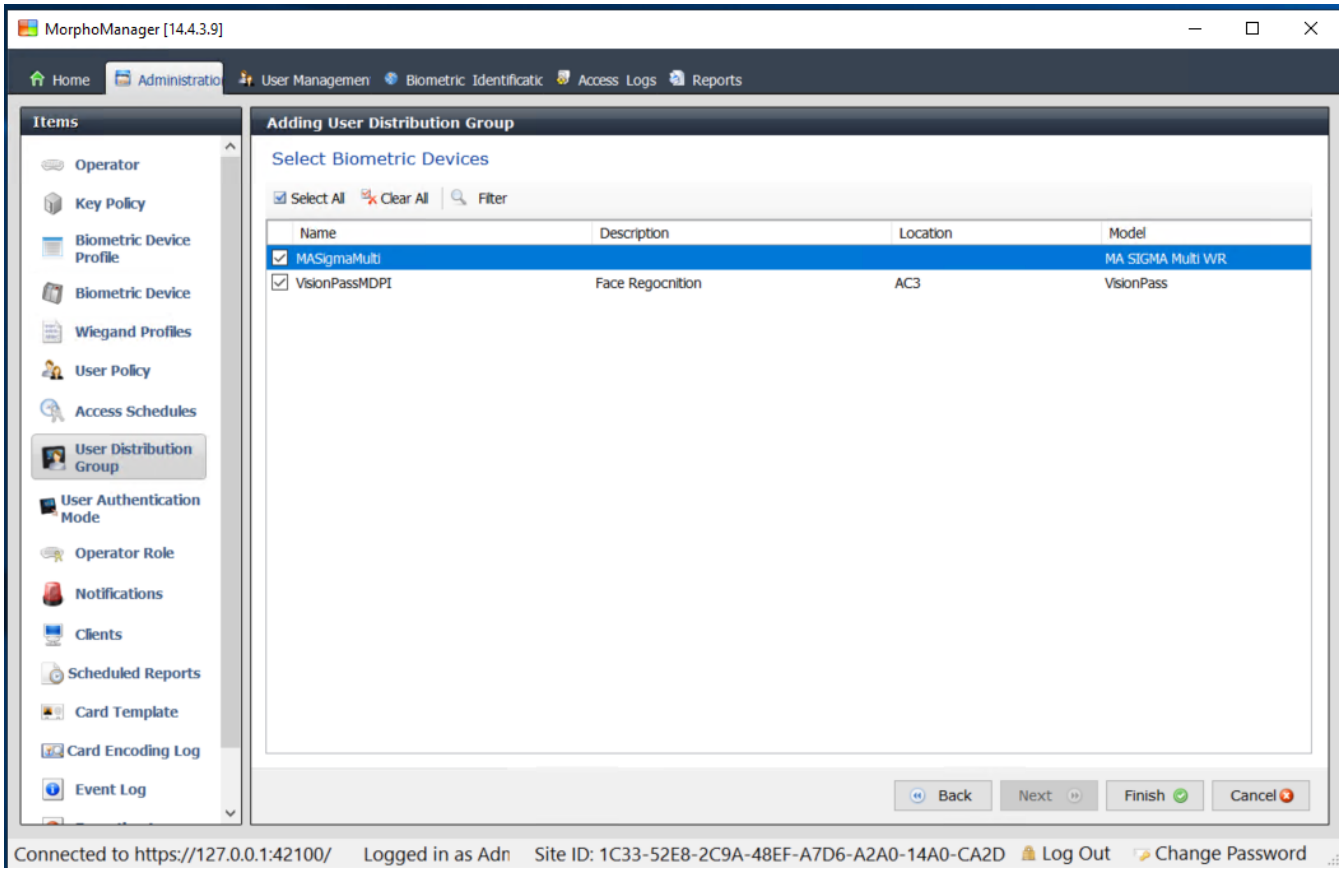
Każda Grupa dystrybucji użytkownika musi być zmapowana do co najmniej jednej Klasy osób w systemie ACS. W związku z tym konieczne jest utworzenie co najmniej jednej Grupy dystrybucji użytkownika dla każdej używanej Klasy osób.

Procedura:

1. W aplikacji MorphoManager przejdź do menu **Administracja** > **Grupa dystrybucji użytkownika**.
2. Kliknij przycisk **Dodaj**, aby utworzyć nową Grupę dystrybucji użytkownika.



3. Klikaj **Dalej**, aż przejdziesz do strony **Wybierz urządzenia biometryczne**.
4. Zaznacz pola wyboru tych urządzeń biometrycznych, z których będą korzystać osoby należące do Grupy dystrybucji użytkownika.



5. Kliknij przycisk **Finish (Zakończ)**

22.4.5 Konfigurowanie ODBC dla BioBridge

Wstęp

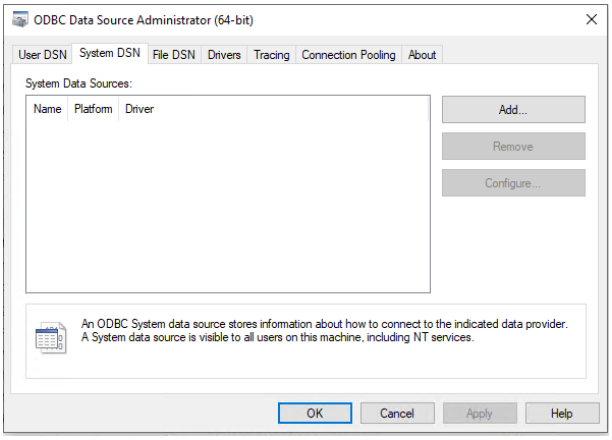
Korzystanie z funkcji BioBridge aplikacji MorphoManager wymaga ODBC. ODBC to standardowy interfejs programistyczny umożliwiający dostęp do różnych baz danych. Zalecany sterownik to `OdbCDriver17SQLServer`

- Dla systemu BIS sterownik znajduje się na jego nośniku instalacyjnym w ścieżce `BIS\3rd_Party\OdbCDriver17SQLServer`
- Dla systemu AMS sterownik należy pobrać z witryny `www.microsoft.com`

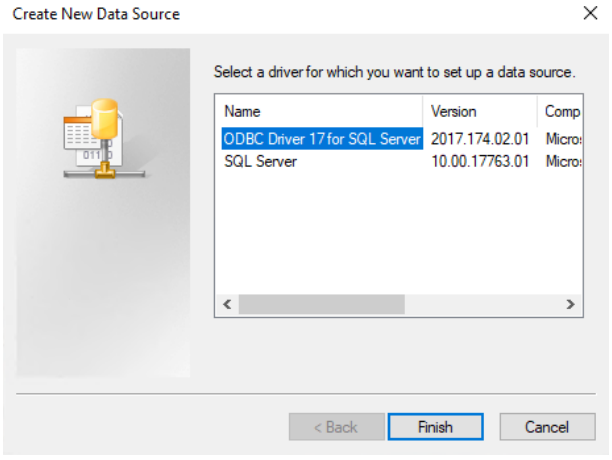
Tworzenie źródła danych

Tworzenie nazwy źródła danych (DSN) dla ODBC

1. W panelu sterowania systemu Windows wybierz opcję **Narzędzia administracyjne**.
2. Wybierz `ODBC Data Sources (64-bit)` z listy.
3. Wybierz kartę **System DSN**.

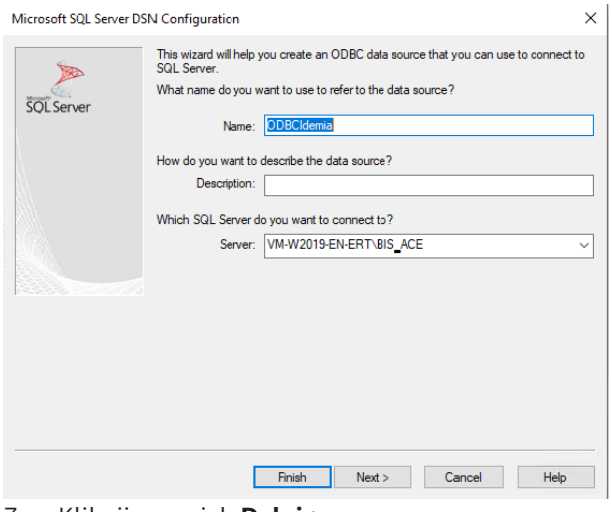


4. Aby wybrać sterownik, kliknij przycisk **Dodaj**.
5. Wybierz `ODBC Driver 17 for SQL Server` jako sterownik i kliknij przycisk **Zakończ**.

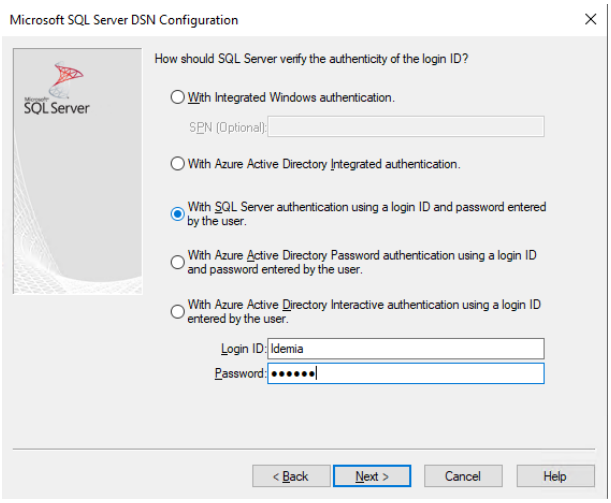


6. Wprowadź następujące informacje o źródle danych.

– **Nazwa**: nazwa źródła danych
– **Opis** (opcjonalnie)
– **Serwer**: nazwa komputera, na którym jest zainstalowana baza danych ACE, a także nazwa bazy danych (domyślna: <MyACS server>\`ACE`)



7. Kliknij przycisk **Dalej >**
   zostanie wyświetlone okno dialogowe dotyczące gromadzenia informacji o logowaniu



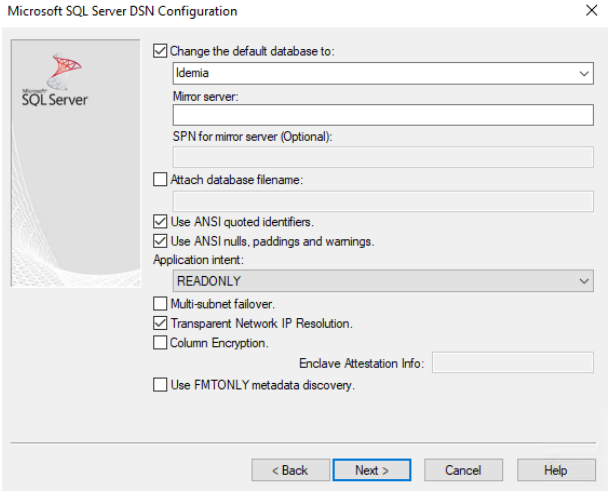
8. Wybierz opcję **Za pomocą uwierzytelniania serwera SQL z użyciem identyfikator logowania...**
9. Wprowadź następujące informacje:

– **Identyfikator logowania**: nazwa użytkownika bazy danych Idemia skonfigurowana w systemie ACS. Jest to zawsze wartość `Idemia`.
– **Hasło**: hasło ustawione dla użytkownika bazy danych Idemia, skonfigurowane w systemie ACS.

10. Kliknij przycisk **Next (Dalej)**.
11. W kolejnych oknach dialogowych zaznacz pola wyboru:

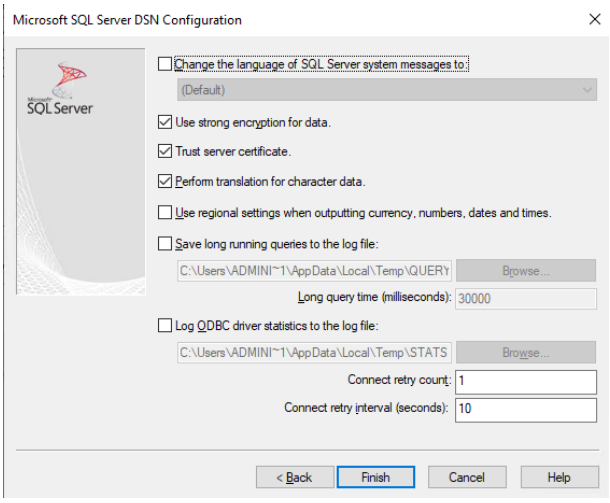
– **Zmień domyślną bazę danych na:** i wybierz `Idemia`
– **Użyj identyfikatorów cytowanych w ANSI**
– **Użyj wartości null, uzupełnień i ostrzeżeń z ANSI**
– **Transparent Network IP Resolution**

12. Ustaw **Cel zastosowania** jako `READONLY`

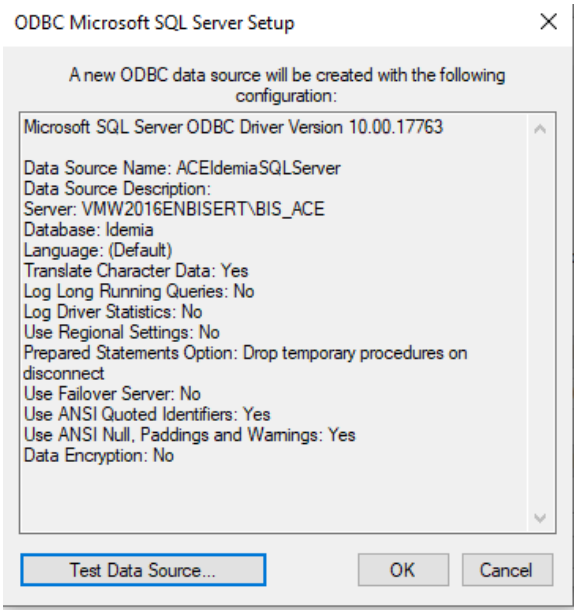


13. Kliknij przycisk **Next (Dalej)**.
14. W kolejnych oknach dialogowych zaznacz pola wyboru

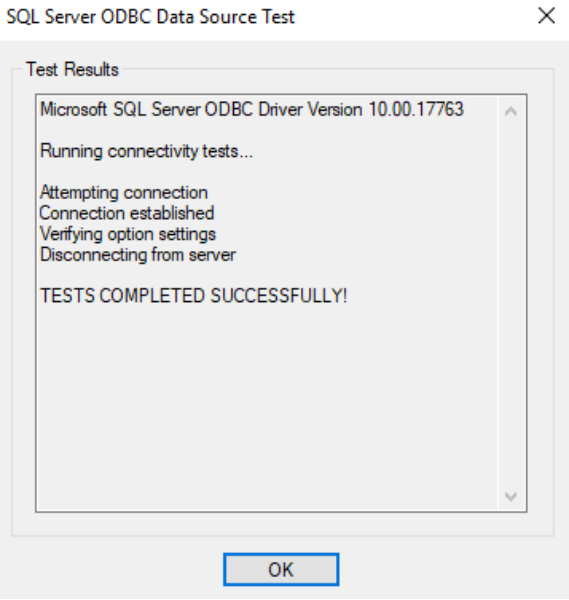
– **Używaj silnego szyfrowania danych**
– **Tłumacz dane znaków**
– **Certyfikat zaufanego serwera**



15. Kliknij przycisk **Finish (Zakończ)**
16. W następnym oknie dialogowym przejrzyj dane podsumowania



17. Kliknij przycisk **Testuj źródło danych...** i upewnij się, że testy zakończyły się pomyślnie



18. Zapisz wszystkie zmiany i zamknij kreatora konfiguracji ODBC.

22.4.6 Konfiguracja systemu BioBridge

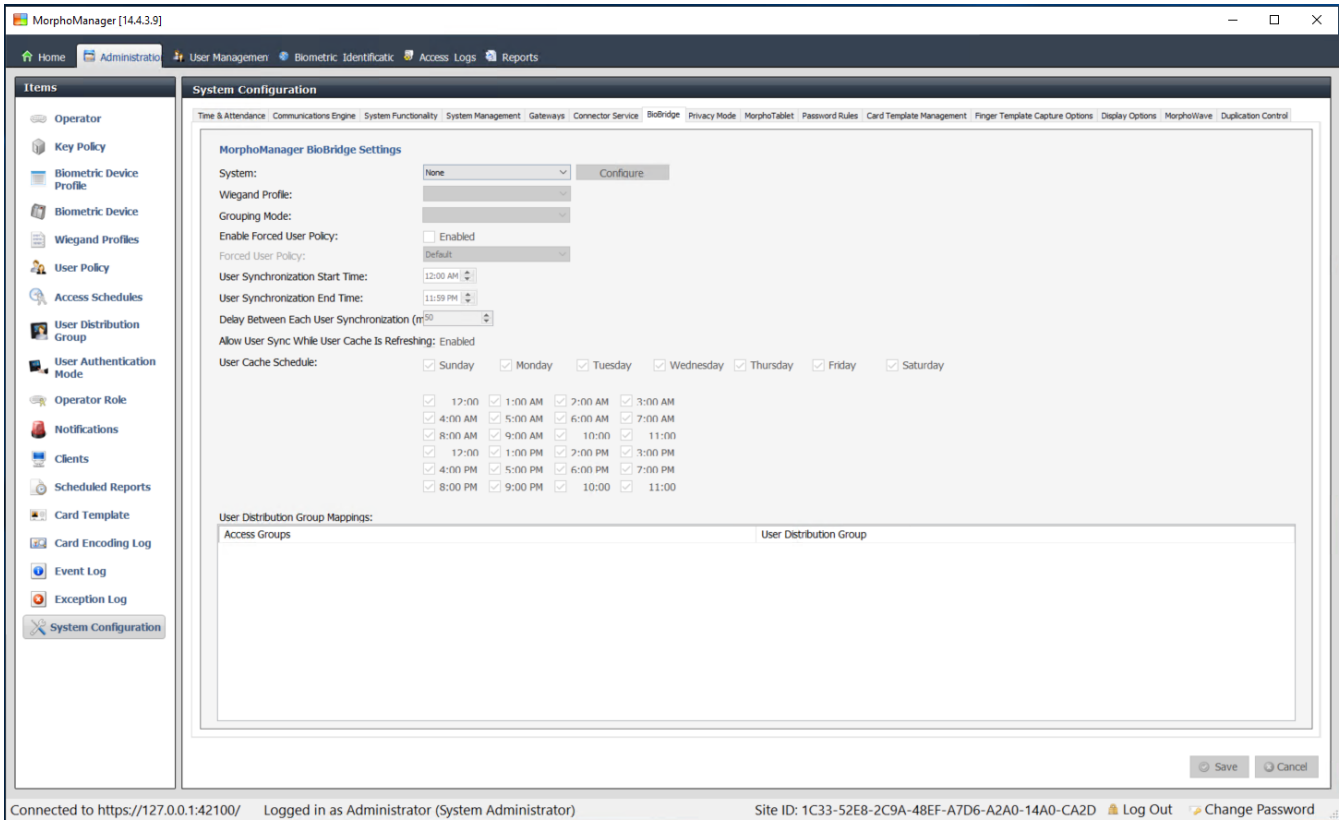
W tej sekcji opisano pozostałe ustawienia niezbędne do korzystania z interfejsu BioBridge w systemach kontroli dostępu.

Wymaganie wstępne

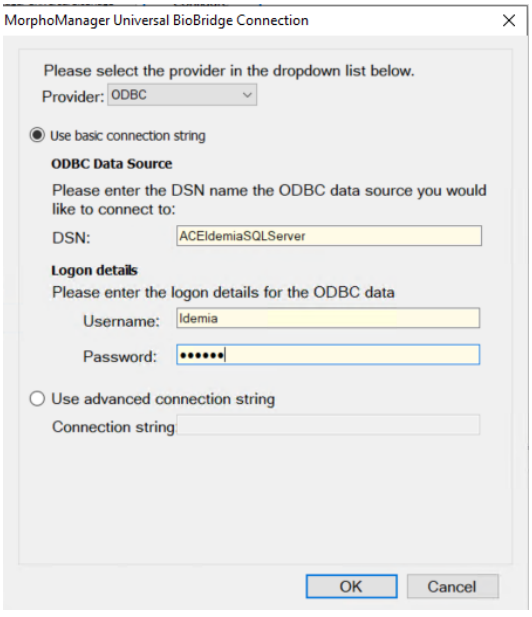
Skonfigurowano ODBC dla interfejsu BioBridge. Patrz *Konfigurowanie ODBC dla BioBridge, Strona 174*.

Procedura:

1. W aplikacji MorphoManager przejdź do menu **Administracja** > **Konfiguracja systemu**.
2. Wybierz kartę **BioBridge**



3. Na liście rozwijanej **System** wybierz `MorphoManager Universal BioBridge`
4. Kliknij przycisk **Konfiguruj**
   Zostanie wyświetlone wyskakujące okienko.



W oknie wyskakującym

1. Na liście rozwijanej **Dostawca** wybierz `ODBC`
2. Wprowadź nazwę DSN (nazwę źródła danych) z konfiguracji ODBC.
3. W obszarze **Szczegóły logowania** wprowadź nazwę użytkownika (`Idemia`) i hasło zgodnie z konfiguracją ODBC.
4. Kliknij przycisk **OK**, aby wrócić do okna dialogowego **Konfiguracja systemu**.

W oknie dialogowym **Konfiguracja systemu**

1. W przypadku **profilu Wiegand**: wybierz z listy określony wcześniej profil Wiegand.

Tryb grupowania:
To ustawienie określa, w jaki sposób aplikacja MorphoManager powinna mapować użytkowników MM Universal BioBridge do Grupy dystrybucji użytkownika w MorphoManager. Wybierz jedną z następujących opcji:

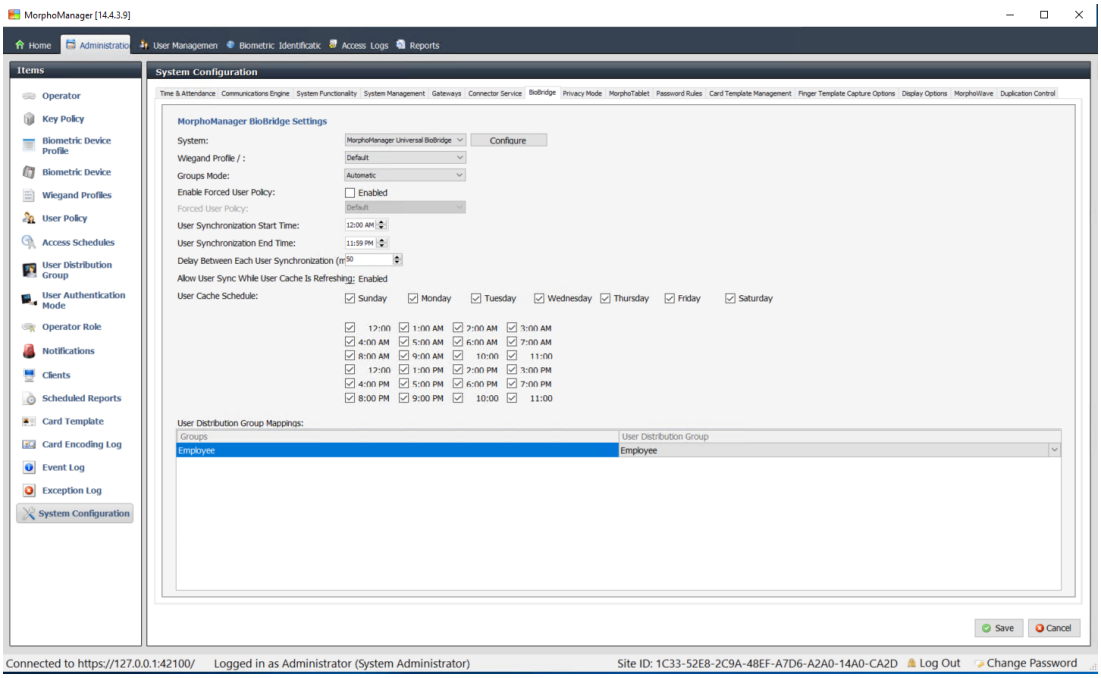
- **Automatycznie**: ten tryb automatycznie dopasowuje **Grupy poziomów dostępu**z MM Universal BioBridge do **Grupy dystrybucji użytkownika aplikacji MorphoManager**, jeżeli posiada taką samą konwencję nazewnictwa.
- **Ręcznie**: Jeśli **Grupy poziom dostępu** MM Universal BioBridge i **Grupy dystrybucji użytkownika** w aplikacji MorphoManager nie są identyczne, można ręcznie dokonać przypisania w ramach **mapowań zasad dotyczących użytkownika**.

Inne ustawienia
W większości przypadków można zachować wartości domyślne następujących ustawień:

Włącz wymuszone zasady dotyczące użytkownika	Zaznaczenie tej opcji spowoduje, że wszyscy użytkownicy zarejestrowani w BioBridge otrzymają zasady dotyczące użytkownika wybrane z listy obok. Jeśli zaznaczysz to pole wyboru, zawsze używaj Zasad dotyczących użytkownika o nazwie `Per User`
Godzina rozpoczęcia i zakończenia synchronizacji użytkownika	Program do synchronizacji użytkowników będzie mógł działać tylko w tych godzinach.
Opóźnienie między synchronizacją poszczególnych użytkowników	Odstęp między synchronizacjami użytkowników. Zwiększenie opóźnienia umożliwia oszczędzanie zasobów systemowych, ale wydłuża czas aktualizowania wszystkich użytkowników.
Zezwalaj na synchronizację użytkowników podczas odświeżania pamięci podręcznej użytkownika	Gdy funkcja ta jest włączona, moduł synchronizacji użytkowników jest uruchamiany jednocześnie z odświeżaniem pamięci podręcznej użytkownika. Jest to bardzo obciążające dla zasobów systemowych. Zaleca się wyłączenie tego ustawienia w przypadku korzystania z dużych baz danych.
Harmonogram odświeżania pamięci podręcznej użytkownika	Dni i godziny, w których można odświeżać pamięć podręczną użytkownika. W celu uzyskania najwyższej dokładności funkcja ta powinna działać cały czas, ale ze względu na wydajność systemów z dużymi bazami danych konieczny jest kompromis.

Mapowania grup dystrybucji użytkownika

- W tabeli mapowania należy upewnić się, że wszystkie **Grupy** (**klasy osób** zdefiniowane w ACS) są zmapowane w **Grupach dystrybucji użytkownika** (w MorphoManager).



22.5 Konfigurowanie klienta rejestracji BioBridge

Wstęp

Klient rejestracji BioBridge to komputer, na którym można tworzyć rekordy biometryczne dla użytkowników systemu kontroli dostępu. Konfiguracja klienta rejestracji w BioBridge ma 3 części:

- Dodawanie operatora rejestracji do aplikacji MorphoManager
- Konfigurowanie komputerów klienckich MorphoManager pod kątem rejestrowania
- Testowanie klienta rejestracji

Wymagania wstępne

MorphoManager BioBridge jest instalowany na każdej stacji roboczej ACE, z której wykonywane jest rejestrowanie biometryczne w systemach IDEMIA.

22.5.1 Dodawanie operatora rejestracji do aplikacji MorphoManager

Procedura

Postępuj zgodnie z instrukcjami zawartymi w instrukcji instalacji klienta MorphoManager.

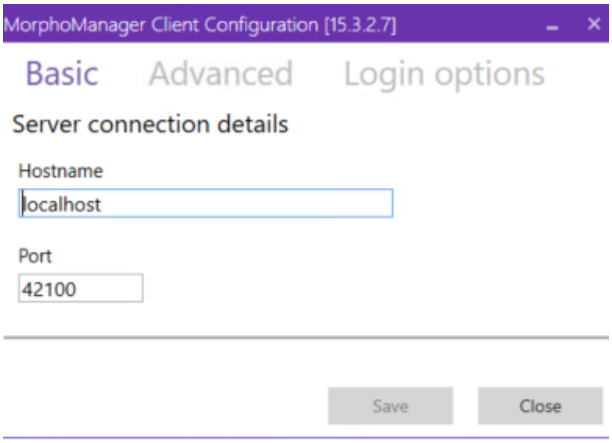
Uwaga: ze względów bezpieczeństwa zaleca się korzystanie z kont użytkowników usługi Active Directory.

22.5.2 Konfigurowanie komputerów klienckich MorphoManager pod kątem rejestrowania

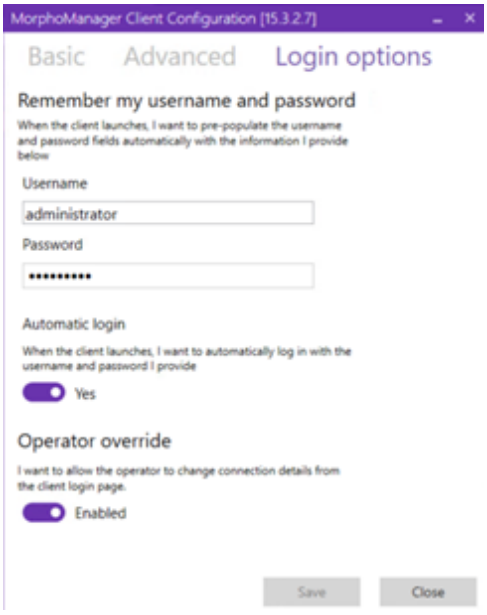
Tę procedurę należy wykonać na każdym komputerze, który ma być używany do rejestracji biometrycznej.

Procedura

1. W katalogu instalacyjnym aplikacji MorphoManager (domyślnie: `C:\Program,Files(x86)\Morpho\MorphoManager\Client\`) wykonaj plik `ID1.ECP4.MorphoManager.AdvancedClientConfig.exe` jako administrator

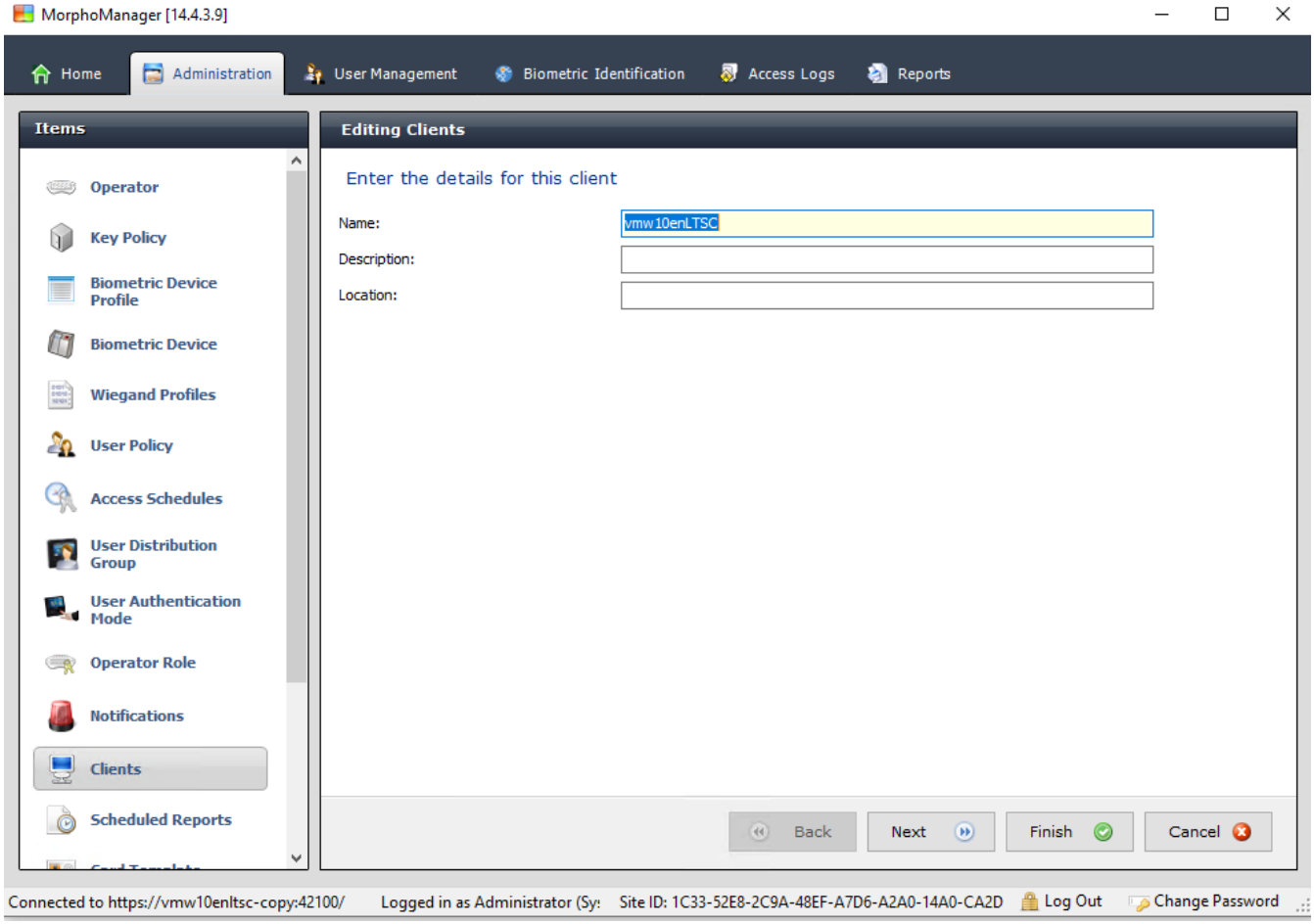


2. Na karcie **Podstawowe** wprowadź nazwę hosta serwera Morpho na karcie **Nazwa hosta**.
3. Aby uzyskać bezpieczną instalację, skorzystaj z usługi Active Directory albo podaj macierzyste nazwę użytkownika i hasło, jak opisano w dokumentacji oprogramowania Morpho.
4. Alternatywnie (rozwiązanie NIEZALECANE w instalacjach, które muszą być bardzo bezpieczne) na karcie **Opcje logowania**

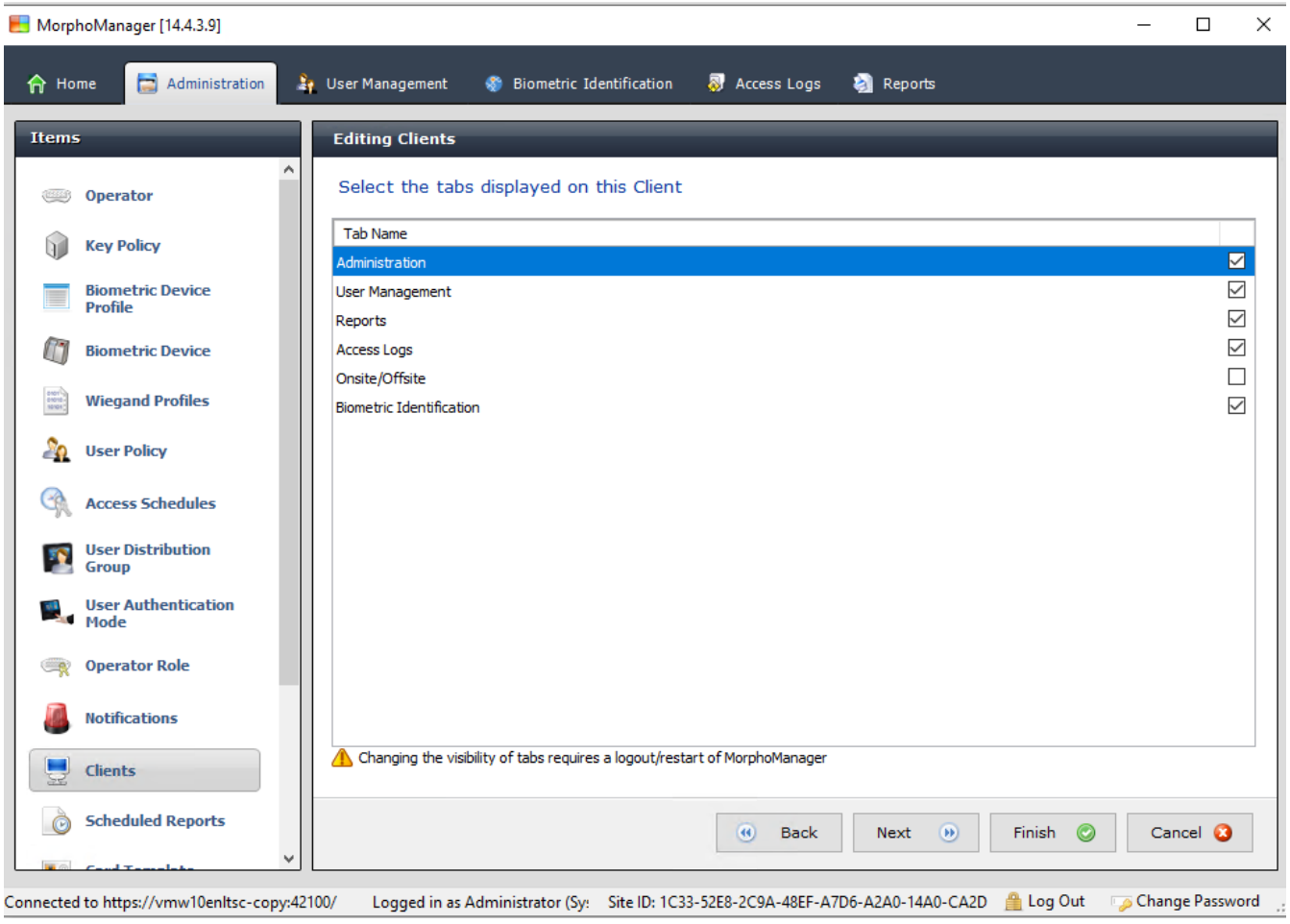


– Wprowadź nazwę użytkownika i hasło wprowadzone przez operatora rejestracji w poprzedniej sekcji
– W przełączniku **Automatyczne logowanie** ustaw wartość `Yes`

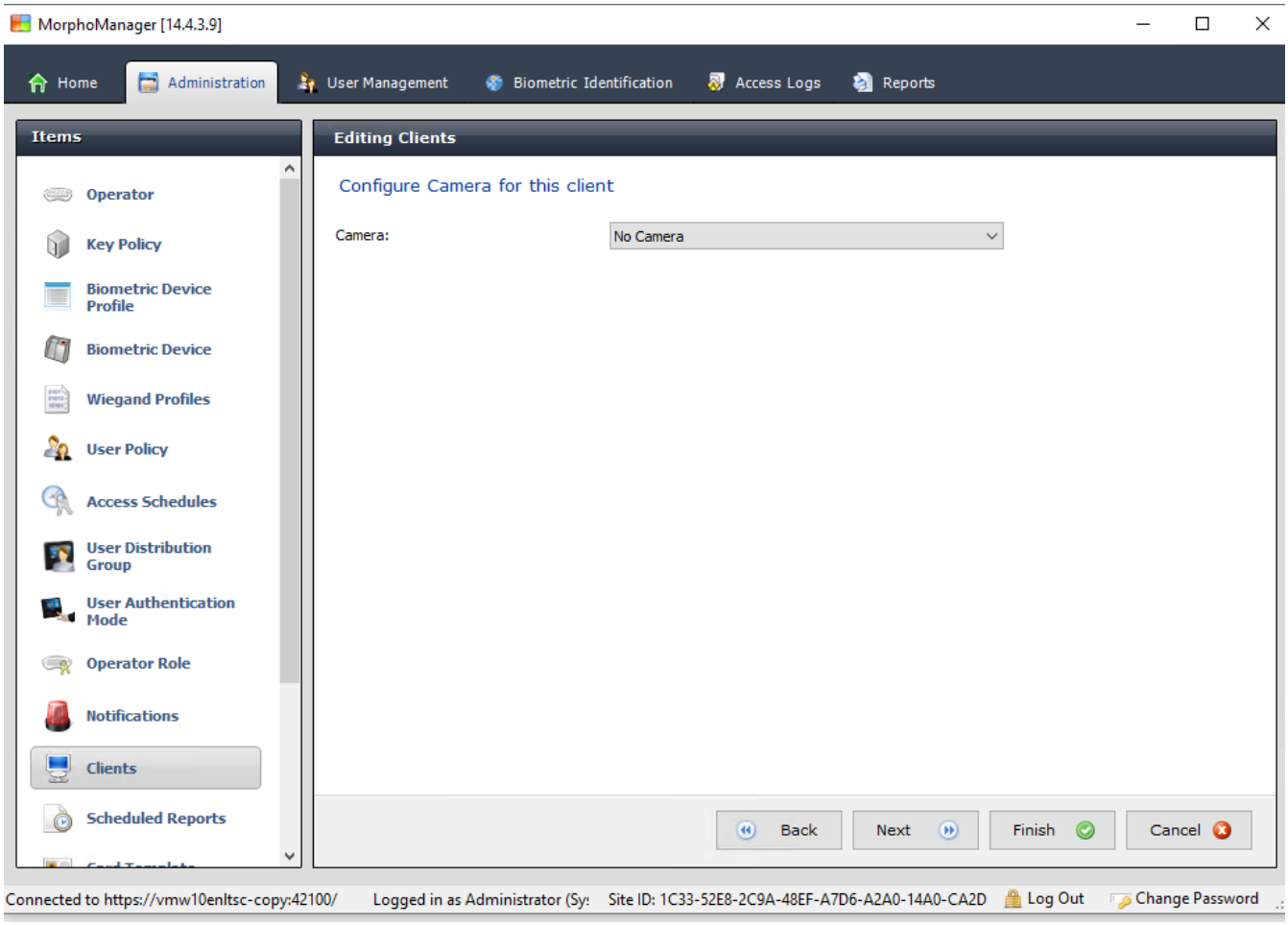
1. W katalogu instalacyjnym aplikacji MorphoManager (domyślnie: `C:\Program Files(x86)\Morpho\MorphoManager\Client\`) wykonaj plik `Start ID1.ECP4.MorphoManager.Client.exe` jako administrator
2. Przejdź do menu **Administracja** > **Klienci**
3. Wybierz komputer kliencki
4. Kliknij przycisk **Edytuj**



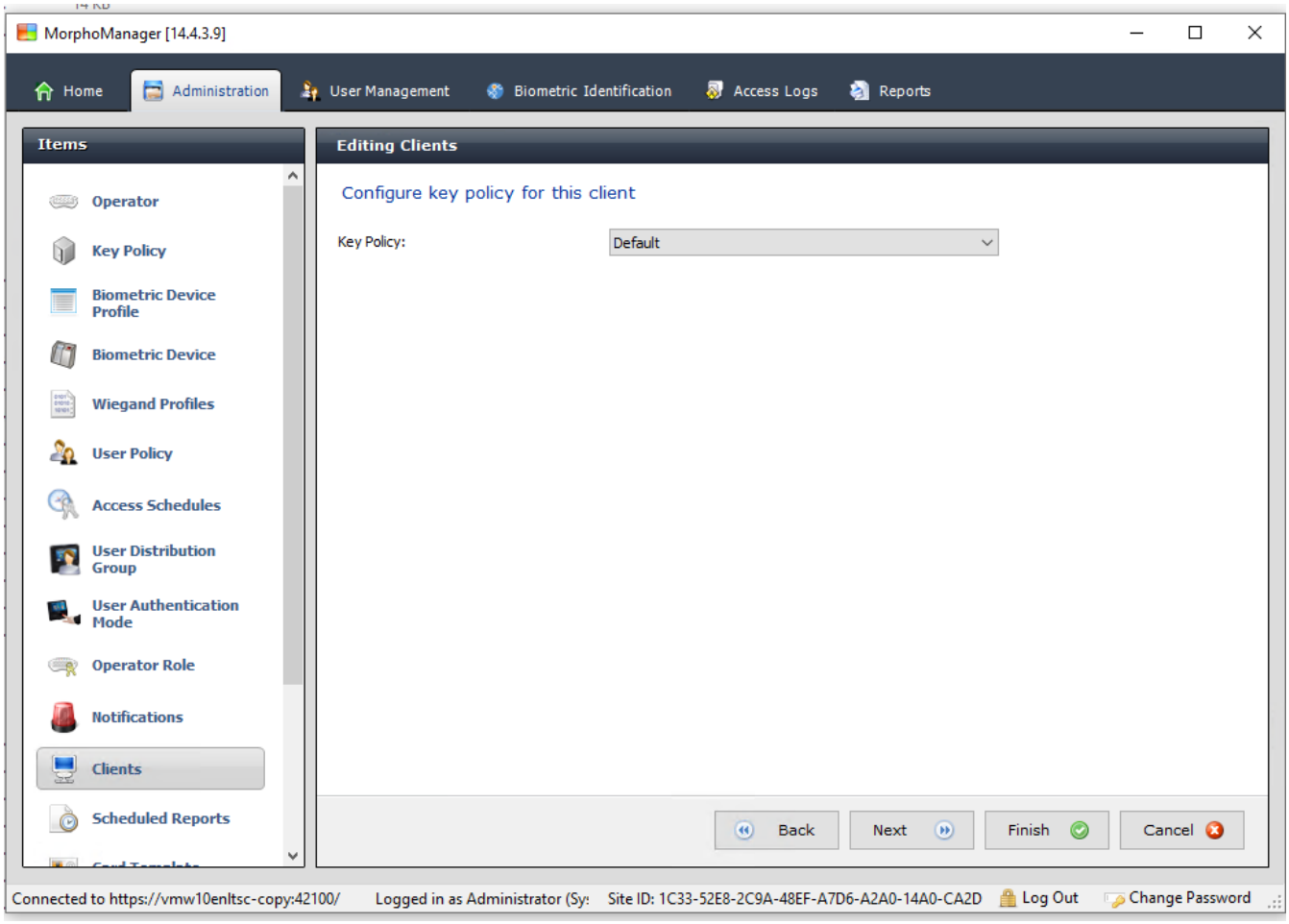
5. Wprowadź nazwę żądanego klienta rejestracji (opcjonalnie można też podać opis i lokalizację)
6. Kliknij przycisk **Dalej>**.



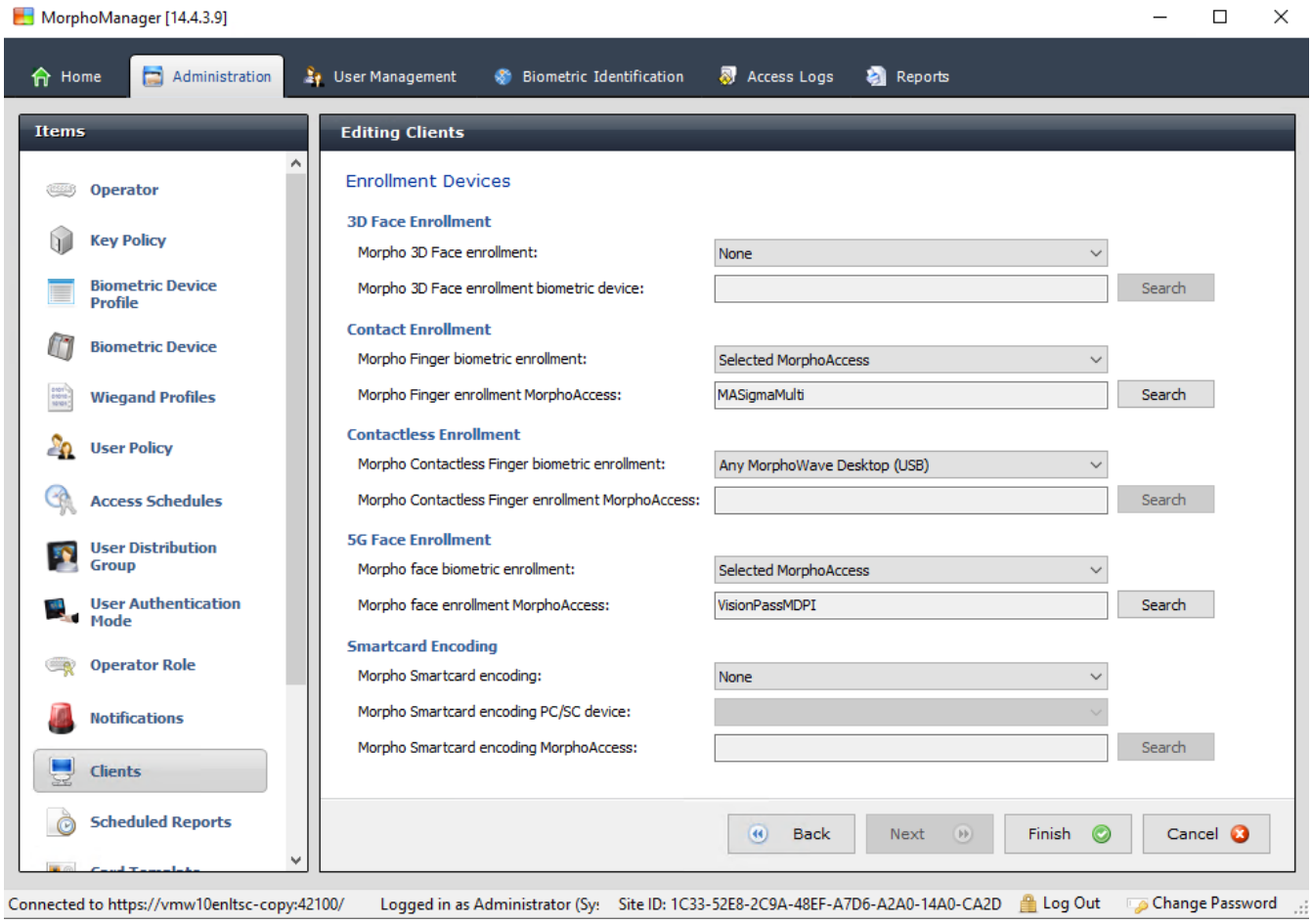
7. Zaznacz pola wyboru kart, które chcesz wyświetlić na komputerze klienckim rejestracji:
   - **Administracja,**
   - **Zarządzanie użytkownikami,**
   - **Raporty,**
   - **Dzienniki dostępu,**
   - **Identyfikacja biometryczna**
8. Kliknij przycisk **Dalej>**.



9. W przypadku **Kamery:** wybierz na liście `No camera`
10. Kliknij przycisk **Dalej>**.



11. W przypadku **Zasady dotyczące kluczy** wybierz na liście `Default`
12. Kliknij przycisk **Dalej>**.



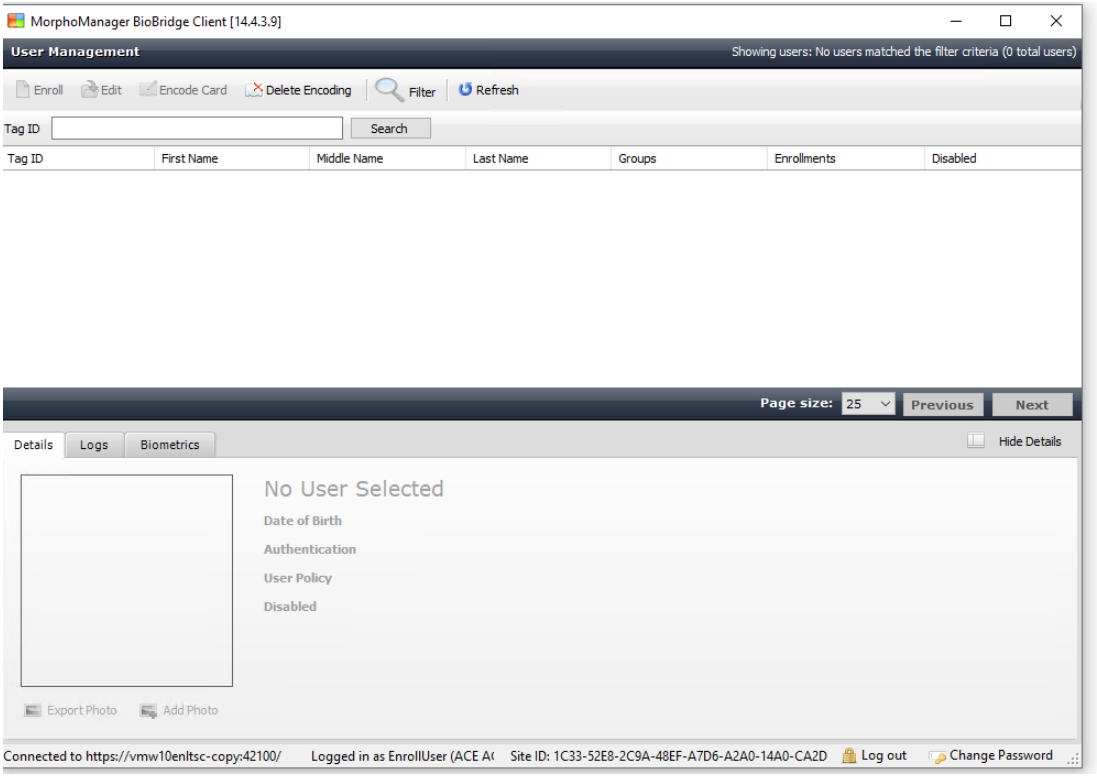
13. Wybierz czytnik rejestracji biometrycznej, który ma być używany na stacji roboczej rejestracji
14. Kliknij przycisk **Finish (Zakończ)**
15. Zamknij aplikację MorphoManager

Patrz

– *Konfigurowanie klienta rejestracji BioBridge, Strona 181*

22.5.3 Testowanie klienta rejestracji

1. W katalogu instalacyjnym aplikacji MorphoManager (domyślnie: `C:\Program,Files(x86)\Morpho\MorphoManager\Client\`) wykonaj plik`ID1.ECP4.MorphoManager.BioBridgeEnrollmentClient.exe`



1. Upewnij się, że możesz wywołać ekran rejestracji bez konieczności wprowadzania nazwy użytkownika i hasła operatora rejestracji.

22.6 Uwagi techniczne i ograniczenia

Oficjalnie obsługiwane systemy operacyjne Windows
IDEMIA obsługuje te same wersje systemu Windows 10, co system ACS firmy Bosch.

Oficjalnie obsługiwana wersja Microsoft SQL Server
Obsługiwana wersja to SQL Server 2017

Jeden system IDEMIA na jeden system dostępowy
System kontroli dostępu firmy Bosch może obsługiwać tylko jeden system IDEMIA.

Jedna karta IDEMIA na jednego posiadacza karty.
Systemy kontroli dostępu firmy Bosch obsługują wiele kart na jednego posiadacza karty, natomiast IDEMIA obsługuje tylko jedną. Dlatego przy zapisie i synchronizacji z BIS pierwsza ważna karta (czyli taka, której status=1) typu „Dostęp”, „Tymczasowy” lub „Parking” jest przypisywana do IDEMII. Jeśli karta zostanie później zablokowana, jej numer jest nadal przesyłany i zapisywany w rejestrze zdarzeń.

Maksymalna liczba posiadaczy kart IDEMIA
BioBridge MorphoManager może obsłużyć do 100 000 posiadaczy kart.

Maksymalna liczba grup dostępu
IDEMIA obsługuje do 5000 grup dostępu (grup dystrybucji użytkowników). Są one mapowane na **klasy osób** w systemie kontroli dostępu firmy Bosch.

Wydajność pobierania szablonów
– 1000 szablonów do 1 urządzenia: pobieranie trwa poniżej 1 minuty.
– 1000 szablonów do 100 urządzeń: pobieranie trwa kilka minut.

IDEMIA nie obsługuje stref
Jeśli system IDEMIA jest zintegrowany, system ACS nie jest w stanie w sposób wiarygodny oddzielić posiadaczy kart z jednej Strefy od operatorów systemu kontroli dostępu z innej Strefy. Jeśli wymagane jest bezwzględne zachowanie prywatności między strefami, nie należy integrować systemu IDEMIA.

Karty wirtualne / dostęp tylko po wprowadzeniu kodu PIN.
IDEMIA nie zapewnia dostępu wyłącznie za pomocą kodu PIN. Wymagana jest karta fizyczna.

Funkcja odcisku palca pod przymusem w systemie IDEMIA
Funkcja odcisku palca pod przymusem w systemie IDEMIA nie jest obecnie obsługiwana przez kontrolery AMC.

Minimalny zestaw kryteriów identyfikacji.
Rejestracja w systemie IDEMIA wymaga co najmniej następujących kryteriów identyfikacji:
– Imię,
– Nazwisko,
– Klasa osób
– Jedna karta fizyczna przypisana do posiadacza karty.

Stany wyświetlane na czytnikach
Na czytnikach Wiegand i OSDP nie są wyświetlane żadne stany czytnika (np. „Urządzenie zablokowane”).

Tworzenie kopii zapasowych i ich przywracanie
Przed przywróceniem kopii zapasowej za pomocą systemu IDEMIA, należy usunąć, a następnie ponownie utworzyć bazę danych IDEMIA za pomocą narzędzia IDEMIA DataBridge. W oknie dialogowym **Urządzenie biometryczne** upewnij się, że wszystkie konfiguracje zostały prawidłowo wysłane do czytników IDEMIA. Jeśli którekolwiek zadanie synchronizacji się nie powiodło, odtwórz konfigurację czytnika:
1. W programie MorphoManager przejdź do okna **Urządzenie biometryczne**.
2. Zaznacz urządzenie, w którym występuje problem.
3. Kliknij przycisk **Odbuduj**.

Zgodność funkcji obsługi kart w systemie ACS z trybami uwierzytelniania w systemie IDEMIA:

Funkcja	Tryb: Karta ORAZ biometria	Tryb: Karta lub Biometria
Karty dostępu: wstawianie	OK	OK
Karty dostępu: aktualizacja	OK	OK
Karty dostępu: usuwanie	OK	OK

Karty dostępu: wiele kart	Tylko pierwsza karta	Pierwsza karta używana w biometrii.
Karta zastępcza	OK	OK
Tymczasowa karta	OK	OK
Karta tymczasowa: tylko okresowo	OK	OK
Karta tymczasowa: dezaktywacja wszystkich kart po upływie okresu	OK	OK
Karta tymczasowa: automatyczna aktywacja kart po ustalonym okresie	OK	OK
Karta tymczasowa: dezaktywacja kart i automatyczna aktywacja	OK	OK
Karty alarmowe	Nieobsługiwane	OK
Tryb biurowy	Nieobsługiwane (*)	Nieobsługiwane (*)
Visitor (Goście)	Istnieje możliwość, że dane biometryczne pierwszego gościa pozostaną przypisane do karty.	Istnieje możliwość, że dane biometryczne pierwszego gościa pozostaną przypisane do karty.
Ochrona	Nieobsługiwane	Brak obsługi biometrii. Karta działa.
Karta parkingowa	OK	OK
Kod PIN	Nieobsługiwane (*)	Nieobsługiwane (*)
Weryfikacja przez zewnętrzne rozwiązanie	Brak kodu PIN (*)	Brak kodu PIN (*)
(*) Czytnik IDEMIA nie może pełnić roli czytnika z klawiaturą		

23 Doprowadzanie do zgodności z normą EN 60839

Wstęp

EN 60839 to rodzina europejskich norm o międzynarodowym zasięgu dotyczących sprzętu i oprogramowania następującej infrastruktury:

– systemy alarmowe i elektroniczne systemy bezpieczeństwa
– elektroniczne systemy kontroli dostępu

Aby używany system kontroli dostępu był zgodny z tą normą, może być konieczne przystosowanie niektórych aspektów konfiguracji. Na liście poniżej omówiono najważniejsze obszary modyfikacji. Kompletną listę można znaleźć w treści normy wdrożonej w konkretnych krajach.

Wymogi, jakie muszą być spełnione, aby system AMS 4.0 miał certyfikat zgodności z normą EN 60839 stopień 2

– System spełnia wymagania całkowitej blokady podwójnego wejścia pod względem używania jednej strefy dla każdego kontrolera MAC.
– Dostępność różnych użytecznych stref czasowych w systemie AMS zależy od liczby kontrolerów MAC. Dla każdego kontrola MAC można skonfigurować osobną strefę czasową.
– Okablowanie styków drzwi nie może blokować otwierania drzwi na potrzeby awaryjnej ewakuacji inicjowanej przez system sygnalizacji pożaru lub włamania.
– Tylko czytniki OSDP używają szyfrowania przez interfejs RS485.
– Dostęp do trybu konfiguracji musi być ściśle kontrolowany. Można to osiągnąć np. poprzez umieszczenie komputerów w strefach bezpiecznych oraz ustanowienie limitów czasu trwania sesji logowania, szczególnie przy braku aktywności na poziomie aplikacji i systemu operacyjnego.
– Okablowanie sieciowe i elektryczne musi być kładzione w zabezpieczonych obszarach albo prowadzone w peszlach.
– W niezabezpieczonych miejscach można montować tylko czytniki kart. Wszystkie pozostałe urządzenia muszą być instalowane w strefach bezpiecznych.
– Minimalna długość weryfikacyjnych numerów PIN w poświadczeniach biometrycznych lub fizycznych musi wynosić co najmniej `4` znaki.
– Minimalna długość kodów identyfikacyjnych numerów PIN musi wynosić co najmniej `8` znaków.
– Komputer serwera głównego, serwery połączeń, serwery kontrolerów MAC i komputery klienckie muszą być zsynchronizowane z sieciowym serwerem czasu.
– Na lokalnych kontrolerach dostępu (np. AMC) musi być włączone monitorowanie zasilania.
– Lokalne kontrolery dostępu (np. AMC) mogą pracować w trybie offline tylko podczas awarii sieci. Na przykład na kontrolerze AMC w parametrze **Limit czasu hosta** nie wolno ustawić wartości `0`.

Reguły dotyczące siły haseł

– Minimalna długość hasła wynosi co najmniej `5` znaków.

24 Definiowanie uprawnień i profili dostępu

24.1 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**

24.2 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.

25 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?

25.1 Osoby

W poniższej tabeli wymieniono dane, które są wyświetlane *domyślnie* w oknach dialogowych **osoby**. Okna dialogowe można w znacznym stopniu dostosowywać. Patrz **Niestandardowe pola na dane osobowe**.
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.

Patrz

– *Niestandardowe pola na dane osobowe, Strona 134*

25.1.1 Opcje kontroli kart i budynków

Przegląd

Na karcie **Kontrola karty** posiadacz karty identyfikacyjnej ma możliwość aktywowania 1 lub 2 ogólnych wyjść kontrolera dostępu. Tę możliwość można przypisać posiadaczowi karty, zaznaczając pole wyboru **Kontrola budynku** w oknie dialogowym **Osoby**. Pola wyboru **Kontrola budynku** (lub **Kontrola karty**) to wstępnie zdefiniowane pola niestandardowe, które są domyślnie widoczne na karcie **Kontrola karty** posiadacza, ale można je umieścić w dowolnym miejscu.

Istnieją dwa podstawowe zadania opcji kontroli budynkiem. Opisano je poniżej:

– Skonfiguruj pole wyboru: nadaj mu odpowiednią etykietę, a w razie potrzeby umieść je na innej karcie w oknie dialogowym **Osoby**.
– Przypisz funkcję do wyjścia kontrolera dostępu AMC i pola wyboru.

Wymagania wstępne

– Wyjście kontrolera dostępu jest połączone elektrycznie z urządzeniem, które ma zostać aktywowane przez kartę.

Ścieżka w oknie dialogowym

– Menu główne AMS > **Konfiguracja** > **opcje konfiguracji** > **Pola niestandardowe** > karta **Kontrola karty**

Konfigurowanie pól wyboru

1. Na stronie **Pola niestandardowe** wybierz kartę **Szczegóły** w górnym okienku.

2. Zlokalizuj funkcję **Kontrola budynku**, 1 lub 2, której chcesz używać.
3. Zastąp etykietę odpowiednią nazwą (zalecane). W razie potrzeby należy umieścić to pole wyboru na karcie innej niż **Kontrola karty**. Więcej informacji na ten temat można znaleźć w sekcji **Podgląd i Edytowanie pól niestandardowych**, do której link znajduje się poniżej.

Przypisanie funkcji do wyjścia kontrolera dostępu i pola wyboru

Zob. sekcję **Parametry i ustawienia kontrolera AMC** na poniższym linku.

1. W drzewie urządzeń **Edytora urządzeń** wybierz kontroler dostępu AMC, którego sygnału wyjściowego chcesz użyć.
2. Na karcie **Wyjścia** w górnym okienku wybierz wyjście, którego chcesz użyć.
3. W środkowym okienku wprowadź **Dane wyjściowe** i wybierz typ **25 Kontroli karty**
4. Kliknij przycisk **>**, aby dodać wyjście do dolnego okienka.
5. W dolnym okienku w kolumnie **Param11** wybierz etykietę funkcji kontroli budynku wybraną w poprzedniej procedurze **Konfigurowanie pół wyboru**.
6. Zapisz drzewo urządzeń.

Patrz

– *Parametry i ustawienia kontrolera AMC, Strona 59*
– *Wyświetlanie podglądu i edytowanie pól niestandardowych, Strona 134*

25.1.2 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.

25.1.3 Rejestrowanie podpisów

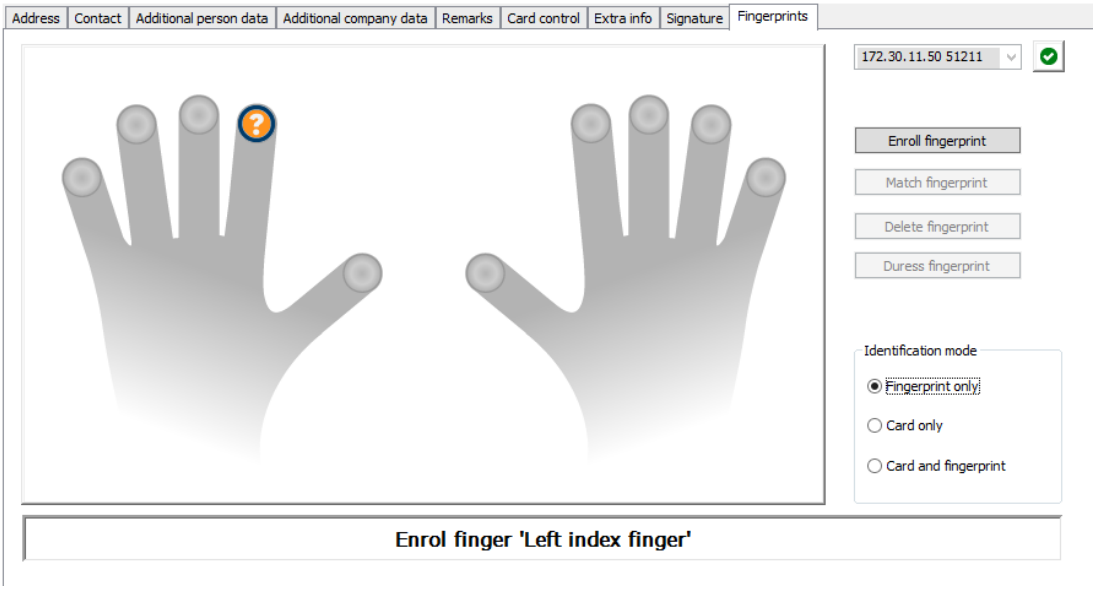
Urządzenie firmy Signotec do przechwytywania podpisów musi być podłączone i skonfigurowane w systemie. W razie wątpliwości należy skontaktować się z administratorem systemu.

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.

25.1.4 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. Ten czytnik rejestracji odcisku palca **nie może** być czytnikiem kontroli dostępu.
- 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:
- Czytniki odcisków palców mogą wysyłać sygnały „przymus” tylko wtedy, jeśli są skonfigurowane w **Edytorze urządzeń** z poniższym ustawieniem karta **Tryb pracy i sieci** > **Szablony na serwerze** > **Karta i odcisk palca**
- 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.

25.2 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.

25.3 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**.

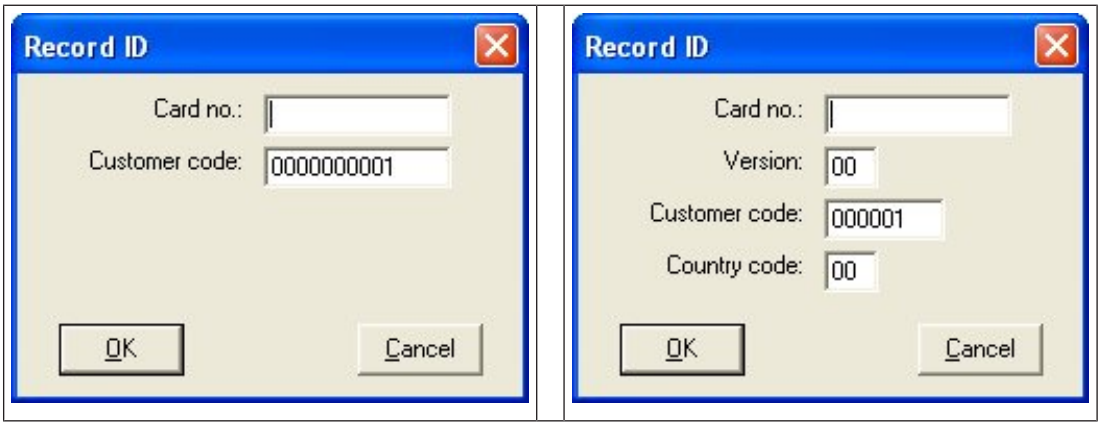
25.3.1 Przypisywanie kart do osób

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**

Wymagania 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 skonfigurowany na stacji roboczej.

Procedura rejestracji

1. Kliknij przycisk po prawej stronie przycisku **Karta rejestrująca** i wybierz skonfigurowany czytnik rejestracji.

– Należy pamiętać, że aby zmienić wybór czytnika rejestrującego, należy zalogować się do menedżera okien dialogowych systemu ACE jako administrator.

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. W oknie wyskakującym

– Wybierz opcję **Zastąp kartę**, jeśli oryginalna została zgubiona lub nieodwracalnie uszkodzona.
– Należy wybrać opcję **Karta tymczasowa**, jeśli oryginalna została chwilowo gdzieś zapodziana lub pozostawiona w domu, a wymagane jest tylko jej tymczasowe zastąpienie.
  – Wprowadź okres ważności karty tymczasowej.
  – Wybierz, czy chcesz teraz dezaktywować wszystkie inne karty.
  – Zaznacz to pole wyboru, jeśli oryginalne karty powinny zostać automatycznie ponownie aktywowane po wygaśnięciu karty tymczasowej.

4. Kliknij przycisk **OK**, aby zapisać ustawienia.

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.

25.3.2 Drukowanie kart identyfikacyjnych

Wymagania wstępne

– W systemie powinien już znajdować się zestaw danych osobowych nowego posiadacza karty.
– Stacja robocza z podłączonym następującym sprzętem (z reguły przez USB):

- Drukarka kart identyfikacyjnych
- Aparat do robienia zdjęć do kart identyfikacyjnych.

Procedura

Ścieżka w oknie dialogowym

Aplikacja kliencka AMS: **Dane osobowe** > **Drukuj karty identyfikacyjne**

1. Wczytaj zestaw danych osobowych, dla których ma zostać wydrukowana karta.
2. W menu rozwijanym **Layout (Układ)** z zapisanych szablonów wybierz odpowiedni układ.
3. Uzyskaj zdjęcie do identyfikatora za pomocą jednej z następujących metod:
   - Kliknij przycisk **Capture (Zrób zdjęcie)** i z listy podłączonych aparatów wybierz odpowiednie urządzenie.
   - Kliknij przycisk **Import picture (Importuj zdjęcie)** i użyj ramki do przycinania, aby wybrać ten fragment fotografii, który ma być nadrukowany na karcie.
4. Kliknij opcję **Preview (Podgląd)**, aby upewnić się, że na karcie będą widniały prawidłowe dane w odpowiednim układzie.
5. Kliknij przycisk **Print (Drukuj)**, aby wydrukować kartę.

Obsługiwane aparaty

Wszystkie urządzenia USB, które system operacyjny rozpozna jako aparaty/kamery.

25.3.3 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 193*.
- 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.

25.3.4 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 **Rozszerzony czas otwierania drzwi** daje osobom niepełnosprawnym więcej czasu (domyślnie 3 razy więcej) na przejście się przez drzwi, zanim pojawi się komunikat **Drzwi są otwarte zbyt długo**.
Uwaga: domyślny współczynnik rozszerzeń można zresetować we właściwościach kontrolera MAC w edytorze urządzeń.
Wybierz **Globalne ustawienia dostępu** > **Współczynnik czasu dla osób niepełnosprawnych**

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**.

Patrz
– *Osoby upoważnione do ustawiania trybu Biuro, Strona 205*

25.3.5 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.

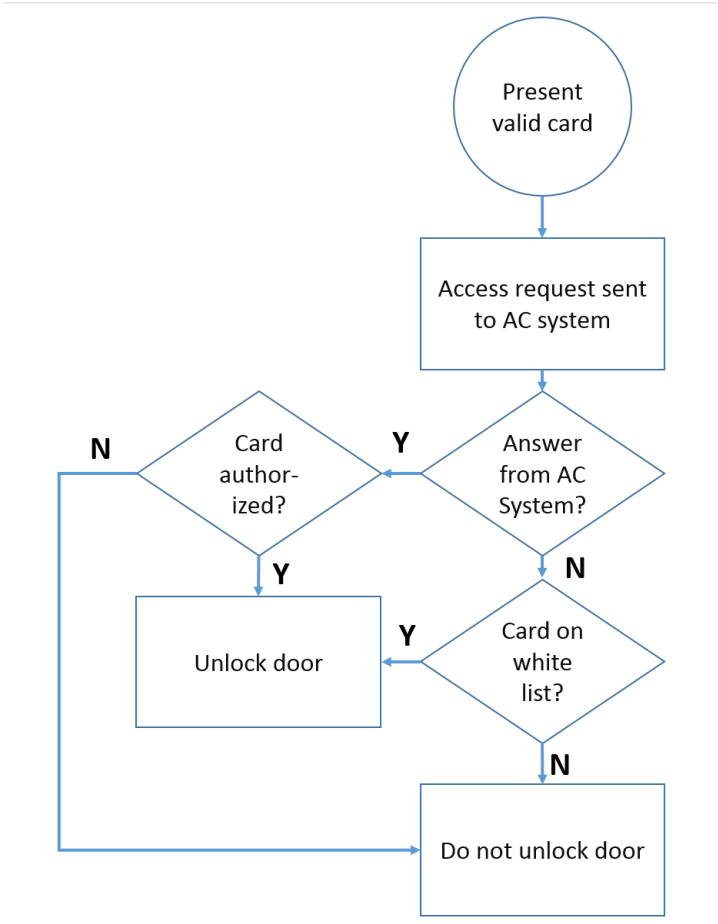
Uwaga!
Tryb biura i parametry urządzeń do drzwi
Tryb biura zastępuje parametr **Odblokuj drzwi** na karcie **Opcje** drzwi w edytorze urządzeń, zezwalając tylko na **0 Tryb normalny** i **1 Odblokowane**.

25.3.6 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.

25.3.7 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

- Czytnik rejestracji został skonfigurowany w Twoim systemie.
- 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**.

25.4 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.

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 blokadę tymczasową**
   Należy pamiętać, że **Blokowanie** nie spowoduje usunięcia kart tymczasowych. Karty tymczasowe wygasną automatycznie po upływie ich okresów ważności. W razie potrzeby usuń je ręcznie.

Uwagi na temat kart tymczasowych

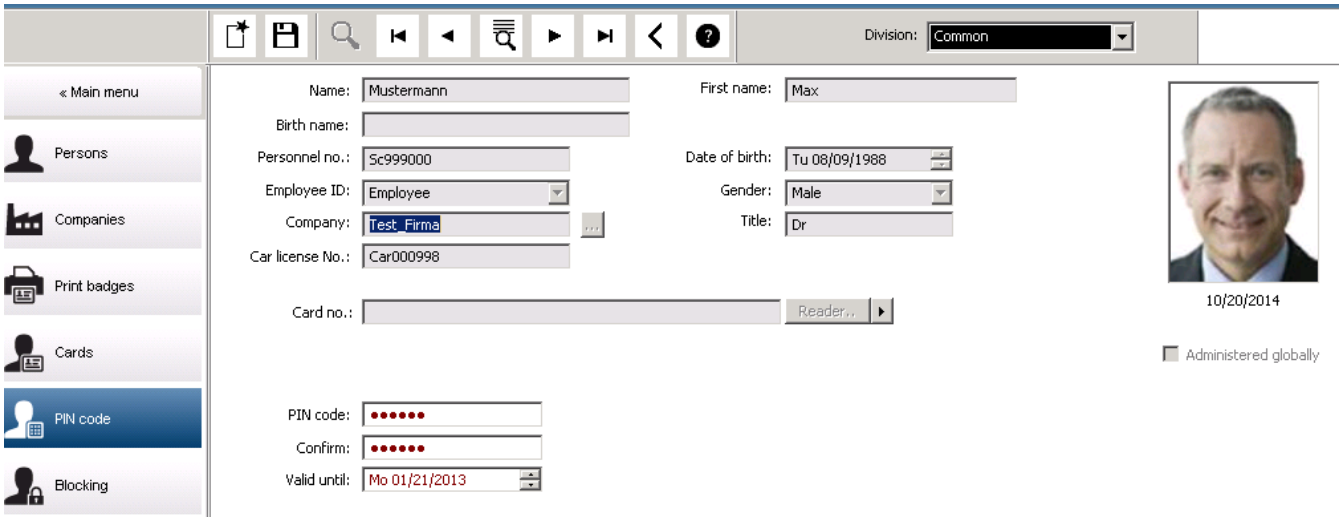
- System nie pozwala na zastępowanie kart tymczasowych innymi kartami tymczasowymi.
- System nie pozwala, aby karta osobista miała więcej niż jedną kartę tymczasową na zamianę.
- Aby zobaczyć szybkie podsumowanie wszystkich kart posiadanych przez osobę, umieść kursor myszy nad małym panelem najbardziej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

25.5 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.

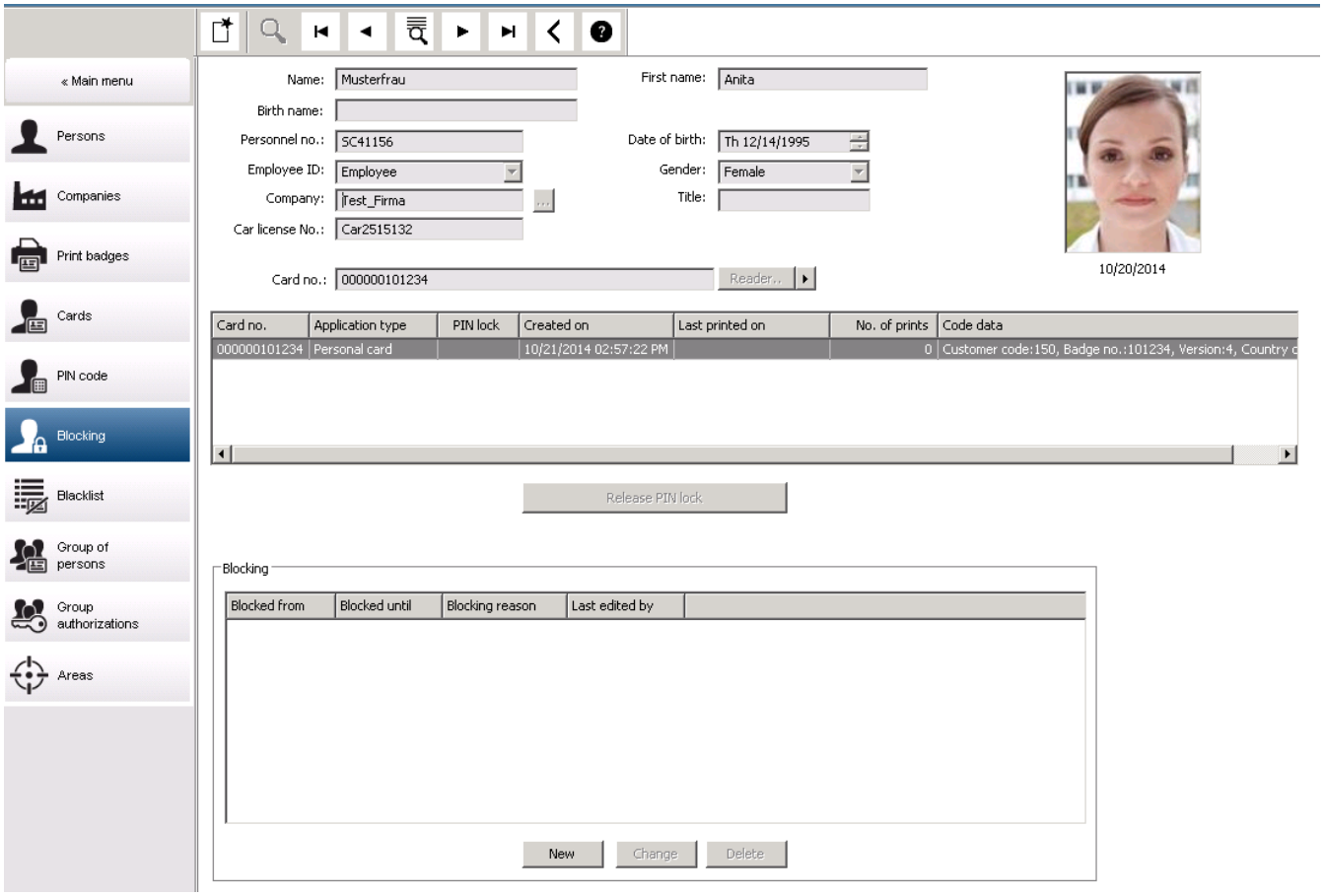
Uwaga!
Sposób wprowadzania kodu PIN przez posiadaczy kart zależy od rodzaju czytników skonfigurowanych w systemie. Na przykład:
W czytnikach RS485 należy wpisać: **4 #** `<the PIN>`
W czytnikach Wiegand i innych należy wpisać: `<the PIN>` **#**
Posiadacze kart powinni zostać poinformowani, jak mają wprowadzać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

25.6 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.

25.7 Karty wymienione na czarnej liście

Okno dialogowe: Czarna lista

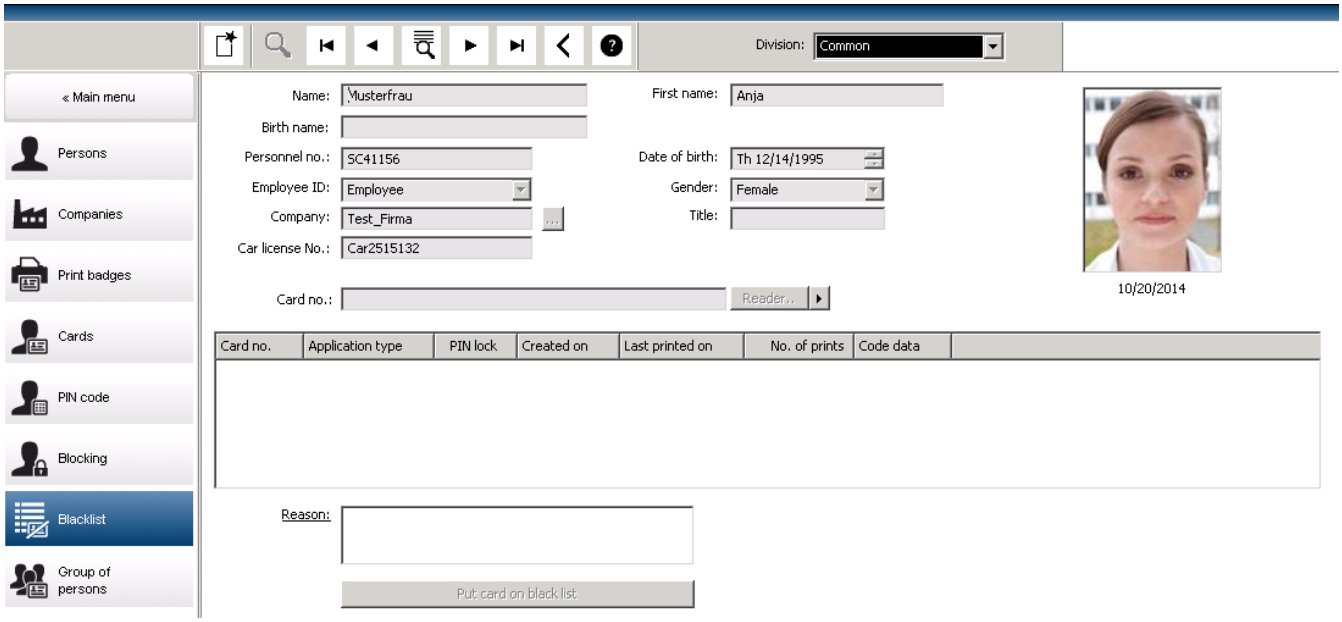
Wszystkie karty, które już nigdy nie powinny być używane, ponieważ np. je skradziono lub zgubiono, są wprowadzane w tabeli czarnej listy.

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.

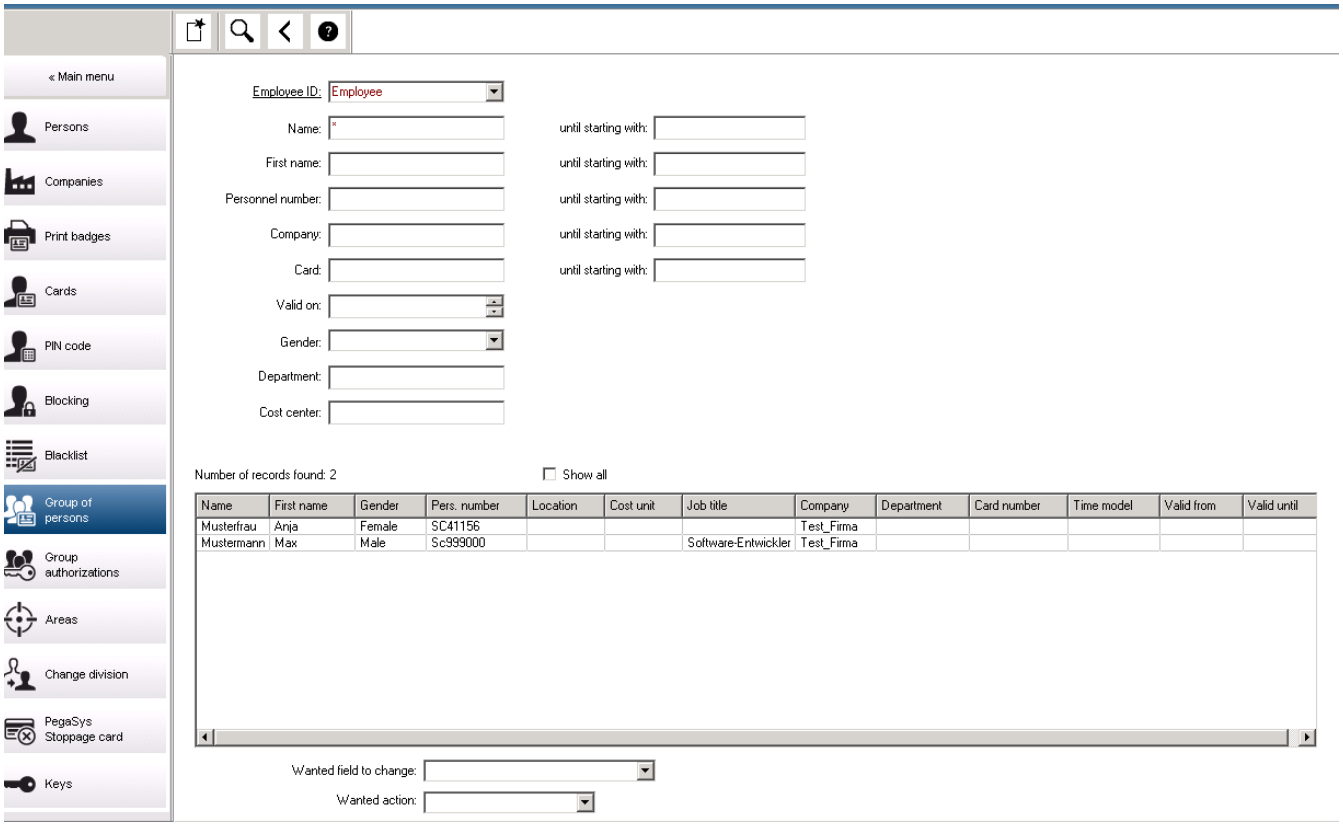
Uwaga!

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.

25.8 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

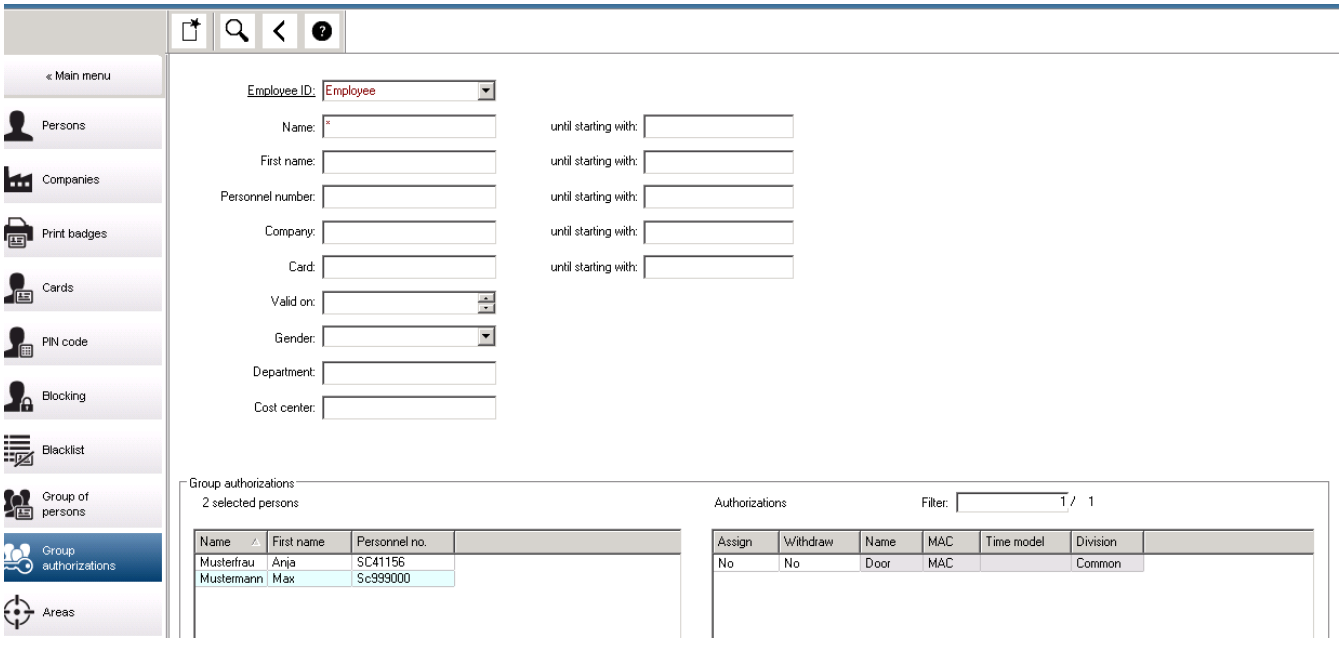
Następnie można wybierać spośród opcji modyfikacji:

- 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.

25.8.1 Grupa uprawnień

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.

25.9 Zmiana strefy przypisanej pracownikom

Wstęp

Zmień strefę to zaawansowane okno dialogowe służące do zmiany strefy grupy osób w zapisach personalnych w systemie.

Uwaga!
Z tej funkcji należy korzystać bardzo uważnie!
Zmiana strefy ma daleko idące konsekwencje w zapisach zmienianych danych osobowych.

Wymagania wstępne

Operator, który wprowadza zmiany dotyczące strefy w rekordach personelu, musi mieć uprawnienia zarówno do edytowania tych osób, jak i odpowiednich stref.

Ścieżka w oknie dialogowym

Menu główne > **Dane osobowe** > **Zmień strefę**

Procedura

1. W okienku **Filtruj osoby** wprowadź kryteria filtrowania w co najmniej jednym z następujących pól:

Filtr	Uwagi/opis
Nazwisko	Użyj gwiazdki jako dowolnego dopasowania do wszystkich osób lub liter **bez** gwiazdki
Numer personalny od/ do	Użyj obu pól, aby określić zakres wartości
Identyfikator pracownika (Typ pracownika)	Wybierz z listy
Strefa	Przycisk Zastosuj filtr pokazuje tylko osoby z tej strefy
Firma	Wybierz spośród dostępnych firm
Dział	
Numer karty od/do	Użyj obu pól, aby określić zakres wartości

2. Kliknij przycisk **Zastosuj filtr**
   Wszystkie osoby pasujące do filtra zostaną wyświetlone na liście **Wybrane osoby**.
3. Aby dokładniej dostosować zestaw wybranych osób, kliknij jeden lub więcej wierszy na liście **Wybrane osoby**, a następnie kliknij przycisk **Usuń**. W razie potrzeby używaj klawiszy Ctrl i Shift, aby zaznaczyć kilka wierszy.

– **WAŻNE:** przed kontynuowaniem upewnij się, że lista **Wybrane osoby** zawiera tylko osoby, których strefę chcesz zmienić.

4. Na liście **Nowa strefa** wybierz strefę docelową dla wybranych osób.
5. Kliknij przycisk **Zmień strefę osób**
   Wszystkie osoby z listy **Wybrane osoby** zostaną przeniesione do strefy **Nowa strefa**.

Konsekwencje zmiany z jednej strefy na inną

Osoby

– Uprawnienia dostępu i kontrola ścieżki
– Łącza do poprzedniej strefy zostają usunięte.
– Łącza do danych z kategorii Wspólne zostają zachowane.

Firmy

– Łącza do firm z poprzedniej strefy zostają usunięte.

Konsekwencje zmiany ze strefy Wspólna na inną

– Uprawnienia dostępu i kontrola ścieżki
– Łącza do kategorii Wspólne i do nowej strefy zostają zachowane.
– Łącza do innych stref zostają usunięte.

Konsekwencje zmiany z jednej strefy na strefę Wspólna

Wszystkie łącza zostają zachowane.

25.10 Ustawianie obszaru dla osób lub pojazdów

Wstęp

W tej sekcji opisano sposób zmiany zapisanej lokalizacji posiadacza karty identyfikacyjnej lub jego pojazdu z jednego zdefiniowanego obszaru na inny. Może to być konieczne, jeśli posiadacz karty przejdzie z jednego obszaru do innego bez skanowania swojej karty identyfikacyjnej. W takich okolicznościach kategoryczne systemy blokowania ponownych wejść odmówią posiadaczowi karty dostępu do czasu, dopóki jego rzeczywista i zarejestrowana lokalizacja nie będą identyczne.

Wymagania wstępne

– Obszary dostępu zostały zdefiniowane w systemie i są używane. Aby uzyskać dokumentację, skorzystaj z poniższego łącza.
– Jako operator możesz modyfikować dane posiadacza karty.

Procedura resetowania lokalizacji dla poszczególnych posiadaczy kart i pojazdów

Ścieżka w oknie dialogowym

Menu główne > **Dane osobowe** > **Obszary**

1. Wybierz posiadacza karty z bazy danych w zwykły sposób.
2. Na liście **Lokalizacja** wybierz nową lokalizację
   lub
3. Na liście **Lokalizacji pojazdu** wybierz nową lokalizację pojazdu posiadacza karty
4. Kliknij przycisk  , aby zapisać ustawienia.

Patrz

– *Konfigurowanie obszarów kontroli dostępu, Strona 26*

25.10.1 Procedura resetowania lokalizacji wszystkich posiadaczy kart i pojazdów

Procedura może być niezbędna na przykład po wykonaniu ćwiczeń ewakuacyjnych. Wszystkie lokalizacje są ustawione na **NIEZNANA**, dzięki czemu można wznowić działanie monitorowania sekwencji dostępu i blokowania ponownych wejść.

Procedura

Ścieżka w oknie dialogowym

Menu główne > **Dane systemowe** > **Resetuj nieznane obszary**.

– Kliknij **Ustaw obszary wszystkich obecnych osób jako NIEZNANE**.

lub

– Kliknij **Ustaw obszary wszystkich zaparkowanych samochodów jako NIEZNANE**.

25.11 Dostosowywanie i drukowanie formularzy danych osobowych

Przegląd

Opcja **Formularze** służy do dostosowywania formularzy w celu drukowania danych posiadaczy kart identyfikacyjnych z bazy danych. Ta funkcja może być wymagana przez lokalne przepisy dotyczące ochrony danych osobowych.

Dostępne są szablony formularzy. Szablony te można eksportować jako pliki HTML, dostosować do wymagań i ponownie zaimportować do użytku w menedżerze okien dialogowych.

Utwórz wystąpienie i wydrukuj formularze wybierając kolejno w oknie dialogowym **Dane osobowe** > **Drukowanie kart identyfikacyjnych**.

Ścieżka w oknie dialogowym

– Menu główne AMS > **Konfiguracja** > **Opcje** > **Formularze**

Dostosowywanie formularza

1. Na liście **Dostępne formularze** w oknie dialogowym **Formularze** wybierz szablon, który chcesz dostosować, zazwyczaj jest to `AllPersonalData_EN, `, który zawiera wszystkie pola danych osobowych w bazie danych.
2. Kliknij przycisk **Eksportuj**, aby zapisać formularz w nowym pliku HTML w swoim systemie
3. Użyj edytora HTML, aby dostosować plik HTML do swoich wymagań
4. W oknie dialogowym **Formularze** kliknij przycisk **Wstaw**, aby importować dostosowany plik HTML do menedżera okien dialogowych.
   – (opcjonalnie) Jeśli formularz jest ważny tylko w przypadku określonej strefy, wybierz tę strefę w kolumnie **Strefa**.
   – (opcjonalnie) Kliknij przycisk **Podgląd**, aby wyświetlić formularz w przeglądarce HTML.
   – (opcjonalnie) Kliknij przycisk **Usuń**, aby usunąć formularz z listy.

Tworzenie wystąpienia i drukowanie formularza

1. W menedżerze okien dialogowych przejdź do:

– Główne menu AMS > **Dane osobowe** > **Drukowanie kart identyfikacyjnych**

2. Wczytaj odpowiedni zapis osobowy do formularza
3. Wybierz formularz z listy **Formularz**.
4. Kliknij przycisk **Drukuj formularz**
   – Formularz jest inicjowany z danymi wybranego zapisu osobowego i wysyłany do wybranej drukarki.

26 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.

26.1 Dane gościa

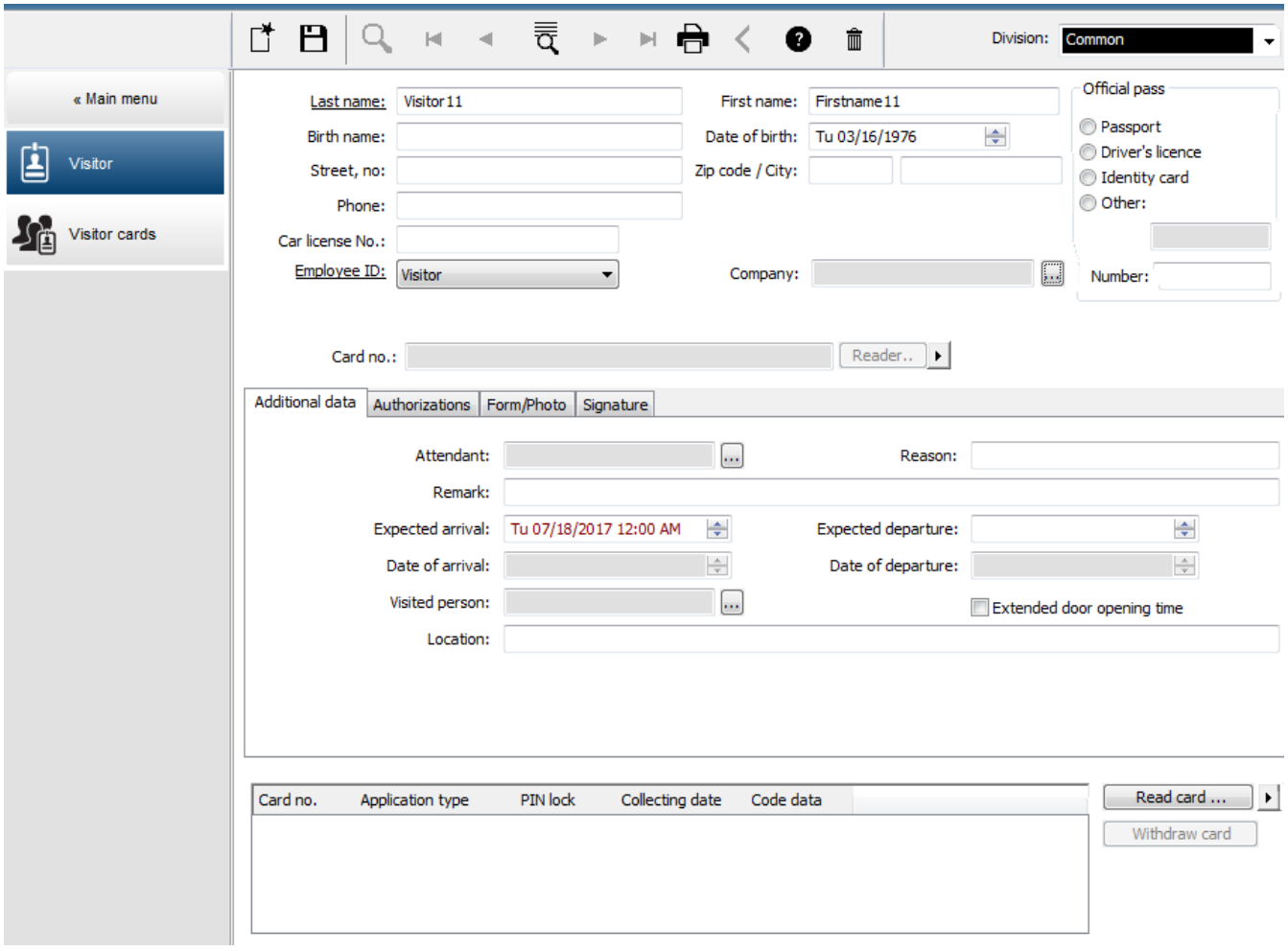
Wstęp

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.

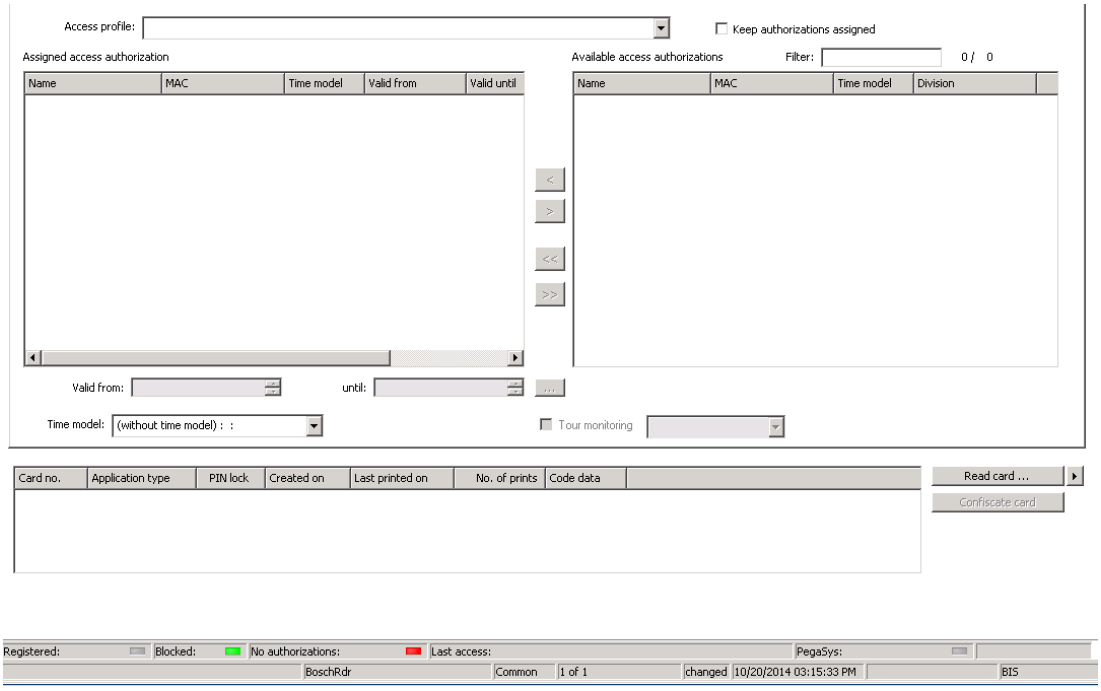
- Okno dialogowe **Goście** jest przeznaczone do wprowadzania danych gości i ich uprawnień dostępu.
- W oknie dialogowym **Karty gości** przeprowadza się rejestrowanie i usuwanie kart gości.

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.



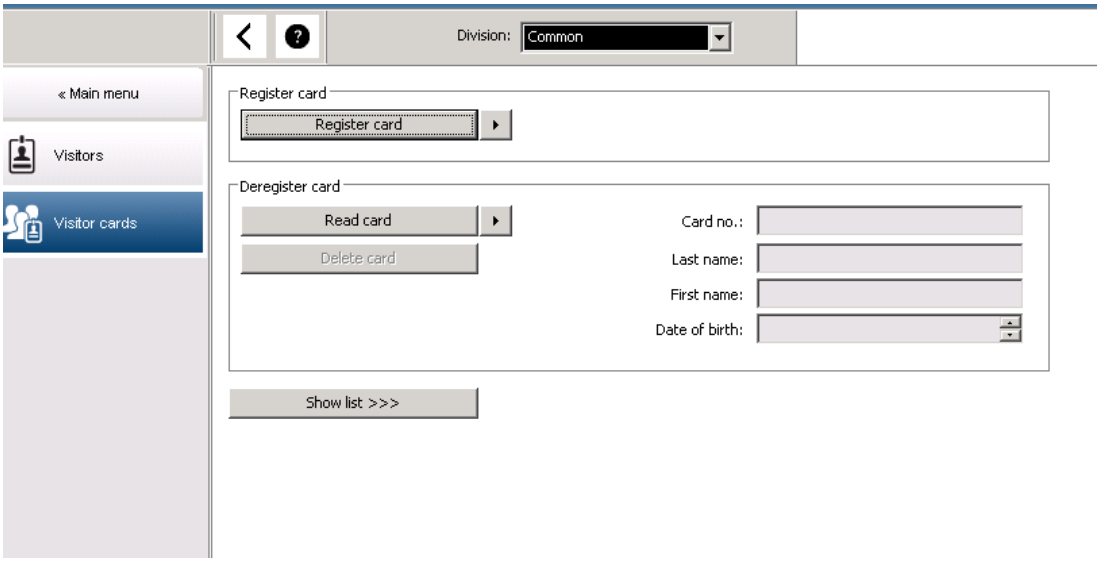
W poniższych polach wprowadzania danych **Powód**, **Lokalizacja** i **Uwaga** można wpisać odpowiednio: powód wizyty, lokalizację, która zostanie odwiedzona, oraz uwagę dotyczącą pobytu.
W przypadku wypełnienia pól **Spodziewane wejście** i **Spodziewane wyjście** dane te pojawią się również w polach **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.



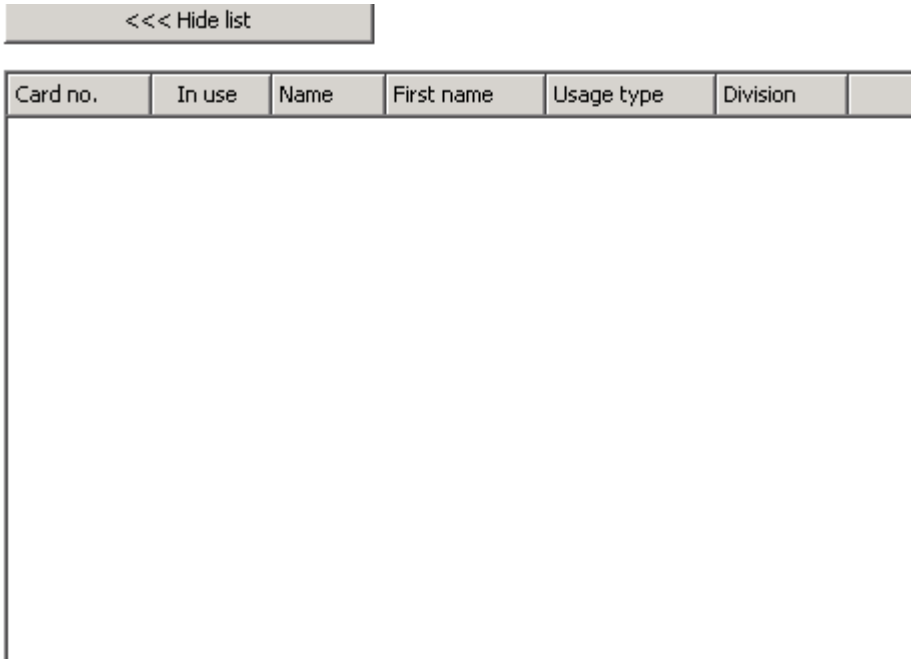
W polu dialogowym **Przypisz autoryzację** można na liście wyboru o tej samej nazwie wybrać jeden z istniejących już profili gości albo zaznaczać poszczególne uprawnienia dostępu na liście **Dostępne uprawnienia dostępu** po prawej stronie i przenosić je na listę **Przypisane uprawnienia dostępu** po 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.



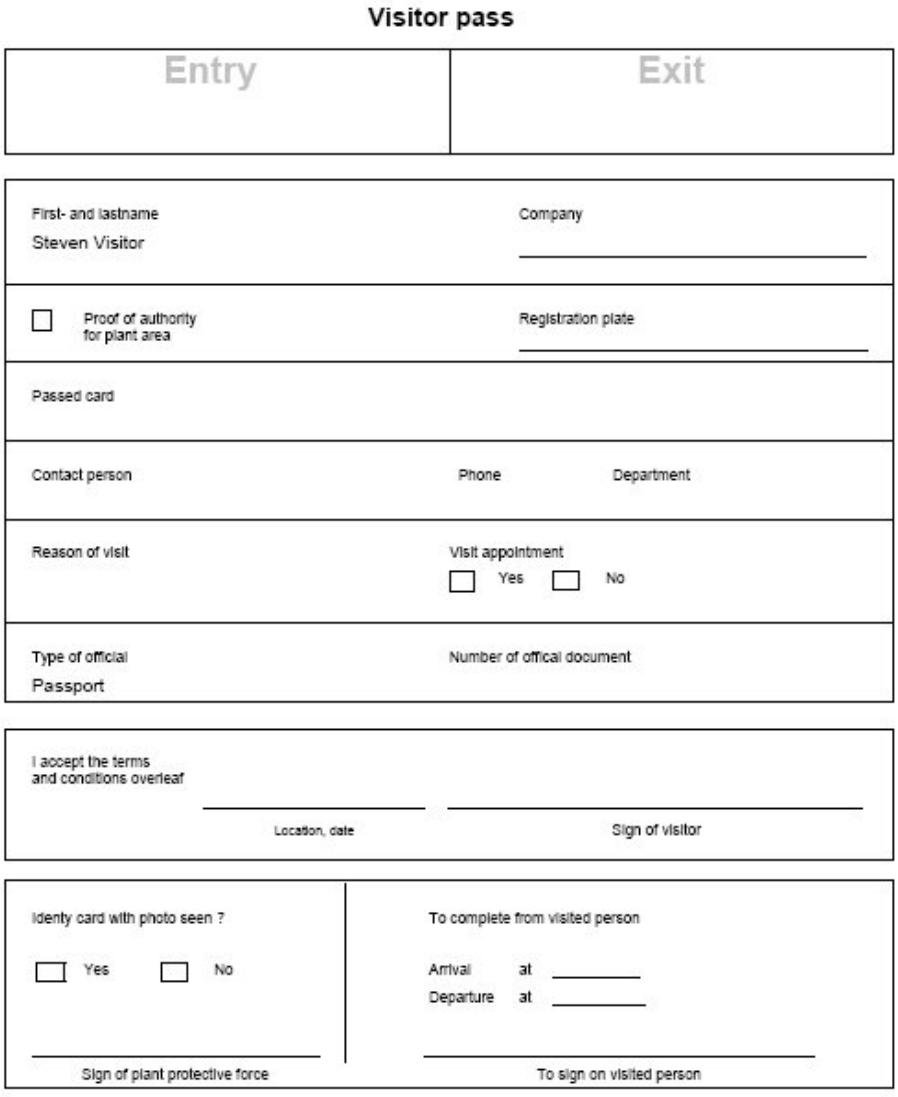
Aby przyspieszyć przydzielanie kart identyfikacyjnych gości, zaleca się zeskanowanie wszystkich istniejących już kart identyfikacyjnych, co umożliwi przydzielanie ich gościom w kolejnym oknie dialogowym.

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

27 Zarządzanie parkingami

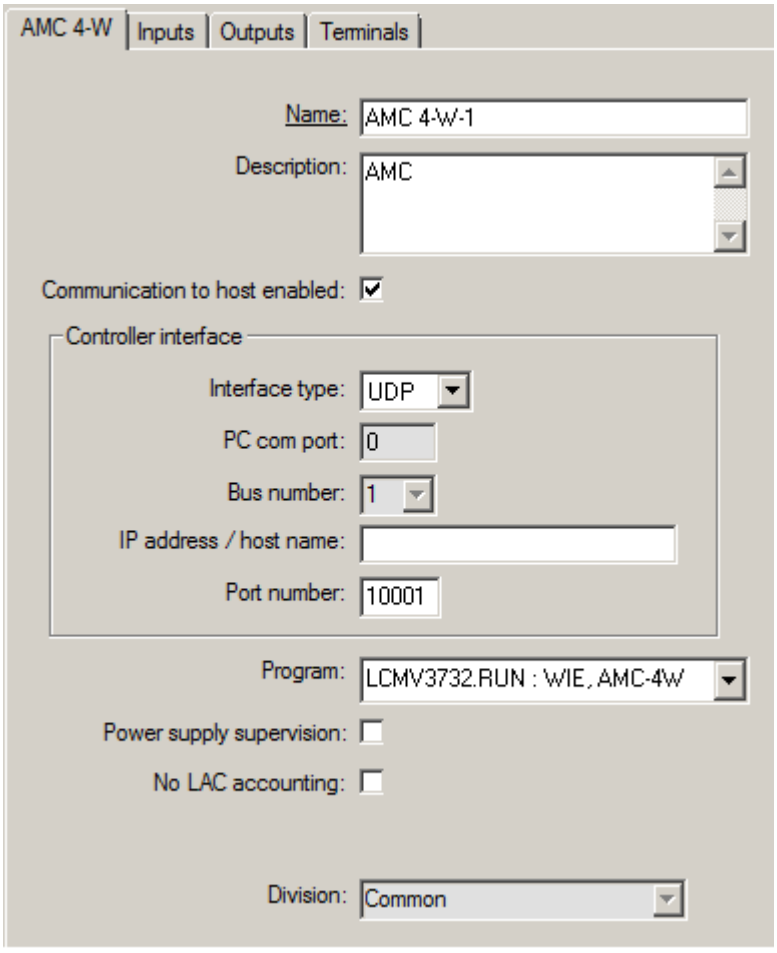
27.1 Uprawnienia do kilku stref parkingowych

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 kontrolerów AMC, należy zaznaczyć w ich konfiguracji pole wyboru **Brak ewidencjonowania LAC**.



27.2 Raport dotyczący parkingu

Parking lot list Date 08.11.2013 , 14:51:23 Page 1

Parking area	Zone	Vehicle count	State
Main Park		51	
	Zone A	30	full
	Zone B	9	--
	Zone C	12	--
Building A		39	
	Zone A	30	full
	Zone B	9	--
Building B		39	
	Zone A	30	full
	Zone B	9	--

27.3 Rozszerzone zarządzanie parkingami

Wstęp

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

– Samochody ciężarowe

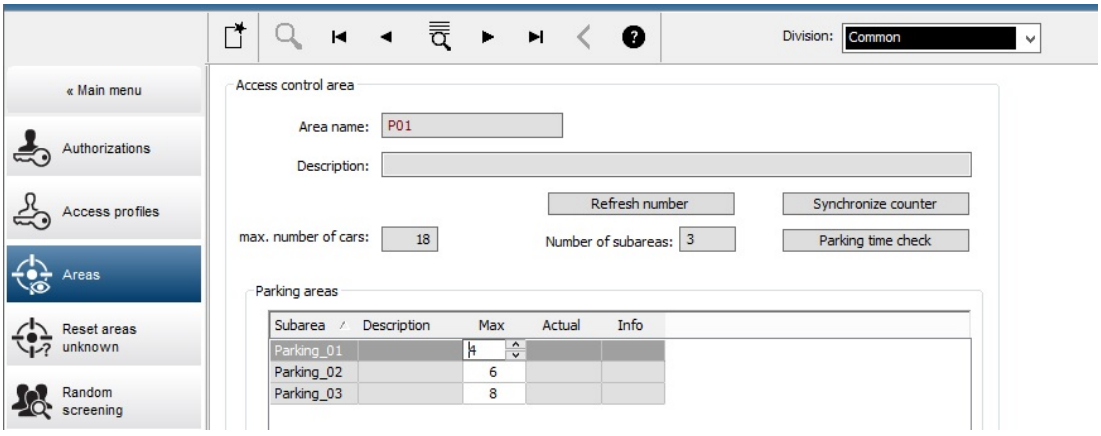
- Dostęp dla osób niepełnosprawnych
- Motocykle

Ścieżka w oknie dialogowym

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

Procedura

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



Uwagi:

- Ustawienia wprowadzone w kolumnie **Maks.** zastępują ustawienia wprowadzone w konfiguracji **Obszary**. Zob. temat **Konfigurowanie obszarów dla pojazdów** na poniższym linku.
- Zero `0` w kolumnie **Maks.** oznacza nieograniczoną liczbę. Zliczanie pojazdów jest wyłączone.

Patrz

- *Konfigurowanie obszarów dla pojazdów, Strona 27*

28 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.

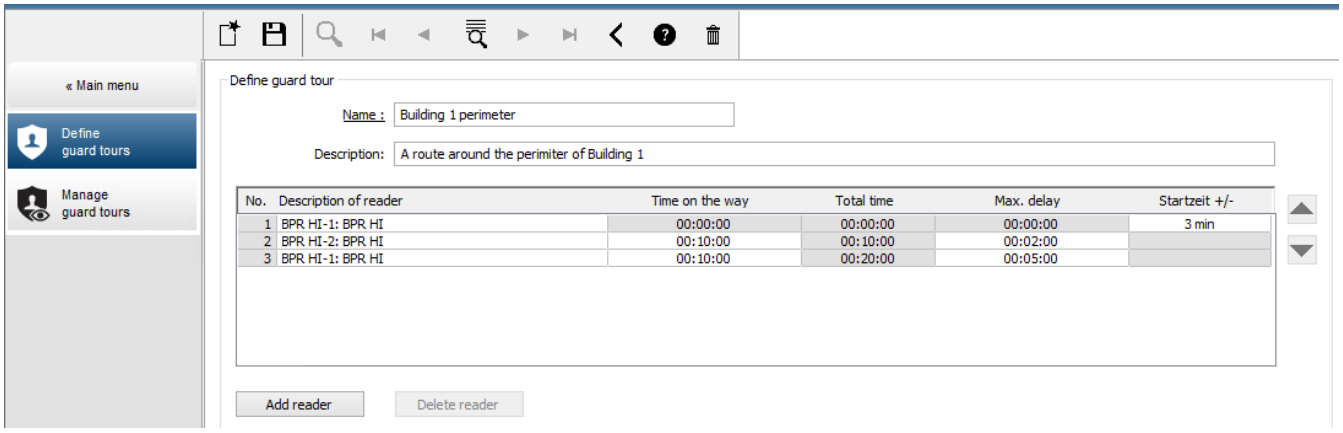
Trasa dozorowa składa się z serii czytników i przybliżonego czasu przejścia między nimi. Określone są również maksymalne dopuszczalne opóźnienie między czytnikami oraz odchylenie (+/-) od czasu rozpoczęcia trasy. Odchylenia wykraczające poza zdefiniowane wartości mogą uruchamiać alarmy i są rejestrowane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

28.1 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.

28.2 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

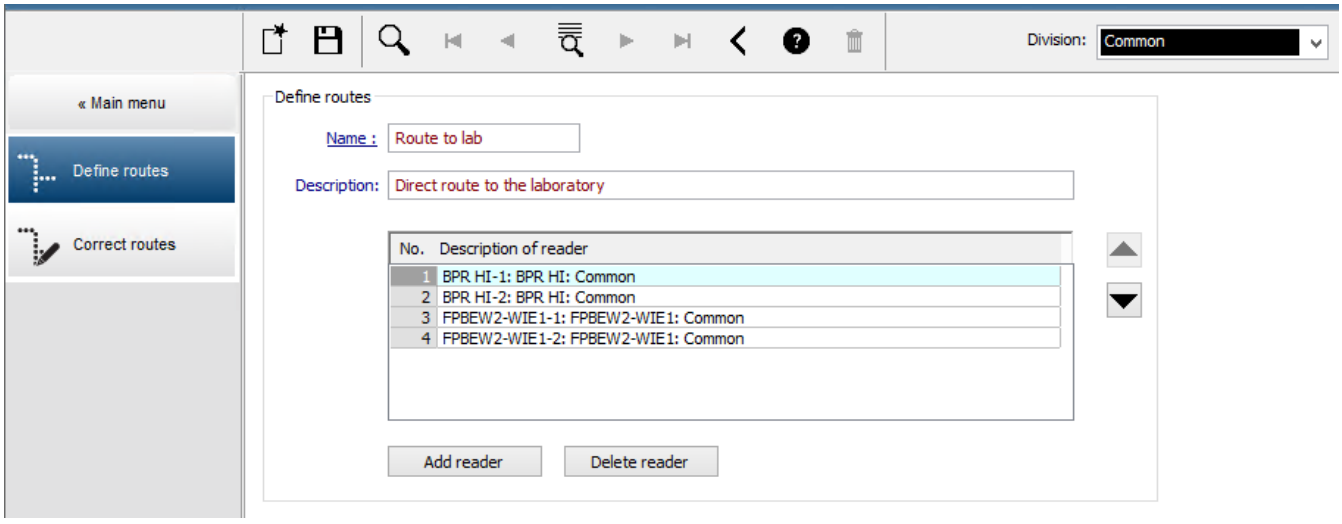
Wszystkie planowane i aktywne patrole są przenoszone na górę listy. Gdy jest kilka zaplanowanych lub aktywnych patroli, wybrany patrol jest oznaczony czerwoną ramką. Kliknij ramkę, aby uzyskać więcej informacji.
Patrol rozpoczyna się po odczytaniu karty pracownika ochrony przez pierwszy czytnik należący 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.

28.3 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**.

29 Losowa kontrola osób

Procedura losowej kontroli

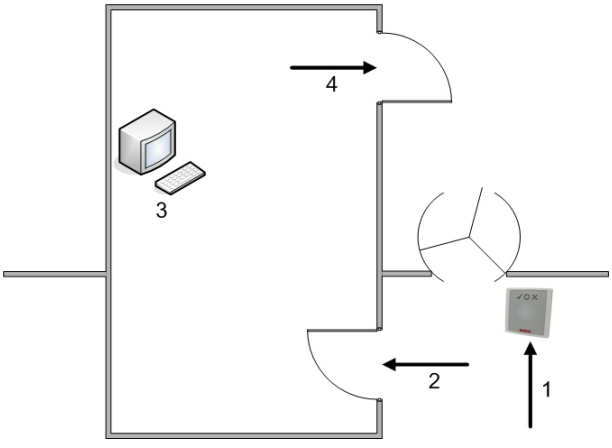
1. Posiadacz karty przykłada ją do czytnika, w którym skonfigurowano losową kontrolę.
   Uwaga
   Wybór losowy obejmuje tylko osoby uprawnione do przechodzenia przez wejście w wyznaczonym kierunku. Sprawdzanie uprawnień odbywa się przed losową kontrolą, więc wszystkie nieupoważnione osoby zostaną natychmiast 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 wyświetlane są „kontrolki LED" 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.

30 Korzystanie z przeglądarki zdarzeń

Wstęp

Przeglądarka zdarzeń umożliwia odpowiednio upoważnionym operatorom badanie zdarzeń zarejestrowanych przez system oraz tworzenie raportów wyświetlanych na ekranie, drukowanych lub eksportowanych do plików `.CSV`.

Aby pobrać i wyświetlić żądane rekordy z bazy danych dziennika zdarzeń, ustaw kryteria filtrowania i kliknij przycisk **Odśwież** . Zależnie od ilości danych proces ten może trwać kilka minut.

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**

30.1 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)
   - 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.

30.2 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)
   - 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.

30.3 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)
   - 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.

31 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.

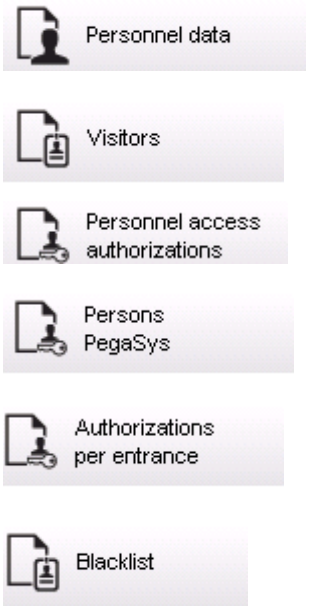
W oknie podglądu znajduje się specjalny pasek narzędzi:

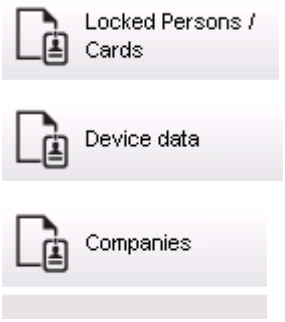
- Kliknij przycisk ✕, aby wyjść z okna podglądu bez drukowania.
- Za pomocą przycisków strzałek ⏮ ◀ 2 of 17 ▶ ⏭ na pasku narzędzi podglądu można przeglądać w przód i w tył oraz wybierać pojedyncze strony po ich numerach.
- Kliknij przycisk  , aby natychmiast rozpocząć drukowanie na domyślnej drukarce.
- 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.

31.1 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.

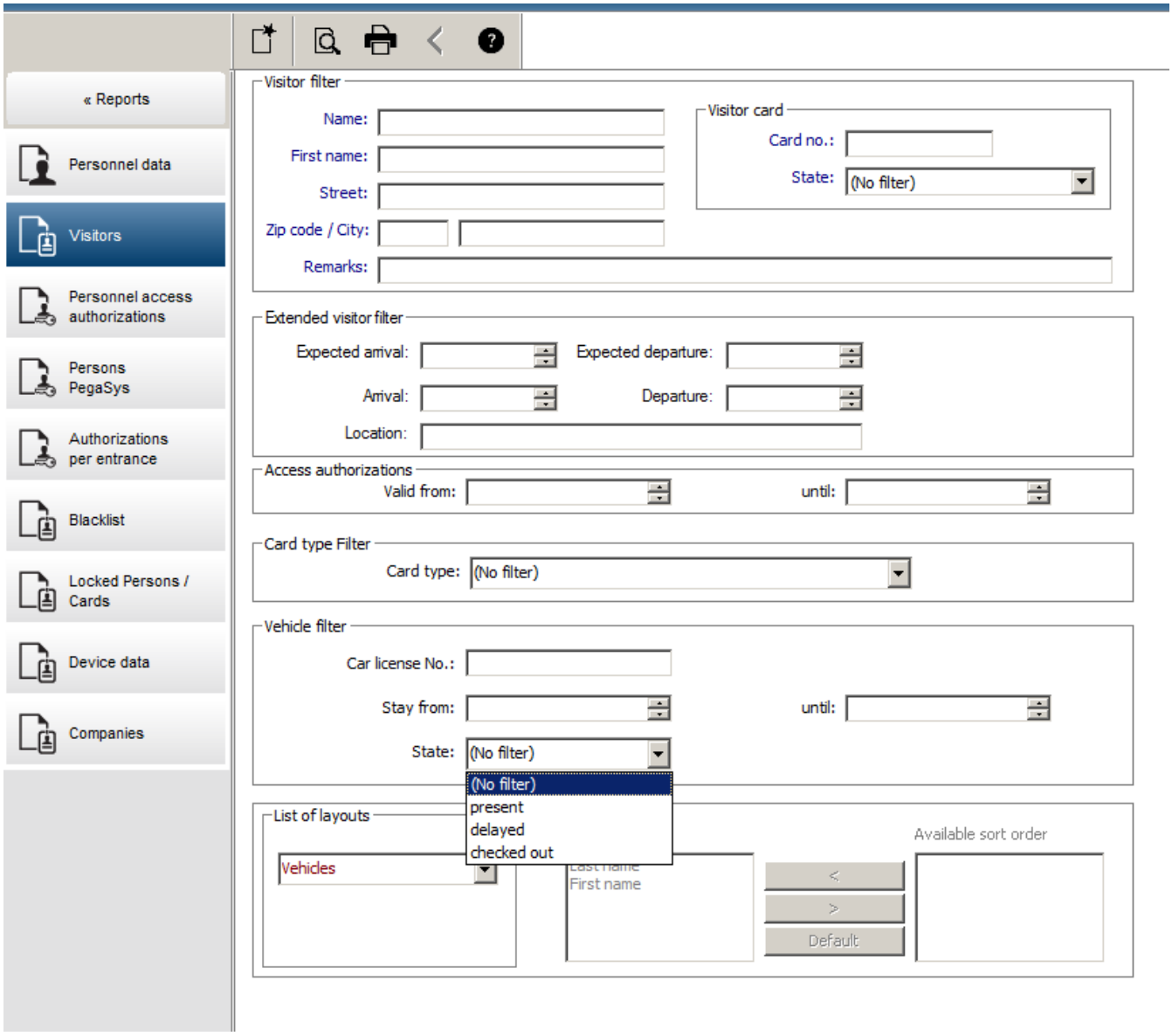
Używając gwiazdek, można na przykład wyszukać firmy, których nazwy zaczynają się określoną literą.

31.1.1 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

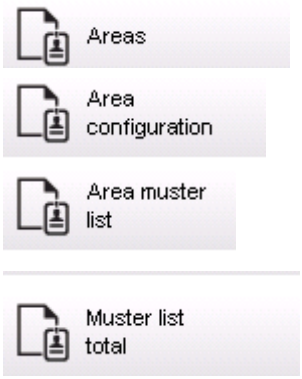
Datum 02.07.2014 , 14:26:14
Seite 1

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

31.2 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.

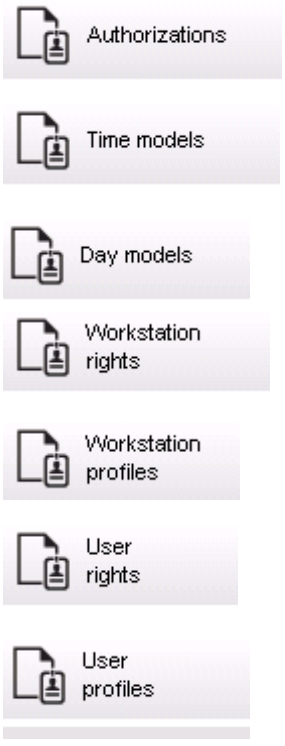
Raport: Konfiguracja obszarów
Wyznaczone obszary i ich podobszary z parkingami oznaczonymi flagami oraz maksymalna liczba osób lub pojazdów.

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.

31.3 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.

32 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 138*.

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 138*

32.1 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.

32.2 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 142*

32.3 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 208*

33 Używanie rejestratora przeciągnięć kartą

Wstęp
Rejestrator przeciągnięć kartą to narzędzie, które pomaga operatorom aplikacji Map View monitorować w czasie rzeczywistym, kto wchodzi na teren obiektu z niego wychodzi.

Przegląd
Rejestrator przeciągnięć kartą to aplikacja wewnątrz aplikacji Map View, która na dynamicznie przewijanej liście pokazuje zdarzenia dostępu z ostatnich 10 minut. Maksymalnie może być wyświetlanych 50 zdarzeń dostępu, a zdarzenia starsze niż 10 minut są automatycznie usuwane z listy. Operator może monitorować wszystkie czytniki w systemie lub wybrać podzbiór.
Każdy rekord na liście zawiera szczegółowe informacje o zdarzeniu oraz użyte poświadczenie. Na przykład:
- Imię i nazwisko posiadacza karty oraz jego zdjęcie zapisane w systemie, co umożliwia wizualne potwierdzenie tożsamości.
- Sygnatura czasowa.
- Nazwa firmy i/lub działu, jeśli są zapisane w systemie.
- Wejście i czytnik, przy którym użyto poświadczenia.
- Kategoria zdarzenia z kolorową etykietą:
  - Zielona: Kompletny dostęp przy użyciu prawidłowego poświadczenia.
  - Żółta: Niekompletny dostęp przy użyciu prawidłowego poświadczenia, np. posiadacz wyłączył blokadę, ale nie otworzył drzwi.
  - Czerwona: Nieudana próba uzyskania dostępu przy użyciu nieprawidłowego poświadczenia. Jest wyświetlany rodzaj nieprawidłowości, np. poświadczenie znajduje się na czarnej liście, jest nieznane lub wygasło.

Rejestrator przeciągnięć kartą nie prowadzi własnych archiwów — zdarzenia dostępu wyodrębnia i wyświetla z bazy danych systemu. Dynamicznie przewijaną listę można wstrzymywać w celu bliższego przestudiowania albo otworzyć w osobnym oknie i przeglądać równolegle z innymi aplikacjami wewnątrz aplikacji Map View.

Uwaga!
Opóźnienie po edycji
Modyfikacje zdjęć identyfikacyjnych i innych danych posiadacza karty dokonane w systemie AMS zwykle pojawiają się w rejestratorze przeciągnięć kartą po kilku minutach. Dopóki nie nastąpi synchronizacja, rejestrator przeciągnięć kartą nadal reaguje w czasie rzeczywistym na starsze dane.

Wymagania wstępne
Aby operator mógł używać rejestratora przeciągnięć kartą, musi mieć specjalne uprawnienie w swoim profilu użytkownika.
1. W głównej aplikacji systemu AMS wybierz kolejno opcje **Konfiguracja** > **Profile użytkownika**.
2. Wczytaj nazwę profilu odpowiedniego operatora.
3. W tabeli wybierz kolejno opcje **Mapy menedżera dostępu** > **Funkcje specjalne** > Rejestrator przeciągnięć kartą.

Uruchamianie rejestratora przeciągnięć kartą

- W aplikacji Map View kliknij przycisk  , aby uruchomić narzędzie.

Wybieranie czytników do monitorowania

Jeśli czytniki nie zostały jeszcze wybrane lub jeśli chcesz zmienić dokonany wybór, wykonaj następujące czynności:

1. W oknie rejestratora przeciągnięć kartą kliknij przycisk  (Ustawienia). Zostanie otwarte okno **Filtruj urządzenia**.
2. W drzewie urządzeń zaznacz pola wyboru obok wejść lub czytników, które chcesz monitorować. Pola wyboru działają w następujący sposób:
   Po zaznaczeniu wejścia jego wszystkie urządzenia podrzędne zostaną domyślnie zaznaczone.
   Następnie można wyczyścić pola wyboru poszczególnych niepotrzebnych urządzeń podrzędnych.
   W przypadku zaznaczenia **wszystkich** elementów podrzędnych urządzenia nadrzędnego pole wyboru elementu nadrzędnego jest białe. Jeżeli zostaną zaznaczone tylko **niektóre** urządzenia podrzędne, pole wyboru elementu nadrzędnego jest szare.
3. Kliknij przycisk **OK**, aby zakończyć zaznaczanie czytników i zamknąć okno **Filtruj urządzenia**.

Wyświetlanie wybranych czytników na mapie

- Kliknij dwukrotnie rekord w rejestratorze przeciągnięć kartą.

⇨ Działanie rejestratora przeciągnięć kartą zostanie automatycznie wstrzymane.

⇨ W głównym oknie aplikacji Map View zostanie wyświetlona pierwsza pasująca scena mapy istniejąca w hierarchii map oraz podświetlony czytnik, który został dwukrotnie kliknięty.

Wstrzymywanie rejestratora przeciągnięć kartą

- W oknie rejestratora przeciągnięć kartą kliknij przycisk  lub kliknij dwukrotnie rekord na liście, aby wstrzymać wyświetlanie dynamicznego obrazu.

⇨ Dynamiczny obraz zostanie zamrożony. Przychodzące rekordy zdarzeń będą buforowane, ale nie wyświetlane.

⇨ W górnej części listy znajdzie się informacja o tym, że strumień zdarzeń został wstrzymany.

Wznawianie wstrzymanego rejestratora przeciągnięć kartą

- W oknie rejestratora przeciągnięć kartą kliknij przycisk  , aby wznowić wyświetlanie dynamicznego obrazu.

⇨ Na dynamicznej liście będą wyświetlane chronologicznie (najpierw najnowsze) wszystkie zdarzenia dostępu (maksymalnie 50), które zaistniały w wybranych czytnikach w ciągu ostatnich 10 minut.

⇨ Zdarzenia dostępu starsze niż 50 najnowszych oraz starsze niż 10 minut są usuwane z listy.

⇨ Nowe zdarzenia dostępu są ponownie wyświetlane w czasie rzeczywistym w chwili wystąpienia.

Duplikowanie rejestratora przeciągnięć kartą w osobnym oknie

Należy pamiętać, że można otworzyć tylko jedno zdublowane okno rejestratora naraz.

1. W oknie rejestratora przeciągnięć kartą kliknij przycisk  (Dodatkowe okno).
   Osobne okno jest duplikatem, a **nie** elementem niezależnym od rejestratora w głównym oknie. Używa tych samych ustawień.
   Teraz w głównym oknie można równolegle obsługiwać inne aplikacje dostępne w aplikacji Map View, takie jak lista alarmów.
2. Po zakończeniu pracy z osobnym oknem należy je zamknąć z paska tytułu.

33.1 Przypadki specjalne

Rejestrator przeciągnięć kartą w aplikacji Map View a drzwi z modułem B901

Aby aplikacja **Rejestrator przeciągnięć kartą** dostępna wewnątrz aplikacji AMS Map View otrzymywała poprawne informacje, identyfikatory drzwi wyposażonych w kontroler B901 muszą być takie same, jak identyfikatory punktów drzwiowych. Innymi słowy drzwi 1 muszą być przypisane do punktu drzwiowego 1, drzwi 2 do punktu drzwiowego 2 itd.

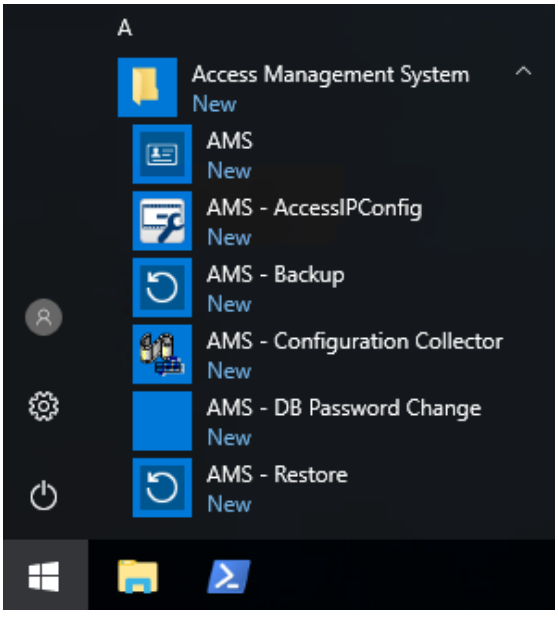
Doors 1 - 4	Door 1	Door 2	Door 3	Door 4
Door Name Text	Door 1	Door 2	Door 3	Door 4
Door Name Text (Second Language)				
Door Source	SDI2 (B901)	SDI2 (B901)	SDI2 (B901)	SDI2 (B901)
Entry Area	1	1	1	1
Associated Keypad #	Keypad 1	Keypad 1	Keypad 1	Keypad 1
Custom Function	Disabled	Disabled	Disabled	Disabled
Door Point	1	2	3	4
Door Point Debounce	600ms	600ms	600ms	600ms

Przypisań tych należy dokonać w ustawieniach kontrolera drzwi B901 w narzędziu RPS używanym do konfigurowania central alarmowych sygnalizacji włamania i kontrolerów.

34 Tworzenie kopii zapasowych i ich przywracanie

Funkcja **Kopia zapasowa i przywracanie** umożliwia przeniesienie systemu wraz z jego danymi do nowej wersji AMS lub na nowy komputer.
Funkcję **Tworzenie kopii zapasowych i ich przywracanie** można uruchomić tylko na komputerze, na którym jest zainstalowany serwer systemu AMS. W menu Start systemu Windows dostępne są dwa skróty:

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

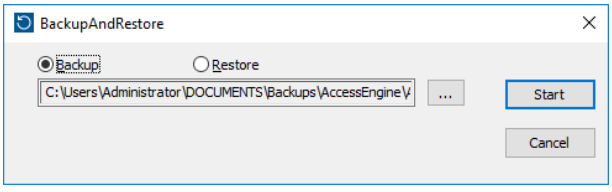


34.1 Tworzenie kopii zapasowej systemu

W tej sekcji opisano sposób tworzenia kopii zapasowej aplikacji AMS i lokalizowania plików kopii zapasowej systemu SQL Server.

Tworzenie kopi zapasowej aplikacji AMS

1. W menu Start systemu Windows kliknij prawym przyciskiem myszy pozycję **Kopia zapasowa AMS** i wybierz opcję **Uruchom jako administrator**.
   - Narzędzie **Kopia zapasowa i przywracanie** wykona domyślnie ustawioną opcję **Kopia zapasowa**.



2. Wprowadź ścieżkę, w której ma zostać zapisany plik `.GZ`.
3. Kliknij przycisk **Rozpocznij**, aby rozpocząć tworzenie kopii zapasowej.
   - Narzędzie **Kopia zapasowa i przywracanie** służy do tworzenia jednego pliku `.GZ` i wyświetlania postępu w wyskakującym oknie.
4. Skopiuj ten plik do bezpiecznej pamięci masowej na innym komputerze. W celu zapewnienia bezpieczeństwa danych **nie** należy pozostawiać kopii tylko na serwerze DMS.

Zlokalizuj i skopiuj pliki kopii zapasowej serwera SQL.

1. Korzystając z eksploratora plików na komputerze serwerze z systemem AMS, należy przejść do lokalizacji, w której serwer SQL przechowuje swoje pliki `.BAK`.
   - Ścieżka dostępu do plików jest następująca, gdzie `<version>` i `<instance name>` są zmiennymi zależnymi od posiadanego systemu:
     `C:`
     `\Program files\Microsoft SQL Server\MSSQL<version>.<instance name>\MSSQL\Backup\`
   - Nazwy plików mają postać:
     `acedb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`
     `Bosch.AlarmDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`
     `Bosch.EventDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`
     `Bosch.MapDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`
     `Bosch.MapViewDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`
     `Bosch.StatesDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak`
2. Skopiuj **wszystkie** pliki do bezpiecznej pamięci masowej `.BAK` na innym komputerze. W celu zapewnienia bezpieczeństwa danych **nie** należy pozostawiać kopii tylko na serwerze DMS.

Uwaga!
Domyślna ścieżka do dziennika zdarzeń AMS to:
`C:\Program Files (x86)\Access Management System\Access Engine\AC\LgfLog\`

34.2 Przywracanie kopii zapasowej

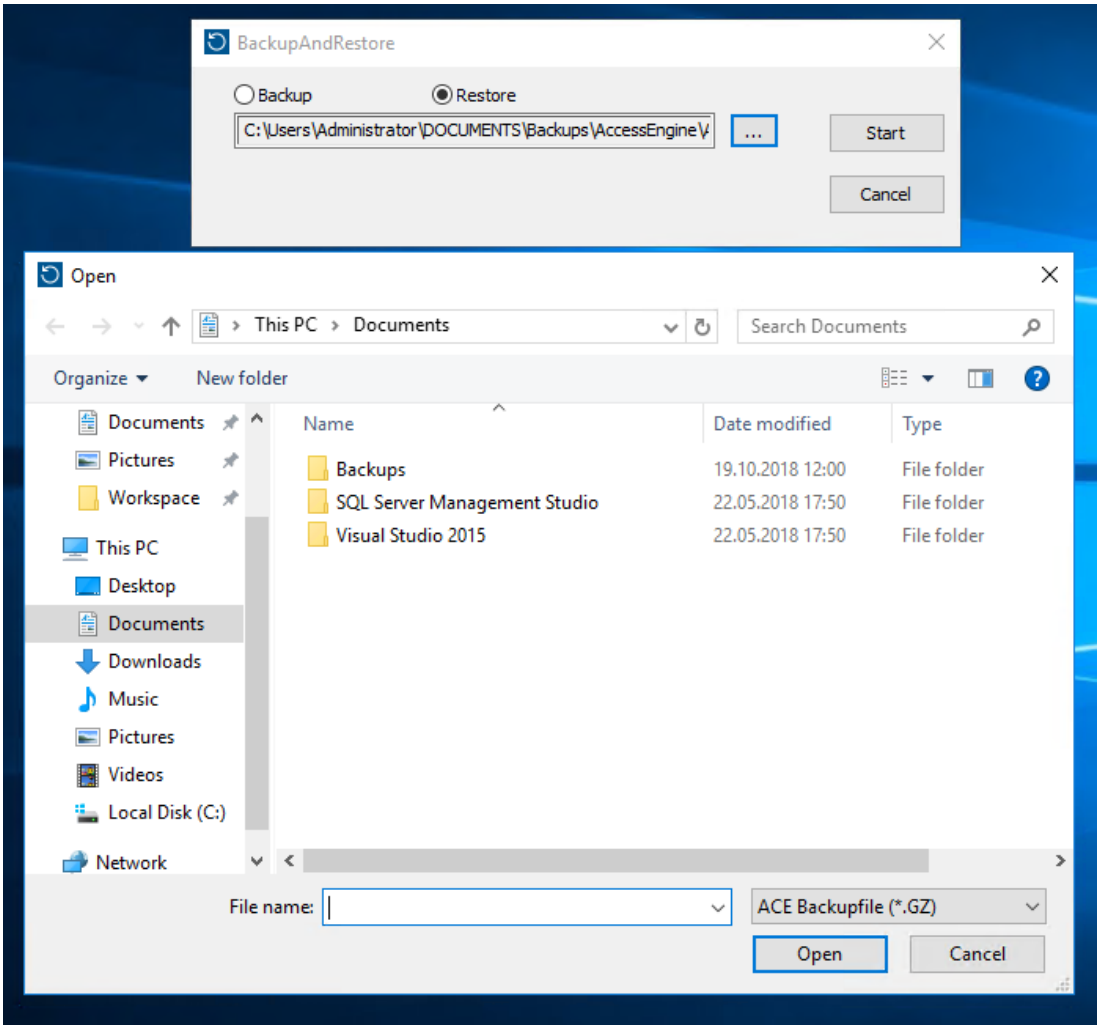
Wymagania wstępne

- Plik `GZ` utworzony przez narzędzie **Kopia zapasowa i przywracanie**.
- Pliki `.BAK`utworzone przez SQL Server, które zostaną naruszone podczas wykonywania kopii zapasowej .
- Konto w programie SQL z uprawnieniami **sysadmin**, takie jak `sa`.
- Odpowiednio przygotowany komputer docelowy do obsługi **licencji** i **certyfikatów**:
  - **Licencje**: komputer docelowy (na który kopia zapasowa jest przywracany) wymaga co najmniej równoważnych licencji do tych, na którym utworzono kopię zapasową.
  - **Certyfikaty**: wszystkie urządzenia klienckie komputera docelowego będą wymagały nowych certyfikatów wygenerowanych przez instalację na komputerze docelowym, a nie tych na oryginalnym komputerze.
    Zapoznaj się z **Instrukcją instalacji AMS**, aby wygenerować i zainstalować certyfikaty klienta.

Procedura

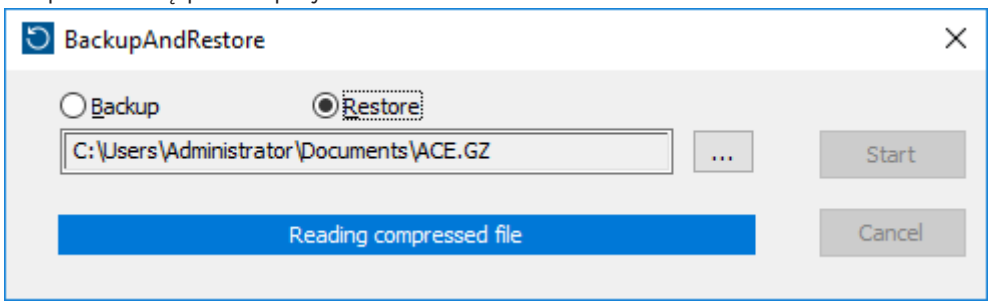
1. W programie AMS kliknij kolejno pozycje **Plik** > **Zakończ**, aby przerwać działanie aplikacji AMS.
2. Po zakończeniu działania programu uruchom aplikację systemu Windows **Usługi** i upewnij się, czy wszystkie usługi systemów `Access Engine` i `Access Management System` zostały zatrzymane. Jeśli nie, zatrzymaj je tu.
3. **Tylko wtedy, gdy** korzystasz z kontrolera RMAC (nadmiarowy MAC awaryjny) z głównym lub 1. MAC, przejdź do następnego podrozdziału i wykonaj opisaną tam procedurę przed powrotem do tego kroku.

4. Skopiuj pliki MSSQL `.BAK` zapisane z oryginalnego komputera do dokładnie takiej samej lokalizacji (ścieżki) na nowym komputerze.
   – Ścieżka dostępu do plików jest następująca, gdzie `<version>` i `<instance name>` są zmiennymi zależnymi od posiadanego systemu:
   `C:\Program files\Microsoft SQL Server\MSSQL<version>.<instance name>\MSSQL\Backup\`
5. W menu Start systemu Windows kliknij prawym przyciskiem myszy pozycję **Przywróć AMS** i wybierz opcję **Uruchom jako administrator**.
   – Narzędzie **Kopia zapasowa i przywracanie** wykona domyślnie opcję **Przywróć**.
6. Kliknij przycisk **[...]**, aby zlokalizować plik `GZ` kopii zapasowej w systemie i kliknij przycisk **Otwórz**, aby go wybrać.



7. Kliknij przycisk **Rozpocznij**, aby rozpocząć proces przywracania.
8. Po pojawieniu się monitu o podanie poświadczeń dla serwera wprowadź poświadczenia administratora systemu MSSQL, np. `sa`, a nie poświadczenia logowania do serwera.

– Rozpocznie się proces przywracania



9. Po zakończeniu procesu przywracania uruchom aplikację **Usługi** systemu Windows i ręcznie uruchom ponownie wszystkie usługi `Access Engine` i `Access Management System`.
10. Uruchom jako administrator program instalacyjny `AMS Server Setup.exe`, aby zsynchronizować dane kopii zapasowej z bieżącymi danymi systemowymi.

Patrz

– *Tworzenie kopii zapasowej systemu, Strona 248*

34.2.1 Przywracanie RMAC w nowej instalacji

Uwaga: ta procedura jest odpowiednia tylko w przypadku, gdy przywraca się kopię zapasową systemu z adresami MAC i RMAC na innych urządzeniach.

Wstęp

W przypadku przywracania kopii zapasowej na nowych komputerach należy ponownie skonfigurować adresy IP urządzeń MAC i RMAC, które były zapisane w pliku kopii zapasowej, na adresy IP nowego sprzętu. Tę konfigurację należy wykonać, uruchamiając narzędzie MACInstaller na nowym sprzęcie.

Narzędzie MACInstaller można znaleźć na nośniku instalacyjnym na ścieżce `\AddOns\MultiMAC\MACInstaller.exe`

Użycie narzędzia MACInstaller zostało szczegółowo opisane w rozdziale *Korzystanie z narzędzia MACInstaller, Strona 56*

Procedura

1. Uruchom narzędzie MACInstaller na komputerze, na którym działa 1. MAC. Komputer ten może być serwerem DMS lub dedykowanym serwerem z 1. MAC.
   – W narzędziu należy ustawić nowe adresy IP podstawowego adresu MAC (tego komputera) oraz RMAC.
2. Uruchom narzędzie MACInstaller na komputerze, na którym działa RMAC.
   – W narzędziu należy ustawić nowe adresy IP podstawowego MAC i RMAC (tego komputera).
3. Wróć do kroku, w którym opuściłeś **procedurę przywracania**.

Patrz

– *Korzystanie z narzędzia MACInstaller, Strona 56*

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.

ACS

ogólne określenie system kontroli dostępu firmy Bosch, na przykład AMS (Access Management System) lub ACE (BIS Access Engine).

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.

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.

CSN

Numer wyboru karty.

Czytnik wprowadzania obszaru docelowego (DET)

Urządzenie, na którym pasażerowie wind mogą wprowadzać żądania obszarów docelowych w grupie wind.

Data Management System (DMS)

Nadrzędny proces zarządzania danymi kontroli dostępu w systemie. System DMS dostarcza dane do głównych kontrolerów dostępu (MAC), które z kolei dostarczają dane do lokalnych kontrolerów dostępu (zazwyczaj AMC).

DCP

hasło, za pomocą którego ACS generuje klucz główny używany do szyfrowania komunikacji w sieci ze wszystkimi podrzędnymi kontrolerami dostępu, czyli z reguły urządzeniami AMC.

DSN

Nazwa źródła danych. Nazwa źródła danych w bazie danych ODBC (Open Database Connectivity).

DTLS

Datagram Transport Layer Security to bezpieczny protokół komunikacyjny zabezpieczający przed podsłuchiwaniem i włamaniami.

entropia hasła

współczynnik określający, na ile silne jest hasło, obliczany na podstawie takich parametrów, jak jego losowość, liczba dostępnych symboli oraz rzeczywista liczba użytych symboli.

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.

grupa wind

Grupa wind w sposób skoordynowany obsługujących te same piętra. Każda grupa wind jest zarządzana przez serwer wprowadzania obszaru docelowego (DES).

IDS (SSW)

System sygnalizacji włamania, nazywany również jako systemem alarmu włamaniowego.

Klucz główny

Kod generowany przez system z poziomu DCP (device communication password, hasła komunikacji urządzenia), używany do zabezpieczania urządzeń kontroli dostępu. Klucz główny nigdy nie jest widoczny dla żadnego użytkownika.

Klucz sprzętowy AMC.

Wewnętrzny kod uwierzytelniający generowany przez kontroler AMC na podstawie określonych parametrów sprzętowych. Nie jest on widoczny dla użytkownika.

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.

Losowy klucz LCD

Tymczasowy kod alfanumeryczny generowany na nowo przez kontroler AMC przy każdym uruchomieniu. Klucz może być wyświetlany na ekranie ciekłokrystalicznym (LCD) kontrolera AMC i może być wymagany przez oprogramowanie narzędziowe do uwierzytelniania komunikacji w sieci.

MAC (główny kontroler dostępu)

W systemach kontroli dostępu program serwerowy, który koordynuje i kontroluje lokalne kontrolery dostępu, zwykle AMC (modułowy kontroler 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.

Narzędzie IPConfig

Oddzielny dodatkowy program do konfigurowania ustawień sieci i zabezpieczeń sieciowych urządzeń sprzętowych w ramach systemu kontroli dostępu.u.

Obszar (uzbrajanie)

Grupowanie wejść modelu 14 w systemie kontroli dostępu. Uzbrojenia lub rozbrojenia systemu włamania dla jednego z tych wejść skutkuje jednocześnie na wszystkich wejściach, na których parametr Obszar uzbrojenia ma to samo oznaczenie jednoliterowe.

przemykanie

Obchodzenie systemu kontroli dostępu poprzez podążanie bardzo blisko za uprawnionym posiadaczem karty bez okazywania własnych danych uwierzytelniających na wejściu.

Punkt

Czujnik wykrywający włamanie do obszaru kontrolowanego. W niektórych kontekstach punkty mogą być nazywane strefami lub czujnikami.

REX

„Żądanie wyjścia”. Sygnał żądania, aby drzwi zostały odblokowane od wewnątrz w celu umożliwienia wyjścia. Sygnał jest zazwyczaj wyzwalany przyciskiem lub prętem po wewnętrznej stronie wejścia, a czasami przez czujkę ruchu.

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.

RPS

Oprogramowanie do zdalnego programowania. Program zarządzający centralami alarmowymi sygnalizacji pożaru lub włamania w sieci.

Serwer kontrolera MAC

Sprzęt: komputer (inny niż serwer DMS) w systemie Access Engine (ACE) lub Access Management (AMS)), w którym działa MAC lub RMAC.

Serwer wprowadzania obszaru docelowego (DES)

Komputer zarządzający bankiem wind w celu optymalizacji czasów podróży.

SmartIntego

Cyfrowy system blokowania w technologii Simons Voss. System SmartIntego jest zintegrowany z niektórymi systemami kontroli dostępu firmy Bosch.

System wysyłania do obszaru docelowego (DDS)

nazywany też systemem zarządzania obszarami docelowymi, ale używaj skrótu DDS. Otis CompassPlus jest rodzajem DDS.

Tryb biuro

Zawieszenie kontroli dostępu przy wejściu w godzinach pracy biura.

Tryb konfiguracji

domyślny stan urządzeń kontroli dostępu w edytorze urządzeń. Zmiany są natychmiast stosowane i propagowane do urządzeń podrzędnych.

Tryb normalny

W przeciwieństwie do trybu Biuro w trybie normalnym udziela się dostępu tylko osobom, które zaprezentują w czytniku prawidłowe poświadczenia.

Tryb pracy

stan urządzenia kontroli dostępu w edytorze urządzeń, kiedy reaguje ono na polecenia wydawane poza edytorem urządzeń. Zmiany konfiguracji obowiązują dopiero po zakończeniu trybu pracy i przywróceniu trybu konfiguracji.

Urządzenie przekierowujące wprowadzanie obszaru docelowego (DER)

Komputer znajdujący się na tym samym poziomie co serwer wprowadzania obszaru docelowego (DES) w systemie Otis CompassPlus. Łączy się on ze wszystkimi grupami wind, a jego zadaniem jest poprawa wydajności pracy urządzeń DES.

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.

wyciszenie

zawieszanie alarmu w konkretnie określonej sytuacji.

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com

Building solutions for a better life.

202309211028