

Access Professional Edition



BOSCH

pl

Configuration Manual

Spis treści

1	Przegląd systemu	6
1.1	Ograniczenia i opcje	7
1.2	Instalacja na pojedynczym komputerze	9
1.3	Instalacja na wielu komputerach	10
1.4	Wymagania wstępne dla systemu	11
1.5	Komputer jedнопłytowy	13
2	Informacje ogólne	16
2.1	Wstęp	16
2.2	Logowanie użytkownika	19
2.3	Menu i pasek narzędzi	24
2.4	Ogólne ustawienia systemu	28
2.5	Układ okna dialogowego	33
2.6	Menu i pasek narzędzi	34
2.7	Układ okna dialogowego	39
2.8	Menu i paski narzędzi	40
2.9	Konfiguracja rejestracji	42
2.9.1	Rejestracja za pomocą czytników podłączonych do kontrolera AMC	45
2.10	Obsługa serwera SQL	49
2.11	Instalacja bazy danych SQL	53
3	Konfiguracje	60
3.1	Tworzenie nowych konfiguracji	60
3.2	Otwieranie konfiguracji	63
3.3	Aktywacja nowej konfiguracji	65
3.4	Przesyłanie konfiguracji do kontrolerów	66
4	Kontrolery	71
4.1	Definiowanie i modyfikowanie nowych kontrolerów	71
4.2	Ustawienia kontrolera	78
5	Sygnały	81
5.1	Sygnały wejściowe	81
5.2	Sygnały wyjściowe	85
5.3	Definiowanie warunków sygnałów wyjściowych	92
5.4	Tworzenie modułów rozszerzeń	99

6	Entrances (Wejścia)	102
6.1	Tworzenie i modyfikacja modeli drzwi	102
6.2	Wskazania i ustawianie parametrów	110
6.3	Modele drzwi z ustawieniami specjalnymi	120
7	Strefy	122
8	Personnel Groups (Grupy personelu)	128
8.1	Dostęp grupy w przypadku czytników z klawiaturą	132
8.2	Ograniczenia dotyczące dostępu grupy	133
9	Uprawnienia dostępu	134
9.1	Tworzenie i przypisywanie	134
9.2	Uprawnienia specjalne	139
10	Dni specjalne	144
10.1	Tworzenie i edytowanie	144
11	Modele dzienne	148
11.1	Tworzenie i edytowanie	148
12	Modele czasowe	151
12.1	Tworzenie i edytowanie	154
13	Teksty	157
13.1	Displaytexts (Wyświetlany tekst)	158
13.2	Event Log messages (Komunikaty dziennika zdarzeń)	159
14	Additional Personnel data (Dodatkowe pola danych osobowych)	163
15	Przeglądanie map i zarządzanie alarmami	167
15.1	Konfiguracja mapy	168
15.2	Dodawanie urządzenia do mapy	171
16	Definicja karty	174
17	Dodatek	179
17.1	Sygnały	179
17.2	Domyślne modele drzwi	181
17.3	Model drzwi 01	183
17.4	Model drzwi 03	186
17.5	Model drzwi 06c	187
17.6	Model drzwi 07	188
17.7	Model drzwi 10	192
17.8	Model drzwi 14	195

17.9	Przykłady konfiguracji słuz osobowych	198
17.10	Konfiguracja modelu drzwi 07	201
17.11	Instrukcje dotyczące uzbrajania/rozbrajania	203
17.12	Procedury kontroli dostępu	205
17.13	Porty Access PE	209
17.14	Wymagania normy UL 294	210
18	Rodzaje kodów PIN	212

1 Przegląd systemu

System Access Professional Edition (w dalszej części dokumentu nazywany **Access PE**) składa się z czterech modułów.

- Usługa LAC: proces, który polega na ciągłej komunikacji z lokalnymi kontrolerami dostępu LAC (ang. Local Access Controllers, w dalszej części dokumentu nazywane kontrolerami). AMC: modułowe kontrolery dostępu (ang. Access Modular Controllers), które stosowane są jako kontrolery.
- Konfigurator
- Zarządzanie personelem
- Analiza dziennika

Te cztery elementy mogą być podzielone na moduły instalowane i pracujące na serwerze i kliencie.

Usługa LAC musi pozostawać w stałej łączności z kontrolerami, ponieważ po pierwsze, stale otrzymuje od nich komunikaty o ruchach, obecności i nieobecności użytkowników, po drugie, przesyła do kontrolerów zmiany dotyczące danych, np. związane z przyznaniem nowych kart, ale głównie dlatego, że przeprowadza kontrole metapoziomowe (sekwencyjne kontrole dostępu, kontrole funkcji zapobiegającej przekazaniu karty osobie niepowołanej, kontrole losowe).

Konfigurator również powinien pracować na serwerze, jednak można go zainstalować na klienckich stacjach roboczych i z nich go obsługiwać.

Moduły Zarządzanie personelem i Analiza dziennika należą do komponentów klienta i mogą być uruchamiane dodatkowo na serwerze lub na innym komputerze połączonym przez sieć z serwerem.

Istnieje możliwość zastosowania następujących kontrolerów:

- AMC2 4W (z czterema interfejsami czytników Wiegand) – może zostać rozszerzony za pomocą modułu AMC2 4W-EXT
- AMC2 4R4 (z czterema interfejsami RS485 dla czytników)

1.1 Ograniczenia i opcje

Access PE może być stosowany z systemami, które nie przekraczają poniższych ograniczeń w zakresie ilości podłączonych elementów lub ilości zarządzanych danych:

- maks. 10 000 kart
- do trzech kart na osobę
- długość kodu PIN: 4–8 znaków (konfigurowalny)
- Rodzaje kodów PIN:
 - Kod weryfikacyjny PIN
 - Kod identyfikacyjny PIN
 - Kod uzbrojenia PIN
 - Kod PIN do drzwi
- Warianty dostępu:
 - Tylko za pomocą karty
 - Tylko za pomocą kodu PIN
 - PIN lub karta
- Maks. 255 modeli czasowych
- Maks. 255 uprawnień dostępu
- Maks. 255 uprawnień obszarowych/czasowych
- Maks. 255 grup uprawnień dostępu
- Maks. 16 stanowisk
- Maks. 512 czytników
- Maks. 3 moduły rozszerzeń WE/WY (AMC2 8I-8O-EXT, AMC2 16I-16O-EXT lub AMC2 16I-EXT) na kontroler
- Poniższe ograniczenia dotyczą każdego typu kontrolera:

Kontroler	AMC2 4W	AMC2 4W z AMC2 4W-EXT	AMC2 4R4
Czytniki/wejścia			
Maks. liczba czytników na AMC	4	8	8
Maks. liczba czytników na interfejs/szynę	1	1	8

Tabela 1.1: Ograniczenia systemu – czytniki i wejścia**System wizyjny – ograniczenia i opcje**

- Maks. 128 kamer
- Maksymalnie 5 kamer na wejście
 - 1 kamera identyfikacyjna
 - 2 kamery monitorujące strefę tylną
 - 2 kamery monitorujące strefę przednią
 - Jedną z tych kamer można skonfigurować jako kamerę alarmową i rejestracyjną.

System blokowania offline (OLS) – ograniczenia i opcje

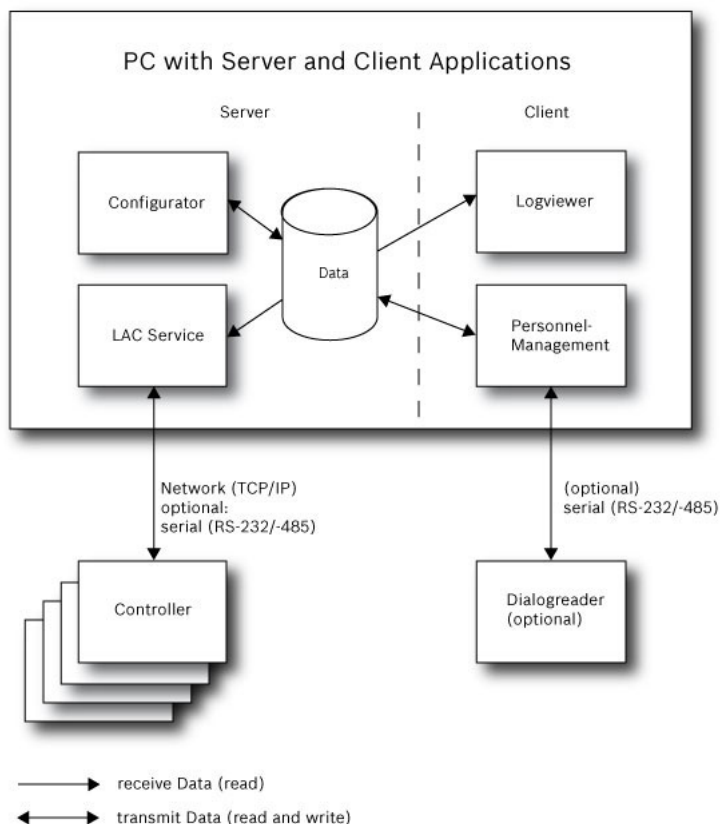
- Maks. 256 drzwi
- Liczba wejść i grup uprawnień dostępu w uprawnieniach zależy od długości zestawu danych, które można zapisać na kartach.
- Maks. 15 modeli czasowych
- Do 4 okresów na model czasowy
- Maks. 10 dni specjalnych/świąt (z systemu online)
- Funkcja OLS dotyczy jedynie karty numer 1.

**Uwaga!**

Urządzenia USB podłączone do pulpitu zdalnego jako np. czytniki rejestracji nie są obsługiwane.

1.2 Instalacja na pojedynczym komputerze

Na poniższym rysunku pokazano kompletny system Access PE zainstalowany na pojedynczym komputerze. Kontrolery mogą być dołączane za pośrednictwem interfejsu szeregowego. Jeżeli stosowany jest czytnik dialogowy, podłączany jest on również za pośrednictwem interfejsu szeregowego.



Rysunek 1.1: Status systemu – konfiguracja z pojedynczym komputerem

1.3 Instalacja na wielu komputerach

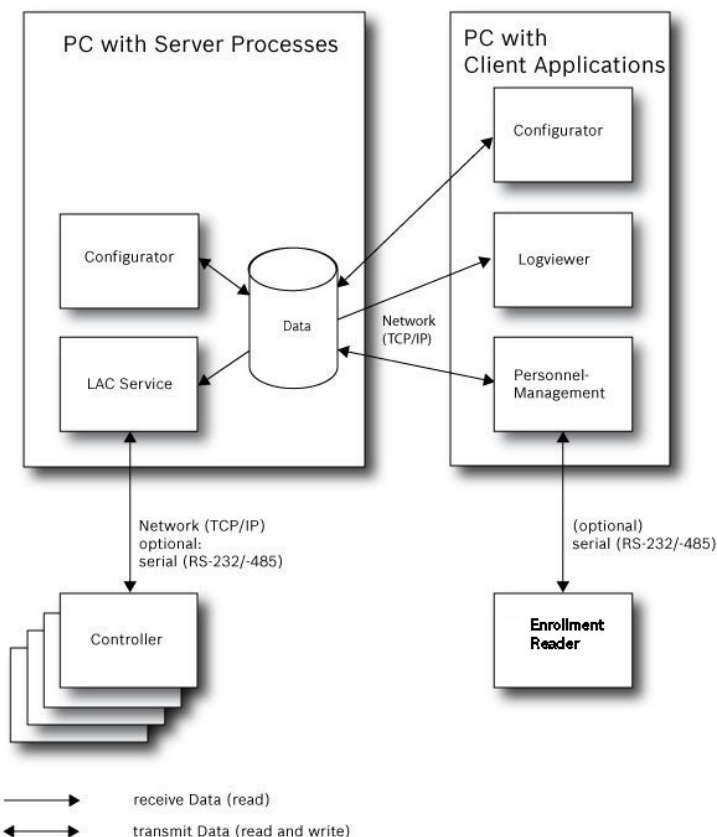
Na poniższym rysunku pokazano system Access PE podzielony na dwa komputery. Jest to szczególnie korzystne w przypadkach, kiedy serwer obsługujący kontrolery znajduje się w zamkniętym pomieszczeniu komputerowym, ale dane personelu są przetwarzane gdzie indziej, na przykład przez dział personalny znajdujący się w innym miejscu. Klient Access PE może zostać zainstalowany na maks. 16 komputerach, które mają za pośrednictwem sieci dostęp do wspólnych danych na serwerze.

Klienckie stacje robocze można skonfigurować w taki sposób, aby używały dwóch monitorów. Pozycje okien są zachowywane przez system operacyjny; podczas sesji logowania należy zapewnić znane operatorowi środowisko.

Uwaga!



Po wybraniu opcji **Odinstaluj w celu aktualizacji** należy upewnić się, że wszystkie pliki zostały usunięte z folderu. : \\BOSCH\Access Professional Edition z wyjątkiem folderu **SaveData**.



Rysunek 1.2: Przegląd systemu – system podzielony

1.4 Wymagania wstępne dla systemu

Wymagania dotyczące instalacji systemu Access PE:

Systemy operacyjne (jeden z wymienionych):

- Windows 10 X64 Professional
- Windows 2008 R2
- Windows 2008 Server
- Windows 7

**Uwaga!**

Oprogramowanie Access Professional Edition w wersji 3.1 i wyższych nie jest kompatybilne z żadną wersją systemu Microsoft Windows XP.

Wymagania sprzętowe

Serwer i klient wymagają standardowego komputera PC z systemem Windows i następującym wyposażeniem:

- Procesor 4 GHz
- Pamięć RAM min. 4 GB
- 20 GB wolnego miejsca na dysku (serwer)
- 1 GB wolnego miejsca na dysku (klient)
- Karta sieciowa 100 Mbit Ethernet (PCI)
- Karta graficzna o rozdzielczości 1024 × 768 obsługująca 32 tys. kolorów
- Obsługiwane rozdzielczości:
 - 1024 × 768
 - 1280 × 1024
 - 2048 × 768
 - 2560 × 1024
- Napęd CD/DVD-ROM
- Moduły rozszerzeń we/wy
- Klawiatura i mysz USB

1.5 Komputer jednopłytowy

Oprogramowanie Access Professional Edition (APE) można uruchamiać na **komputerze jednopłytowym (SBC, Single-Board Bomputer)**.

Zasadniczo możliwości **komputera SBC**, takiego jak Intel Compute Stick STK1AW32SC, lub innego sprzętu niższej klasy mogą **nie spełniać wymagań wstępnych systemu** dotyczących oprogramowania Access Professional Edition (zob. rozdział 1.4).

Uwaga!

Komputera SBC można używać tylko w przypadku, gdy sieć LAN lub WIFI oraz podłączony sprzęt są stale dostępne.



Komputer SBC należy skonfigurować przy użyciu ograniczonego zestawu funkcji, jak to określono dla **licencji podstawowej** (maksymalnie 16 czynników).

W związku z niską wydajnością sprzętu podłączonego bezprzewodowo komputera SBC **nie** należy używać z funkcjami **Zarządzanie alarmami** i **Zarządzanie wideo**, ponieważ dla tych funkcji podstawowe znaczenie ma stabilność sieci.

Oprogramowanie APE zostało przetestowane na następującym urządzeniu, które może służyć jako punkt odniesienia, jeśli chodzi o minimalne wymagania systemu pozwalające na korzystanie z licencji podstawowej:

Intel Compute Stick STK1AW32SC

Nazwa produktu	Intel BOXSTCK1A32WFCR
Wymiary	147 x 89 x 0,7 mm
Marka procesora	Intel Atom x5-Z8-300, 4x1,44 GHz
Rozmiar pamięci RAM	2 GB

Nazwa produktu	Intel BOXSTCK1A32WFCR
Technologia pamięci	DDR3L
Typ pamięci komputera	DDR3 SDRAM
Rozmiar dysku twardego	32 GB
Napięcie	1,35 V
Moc	4 W
Źródło zasilania	USB
System operacyjny	Windows 10

Warunki wstępne w systemie operacyjnym Windows

W przypadku pracy ze sprzętem niższej klasy, np. komputerem SBC, zaleca się określenie następujących ustawień i warunków wstępnych właściwych dla sprzętu i systemu operacyjnego, aby zapewnić bezproblemowe działanie oprogramowania APE:

- Należy używać stałych adresów IP.
- Należy wyłączyć wszystkie opcje oszczędzania energii.
 - Należy wybrać plan zasilania dla dużej wydajności.
 - Należy wyłączyć opcje oszczędzania energii w ustawieniach USB.
- Należy wyłączyć funkcje hibernacji.
- Należy wyłączyć automatyczne aktualizacje systemu operacyjnego Windows.
- W przypadku niestabilnego połączenia WiFi należy zastosować kartę USB Ethernet.
- Należy upewnić się, że rozdzielczość ekranu odpowiada wymaganiom sprzętowym komputera SBC. W przypadku urządzenia testowanego przykładowo zalecaną rozdzielczością jest 1920x1080.
- Należy upewnić się, że jest dostępna wystarczająca ilość pamięci. Zaleca się 5 GB wolnej pamięci na instalację systemu operacyjnego i oprogramowania APE. W przypadku

braku wystarczającej ilości pamięci wewnętrznej należy użyć zewnętrznego dysku twardego lub zastosować do komputera SBC kartę microSD.

- Należy regularnie tworzyć dyski CD odzyskiwania systemu Windows i zapisywać punkty wejścia.



Uwaga!

W przypadku korzystania z komputera jedнопłytkowego (SBC) tworzenie dysków CD odzyskiwania i używanie punktów wejścia może być niemożliwe.

2 Informacje ogólne

2.1 Wstęp

Access PE to system kontroli dostępu, który został zaprojektowany z myślą o nadzorowaniu małych i dużych obiektów o wysokich wymaganiach w zakresie bezpieczeństwa i elastyczności.

Swą dużą niezawodność oraz możliwości w zakresie rozbudowy Access PE zawdzięcza koncepcji trzech platform: nadrzędną platformą jest platforma administracyjna wraz z usługami kontrolnymi. Na tej płaszczyźnie wykonywane są wszystkie zadania administracyjne, jak na przykład rejestracja nowych kart oraz przydzielanie uprawnień dostępu.

Druga platforma tworzona jest przez lokalne kontrolery dostępu (LAC) nadzorujące każdą grupę drzwi lub wejść. Nawet jeśli system jest w trybie offline, moduł LAC jest zdolny do niezależnego podejmowania decyzji w zakresie kontroli dostępu. Moduły LAC są odpowiedzialne za prawidłowy przebieg procedur na przejściach, nadzorują np. czas otwarcia drzwi lub pytają o kod PIN przy wejściach o znaczeniu krytycznym.

Trzecia platforma składa się z czytników kart identyfikacyjnych, które, podobnie jak kontrolery, są identyczne we wszystkich punktach kontroli dostępu firmy BOSCH. Zapewniają one nie tylko bardzo wysoki poziom bezpieczeństwa, lecz umożliwiają również nieskomplikowane rozszerzenie systemu przy jednoczesnym zachowaniu dotychczasowych komponentów.

Wersja wielostanowiskowa oprogramowania Access PE umożliwia kontrolowanie systemu z różnych stanowisk.

Zróznicowane poziomy uprawnień regulują dostęp użytkowników do systemu i są gwarancją bezpieczeństwa.

Dlatego też np. na jednym stanowisku można zarządzać kartami, a na innym skontrolować, czy dany pracownik jest obecny w budynku.

System Access PE umożliwia niezwykle elastyczną konfigurację uprawnień dostępu, modeli czasowych oraz parametrów wejść. Poniższe zestawienie stanowi przegląd najważniejszych funkcji:

Szybkie i łatwe przydzielanie kart identyfikacyjnych

Przydzielenie karty (do trzech) danej osobie odbywa się poprzez wprowadzenie danych ręcznie lub za pośrednictwem czytnika cyfrowego, połączonego z komputerem za pomocą interfejsu szeregowego. Wszystkie przypisane karty są aktywne. W przypadku wymiany karty identyfikacyjnej stara karta zostaje automatycznie zastąpiona nową i traci swoją ważność; dzięki temu nie zdarzy się sytuacja, że stara karta, która przez nieuwagę lub z powodu niemożności anulowania nie została dezaktywowana, będzie nadal wykorzystywana.

Uprawnienia dostępu (również dla grup)

Jedna osoba może otrzymać zarówno uprawnienia grupowe, jak i uprawnienia indywidualne. Uprawnienia można ograniczyć co do obszaru jak i czasowo, z dokładnością co do minuty.

Uprawnienia grupowe można wykorzystać do przydzielania i ograniczania uprawnień dostępu dla dowolnego posiadacza identyfikatora lub dla wszystkich posiadaczy jednocześnie.

Uprawnienia grupowe mogą zostać uzależnione od modeli czasowych, ograniczających ich działanie do wybranych godzin w ciągu dnia.

Śledzenie dostępu

Dzięki definiowaniu stref można nadzorować i wymuszać prawidłową kolejność przejść. Nawet bez monitorowania, za pomocą tej konfiguracji można wyświetlić miejsce przebywania posiadacza karty.

Funkcja zapobiegająca przekazaniu karty osobie niepowołanej

Jeśli dana karta została odczytana, wówczas przez określony czas nie może być ponownie użyta w tym samym przejściu. Dzięki temu użytkownik po przejściu bramki nie będzie mógł przekazać swojej karty nieuprawnionej osobie, umożliwiając w ten sposób niedozwolone przejście.

Automatyczna blokada kart po upływie terminu ważności

Goście oraz pracownicy tymczasowi często wymagają dostępu tylko przez ograniczony czas.

Wystawiając kartę można określić jej okres ważności. Po upływie terminu karta automatycznie traci ważność.

Modele czasowe i modele dzienne

Każdej osobie można przydzielić modele czasowe, które decydują o tym, w jakim czasie wstęp jest dozwolony. Modele czasowe można zdefiniować elastycznie, przydzielając modele dzienne określające, które dni tygodnia, weekendy, dni świąteczne i dni specjalne różnią się od dni normalnych.

Identyfikacja na podstawie kodu PIN

Zamiast karty można używać specjalnego kodu PIN, który należy wprowadzić.

Weryfikacja za pomocą kodu PIN

Dla obszarów ściśle chronionych można zdefiniować konieczność wprowadzenia dodatkowych kodów PIN. Funkcję tą można także połączyć z modelami czasowymi, np. aby podanie kodu PIN wymagane było wyłącznie poza godzinami pracy lub w dni wolne.

Elastyczne zarządzanie drzwiami

Elastyczne przydzielanie parametrów do poszczególnych modeli drzwi zapewnia optymalną równowagę między bezpieczeństwem i komfortem. Dla każdego wejścia można zdefiniować czas otwarcia, zanim alarm zostanie uruchomiony. Wbudowana instalacja alarmowa może, opcjonalnie, zablokować przejście.

Okresowe otwarcie drzwi

Dla ułatwienia dostępu wybrane drzwi można na określony czas ustawić w trybie stałego zezwolenia. Takie zezwolenie może być przydzielone ręcznie lub automatycznie za pośrednictwem modelu czasowego.

Czas i udział

Punktom dostępu można przyporządkować parametry zapisu czasu wejścia oraz wyjścia pracowników w celu kontroli czasu pracy.

Tworzenie karty

Dzięki dodatkowemu modułowi o nazwie **Personalizacja kart** (CP) system kontroli dostępu zintegrowano z oprogramowaniem do wystawiania kart identyfikacyjnych, co umożliwia operatorowi tworzenie takich kart bez przełączania się do innych aplikacji.

Przypisywanie zdjęć

Jeśli moduł dodatkowy **Personalizacja kart** (CP) nie został aktywowany, nie można importować i przypisywać identyfikatora fotograficznego do posiadacza karty.

System blokowania offline

Strefy nieobjęte, z jakiegokolwiek powodu, systemem kontroli dostępu online o wysokiej dostępności mogą być blokowane w trybie offline.

Zarządzanie urządzeniami wizyjnymi

Wejścia można dodatkowo wyposażać w kamery do identyfikacji i śledzenia ruchów osób, które z tych wejść korzystają.

2.2 Logowanie użytkownika

- Aplikacje użytkownika można uruchomić za pomocą ikon pulpitu:



Zarządzanie personelem



Konfigurator



Analiza dziennika



Zarządzanie mapami i alarmami



Weryfikacja wideo

lub wybierając narzędzia za pośrednictwem poleceń **Start > Programy > Access Professional Edition**

- Aplikację **Zarządzanie mapami i alarmami** można



uruchomić za pomocą ikony na pulpicie lub wybierając kolejno **Start > Programy > Access Professional Edition > Map & Alarm Management**.

- Aplikację **Weryfikacja wideo** można uruchomić za pomocą



ikony na pulpicie lub wybierając kolejno **Start > Programy > Access Professional Edition > Weryfikacja wideo**.

- Aplikację **Konfigurator** można uruchomić za pomocą ikony



na pulpicie lub wybierając kolejno **Start > Programy > Access Professional Edition > Konfigurator**.

- Aplikację **Analiza dziennika** można uruchomić za pomocą



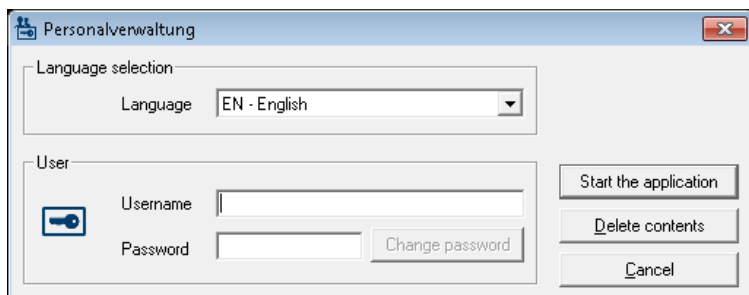
ikony na pulpicie lub wybierając kolejno **Start > Programy > Access Professional Edition > Analiza dziennika**.

- Aplikację **Zarządzanie personelem** można uruchomić za



pomocą ikony na pulpicie lub wybierając kolejno
Start > Programy > Access Professional Edition > Zarządzanie personelem.

Aplikacje systemu są chronione przed nieuprawnionym użyciem. Aby uzyskać dostęp do funkcji, należy wpisać prawidłowe dane w polu **nazwa użytkownika** oraz **hasło**.



Górnej listy rozwijanej można użyć do wybrania wymaganego **języka**. Domyślny jest język zastosowany podczas instalowania aplikacji. W przypadku zmiany użytkownika bez restartowania aplikacji zachowany zostanie ostatnio używany język. Z tego powodu okno logowania może wyświetlić się w innym języku. Aby tego uniknąć należy ponownie zalogować się w Access PE. Aplikacje Access PE mogą zostać uruchomione w następujących językach:

- angielski
- niemiecki
- rosyjski
- polski
- chiński (PRC)
- holenderski
- hiszpański

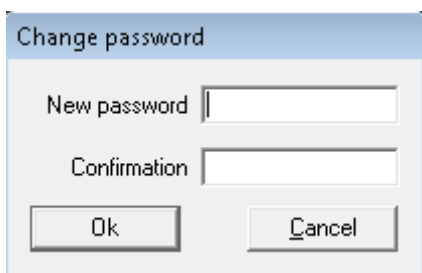
– portugalski (Brazylia)

Uwaga!



Wszystkie ustawienia, tj. nazwy urządzeń, etykiety, modele oraz uprawnienia będą wyświetlane w języku, w którym zostały przygotowane. Również przyciski i etykiety obsługiwane przez system operacyjny mogą być wyświetlane w języku tego systemu.

Po wpisaniu prawidłowych danych w polach nazwy użytkownika i hasła uaktywni się przycisk **Zmień hasło**. Można dzięki niemu utworzyć nowe okno dialogowe umożliwiające zmianę hasła.



Z kolei użycie przycisku **Uruchom aplikację** powoduje skontrolowanie uprawnień użytkownika i ewentualnie otwarcie aplikacji. Jeśli kontrola uprawnień wypadnie negatywnie, zostanie wyświetlony komunikat o błędzie **Nieprawidłowa nazwa użytkownika lub hasło!**.

Logowanie przez aplikację Zarządzanie personelem

Jeśli użytkownik zalogował się już w programie Zarządzanie personelem Access PE i posiada uprawnienia umożliwiające dostęp do innych narzędzi, może uruchomić aplikacje **Analiza dziennika**, **Konfigurator**, **Zarządzanie alarmami** i **Weryfikacja wideo**, korzystając z przycisków na pasku narzędzi.

Jeśli użytkownik zalogował się już w programie **Zarządzanie personelem** Access PE i posiada uprawnienia umożliwiające dostęp do aplikacji **Analiza dziennika**, może bezpośrednio za



pomocą przycisku , dostępnego na pasku narzędzi, wywołać funkcję **analizy dziennika** bez konieczności ponownego logowania do aplikacji Analiza dziennika.

Jeśli użytkownik zalogował się już w programie **Zarządzanie personelem** Access PE i posiada uprawnienia umożliwiające dostęp do aplikacji **Konfigurator**, może bezpośrednio za pomocą



przycisku , dostępnego na pasku narzędzi, wywołać funkcję **konfiguratora** bez konieczności ponownego logowania do aplikacji Konfigurator.

Jeśli użytkownik zalogował się już w programie **Zarządzanie personelem** Access PE i posiada uprawnienia umożliwiające dostęp do aplikacji **Weryfikacja wideo**, może bezpośrednio za



pomocą przycisku , dostępnego na pasku narzędzi, wywołać funkcję **weryfikacji wideo** bez konieczności ponownego logowania do aplikacji Konfigurator.

Jeśli użytkownik zalogował się już w programie **Zarządzanie personelem** Access PE i posiada uprawnienia umożliwiające dostęp do aplikacji **Zarządzanie alarmami**, może bezpośrednio




za pomocą przycisku , dostępnego na pasku narzędzi, wywołać funkcję **zarządzania alarmami** bez konieczności ponownego logowania do aplikacji Konfigurator.








2.3 Menu i pasek narzędzi







Poniższe funkcje można wywołać za pomocą menu, ikon na pasku narzędzi lub specjalnych kombinacji klawiszy.

Funkcja	Ikona/ Skrót	Opis
Menu Plik		
Nowy	 Crtl + N	Usuwa wszystkie dane z okien dialogowych konfiguracji (oprócz ustawień standardowych), przygotowując je do nowej konfiguracji.
Otwórz...	 Crtl + O	Otwiera okno dialogowe wyboru w celu pobrania innej konfiguracji.
Zapisz	 Crtl + S	Zapisuje zmiany do bieżącego pliku konfiguracji.
Zapisz jako...		Zapisuje bieżącą konfigurację do nowego pliku.
Aktywuj konfigurację		Aktywuje pobraną konfigurację i zapisuje tę dotychczas aktywną.
Wyślij konfigurację do LAC		Przesyła zapisane zmiany konfiguracji do usługi LAC.

Funkcja	Ikona/ Skrót	Opis
Pokaż konfiguracje ostatnio aktywne		Otwiera konfiguracje bezpośrednio, bez konieczności korzystania z okna dialogowego funkcji Otwórz .
Zakończ		Zamyka aplikację Access PE Configurator.

Funkcja	Ikona/ Skrót	Opis
Menu Widok		
Pasek narzędzi		Wyświetla lub ukrywa pasek narzędzi (ustawienie domyślne = wyświetlanie).
Pasek stanu		Wyświetla lub ukrywa pasek stanu przy dolnej krawędzi okna dialogowego (ustawienie domyślne = wyświetlanie).
Menu Konfiguracja		
Informacje ogólne		Otwiera okno dialogowe Ustawienia ogólne do konfigurowania kontrolerów i ustawiania ogólnych parametrów systemu.
Sygnały wejściowe		Otwiera okno dialogowe do ustawiania parametrów sygnałów wejściowych .

Funkcja	Ikona/ Skrót	Opis
Sygnały wyjściowe		Otwiera okno dialogowe do ustawiania parametrów sygnałów wyjściowych .
Wejścia		Otwiera okno dialogowe Wejścia do ustawiania parametrów drzwi i czytników kart.
Strefy		Otwiera okno dialogowe Konfiguracja obszaru do podzielenia zabezpieczonej instalacji na strefy wirtualne.
Wakacje		Otwiera okno dialogowe Wakacje do zdefiniowania dni wolnych od pracy i dni specjalnych.
Modele dzienne		Otwiera okno dialogowe Modele dzienne do utworzenia okresów czasowych danego dnia w celu aktywowania określonych funkcji dostępu.
Modele czasowe		Otwiera okno dialogowe Modele czasowe do zdefiniowania stref czasowych zależnych od dnia tygodnia lub kalendarza.
Grupy personelu		Otwiera okno dialogowe Grupy personelu do dzielenia personelu na logiczne grupy.

Funkcja	Ikona/ Skrót	Opis
Grupy uprawnień dostępu		Otwiera okno dialogowe Grupy uprawnień dostępu do tworzenia grup z uprawnieniami do wejścia.
System blokowania offline		Otwiera okno dialogowe System blokowania offline na potrzeby konfiguracji specjalnych elementów instalacji (wejścia, modele czasowe, grupy uprawnień dostępu).
Wyświetlane teksty		Otwiera okno dialogowe Wyświetlane teksty do edycji tekstów wyświetlanych na czytnikach kart.
Komunikaty dziennika		Otwiera okno dialogowe Komunikaty dziennika do edycji i kategoryzacji komunikatów dziennika.
Dodatkowe pola danych osobowych		Otwiera okno dialogowe Dodatkowe pola danych osobowych do definiowania pól danych dla personelu.
Karty Wiegand		Otwiera okno dialogowe Karty Wiegand do definiowania struktury danych na karcie identyfikacyjnej.

Funkcja	Ikona/ Skrót	Opis
Zarządzanie urządzeniami wizyjnymi		Otwiera okno dialogowe Urządzenia wizyjne do konfigurowania kamer w taki sposób, aby mogły być wykorzystywane do weryfikacji wideo.
Przeglądanie map i zarządzanie alarmami		Otwiera przeglądarkę map z widokiem obszarów map i urządzeń sterujących, a także listą alarmów do obsługi.
Menu ? Pomoc		
Tematy pomocy		Otwiera ten plik pomocy.
Informacje o Konfiguratorze Access Professional Edition		Wyświetla informacje ogólne o aplikacji Konfiguratorze Access Professional Edition.

2.4 Ogólne ustawienia systemu

Ogólne ustawienia systemu wyświetlane są poniżej listy ustawień kontrolera. Ustawienia te dotyczą wszystkich instalacji.

Default card data

Country code Customer code

LAC subsystem process

Poll interval on serial connected LAC in ms

Read-timeout on serial connected LAC in ms

Create TA-data at

☐ Export personnel and TA data

☐ Show welcome/leaving message

☐ Show cardholder name in display

PIN code

Number of digits Number of retries before blocking

☐ use separate IDS pin

Logbook parameter

Number of files (one logfile per day, 0 = unlimited)

Directories

Database

Event log

Import files ...

Export files ...

DLL-files

Pictures ...

Test logs

Parametr	Domyślne	Opis
Kod kraju	00	Części danych karty identyfikacyjnej dodawane są do wprowadzonego ręcznie numeru karty.
Kod klienta	056720	
Czas zwłoki szeregowo podłączonego kontrolera LAC w ms	200	Wyrażenie w milisekundach przedziału czasowego, w którym usługa LAC sprawdza kontroler w celu weryfikacji nienaruszalności łącza.
Ograniczenie czasowe odczytu z szeregowo podłączonego kontrolera LAC w ms	500	Zakres wartości dla czasu zwłoki: od 1 do 500 Dostępne wartości ograniczenia czasowego odczytu: od 1 do 3000
Utwórz dane czasowe o godz.	00:01	Godzina, o której utworzony ma zostać plik z zapisem czasu i udziału.

Parametr	Domyślne	Opis
Eksport danych osobowych i zdarzeń w czasie	nieaktywne	Jeśli ta opcja jest aktywna, powoduje zapisywanie danych czasu i udziału w sposób ciągły do pliku eksportu. Jeśli nie jest aktywna, plik danych tworzony jest w czasie określonym parametrem Utwórz dane czasowe o godz.
<p>Plik zawierający sygnatury czasowe udziału tworzony jest w katalogu: C:\Program Files\Bosch\Access Professional Edition\PE\Data\Export Pod nazwą TA_<bieżąca data RRRRMMDD>.dat</p>		
Wyświetl tekst powitalny/pożegnalny	aktywne	W przypadku odpowiedniego typu i ustawień czytnika (Przybycie, Wyjście lub Sprawdzenie poprawności w oknie dialogowym Wejścia) czytnik wyświetli teksty powitalne/pożegnalne, które zapisane zostały dla posiadacza karty w oknie dialogowym Dane osobowe aplikacji Zarządzanie personelem. Nie dotyczy czytników Wiegand.
Pokaż nazwę posiadacza karty na czytniku	aktywne	W przypadku czytników posiadających wyświetlacz pole Wyświetlana nazwa będzie zgodne z zapisem w danych osobowych posiadacza karty. Nie dotyczy czytników Wiegand.

Parametr	Domyślne	Opis
Liczba cyfr	4	Określa liczbę cyfr wymaganych przez kod weryfikacyjny PIN lub kod uzbrojenia PIN. To ustawienie stosuje się także do kodu PIN drzwi, który można ustawić podczas konfigurowania wejść. Możliwe wartości: od 4 do 8
należy użyć oddzielnego kodu PIN systemu sygnalizacji włamania		Jeśli nie ustawiono oddzielnego kodu PIN systemu sygnalizacji włamania, wówczas do uzbrojenia systemu sygnalizacji włamania można użyć kodu weryfikacyjnego PIN. Pola do wprowadzania kodu uzbrojenia PIN w oknie dialogowym danych osobowych stają się aktywne tylko w przypadku zaznaczenia pola wyboru. W tym przypadku nie można już użyć kodu weryfikacyjnego PIN do uzbrojenia systemu sygnalizacji włamania.

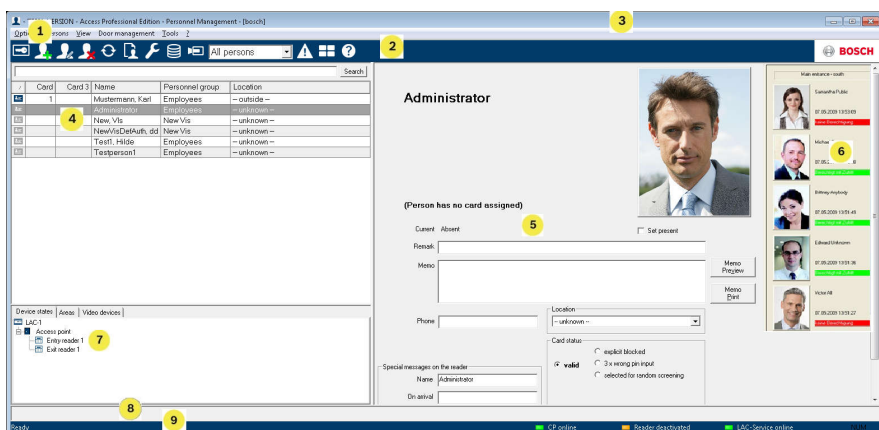
Parametr	Domyślne	Opis
Liczba prób przed zablokowaniem	3	Liczba nieudanych prób wprowadzenia kodu PIN. Jeśli posiadacz karty błędnie wprowadzi kod PIN określoną ilość razy, spowoduje to zablokowanie karty w całym systemie. Blokada może zostać usunięta przez upoważnionego użytkownika systemu (Zarządzanie personelem). Możliwe wartości: od 1 do 9
Parametr dziennika	366	Liczba dzienników na dzień Możliwe wartości: od 180 do 9999
Ścieżki katalogów do: Baza danych Plik rejestru Pliki importu Pliki eksportu Pliki DLL Dane obrazów Logowanie testowe	C:\Program Files \BOSCH \Access Professiona l Edition\PE \Data... \Db \MsgLog \Import \Export \Dll \Pictures \Log	Są to ścieżki domyślne. Katalogi dla plików importu, eksportu i obrazów mogą zostać zmienione.

**Uwaga!**

W przypadku używania kontrolerów i czytników Wiegand, aby użyć kodu PIN identyfikacyjnego, uzbrojenia lub drzwi, należy aktywować definicję karty Wiegand **PIN lub karta** (Nr 6).

2.5 Układ okna dialogowego

Okno dialogowe składa się z następujących elementów:



- 1 = **Pasek menu** – zawiera funkcje okna dialogowego, wyświetlane zgodnie z porządkiem menu.
- 2 = **Pasek narzędzi** – klawisze skrótu dla najważniejszych funkcji okna dialogowego.
- 3 = **Pasek tytułu** – odpowiada standardowi Windows i zawiera przyciski do minimalizacji lub zamykania okna dialogowego. Nazwa zalogowanego użytkownika jest widoczna w kwadratowym nawiasie.
- 4 = **Tabela osób** – wyświetla listę osób ujętych w systemie wraz z ich statusem uczestnictwa (uprawnienia i miejsce).



- 5 = **Pole dialogowe** — przy pierwszym otwarciu tego pola lub gdy żaden użytkownik nie jest zalogowany, widoczny jest neutralny obraz (mapa świata). Po wybraniu hasła z listy osób wyświetlone zostaną dane tej osoby.
- 6 = **Karty użyte online** — wymienia pięć ostatnich osób (wraz z ich obrazem z bazy danych), które przesunęły swoje karty w czytnikach przy wybranych wejściach.
- 7 = **Stan urządzenia** — lista skonfigurowanych urządzeń i wejść oraz ich stan połączenia. Udostępnia funkcje sterowania drzwiami.
- 8 = **Wyświetlanie zdarzeń** — awarie są sygnalizowane przez świecący czerwony pasek (świeci trzy razy) zawierający szczegóły wyjaśniające przyczynę.
- 9 = **Pasek stanu** — wyświetla informacje o przyciskach i pozycjach menu obsługiwanych przy pomocy kursora. Wskazanie stanu programu do personalizacji kart (CP), czytników z wyświetlaczem oraz usług LAC.


Aktywowanie komponentu **Weryfikacja wideo** spowoduje dodanie nowych funkcji do tego okna dialogowego; patrz Personnel Management (Zarządzanie personelem).




Aktywowanie komponentu **Weryfikacja wideo** spowoduje dodanie nowych funkcji do tego okna dialogowego.





2.6 Menu i pasek narzędzi

Poniższe funkcje są dostępne za pośrednictwem menu oraz przycisków na pasku narzędzi.

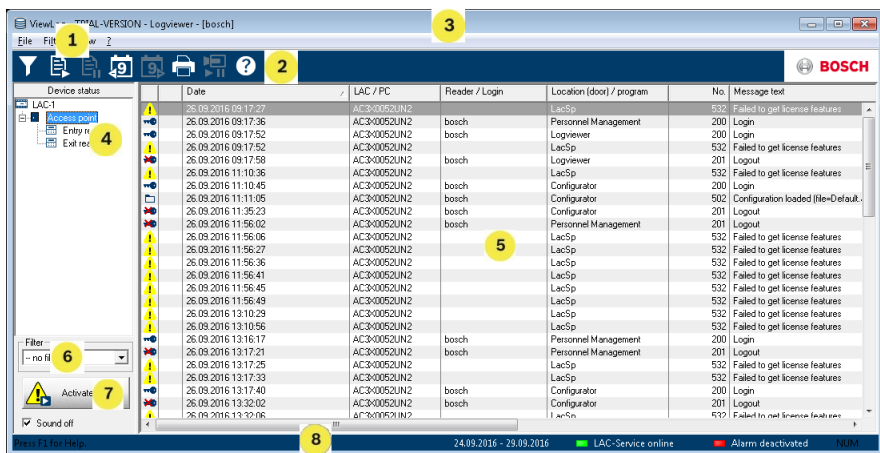
Funkcja	Ikona	Opis
Menu Opcje		
Odśwież		Aktualizuje listę osób.
Zakończ		Zamyka aplikację Access PE – Zarządzanie personelem.
Menu Osoby		
Nowa osoba		Otwiera okno dialogowe danych osobowych i kart identyfikacyjnych z pustymi polami.
Edytuj osobę		Otwiera okno dialogowe danych osobowych i kart identyfikacyjnych z danymi wybranej osoby.
Usuń osobę		Usuwa zaznaczoną osobę po potwierdzeniu wyświetlonego zapytania.
Wyślij wybraną osobę do usługi LAC		Wysyła dane wybranej osoby do usługi LAC i raportuje powodzenie.
Wyślij wszystkie osoby do usługi LAC		Wysyła dane wszystkich osób do usługi LAC i raportuje powodzenie.
Ustaw nieobecność wszystkich osób		Po potwierdzeniu wyświetlonego zapytania ustawia nieobecność wszystkich osób.

Funkcja	Ikona	Opis
Ustaw lokalizację wszystkich obecnych jako nieznana		Ustawia lokalizację wszystkich osób jako nieznana i dezaktywuje śledzenie dostępu dla następnych zgłoszeń każdej z tych osób.
Przeglądaj/drukuj raporty		Otwiera okno dialogowe z funkcją tworzenia list raportów.
	Sterowanie listami	Ogranicza wyświetlanie osób na liście do wybranych grup personelu.
Menu Widok		
Pasek narzędzi		Wyświetla lub ukrywa pasek narzędzi. Wartość domyślna = włączony.
Pasek stanu		Wyświetla lub ukrywa pasek stanu. Wartość domyślna = włączony.
Dane osobowe: Stan Numer karty Numer personalny Firma Grupa personelu Telefon Lokalizacja		Wybór kolumn, które zostaną dodatkowo wyświetlone w przeglądzie osób obok kolumn symbolów i nazw. Domyślnie = Stan – Firma – Lokalizacja
Menu Zarządzanie drzwiami		

Funkcja	Ikona	Opis
Otwórz drzwi	Te funkcje są również	Zaznaczone na liście urządzeń wejście zostanie wyświetlone i może zostać otwarte (jednorazowo).
Otwórz na stałe	ż dostępne w menu	Zaznaczone na liście urządzeń wejście zostanie wyświetlone i może zostać otwarte (na stałe).
Zamknij drzwi	kontekstowym (prawy klawisz myszy) poszczególnych drzwi/wejść.	Zaznaczone na liście urządzeń wejście zostanie wyświetlone i może zostać zamknięte.
Menu Narzędzia		
Logowanie użytkownika		Zarządzanie personelem – logowanie/wylogowywanie.
Uruchom Konfigurator		Uruchamia aplikację Konfigurator i przesyła do niej dane z aplikacji zarządzania personelem.
Uruchom analizę dziennika		Uruchamia aplikację Analiza dziennika i przesyła do niej dane z aplikacji zarządzania personelem.

Funkcja	Ikona	Opis
Uruchom weryfikację wideo		Otwiera aplikację do weryfikacji wideo.
Uruchom zarządzanie alarmami i mapami		Otwiera aplikację Przeglądanie map i zarządzanie alarmami
Panel wideo		Pokazuje w oknie dialogowym cztery ekrany odpowiadające poszczególnym sygnałom wizyjnym z kamer.
Właściwości		Otwiera okno dialogowe do ustawiania parametrów ogólnych systemu.
Menu ? (Pomoc)		
Tematy pomocy		Otwiera ten plik pomocy.
Informacje o Access Professional Edition – Zarządzanie personelem		Otwiera okno informacyjne dotyczące aplikacji Zarządzanie personelem.

2.7 Układ okna dialogowego









- 1 = **Pasek menu** – zawiera funkcje okna dialogowego, dostępne w poszczególnych menu.
- 2 = **Pasek narzędzi** – zawiera najważniejsze funkcje okna dialogowego w formie przycisków.
- 3 = **Pasek tytułu** – odpowiada standardowi Windows i zawiera przyciski do minimalizacji lub zamykania okna dialogowego. W kwadratowym nawiasie wyświetlana jest nazwa zalogowanego użytkownika.
- 4 = **Stan urządzenia** – lista skonfigurowanych urządzeń i wejść oraz ich stan połączenia.
- 5 = **Lista komunikatów** – lista zgłoszonych komunikatów. Wskazanie może być ograniczone przez niektóre ustawienia filtrów.
- 6 = **Wybór filtra** – lista wyboru, zawiera zdefiniowane i zachowane filtry, umożliwiając ich ustawienie.

- 7 = **Aktywacja alarmu** – umożliwia aktywację/dezaktywację alarmu dla komunikatów. Pojawieniu się komunikatu może dodatkowo towarzyszyć sygnał akustyczny.
- 8 = **Pasek stanu** – informacje o datach otwartych dzienników. Status usługi LAC. Ustawienia alarmu.

2.8 Menu i paski narzędzi

Następujące funkcje do analizy dziennika dostępne są w menu oraz przyciskach na pasku narzędzi.

Menu	Funkcja	Przycisk	Opis
Plik	Drukuj...		Drukowanie wyświetlonych komunikatów dziennika.
	Zakończ		Zamyka okno dialogowe analizy dziennika.
Filtr	Definicja filtra		Otwiera okno dialogowe filtrowania komunikatów.

Menu	Funkcja	Przycisk	Opis
	Pokazuj komunikaty na bieżąco		Aktywuje bieżące wskazanie aktualnych komunikatów. Przycisk ten jest aktywny tylko wtedy, gdy funkcja nie jest włączona, a filtr komunikatu obejmuje aktualny dzień. Domyślnym ustawieniem jest bieżące wskazanie aktualnych komunikatów.
	Wyłącz wskazywanie komunikatów na bieżąco		Przerywa bieżące wskazanie aktualnych komunikatów. Przycisk ten jest aktywny tylko wtedy, gdy włączone jest wskazywanie komunikatów na bieżąco.
	Komunikaty poprzedniego dnia		Przejdź do komunikatów z dnia poprzedniego.
	Komunikaty następnego dnia		Przejdź do komunikatów z dnia następnego.

Menu	Funkcja	Przycisk	Opis
Widok	Pasek narzędzi		Ukrywa/wyświetla pasek narzędzi. Wartość domyślna = włączony
	Pasek stanu		Ukrywa/wyświetla pasek stanu. Wartość domyślna = włączony
bez pozycji z menu			
			
			
? Pomoc	Tematy pomocy		Otwiera ten plik pomocy.
	Informacje o Analizie dziennika		Otwiera okno informacji o aplikacji Informacje o Analizie dziennika.

2.9 Konfiguracja rejestracji

Za pośrednictwem menu **Czytniki rejestracji (RS232) > Narzędzia > Ustawienia** można wywołać okno dialogowe umożliwiające wykonanie podstawowej konfiguracji (aktywacja, modyfikacja) z dowolnej stacji roboczej.

- Administracyjne stanowiska pracy, na których przydzielane są karty identyfikacyjne, można wyposażać w czytnik rejestracji. Czytnik należy skonfigurować zgodnie z informacjami od producenta lub na podstawie danych

dostarczonych wraz z produktem. Jeśli czytnik rejestracji jest już skonfigurowany, funkcja ręcznego wprowadzania danych będzie dezaktywowana.

Poniżej podano wymagane ustawienia dla obsługiwanych czytników:

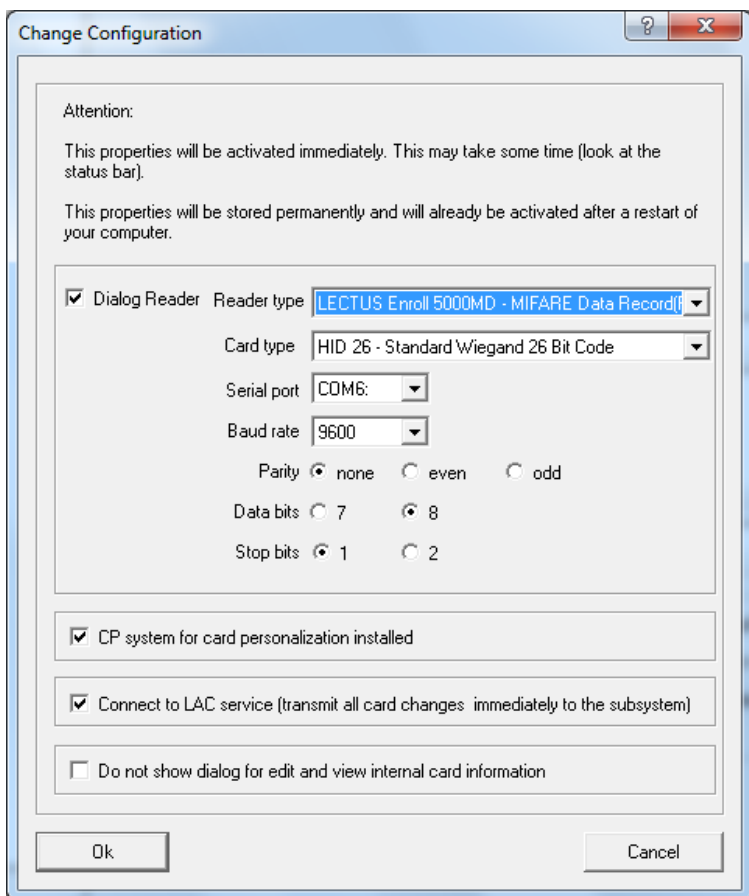
Nazwa czytnika	Szybkość transmisji	D	P	S
DELTA 1200 Prox RS232	9600	8	N	1
DELTA 1200 iClass RS232	57600	8	E	1
DELTA 1200 USB Hitag, Legic, Mifare	9600	8	N	1
DELTA 1200 RS232 Hitag, Legic, Mifare	19200	8	N	1
Rosslare ARD-1200EM USB	9600	8	N	1
LECTUS secure 5000 WI	9600	8	N	1

D =	Bity danych	N =	brak
P =	Parzystość	E =	parzyste
S =	Bity stopu	O =	nieparzyste

**Uwaga!**

Czytniki Delta 1200 Series i Rosslare ARD-1200EM Series nie zostały ocenione przez firmę UL.

- **Chip card system** (System kart chipowych)
Wyświetla technologię kart – w przypadku Access PE można używać MIFARE classic oraz Hitag1.



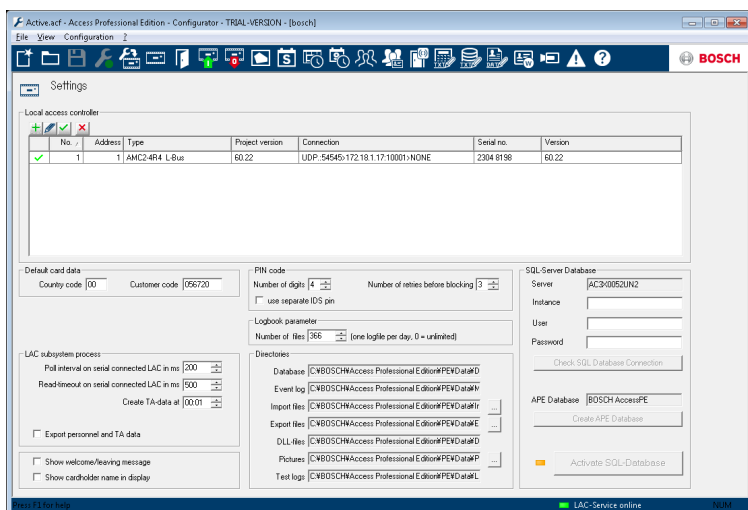
- Jeśli system został zainstalowany wraz z opcjonalnym programem do wystawiania kart **Personalizacja kart** (CP), połączenie z tym programem jest zaznaczone w ustawieniach. Dezaktywacja tej opcji zablokuje wszystkie funkcje związane z wystawianiem kart.
- Dodatkowo zaznaczone jest automatyczne przesyłanie danych osobowych przez **Połączenie z serwerem LAC**. To pole wyboru powinno być zawsze zaznaczone.

- W tym miejscu można wyłączyć wyświetlanie informacji o karcie podczas przypisywania kart. To ustawienie jest niezbędne tylko wtedy, gdy istnieją odstępstwa od ustawień domyślnych (zob. Ustawienia ogólne w aplikacji Konfigurator Access PE) i niektóre karty identyfikacyjne muszą otrzymać inne dane.

2.9.1 Rejestracja za pomocą czytników podłączonych do kontrolera AMC

Upewnij się, że przynajmniej jeden czytnik jest skonfigurowany za pomocą opcji **Model drzwi 06c**, który jest modelem drzwi do rejestracji.

Uruchom **Konfigurator** i wybierz **LAC** (np. AMC2...)



Kliknij symbol **Wejścia**, aby dodać nowy czytnik wejścia:

Define Entrance

Description:


Please configure LAC, GID and doormodel



LAC: GID:

Door model:








☐ Video verification Surv. camera: [Video configuration](#)

Reader configuration

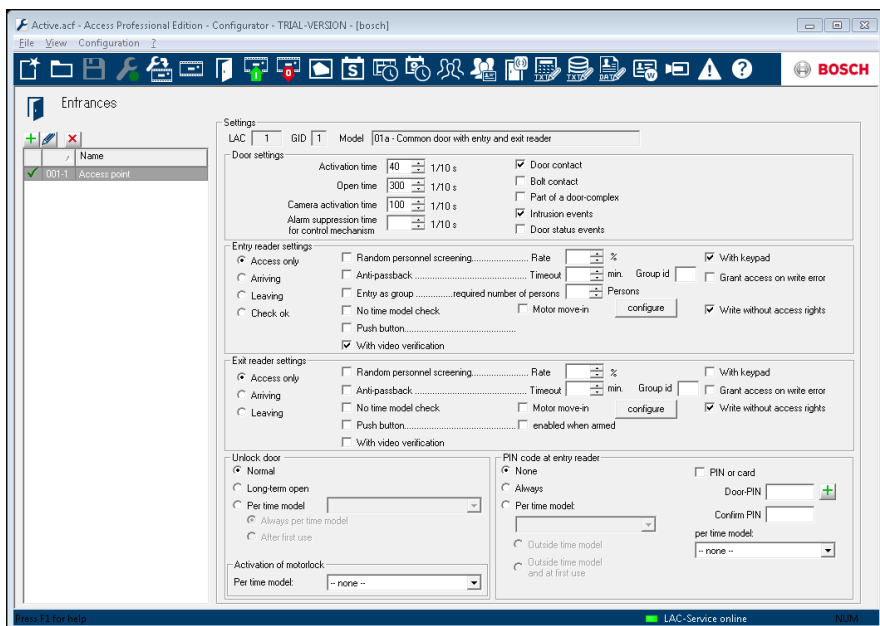
Access-reader: Reader type: Address:  Write access:

 Device data from cache  Search device data

Signal definition

	Signal description	On dev...	GID / Board	DID	Connection
	Door sensor				
	Pushbutton: Door open				
	Boltsensor				
	Entrance locked				
	Sabotage signal				
	Local Open Enable				
	Door opener				

Zostanie otwarte okno dialogowe **Definiuj wejście**:



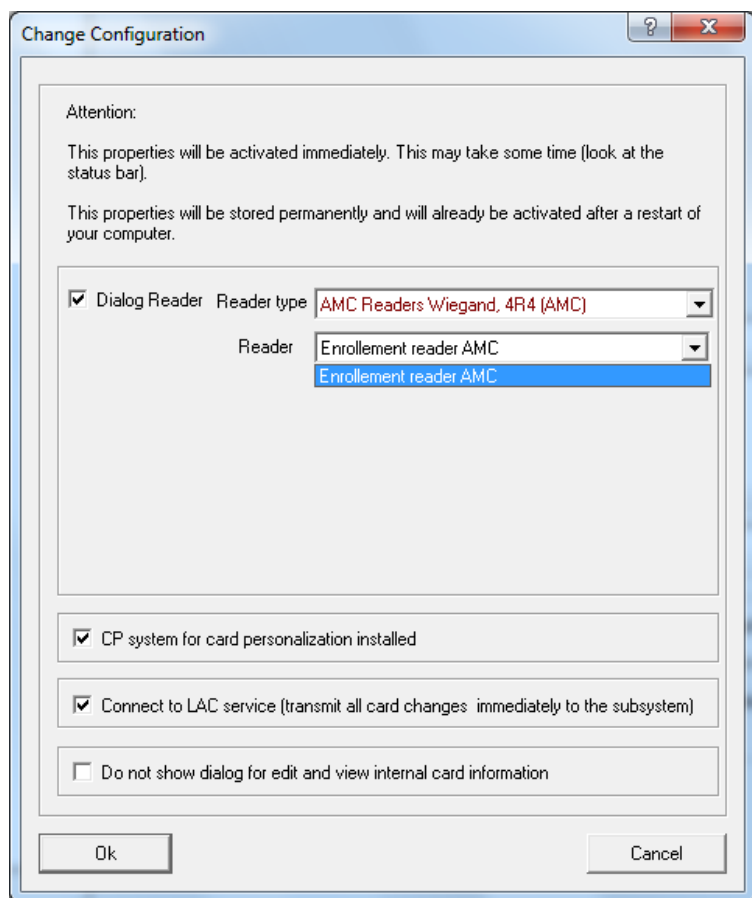
W tym oknie dialogowym można:

- Wprowadzić opis (np. Enrollment Reader AMC)
- Wybrać LAC i ID grupy (GID)
- Wybrać typ czytnika (np. Wiegand)
- Wybrać numer od 1 do 8 jako Adres czytnika dostępu

Kliknij OK, aby potwierdzić konfigurację rejestracji.

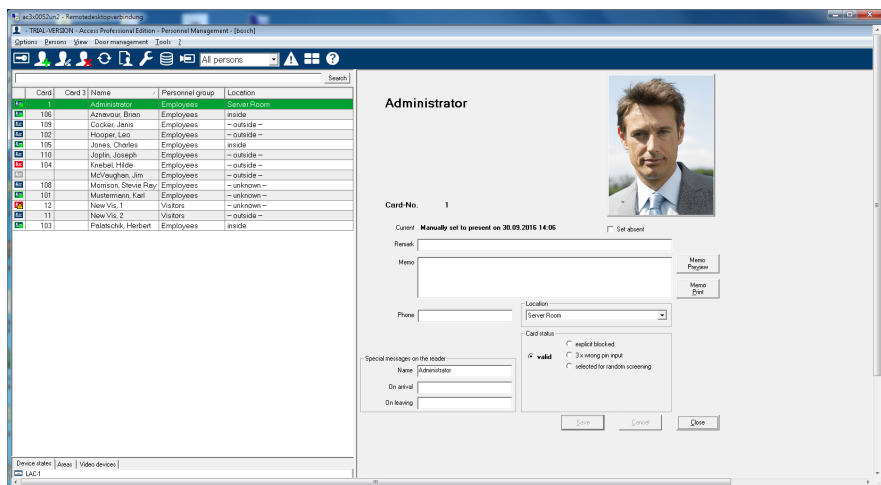
Aby przypisać konfigurację czytnika do konkretnej stacji roboczej, należy przejść do ustawień klienta APE.

- Narzędzia > Właściwości.



Aby aktywować proces rejestracji, wybierz dostępny czytnik rejestracji.

Upewnij się, że wybrany czytnik rejestracji jest w trybie online. Jeżeli nie będzie natychmiastowej reakcji, ponownie uruchom okno dialogowe Zarządzanie personelem.



2.10 Obsługa serwera SQL

Wszystkie dane zapisane w dzienniku zdarzeń mogą być również przechowywane w bazie danych SQL. Jako materiał referencyjny może posłużyć wersja systemu Microsoft® SQLServer® 2014 edycja Express, SP 1x 64 zainstalowana w systemie Windows 10 x64 Pro.

Połączenie z serwerem SQL można skonfigurować w prawej dolnej części ekranu **Ustawienia**.

Szczegółowe informacje można znaleźć w podręczniku instalacji.



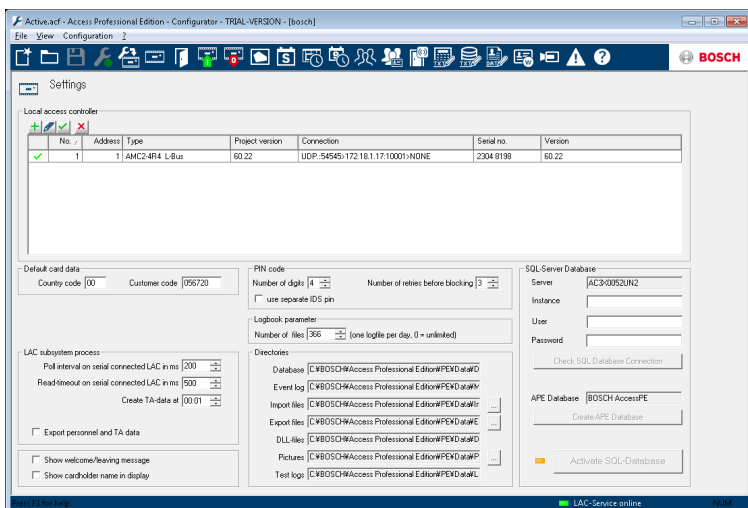
Uwaga!

Bazę danych SQL należy zainstalować na tej samej maszynie fizycznej lub wirtualnej co serwer APE.

Uwaga!

W celu konfiguracji bazy danych SQL należy uruchomić Konfigurator na komputerze z serwerem APE.

W tym przypadku nie należy uruchamiać Konfiguratora na kliencie.



- Identyfikator instancji bazy danych należy wpisać w polu **Instancja**.
- Jeśli wymagane są dane uwierzytelniające, należy wpisać **Nazwę użytkownika i Hasło**.
- Kliknij przycisk Sprawdź **połączenie z bazą danych SQL**.
- Jeżeli serwer bazy danych APE jeszcze nie istnieje, kliknij **Utwórz bazę danych APE**.

Sprawdź połączenie z bazą danych SQL

SQL-Server Database

Server AC3X0013BT1

Instance SQLExpress

User

Password

Check SQL Database Connection

APE Database BOSCH AccessPE

Create APE Database

Activate SQL-Database

LAC-Service online NUM RF

Zmień nazwę nowego ważnego identyfikatora instancji. Sprawia, że nowa baza danych APE jest tworzona w określonej instancji.

Jeżeli baza danych APE już istnieje lub została właśnie utworzona, kliknij opcję **Aktywuj bazę danych SQL**.

Przy aktualizacji do wersji APE przy użyciu bazy danych SQL system nie importuje istniejących danych dziennika.

Po przekroczeniu limitu 100 000 wiadomości system przerwie buforowanie zdarzeń. Po przywróceniu usługi SQL buforowane wiadomości zostaną dodane do bazy danych SQL. Bufor wiadomości nie jest zawarty w kopii zapasowej systemu APE.

Uwaga!

Użytkownik odpowiada za konserwację bazy danych, tj. usuwanie starych wpisów, aktualizację oprogramowania SQL itp.

Uwaga!

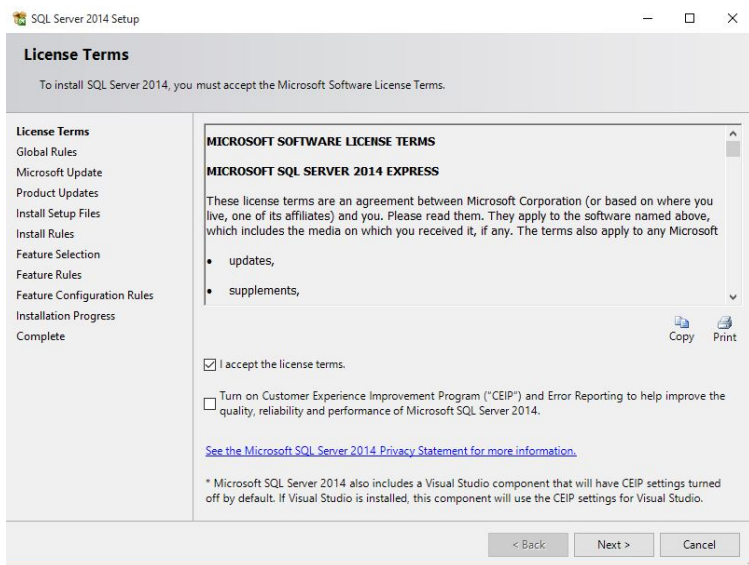
Usługę bazy danych SQL można włączyć lub wyłączyć. Jeśli usługa jest wyłączona, pole komunikatu systemu Windows poinformuje o tym użytkownika.

2.11 Instalacja bazy danych SQL

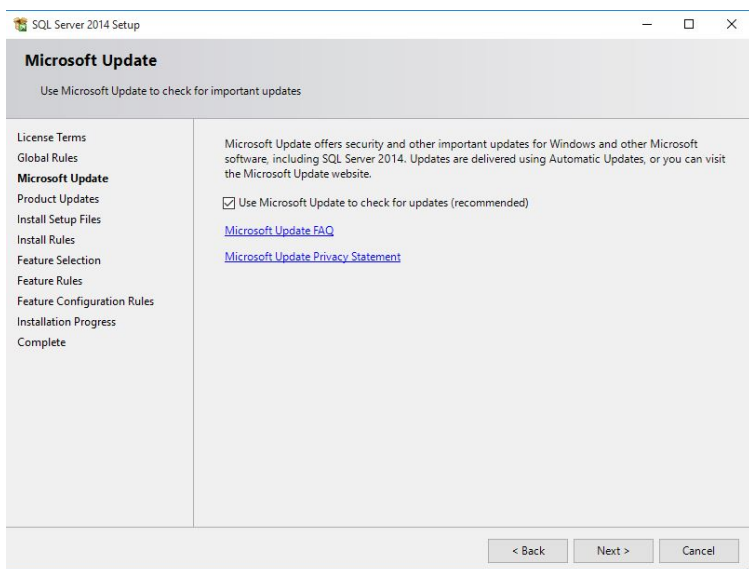
Pobierz **Microsoft® SQL Server® 2014 SP1 edycja Express** ze strony głównej firmy Microsoft. Po uruchomieniu aplikacji wyświetla się **Centrum instalacji serwera SQL**. Wybierz opcję **Instalacja**.



- Wybierz opcję **Nowy serwer SQL**.
Wybierz **warunki umowy licencyjnej**.

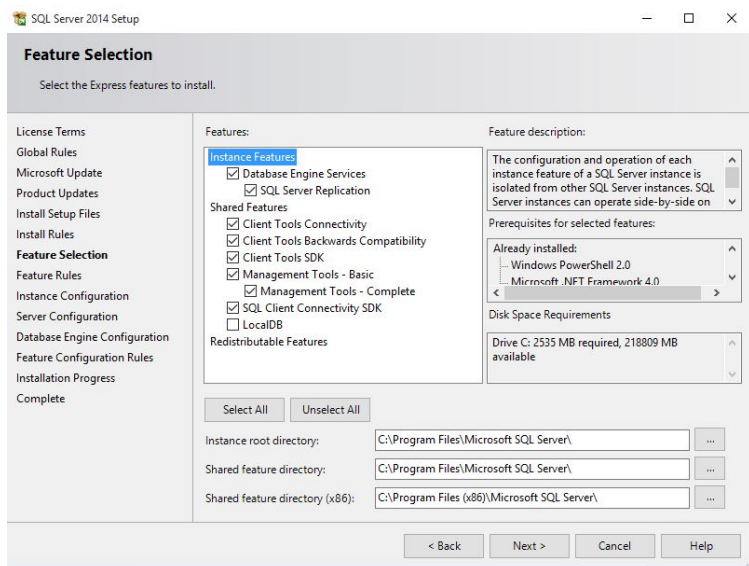


- Zaakceptuj warunki umowy licencyjnej i kliknij **Dalej >**, aby kontynuować.
- Wybierz usługę **Microsoft Update**.

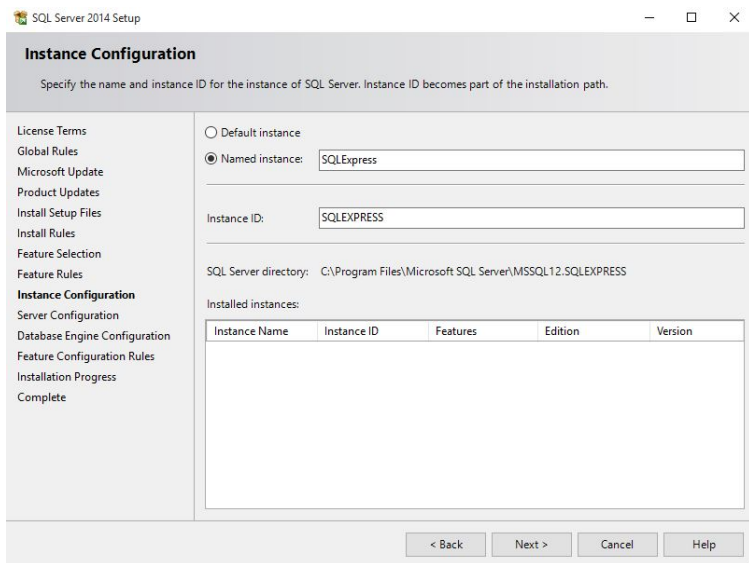


- Wybierz opcję **Sprawdź dostępność aktualizacji w usłudze Microsoft Update**, a następnie kliknij **Dalej >**, aby kontynuować.

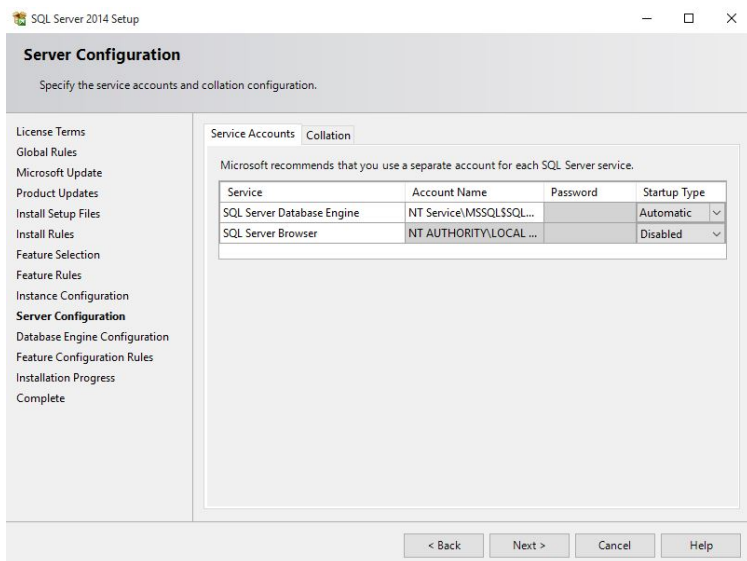
Wybierz opcję **Wybór funkcji**.



- Zaznacz na liście wybrane **Funkcje** i kliknij **Dalej >**, aby kontynuować.
- Wybierz opcję **Konfiguracja instancji**.

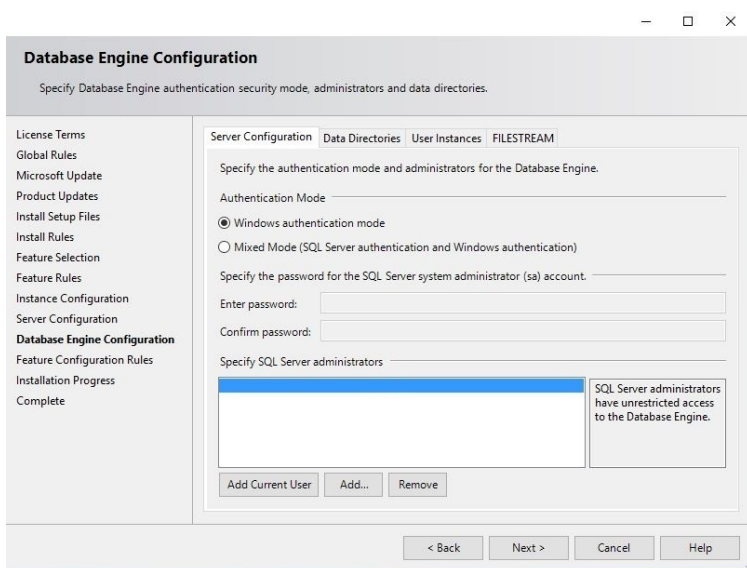


- Wybierz jedno z pól opcji: **Domyślna instancja** lub **Nazwana instancja**.
 - Kliknij przycisk **Dalej**, aby kontynuować.
- Wybierz opcję **Konfiguracja serwera**.



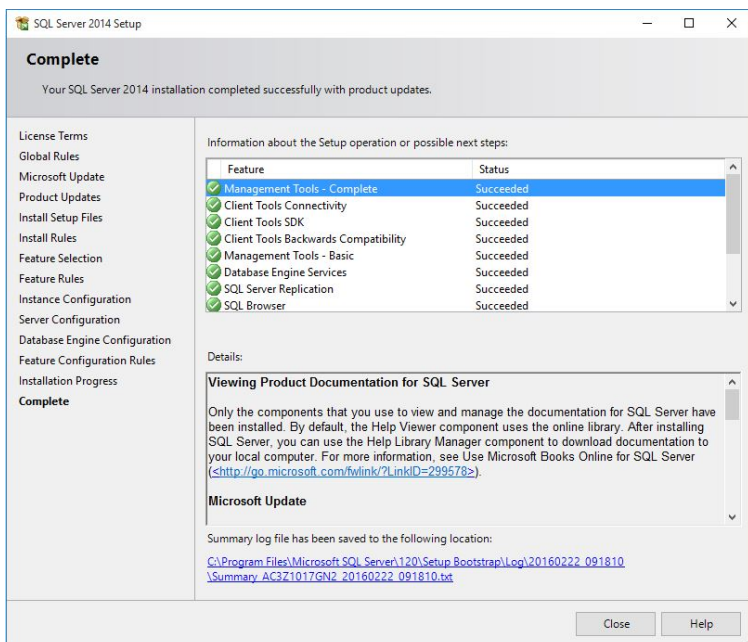
- Wybierz wymagane **Konta usługi** i kliknij **Dalej >**, aby kontynuować.

Wybierz opcję **Konfiguracja silnika bazy danych**.



- Wybierz kartę **Konfiguracja serwera** i aktywuj pole opcji **Tryb uwierzytelniania systemu Windows**.
- Kliknij przycisk **Dalej**, aby kontynuować.

Wybierz opcję **Zakończ** i w kolumnie **Status** sprawdź stan instalacji wymaganych funkcji. Może to potrwać kilka minut.



- Instalacja została zakończona. Aby zakończyć instalację, kliknij przycisk **Zamknij**.



Uwaga!

Jeśli instalacja nie powiodła się, skontaktuj się z działem obsługi klienta firmy Microsoft.

Użytkownik końcowy bazy danych SQL odpowiada za:

- utworzenie danych uwierzytelniających, dających dostęp do bazy danych SQL,

- utworzenie kopii zapasowej serwera SQL, ponieważ system APE nie obsługuje tworzenia kopii zapasowych baz danych SQL,
- zarządzanie bezpieczeństwem serwera SQL.

3 Konfiguracje

Układ systemu (gdzie znajdują się poszczególne wejścia i jakie są to wejścia, ile jest czytników i jakiego typu, w jaki sposób są skonfigurowane uprawnienia dostępu) jest zapisany w specjalnych plikach. Dopuszczalna jest każda ilość takich plików konfiguracyjnych – jednak tylko jeden może mieć zastosowanie do aktualnego systemu. Umożliwia to testowanie nowych scenariuszy, przeprowadzanie próbnych uruchomień i dokonywanie szybkich zmian w systemie.

3.1 Tworzenie nowych konfiguracji

Wszystkie konfiguracje Access PE zapisywane są w katalogu **C:\BOSCH\Access Professional Edition\PE\Data\Cfg** (pod warunkiem, że podczas instalacji wybrano standardowe ścieżki i katalogi). Podczas instalacji tworzone są dwa pliki konfiguracji, mianowicie **Active.acf** i **Default.acf**. Podczas gdy plik **Active.acf** może zawierać kilka przykładowych danych, ułatwiających użytkownikowi konfigurację, w pliku **Default.acf** dostępne są jedynie wstępnie zdefiniowane parametry systemowe.

Parametry systemowe obejmują następujące elementy:

- Strefa pomieszczeń **--outside--** (--poza--).
- Przykładowe święta i dni specjalne
- Grupy personelu **Employees** (Pracownicy) i **Visitors** (Goście)
- Wyświetlane teksty dla czytnika.
- Treść komunikatów dziennika.

Przy uruchamianiu programu Access PE używana jest zawsze konfiguracja **Active.acf**.


Konfiguracja może mieć różne stany i ważne jest rozróżnienie między nimi:

- konfiguracja **Active** (Aktywna) = jej ustawienia, parametry itp., są w tej chwili wykorzystywane przez komponenty systemu;


- konfiguracja **Open** (Otwarta) (także pobrana) = jej ustawienia są w tej chwili edytowane przez użytkowników systemu. Może zostać ona później zapisana w oddzielnym pliku .acf i/lub aktywowana później, ale **dopóki nie zostanie aktywowana, nie ma wpływu na działanie systemu.**

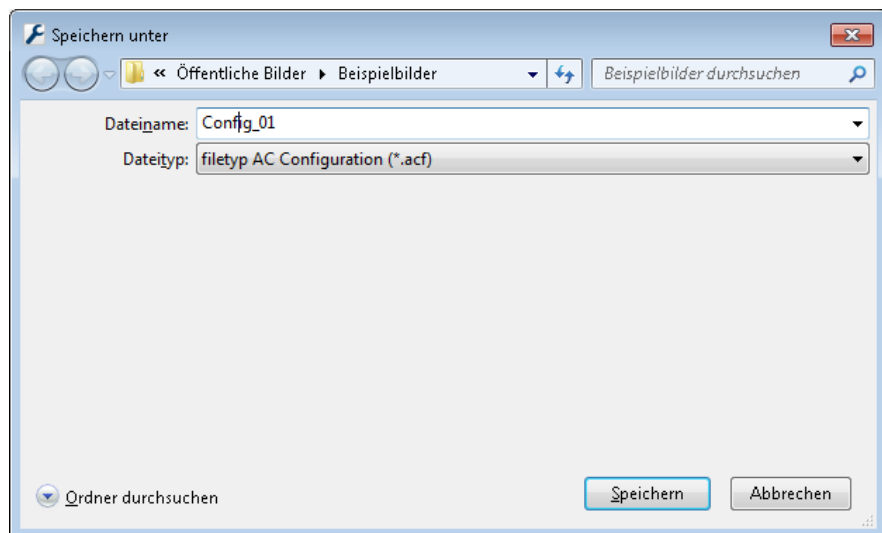
Dla programu Access PE można utworzyć i zapisać dowolną ilość konfiguracji. Ponieważ nowe konfiguracje są tworzone i edytowane niezależnie od bieżącego systemu, istnieje na przykład możliwość definiowania nowych stref, które zostaną włączone w instalację monitorowania w terminie późniejszym.



Po naciśnięciu przycisku  w pasku narzędzi otwarta (wczytana) zostanie konfiguracja domyślna z podstawowymi ustawieniami, zapisana w pliku **Default.acf**. W przypadku modyfikacji tworzącej nową konfigurację należy ją zapisać pod inną i odpowiednią nazwą.



Przycisk  otwiera okno dialogowe zapisu pliku w katalogu Cfg. Domyślna nazwa pliku **untitled.acf** powinna zostać zastąpiona nazwą bardziej opisową.

**Ostrzeżenie!**

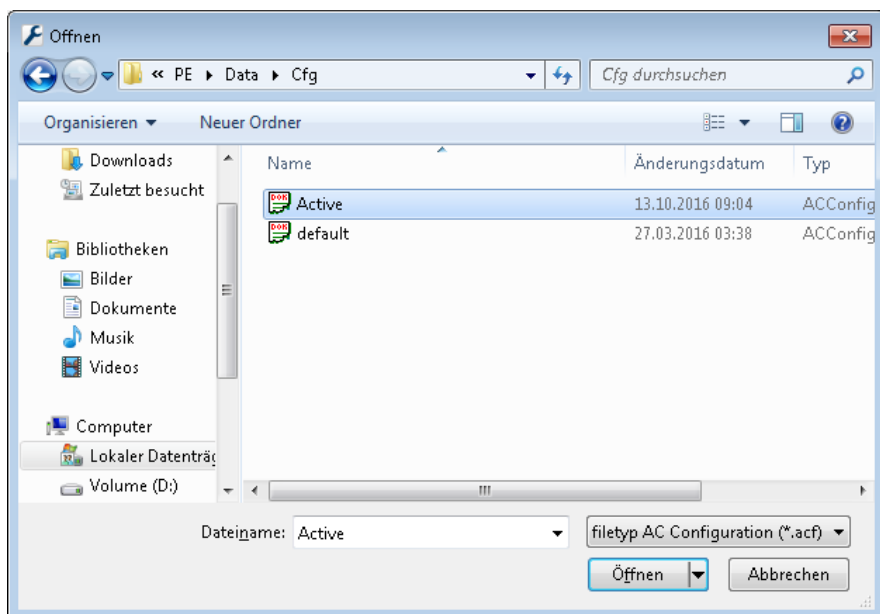
Nazwy plików domyślnych konfiguracji active.acf i default.acf nigdy nie powinny być zmieniane, a pliki nadpisywane. Modyfikacje pliku default.acf zawsze należy zapisywać pod nową nazwą.

3.2 Otwieranie konfiguracji

Konfigurator jest uruchamiany zawsze z konfiguracją **Active.acf**. Jeśli natomiast praca ma się odbywać w innej konfiguracji,



wówczas za pomocą przycisku można otworzyć jedną z istniejących konfiguracji w katalogu **C:\BOSCH\Access Professional Edition\PE\Data\Cfg** (domyślny katalog instalacji).



Jeśli użytkownik chce dokonać zmiany lub rozszerzenia istniejącej konfiguracji bez ich aktywowania, może otworzyć konfigurację bazową, zmodyfikować ją, a następnie zapisać pod inną nazwą. W ten sposób można ponownie wykorzystywać i rozszerzyć istniejące już elementy konfiguracji bez konieczności rozpoczynania za każdym razem od podstawowych ustawień zawartych w pliku **default.acf**.

**Uwaga!**

Aktywną konfigurację można też zapisać pod inną nazwą, tworząc tym samym jej kopię, którą można potem pobrać i przetworzyć.

3.3 Aktywacja nowej konfiguracji

Konfigurator oferuje możliwość zarządzania wieloma konfiguracjami w różnych plikach .acf. Aktywna konfiguracja dostępna jest zawsze w pliku **Active.acf**.



Przestroga!

Ponieważ podczas aktywowania nowej konfiguracji plik **active.acf** jest nadpisywany, zaleca się wykonanie kopii bezpieczeństwa aktywnej konfiguracji i zapisanie pod inną nazwą pliku.

Aktywować można wyłącznie otwarte pliki konfiguracji. Dlatego poprzednio zmienioną i zapisaną konfigurację należy otworzyć. Aby aktywować nową konfigurację, należy wykonać następujące czynności:

- Menu: **File > Activate configuration** (Plik > Aktywuj konfigurację) lub



- naciśnij przycisk na pasku narzędzi.

Aktywacja otwartej konfiguracji odbywa się w trzech etapach:

- Najpierw potwierdzenie wyświetlonego zapytania bezpieczeństwa:

Do you really want to replace the current configuration with the new configuration? (Czy na pewno chcesz zastąpić bieżącą konfigurację nową konfiguracją?)

- Aktywna w tym momencie konfiguracja zostanie zapisana w pliku kopii bezpieczeństwa o nazwie: **\$rrrrMMddggmmss - Active.acf** (r = rok; M = miesiąc; d = dzień; g = godzina; m = minuta; s = sekundy).
- Otwarta konfiguracja zostanie zapisana pod nazwą **Active.acf**, tzn. stara konfiguracja zostanie zastąpiona nową!

Okno informacyjne pokaże nazwę zapisanego pliku: **New configuration was saved as <filename>!** (Nowa konfiguracja została zapisana jako <nazwapliku>!)

3.4 Przesyłanie konfiguracji do kontrolerów

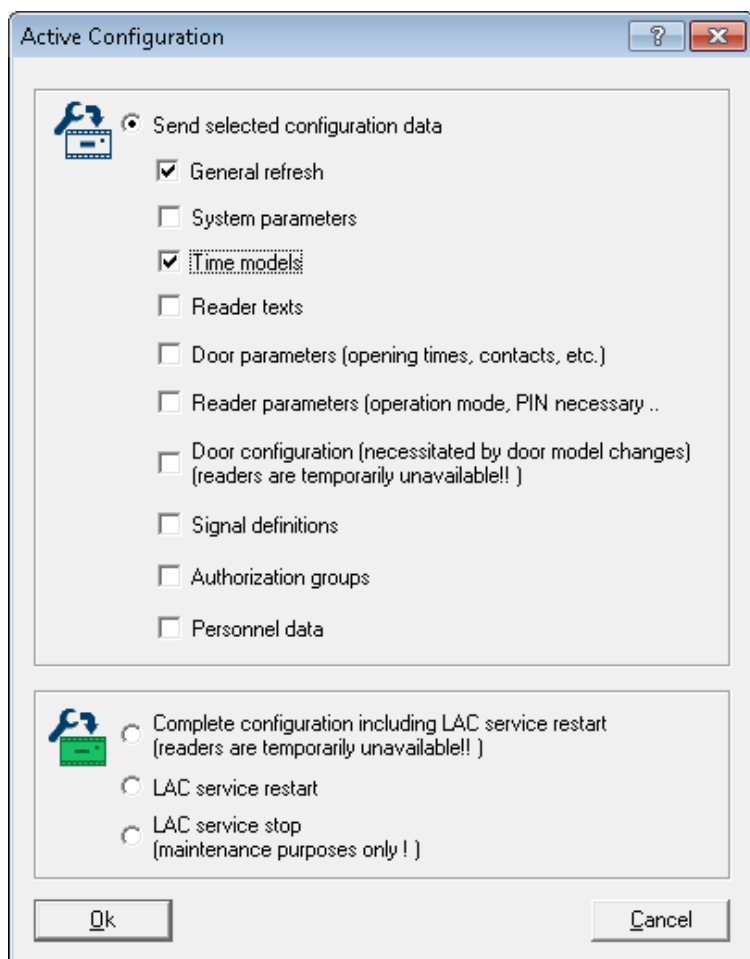
Po dokonaniu zmian w aktywnej konfiguracji **Active.acf** należy przesłać te zmiany do kontrolerów. Można to zrobić w dwojaki sposób:

- menu **File** (Plik) > **Send configuration to LAC service** (Wyślij konfigurację do LAC);



- korzystając z przycisku  w pasku narzędzi.

W wyświetlonym następnie oknie (patrz poniżej) można określić, które zmiany zostaną przesłane do kontrolerów.



Zmienione i zachowane dane są tutaj wstępnie selekcjonowane. Można wybierać dodatkowe pozycje lub usuwać zaznaczenia pól wyboru.

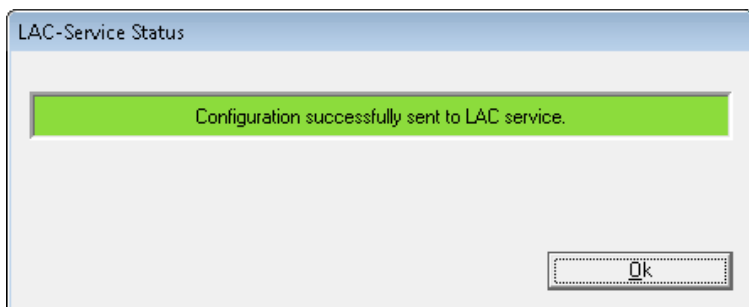
Po wybraniu elementów, które trafią do kontrolerów, należy potwierdzić wybór przyciskiem **OK**.

Dane konfiguracji	Wysłanie do kontrolerów LAC jest konieczne w następujących sytuacjach:
General refresh (Zmiany ogólne)	... zmieniono komunikaty dziennika, dodatkowe pola lub definicje kart identyfikacyjnych.
System parameters (Parametry systemu)	... sprzęt LAC uległ zmianie.
Modele czasowe	... zostały zmienione dni świąteczne, modele dzienne lub czasowe.
Reader texts (Teksty czytnika)	... zmieniono wyświetlane teksty.
Door parameters (Parametry drzwi)	... w opcjach wejść zmieniono jedną lub więcej z poniższych pozycji: <ul style="list-style-type: none"> – czas otwarcia (w 1/10 s) – kontaktron drzwiowy – dane dotyczące udostępniania drzwi (czasy otwarcia, kontaktrony, profile czasowe itp.)
Reader parameters (Parametry czytników)	... w opcjach wejść zmieniono jedną lub więcej z poniższych pozycji: <ul style="list-style-type: none"> – dane dla czytników wejścia lub wyjścia – czas wyciszenia alarmu (w 1/10 s). – blokada podwójnego wejścia – przyciski otwarcia drzwi

Dane konfiguracji	Wysłanie do kontrolerów LAC jest konieczne w następujących sytuacjach:
Door configuration (Konfiguracja drzwi)	... w wejściach zostały zmienione modele drzwi. Ostrzeżenie: Wprowadzenia nowych danych lub zmiany adresów (numer seryjny, typ czytnika) można dokonać jedynie w specjalnym oknie Define Entrance (Definiuj wejście).
Signal definitions (Definicje sygnałów)	... zostały zmienione parametry sygnałów wejścia lub wyjścia
Authorization groups (Grupy uprawnień dostępu):	... zostały zmienione grupy uprawnień dostępu bez modelu czasowego lub model czasowy został dodany lub usunięty.
Personnel data (Dane osobowe)	... zostały utworzone nowe dane osobowe lub zmieniono istniejące, bądź też zmieniono grupy uprawnień albo modele czasowe.
Complete configuration including LAC-Services restart (Kompletna konfiguracja – wraz z ponownym uruchomieniem usług LAC)	.. zakończyła się pierwsza konfiguracja oprogramowania Access PE Wyzerowanie kontrolera może również spowodować wczytanie do kontrolerów kompletnej konfiguracji.

Dane konfiguracji	Wysłanie do kontrolerów LAC jest konieczne w następujących sytuacjach:
LAC service restart (Ponowne uruchomienie usług LAC)	... w ustawieniach ogólnych zmieniono czas zwłoki lub czas zapisu danych czasowych.
LAC service stop (Wyłączenie usług LAC)	Tej opcji menu należy używać tylko w sytuacjach wyjątkowych, np. podczas odinstalowywania, aby uniknąć ponownego uruchamiania komputera.

Aplikacja Configurator (Konfigurator) wysyła do **usługi LAC** polecenie przestania danych konfiguracji do kontrolerów. Usługa LAC odpowiada za obustronną komunikację z kontrolerami. Podczas instalacji program ten zostaje skonfigurowany jako usługa systemu Windows, która uruchamia się automatycznie przy uruchamianiu komputera. Zakończone powodzeniem przesyłanie danych do usługi LAC zostanie potwierdzone następująco:





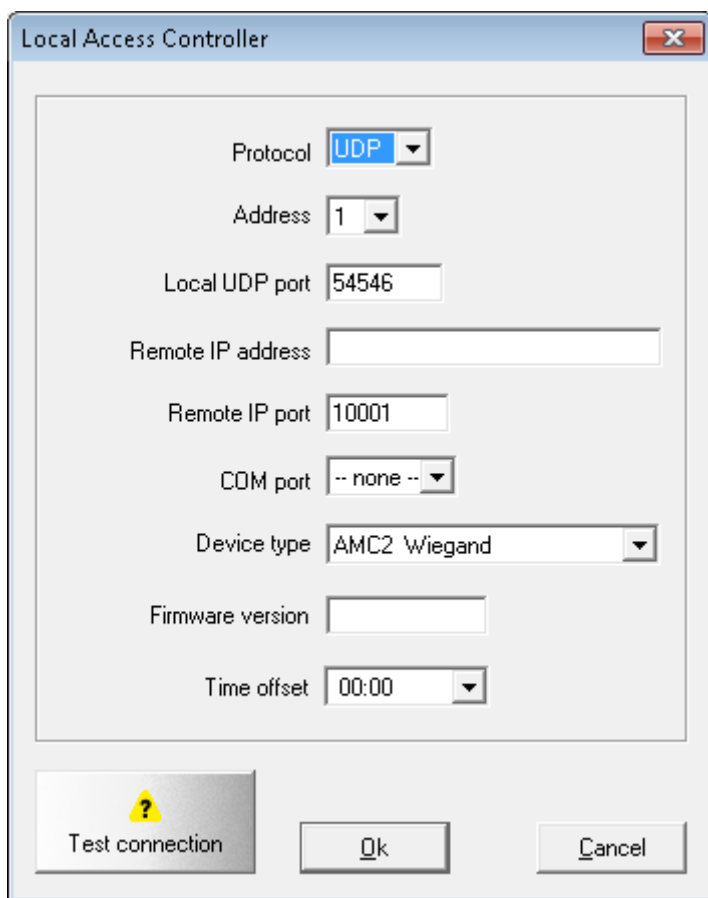
4 Kontrolery

Lokalne kontrolery dostępu (LAC) to punkty w systemie Access PE, w których podejmuje się większość decyzji związanych z kontrolą dostępu. Poza funkcjami sterowania całym systemem, takimi jak sekwencyjna kontrola dostępu, kontrolery mogą podejmować niezależne decyzje dotyczące przyznawania dostępu. Z tego względu, w ich pamięci znajdują się dane związane z dostępem, aby możliwa była także praca w trybie offline, w ograniczonym zakresie.

W systemie Access PE używa się przeważnie kontrolerów AMC2 (Access Modular Controller – Modułowy kontroler dostępu). Jeśli chodzi o zamienniki pochodzące ze starych systemów, można też konfigurować kontrolery LACi (Local Access Controller integral – Lokalny integralny kontroler dostępu).

4.1 Definiowanie i modyfikowanie nowych kontrolerów

Przyciski  (dodaj) i  (modyfikuj element wybrany z listy) otwierają okno dialogowe do konfigurowania interfejsów między serwerem Access PE a kontrolerami.



Local Access Controller

Protocol **UDP**

Address **1**

Local UDP port **54546**

Remote IP address


Remote IP port **10001**

COM port **-- none --**

Device type **AMC2 Wiegand**

Firmware version

Time offset **00:00**

 Test connection

Ok

Cancel

Do każdego kontrolera należy przypisać protokół. Dostępne są następujące ustawienia:

COM	Podłączenie za pośrednictwem szeregowego interfejsu (COM) z podaniem numeru interfejsu COM (COMx)
CIP	Podłączenie za pośrednictwem protokołu TCP/IP z wykorzystaniem interfejsu COM, wymagające numeru (COMx) wirtualnego portu COM; dostępne tylko dla LACi z konwerterem IP/ Szeregowy.
UDP	Podłączenie za pomocą protokołu UDP z podaniem lokalnego portu UDP oraz adresu IP (ewentualnie nazwy sieci w przypadku korzystania z DHCP).



Uwaga!

Należy pamiętać, że przy stosowaniu interfejsów CIP i UDP, przełącznik adresu DIL w kontrolerze na pozycji **5** ustawiony jest na **ON** (WŁ.).

Zależnie od wybranego protokołu wymagane jest wprowadzenie pozostałych danych, zgodnie z następującą tabelą:

Parametr	COM	CIP	UDP	Uwaga
Adres	od 1 do 8	od 1 do 8	zawsze 1	W przypadku parametrów COM oraz CIP przełącznik DIL w kontrolerze musi mieć identyczne ustawienie adresu.
Lokalny port UDP	Nieaktywny	Nieaktywny	kolejny	Port, za pomocą którego serwer Access PE ma otrzymywać informacje z kontrolera. Nowy kontroler otrzyma kolejny wolny port, zależnie od położenia, ale te dane można zmienić.

Parametr	COM	CIP	UDP	Uwaga
Zdalny adres IP	Nieaktywny	Nieaktywny	Adres IP lub nazwa sieci	Jeśli w danej sieci stosowany jest protokół DHCP, należy podać nazwę sieci. W przeciwnym razie wprowadzany jest adres IP kontrolera.
Zdalny port IP	Nieaktywny	Nieaktywny	wartość niezmienialna 10001	Port kontrolera umożliwiający odbiór danych z serwera.
COM-Port	Lista rozwijana portów COM	Lista rozwijana portów COM	<brak>	Numer portu COM serwera Access PE, do którego podłączony jest ten kontroler.
Typ kontrolera LAC	Lista rozwijana kontrolerów	Lista rozwijana kontrolerów	Lista rozwijana kontrolerów	Dostępne są następujące typy kontrolerów:
	AMC-Wiegand			z interfejsem czytnika Wiegand
	AMC-RS485-BG900			z interfejsem czytnika RS485

Parametr	COM	CIP	UDP	Uwaga
	AMC-RS485-L-BUS			z interfejsem czytnika RS485 dla czytnika I-BPR
	AMC-RS485-OSDP			z interfejsem czytnika RS485 dla czytników OSDP
	LACi-BG900			z interfejsem czytnika RS485
	LACi-L-Bus			z interfejsem czytnika RS485 dla czytnika I-BPR
Wersja programu (Projekt)	brak	brak	brak	może być używany do określenia wersji oprogramowania
Przesunięcie czasu	<p>Pole kombi służące do określenia przesunięcia czasu z serwera w przypadku, gdy kontroler AMC znajduje się w innej strefie czasowej.</p> <p>Możliwe wartości to: od -12:00 do +12:00 w 30-minutowych odstępach.</p> <p>Czas przesyłany z serwera do kontrolera AMC (lub odwrotnie) jest korygowany przez to przesunięcie.</p> <p>Lokalny czas kontrolera AMC jest stosowany w komunikatach o zdarzeniach i można go zobaczyć w dzienniku zdarzeń.</p>			

Test kontrolera (LAC)

Wykorzystując wprowadzone wartości, można jeszcze przed zapisem przetestować dostęp do każdego kontrolera. Dzięki temu można szybko i sprawnie skorygować lub uzupełnić błędne dane.

Użycie przycisku **Test LAC** umieszczony przy dolnej krawędzi okna dialogowego powoduje próbę utworzenia połączenia z kontrolerem na bazie wprowadzonych danych. Test ten może być również przeprowadzony po instalacji poprzez wyselekcjonowanie wybranego kontrolera w polu listy i

naciśnięcie przycisku .

Test wyświetla jeden z trzech wyników, za pomocą ikon pokazanych poniżej, które są również widoczne w pierwszej kolumnie listy.



Ten kontroler nie został jeszcze przetestowany.



Test wypadł pozytywnie. Połączenie zostało utworzone.



Test nie powiódł się.



Uwaga!

Ikony pokazują tylko wynik ostatnio przeprowadzonego testu.

Nie są one stale aktualizowanym wskaźnikiem dostępności każdego z kontrolerów.

Test kontrolera składa się z różnych faz, z których część może zostać pominięta:


- Uruchomienie usługi LAC.
- Pobieranie programu LAC.
- Stany oczekiwania:
 - Wczytywanie danych konfiguracji z kontrolera.
 - Odbieranie komunikatu statusu z kontrolera.
- Wyświetlanie wyniku próby uzyskania połączenia.

Zależnie od wyniku, wyświetlane jest okno **LAC-Service Status** (Status usługi LAC). Po kliknięciu przycisku **OK** wynik testu wyświetlany jest na liście.

4.2 Ustawienia kontrolera

W oknie dialogowym **General Settings** (Ustawienia ogólne),



które otwiera przycisk , definiowane i konfigurowane są moduły lokalnych kontrolerów dostępu (LAC).

	No.	Address	Type	Project version	Connection	Serial no.	Version
✓	1	1	AMC2-4R4 L-Bus	60.22	UDP:54545>172.18.1.17:10001>NONE	2304 8198	60.22

Przyciski umieszczone nad polem listy posiadają następujące funkcje:



Dodaj nowy kontroler.



Edytuj zaznaczony kontroler.






Testuj zaznaczony kontroler.



Usuń zaznaczony kontroler.

W polu listy dostępny jest wykaz wszystkich zainstalowanych kontrolerów, oraz następujące informacje:

Kolumna	Zawartość	Opis
	 ,  , lub 	Wynik testu LAC: negatywny, jeszcze nie zakończony lub pozytywny
Nr	od 1 do 128	Numer kontrolera.
Adres	1 do 8	Ustawiony przełącznikiem DIL i skonfigurowany adres kontrolera. W przypadku protokołu UDP zawsze 1.
Typ	AMC-Wiegand AMC-4R4 BG900 AMC-4R4 L-Bus LACi BG900 LACi L-Bus	Wybrany typ kontrolera
Projectversion (Wersja projektu)	Przykład: 37.02	Specjalna wersja oprogramowania do projektów wczytana do kontrolera.
Connection (Połączenie)	Przykład: UDP.: 54545>AMC- DEMO: 10001>NONE	Parametry interfejsu: Protokół: lokalny port UDP>nazwa sieciowa lub adres IP: Zdalny port IP>port COM
Nr seryjny	Przykład: 9999 9999	Nr seryjny kontrolera.
Version (Wersja)	Przykład: 37.02	Numer wersji oprogramowania wczytanego do kontrolera.

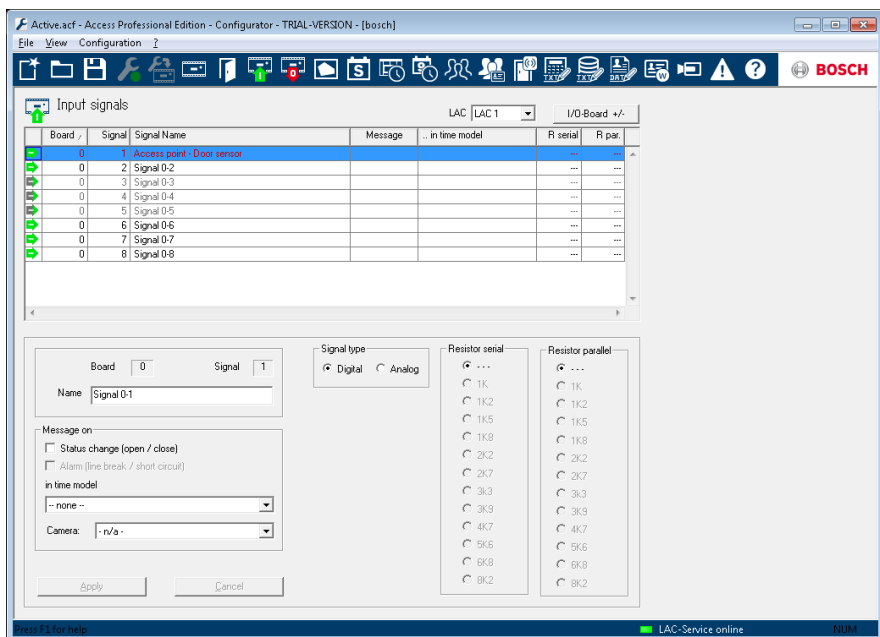
W dolnej części okna dialogowego znajdują się ustawienia ogólne (General settings), dla wszystkich urządzeń i aplikacji instalacji programu Access PE.

5 Sygnały

Sygnały wejściowe i wyjściowe kontrolerów mogą służyć, na przykład, do określania stanów drzwi i do sterowania drzwiami. Co więcej, sygnały te można też wykorzystać do skojarzenia dodatkowych funkcji kontrolnych z żądaniami dostępu. Pozwala to na sterowanie i włączanie kamer, optycznych lub akustycznych urządzeń sygnalizujących i systemów alarmowych.



5.1 Sygnały wejściowe



Podczas gdy sterowanie drzwiami oraz inne sygnały sterowania wraz z komunikatami o stanie konfigurowane są w oknie dialogowym **Entrances** (Wejścia), okno dialogowe **Input Signals** (Sygnały wejściowe) dotyczy szczegółowego definiowania typów sygnałów wejściowych i ich monitorowania.



W momencie otwarcia tego okna dialogowego wyświetlany jest zawsze pierwszy kontroler. Wybierz z listy wyboru **LAC** żądany kontroler, kierując się bieżącą numeracją. W momencie ustawienia kontrolera program standardowo tworzy 8 sygnałów wejściowych i 8 sygnałów wyjściowych. Jeśli używany kontroler może obsługiwać więcej sygnałów, można skorzystać z przycisku **I/O boards +/-** (Moduły WE/WY +/-) do skonfigurowania dodatkowych sygnałów.

Wszystkie wprowadzone sygnały wyświetlane są na liście. Poszczególne ustawienia wyświetlane są w pojedynczych kolumnach, natomiast ustawienia zaznaczonych sygnałów widoczne są w wykazie parametrów pod polem listy. Wszystkie ustawienia można wprowadzić zarówno w poszczególnych kolumnach listy, jak również w wykazie parametrów, jak pokazano w poniższej tabeli.

Kolumna	Parametr	Opis
1 (bez nazwy)	-	Oznaczenie stanu sygnału:  = sygnał aktywny  = sygnał nieaktywny Podwójnym kliknięciem na ikonie można zmienić dotychczasowy stan.
Board (Moduł)	Board (Moduł)	Numer modułu, w którym występuje sygnał. 0 = moduł podstawowy 1 = moduł rozszerzeń Tego parametru nie można zmienić.

Kolumna	Parametr	Opis
Signal (Sygnał)	Signal (Sygnał)	Numeracja sygnału dla danego modułu (1 do 16). Tego parametru nie można zmienić.
Signal name (Nazwa sygnału)	Name (Nazwa)	Nazwa sygnału. Przy ustawieniach standardowych sygnały otrzymują następujące oznaczenia: Sygnał <Nr modułu>-<Nr sygnału> Dwukrotne kliknięcie w tej kolumnie umożliwia użytkownikowi edycję nazwy.
Komunikat	Message on... (Komunikaty przy...) State change (open / close) (Zmiana stanu (otwarty / zamknięty)): Alarm:	Wizualizacja ustawień parametrów na liście:   (jest możliwa tylko w przypadku typu sygnału Analog (Analogowy)) Dwukrotne kliknięcie w tej kolumnie umożliwia zmianę ikony komunikatu.
	Camera (Kamera)	Do kamery z listy wyboru można przypisać określone sygnały wejściowe. Aktywowanie odpowiedniego sygnału spowoduje utworzenie komunikatu dziennika, który można użyć do pobrania obrazów z kamery.

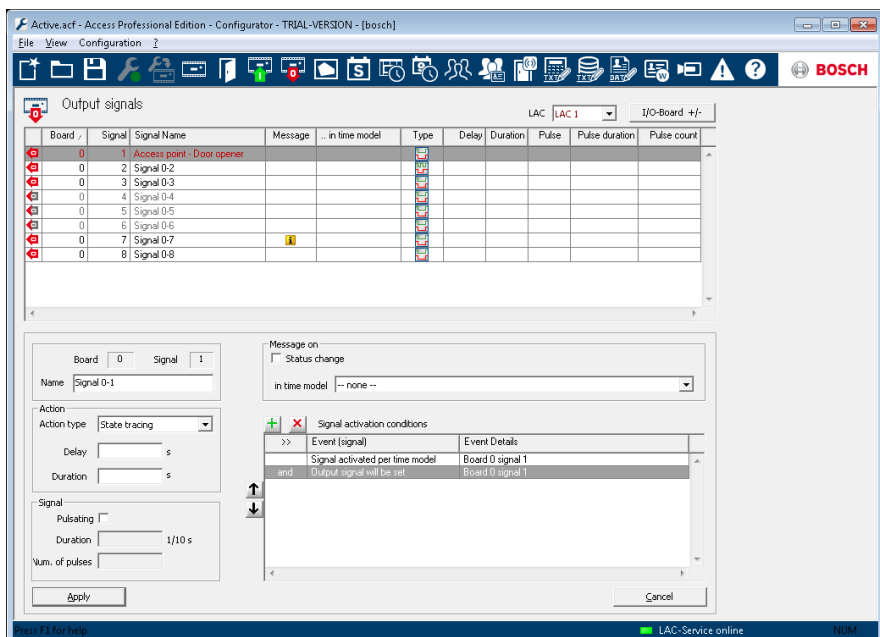
Kolumna	Parametr	Opis
- only on time model... (tylko w modelu czasowy m...)	during time model (w modelu czasowym)	Wskazuje wybrany model czasowy. Dwukrotne kliknięcie w tej kolumnie umożliwia użytkownikowi wybór z listy modeli czasowych.
<brak>	Signal type (Typ sygnału) Digital (Cyfrowy) Analog (Analogowy)	Opcja Analog (Analogowy) aktywuje pola opcji, umożliwiając wybór wartości rezystancji.
R serial (R szeregow a)	Serial resistance (Rezystancja szeregow a)	Dwukrotne kliknięcie w tej kolumnie otwiera listę wyboru wartości rezystancji. Wybór szeregowej lub równoległej wartości rezystancji automatycznie zmienia typ sygnału na analogowy.
R par. (R równoległa)	Parallel resistance (Rezystancja równoległa)	

Uwaga!

Nie wszystkie z wymienionych wartości można ze sobą łączyć – wiadomości dotyczące tworzenia właściwych par wartości rezystancji można znaleźć w instrukcji instalacji urządzenia AMC2.

5.2 Sygnały wyjściowe

W tym oknie dialogowym ustawiane są parametry sygnałów wyjściowych i, jeśli jest to konieczne, definiowane są kolejne moduły.






W momencie otwarcia tego okna dialogowego wyświetlany jest zawsze pierwszy kontroler. Wybierz z listy wyboru **LAC** żądany kontroler, kierując się bieżącą numeracją. W momencie ustawienia kontrolera program standardowo tworzy 8 sygnałów wejściowych i 8 sygnałów wyjściowych. Jeśli używany kontroler może obsługiwać więcej sygnałów, można skorzystać z przycisku **I/O boards +/-** (Moduły WE/WY +/-) do skonfigurowania dodatkowych sygnałów.






Wszystkie wprowadzone sygnały wyświetlane są na liście. Poszczególne ustawienia wyświetlane są w pojedynczych kolumnach, natomiast ustawienia zaznaczonych sygnałów

widoczne są w wykazie parametrów pod polem listy. Wszystkie ustawienia można wprowadzić zarówno w poszczególnych kolumnach listy, jak również w wykazie parametrów, jak pokazano w poniższej tabeli.

Wymienione tutaj ustawienia sygnałów wyjściowych można uzupełnić, wprowadzając dodatkowe **warunki**, które muszą zostać spełnione, aby sygnał wyjściowy był aktywowany.

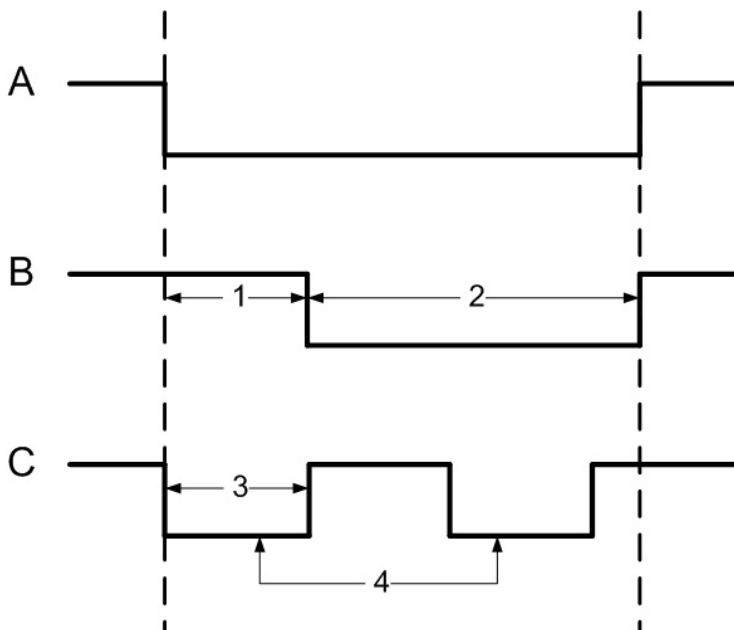
Kolumna	Parametr	Opis
1 (bez nazwy)	-	Oznaczenie stanu sygnału:  = sygnał aktywny  = sygnał nieaktywny Podwójnym kliknięciem na ikonie można zmienić dotychczasowy stan.
Board (Moduł)	Connection (Połączenie)	Numer modułu, w którym występuje sygnał. 0 = moduł podstawowy 1 = moduł rozszerzeń Tego parametru nie można zmienić.
Signal (Sygnał)		Numeracja sygnału dla danego modułu (1 do 16). Tego parametru nie można zmienić.

Kolumna	Parametr	Opis
Signal name (Nazwa sygnału)	Name (Nazwa)	Nazwa sygnału. Przy ustawieniach standardowych sygnały otrzymują następujące oznaczenia: Sygnał <Nr modułu>-<Nr sygnału> Sygnały zdefiniowane i aktywowane w oknie dialogowym Define entrance (Definiuj wejście) zostaną wyświetlone z nazwą wejścia oraz opisem sygnału. Dwukrotne kliknięcie w tej kolumnie umożliwia użytkownikowi edycję nazwy.
Komunikat	Message on... (Komunikaty przy...) State change (Zmiana stanu)	Wizualizacja ustawień parametrów na liście:  Dwukrotne kliknięcie w tej kolumnie powoduje włączenie lub wyłączenie ustawienia.
- only on time model... (tylko w modelu czasowym...)	during time model (w modelu czasowym)	Wyświetlenie i wybór modelu czasowego.

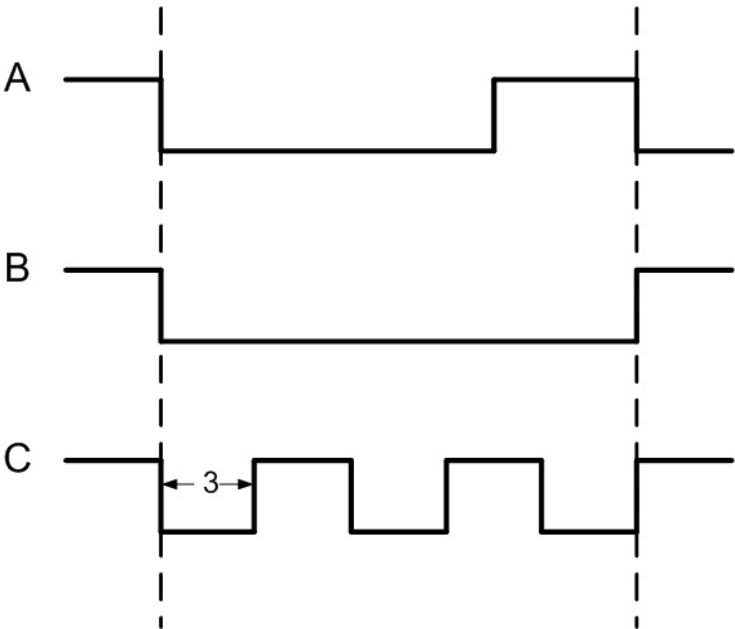
Kolumna	Parametr	Opis
Typ	Typ czynności: Momentary (Chwilowa) Follow state (Śledzenie stanu) Toggle (Przełącz)	Dostępne są trzy typy czynności:    Dwukrotne kliknięcie w tej kolumnie umożliwia zmianę typu czynności w pokazanej kolejności.
Opóźnienie	Opóźnienie	Opóźnienie w sekundach przed przesłaniem sygnału [0 - 9999].
Duration (Czas trwania)	Duration (Czas trwania)	Opóźnienie w sekundach przed przesłaniem sygnału [0 - 9999; 0 = zawsze lub dopóki nie zostanie przerwane przez komunikat o anulowaniu].
Pulse (Impulsowy)	Pulsating (Pulsujący)	Aktywuje nadawanie impulsowe, w przeciwnym razie sygnał nadawany jest ze stałą prędkością. Dwukrotne kliknięcie wprawdzie uaktywnia opcję, jednak oznacza ją jako niezdefiniowaną, powodując obok umieszczenie symbolu  , aż do chwili określenia czasu trwania i ilości impulsów. Następnie oznaczany jest on symbolem  .

Kolumna	Parametr	Opis
Pulse duration (Czas trwania impulsu)	Duration (Czas trwania)	Czas trwania impulsu.
Pulse count (Ilość impulsów)	Liczba impulsów	Ilość impulsów na sekundę.

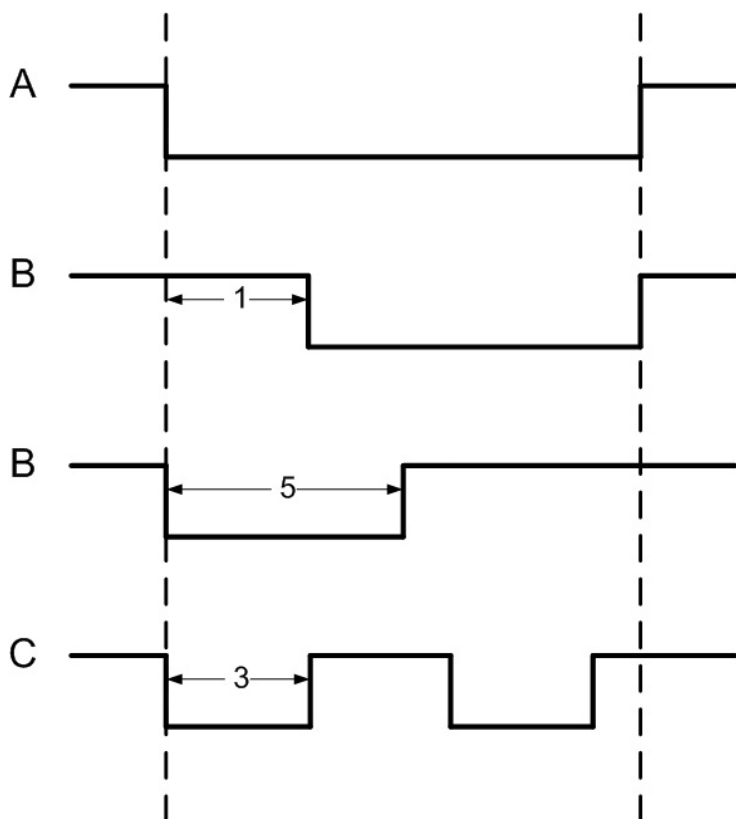
Typ czynności: Chwilowa



Typ czynności: Przełącz



Typ czynności: Śledzenie stanu



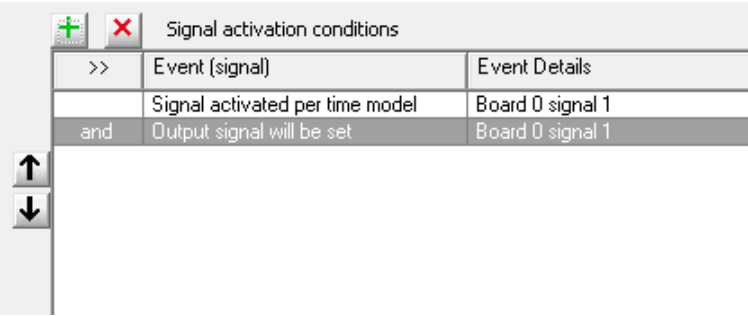
A =	stan odpytywania
B =	stabilny
C =	impulsowy
1 =	czas zwłoki
2 =	okres działania
3 =	szerokość impulsu
4 =	ilość impulsów (= 2)


5 =	maks. czas aktywacji
-----	----------------------

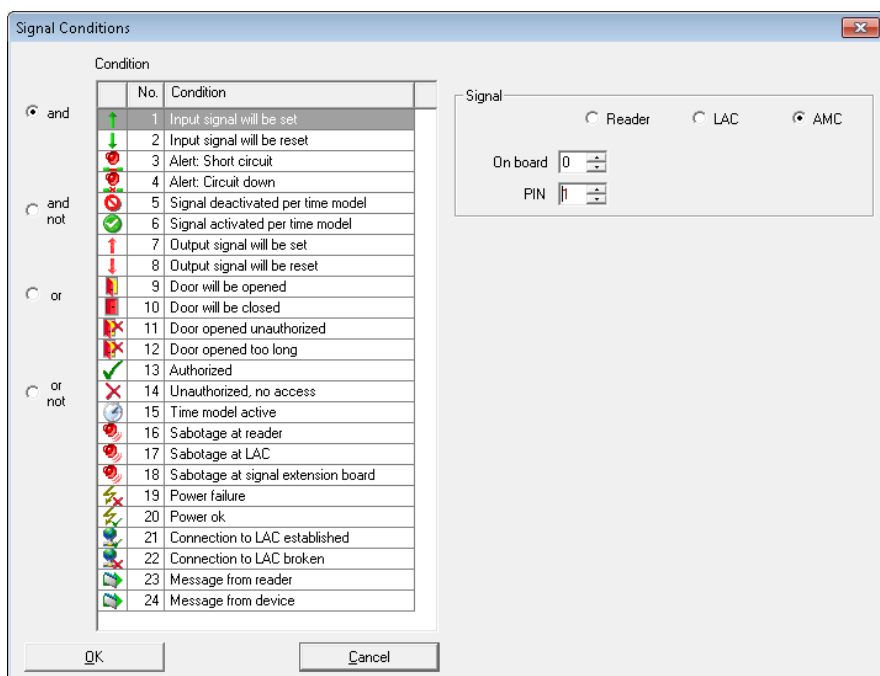
5.3 Definiowanie warunków sygnałów wyjściowych

W oknie dialogowym **Output signals** (Sygnały wyjściowe) można definiować ustawienia, oraz dodatkowe warunki, które jedynie w określonych sytuacjach spowodują aktywację sygnałów wyjściowych.


Specjalne warunki sygnałów zaznaczonych na liście głównej definiowane są w prawym dolnym rogu okna dialogowego.



Naciśnij przycisk , aby otworzyć poniższe okno dialogowe. Okno to służy do konfiguracji stosownych warunków.



Wprowadzając warunek aktywacji, należy pamiętać o uzupełnieniu informacji, np. na tematżądanego sygnału wyjścia lub czytnika, zanim warunek zostanie zatwierdzony przyciskiem **OK**.

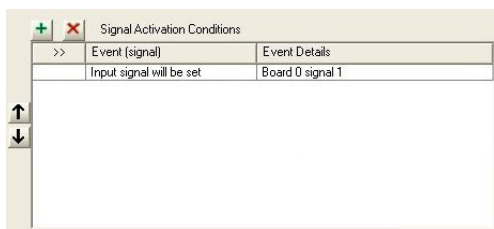
Do każdego sygnału można zastosować dowolną ilość warunków. Aby przypisać kolejny nowy warunek, należy za każdym razem otworzyć okno przez naciśnięcie przycisku .



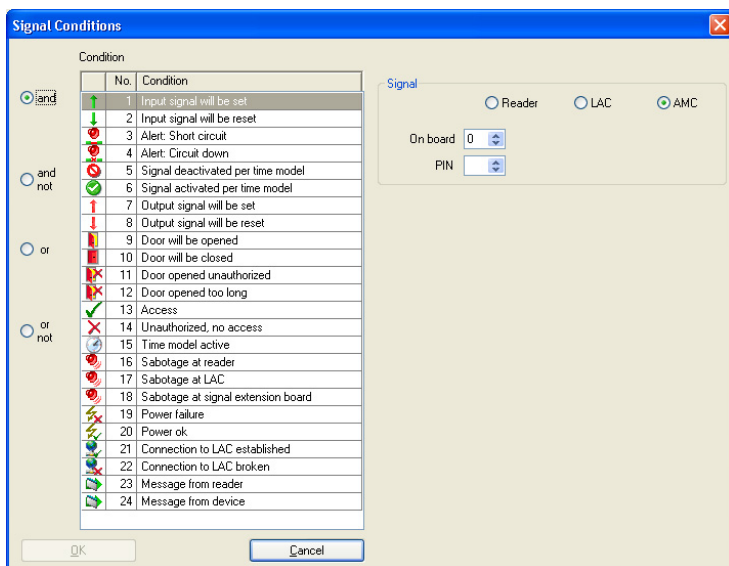
Uwaga!

Wybrać można wyłącznie sygnały i urządzenia (wejścia, czytniki, drzwi) podłączone do kontrolera, do którego przyporządkowywane są parametry sygnału wyjścia.

Dla warunku dostępne są dwie opcje: **normal** (normalny) (jeśli warunek ma zostać spełniony) oraz **not** (nie) (jeśli warunek ma nie być spełniony).



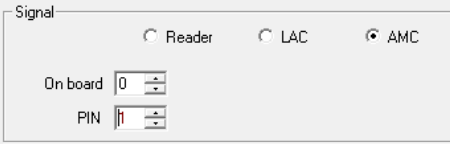
Każdy kolejny warunek zostanie połączony z pierwszym warunkiem za pomocą operatorów **and** (i), **and not** (i nie), **or** (lub) lub **or not** (lub nie).

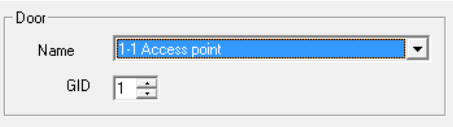
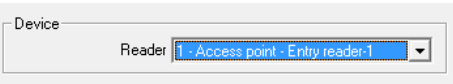


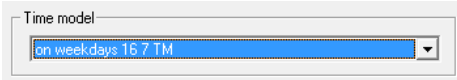
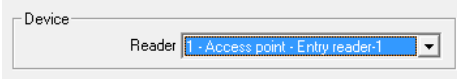
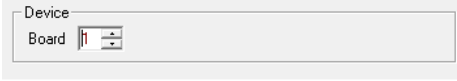
Signal Activation Conditions		
>>	Event (signal)	Event Details
	Input signal will be set	Board 0 signal 1
and	Output signal will be reseted	Board 0 signal 1
and not	Access	Reader address 3
or	Door opened unauthorized	Door: access point
or not	Sabotage at reader	Reader address 3

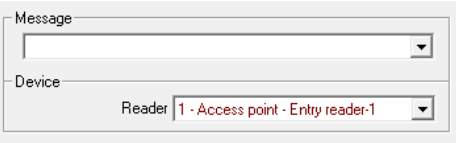

Warunki są realizowane w kolejności, w której są wymienione. Jeśli ten porządek nie odzwierciedla wymaganej procedury, pozycje warunków można zmienić. Wybierz z listy odpowiedni warunek i zmień jego pozycję, naciskając przycisk ↑ lub ↓.

Do każdego warunku należy obowiązkowo wprowadzić następujące informacje uzupełniające:

Warunek	Dane uzupełniające
Input signal will be set (Sygnał wejściowy będzie ustawiony)	Informacja na temat urządzenia, w którym występuje sygnał. Wybór modułu. Wybór połączenia.
Input signal is set (Sygnał wejściowy jest aktywny)	
Alert: Short circuit (Alarm: Zwarcie)	
Alert: Connection broken (Alarm: Zerwane połączenie)	
Signal deactivated by time model (Dezaktywacja sygnału przez model czasowy)	

Warunek	Dane uzupełniające
Signal activated by time model (Aktywacja sygnału przez model czasowy)	
Output signal will be set (Sygnał wyjściowy będzie ustawiony)	
Output signal will be reset (Sygnał wyjściowy będzie wyzerowany)	
Door will be opened (Drzwi zostaną otwarte)	<p>Wybór wejścia. Automatyczne ustawienie GID (ID grupy).</p> 
Door will be closed (Drzwi zostaną zamknięte)	
Door opening unauthorized (Niedozwolone otwarcie drzwi)	
Door open too long (Drzwi są otwarte zbyt długo)	
Access (Uprawniony dostęp)	
	<p>Wybór czytnika.</p> 

Warunek	Dane uzupełniające
Unauthorized, no access (Brak uprawnień, wstęp wzbroniony)	
Time model active (Model czasowy aktywny)	Selection of the time model (Wybór modelu czasowego) 
Sabotage at reader (Sabotaż czytnika)	Wybór czytnika. 
Sabotage at LAC (Sabotaż kontrolera LAC)	Dodatkowe informacje nie są wymagane.
Sabotage an signal extension board (Sabotaż w module rozszerzenia sygnału)	Wybór modułu. 
Power failure (Awaria zasilania)	Dodatkowe informacje nie są wymagane.
Power ok (Zasilanie poprawne)	
Connection LAC -> APE established (Ustanowione połączenie LAC -> APE)	

Warunek	Dane uzupełniające
Connection LAC -> APE broken (Zerwane połączenie LAC -> APE)	
Message from reader (Komunikat z czytnika)	<p>Wybór komunikatu z gotowej listy komunikatów.</p> <p>Wybór czytnika.</p> 
Message from device (Komunikat z urządzenia)	<p>Wybór komunikatu z gotowej listy komunikatów.</p> <p>Wybór modułu.</p> 

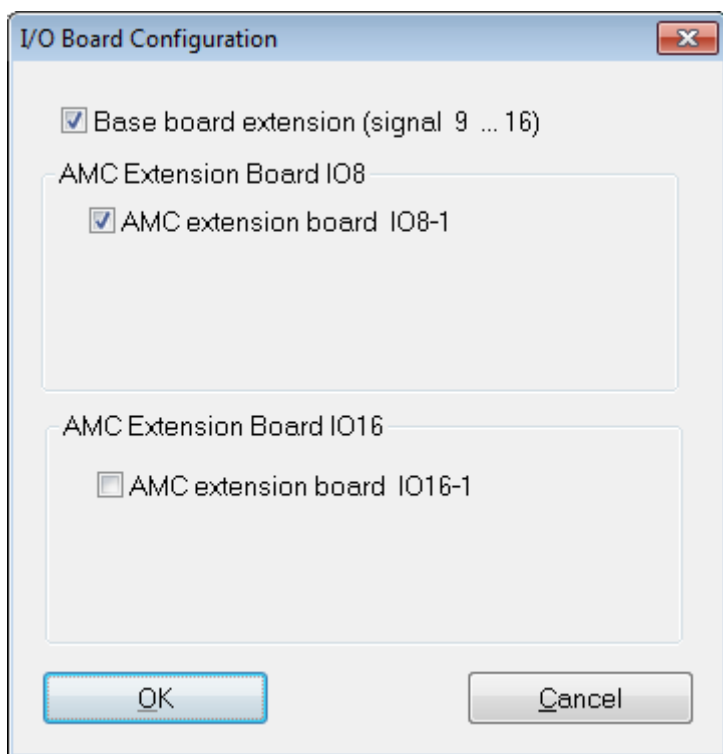
5.4 Tworzenie modułów rozszerzeń

Korzystając z okien dialogowych, moduły rozszerzeń można konfigurować w zakresie sygnałów **wejściowych** i **wyjściowych**. Ustawienia skonfigurowane w jednym oknie dialogowym będą aktywne w drugim.

W systemie kontroli dostępu Access PE można wykorzystywać i konfigurować trzy typy modułów rozszerzeń – wszystkie trzy są przetwarzane za pośrednictwem jednego z okien dialogowych dotyczących sygnałów.

- **AMC2 4W-EXT** – do podłączenia do interfejsu rozszerzeń kontrolera AMC typu Wiegand (AMC2 4W)
- **AMC2 8I-8O-EXT** – 8 dodatkowych sygnałów
- **AMC2 16I-16O-EXT** – 16 dodatkowych sygnałów

W oknie wyboru **LAC**, znajdującym się nad oknem listy, wybierz kontroler. Kontrolery te mają 8 sygnałów na płycie głównej (=0). Aby utworzyć moduł rozszerzeń, kliknij przycisk oznaczony **I/O Board +/-** (Moduł WE/WY +/-), który spowoduje otwarcie następującego okna dialogowego:



Zaznaczając jedno lub dwa pola, można dokonać następujących ustawień:

- **AMC Main Board** (Signals 9 - 16) (Płyta główna AMC (sygnały 9 - 16))
Tworzy moduł rozszerzeń Wiegand **AMC2 4W-EXT**.
Moduł ma takie same interfejsy jak kontroler AMC2-4W (4 interfejsy czytnika Wiegand, 8 sygnałów wejściowych i 8 sygnałów wyjściowych). Jednak nie może on działać niezależnie i musi zostać podłączony do modułu AMC2-4W.
Rozszerzenie to może współpracować tylko z kontrolerem AMC2-4W.
Moduł AMC2 4W-EXT może zostać skonfigurowany z **trzema** dodatkowymi modułami WE/WY.

W polu listy sygnałów wejściowych i wyjściowych modułu rozszerzeń, podobnie jak w przypadku kontrolera, podany jest numer karty 0 oraz sygnały numerowane od 9 do 16.

– **AMC Extension Board IO8 (Moduł rozszerzeń AMC IO8)**

Moduł z 8 sygnałami wejściowymi i 8 sygnałami wyjściowymi jako rozszerzenie interfejsu kontrolera.

Moduł ten może zostać podłączony do dowolnego kontrolera AMC2, a kiedy używany jest z kontrolerem AMC2-4W, może zostać połączony również z modułem rozszerzeń Wiegand AMC2 4W-EXT.

W polu listy sygnałów wejściowych i wyjściowych moduł rozszerzeń tworzony jest z numerem karty 1 i sygnałami numerowanymi od 1 do 8.

– **AMC Extension Board IO16 (Moduł rozszerzeń AMC IO16)**

Moduł z 16 sygnałami wejściowymi i 16 sygnałami wyjściowymi jako rozszerzenie interfejsu kontrolera.

Moduł ten może zostać podłączony do dowolnego kontrolera AMC2, a kiedy używany jest z kontrolerem AMC2-4W, może zostać połączony również z modułem rozszerzeń Wiegand AMC2 4W-EXT.

W polu listy sygnałów wejściowych i wyjściowych moduł rozszerzeń tworzony jest z numerem karty 1 i sygnałami numerowanymi od 1 do 16.

Uwaga!





Dokonane w tym miejscu ustawienia funkcji **I/O boards** (Moduły WE/WY) dotyczą zarówno sygnałów wejścia, jak i wyjścia danego kontrolera, i mogą być wprowadzone w obu oknach dialogowych.

6 Entrances (Wejścia)

Kiedy mówimy o przejściach, zawsze mamy na myśli pewną całość składającą się z różnych komponentów, które należą do systemu kontroli dostępu. Oprócz drzwi (które mogą być także bramką obrotową, służą osobową, barierką lub windą), system zawiera również co najmniej jeden czytnik i, potencjalnie, przyciski oraz urządzenia do sterowania (rygle, elektrozamki itd.). W niektórych przypadkach, w ramach dodatkowych funkcji sterowania, system obejmuje też optyczne lub akustyczne urządzenia sygnalizujące bądź kamery.

6.1 Tworzenie i modyfikacja modeli drzwi

Nowe wejście można utworzyć za pomocą przycisku  lub poprzez menu kontekstowe pola listy (klikając prawy klawisz myszy i wybierając opcję **Nowe wejście**). Aby w zaznaczonym wejściu zmienić nazwę, model drzwi lub adresy urządzeń, należy nacisnąć przycisk , dwukrotnie kliknąć zaznaczone wejście albo użyć menu kontekstowego (klikając prawy klawisz myszy i wybierając opcję **Zmień wejście**).

Define Entrance

Description:

Please configure LAC, GID and doormodel

LAC: GID:

Door model:

☐ Video verification Surv. camera: [Video configuration](#)

Reader configuration

Reader type: Address: Write access:

Signal definition

	Signal description	On dev...	GID / Board	DID	Connection
	Door sensor				
	Pushbutton: Door open				
	Boltsensor				
	Entrance locked				
	Sabotage signal				
	Local Open Enable				
	Door opener				

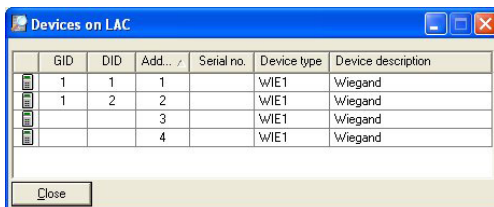
Przy tworzeniu nowego wejścia należy wpisać jego nazwę. Nazwa powinna być unikatowa i charakterystyczna, ponieważ na jej podstawie przydzielane będą uprawnienia dostępu podczas konfiguracji grup oraz uprawnienia indywidualne w programie zarządzania personelem.

Następnie należy wybrać ID grupy (GID) oraz numer kontrolera, do którego ma zostać podłączone wejście. Zazwyczaj należy poświęcić uwagę wyłącznie numerowi kontrolera, ponieważ program Access PE automatycznie przypisuje kolejny wolny GID.

Odpowiedni model drzwi należy wybrać w polu wyboru **Model drzwi**. Wstępnie zdefiniowane modele drzwi oraz funkcjonalność każdego z nich opisano w Dodatku.

Zgodnie z wariantem modelu drzwi wyświetlone zostaną pola wyboru czytników wejścia lub wyjścia, w których należy wybrać typ czytnika. Każdy czytnik musi otrzymać unikatowy adres w ramach kontrolera. W przypadku czytników z interfejsem **Wiegand** wystarczy wprowadzić **indywidualny numer interfejsu kontrolera**. W przypadku czytników z interfejsem **RS485** zasadnicze znaczenie ma przypisany **adres DIP**.

Przycisk **Wyszukaj dane urządzenia** umożliwia sporządzenie i wyświetlenie listy czytników dla danego kontrolera. Po przetworzeniu dane te zostaną umieszczone w pamięci podręcznej i mogą być w każdej chwili wywołane za pomocą przycisku **Dane urządzenia z pamięci podręcznej**. Jeśli nastąpią zmiany w konfiguracji, dane w pamięci podręcznej staną się nieaktualne i konieczne będzie ponowne utworzenie listy.



	GID	DID	Add...	Serial no.	Device type	Device description
	1	1	1		WIE1	Wiegand
	1	2	2		WIE1	Wiegand
			3		WIE1	Wiegand
			4		WIE1	Wiegand

Close

Uwaga!



Adresy czytnika muszą odpowiadać zainstalowanym w rzeczywistości urządzeniom.

W przypadku kontrolerów typu **AMC-Wiegand** można podłączyć maksymalnie cztery czytniki, natomiast w przypadku typów **AMC-RS485** i **LACi** maksymalnie osiem czytników.

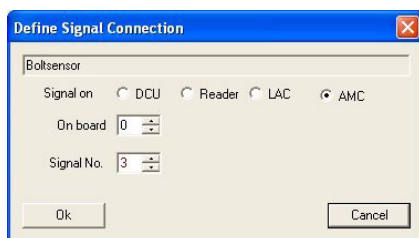
Zastosowanie adresu czytnika 9:

Adres czytnika 9 został utworzony jako wsparcie do ustawiania parametrów i pełni funkcję bufora w przypadku niezbędnych zmian parametrów. Jeśli przyporządkowano wszystkie adresy danego kontrolera i teraz konieczna jest zmiana parametrów, wówczas aby zwolnić jeden adres, można dla jednego z czytników wybrać czasowo adres 9.

Przykład: Chcemy zamienić czytniki 4 i 7. Z racji faktu, iż nie można nadać dwukrotnie tego samego adresu, najpierw należy przypisać czytnik 4 do adresu 9. Następnie należy przestawić czytnik 7 na adres 4, a potem czytnik 9 (= pierwotnie 4) na adres 7.

Definicja sygnału

Po wybraniu modelu drzwi, w polu listy wyświetlone zostaną wszystkie dostępne dla tego modelu sygnały wejścia i wyjścia. Zaznaczenie wpisu na liście i naciśnięcie przycisku **+**, umieszczonego po lewej stronie pola listy, lub dwukrotne kliknięcie wpisu otworzy okno dialogowe do definicji sygnałów.



Wyświetlony zostanie sygnał wybrany z listy. Działanie sygnału definiowane jest w domyślnych parametrach kontrolera, ale może, w razie potrzeby, zostać zmienione.

Dodatkowo wyświetlana jest karta, z której pochodzi sygnał i numer interfejsu sygnału. Wykaz sygnałów kontrolera lub karty rozszerzeń należy sprawdzić w odpowiednim podręczniku instalacji danego urządzenia.

Uwaga!

Należy zwrócić się do technika z prośbą o wydanie wykazu okablowania sygnałów, który umożliwi ustawienie identycznych parametrów w Access PE.

Dokonanie na tym etapie nieprawidłowych ustawień może być przyczyną poważnych błędów w funkcjonowaniu sterowania drzwiami oraz przetwarzaniu ich sygnałów.

W oknie dialogowym należy wybrać rodzaj podłączenia: DCU (kontroler drzwi), czytnik, LAC lub AMC. Przy wyborze DCU lub czytnika wymagane jest dodatkowo wprowadzenie GID oraz DID urządzenia. Obowiązują przy tym następujące zasady:

- **Czytnik**
 - GID = GID czytnika na wejściu
 - DID = 1 przy pierwszym czytniku **wejścia**, = 2 przy drugim czytniku **wejścia** = 3 przy pierwszym czytniku **wyjścia**, = 4 przy drugim czytniku **wyjścia**
 - Nr sygnału = sygnał w czytniku 1 ... 4
- **LAC**
 - Nr sygnału = sygnał w LAC 1 ... 16
- **AMC**
 - Na karcie = nr karty.. 0 lub 1
 - Nr sygnału = sygnał w AMC 1 ... 8 lub, w przypadku kart rozszerzeń, 1 ... 16

Ustawione połączenia zostaną wyświetlone w polu listy w odpowiednich kolumnach. Poza tym w pierwszej kolumnie znajdują się różne symbole określające stan sygnałów:

	Sygnał wejściowy nie jest ustawiony
	Sygnał wejściowy jest ustawiony
	Sygnał wyjściowy nie jest ustawiony
	Sygnał wyjściowy jest ustawiony

Zdefiniowany wcześniej sygnał można usunąć za pomocą przycisku -.

Powyższy przykład pokazuje konfigurację modelu drzwi za pomocą czytnika **Wiegand**.

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

Define Entrance

Description: **Main entrance**

Please configure LAC, GID and doormodel

LAC: **1** GID: **1**

Door model: **01c - Common door with entry or exit reader**

☐ Video verification Surv. camera: **Bosch** **Video configuration**

Reader configuration

Access-reader: **OSDP Keyb+Disp** Reader type: **1** Address: **1** Encryption: ☒ **On** Write access: **read only**

Device data from cache **Search device data**

Signal definition

	Signal description	On dev...	GID / Board	DID	Connection
	Door sensor				
	Pushbutton: Door open				
	Bolt sensor				
	Entrance locked				
	Sabotage signal				
	Local Open Enable				
	Door opener				
	Lock opposite direction to set				

Ok **Cancel**

Domyślnie opcja **Szyfrowanie** nie jest zaznaczona. W przypadku czytników obsługujących **bezpieczny protokół OSDPv2** należy wybrać opcję **Szyfrowanie**:

Encryption

☒ **On**

Wybór czytnika OSDP:

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

Obsługiwane są 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

Nie wolno podłączać produktów należących do różnych rodzin (np. **LECTUS duo** lub **LECTUS secure**) za pośrednictwem jednej magistrali OSDP. Do jednej magistrali OSDP nie można jednocześnie podłączyć produktów skonfigurowanych jako „zaszyfrowane” i „niezaszyfrowane”; wszystkie muszą należeć do jednej z tych kategorii.

Ostrzeżenie!

UWAGA! WAŻNA INFORMACJA!



Na potrzeby przesyłania zaszyfrowanych danych do czytnika OSDP generowany jest klucz. Należy koniecznie zapisać plik d:\...\BOSCH\Access Professional Edition\PE\cfg\Active.acf na bezpiecznym dysku lokalnym.

Plik ten jest potrzebny do przywrócenia istniejącej instalacji.



Ostrzeżenie!

Jeśli **bezpieczne czytniki OSDPv2** są używane w trybie zabezpieczonym, wymagają wstępnego „klucza master”.

W przypadku jego utraty czytników nie można skonfigurować tak, aby akceptowały nowy klucz master!

Jeśli ten klucz zostanie utracony, we wszystkich czytnikach konieczne będzie przywrócenie ustawień fabrycznych przez Obsługę techniczną!



Uwaga!

Firma UL nie wydała opinii na temat korzystania z czytników OSDP
Konsekwencje

6.2 Wskazania i ustawianie parametrów

Wszystkie wejścia, które rozpoznaje system, są wyświetlane na liście po lewej stronie. Kliknięcie wejścia na tej liście powoduje wyświetlenie jego danych w prawej części okna, w polach parametrów.

Wzdłuż górnej krawędzi pola listy znajdują się następujące przyciski:



Dodaj wejście.




Modyfikuj wejście.



Usuń wejście.

Nad polami parametrów wyświetlane są następujące opcje połączenia poszczególnych wejść:

- LAC** Kolejny numer kontrolera, który został przyporządkowany do wejścia.
- GID** Numer grupy, którą tworzą: wejście wraz z drzwiami oraz czytnikami.
- Model** Nazwa i opis wybranego modelu drzwi.

Wejścia można modyfikować przez kliknięcie przycisku  lub dwukrotne kliknięcie wejścia na liście.

Można skonfigurować następujące **parametry drzwi**:

Parametr drzwi	Opis
Czas aktywacji (w 1/10 s)	Jeśli w futrynie nie skonfigurowano kontaktronu, przez cały ten czas uruchomiony będzie automat do otwierania drzwi. Jeśli kontaktron jest skonfigurowany, mechanizm otwierania drzwi wyłączy się w momencie otrzymania sygnału, że drzwi są otwarte. Wartość domyślna = 40
Czas otwarcia (w 1/10 s)	Maksymalny czas, przez jaki drzwi są otwarte, zanim zostanie wysłany sygnał wskazujący na zbyt długie otwarcie drzwi. Wartość domyślna = 300
Czas aktywacji kamery (w 1/10 s)	Jeśli wejście jest wyposażone w kamerę do dozoru, będzie ona załączona przez czas określony tym parametrem. Wartość domyślna = 100
Czas wyciszenia alarmu dla mechanizmu kontroli (w 1/10 s)	Czas trwania wyciszenia alarmu przed uruchomieniem automatu do otwierania drzwi. Wyciszenie alarmu jest skuteczne tylko wówczas, gdy czas ten jest większy od 0. Wartość domyślna = 0

Parametr drzwi	Opis
Kontaktron drzwiowy	Jeśli w futrynie drzwi wbudowany jest specjalny kontaktron, to określenie dla niego parametru ułatwia systemowi nadzorowanie przechodzenia osób. Dodatkowo wyłączy się sygnał otwarcia drzwi, jeśli otwieranie drzwi zostanie zarejestrowane przez kontaktron. Sygnał ten steruje również funkcją czasu wyciszenia alarmu .
Styk rygla	Jeśli w drzwi wbudowany jest specjalny styk rygla, to określenie dla niego parametru umożliwi systemowi stwierdzenie, czy drzwi są rzeczywiście zamknięte.
Element zespołu drzwiowego	Umożliwia ustawienie drzwi jako elementu składowego zespołu drzwiowego, np. służy osobowej lub służy powietrznej. Wówczas na podstawie sygnałów wysyłanych do zespołu drzwiowego można mieć pewność, że jednocześnie otwarte są tylko jedne drzwi. Jeśli tylko jedne drzwi zdefiniowane są jako element zespołu drzwiowego, wówczas synchronizacja nie jest aktywna.
Zdarzenia włamania	W tym miejscu można określić, czy w przypadku niedozwolonego otwarcia drzwi pojawi się komunikat. Jednak w tym przypadku niezbędny jest kontaktron drzwiowy .
Zdarzenia stanu drzwi	Jeśli wbudowany jest kontaktron drzwiowy , system może zasygnalizować każdorazowe otwarcie/zamknięcie drzwi.

Dla jednego wejścia można określić następujące ustawienia czytnika:

Ustawienia czytnika Czytniki wejść i wyjść	Opis
Tylko kontrola dostępu	W momencie przejścia osoby czytnik generuje jedynie komunikat dostępu.
Przybycie	Przejdzie przez ten czytnik kart spowoduje wygenerowanie dodatkowo zapisu rejestracji czasu pracy i zapisanie obecności danej osoby.
Opuszczenie	Przejdzie przez ten czytnik kart spowoduje wygenerowanie dodatkowo zapisu rejestracji czasu pracy i zapisanie nieobecności danej osoby.
<p>Zapisy dokonane w czytnikach zaprogramowanych do kontroli czasu pracy zachowywane są w zawsze w nowym pliku, tworzonym codziennie w katalogu C:\Bosch\Access Professional Edition\PE\Data\Export (ścieżka domyślna). Tworzony jest plik o nazwie TA_<Bieżąca data RRRRMMDD>.dat, który może zostać poddany edycji. Pola rozdzielone są średnikiem i mogą być edytowane na przykład w aplikacjach arkuszy kalkulacyjnych innych producentów. Każdy rekord przejścia zawiera następujące dane: Nazwisko; Imię; Nazwa firmy; Numer osobisty.; Numer karty.; Pola dodatkowe 1–10 (jeśli mają parametry); Nazwa wejścia; Data (rrrrmmdd); Godzina (ggmmss plus litera „s” wskazująca czas letni); Kierunek przejścia wyrażony numerycznie (1 = wejście, 2 = wyjście); Kierunek jako łańcuch tekstowy (WEJŚCIE, WYJŚCIE)</p>	

Ustawienia czytnika Czytniki wejść i wyjść	Opis
Sprawdzanie poprawności	<p>Tylko w przypadku czytników wejścia.</p> <p>Parametr umożliwia ustawienie czytnika jako czytnika zwolnienia do odblokowania kart osób wybranych do losowej kontroli.</p> <p>Należy jednak zapewnić, że czytnik zwolnienia nie będzie jednocześnie skonfigurowany jako czytnik przesiewowy, wybierający losowo osoby do kontroli.</p>
Losowa kontrola osób – współczynnik (%)	<p>Parametr umożliwia ustawienie czytnika jako czytnika przesiewowego do losowego wyboru kart w celu przeprowadzenia kontroli osób.</p> <p>Oprócz zaznaczenia pola wyboru należy wpisać współczynnik przypadkowości kontroli losowej wyrażony w procentach (1 do 99). Brak danych spowoduje, że przeprowadzona zostanie kontrola wszystkich posiadaczy kart (100%). Należy jednak zapewnić, że czytnik przesiewowy nie będzie jednocześnie skonfigurowany jako czytnik zwolnienia odblokowujący karty zablokowane przez czytniki przesiewowe.</p>

Ustawienia czytnika Czytniki wejść i wyjść	Opis
Czas oczekiwania blokady podwójnego wejścia – ID grupy	<p>Opcja blokuje możliwość ponownego wejścia z tą samą kartą, zgodnie z wprowadzonym czasem oczekiwania, chyba że w tym czasie zarejestrowano wyjście. Zapobiega to nadużyciu kart przez przekazanie ich kolejnej osobie czekającej w bramce obrotowej.</p> <p>Czas oczekiwania w minutach od 1 do 999.</p> <p>W danej grupie może znajdować się kilka czytników. Funkcja zapobiegająca przekazaniu karty osobie niepowołanej obowiązuje dla każdego czytnika z tym samym identyfikatorem grupy. Możliwe wartości: dwa znaki 0–9 i/lub A–Z</p>
Wejście jako grupa – wymagane podanie liczby osób	<p>Tylko w przypadku czytników wejścia.</p> <p>Opcja umożliwia wejście dopiero w momencie, gdy grupa składająca się z co najmniej podanej liczby osób przesunie swoje karty przez czytnik. Możliwe wartości: 2–6.</p>
Z klawiaturą	<p>To pole wyboru należy zaznaczyć, jeśli czytnik przy drzwiach ma klawiaturę.</p>
Bez sprawdzania modelu czasowego	<p>Domyślnie dostęp sprawdzany jest w stosunku do modelu czasowego. Zachowanie to można wyłączyć, ustawiając ten parametr.</p>

Ustawienia czytnika Czytniki wejść i wyjść	Opis
Wejście z podajnikiem kart	Tę opcję należy aktywować w przypadku, gdy czytnik jest wyposażony w podajnik kart.
Przycisk – zawsze aktywny	<p>Parametr umożliwia rozpoznanie sygnału otwarcia drzwi. Sygnał ten może pochodzić z przycisku lub z telefonu, np. kiedy nie jest dostępny żaden czytnik.</p> <p>zawsze aktywny: Przy normalnej konfiguracji ustawień przycisk nie działa, gdy system bezpieczeństwa jest aktywny. Oznacza to, że opuszczenie monitorowanych obszarów nie jest możliwe. Włączenie tej opcji powoduje, że przycisk jest aktywny nawet przy uzbrojonym systemie alarmowym. Po aktywowaniu przycisku ta funkcja będzie obejmować również czytnik wyjścia.</p>

Uwaga!

Kontrole wykraczające poza podstawową weryfikację uprawnień i modeli czasowych (np. sekwencyjne kontrole dostępu, kontrole funkcji zapobiegającej przekazaniu karty osobie niepowołanej, kontrole losowe) są przeprowadzane przez podsystem LAC. Aby ta funkcjonalność była dostępna, serwer Access PE musi działać całą dobę (24 x 7).

Opcję **otwarcia wejścia** można skonfigurować za pomocą następujących parametrów:

Typ otwarcia drzwi	Opis
Normalny	Drzwi są zamknięte, a ich otwarcie jest możliwe dopiero po zbliżeniu do czytnika ważnej karty identyfikacyjnej.
Zezwolenie stałe	Drzwi są otwarte przez dłuższy okres, np. w czasie dnia lub tak długo jak w recepcji znajduje się personel.
Według modelu czasowego	<p>Zezwolenie stałe na otwarcie drzwi odbywa się na podstawie wybranego modelu czasowego w następujących wariantach:</p> <ul style="list-style-type: none">– Zawsze według modelu czasowego: drzwi są otwarte w ustalonych okresach czasu.– Po pierwszym wejściu: po pierwszym wejściu w trakcie ustalonego okresu drzwi pozostaną otwarte aż do końca tego okresu.– Aktywacja przez okno dialogowe: zezwolenie stałe w czasie pracy regulowane jest przez specjalny czytnik z wyświetlaczem.
Aktywacja elektrozamka	Parametr ten określa model czasowy sterujący aktywacją elektrozamka na wejściu (zwykle poza normalnymi godzinami pracy).

Opcję **wprowadzania kodu PIN** w czytniku na wejściu można skonfigurować przy użyciu następujących parametrów:

Kod PIN	Opis
Brak	Kod PIN nie jest wymagany.
Zawsze	Kod PIN jest zawsze wymagany.
Według modelu czasowego	<p>Opcją wprowadzania kodu PIN steruje wybrany model czasowy w następujących wariantach:</p> <ul style="list-style-type: none"> – Poza normalnymi godzinami pracy: poza okresami modelu czasowego należy wprowadzić kod PIN. – Poza normalnymi godzinami pracy i przy pierwszym wejściu: poza okresami modelu czasowego i przy pierwszym wejściu osoby należy wprowadzić kod PIN.
PIN lub karta	Jeśli funkcja jest aktywna, dostęp można uzyskać przez wprowadzenie kodu PIN do drzwi lub za pomocą karty.
Kod PIN do drzwi	opcja wprowadzenia kodu PIN do drzwi – od 4 do 8 cyfr (ustawienia parametrów – ogólne ustawienia systemu)
Weryfikacja	ponowne wprowadzenie kodu PIN do drzwi
Według modelu czasowego	Opcję wprowadzania alternatywnego kodu PIN można ograniczyć do określonych dni i pór dnia za pośrednictwem modelu czasowego.

**Uwaga!**

Kody PIN **identyfikacyjny i do drzwi** nie mogą być używane w przypadku modeli drzwi z funkcją uzbrojenia systemu bezpieczeństwa (modele drzwi 10 i 14).



Uwaga!

Dostęp grupy skonfigurowany w czytniku z klawiaturą nie działa razem z funkcjonalnością PIN lub karta.

6.3 Modele drzwi z ustawieniami specjalnymi

Modele drzwi z ustawieniami specjalnymi

Niektóre modele drzwi wymagają specjalnych informacji dotyczących ustawienia lub specjalnych trybów użytkowania.

Model drzwi 07: winda

Wybór tego modelu rozszerzy okno dialogowe o kilka dodatkowych pól, umożliwiając utworzenie pięter.

Floors served by elevator

AMC I/O

LAC signal	Floor description	Input at reader
0 - 1	1st floor	<input type="checkbox"/>
0 - 2	2nd floor	<input type="checkbox"/>
0 - 3	3rd floor	<input type="checkbox"/>
0 - 4	4th floor	<input type="checkbox"/>
0 - 5	Cafeteria	<input type="checkbox"/>
0 - 6	Server Room	<input type="checkbox"/>
0 - 7		<input type="checkbox"/>
0 - 8		<input type="checkbox"/>

Standardowo jednego kontrolera AMC2 można używać do obsługi 8 pięter. W przypadku spełnienia następujących warunków wstępnych istnieje możliwość zwiększenia tej liczby:

- 64 piętra w przypadku używania kontrolerów Wiegand (AMC2 4W + AMC2 4W-EXT + 3 AMC2 16I-16O-EXT)
- 56 pięter w przypadku używania kontrolerów RS 485 (AMC2 4R4 + 3 AMC2 16I-16O-EXT)

Zdefiniowane tutaj piętra można przydzielić jako Access Authorizations (uprawnienia dostępu).

Model drzwi 14: drzwi z funkcją ponownego uzbrojenia systemu sygnalizacji włamania

Konfiguracja tego modelu drzwi jest taka sama jak wszystkich innych, za wyjątkiem tego, że wraz z uprawnieniem dostępu dla tego wejścia przydzielane jest również uprawnienie do uzbrajania i rozbrajania systemu alarmowego (systemu sygnalizacji włamania). Uprawnienia te zwykle przydzielane są oddzielnie.

Wzdłuż górnej krawędzi pola listy znajdują się następujące przyciski:



Dodaj obszar.



Edytuj obszar.



Usuń obszar.

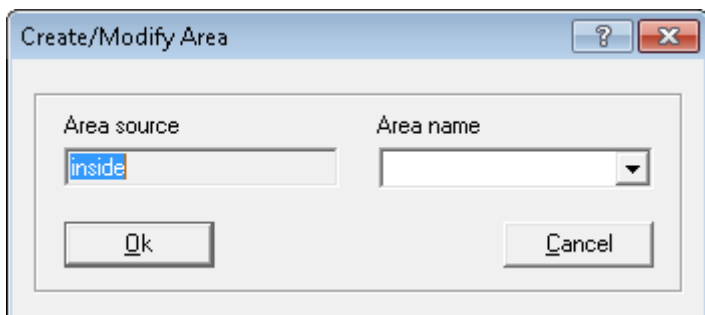
Podczas instalacji system domyślnie tworzy obszar **--outside--** (--poza--). Dla tego obszaru nie można zdefiniować żadnych wejść, ponieważ nie jest on monitorowany.

Na podstawie tego wstępnie zdefiniowanego obszaru można definiować dalsze obszary. Nie muszą one odpowiadać rzeczywistym obszarom, ponieważ są to konstrukcje czysto wirtualne. Obszar może obejmować jeden lub kilka budynków (np. obszar firmy ACME Inc.) albo pojedyncze piętra czy nawet pomieszczenia.

Uwaga!



Tworzenie nowych stref pomieszczeń odbywa się zawsze na podstawie istniejących stref. Dana strefa zaznaczona w polu listy automatycznie staje się **area source** (strefą źródłową) dla nowej strefy. To ustawienie wstępne nie może zostać zmienione, dlatego podczas tworzenia nowych stref należy zwracać uwagę na to, czy zaznaczono właściwą strefę pomieszczeń, która ma stać się **area source** (strefą źródłową).



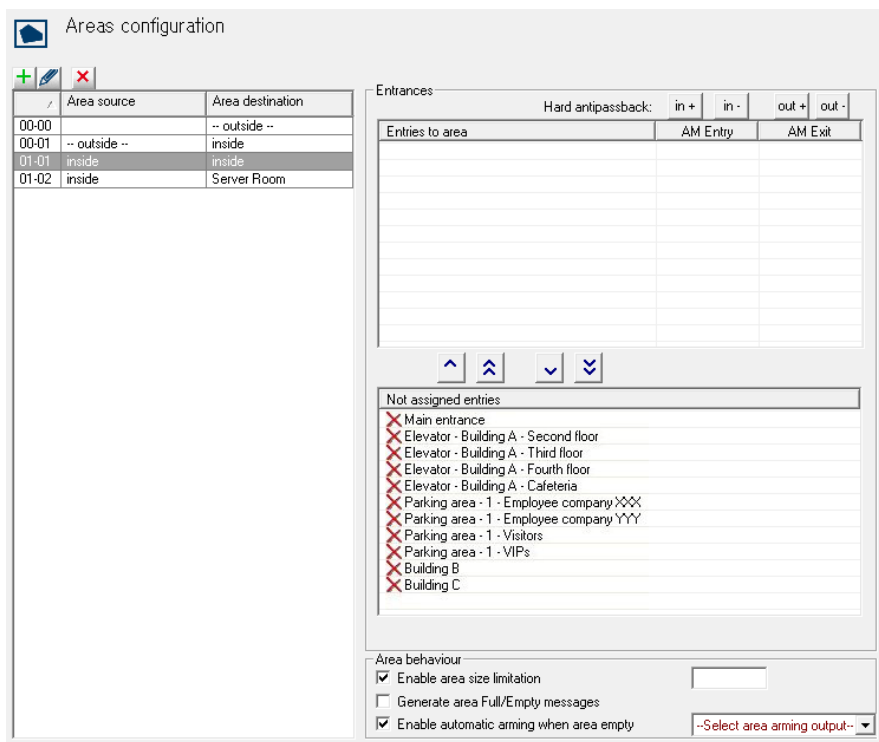
Nazwę strefy można wybrać z listy już utworzonych stref, lub można ręcznie wprowadzić nową.

Strefy należy skonfigurować w taki sposób, aby zagwarantować przejście z jednej do drugiej bez ewentualnych „luk” lub brakujących przejść.

Przykład:

Ze wstępnie zdefiniowanej strefy **--outside--** (--poza--) przechodzi się np. przez wejście główne i dochodzi do strefy **Reception** (Recepcja), a stamtąd do budynków A, B lub C. Tak więc w programie Access PE należy utworzyć strefy, które prowadzą z **area source** (strefy źródłowej) **Reception** (Recepcja) do budynków A, B i C.

Po utworzeniu nowej strefy, należy przyporządkować do niej przynajmniej jedno wejście, aby umożliwić przechodzenie do niej. W tym celu dostępne są dwa pola list po prawej stronie okna dialogowego.



W polu listy **not assigned entrances** (nie przydzielone przejścia) wymienione są wszystkie dostępne przejścia, czyli jeszcze nie przydzielone do żadnej strefy. Aby przyporządkować przejście do strefy wybranej na lewej liście, należy dwukrotnie kliknąć

Areas configuration

+	✎	✖	
/	Area source	Area destination	
00-00	-- outside --	-- outside --	
00-01	-- outside --	inside	
01-01	inside	inside	
01-02	inside	Server Room	

Entrances

Hard antipassback: in + in - out + out -

Entries to area	AM Entry	AM Exit
✓ Building A		
✓ Elevator - Building A - First floor		
✓ Elevator - Building A - Computer room		

⬆ ⬇ ⬅ ➡

Not assigned entries

- ✗ Main entrance
- ✗ Elevator - Building A - Second floor
- ✗ Elevator - Building A - Third floor
- ✗ Elevator - Building A - Fourth floor
- ✗ Elevator - Building A - Cafeteria
- ✗ Parking area - 1 - Employee company XXX
- ✗ Parking area - 1 - Employee company YYY
- ✗ Parking area - 1 - Visitors
- ✗ Parking area - 1 - VIPs
- ✗ Building B
- ✗ Building C

Area behaviour

☒ Enable area size limitation

☐ Generate area Full/Empy messages





☒ Enable automatic arming when area empty --Select area arming output-- ▾

Uwaga!



Wejście można przyporządkować tylko do jednej strefy. Jeśli określone przejścia zostały już przyporządkowane do strefy, wówczas nie będą one widoczne na liście **not assigned entrances** (nie przydzielone przejścia).

Kolumny **AM Entry** (Wejście AM) i **AM Exit** (Wyjście AM) odnoszą się do monitorowania dostępu. Jeśli system ma być używany do monitorowania dostępu, należy odpowiednio skonfigurować czytniki wejścia i wyjścia.

- Na liście **Entries to area** (Wejścia do obszaru) zaznacz wejście, które chcesz skonfigurować, i ustaw je jako wejście przyciskiem , lub jako wyjście przyciskiem , aby uaktywnić monitorowania dostępu. Przycisków  i  można użyć do cofnięcia tych konfiguracji. Funkcje te są również dostępne w menu kontekstowym (kliknij prawym przyciskiem myszy wejście na liście).

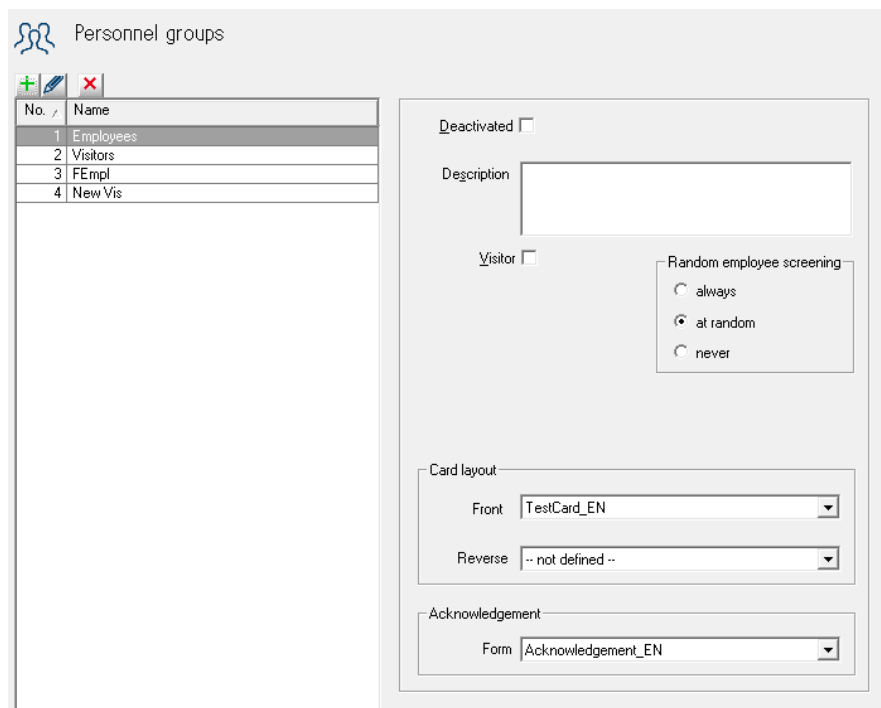
Uwaga!



Kontrole wykraczające poza podstawową weryfikację uprawnień i modeli czasowych (np. sekwencyjne kontrole dostępu, kontrole funkcji zapobiegającej przekazaniu karty osobie niepowołanej, kontrole losowe) są przeprowadzane przez podsystem LAC. Aby ta funkcjonalność była dostępna, serwer Access PE musi działać całą dobę (24 x 7).

8 Personnel Groups (Grupy personelu)

Grupy personelu umożliwiają logiczną strukturyzację personelu firmy. Przykładowo, nowo tworzone w systemie osoby mogą otrzymywać standardowy zakres uprawnień dostępu z predefiniowanych grup personelu.



Personnel groups

No.	Name
1	Employees
2	Visitors
3	FEmpl
4	New Vis

Deactivated ☐

Description

Visitor ☐

Random employee screening

☐ always
☒ at random
☐ never

Card layout

Front

Reverse

Acknowledgement

Form

Po lewej stronie znajduje się lista wszystkich utworzonych dotychczas grup personelu. Przyciski umieszczone nad polem listy posiadają następujące funkcje:



Dodaj nową grupę personelu

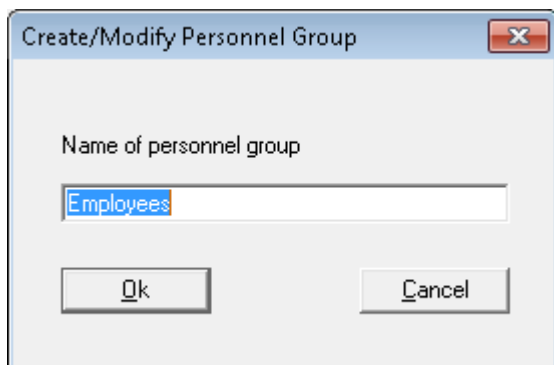


Edytuj zaznaczoną grupę personelu



Usuń zaznaczoną grupę personelu

Zainstalowany system zawiera dwie zdefiniowane grupy personelu: **Employees** (Pracownicy) i **Visitors** (Goście). Odpowiadają one również domyślnym filtrom w aplikacji **Personnel Management** (Zarządzanie personelem) programu Access PE.



W ten sposób można rozróżnić między różnymi grupami pracowników (np. pracownicy biurowi, pracownicy fizyczni, personel sprzątający) i przyporządkować tym grupom standardowe zakresy uprawnień dostępu w oknie dialogowym **Authorization groups** (Grupy uprawnień dostępu). Wybór jednej z tych grup personelu przy wprowadzaniu nowych danych osobowych spowoduje automatyczne przypisanie uprawnień standardowych.

The screenshot shows a configuration window for Personnel Groups. It contains several sections with labels and input fields:

- Deactivated**: A checkbox that is currently unchecked.
- Description**: A large, empty text input field.
- Visitor**: A checkbox that is currently unchecked.
- Random employee screening**: A group box containing three radio buttons:
 - ☐ always
 - ☒ at random
 - ☐ never
- Card layout**: A section containing two dropdown menus:
 - Front**: A dropdown menu with the value "TestCard_EN" selected.
 - Reverse**: A dropdown menu with the value "-- not defined --" selected.
- Acknowledgement**: A section containing one dropdown menu:
 - Form**: A dropdown menu with the value "Acknowledgement_EN" selected.

Dla zaznaczonej grupy personelu można po prawej stronie okna wprowadzić następujące parametry:

Ustawienia	Opis
Deactivated (Nieaktywne)	Dezaktywacja grupy personelu jest pierwszym etapem przygotowującym ją do usunięcia. Ta grupa personelu wprawdzie istnieje, jednak nie można do niej przypisać żadnej nowej osoby. Grupę personelu wolno usunąć pod warunkiem, że nie należą do niej już żadne osoby.
Opis	Do każdej grupy personelu można załączyć szczegółowy opis.
Visitor (Gość)	Dodatkowo można sklasyfikować grupę personelu jako „Visitor” (Goście). Aplikacja Personnel Management (Zarządzanie personelem) umożliwia filtrowanie list personelu w oparciu o kryteria All persons (Wszystkie osoby), Employees (Pracownicy) i Visitors (Goście). Grupa personelu Goście może zostać w ten sposób przeglądana oddzielnie od grupy Pracownicy .
Employee screening (Kontrola pracowników): always (zawsze) at random (losowa) never (nigdy)	Dotyczy wyłącznie czytników ustawionych jako czytniki dla potrzeb losowej kontroli osób. Znaczenie opcji jest następujące: = kontrolowane jest 100% osób. = grupa kontrolowana jest losowo, ze zdefiniowaną wartością procentową. = grupa nie jest nigdy kontrolowana.

Ustawienia	Opis
Badge Layout (Wygląd karty identyfikacyjnej) Front (Przód karty) Back (Tył karty)	Aby utworzyć kartę identyfikacyjną należy w pierwszej kolejności wybrać układ. Dla każdej grupy personelu można stworzyć indywidualne układy. Wybór układu dla strony odwrotnej jest opcjonalny.
Acknowledgement Form (Formularz potwierdzenia)	Wydanie karty identyfikacyjnej jest możliwe po uprzednim złożeniu podpisu na formularzu potwierdzenia odbioru. Formularz ten może mieć różny wygląd w zależności od grupy personelu.

8.1 Dostęp grupy w przypadku czytników z klawiaturą

Jak opisano w pomocy online Przeglądarka konfiguracji, każdy czytnik kart można tak skonfigurować, aby dostęp był udzielany wtedy, gdy pewna liczba autoryzowanych kart zostanie przesunięta przez czytnik. Ta funkcja nazywa się „dostępem grupy”.

Procedura dostępu grupy różni się nieznacznie w zależności od typu czytnika kart. Zasadniczo czytniki z klawiaturą pozwalają na dostęp większej liczby osób niż wynosi skonfigurowana liczba członków grupy, ale wymagają naciśnięcia dodatkowego klawisza w celu potwierdzenia, że przeszła cała grupa.

Czytniki bez klawiatury:

- Należy przesunąć przez czytnik dokładnie taką liczbę autoryzowanych kart, jaką skonfigurowano
- Dostęp zostaje udzielony

Czytniki z klawiaturą (z wyjątkiem IBPR):

- Należy przesunąć przez czytnik co najmniej taką liczbę autoryzowanych kart, jaką skonfigurowano

- Opcjonalnie można przesunąć przez czytnik więcej kart
- Należy nacisnąć na czytniku klawisz Enter lub „#”
- Dostęp zostaje udzielony

Czytniki IBPR z klawiaturą:

- Należy przesunąć przez czytnik co najmniej taką liczbę autoryzowanych kart, jaką skonfigurowano
- Opcjonalnie można przesunąć przez czytnik więcej kart
- Należy nacisnąć na czytniku klawisz „0”
- Należy nacisnąć na czytniku klawisz Enter lub „#”
- Dostęp zostaje udzielony

8.2 Ograniczenia dotyczące dostępu grupy

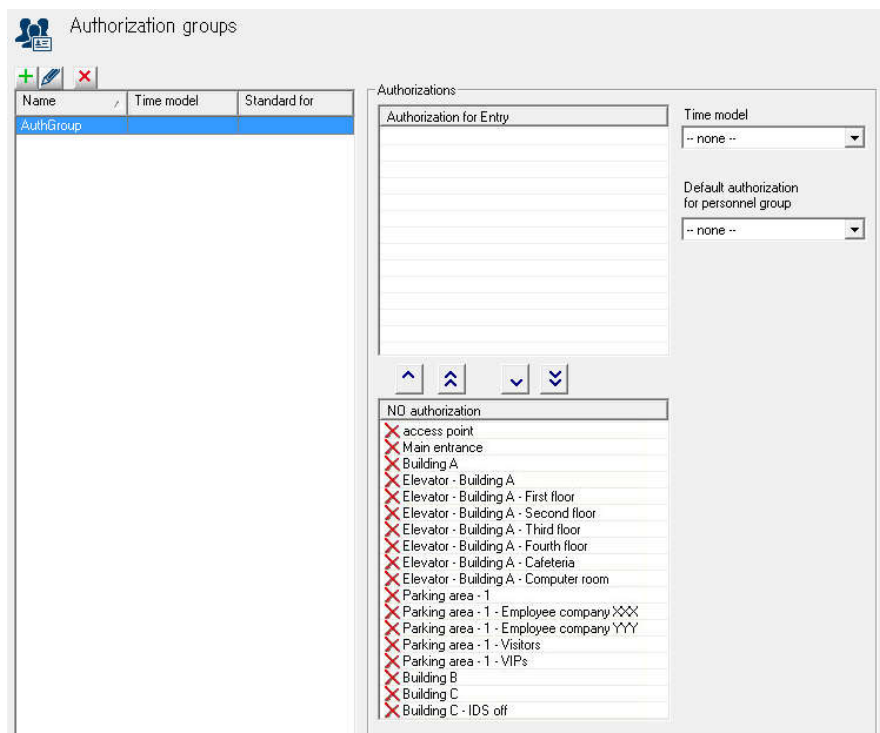
- Dostęp grupy można skonfigurować wyłącznie dla modeli drzwi 1+3.
- Dostęp grupy i ograniczenie dotyczące obszaru osób mogą prowadzić do tego, że w obszarze będzie większa liczba osób niż dozwolona – liczba osób w obszarze jest sprawdzana, gdy cała grupa wejdzie w dany obszar.
- W przypadku dostępu grupy i kilku kart zliczane są karty, a nie wchodzące osoby.
- Dostęp grupy skonfigurowany w czytniku z klawiaturą nie działa razem z funkcjonalnością PIN lub karta (każda konfiguracja wymaga tego samego potwierdzenia).

9 Uprawnienia dostępu

Grupy uprawnień dostępu upraszczają zadania administracyjne administratora systemu i operatora, gdyż umożliwiają grupowanie dowolnej liczby poszczególnych wejść o podobnych wymogach dotyczących dostępu (grupa osób, ograniczenia czasowe itd.) lub wejść znajdujących się blisko siebie pod względem rozmieszczenia. Grupy te można przypisać poszczególnym osobom w jednym kroku.

9.1 Tworzenie i przypisywanie

Authorization groups (Grupy uprawnień dostępu) służą do logicznego grupowania wejść. Nadanie uprawnień w aplikacji **Personnel Management** (Zarządzanie personelem) odbywa się wówczas poprzez przyporządkowanie do jednej (lub kilku) takich grup uprawnień.



Po lewej stronie w formie listy przedstawione są grupy uprawnień dostępu.

Przyciski umieszczone nad polem listy posiadają następujące funkcje:



Dodaj nową grupę uprawnień dostępu.




Edytuj zaznaczoną grupę uprawnień dostępu.



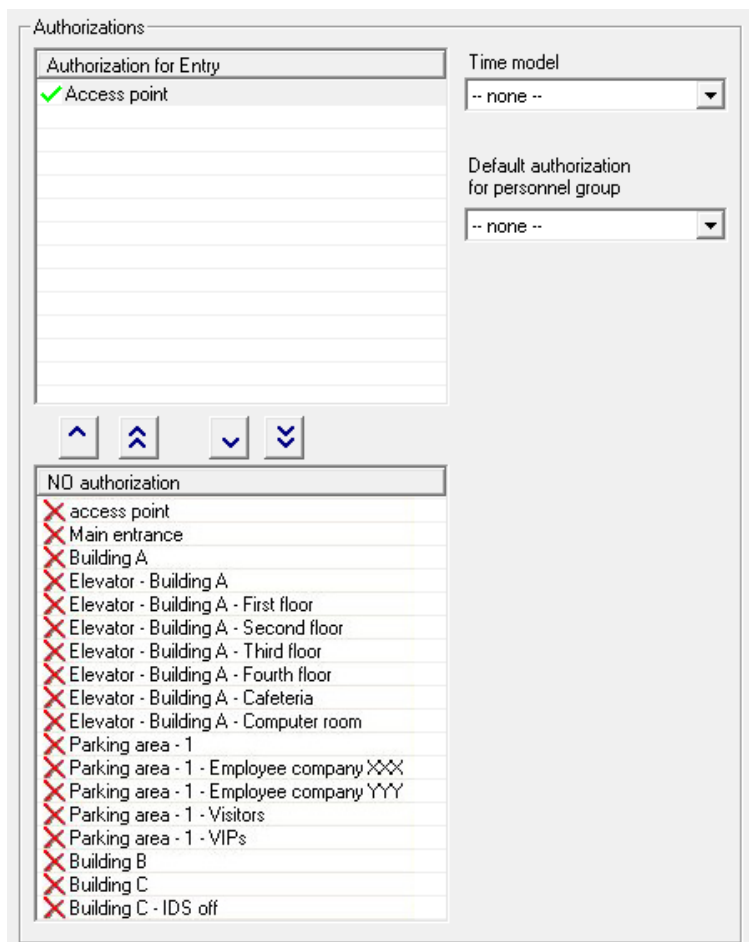
Usuń zaznaczoną grupę uprawnień dostępu.




Przycisk  otwiera okno dialogowe, w którym można wpisać nazwę nowej grupy uprawnień dostępu.



Okna listy po prawej stronie można użyć do przypisania wejść do wybranej grupy uprawnień dostępu.





Przejęcia na liście **NO authorization** (BEZ uprawnień) są dostępne, tj. nie zostały jeszcze przypisane do żadnej grupy uprawnień. Przez dwukrotne kliknięcie na wymaganym wejściu

lub na przycisku , wejście jest przypisywane do aktualnie wybranej grupy uprawnień dostępu, zaznaczonej na liście po

lewej stronie. Przycisk  przesuwa wszystkie wejścia z dolnej

listy do górnej. Natomiast dwukrotne kliknięcie na górnej liście



lub kliknięcie przycisków  lub  powoduje cofnięcie wykonanego przypisania.



Przestroga!

Późniejsze zmiany przyporządkowań przejść oraz modeli czasowych oddziałują na przydzielone już poszczególnym osobom uprawnienia.

Do każdej grupy można przydzielić **model czasowy**, który ogranicza obowiązywanie uprawnień; patrz **Zastosowanie modeli czasowych** (*Modele czasowe, Strona 151*) w części Access PE.

Uwaga!



Grupy uprawnień dostępu, do których przyporządkowano modele czasowe, można dodatkowo wyróżnić, dodając do nazwy przedrostek lub przyrostek np. **DM**. Podczas przydziału uprawnień w aplikacji **Personnel Management** (Zarządzanie personelem) można je potem szybciej odróżnić od uprawnień nieograniczonych.

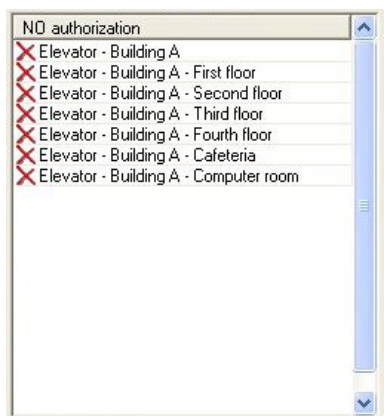
Oprócz tego można daną grupę uprawnień zdefiniować jako **default authorization** (uprawnienia domyślne) dla **personnel group** (grupy personelu) (np. pracownicy lub goście). Grupa uprawnień dostępu zostanie następnie automatycznie przyporządkowana podczas wprowadzania do wybranej grupy osób nowej osoby, w oknie programu **Personnel Management** (Zarządzanie personelem).

9.2 Uprawnienia specjalne

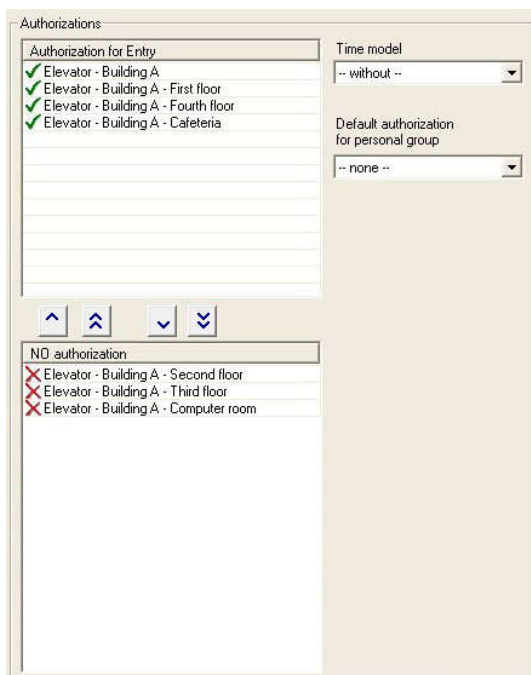
Modele drzwi 07 i 14 do **konfiguracji** wymagają podania dodatkowych informacji (*Modele drzwi z ustawieniami specjalnymi, Strona 120*). Różnią się jednak od innych modeli drzwi także w zakresie przydzielania i użytkowania.

Model drzwi 07: winda

Lista dostępnych uprawnień zawiera specjalny element dla windy, jak również dla każdej kondygnacji.

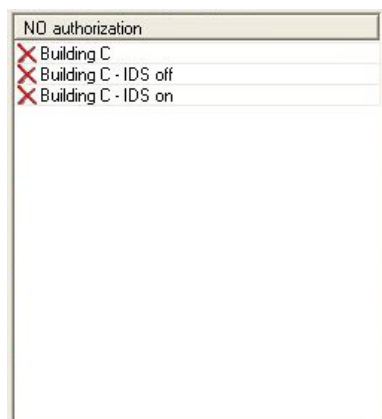


Podczas tworzenia grup uprawnień powinien zostać przydzielony jeden czytnik dla **windy** i **co najmniej jedna kondygnacja**.



Model drzwi 14: Ponowne uzbrajanie systemu sygnalizacji włamania

Lista dostępnych uprawnień zawiera oddzielny element dla wejścia, jak również dla uzbrojenia i rozbrojenia systemu alarmowego.



Uprawnienia te są przydzielane oddzielnie. Posiadacz karty może mieć prawo dostępu do określonego wejścia, ale może nie mieć prawa do uzbrojenia lub rozbrojenia systemu sygnalizacji włamania.

Natomiast, jeśli posiadacz karty ma tylko uprawnienia uzbrojenia/rozbrojenia danego przejścia, wówczas nie może przejść przez dane wejście.

Authorizations

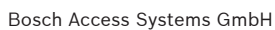
Authorization for Entry	Time model
✓ Building C	-- without --

Default authorization for personal group

-- none --

↑ ↑ ↓ ↓

NO authorization
✗ Building C - IDS off
✗ Building C - IDS on



10 Dni specjalne


Dni specjalne, zdefiniowane w tym oknie dialogowym mają inne ograniczenia niż dni tygodnia, w których przypadają. Model czasowy przydzielony do święta/dnia specjalnego zostanie zastosowany zamiast zwykłego modelu czasowego zaplanowanego na dany dzień tygodnia.




Wstępnie zdefiniowana lista dni specjalnych może być dowolnie zmieniana, zmniejszana lub uzupełniana. Nie mające zastosowania dni świąteczne/specjalne można dezaktywować lub skasować – wówczas w tych dniach obowiązywać będzie normalny model dzienny zwykłego dnia tygodnia. Mogą zostać dodane i indywidualnie zdefiniowane dni świąteczne/specjalne niewystępujące w systemie lub święta i dni specjalne obchodzone w kraju/siedzibie klienta.

Dzięki temu kalendarz może być mały: dni specjalne są powtarzane okresowo, co roku, i należy zdefiniować tylko wyjątki oraz zdarzenia nieregularne w danym roku.

10.1 Tworzenie i edytowanie

W programie Access PE zdefiniowana jest pewna ilość typowych świąt. W zależności od lokalizacji mogą być one zmieniane, można dodawać lub usuwać dni świąteczne.

 Special days




Name	Date
New Year's Day	01.01.*
Epiphany	06.01.*
Good Friday	@easter-2
Easter Sunday	@easter
Easter Monday	@easter+1
1st Mai	01.05.*
Whit Sunday	@easter+49
Whit Monday	@easter+50
1st Sunday in Advent	@advent1
2nd Sunday in Advent	@advent2
3rd Sunday in Advent	@advent3
4th Sunday in Advent	@advent4
Christmas Eve	24.12.*
Christmas Day	25.12.*
Boxing Day	26.12.*
New Year's Eve	31.12.*
Ullis Special	21.09.2016

☐ Deactivated

Categorie Holiday

☐ Priority higher than weekend

 Date

☒ active for offline locking system

Przyciski umieszczone nad polem listy posiadają następujące funkcje:



Utwórz nowy dzień świąteczny/specjalny



Edytuj dzień świąteczny/specjalny





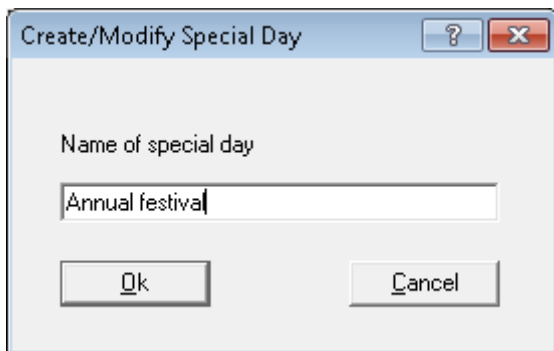
Usuń dzień świąteczny/specjalny

Uwaga!



Usuwanie wstępnie skonfigurowanych dni świątecznych/specjalnych, a szczególnie dni ze **zmiennymi datami** (np. Wielkanoc), nie jest zalecane. Jeżeli nie będą one używane, lepiej je dezaktywować. Dni świątecznych i specjalnych ze zmienną datą nie będzie można później wprowadzić w oknie dialogowym.

W przypadku korzystania z przycisku  lub przycisku  w celu dodawania lub modyfikacji dni świątecznych, otwarte zostanie następujące okno dialogowe, w którym należy wprowadzić nazwę:



Potwierdzenie wprowadzonych danych przyciskiem OK spowoduje wyświetlenie w polu listy zmienionej lub nowej nazwy. Po prawej stronie obok pola listy należy zdefiniować parametry dla zaznaczonego na liście elementu.

Deactivated (Nieaktywne)	Decyduje o tym, czy dany dzień świąteczny/specjalny będzie używany czy nie.
Category (Kategoria)	Aktywne dni świąteczne/specjalne można podzielić na 11 kategorii (święto, dzień specjalny, typ od 1 do 10) i przy tworzeniu modeli czasowych do każdej kategorii przypisać specjalne modele dzienne.

Priority higher than weekend (Priorytet wyższy niż weekend)	Decyduje o priorytetach w przypadku dni świątecznych powtarzających się co roku i przypadających niekiedy w sobotę lub niedzielę. Jeśli opcja jest zaznaczona, również w soboty/niedziele obowiązywać będzie model dzienny dnia świątecznego, w przeciwnym razie pierwszeństwo ma model dzienny soboty/niedzieli.
Data	W przypadku dnia świątecznego powtarzającego się co roku, zamiast roku należy wprowadzić gwiazdkę (*). Niektóre dni świąteczne (np. Boże Narodzenie) mają zawsze stałą datę.

11 Modele dzienne

Modele dzienne regulują fikcyjny przebieg dnia. Niezależnie od dnia tygodnia, model dzienny określa w jakich okresach dnia dostęp może zostać przydzielony lub zabroniony.


Dlatego też dla każdego innego przebiegu dnia należy zdefiniować indywidualny model dzienny.




Model dzienny może składać się z maksymalnie trzech przedziałów godzinowych o określonym czasie rozpoczęcia i zakończenia.

W przypadku stosowania modeli dziennych w modelach czasowych poszczególne modele dzienne zostaną przydzielone do określonych dni kalendarzowych.

11.1 Tworzenie i edytowanie

To okno dialogowe służy do tworzenia i edycji modeli dziennych, stosowanych w modelach czasowych.

 Day models

No.	Name
1	7 - 16 DM
2	16 to 7

periods

1st period

start

end

2nd period

start

end

3rd period

start

end

Po lewej stronie znajduje się lista wszystkich utworzonych dotychczas modeli dziennych.

Przyciski umieszczone nad polem listy posiadają następujące funkcje:





Utwórz nowy model dzienny

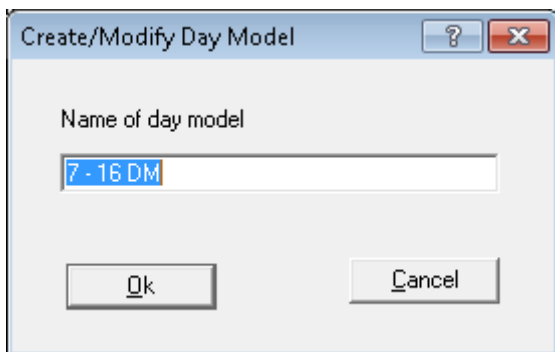


Edytuj zaznaczony model dzienny



Usuń zaznaczony model dzienny

Użyj przycisku , aby dodać lub przycisku , aby edytować modele dzienne:



Potwierdzenie wprowadzonych danych przyciskiem **OK** spowoduje wyświetlenie w polu listy zmienionej lub nowej nazwy. Po prawej stronie obok pola listy można zdefiniować okresy czasu, które mają obowiązywać w wybranym modelu dziennym. Model dzienny może składać się z maksymalnie trzech okresów.

Czas rozpoczęcia kolejnego przedziału czasowego musi być późniejszy od zakończenia poprzedniego przedziału. Aby na przykład utworzyć modele, których zakres przekracza północ, należy zdefiniować dwa przedziały czasowe:

1. Okres od: ... do 24:00
2. Okres od 00:00 do ...

12 Modele czasowe

Modele czasowe ograniczają dostęp do przydzielonych przejść do określonej ilości godzin w ciągu dnia. W ten sposób można na przykład odmówić dostępu w godzinach nocnych lub zezwolić na wejście po bardziej szczegółowej kontroli w weekendy.

Access PE wykorzystuje modele czasowe na kilka sposobów, przykładowo w połączeniu z opcjami/funkcjami:

- **Authorization groups** (Grupy uprawnień dostępu):

Modele czasowe mogą zostać przydzielone do wybranych uprawnień dostępu, aby używanie zawartych w tych uprawnieniach wejść było możliwe tylko w określonym czasie i określonych dniach. Jednocześnie można wykorzystać również uprawnienia dostępu, które nie mają żadnych ograniczeń czasowych.

- **Persons** (Osoby):

Modele czasowe przydzielane do osób ograniczają ogólne użycie karty do zdefiniowanego czasu.

- **Controllers and extension boards** (Kontrolery i moduły rozszerzeń):

Generowanie sygnałów wejścia i wyjścia przez kontrolery i moduły rozszerzeń może być regulowane na poziomie modelu czasowego.

- **Doors** (Drzwi):

Czasem udostępniania drzwi można sterować za pośrednictwem modeli czasu.

- **PIN codes** (Kody PIN):

Wpisanie kodu PIN jako dodatkowej opcji kontrolnej może być wymagane na przykład tylko poza czasem określonym w modelu czasowym.

- **Activation of a motor lock** (Załączenie elektrozamka):

Elektrozamek można skonfigurować tak, aby był załączony tylko w ramach określonego modelu czasowego.

Uwzględniając przeznaczenie modeli czasowych należy utworzyć je w różny sposób.

Przykład:

Jeśli modele czasowe mają być ograniczać dostęp osób do godzin 07:00 do 19:00 w dni robocze, a w weekendy od 09:00 do 15:00, wówczas konieczne są dwa modele:

1. z okresem czasu od 07:00 do 19:00
2. z okresem czasu od 09:00 do 15:00

Jeśli natomiast załączenie elektrozamka ma być regulowane modelem czasowym w taki sposób, aby aktywacja elektrozamka następowała poza wymienionymi wyżej godzinami, należy dwa modele dzienne tego modelu czasowego ustawić następująco:

1. z okresami czasu od 00:00 do 07:00 i od 19:00 do 24:00.
2. z okresami czasu od 00:00 do 09:00 i od 15:00 do 24:00.

Zastosowanie modeli czasowych

Modele czasowe, które są połączone z danymi osobowymi, są kontrolowane tylko, jeśli nie zostało zmienione ustawienie standardowe czytnika, a opcja **No time model check** (Nie sprawdzaj modelu czasowego *Wskazania i ustawianie parametrów*, Strona 110) nie jest zaznaczona.

Z uwagi na wielostronność zastosowania modeli czasowych i zagrożenie powielania przyporządkowań, zaleca się przestrzeganie następujących reguł rozwiązywania konfliktów:

- Jeżeli osobie przydzielono dostęp do określonych wejść na podstawie modelu czasowego i jeżeli tej samej osobie przydzielany jest dostęp do tych samych wejść bez modelu czasowego, wówczas obowiązują **luźniejsze** ograniczenia. To znaczy, że w tym przypadku model nie będzie stosowany.

Przykład:**Osoba otrzymuje następujące uprawnienia :**

- dostęp do wejść A, B, C i D w ramach modelu czasowego od 09:00 do 17:00 każdego dnia;
- indywidualne prawa dostępu do wejść B i D bez modelu czasowego.

Osoba ta ma obecnie dostęp do wejść A i C od 09:00 do 17:00 codziennie i nieograniczony dostęp do wejść B i D.

- Jeśli osobie przydzielono różne uprawnienia dostępu obejmujące te same wejścia, ale zarządzane różnymi modelami czasowymi, wówczas obowiązuje **połączenie** modeli czasowych.

Przykład:

Osoba otrzymuje następujące uprawnienia:

- dostęp do wejść A, B, C i D w ramach modelu czasowego od 07:00 do 13:00 każdego dnia;
- dostęp do wejść B, D, E i F w ramach modelu czasowego od 09:00 do 17:00 każdego dnia.

Osoba ta ma obecnie dostęp do wejść A i C od 07:00 do 13:00, wejść B i D od 07:00 do 17:00 oraz wejść E i F od 09:00 do 17:00.

- Jeśli danej osobie przydzielone zostaną grupy uprawnień dostępu z modelami czasu, a osoba ta dodatkowo otrzyma model czasowy do używania swojej karty identyfikacyjnej, wówczas obowiązuje **część wspólna** zdefiniowanych okresów czasowych.

Przykład:

Osoba otrzymuje następujące uprawnienia:

- grupa uprawnień dostępu do wejść A, B, C i D i model czasowy od 07:00 do 13:00 każdego dnia;
- grupa uprawnień dostępu do wejść B, D, E i F i model czasowy od 09:00 do 17:00 każdego dnia;
- oraz dodatkowo model pracy z okresem czasu od 11:00 do 19:00 każdego dnia.

Osoba ta ma obecnie dostęp do wejść A i C od 11:00 do 13:00 oraz wejść B, D, E i F od 11:00 do 17:00.

12.1 Tworzenie i edytowanie

To okno dialogowe wykorzystywane jest do tworzenia i modyfikowania modeli czasowych, które zależnie do zastosowania, uruchamiają pewne elementy systemu.

Po lewej stronie znajduje się lista wszystkich utworzonych dotychczas modeli czasowych. Przyciski umieszczone nad polem listy posiadają następujące funkcje:





Utwórz nowy model czasowy

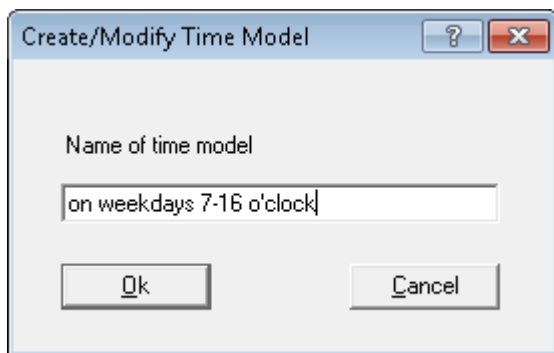


Edytuj zaznaczony model czasowy



Usuń zaznaczony model czasowy

Po naciśnięciu przycisku  w celu utworzenia nowego modelu czasowego lub przycisku  w celu zmiany istniejącego modelu czasowego, otwarte zostanie okno dialogowe, w którym należy wprowadzić nazwę:



Potwierdzenie wprowadzonych danych przyciskiem **OK** spowoduje wyświetlenie w polu listy zmienionej lub nowej nazwy. Następnie w prawej części okna dialogowego, w wybranym modelu czasowym, do każdego dnia tygodnia oraz dni świątecznych i dni specjalnych można przyporządkować modele dzienne (od 1 do 10).

Modele czasowe odzwierciedlać będą wciąż powtarzające się okresy jednego tygodnia. Tradycyjny przebieg dni tygodnia jest opisywany przypisanym modelem dziennym. Dodatkowo, modele dzienne dla normalnych dni tygodnia mogą zostać zastąpione modelami dziennymi dni świątecznych lub dni specjalnych, które przypadają w danych dniach tygodnia.


Uwaga!

Jeśli podczas tworzenia modelu czasowego do danego dnia tygodnia lub dnia specjalnego nie został przyporządkowany model dzienny (tj. pozostawione zostało ustawienie domyślne **<none>** (<brak>)), wówczas dni te będą traktowane jako posiadające modele dzienne bez przerw czasowych; tj. w tym dniu osoba, której przydzielono model czasowy **nie otrzyma zezwolenia na wejście**.

13 Teksty

Każdy wybrany podczas instalacji język aplikacji posiada swoją własną listę tekstów do wyświetlania na czytnikach i w komunikatach dziennika. Teksty na odpowiedniej liście języków są używane w aplikacji Logviewer (Analiza dziennika), na przykład w komunikatach dziennika tworzonych przy wybieraniu języka aplikacji.

13.1 Displaytexts (Wyświetlany tekst)

 Display texts

Language EN - English

	1st row	2nd row
Default message	Date hh:mm	
Welcome	Good morning	Name
Leaving	Good-bye	Name
Authorized	Access	
Not authorized	Not authorized	
Arm IDS?	Arm IDS?	Present card
Close all	Close all doors	and windows!
IDS is activated	IDS armed	
Enter PIN code	Please enter	PIN code: _
Entry not valid	Invalid input	
Please wait	Please wait...	
Reader is offline	Reader offline	
Wrong area	Wrong location	Name
Check required	Random screening	Name
Floor _[]	Please enter	floor number: _

W tym oknie dialogowym można zmienić niektóre teksty wyświetlane w czytniku kart. Wyświetlacz czytnika składa się z dwóch wierszy po 20 znaków każdy.



Przestroga!

W polu tekstu „Enter PIN code” (Wprowadź kod PIN) nie wolno usuwać znaku „_”, gdyż jest on niezbędny do prawidłowego wczytania kodu PIN.
























Teksty te są definiowane przez użytkownika i nie są tłumaczone automatycznie po zmianie języka interfejsu aplikacji. Jednak wykorzystując listę wyboru **Language** (Język) (nad oknem listy) można dla każdego zainstalowanego wariantu językowego Access PE wpisać odpowiedni tekst. Wówczas dane te wraz ze zmianą użytkownika zostaną przedstawione na jego język.

13.2 Event Log messages (Komunikaty dziennika zdarzeń)
























W tym oknie dialogowym można zmienić zarówno tekst, jak i kategorie wszystkich komunikatów generowanych przez kontrolery.

Event log messages





Language EN - English













I	Category	No.	Log text
	Information	1	Cold start (Boot)
	Information	2	Program start
	Alarm	3	Sabotage contact opened
	Message	4	Sabotage contact closed
	Error	5	Power fail
	Message	6	Power ok
	Error	7	Hardware error: @@@@
	Message	8	LAC online
	Error	9	LAC offline
	OK	10	online (ready)
	Malfunction	11	offline (out of order)
	Information	12	New program loaded
	Information	13	Reader initialized
	Information	14	New address assigned
	Error	15	Address not assigned
	Information	16	Personnel data initialized
	Error	17	Invalid parameter received
	Information	18	Program download OK
	Error	19	Error on program download
	Arriving	20	Access
	No access	21	Authorized but no entry
	No authorization	22	Not authorized
	No authorization	23	Card unknown, V: @ Co @ Cu @@@@ No @
	No authorization	24	Access denied, card invalid
	No authorization	25	Access denied, person locked
	No authorization	26	Access denied, card on black list
	No authorization	27	Access denied, locked: invalid PIN entered too often
	No authorization	28	Access denied, time model invalid


Dwukrotne kliknięcie pola, w którym ma zostać dokonana zmiana, w kolumnie **Category** (Kategoria), spowoduje otwarcie listy wyboru dostępnych kategorii.

	!	Category	No. /	Log text
		Information	1	Cold start (Boot)
		Information	2	Program start
		Alarm	3	Sabotage contact opened
		Message	4	Sabotage contact closed
		Error	5	Power fail
		Message	6	Power ok
		Error	7	Hardware error: @@@@ @@@@ @@@@
		Message	8	LAC online
		Error	9	LAC offline
		OK	10	online (ready)
		No access	11	offline (out of order)
		No authorization	12	New program loaded
		Malfunction	13	Reader initialized
		OK	14	New address assigned
		IDS armed	15	Address not assigned
		IDS not armed	16	Personnel data initialized
		Program Startup	17	Invalid parameter received
		Program Shutdown	18	Program download OK
		Operator action	19	Error on program download
		Information	20	Access
		Error	21	Authorized but no entry
		Arriving		
		No access		













Każda kategoria jest przedstawiona za pomocą niepowtarzalnego symbolu w pierwszej kolumnie. Symbole te służą również do klasyfikacji nadchodzących komunikatów dzienniku zdarzeń. Mogą zostać użyte następujące symbole i kategorie:

-  Dziennik zdarzeń niedostępny
-  Informacje
-  Komunikat
-  Błąd

	Alarm
	Przybycie
	Opuszczenie
	Brak dostępu
	Brak autoryzacji
	Usterka
	OK
	System sygnalizacji włamania uzbrojony
	System sygnalizacji włamania nieuzbrojony
	Uruchomienie programu
	Zamknięcie programu
	Działanie operatora

W drugiej kolumnie (z nagłówkiem **!**) należy wybrać komunikaty, które będą funkcjonować jako specjalne komunikaty alarmowe w oknie dialogowym **Alarm Management** (Zarządzanie alarmami). Dwukrotne kliknięcie w odpowiednim polu spowoduje ustawienie lub usunięcie symbolu alarmowego . Domyślnie podczas procedury instalacji jako komunikaty alarmowe definiowane są komunikaty z kategorii **Alarm** i **Error** (Błąd).

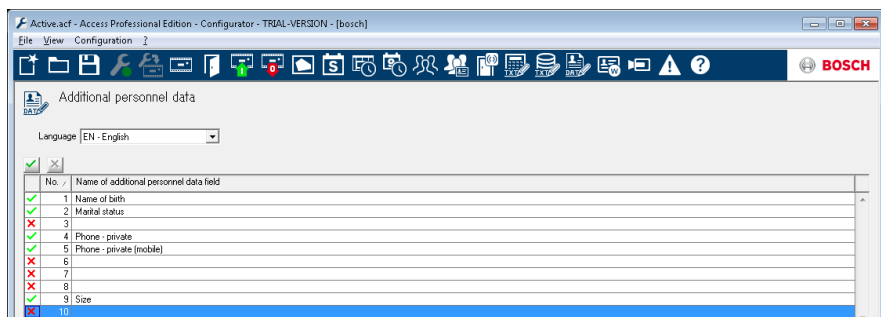
Żądany tekst można zmodyfikować przez dwukrotne kliknięcie pola, w którym ma zostać dokonana zmiana, w kolumnie **Log text** (Tekst dziennika).

	Category	No.	Log text
	Information	1	Cold start (Boot)
	Information	2	Program start
	Alarm	3	Sabotage contact opened
	Message	4	Sabotage contact closed
	Error	5	Power fail
	Message	6	Power ok
	Error	7	Hardware error: @@@@ @@@@ @@@@
	Message	8	LAC online
	Error	9	LAC offline
	OK	10	online (ready)
	Malfunction	11	offline (out of order)
	Information	12	New program loaded

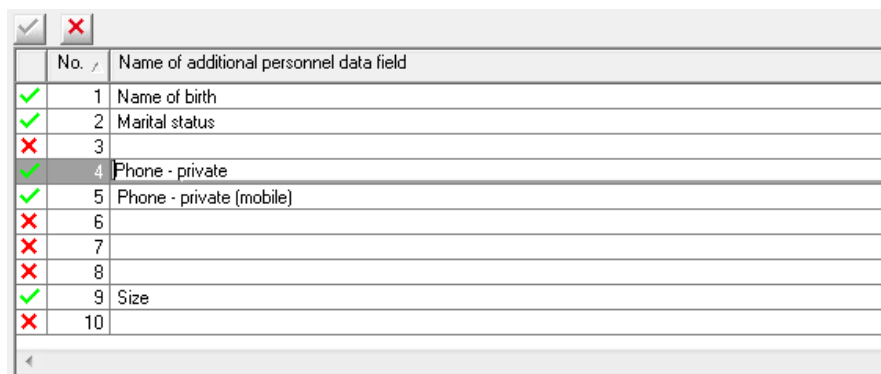
Teksty te są definiowane przez użytkownika i nie są tłumaczone automatycznie po zmianie języka interfejsu aplikacji. Jednak wykorzystując listę wyboru **Language** (Język) (nad oknem listy) można dla każdego zainstalowanego wariantu językowego Access PE wpisać odpowiedni tekst. Wówczas dane te wraz ze zmianą użytkownika zostaną przedstawione na jego język.

14 Additional Personnel data (Dodatkowe pola danych osobowych)





Oprócz wstępnie zdefiniowanych już pól wprowadzania danych osobowych, można jeszcze zdefiniować dziesięć dodatkowych.



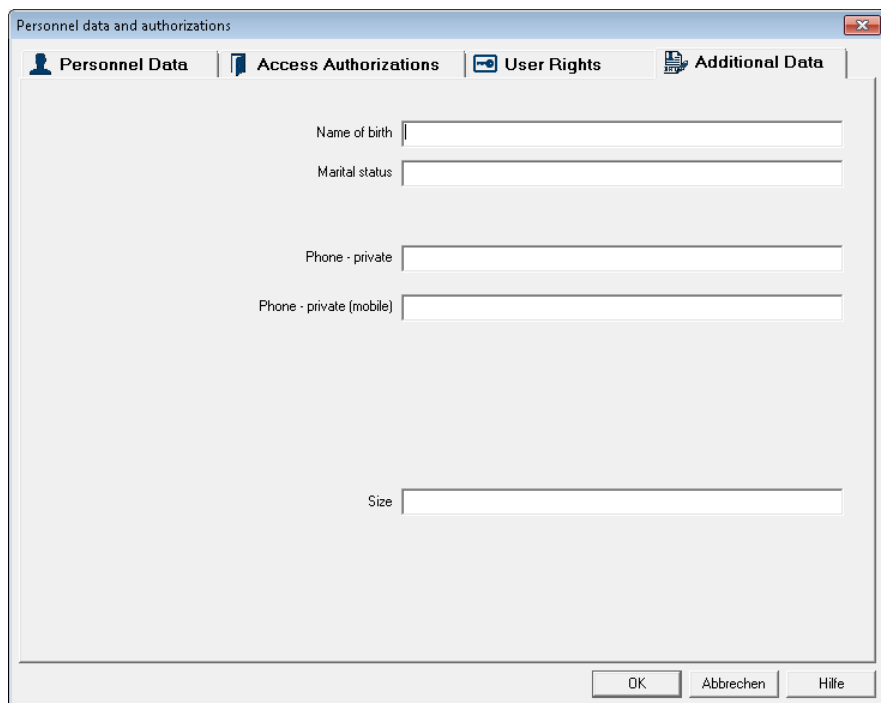
Pole listy zawiera dziesięć wierszy przeznaczonych dla nowych pól. Podwójne kliknięcie wybranego pola kolumny **Name of additional personnel data field** (Nazwa dodatkowego pola danych osobowych) umożliwi jego edycję i wprowadzenie nazwy.



Uwaga!

Nadanie nazwy nie powoduje uaktywnienia pola. Aktywacja jest wykonywana podwójnym kliknięciem przycisku  w pierwszej kolumnie lub kliknięciem przycisku . Kiedy pole jest aktywne, ikona  zastępowana jest ikoną .

Po aktywacji przynajmniej jednego nowego pola, w aplikacji Personnel Management (Zarządzanie personelem) pojawi się dodatkowa karta **Additional data** (Dodatkowe dane) (okno dialogowe danych osobowych i uprawnień dostępu). Kolejność pól nie musi być przy tym zachowana – w miejscach pól nieaktywnych występują odpowiednie luki.



Personnel data and authorizations

Personnel Data | Access Authorizations | User Rights | **Additional Data**

Name of birth

Marital status

Phone - private

Phone - private (mobile)

Size

OK Abbrechen Hilfe

W każdym polu można wpisać do 40 dowolnych znaków.

Uwaga!



Każde pole wprowadzania danych jest przyporządkowane do określonego pola bazy danych, więc istnieje możliwość segregacji według różnych treści lub sortowania tych danych w sprawozdaniach. Jeśli utworzono już zestawy danych zawierające dane dla poszczególnych pól dodatkowych, wówczas pole to nie może zostać zmienione bez zagrożenia utraty danych.

Nazwy dodatkowych pól danych są definiowane przez użytkownika i nie są tłumaczone automatycznie po zmianie języka interfejsu aplikacji. Wykorzystując listę wyboru **Language** (Język) (nad oknem listy) można dla każdego zainstalowanego wariantu językowego Access PE wpisać odpowiedni tekst. Wówczas dane te wraz ze zmianą użytkownika zostaną przedstawione na jego język.

Aktywacja/dezaktywacja dodatkowych pól

Dodatkowe pola należy nie tylko nazwać, lecz również aktywować. Aby to zrobić, kliknij dwukrotnie symbol w pierwszej

kolumnie lub kliknij przycisk . Symbol zmienia się z  na





Karta **Additional data** (Dodatkowe dane) zostanie wyświetlona w programie **Personnel Management** (Zarządzanie personelem), zawierającym zdefiniowane pole, dopiero po aktywacji przynajmniej jednego pola.



Uwaga!

Pola bez nazw mogą również zostać uaktywnione.

Aktywne pola można następnie także dezaktywować podwójnym kliknięciem przycisku  lub kliknięciem przycisku . Zostanie przy tym wyświetlony komunikat ostrzegawczy, w którym należy wybrać jedną z dwóch opcji dezaktywacji:

Uwaga!

Deactivation of fields deletes corresponding personnel data only if the field description is also deleted. (Dezaktywacja pól spowoduje usunięcie zamieszczonych tam danych osobowych tylko wtedy, gdy usunięty zostanie również opis pola). Do you wish to delete the field description and thus the personnel data also? (Czy chcesz usunąć opis pola, a przez to także dane osobowe?)

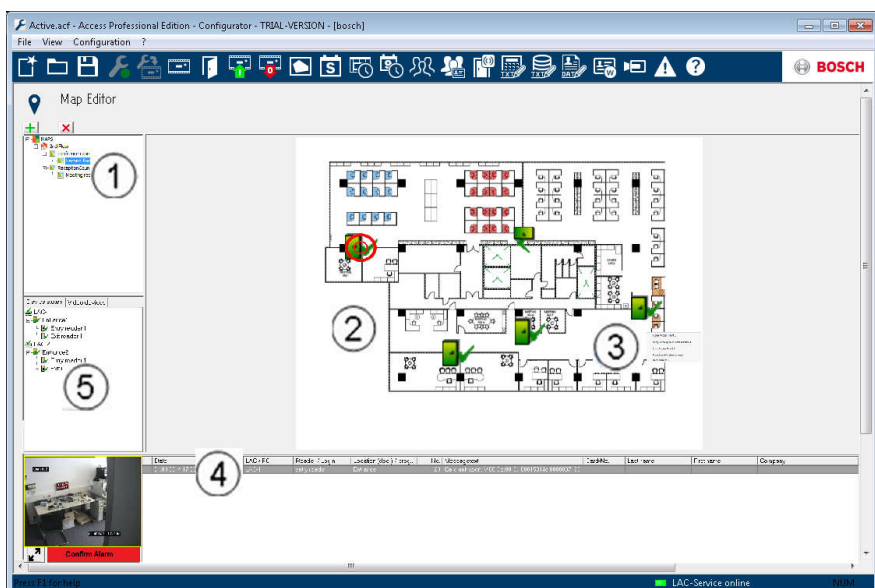


- | | |
|-----|---|
| Nie | = Dezaktywacja pola przy jednoczesnym zachowaniu jego nazwy i zawartości. |
| Tak | = Dezaktywacja pola oraz usunięcie jego nazwy i zawartości. |

15 Przeglądanie map i zarządzanie alarmami

Funkcja Przeglądanie map systemu Access PE umożliwia bezpośrednie sterowanie urządzeniami takimi jak przejścia, czytniki, kamery z poziomu samej mapy.

Dzięki liście alarmów systemu Access PE operator może zobaczyć wszystkie odbierane sygnały alarmowe. Operator może zaakceptować alarmy. W przypadku wystąpienia alarmu wyświetlona zostaje mapa lokalizacji. Animowana ikona wskazuje urządzenie, które aktywowało alarm. Pokazywany jest też podgląd na żywo, umożliwiający weryfikację alarmu.



1. Drzewo map
2. Aktywna mapa lokalizacji
3. Kontrola urządzenia z poziomu samej mapy, elementy sterujące są wyświetlane na mapie.
4. Lista alarmów z informacją o zdarzeniu (m.in. obrazem wideo)

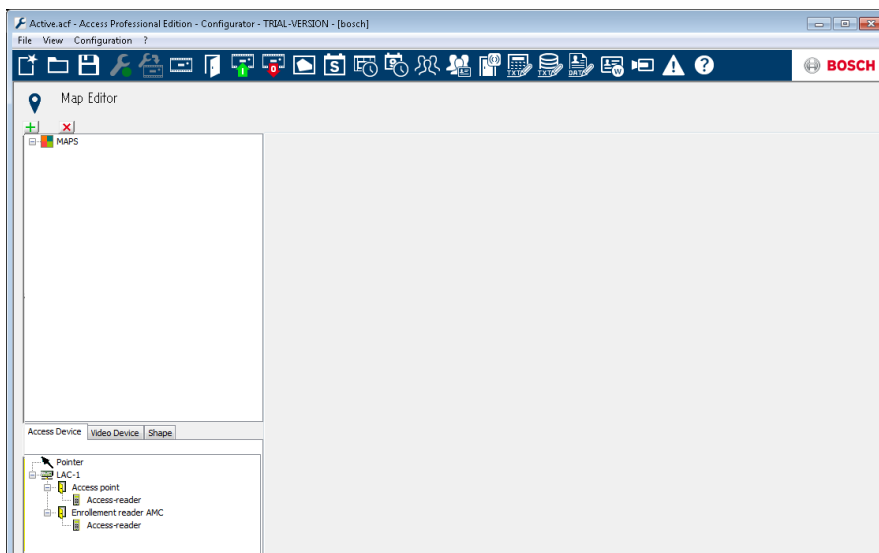
5. Drzewo map z przeglądem stanu i elementami sterującymi


Funkcje Przeglądanie map:

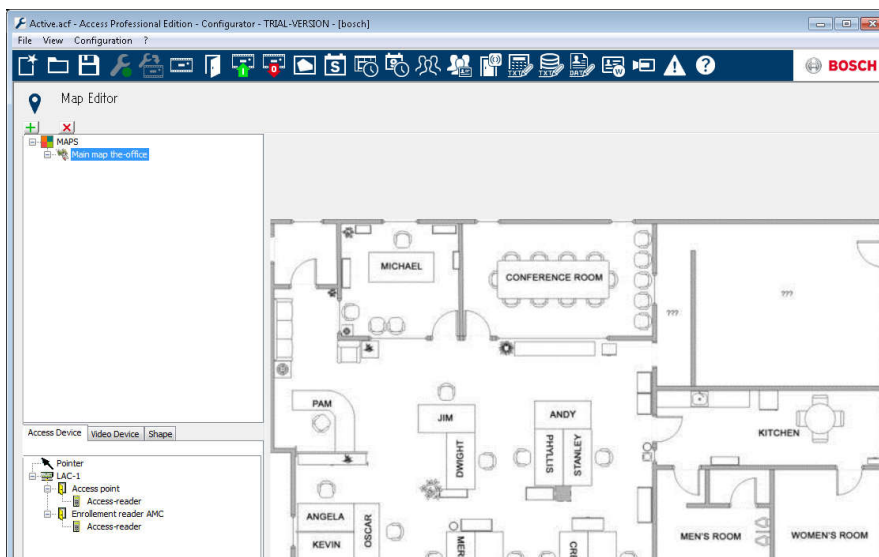
- Mapa główna ułatwiająca nawigację
- Nawigacja między widokiem z kamery i planem budynku poprzez hiperłącze
- Nawigacja poprzez strukturę drzewa urządzeń obsługująca do trzech poziomów
- Interaktywne mapy graficzne do alarmów ze integrowaną listą alarmów
- Widok na żywo i funkcja sterowania drzwiami z poziomu mapy oraz drzewa urządzeń
- 128 map na system
- 64 urządzenia na mapę
- 64 hiperłączy na mapę
- Maksymalnie 2 MB na mapę
- Przeglądarka map wykorzystuje standardowe formaty obrazów: .bmp, .jpg, .png

15.1 Konfiguracja mapy

Uruchom Edytor map



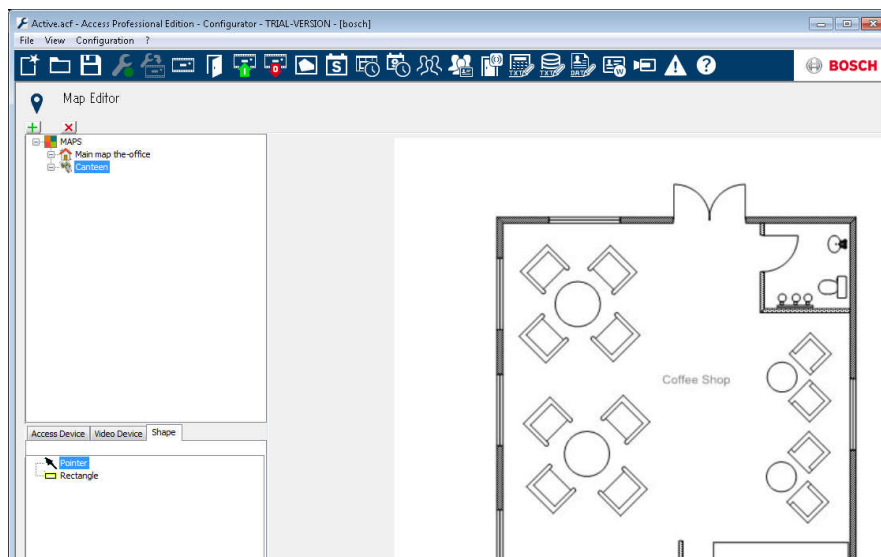
Aby dodać mapę, kliknij przycisk .



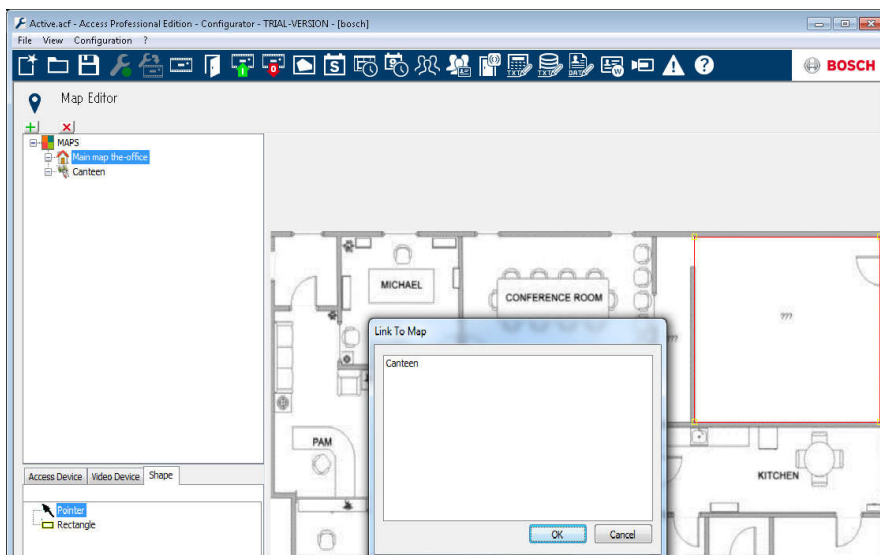
Mapa będzie wyświetlana w oknie dialogowym

- Mapę tą można skonfigurować jako **Mapa główna**

Dodaj do drzewa map widok szczegółowy np. widok stołówki.



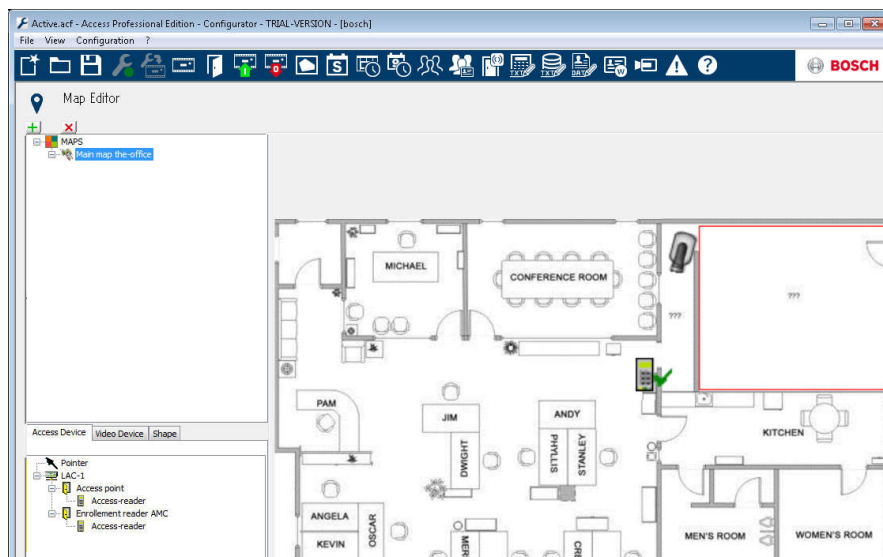
- Aby połączyć nową **Mapę stołówki** z mapą główną, należy przejść do zakładki **Kształt** i wybrać pozycję **Prostokąt**.
- Umieścić prostokąt nad obszarem mapy, który ma być wyświetlany jako widok szczegółowy (w przykładzie poniżej pokazany jako czerwony prostokąt).
- Wybierz na wyświetlaczu **Łącze do mapy** odpowiedni widok szczegółowy, w tym przypadku będzie to „Stołówka”.



15.2 Dodawanie urządzenia do mapy

Wybierz zakładkę **Urządzenia** i dodaj urządzenia do mapy przeciągając je myszą na obszar mapy. W poniższym przykładzie zostały dodane następujące urządzenia:

- Jeden punkt dostępu
- Jeden czytnik
- Dwie kamery



- Kliknij urządzenie na mapie i zmień jego rozmiar trzymając naciśnięty przycisk myszy,
- Kliknij urządzenie i obróć je za pomocą kółka przewijania myszy.

Typy urządzeń	Elementy sterujące
Punkt dostępu (przejście)	Otwórz drzwi
	Otwórz drzwi na stałe/Resetuj zezwolenie na stałe
	Zablokuj drzwi/Odblokuj drzwi
	Przednia kamera identyfikacyjna
	Tylna kamera identyfikacyjna
	Kamera z tyłu
	Kamera z przodu

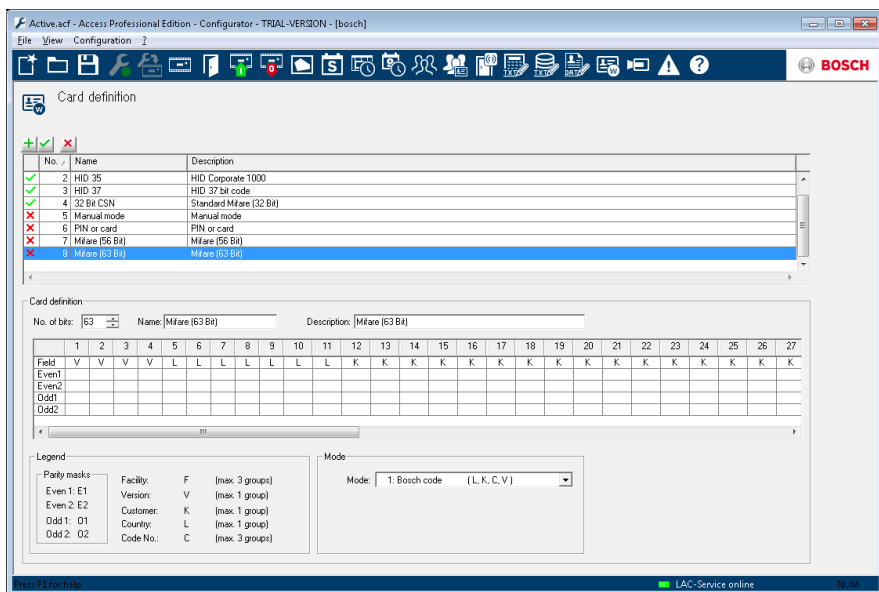
Typy urządzeń	Elementy sterujące
Czytnik	Wszystkie elementy sterujące wejścia
Camera (Kamera)	Wideo na żywo

Typy urządzeń	Alarmy
Punkt dostępu (przejście)	Drzwi otwarte bez autoryzacji
	Drzwi otwarte zbyt długo
	(*Wszystkie alarmy czytników są takie same, jak alarmy wejść)
Czytnik	Błąd czytnika
Camera (Kamera)	nie dot.

*) Te zdarzenia alarmowe mogą być dostosowywane przez użytkowników. Oznacza to, że można skonfigurować dowolne zdarzenie jako zdarzenie alarmowe za pomocą komunikatu **AcConfig -> Event Log** (AcConfig -> Dziennik zdarzeń). Podwójne kliknięcie w drugiej kolumnie spowoduje uaktywnienie alarmu.

16 Definicja karty

W tym oknie definiowane są dane, które rejestruje czytnik, tak aby również w terminie późniejszym system mógł zapisywać nowe definicje kart.




Sterowanie listami zawiera istniejące definicje kart. Domyślne ustawienia systemu obejmują sześć standardowych wpisów, z których pierwsze cztery są aktywne (oznaczone zielonym haczykiem w pierwszej kolumnie). Wszystkie ustawienia, za wyjątkiem **Input Mode** (Tryb wprowadzania danych) są zabezpieczone przed zapisem i nie mogą być modyfikowane ani usuwane.



Uwaga!

W przypadku używania kontrolerów i czytników Wiegand, aby użyć kodu PIN identyfikacyjnego, uzbrojenia lub drzwi, należy aktywować definicję karty Wiegand **PIN lub karta** (Nr 6).

Aby dodać nową definicję, należy kliknąć przycisk . Na podstawie danych producenta wybierana jest i wprowadzana liczba bitów (**number of bits**) oraz ich podział na elementy kodu.



Uwaga!

Maksymalna liczba bitów dla wszystkich definicji wynosi 64.
Maksymalna liczba bitów dla każdego elementu kodu (urządzenie, wersja, klient, kraj i numer kodowy) wynosi 32.

Aby ułatwić rozróżnienie definicji karty, można nadać jej jednoznaczną nazwę oraz opis.

Wprowadzenie wartości w polu **No. of bits** (Liczba bitów) zmienia odpowiednio ilość kolumn na poniższej liście.

Wyświetlane pięć wierszy umożliwia, według potrzeby, aktywację/dezaktywację poszczególnych bitów.

Dla każdej kolumny wiersza **Field** (Pole), wprowadzając poniższe wartości, można teraz określić interpretację poszczególnych części kodu.

- F Urządzenie: element kodu określający przynależność do urządzenia.
- V Wersja: element kodu określający wariant wersji.
- K Element kodu określający klienta.
- L Kraj: element kodu określający kod kraju.

C	Nr kodu: element kodu określający numer karty.		
E1	Parzyste 1: bit anulowania dla pierwszej maski parowania parzystości	Po wprowadzeniu jednej z tych wartości, zaznaczone zostanie pole wyboru obok odpowiedniego wiersza.	
E2	Parzyste 2: bit anulowania dla drugiej maski parowania parzystości		
O1	Nieparzyste 1: bit anulowania dla pierwszej maski parowania nieparzystości		
O2	Nieparzyste 2: bit anulowania dla drugiej maski parowania nieparzystości		
1	Stałe wartości bitów zawartych w kodzie		
0			

Definiując **Manual Mode** (Tryb ręczny) lub tworząc nowy przykład, można określić **Mode** (Tryb), który będzie wyznaczał sposób odczytywania kodu; np. w przypadku wybrania trybu **PIN or card** (PIN lub karta) odczytany zostanie tylko numer kodowy, tj. tylko elementy oznaczone literą **C**. Dostępne są następujące warianty trybów:

Numer seryjny	Tryb	Sprawdzone elementy kodu
0	Urządzenie + nr kodu	F,C
1	Kod Bosch	L,K,C,V
100	Ręczny	C
200	PIN lub karta	C

Wyjaśnienie:

Wysyłany przez czytnik w momencie prezentacji karty identyfikacyjnej „telegram” ma postać szeregu zer i jedynek. W zależności od typu czytnika, długość tych telegramów, czyli liczba bitów, jest dokładnie określona. Taki telegram, oprócz danych użytkowych zapisywanych w postaci danych kodu, zawiera również wartości kontrolne umożliwiające rozpoznawanie go jako telegramu karty oraz weryfikację prawidłowości przekazu. Weryfikację prawidłowości przekazu przeprowadza się na podstawie bitów parzystości, które jako suma kontrolna cyfr wybranych bitów w masce muszą wynosić zero (parowanie parzystości) lub jeden (parowanie nieparzystości). Kontrolery można skonfigurować tak, aby obliczały jedną lub dwie sumy kontrolne cyfr dla parowania parzystości i jedną lub dwie sumy kontrolne cyfr dla parowania nieparzystości. Na liście w poszczególnych wierszach można dla sumy kontrolnej cyfr parzystości (Parzyste1, Parzyste2, Nieparzyste1 i Nieparzyste2) zaznaczyć bity, które mają zostać włączone do sumy kontrolnej.

W najwyższym wierszu (polu) dla każdej wykorzystanej sumy cyfr ustalany jest jeden bit, który wyrównuje sumę cyfr zgodnie z typem parzystości. Jeśli opcja parzystości nie jest wykorzystywana (Parzyste1, Parzyste2, Nieparzyste1, Nieparzyste2), wiersz pozostanie pusty.

Aktywacja/dezaktywacja definicji kart

Symbol w pierwszej kolumnie pola listy oznacza stan aktywacji poszczególnych definicji kart.



aktywne



nieaktywne

Stan można zmienić, klikając dwukrotnie symbol.

Wyświetlane komunikaty informują o konsekwencjach usunięcia definicji karty, która jest w użyciu.

Uwaga!

Incorrect card encoding or a bad combination may lead to all cards become unreadable! (Nieprawidłowe kodowanie karty lub nieprawidłowa kombinacja mogą spowodować, że kart nie będzie można odczytać!) Do you really wish to activate the selected card encoding? (Czy naprawdę chcesz aktywować wybrane kodowanie kart?).

Uwaga!

All current cards using this encoding will become unreadable! (Odczyt wszystkich bieżących kart wykorzystujących to kodowanie nie będzie możliwy!) Do you really wish to deactivate the selected card encoding? (Czy naprawdę chcesz dezaktywować wybrane kodowanie kart?).

17 Dodatek

17.1 Sygnały

Lista dostępnych sygnałów wejściowych i wyjściowych.

Sygnały wejściowe	Opis
Czujnik drzwi	
Przycisk żądania wyjścia	Przycisk otwarcia drzwi.
Czujnik rygla	Służy wyłącznie do przekazywania komunikatów. Nie zapewnia funkcji sterowania.
Wejście zablokowane	Służy do tymczasowego blokowania przeciwnych drzwi w słuzach. Umożliwia także blokowanie na stałe.
Sabotaż	Sygnał sabotażu z kontrolera zewnętrznego.
Bramka obrotowa w pozycji normalnej	Bramka obrotowa jest zamknięta.
Przejsście zakończone	Przejsście 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.

Sygnaly wejściowe	Opis
System sygnalizacji włamania jest uzbrojony	System sygnalizacji włamania jest uzbrojony.
Przycisk żądania uzbrojenia systemu sygnalizacji włamania	Przycisk uzbrajania systemu sygnalizacji włamania.
Włączenie otwarcia lokalnego	Sygnal zostanie użyty, jeśli układ drzwi otworzy drzwi bez udziału kontrolera AMC. Kontroler AMC nie wyśle komunikatu o włamaniu, lecz o „lokalnym otwarciu drzwi”.

Sygnaly wyjściowe	Opis
Automat do otwierania drzwi	
Zamknięcie przeciwnych drzwi śluzy	Zamyka drzwi z przeciwnej strony śluzy. Zostanie użyty po otwarciu drzwi.
Wyciszenie alarmu	...do systemu sygnalizacji włamania. Zostanie użyty, kiedy drzwi są otwarte, aby uniknąć utworzenia przez system sygnalizacji włamania komunikatu o włamaniu.
Zielony wskaźnik	Zielony wskaźnik świeci, kiedy drzwi są otwarte.

Sygnaly wyjściowe	Opis
Door open too long (Drzwi są otwarte zbyt długo)	Impuls trwający 3 s. Jeśli drzwi są otwarte zbyt długo.
Aktywacja kamery	Kamera zostanie włączona na początku przejścia.
Bramka obrotowa otwarta dla przechodzenia do wewnątrz	
Bramka obrotowa otwarta dla przechodzenia na zewnątrz	
Drzwi są otwarte na stałe	Informuje, że drzwi są otwarte na stałe.
Uzbrojenie systemu sygnalizacji włamania	Impuls lub stałe połączenie umożliwiające uzbrojenie systemu sygnalizacji włamania.
Rozbrojenie systemu sygnalizacji włamania	Impuls umożliwiający rozbrojenie systemu sygnalizacji włamania.

17.2 Domyślne modele drzwi

Standardowe modele drzwi

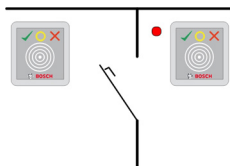
Dostępne są następujące domyślne modele drzwi:

- 01a Pojedyncze drzwi z czytnikiem wejścia i wyjścia
- 01b Pojedyncze drzwi z czytnikiem wejścia i przyciskiem
- 01c Pojedyncze drzwi z czytnikiem wejścia
- 03a Kontrolowana bramka obrotowa z czytnikiem wejścia i wyjścia
- 03b Kontrolowana bramka obrotowa z czytnikiem wejścia i przyciskiem
- 03c Kontrolowana bramka obrotowa z czytnikiem wejścia
- 06c Rejestracja przez AMC – brak kontroli wejść!
- 07a Winda z maksymalnie 16 piętrami
- 07b Winda z maksymalnie 16 piętrami
- 10a Pojedyncze drzwi z czytnikiem wejścia i wyjścia oraz funkcją ponownego uzbrojenia systemu sygnalizacji włamania
- 10b Pojedyncze drzwi z czytnikiem wejścia, przyciskiem otwierania drzwi oraz funkcją ponownego uzbrojenia systemu sygnalizacji włamania
- 10c Pojedyncze drzwi z czytnikiem wejścia oraz funkcją ponownego uzbrojenia systemu sygnalizacji włamania
- 10d Pojedyncze drzwi z czytnikiem wejścia i wyjścia oraz zdecentralizowaną funkcją ponownego uzbrojenia systemu sygnalizacji włamania
- 10e Pojedyncze drzwi z czytnikiem wejścia, przyciskiem otwierania drzwi oraz zdecentralizowaną funkcją ponownego uzbrojenia systemu sygnalizacji włamania
- 10f Pojedyncze drzwi z czytnikiem wejścia oraz zdecentralizowaną funkcją ponownego uzbrojenia systemu sygnalizacji włamania

- 14a Pojedyncze drzwi z czytnikiem wejścia i wyjścia oraz funkcją ponownego uzbrojenia systemu sygnalizacji włamania (uprawnienie do uzbrojenia)
- 14b Pojedyncze drzwi z czytnikiem wejścia, przyciskiem otwierania drzwi oraz funkcją ponownego uzbrojenia systemu sygnalizacji włamania (uprawnienie do uzbrojenia)
- 14c Pojedyncze drzwi z czytnikiem wejścia oraz funkcją ponownego uzbrojenia systemu sygnalizacji włamania
- 14d Pojedyncze drzwi z czytnikiem wejścia i wyjścia oraz zdecentralizowaną funkcją ponownego uzbrojenia systemu sygnalizacji włamania
- 14e Pojedyncze drzwi z czytnikiem wejścia, przyciskiem otwierania drzwi oraz zdecentralizowaną funkcją ponownego uzbrojenia systemu sygnalizacji włamania
- 14f Pojedyncze drzwi z czytnikiem wejścia oraz zdecentralizowaną funkcją ponownego uzbrojenia systemu sygnalizacji włamania

17.3 Model drzwi 01

Drzwi pojedyncze



Sygnaly:

Sygnaly wejściowe	Sygnaly wyjściowe
Czujnik drzwi	Automat do otwierania drzwi
Przycisk otwierania drzwi: drzwi otwarte	Śluza: blokada przeciwnych drzwi
Czujnik rygla	Wyciszenie alarmu
Wejście zablokowane	Zielony wskaźnik
Sygnal sabotażu	Aktywacja kamery
	Drzwi są otwarte zbyt długo

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

Uwaga:

Zablokowanie śluzy jest możliwe tylko wtedy, gdy w ustawieniach parametrów drzwi stanowią część śluzy.

Jeśli drzwi nie są częścią śluzy, sygnał wejściowy 03 jest interpretowany jako blokada czytnika. W takim przypadku w chwili pojawienia się sygnału wejściowego 03 czytnik zostaje zablokowany.

Wyciszenie alarmu jest skuteczne tylko wówczas, gdy czas wyciszenia przed otwarciem drzwi jest większy od 0.

Istnieje możliwość dołączenia dodatkowych czytników kart identyfikacyjnych. Dzięki zastosowaniu drugich drzwi z funkcją blokowania można stworzyć śluzę pozwalającą na zabezpieczenie wejścia/wyjścia personelu. Jest to korzystne w przypadku przejazdów dla samochodów, zalecany jest jednak montaż dodatkowego czytnika do obsługi z samochodów osobowych i ciężarowych.

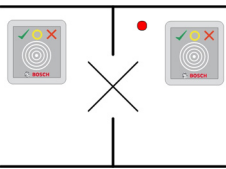


Uwaga!

Funkcja dostępu wyłącznie dla pojedynczych osób może zostać ustawiona wyłącznie w przypadku modelu drzwi 03.

17.4 Model drzwi 03

Kontrolowana bramka obrotowa



Sygnaly:

Sygnaly wejściowe	Sygnaly wyjściowe
Bramka obrotowa w pozycji normalnej	Bramka obrotowa otwarta dla przechodzenia do wewnątrz
Przycisk otwierania drzwi: drzwi otwarte	Bramka obrotowa otwarta dla przechodzenia na zewnątrz
Wejście zablokowane	Śluz: blokada przeciwnych drzwi
Sygnał sabotażu	Wyciszenie alarmu
	Aktywacja kamery
	Drzwi są otwarte zbyt długo

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

Uwaga:

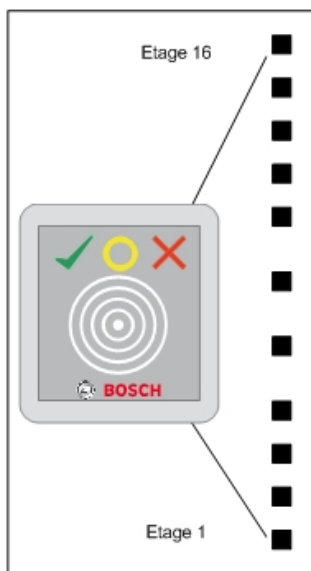
Zablokowanie śluzy jest możliwe tylko wtedy, gdy drzwi są skonfigurowane jako część śluzy. Jeśli drzwi nie są częścią śluzy, sygnał wejściowy 03 jest interpretowany jako blokada czytnika. W takim przypadku w chwili pojawienia się sygnału wejściowego 03 czytnik zostaje zablokowany.

Dzięki zastosowaniu drugich drzwi z funkcją blokowania można stworzyć śluzę pozwalającą na zabezpieczenie wejścia/wyjścia personelu. Zależnie od konstrukcji wejście to może umożliwiać przechodzenie wyłącznie pojedynczo.

17.5 Model drzwi 06c

Model drzwi 06c umożliwia skonfigurowanie czytnika podłączonego do kontrolera AMC jako urządzenia rejestrującego. Nie umożliwia sterowania wejściami.

17.6 Model drzwi 07



Warianty modelu:

- | | |
|-----|---------------------------|
| 07a | Winda |
| 07b | Winda z wejściem czytnika |

Uwaga!

Standardowo jednego kontrolera AMC2 można używać do obsługi 8 pięter. W przypadku spełnienia następujących warunków wstępnych istnieje możliwość podłączenia większej liczby wejść:

64 piętra w przypadku używania kontrolerów Wiegand (AMC2 4W + AMC2 4W-EXT + 3 AMC2 16I-16O-EXT)

56 pięter w przypadku używania kontrolerów RS 485 (AMC2 4R4 + 3 AMC2 16I-16O-EXT)

Sygnały wejścia modelu 07a:

Sygnały wejściowe	Sygnały wyjściowe
Dostępne	Piętro 01
Dostępne	Piętro 02
Dostępne	Piętro 03
Dostępne	Piętro 04
...	...
Dostępne	Piętro 16

Procedura:

Najpierw posiadacz karty przywołuje windę. Może tego dokonać za pośrednictwem przycisku windy lub za pośrednictwem czytnika kart (np. model drzwi 01c).

W windzie znajduje się kolejny czytnik kart (model drzwi 07a). Czytnik ten zapewnia dostęp do tych pięter, do których uprawnienia posiadana przez użytkownika karta identyfikacyjna. Piętra, do których dostęp jest uprawniony, zostaną wyświetlone użytkownikowi, przykładowo przez podświetlenie przycisków tylko dla tych pięter. Użytkownik może wybrać wówczas jedno z pięter do wstępu na które jest uprawniony.

Sygnały wejścia modelu 07b:

Sygnały wejściowe	Sygnały wyjściowe
Klawisz wejścia – piętro 01	Piętro 01
Klawisz wejścia – piętro 02	Piętro 02
Klawisz wejścia – piętro 03	Piętro 03
Klawisz wejścia – piętro 04	Piętro 04
...	...
Klawisz wejścia – piętro 16	Piętro 16

Procedura:

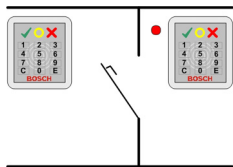
Najpierw posiadacz karty przywołuje windę. Może tego dokonać za pośrednictwem przycisku windy lub za pośrednictwem czytnika kart (np. model drzwi 01c).

W windzie posiadacz karty przesuwa ją przez kolejny czytnik kart (model drzwi 07b), a następnie naciska przycisk wybranego piętra. Kontroler AMC sprawdza, czy użytkownik ma uprawnienie dostępu do wybranego piętra. Jeśli tak, winda jedzie na to piętro.

Dodatkowo, ten model drzwi posiada parametr Public Access (Dostęp publiczny), który może zostać indywidualnie ustawiony dla każdego z pięter. Jeśli ustawiony jest ten parametr, uprawnienie dostępu do piętra nie jest sprawdzane, tj. każdy użytkownik może wejść na to piętro. Dodatkowo, dostęp publiczny może zostać powiązany z modelem czasowym, tak że uprawnienie dostępu sprawdzane jest przez AMC jedynie poza godzinami określonymi w modelu czasowym.

17.7 Model drzwi 10

Pojedyncze drzwi z funkcją uzbrojenia/rozbrojenia systemu sygnalizacji włamania



Sygnaly:

Sygnaly wejściowe	Sygnaly wyjściowe
Czujnik drzwi	Automat do otwierania drzwi
Przycisk otwierania drzwi: drzwi otwarte	Rozbrojenie systemu sygnalizacji włamania (tylko dla modeli d i f z impulsem 1 s)
System sygnalizacji włamania gotowy do uzbrojenia	Kamera/elektrozamek
System sygnalizacji włamania uzbrojony	Uzbrojenie systemu sygnalizacji włamania (tylko dla modeli d i f z impulsem 1 s)
Sygnal sabotażu	Drzwi są otwarte zbyt długo (włamanie)
Uzbrajanie systemu sygnalizacji włamania	

Warianty modelu:

- | | |
|-----|---|
| 10a | Pojedyncze drzwi z czytnikiem wejścia i wyjścia oraz funkcją ponownego uzbrojenia systemu sygnalizacji włamania |
| 10b | Pojedyncze drzwi z czytnikiem wejścia, przyciskiem otwierania drzwi oraz funkcją ponownego uzbrojenia systemu sygnalizacji włamania |
| 10c | Pojedyncze drzwi z czytnikiem wejścia oraz funkcją ponownego uzbrojenia systemu sygnalizacji włamania |
| 10d | Pojedyncze drzwi z czytnikiem wejścia i wyjścia oraz zdecentralizowaną funkcją ponownego uzbrojenia systemu sygnalizacji włamania |
| 10e | Pojedyncze drzwi z czytnikiem wejścia, przyciskiem otwierania drzwi oraz zdecentralizowaną funkcją ponownego uzbrojenia systemu sygnalizacji włamania |
| 10f | Pojedyncze drzwi z czytnikiem wejścia oraz zdecentralizowaną funkcją ponownego uzbrojenia systemu sygnalizacji włamania |

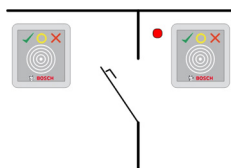
Uwagi:

Za pomocą przycisku **E** na czytniku wejścia można uzbroić system sygnalizacji włamania. W tym przypadku niezbędna jest również karta z uprawnieniami oraz wprowadzenie kodu PIN. Rozbrojenie systemu sygnalizacji włamania następuje po pierwszym uprawnionym wejściu, przy czym w takim wypadku też konieczna jest identyfikacja za pomocą kodu PIN. W modelach od a do c sterowanie tym odbywa się przez sygnał wyjściowy uzbrojenia/rozbrojenia systemu sygnalizacji włamania.

W modelach **d** do **f** uzbrojenie lub rozbrojenie jest wyzwalane przez oddzielny impuls trwający 1 sekundę. Podłączony przekaźnik bistabilny może kontrolować system sygnalizacji włamania dla kilku drzwi (DCU / moduły sterowania drzwiami), podczas gdy sygnały wymagają podłączenia logicznego LUB do przekaźnika. Sygnały **IDS is armed** (System sygnalizacji włamania jest uzbrojony) i **IDS is disarmed** (System sygnalizacji włamania jest rozbrojony) należy powielić dla wszystkich podłączonych DCU.

17.8 Model drzwi 14

Drzwi ze sterowaniem systemem sygnalizacji włamania



Sygnały:

Sygnały wejściowe	Sygnały wyjściowe
Czujnik drzwi	Automat do otwierania drzwi
Przycisk otwierania drzwi: drzwi otwarte	Rozbrojenie systemu sygnalizacji włamania (tylko dla modeli d i f z impulsem 1 s)
System sygnalizacji włamania gotowy do uzbrojenia	Kamera/elektrozamek
System sygnalizacji włamania uzbrojony	Uzbrojenie systemu sygnalizacji włamania (tylko dla modeli d i f z impulsem 1 s)
Sygnał sabotażu	Drzwi są otwarte zbyt długo (włamanie)
Uzbrajanie systemu sygnalizacji włamania	

Warianty modelu:

- | | |
|-----|---|
| 14a | Pojedyncze drzwi z czytnikiem wejścia i wyjścia oraz funkcją uzbrojenia/rozbrojenia systemu sygnalizacji włamania |
| 14b | Pojedyncze drzwi z czytnikiem wejścia, przyciskiem otwierania drzwi oraz funkcją uzbrojenia/rozbrojenia systemu sygnalizacji włamania |
| 14c | Pojedyncze drzwi z czytnikiem wejścia oraz funkcją uzbrojenia/rozbrojenia systemu sygnalizacji włamania |
| 14d | Pojedyncze drzwi z czytnikiem wejścia i wyjścia oraz zdecentralizowaną funkcją uzbrojenia/rozbrojenia systemu sygnalizacji włamania |
| 14e | Pojedyncze drzwi z czytnikiem wejścia, przyciskiem otwierania drzwi oraz zdecentralizowaną funkcją uzbrojenia/rozbrojenia systemu sygnalizacji włamania |
| 14f | Pojedyncze drzwi z czytnikiem wejścia oraz zdecentralizowaną funkcją uzbrojenia/rozbrojenia systemu sygnalizacji włamania |

Uwagi:

W modelach 14, w przeciwieństwie do modeli 10, można stosować czytniki z klawiaturą lub bez. Kolejna różnica polega na przydzielaniu uprawnień do uzbrajania i rozbrajania systemu sygnalizacji włamania: tylko posiadacz identyfikatora z odpowiednimi uprawnieniami może uzbrajać lub rozbrajać system sygnalizacji włamania.

Procedura uzbrajania i rozbrajania systemu nie odbywa się tu za pomocą kodu PIN, lecz przy użyciu przycisku w pobliżu czytnika, posiadającego taką samą funkcję, jak przycisk 7 w klawiaturach czytników. Po naciśnięciu tego przycisku stan instalacji zostanie wskazany kolorową diodą LED czytnika.

- Nieuzbrojony = naprzemienne miganie światła zielonego i czerwonego
- Uzbrojony = stałe światło czerwone

Zbliżenie identyfikatora z uprawnieniami spowoduje uzbrojenie systemu sygnalizacji włamania.

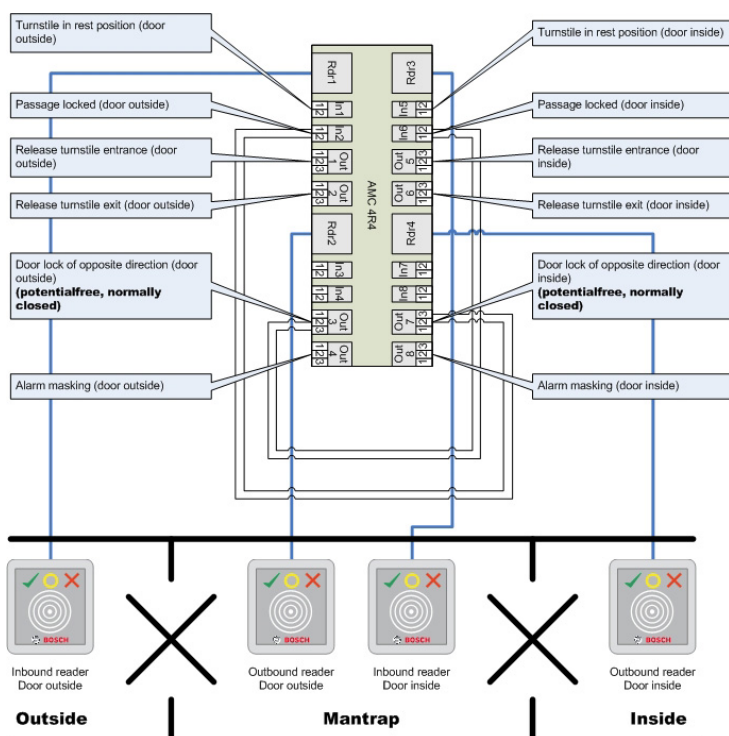
Rozbrojenie następuje w wyniku naciśnięcia przycisku i zbliżenia identyfikatora z uprawnieniami.

W tym przypadku drzwi nie zostaną automatycznie otwarte. W tym celu należy ponownie, po rozbrojeniu, zbliżyć identyfikator.

17.9 Przykłady konfiguracji służ osobowych

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).

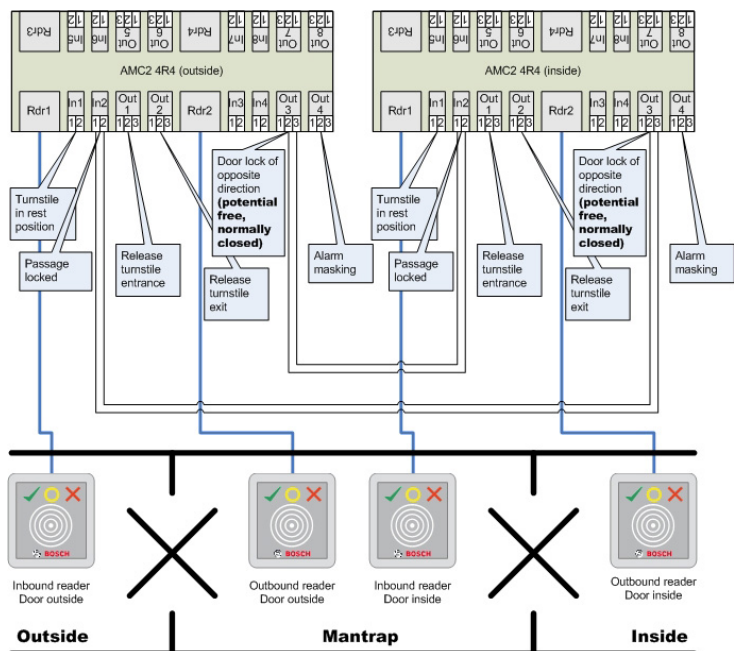
Konfiguracja służi osobowej z dwoma bramkami obrotowymi (DM 03a)



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

Uwaga!

Sygnał wyjściowy (Out 3 (Wyjście 3)) powinien zostać ustawiony jako beznapięciowy (tryb suchy). Sygnał „door lock of opposite direction” (blokada drzwi dla kierunku przeciwnego) musi zostać ustawiony jako zamknięty (oporność=0) przy wyłączeniu zasilania. W przypadku wyjść 3 i 7 użyć styków normalnie zamkniętych (NC).

Konfiguracja ochrony miejsc specjalnych z dwiema bramkami obrotowymi (DM 03a), których obsługa podzielona jest między dwa kontrolery.

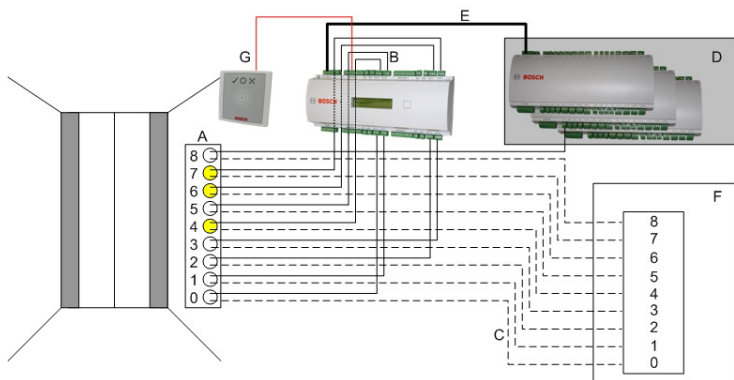
Połączenia do blokady drzwi dla kierunku przeciwnego zapewniają, że w danym momencie można otworzyć tylko jedną bramkę obrotową.

Uwaga!

Sygnał wyjściowy (Out 3 (Wyjście 3)) powinien zostać ustawiony jako beznapięciowy (tryb suchy). Sygnał „door lock of opposite direction” (blokada drzwi dla kierunku przeciwnego) musi zostać ustawiony jako zamknięty (oporność=0) przy wyłączeniu zasilania. W przypadku wyjść 3 i 7 użyć styków normalnie zamkniętych (NC).

17.10 Konfiguracja modelu drzwi 07

Poniżej pokazano okablowanie windy z modelem drzwi 07a



Legenda:

A = Przyciski pięter w windzie

B = (linia ciągła) sygnały wejściowe AMC

C = (linia przerywana) połączenie do sterowania windy

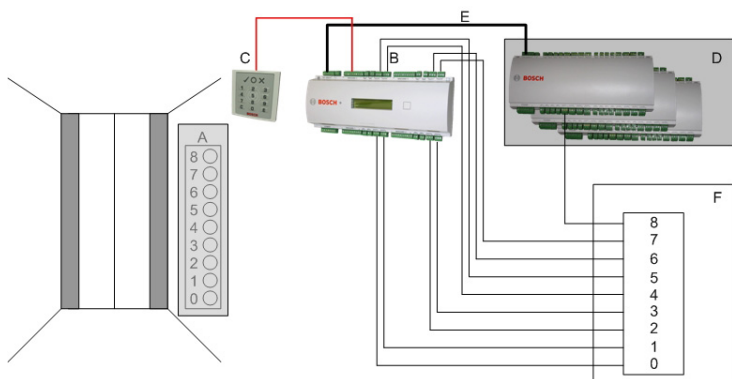
D = Można przyłączyć moduł rozszerzeń WE/WY (AMC2 8I-8O-EXT, AMC2 16I-EXT lub AMC2 16I-16O-EXT)

E = Przesyłanie danych i zasilania z AMC do modułów WE/WY

F = Sterowanie windy

G = Czytnik (model drzwi 07a)

Poniżej pokazano okablowanie windy z modelem drzwi 07b

**Legenda:**

A = Przyciski pięter w windzie

B = (linia ciągła) sygnały wejściowe AMC

C = (linia przerywana) sygnały wyjściowe AMC

D = Można przyłączyć moduł rozszerzeń WE/WY (AMC2 8I-8O-EXT, AMC2 16I-EXT lub AMC2 16I-16O-EXT)

E = Przesyłanie danych i zasilania z AMC do modułów WE/WY

F = Sterowanie windy

G = Czytnik (model drzwi 07b)

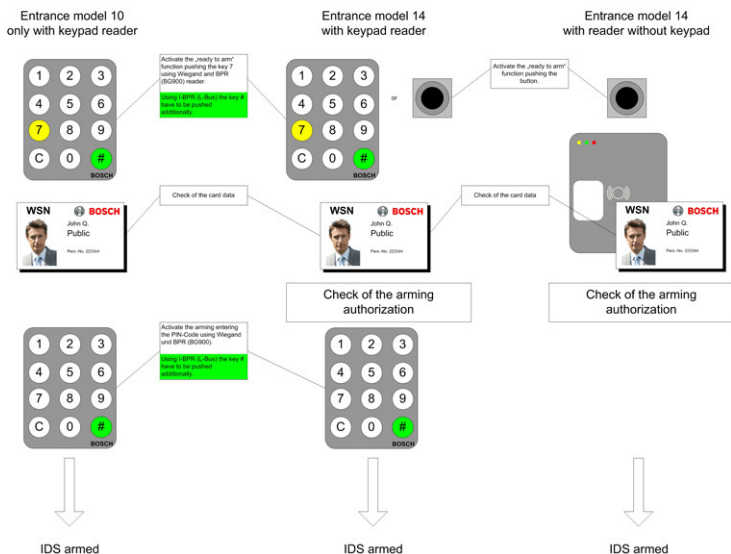
Uwaga!

Podczas prowadzenia okablowania poszczególnych pięter (do 16) do wyjść kontrolera AMC należy podłączyć najpierw sygnały samego kontrolera, a następnie pierwszych osiem wyjść (jeśli występują) dowolnych modułów rozszerzeń we/wy w kolejności rosnącej. [W przypadku, gdy stosowane są moduły rozszerzeń Wiegand (AMC2 4W-EXT), należy podłączyć ich wyjścia w kolejności rosnącej po podłączeniu wyjść kontrolera AMC2 i przed podłączeniem wyjścia któregośkolwiek z modułów rozszerzeń we/wy.] Z tego względu nie jest możliwe skonfigurowanie innych rodzajów drzwi lub kolejnych wind do obsługi przez kontroler AMC stosowany do sterowania windami.

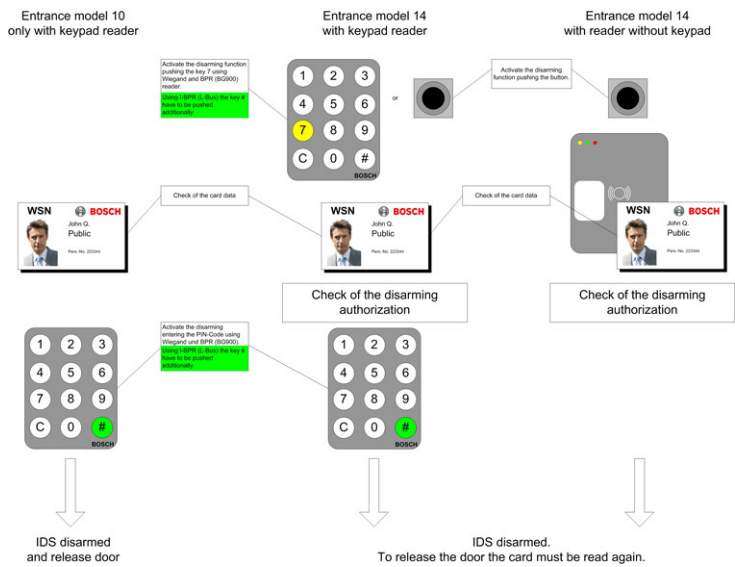


17.11 Instrukcje dotyczące uzbrajania/ rozbrajania

Porównanie **uzbrajania** systemu alarmowego na wejściu
(drzwiach) w modelach 10 i 14.



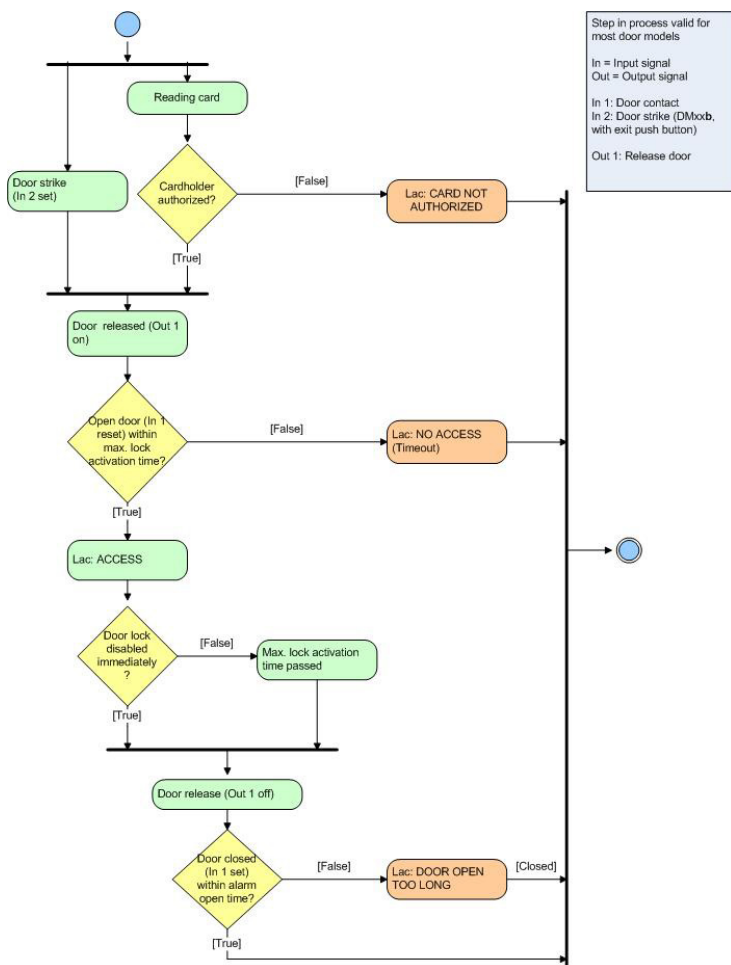
Porównanie **rozbrajania** systemu alarmowego na wejściu
(drzwiach) w modelach 10 i 14.



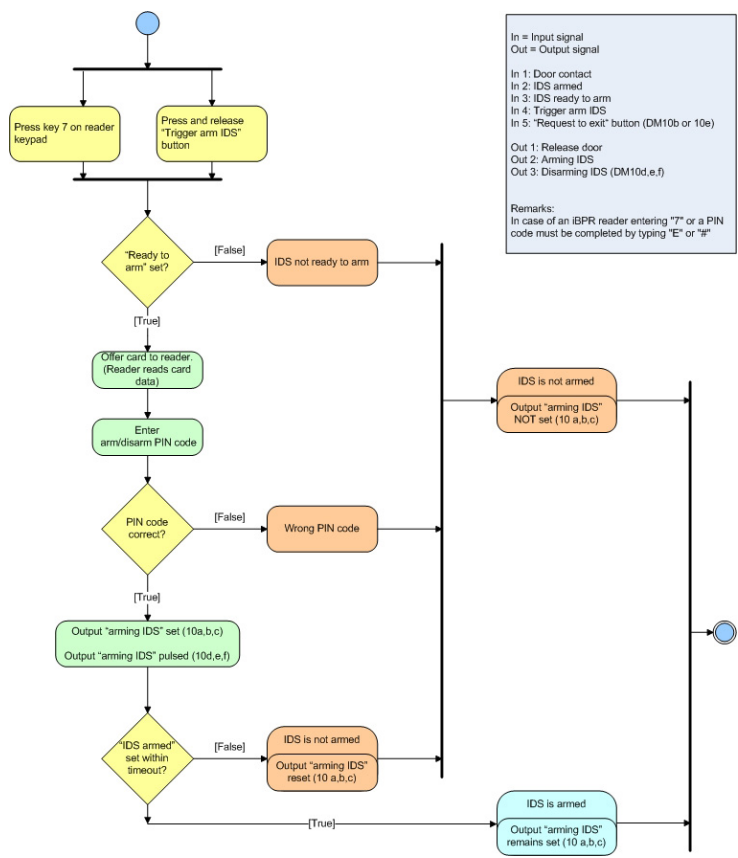
17.12 Procedury kontroli dostępu

Schematy procedur kontroli dostępu

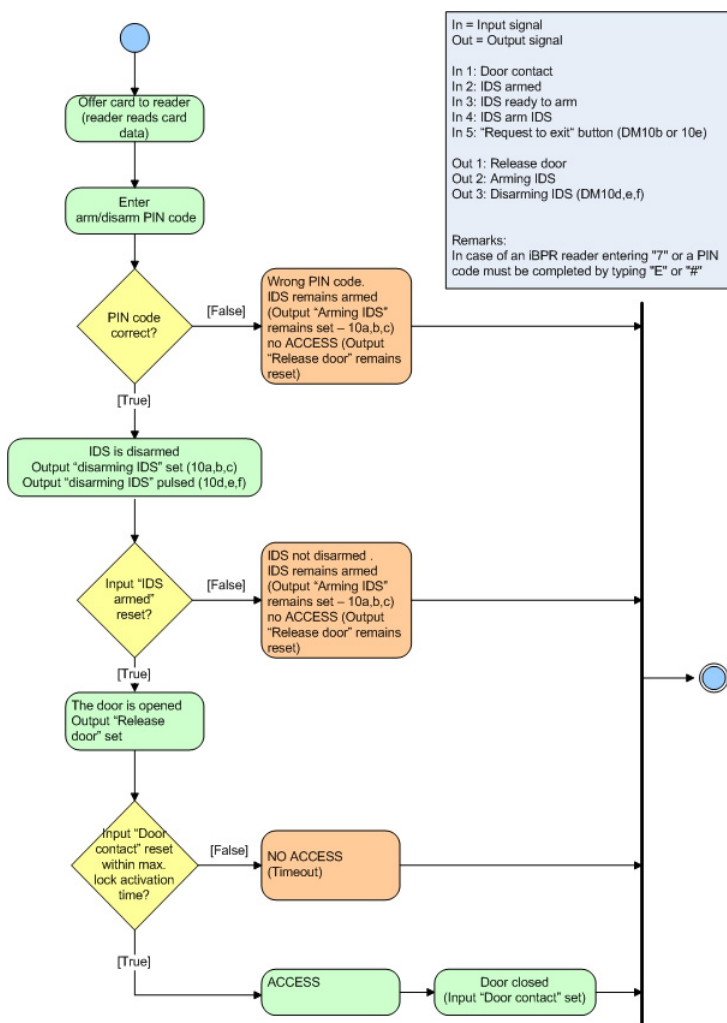
Model drzwi DM01



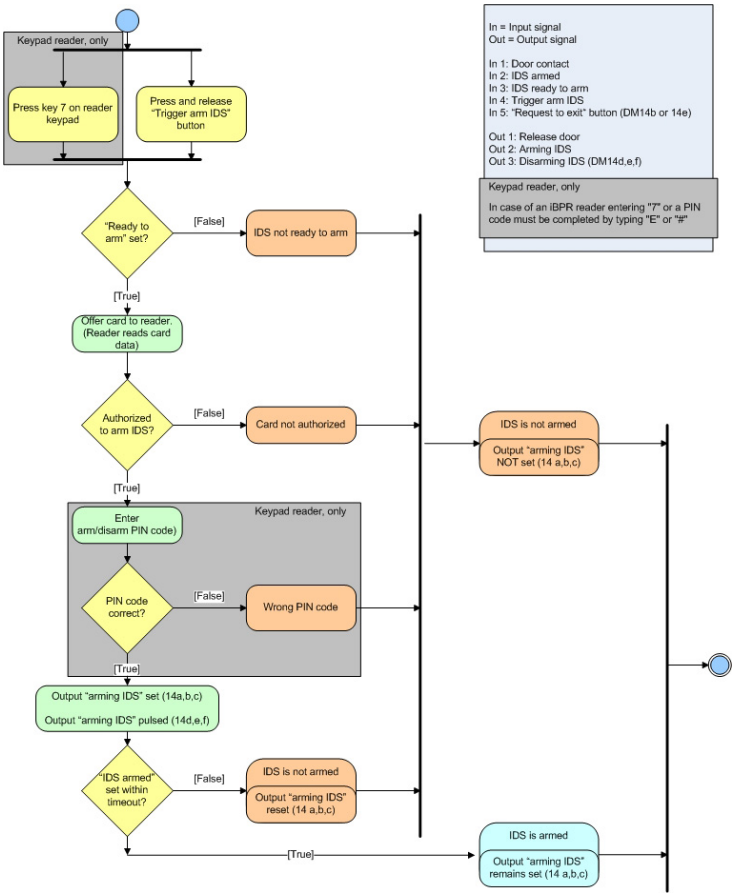
Model drzwi DM10 - uzbrajanie



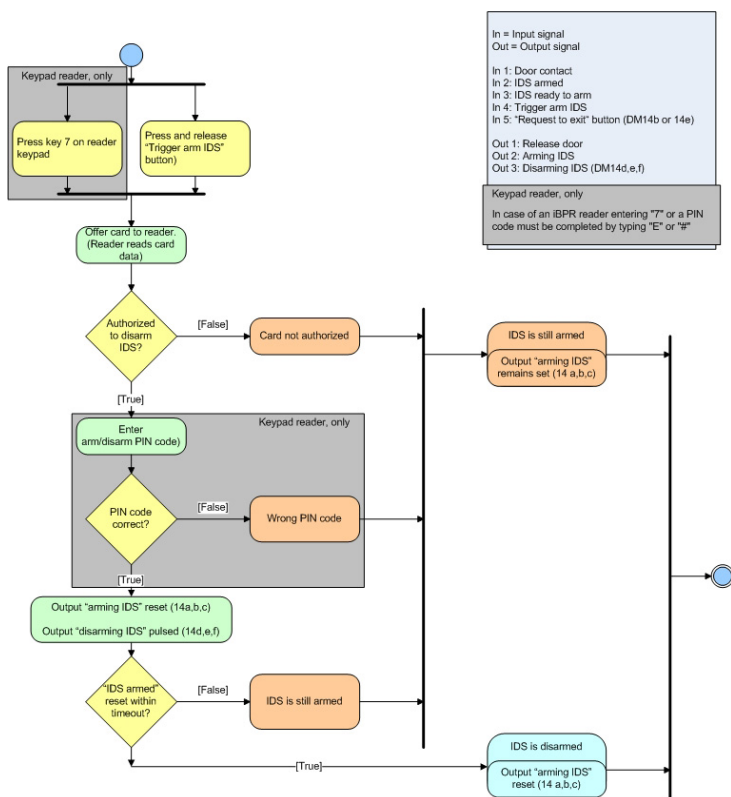
Model drzwi DM10 - rozbrajanie



Model drzwi DM14 - uzbrajanie



Model drzwi DM14 - rozbrajanie



17.13 Porty Access PE

Poszczególne procesy i aplikacje w programie Access PE wykorzystują opisane poniżej porty.

Połączenie między...	Klient/AMC	Serwer
Klient – LacSp	Niezdefiniowany	43434/tcp
AcPers – CP	Niezdefiniowany	20005/tcp
LacSp – AMC	10001/udp	54545/udp i wyżej

17.14 Wymagania normy UL 294

Funkcje, które nie zostały ocenione przez firmę UL:

- System weryfikacji wideo
- Przeglądanie map i zarządzanie alarmami z weryfikacją map i wideo
- Odtwarzacz wideo
- Projektant identyfikatorów
- Modele Delta 1200 Series
- Modele Rosslare ARD-1200EM Series
- Kontrolery LAC
- Kontrolery LACi
- Kontrolery APC-AMC2-4R4CF
 - Protokół interfejsu czytnika BG 900
 - Protokół interfejsu czytnika L-BUS
- System sygnalizacji włamania – uzbrajanie/rozbrajanie
- Używanie windy
- SMS-y
- Używanie alarmu włamaniowego

Funkcje ocenione przez firmę UL:

- Czytniki w 26-bitowym formacie Wiegand
- Kontrolery AMC2:
 - APC-AMC2-4WCF
 - API-AMC2-4WE
 - API-AMC2-8IOE
 - API-AMC2-16IOE
- APE-SW jako dodatkowy sprzęt monitorujący

Następujące modele czytników kart firmy Bosch zostały ocenione przez firmę UL pod kątem zgodności z systemem oprogramowania APE-SW firmy Bosch:

- LECTUS secure 1000 WI
- LECTUS secure 4000 WI
- LECTUS secure 5000 WI

18 Rodzaje kodów PIN

Access Professional Edition zapewnia każdemu posiadaczowi karty identyfikacyjnej maksymalnie trzy osobiste numery identyfikacyjne (**PIN**), które można wykorzystać do różnych celów:

- **Verification-PIN (Kod weryfikacyjny PIN)**

Ten kod PIN może być wymagany jako dodatkowe zabezpieczenie na specjalnie chronionych wejściach. Kod weryfikacyjny PIN jest porównywany z zapisanymi danymi posiadacza karty w celu zyskania pewności, że jest on/ona prawdziwym właścicielem przedstawionej karty. Każdy osó**b** może wybrać własny kod PIN o długości 4-8 cyfr, zgodnie z pewnymi ogólnymi zasadami (np. kod nie może być ciągiem kolejnych cyfr ani palindromem). [Parametr dotyczący długości kodu PIN ma takie samo zastosowanie zarówno w przypadku kodów PIN weryfikacyjnych, uzbrojenia, jak i do drzwi]. Kod weryfikacyjny PIN nie musi być niepowtarzalny w systemie. Jeśli nie zdefiniowano oddzielnego kodu PIN uzbrojenia [tj. nie zaznaczono pola wyboru **use separate IDS-PIN** (zastosuj oddzielny kod PIN systemu sygnalizacji włamania) w oknie dialogowym Configurator > Settings (Konfigurator > Ustawienia)], wówczas do uzbrajania/rozbrajania systemu sygnalizacji włamania można używać kodu weryfikacyjnego PIN.

- **Arming-PIN / IDS-PIN (Kod uzbrojenia PIN / PIN systemu sygnalizacji włamania)**

Ten specjalny kod PIN służy wyłącznie do uzbrajania i rozbrajania systemu alarmowego. W przypadku modeli drzwi 10 i 14 należy najpierw nacisnąć przycisk 7 lub przycisk otwierania drzwi. Każdy osó**b** może wybrać własny kod PIN o długości 4-8 cyfr, zgodnie z pewnymi ogólnymi zasadami (np. kod nie może być ciągiem kolejnych cyfr ani palindromem).

[Parametr dotyczący długości kodu PIN ma takie samo zastosowanie zarówno w przypadku kodów PIN weryfikacyjnych, uzbrojenia, jak i do drzwi]. Kod PIN uzbrajania nie musi być niepowtarzalny w systemie. Jeśli posiadacz karty chce przejść przez drzwi, w przypadku których wymagane jest podanie kodu PIN, wówczas należy wprowadzić kod weryfikacyjny PIN. Jeśli pole wyboru **use separate IDS-PIN** (zastosuj oddzielny kod PIN systemu sygnalizacji włamania) zostało zaznaczone (Configurator > General settings (Konfigurator > Ustawienia ogólne)), wówczas do uzbrajania/rozbrajania systemu sygnalizacji włamania nie można już używać kodu weryfikacyjnego PIN. Dopiero wtedy w oknie dialogowym danych osobowych stają się widoczne odpowiednie pola do wprowadzania danych.



Uwaga!

W celu zapewnienia kompatybilności z wcześniejszymi wersjami Access PE zaznaczenie pola wyboru oddzielnego kodu PIN systemu sygnalizacji włamania jest domyślnie usuwane.

– Identification-PIN/ ID-PIN (Kod identyfikacyjny PIN / PIN ID)

Ten kod PIN identyfikuje kartę danej osoby i dlatego musi być niepowtarzalny w całym systemie. Dzięki wprowadzeniu tego kodu PIN udzielony zostaje dostęp, zgodnie ze wszystkimi zdefiniowanymi dla danej osoby uprawnieniami. Aby zapewnić niepowtarzalność kodu PIN, jest on generowany przez system i przypisywany danej osobie, przy czym w przypadku tego kodu również obowiązują ogólne zasady (żadnych kolejnych cyfr ani palindromów). Podobnie jak w przypadku uwierzytelniania fizycznego dostępu, kod identyfikacyjny PIN egzekwuje przypisane ograniczenia (blokada, modele czasowe, uprawnienia itd.).

W zależności od protokołu czytnika, należy wprowadzić kod identyfikacyjny PIN wraz z wymaganymi dodatkowo znakami. W przypadku czytników kod PIN należy wprowadzić w następujący sposób: **4 # (Enter) PIN # (Enter)**. W przypadku wszystkich innych protokołów kod PIN jest wprowadzany bezpośrednio, a po nim następuje **# (Enter)**.

Długość kodu PIN można skonfigurować w zakresie od 4 do 8 cyfr.

[Uwaga: Długość kodów PIN ID powinna mieć związek z wielkością instalacji, aby utrudnić odgadnięcie aktywnych kodów PIN. Przykładowo, jeśli instalacja obejmuje 1000 posiadaczy kart, kody PIN powinny mieć długość co najmniej 6 cyfr, aby odgadnięcie ważnego kodu było wystarczająco mało prawdopodobne, a losowe wybieranie cyfr powodowało generowanie alarmów.]

Opisane wyżej rodzaje kodów PIN odnoszą się do osób i dlatego są definiowane i zachowywane wraz z innymi danymi osobowymi. Czwartym rodzajem kodu jest tak zwany PIN do drzwi.

– **Door-PIN (Kod PIN do drzwi)**

Ten kod PIN jest przypisany do danego wejścia (Configurator > Entrances (Konfigurator > Wejścia)). Musi być znany wszystkim osobom upoważnionym do korzystania z danego wejścia. W przypadku takich wejść zamiast kodu PIN można używać karty (patrz = Funkcja **PIN lub karta**). Długość tego kodu PIN również może wynosić od 4 do 8 cyfr. Jeśli opcja używania kodu PIN do drzwi jest wyłączona (np. przez model czasowy), dostęp można uzyskać na podstawie karty. W tym przypadku kod identyfikacyjny PIN też nie zadziała.



Uwaga!

Nie można używać kodu PIN identyfikacyjnego i do drzwi w przypadku drzwi z funkcją uzbrajania systemu sygnalizacji włamania, modeli 10 i 14.

Bosch Access Systems GmbH

Charlottenburger Allee 50

52068 Aachen

Germany

www.boschsecurity.com

© Bosch Access Systems GmbH, 2016