



BOSCH

Access Professional Edition

pl

Instrukcja konfiguracji

Spis treści

1	Przegląd	5
1.1	Konstrukcja modułowa	5
1.2	Moduły serwera i klienta	5
2	Informacje ogólne	6
2.1	Wstęp	6
2.2	Logowanie użytkownika	7
2.3	Pasek narzędzi aplikacji Configurator (Konfigurator)	10
2.4	Ogólne ustawienia systemu	14
3	Konfiguracje	17
3.1	Tworzenie nowych konfiguracji	17
3.2	Otwieranie konfiguracji	19
3.3	Aktywacja nowej konfiguracji	20
3.4	Przesyłanie konfiguracji do kontrolerów	20
4	Kontrolery	24
4.1	Definiowanie i modyfikowanie nowych kontrolerów	24
4.2	Ustawienia kontrolera	27
5	Sygnały	30
5.1	Sygnały wejściowe	30
5.2	Sygnały wyjściowe	32
5.3	Definiowanie warunków sygnałów wyjściowych	37
5.3.1	Aktywuj funkcję kontroli za pomocą karty	41
5.4	Tworzenie modułów rozszerzeń	43
6	Entrances (Wejścia)	45
6.1	Tworzenie i modyfikacja modeli drzwi	45
6.2	Wskazania i ustawianie parametrów	49
6.3	Office mode (Tryb biuro)	55
6.4	Modele drzwi z ustawieniami specjalnymi	55
6.5	Przypisywanie urządzeń wizyjnych do wejścia	56
7	Strefy	58
8	Personnel Groups (Grupy personelu)	63
8.1	Dostęp grupy w przypadku czytników z klawiaturą	65
8.2	Ograniczenia dotyczące dostępu grupy	66
9	Uprawnienia dostępu	67
9.1	Tworzenie i przypisywanie	67
9.2	Uprawnienia specjalne	70
10	Dni specjalne	73
10.1	Tworzenie i edytowanie	73
11	Modele dzienne	75
11.1	Tworzenie i edytowanie	75
12	Modele czasowe	77
12.1	Tworzenie i edytowanie	79
13	Teksty	81
13.1	Displaytexts (Wyświetlany tekst)	81
13.2	Event Log messages (Komunikaty dziennika zdarzeń)	81
14	Additional Personnel data (Dodatkowe pola danych osobowych)	85
15	Zarządzanie urządzeniami wizyjnymi	88
15.1	Otwieranie aplikacji Configurator	88
15.2	Znajdowanie urządzeń wizyjnych	88

15.3	Dodawanie urządzenia wizyjnego do systemu kontroli dostępu	88
15.4	Zmianie danych połączenia	89
15.5	Zmiana danych urządzenia wizyjnego	90
15.6	Wyświetlanie obrazu na żywo	91
15.7	Wyświetlanie zapisów archiwalnych	91
15.8	Wyświetlacze i procesy	92
16	Konfigurowanie mapy	95
17	Dodawanie urządzenia do mapy	97
18	Definicja karty	99
19	Konfigurowanie alertów zagrożenia	102
19.1	Konfigurowanie sprzętu do obsługi alarmów zagrożenia	102
20	Dodatek	104
20.1	Sygnaly	104
20.2	Domyślne modele drzwi	105
20.3	Model drzwi 01	107
20.4	Model drzwi 03	109
20.5	Model drzwi 06c	109
20.6	Model drzwi 07	110
20.7	Model drzwi 10	112
20.8	Model drzwi 14	114
20.9	Przykłady konfiguracji śluz osobowych	116
20.10	Konfiguracja modelu drzwi 07	118
20.11	Instrukcje dotyczące uzbrajania/rozbrajania	119
20.12	Procedury kontroli dostępu	120
20.13	Porty Access PE	124
21	Rodzaje kodów PIN	125
22	Wymagania normy UL 294	127

1 Przegląd

1.1 Konstrukcja modułowa

System Access Professional Edition (w dalszej części dokumentu nazywany w skrócie **Access PE**) to kompleksowe, autonomiczne rozwiązanie do kontroli dostępu dla firm małej i średniej wielkości. Składa się ono z kilku modułów:

- Usługa LAC: proces, który polega na ciągłej komunikacji z lokalnymi kontrolerami dostępu LAC (ang. Local Access Controllers, w dalszej części dokumentu nazywanych kontrolerami). AMC: modułowe kontrolery dostępu (ang. Access Modular Controllers), które są stosowane jako kontrolery.
- Konfigurator (Konfigurator)
- Personnel Management (Zarządzanie personelem)
- Log Viewer (Analiza dziennika)
- Alarm Management (Zarządzanie alarmami)
- Video Verification (Weryfikacja wideo)

1.2 Moduły serwera i klienta

Składniki te można podzielić na moduły instalowane i pracujące na serwerze i na klientach. 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).

Aplikacja Konfigurator (Konfigurator) również powinna pracować na serwerze, jednak można ją też zainstalować na klienckich stacjach roboczych i obsługiwać z ich poziomu.

Moduły Personnel Management (Zarządzanie personelem) i Log Viewer (Analiza dziennika) należą do składników 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) – można rozszerzyć za pomocą modułu AMC2 4W-EXT
- AMC2 4R4 (z czterema interfejsami RS485 do czytników)

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, np. 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 działa w trybie offline, kontroler LAC jest zdolny do niezależnego podejmowania decyzji w zakresie kontroli dostępu. Kontrolery LAC są odpowiedzialne za prawidłowy przebieg procedur na przejściach, nadzorując np. czas otwarcia drzwi lub pytając o kod PIN przy wejściach o znaczeniu krytycznym.

Trzecia platforma składa się z czytników kart.

Komunikacja między klientem, serwerem a posiadaczami kart jest zaszyfrowana za pomocą mechanizmu AES.

Wersja wielostanowiskowa oprogramowania Access PE umożliwia kontrolowanie systemu z różnych stanowisk. Zróżnicowane 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 jego 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 wyposażyć w kamery do identyfikacji i śledzenia ruchów osób, które z tych wejść korzystają.

2.2

Logowanie użytkownika

Dostępne są poniższe aplikacje. Szczegółowe informacje na ich temat można znaleźć w poszczególnych instrukcjach obsługi:



Zarządzanie personelem



Konfigurator



Analiza dziennika



Zarządzanie mapami i alarmami



Weryfikacja wideo



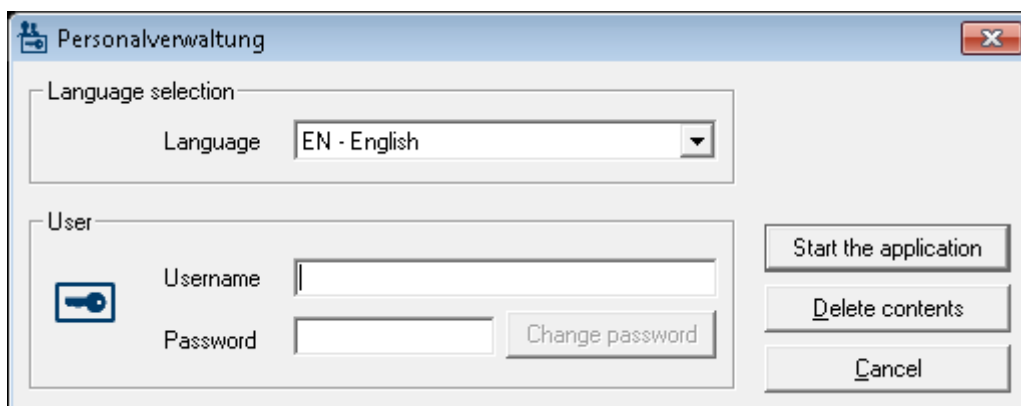
Uwaga!

Logowanie przez klienta możliwe jest tylko, gdy na serwerze aktywna jest licencja LAC.

Logowanie klienta

Aplikacje systemu są chronione przed nieuprawnionym użyciem. **Domyślne dane uwierzytelniające**, które służą do pierwszego uruchomienia:

- Nazwa użytkownika: **bosch**
- Hasło: **bosch**



Po wpisaniu prawidłowych danych w polach Nazwa użytkownika/Hasło, uaktywniony zostanie przycisk **Zmień hasło**.

Po 3 nieudanych próbach, dostęp do systemu zostanie na pewien czas ograniczony. Dotyczy to przycisków „Uruchom aplikację” oraz „Zmień hasło”.

Na górnej liście rozwijanej można wybrać odpowiedni **język**. Domyślnie stosowany jest język wybrany podczas instalowania aplikacji. W przypadku zmiany użytkownika bez restartowania aplikacji zachowany zostanie ostatnio używany język. Z tego powodu okno logowania może się wyświetlić się w nieprawidłowym języku. Aby tego uniknąć, należy ponownie zalogować się w systemie Access PE.

Aplikacje systemu Access PE można uruchamiać w następujących językach:

- angielski,
- niemiecki,
- francuski,
- japoński,
- rosyjski,

- polski,
- chiński (ChRL),
- niderlandzki,
- hiszpański,
- portugalski (Brazylia).

**Uwaga!**

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

Po kliknięciu przycisku **Zmień hasło** wpisz nową nazwę użytkownika i hasło w oknie dialogowym:

Change password

New password

Confirmation

Ok Cancel






**Uwaga!**








Należy pamiętać, aby zmienić domyślne hasło!








Z kolei użycie przycisku **Uruchom aplikację** powoduje skontrolowanie uprawnień użytkownika i ewentualne uruchomienie aplikacji. Jeśli kontrola uprawnień wypadnie negatywnie, pojawi się komunikat o błędzie **Wrong username or password!** (Nieprawidłowa nazwa użytkownika lub hasło!).



2.3 Pasek narzędzi aplikacji Configurator (Konfigurator)

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

Funkcja	Ikona/ skrót	Opis
Menu File (Plik)		
New (Nowy)	 Ctrl + N	Powoduje usunięcie wszystkich danych z okien dialogowych konfiguracji (oprócz ustawień standardowych) w celu przygotowania ich do nowej konfiguracji.
Open... (Otwórz...)	 Ctrl + O	Powoduje otwarcie okna dialogowego wyboru w celu pobrania innej konfiguracji.
Save (Zapisz)	 Ctrl + S	Służy do zapisywania zmian w bieżącym pliku konfiguracji.
Save as... (Zapisz jako...)		Umożliwia zapisanie bieżącej konfiguracji w nowym pliku.
Aktywuj konfigurację		Umożliwia uaktywnienie pobranej konfiguracji i zapisanie tej, która była dotąd prawidłowa.
Wyślij konfigurację do LAC		Powoduje przestanie do usługi LAC zapisanych zmian konfiguracji.
Pokaż ostatnie prawidłowe konfiguracje		Powoduje bezpośrednie otwarcie konfiguracji bez konieczności korzystania z okna dialogowego funkcji Otwórz .
Zakończ		Powoduje zakończenie działania aplikacji Access PE Configurator.
Menu Widok		
Pasek narzędzi		Umożliwia wyświetlanie i ukrywanie paska narzędzi (ustawienie domyślne = wyświetlanie).

Funkcja	Ikona/ skrót	Opis
Status bar (Pasek stanu)		Umożliwia wyświetlanie i ukrywanie paska stanu przy dolnej krawędzi okna dialogowego (ustawienie domyślne = wyświetlanie).
Menu Configuration (Konfiguracja)		
Informacje ogólne		Umożliwia otwieranie okna dialogowego General Settings (Ustawienia ogólne), które służy do konfigurowania kontrolerów i ogólnych parametrów systemu.
Input signals (Sygnały wejściowe)		Umożliwia otwieranie okna dialogowego, które służy do ustawiania parametrów sygnałów wejściowych .
Output signals (Sygnały wyjściowe)		Umożliwia otwieranie okna dialogowego, które służy do ustawiania parametrów sygnałów wyjściowych .
Entrances (Wejścia)		Umożliwia otwieranie okna dialogowego Entrances (Wejścia), które służy do ustawiania parametrów drzwi i czytników kart.
Areas (Obszary)		Umożliwia otwieranie okna dialogowego Area Configuration (Konfiguracja obszaru), które służy do dzielenia zabezpieczonej instalacji na strefy wirtualne.
Holidays (Wakacje)		Umożliwia otwieranie okna dialogowego Holidays (Wakacje), które służy do definiowania dni wolnych od pracy i dni specjalnych.
Day Models (Modele dienne)		Umożliwia otwieranie okna dialogowego Day Models (Modele dzienne), które służy do tworzenia okresów w obrębie danego dnia w celu uaktywniania określonych funkcji dostępu.

Time Models (Modele czasowe)		Umożliwia otwieranie okna dialogowego Time Models (Modele czasowe), które służy do definiowania stref czasowych zależnych od dnia tygodnia lub kalendarza.
Personnel Groups (Grupy personelu)		Umożliwia otwieranie okna dialogowego Personnel Groups (Grupy personelu), które służy do dzielenia personelu na grupy logiczne.
Access Authorization Groups (Grupy uprawnień dostępu)		Umożliwia otwieranie okna dialogowego Access Authorization Groups (Grupy uprawnień dostępu), które służy do tworzenia grup z uprawnieniami do wejść.
Offline locking system (System blokowania offline)		Umożliwia otwieranie okna dialogowego Offline locking system (System blokowania offline), które służy do konfigurowania specjalnych elementów instalacji (wejść, modeli czasowych i grup uprawnień dostępu).
Display Texts (Wyświetlane teksty)		Umożliwia otwieranie okna dialogowego Display Texts (Wyświetlane teksty), które służy do edytowania tekstów wyświetlanych na czytnikach kart.
Log Messages (Komunikaty dziennika)		Umożliwia otwieranie okna dialogowego Log Messages (Komunikaty dziennika), które służy do edytowania komunikatów dziennika i podziału ich na kategorie.
Additional personnel fields (Dodatkowe pola danych osobowych)		Umożliwia otwieranie okna dialogowego Additional personnel fields (Dodatkowe pola danych osobowych), które służy do definiowania pól danych dla personelu.

Wiegand - cards (Karty Wiegand)		Umożliwia otwieranie okna dialogowego Wiegand - cards (Karty Wiegand), które służy do definiowania struktury danych na karcie identyfikacyjnej.
Administering video devices (Zarządzanie urządzeniami wizyjnymi)		Umożliwia otwieranie okna dialogowego Video devices (Urządzenia wizyjne) pozwalającego na konfigurowanie kamer w taki sposób, aby mogły służyć do weryfikacji wideo.
Map Viewer and Alarm management (Przeglądanie map i zarządzanie alarmami)		Umożliwia otwieranie okna Przeglądarka map z widokiem obszarów map i urządzeń sterujących, a także listą alarmów do obsługi.
Menu Ustawienia		
Aktywacja licencji		Otwiera menu umożliwiające zaznaczenie bądź odznaczenie licencji
Resetuj teksty komunikatów i czytnika		Otwiera żądanie w przypadku konieczności aktualizacji tekstów dziennika i czytnika.
Menu ? (Pomoc)		
Tematy pomocy		Umożliwia wyświetlanie tego pliku pomocy.
Informacje o aplikacji Konfigurator Access Professional Edition		Umożliwia wyświetlanie ogólnych wiadomości o aplikacji Konfigurator 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 <input type="text" value="00"/> Customer code <input type="text" value="056720"/>	PIN code Number of digits <input type="text" value="4"/> Number of retries before blocking <input type="text" value="3"/> <input type="checkbox"/> use separate IDS pin
LAC subsystem process Poll interval on serial connected LAC in ms <input type="text" value="200"/> Read-timeout on serial connected LAC in ms <input type="text" value="500"/> Create TA-data at <input type="text" value="00:01"/> <input type="checkbox"/> Export personnel and TA data	Logbook parameter Number of files <input type="text" value="366"/> (one logfile per day, 0 = unlimited)
<input type="checkbox"/> Show welcome/leaving message <input type="checkbox"/> Show cardholder name in display	Directories Database <input type="text" value="C:\BOSCH\Access Professional Edition\PE\Data\D"/> Event log <input type="text" value="C:\BOSCH\Access Professional Edition\PE\Data\lv"/> Import files <input type="text" value="C:\BOSCH\Access Professional Edition\PE\Data\lr"/> ... Export files <input type="text" value="C:\BOSCH\Access Professional Edition\PE\Data\E"/> ... DLL-files <input type="text" value="C:\BOSCH\Access Professional Edition\PE\Data\D"/> Pictures <input type="text" value="C:\BOSCH\Access Professional Edition\PE\Data\P"/> ... Test logs <input type="text" value="C:\BOSCH\Access Professional Edition\PE\Data\L"/>

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.
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.
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		

Parametr	Domyślne	Opis
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.
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.
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

Parametr	Domyślne	Opis
		Możliwe wartości: od 180 do 9999. UWAGA: W przypadku wpisania wartości <180 zostanie ona automatycznie zmieniona na wartość minimalną 180.
Ścieżki katalogów do: Baza danych Plik rejestru Pliki importu Pliki eksportu Pliki DLL Dane obrazów Logowanie testowe	C:\Program Files\BOSCH \Access Professional 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**.

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 (*.cfg) – jednak tylko jeden o nazwie ***active.cfg** może aktywować aktualny system. Umożliwia to testowanie nowych scenariuszy, przeprowadzanie próbnych uruchomień i dokonywanie szybkich zmian w systemie.

3.1 Tworzenie nowych konfiguracji

Wszystkie konfiguracje oprogramowania Access PE zapisywane są w katalogu **C:\BOSCH\Access Professional Edition\PE\Data\Cfg** (pod warunkiem że podczas instalacji wybrano standardowe ścieżki dostępu i katalogi). Podczas instalacji tworzone są dwa pliki konfiguracji: **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:

- Obszar **--outside--** (--poza--).
- Przykładowe święta i dni specjalne.
- Grupy personelu **Employees** (Pracownicy) i **Visitors** (Goście).
- Teksty wyświetlane na czytnikach.
- Treść komunikatów dziennika.


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

Konfiguracja może mieć różne stany i dlatego ważna jest umiejętność rozróżniania między nimi:

- konfiguracja **Aktywna** – jej ustawienia, parametry itp. są obecnie wykorzystywane przez składniki systemu;
- konfiguracja **Otwarta** (albo inaczej: pobrana) – jej ustawienia są obecnie edytowane przez użytkowników systemu. Może ona zostać później zapisana w oddzielnym pliku .acf i/lub aktywowana w późniejszym czasie, ale **dopóki nie zostanie aktywowana, nie ma wpływu na działanie systemu**.

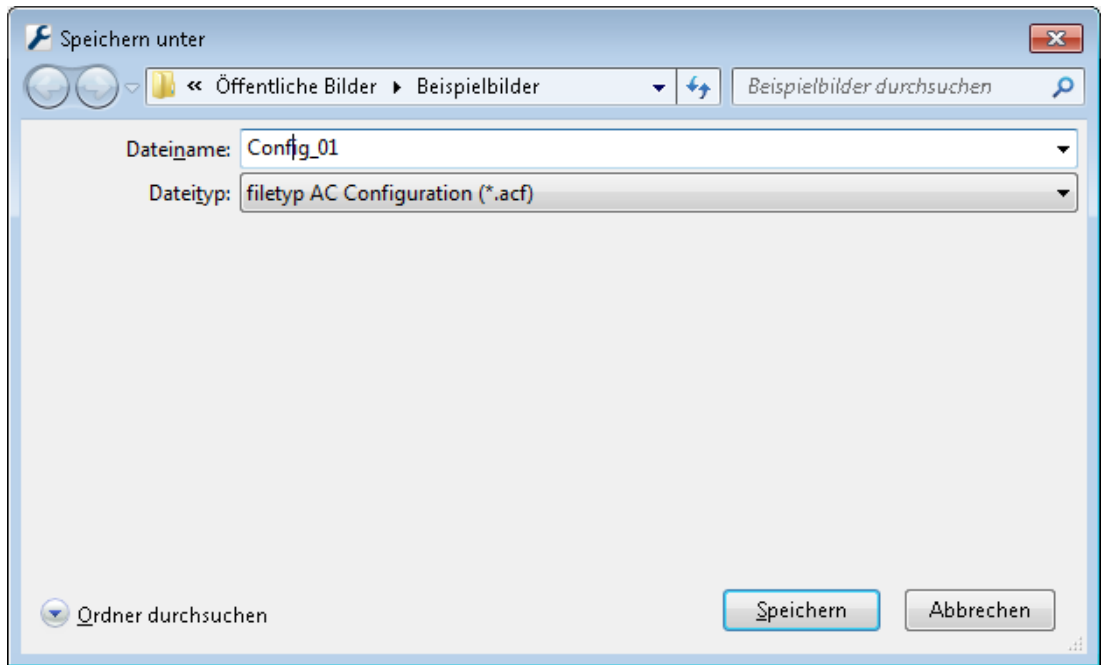
Można tworzyć i zapisywać dowolną liczbę konfiguracji systemu Access PE. Nowe konfiguracje są tworzone i edytowane niezależnie od bieżącego systemu, więc występuje np. możliwość definiowania nowych stref, które zostaną włączone do instalacji monitorowania w późniejszym czasie.




Korzystając z przycisku  na pasku narzędzi, można otwierać (wczytywać) konfigurację domyślną z podstawowymi ustawieniami, zapisaną w pliku **Untitled.acf**. W przypadku wprowadzenia zmian powodujących utworzenie nowej konfiguracji należy ją zapisać pod inną, właściwą dla niej nazwą.

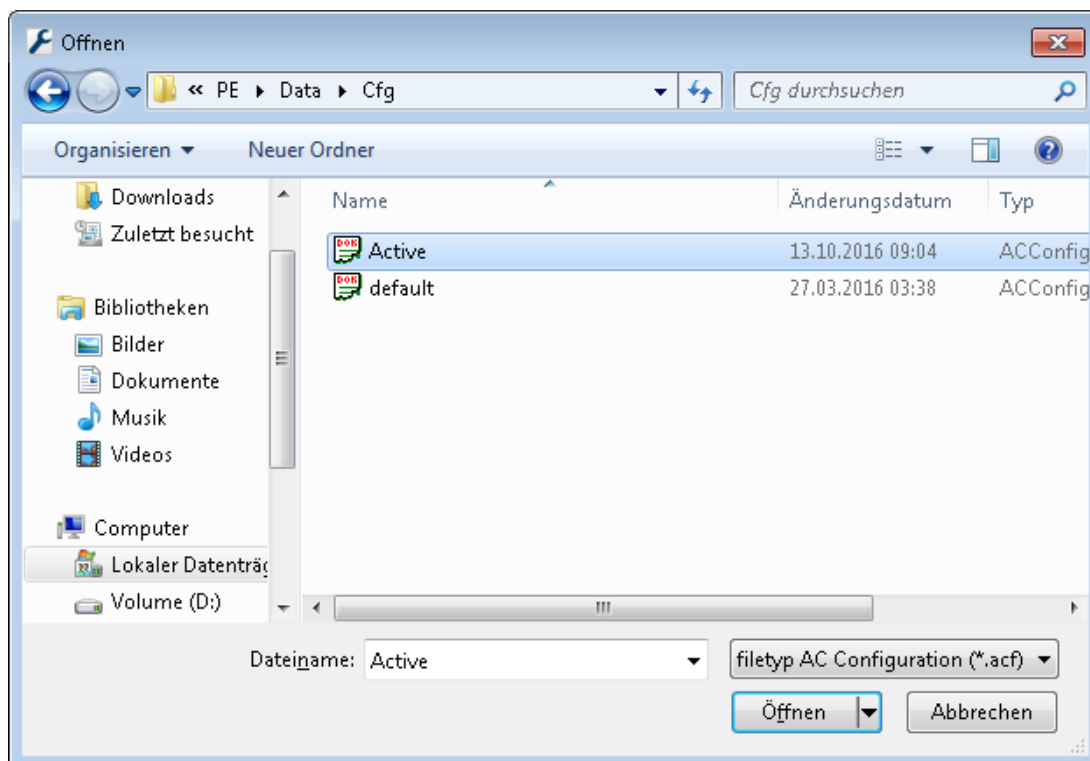


Przycisk  umożliwia otwieranie okna dialogowego, które służy do zapisywania plików w katalogu Cfg. Domyślna nazwa pliku **untitled.acf** powinna zostać zastąpiona nazwą objaśniającą jego przeznaczenie.



3.2 Otwieranie konfiguracji

Aplikacja Configurator (Konfigurator) jest zawsze uruchamiana z konfiguracją **Active.acf**. Jeśli ma zostać w nim użyta inna konfiguracja, należy za pomocą przycisku  otworzyć jedną z konfiguracji znajdujących się w katalogu **C:\BOSCH\Access Professional Edition\PE\Data\Cfg** (katalog domyślny).



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



Uwaga!

Aktywną konfigurację również można 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**.



Przeostroga!

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

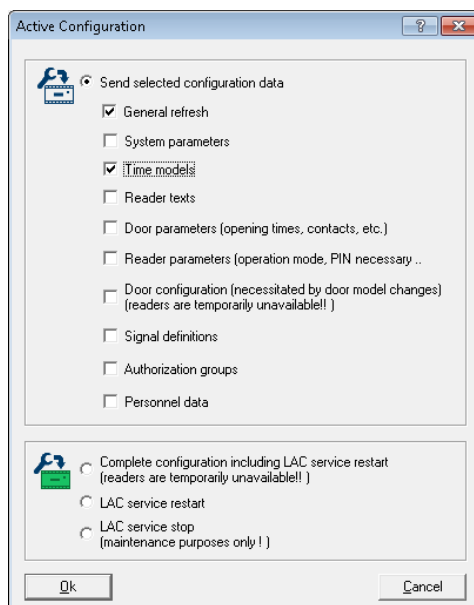
Po dokonaniu zmian w aktywnej konfiguracji **Active.acf** należy przesłać te zmiany do kontrolerów. Można to zrobić w dwojaki sposób:

- 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.



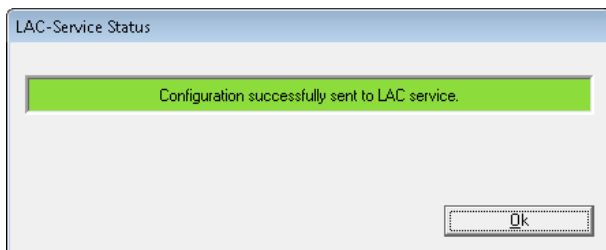
Zmienione i zachowane dane są tutaj wstępnie selekcjonowane. Można wybierać dodatkowe pozycje lub usuwać zaznaczenia pól wyboru.

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

Dane konfiguracji	Wysłanie do kontrolerów LAC jest konieczne w następujących sytuacjach:
	– przyciski otwarcia drzwi
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.
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 przesłania 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:

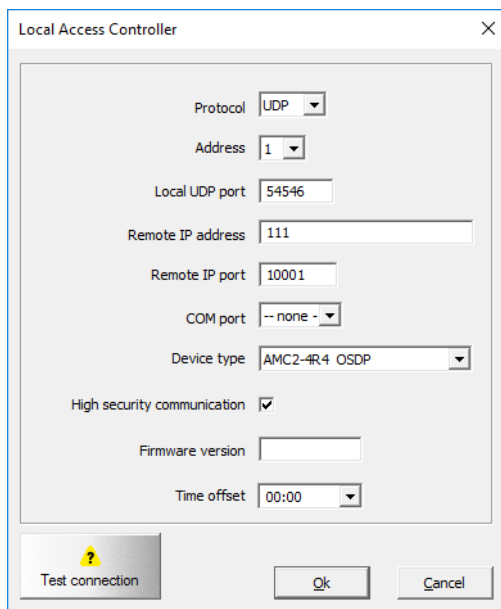


4 Kontrolery

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 używane są kontrolery AMC2 (Access Modular Controller).

4.1 Definiowanie i modyfikowanie nowych kontrolerów

Przyciski  (dodaj) i  (modyfikuj element wybrany z listy) powodują otwarcie okna dialogowego, które służy do konfigurowania interfejsów między serwerem Access PE a kontrolerami.



Uwaga!

Pole wyboru „High Security Communication is displayed under” (Komunikacja o wysokim poziomie bezpieczeństwa) znajduje się w obszarze „Device type” (Typ urządzenia). Przed przełączeniem na inny typ urządzenia należy najpierw usunąć zaznaczenie tego pola wyboru.

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:

Para- metr	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	ko- lejny	Port, za którego pomocą serwer Access PE ma otrzymywać informacje z kontrolera. Nowy kontroler otrzyma kolejny wolny port, zależnie od położenia, ale te dane można zmienić.
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 niezmienna a 10001	Port kontrolera umożliwiający odbiór danych z serwera.

Para- metr	COM	CIP	UDP	Uwaga
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-4W Wiegand			z interfejsem czytnika Wiegand
	AMC2-2W Wiegand			z interfejsem RS485 i czytnika Wiegand
	AMC-4R4-BG900			z interfejsem czytnika RS485
	AMC-4R4-L-BUS			z interfejsem czytnika RS485
	AMC-4R4-OSDP			z interfejsem czytnika RS485
Komunikacja o wysokim poziomie bezpieczeństwa	Pole wyboru do włączania zaleźnego od kontrolera, opartego na sesjach szyfrowania komunikacji między hostem a kontrolerem z użyciem mechanizmu AES 128.			
Wersja oprogramowania układowego (projekt)	brak	brak	brak	może służyć do określenia wersji oprogramowania
Przesunięcie czasu	Pole kombi służące do określenia przesunięcia czasu z serwera w przypadku, gdy kontroler AMC znajduje się w innej strefie czasowej. Możliwe wartości to: od -12:00 do +12:00 w 30-minutowych odstępach. Czas przesyłany z serwera do kontrolera AMC (lub odwrotnie) jest korygowany przez to przesunięcie. Lokalny czas kontrolera AMC jest stosowany w komunikatach o zdarzeniach i można go zobaczyć w dzienniku zdarzeń.			

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** umieszczonego 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 czterech wyników, za pomocą ikon pokazanych poniżej, które są również widoczne w pierwszej kolumnie listy.



Kontroler jeszcze nie został przetestowany lub nie jest włączony.



Test wypadł pozytywnie. Połączenie zostało utworzone.



Test nie powiódł się.



Nadal jest w stanie oczekiwania.



Uwaga!

Te ikony wskazują bieżący stan i zostaną automatycznie zaktualizowane. Próby ponownego połączenia mogą opóźnić aktualizację stanu.

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 **Ustawienia ogólne**, które otwiera się przyciskiem , można definiować i konfigurować moduły lokalnych kontrolerów dostępu (LAC).

Local access controller							
No. /	Address	Type	Project version	Connection	Version	enabled	
✓ 1	1	AMC2 Wiegand		UDP..54545>AMC-?????:10001>NONE		<input type="checkbox"/>	

Przyciski umieszczone nad polem listy mają następujące funkcje:



Add (Dodaj): dodawanie nowego kontrolera.



Modify (Modyfikuj): modyfikowanie zaznaczonego kontrolera.



Test (Testuj): testowanie zaznaczonego kontrolera.



Delete (Usuń): usuwanie zaznaczonego kontrolera.

W polu listy znajdują się: wykaz wszystkich zainstalowanych kontrolerów oraz następujące informacje:

Kolumna	Zawartość	Opis
	, , lub	Wynik testu kontrolera LAC: negatywny, jeszcze nie zakończony lub pozytywny
No. (Nr)	od 1 do 128	Numer kontrolera.
Adres	od 1 do 8	Adres kontrolera ustawiony za pomocą przełącznika DIL. W przypadku protokołu UDP zawsze 1.
Typ	AMC-Wiegand AMC-4R4 BG900 AMC-4R4 L-Bus AMC-4R4 OSDP AMC2-2W	Wybrany typ kontrolera.
Wersja projektu	Przykład: 37.50	Specjalna wersja oprogramowania do projektów wczytana do kontrolera.
Connection (Połączenie)	Przykład: UDP.: 54545>AMC- DEMO: 10001>NONE	Interface parameters (Parametry interfejsu): Protokół: lokalny port UDP>nazwa sieciowa lub adres IP: Zdalny port IP>port COM
Wersja	Przykład: 37.02	Numer wersji oprogramowania wczytanego do kontrolera.
Włączony	Aktywny albo nieaktywny	Jeśli to pole wyboru nie jest zaznaczone, usługi LAC nie będą

Kolumna	Zawartość	Opis
		się łączyć z AMC2. AMC2 będzie działać niezależnie.

W dolnej części okna dialogowego znajdują się ustawienia ogólne (General settings) dotyczące wszystkich urządzeń i aplikacji objętych działaniem systemu Access PE.

**Uwaga!**

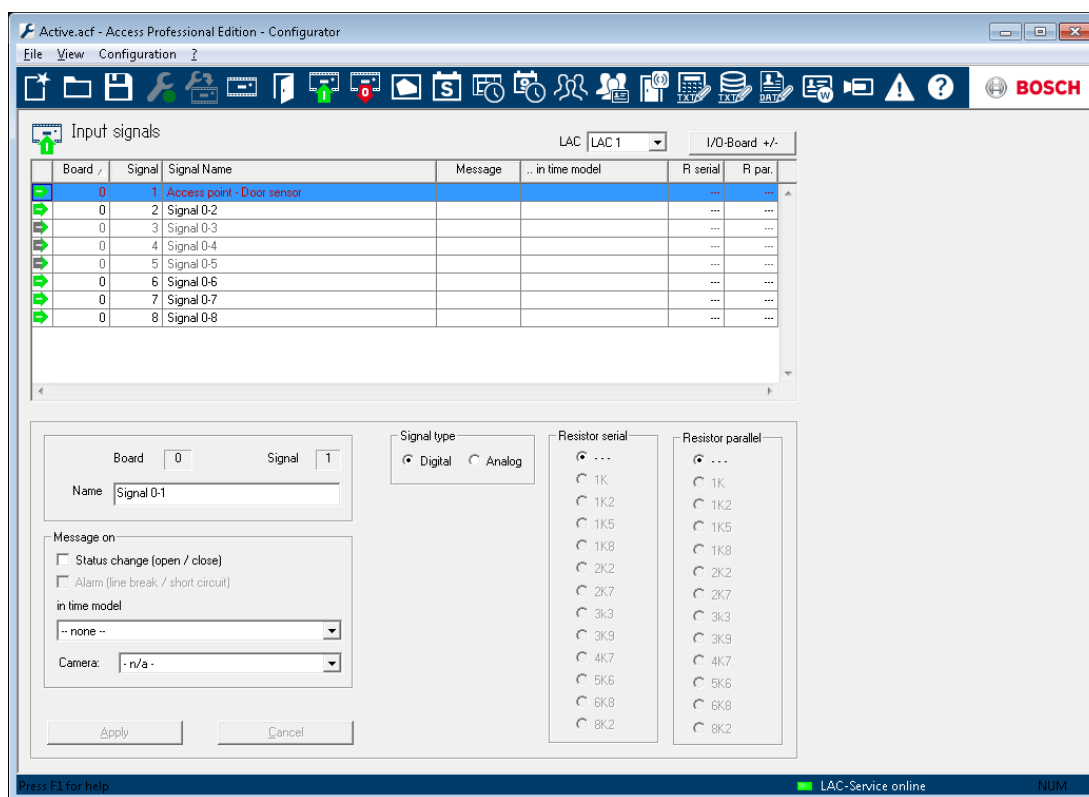
Po instalacji lub aktualizacji należy kliknąć pole wyboru **Enabled** (Włączone), aby uaktywnić wybrany kontroler AMC2.

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.
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.

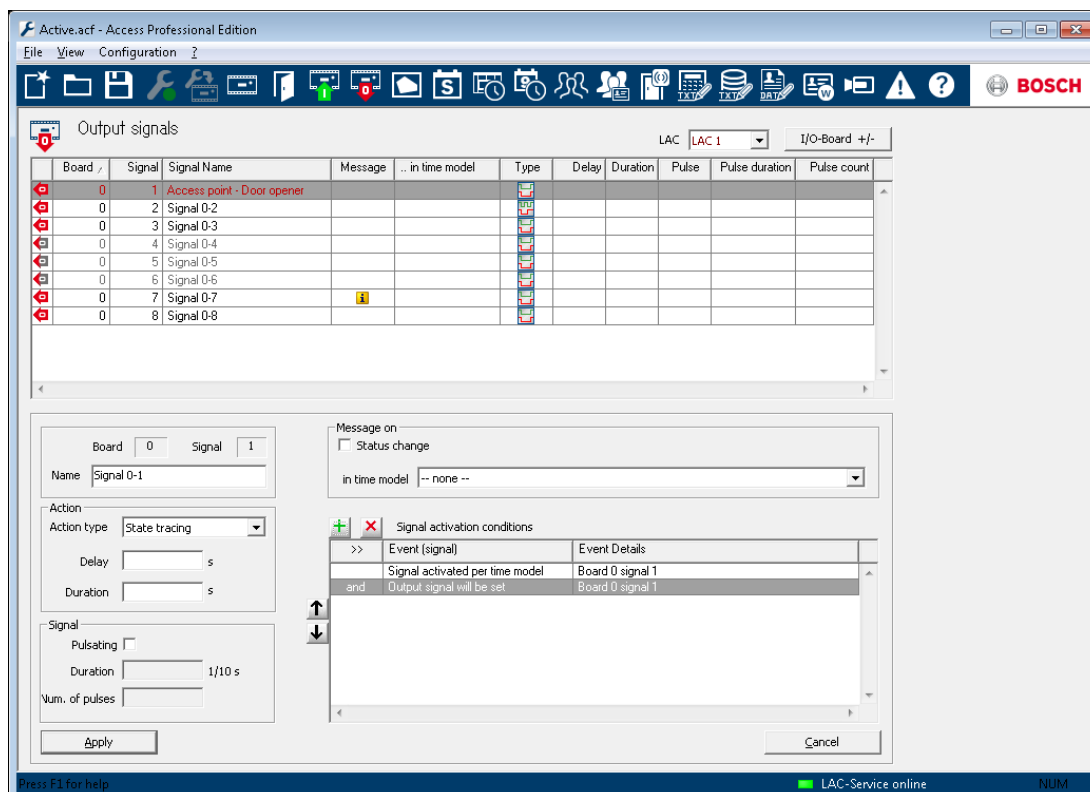
Kolumna	Parametr	Opis
- only on time model... (tylko w modelu czasowym...)	during time model (w modelu czasowym)	Wskazuje wybrany model czasowy. Dwukrotne kliknięcie w tej kolumnie umożliwia użytkownikowi wybór z listy modeli czasowych.
<brak>	Signal type (Typ sygnału) Digital (Cyfrowy) Analog (Analogowy)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

**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.

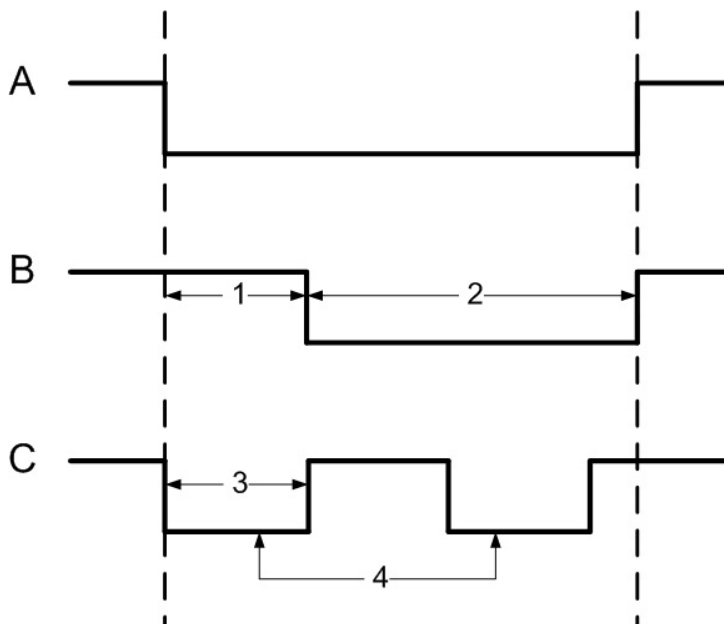
Wymienione tutaj ustawienia sygnałów wyjściowych można uzupełnić, wprowadzając dodatkowe **warunki**, które muszą zostać spełnione, aby sygnał wyjściowy był aktywowany.

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.

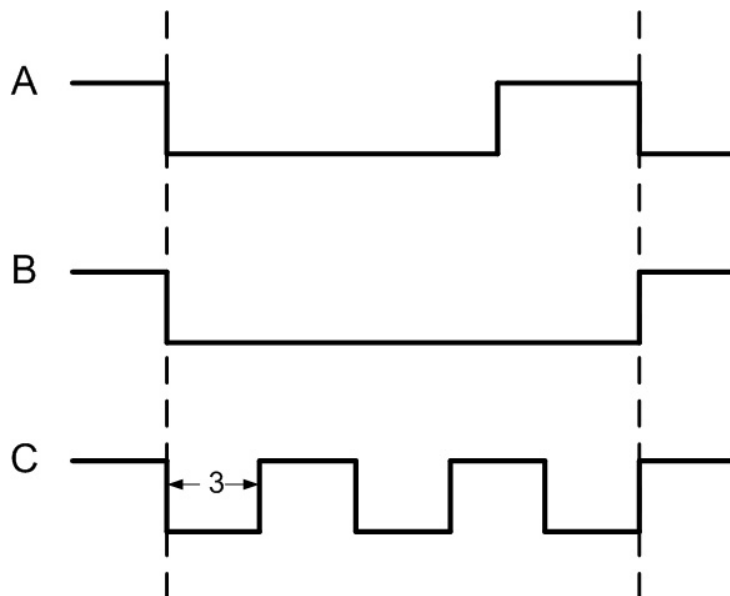
Kolumna	Parametr	Opis
Signal (Sygnał)		Numeracja sygnału dla danego modułu (1 do 16). Tego parametru nie można zmienić.
Signal name (Nazwa sygnału)	Name (Nazwa)	Nazwa sygnału. Przy ustawieniach standardowych sygnały otrzymują następujące oznaczenia: Sygnał <Nr modułu>-<Nr sygnału> Sygnały zdefiniowane 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.
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].

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

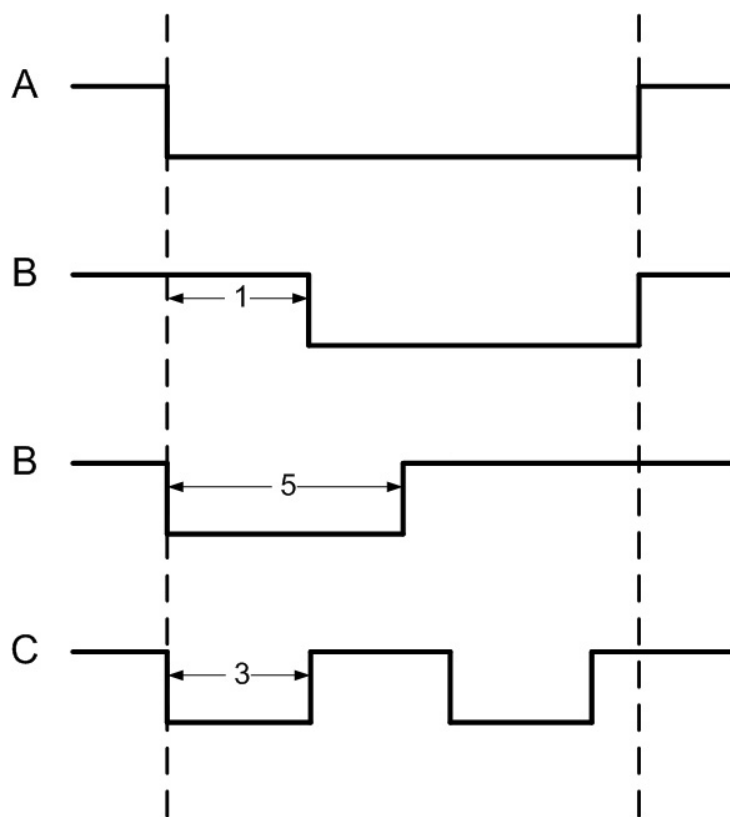
Typ czynności: Chwilowa



Typ czynności: Przełącz



Typ czynności: Śledzenie stanu

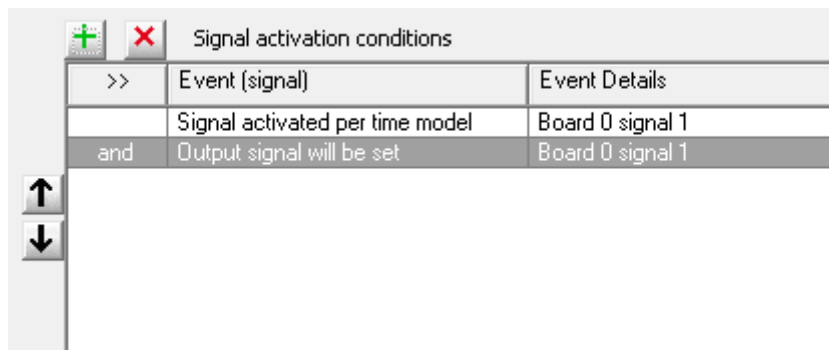



A =	stan odpytywania
B =	stabilny
C =	impulsowy
1 =	czas zwłoki
2 =	okres działania

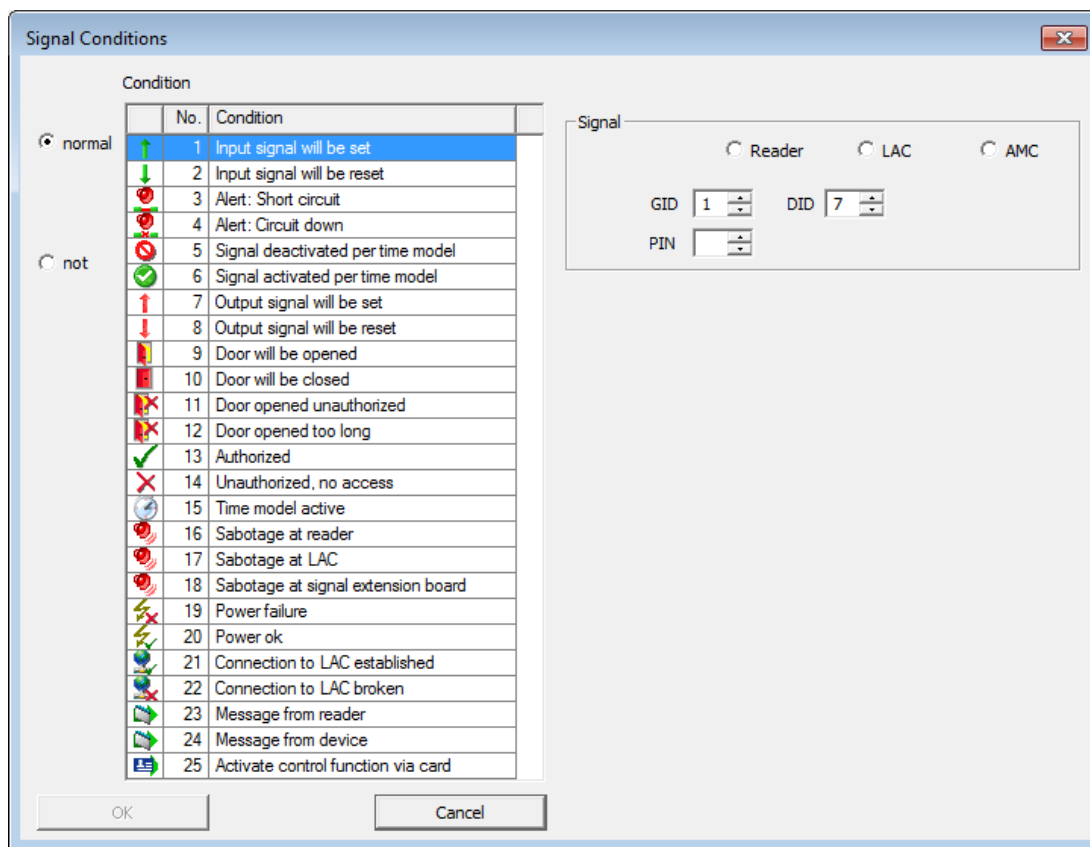
3 =	szerokość impulsu
4 =	ilość impulsów (= 2)
5 =	maks. czas aktywacji

5.3 Definiowanie warunków sygnałów wyjściowych


W oknie dialogowym **Sygnały wyjściowe** można definiować ustawienia oraz dodatkowe warunki, które jedynie w określonych sytuacjach spowodują aktywację sygnałów wyjściowych. Specjalne warunki sygnałów zaznaczonych na liście głównej zdefiniowane są w prawym dolnym rogu okna dialogowego.



Kliknij przycisk , aby otworzyć poniższe okno dialogowe. Okno to służy do konfigurowania stosownych warunków.



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

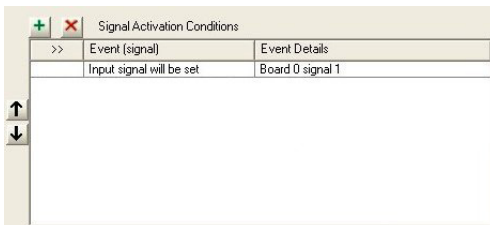
Do każdego sygnału można zastosować dowolną ilość warunków. Aby przypisać kolejny nowy warunek, należy za każdym razem otworzyć okno przez naciśnięcie przycisku .



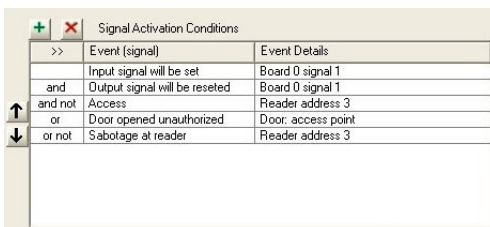
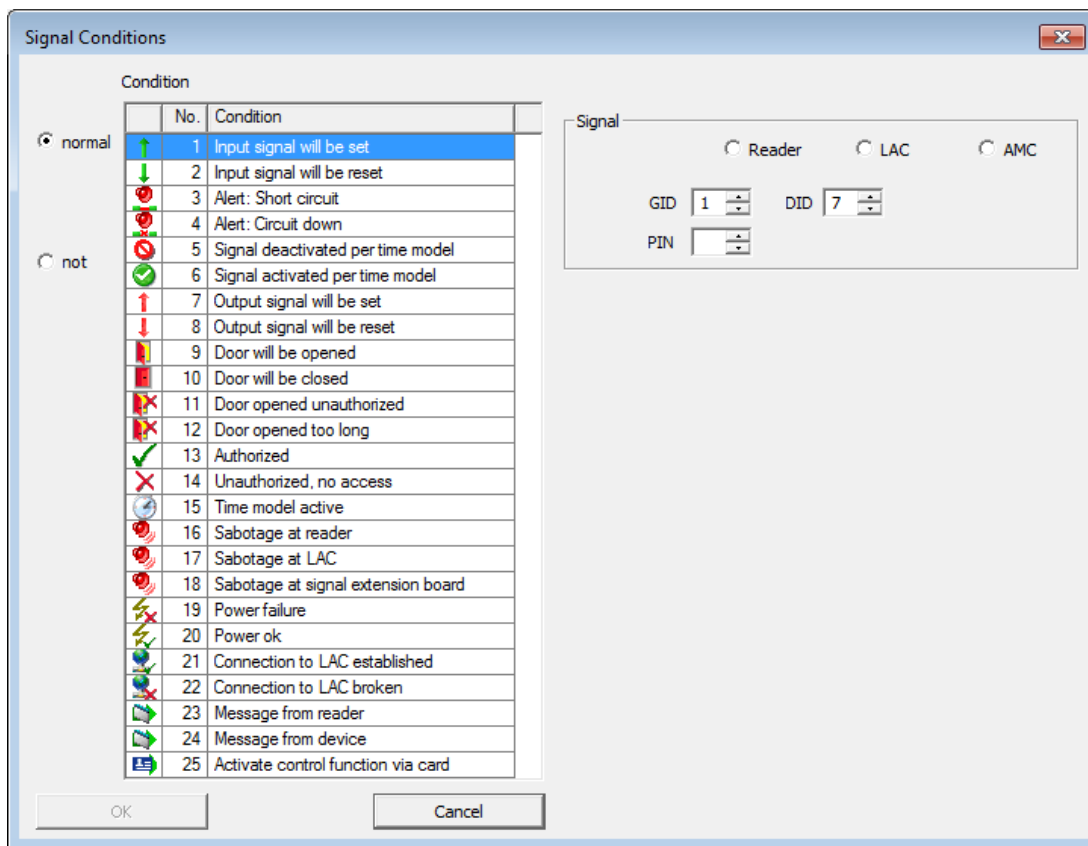
Uwaga!

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: **normalny** (jeśli warunek ma zostać spełniony) oraz **nie** (jeśli warunek ma nie być spełniony).

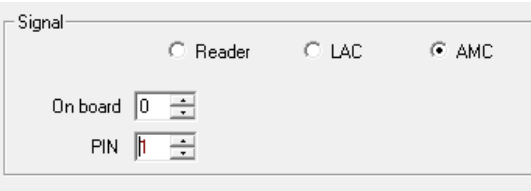
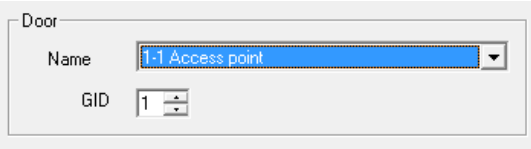



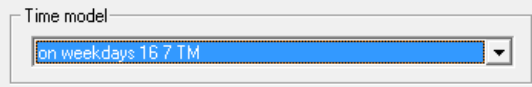
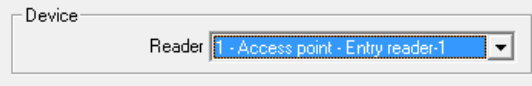
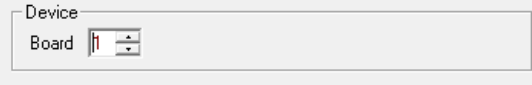
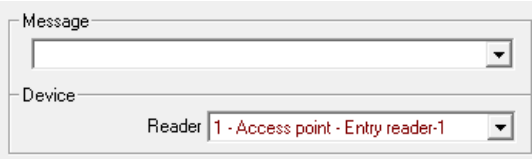
Każdy kolejny warunek zostanie połączony z pierwszym warunkiem za pomocą operatorów **i**, **i nie**, **lub** lub **lub nie**.



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:

Stan	Dane uzupełniające	
Input signal will be set (Sygnał wejściowy zostanie ustawiony)	<p>Informacja na temat urządzenia, w którym występuje sygnał. Wybór modułu. Wybór połączenia.</p> 	
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)		
Signal activated by time model (Aktywacja sygnału przez model czasowy)		
Output signal will be set (Sygnał wyjściowy zostanie ustawiony)		
Output signal will be reset (Sygnał wyjściowy zostanie wyzerowany)		
Door will be opened (Drzwi zostaną otwarte)		<p>Wybór wejścia. Automatyczne ustawienie GID (identyfikatora grupy).</p> 
Door will be closed (Drzwi zostaną zamknięte)		
Door opening unauthorized (Niedozwolone otwarcie drzwi)		
Drzwi są otwarte zbyt długo		
Dostęp		

Stan	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 prawidłowe)	
Connection LAC -> APE established (Nawiązane połączenie LAC -> APE)	
Connection LAC -> APE broken (Zerwane połączenie LAC -> APE)	
Message from reader (Komunikat z czytnika)	Wybór komunikatu z gotowej listy komunikatów. Wybór czytnika. 
Message from device (Komunikat z urządzenia)	Wybór komunikatu z gotowej listy komunikatów. Wybór modułu.

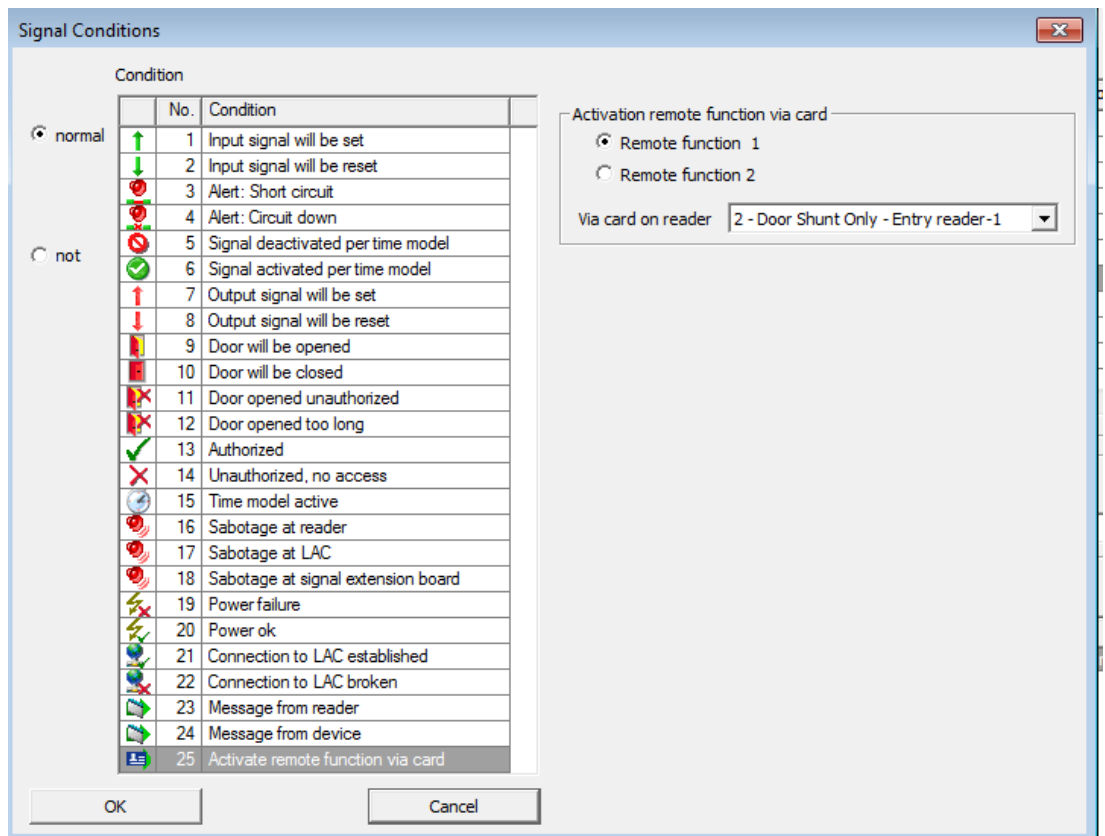
Stan	Dane uzupełniające
	<div style="border: 1px solid gray; padding: 5px;"> Message <input type="text"/> Device Board <input type="text" value="1"/> </div>
Aktywuj funkcję kontroli za pomocą karty	Ustaw wyjście z uwzględnieniem uprawnień przydzielonych posiadaczowi karty. Zobacz rozdział Activate control function via card (Aktywacja funkcji kontroli za pomocą karty). <div style="border: 1px solid gray; padding: 5px;"> Activation remote function via card <input checked="" type="radio"/> Remote function 1 <input type="radio"/> Remote function 2 Via card on reader <input type="text" value="2 - Door Shunt Only - Entry reader-1"/> </div>

5.3.1

Aktywuj funkcję kontroli za pomocą karty

Ta funkcja kontroli umożliwi osobie wywoływanie dwóch różnych sygnałów wyjściowych. Aby można było użyć tej opcji, muszą zostać spełnione następujące wymagania:

- Musi istnieć konfiguracja dla osoby z uprawnieniem do uaktywnienia funkcji kontroli.
- Karta tej osoby musi być ważna i uprawniać do dostępu do wejścia.
- W obszarze **Signal conditions** (Warunki sygnału) należy wybrać sygnał wyjściowy **25 - Activate remote function via card** (25 – aktywuj funkcję zdalną za pomocą karty).
- Funkcja zdalna musi być wybrana, a czytnik musi być przypisany.



Sposób postępowania:

- Umieść kartę w czytniku. Nastąpi sprawdzenie uprawnień osoby.
- W przypadku uprawnienia sygnał wyjściowy zostanie ustawiona zgodnie z konfiguracją.

5.4 Tworzenie modułów rozszerzeń

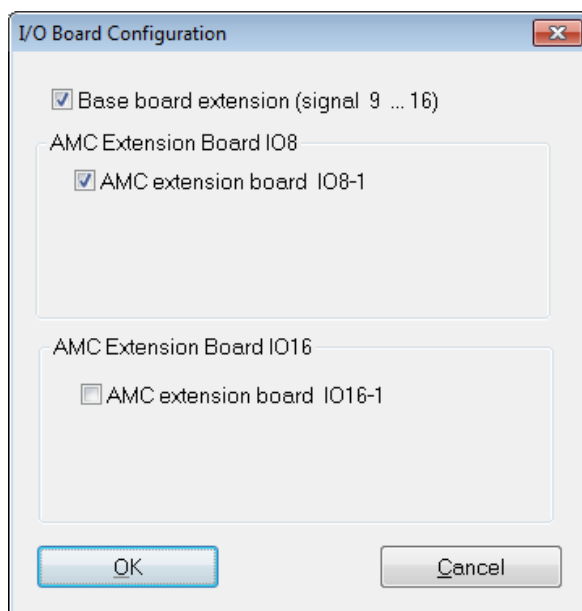
Korzystając z okien dialogowych, moduły rozszerzeń można konfigurować w zakresie sygnałów **wejściowych** i **wyjściowych**. Ustawienia skonfigurowane w jednym oknie dialogowym będą aktywne w drugim.

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!

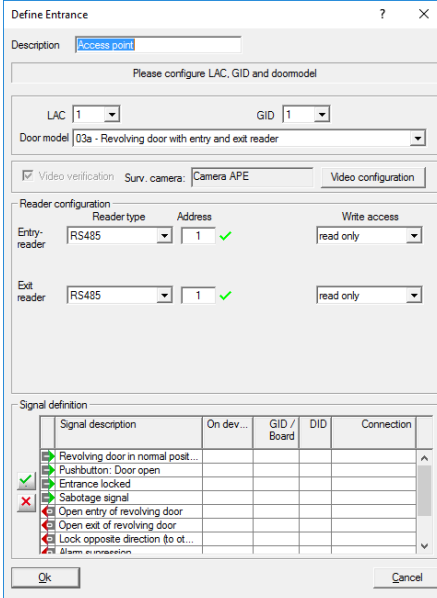
Dokonane w tym miejscu ustawienia funkcji **I/O boards** (Moduły WE/WY) dotyczą zarówno sygnałów wejścia, jak i wyjścia danego kontrolera, i mogą być wprowadzone w obu oknach dialogowych.

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 (rygły, 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**).



Signal description	On dev...	GID / Board	DID	Connection
Revolving door in normal posit...				
Pushbutton: Door open				
Entrance locked				
Sabotage signal				
Open entry of revolving door				
Open exit of revolving door				
Lock opposite direction (to ot...				
...				

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**.

**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.

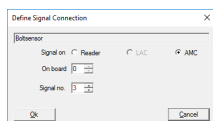
Zastosowanie adresu czytnika 9:

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 czytnik 4 i 7. Nie można jednak nadać dwukrotnie tego samego adresu, dlatego najpierw ustawiamy czytnik 4 na adres 9. Zmieniając teraz parametry można czytnik 7 przestawić 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 karty rozszerzeń, 1... 16

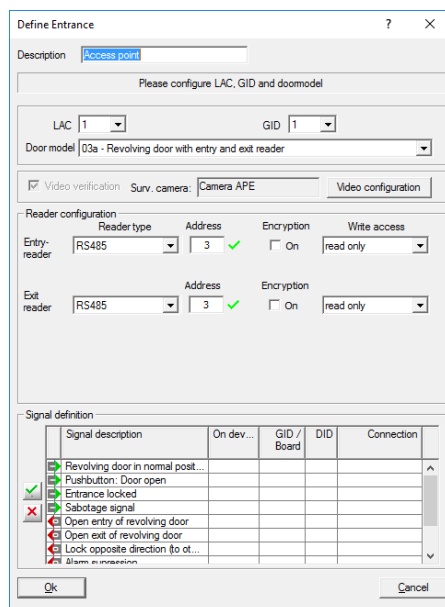
Ustawione połączenia zostaną wyświetlone w polu listy w odpowiednich kolumnach. Poza tym w pierwszej kolumnie znajdują się różne symbole określające stan sygnałów:

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

Zdefiniowany sygnał można usunąć za pomocą przycisku

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

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



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



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

**Uwaga!**

W przypadku stosowania kart kodowanych Mifare firmy Bosch z czytnikiem OSDP należy wybrać typ karty **Mifare (63 Bity)**, aby uaktywnić kodowanie firmy Bosch.

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!

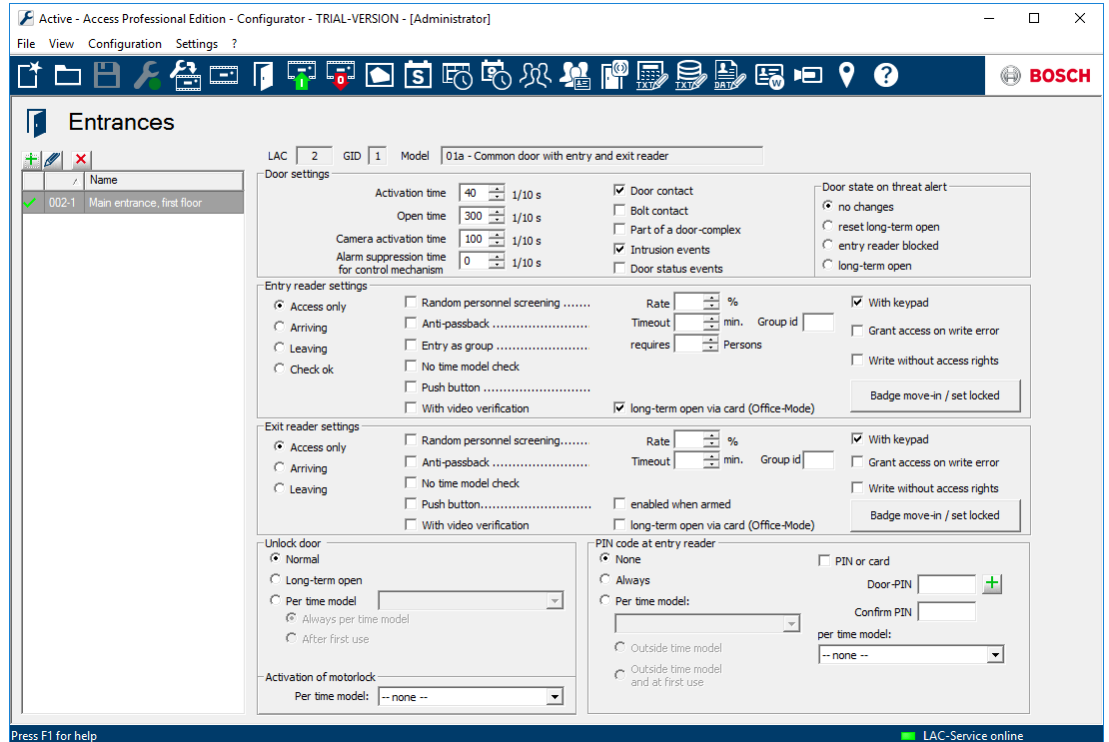
Jeśli ten klucz zostanie utracony, we wszystkich czytnikach konieczne będzie przywrócenie ustawień fabrycznych przez Obsługę techniczną!

**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
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 umożliwia systemowi stwierdzenie, czy drzwi są rzeczywiście zamknięte.
Element zespołu drzwiowego	Umożliwia ustawienie drzwi jako elementu składowego zespołu drzwiowego, np. śluzy osobowej lub śluzy 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.
Stan drzwi w momencie alertu zagrożenia	Konfigurowanie stanów drzwi dla alertu zagrożenia (patrz rozdział <i>Configuring threat alerts</i> (Konfigurowanie alertów zagrożenia))

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	Przejście przez ten czytnik kart spowoduje wygenerowanie dodatkowo zapisu rejestracji czasu pracy i zapisanie obecności danej osoby.
Opuszczenie	Przejście 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).</p> <p>Tworzony jest plik o nazwie TA_<Bieżąca data RRRRMMDD>.dat, który może zostać poddany edycji. Pola rozdzielone są średnikami i mogą być edytowane na przykład w aplikacjach arkuszy kalkulacyjnych innych producentów.</p> <p>Każdy rekord przejścia zawiera następujące dane: Nazwisko; Imię; Nazwa firmy; Numer osobisty.; Numer karty.; Pola dodatkowe 1–10 (jeśli mają parametry); Nazwa wejścia; Data (rrrrmdd); Godzina (ggmmss plus litera „s” wskazująca czas letni); Kierunek przejścia wyrażony numerycznie (1 = wejście, 2 = wyjście); Kierunek jako łańcuch tekstowy (WEJŚCIE, WYJŚCIE)</p>	
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%).</p> <p>Należy jednak zapewnić, że czytnik przesiewowy nie będzie jednocześnie skonfigurowany jako czytnik zwolnienia odblokowujący karty zablokowane przez czytniki przesiewowe.</p>
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 480.</p>

Ustawienia czytnika Czytniki wejść i wyjść	Opis
	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: 1–2 znaki 0–9 i/lub A–Z
Wejście jako grupa – wymagane podanie liczby osób	Tylko w przypadku czytników wejścia . Opcja umożliwi wejście dopiero w momencie, gdy grupa składająca się z co najmniej podanej liczby osób przesunie swoje karty przez czytnik. Możliwe wartości: 2–6.
Z klawiaturą	To pole wyboru należy zaznaczyć, jeśli czytnik przy drzwiach ma klawiaturę.
Bez sprawdzania modelu czasowego	Domyślnie dostęp sprawdzany jest w stosunku do modelu czasowego. Zachowanie to można wyłączyć, ustawiając ten parametr.
Wejście z podajnikiem kart	Tę opcję należy aktywować w przypadku, gdy czytnik jest wyposażony w podajnik kart.
Przycisk – zawsze aktywny	Parametr umożliwi rozpoznanie sygnału otwarcia drzwi. Sygnał ten może pochodzić z przycisku lub z telefonu, np. kiedy nie jest dostępny żaden czytnik. 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 uaktywnieniu przycisku funkcja ta będzie obejmować również czytnik wyjścia.
With video verification (Z weryfikacją wideo)	Jeśli weryfikacja wideo ma być aktywna, należy zaznaczyć to pole wyboru.
Długotrwałe otwarcie za pomocą karty (tryb biurowy)	Opcja ta opisuje zawieszenie kontroli dostępu przy wejściu w godzinach pracy biura. Wejście pozostaną otwarte w tych godzinach, aby zezwalały na nieutrudniony dostęp publiczny (zob. rozdział Tryb biurowy).



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	Zezwolenie stałe na otwarcie drzwi odbywa się na podstawie wybranego modelu czasowego w następujących wariantach: <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	Opcję wprowadzania kodu PIN steruje wybrany model czasowy w następujących wariantach: <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.

Więcej informacji

- *Konfigurowanie alertów zagrożenia, Strona 102*

6.3 Office mode (Tryb biuro)

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

Dla trybu biuro muszą być spełnione następujące warunki:

- Musi być skonfigurowane jedno lub więcej wejść z przedłużonym okresem braku blokowania.
- Przy wejściu należy użyć co najmniej jeden czytnik z klawiaturą.
- Jeden lub więcej użytkowników musi mieć uprawnienia do włączenia i wyłączenia trybu biuro.
- Ich karty muszą być ważne i muszą umożliwiać dostęp poza godzinami pracy w trybie biuro.

Sposób postępowania:

- Nacisnąć na czytniku klawisz „3”.
- Wczytać kartę. Nastąpi sprawdzenie uprawnień osoby.
- Jeśli uprawnienia są ważne stan drzwi zostanie zmieniony na stale otwarte.
- Stan drzwi przełącza się po każdym wykonaniu podanych wyżej kroków.



Uwaga!

Opcja Tryb biuro nie powoduje otwarcia drzwi zablokowanych.

Jeśli tryb biuro jest skonfigurowany dla określonych drzwi, nie musi być dla nich skonfigurowany model czasowy.

6.4 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.

6.5

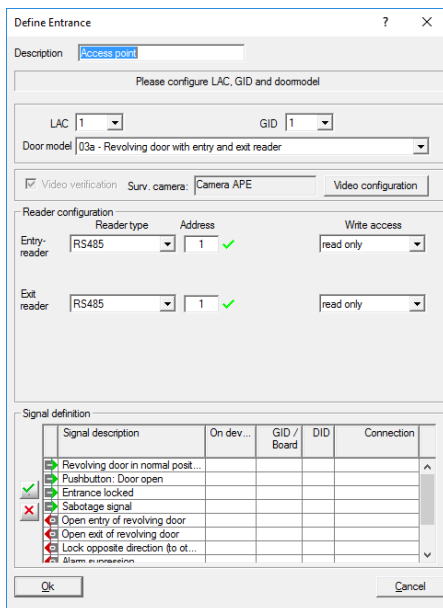
Przypisywanie urządzeń wizyjnych do wejścia

Okno dialogowe tworzenia wejścia zawiera opcję konfiguracji kamer związanych z tym wejściem.

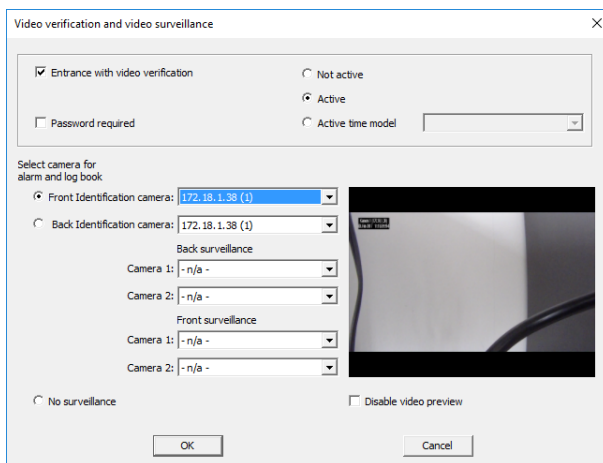
Aby włączyć i skonfigurować ustawienia opcji **Video verification** (Weryfikacja wideo), można skorzystać ze specjalnego okna dialogowego, które służy do wprowadzania zmian i konfigurowania innych ustawień. Okno to można otworzyć, klikając przycisk **Video configuration** (Konfiguracja wideo). Należy wykonać następujące czynności:

- Zaznacz pole wyboru **Video verification** (Weryfikacja wideo) w przypadku czytników przypisanych do danego wejścia.
- Kliknij przycisk  lub kliknij dwukrotnie wybrany kontroler LAC w sekcji **Entrances** (Wejścia).

Pojawi się następujący ekran:

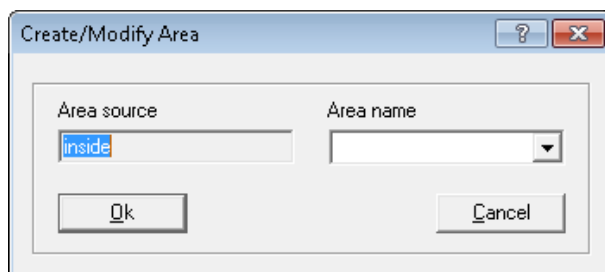


Kliknij przycisk **Video configuration** (Konfiguracja wideo), aby otworzyć ekran konfiguracji:



**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.

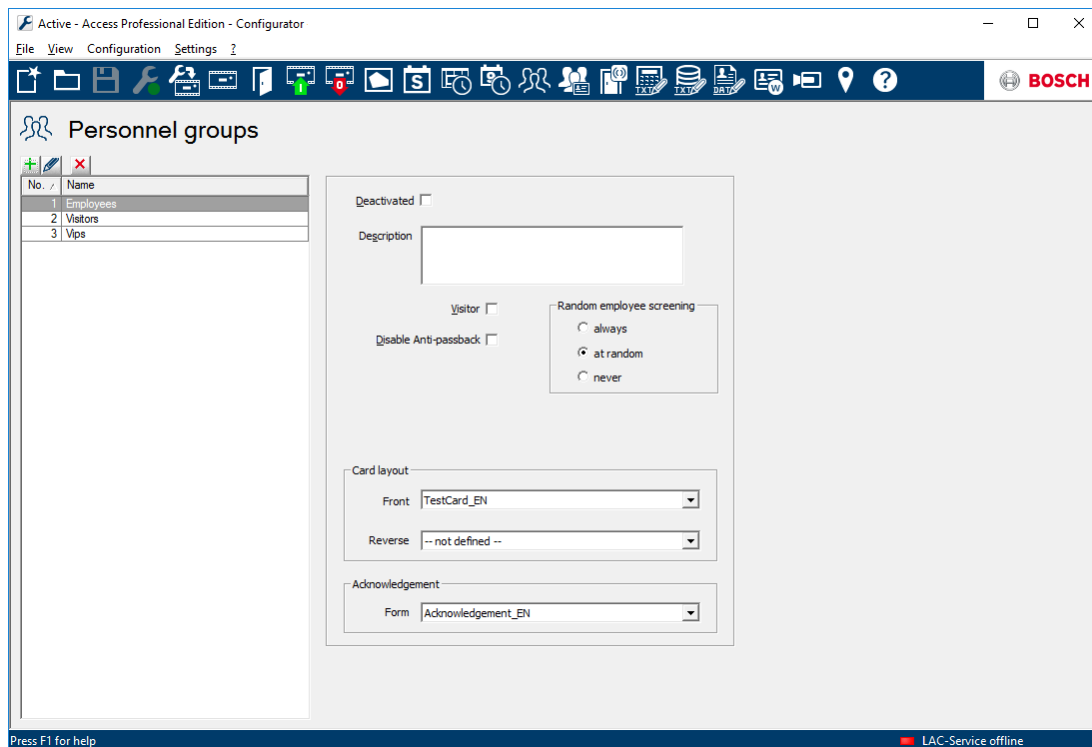
Przykład:

Ze wstępnie zdefiniowanej strefy pomieszczeń **--poza--** przechodzi się np. przez wejście główne i dochodzi do strefy pomieszczeń **Recepcja**. Stamtąd do budynków A, B lub C. Tak więc w programie Access PE utworzone muszą zostać strefy pomieszczeń, które prowadzą ze **strefy źródłowej Recepcja** do budynków A, B i C.

Po utworzeniu nowej strefy należy przyporządkować do niej przynajmniej jedno wejście. Aby możliwe było wejście do strefy, konieczny jest przynajmniej jeden czytnik wejścia. W tym celu dostępne są dwa pola list po prawej stronie okna dialogowego.

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.



Po lewej stronie znajduje się lista wszystkich utworzonych dotychczas grup personelu. Wzdłuż górnej krawędzi pola listy znajdują się następujące przyciski:



Add (Dodaj): dodawanie nowej grupy personelu

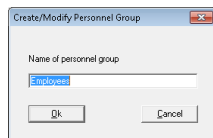


Modify (Modyfikuj): modyfikowanie zaznaczonej grupy personelu



Delete (Usuń): usuwanie zaznaczonej grupy personelu

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



W ten sposób można rozróżniać między 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 odpowiadających danej grupie.

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

Ustawienia	Opis
Nieaktywny	Dezaktywacja grupy personelu jest pierwszym etapem przygotowującym ją do usunięcia. Taka grupa personelu wprowadzie nadal występuje w systemie, jednak nie można do niej przypisać żadnej nowej osoby. Grupę personelu wolno usunąć pod warunkiem, że nie należą już do niej żadne osoby.
Opis	Do każdej grupy personelu można załączyć szczegółowy opis.
Visitor (Goście)	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). Dzięki temu grupę personelu Visitor (Goście) może przeglądać osobno od grupy Employee (Pracownicy).

Ustawienia	Opis
Disable Anti-passback (Wyłącz zapobieganie podwójnemu przejściu)	Określoną grupę osób (np. VIP-ów) można wykluczyć z zakresu funkcji zapobiegania podwójnemu przejściu
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.
Badge Layout (Wygląd karty identyfikacyjnej) Front (Przód) Back (Tył)	Aby utworzyć kartę identyfikacyjną, należy w pierwszej kolejności wybrać jej 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**

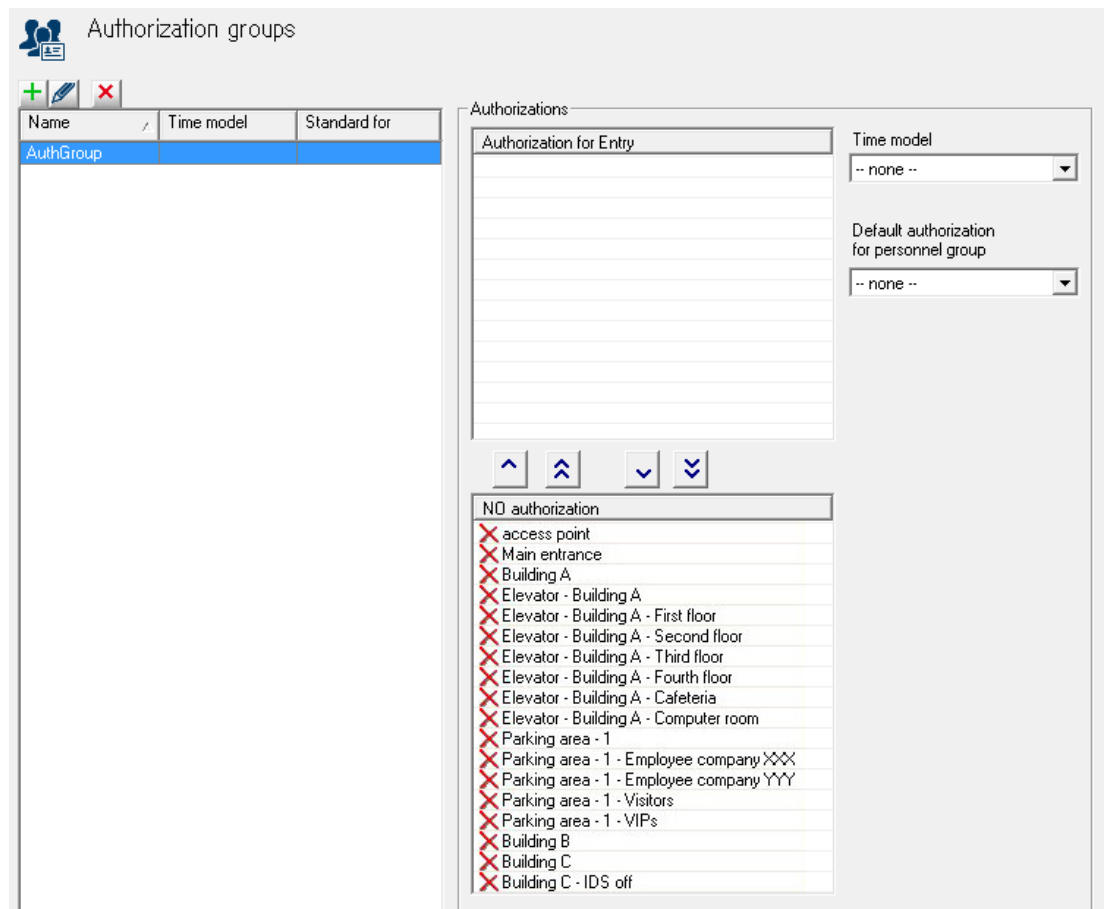
- Dostęp grupy można skonfigurować wyłącznie dla modeli drzwi 1+3.
- Dostęp grupy i ograniczenie dotyczące obszaru osób mogą prowadzić do tego, że w obszarze będzie większa liczba osób niż dozwolona – liczba osób w obszarze jest sprawdzana, gdy cała grupa wejdzie w dany obszar.
- W przypadku dostępu 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. Wzdłuż górnej krawędzi pola listy znajdują się następujące przyciski:




Add (Dodaj): dodawanie nowej grupy uprawnień dostępu.

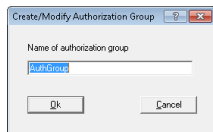


Modify (Modyfikuj): modyfikowanie zaznaczonej grupy uprawnień dostępu.

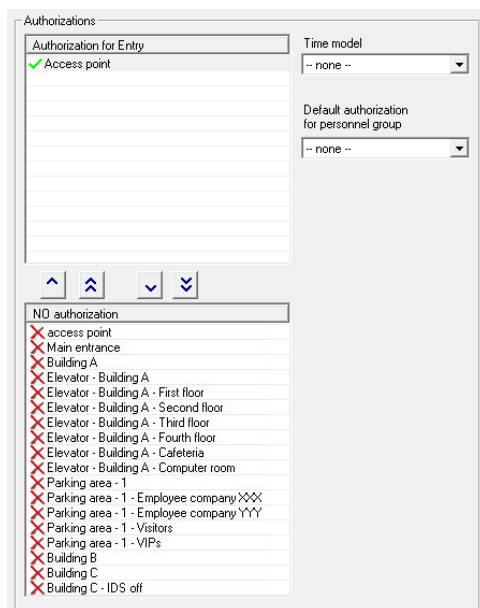






Delete (Usuń): usuwanie zaznaczonej grupy uprawnień dostępu.

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.



Przejścia 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.

Authorizations

Authorization for Entry

- ✓ Access point Delta Rdr
- ✓ 1st floor right
- ✓ 1st floor left
- ✓ garage

Time model

on weekdays 7-16 o'clock

Default authorization for personnel group

Employees

NO authorization

- ✗ Demo Suitcase Rdr 1
- ✗ Demo Suitcase Rdr 2
- ✗ Enrollment reader
- ✗ Enroll 1

Do każdej grupy można przydzielić **model czasowy**, który ogranicza obowiązywanie uprawnień; patrz **Zastosowanie modeli czasowych** (*Modele czasowe, Strona 77*) w systemie 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.

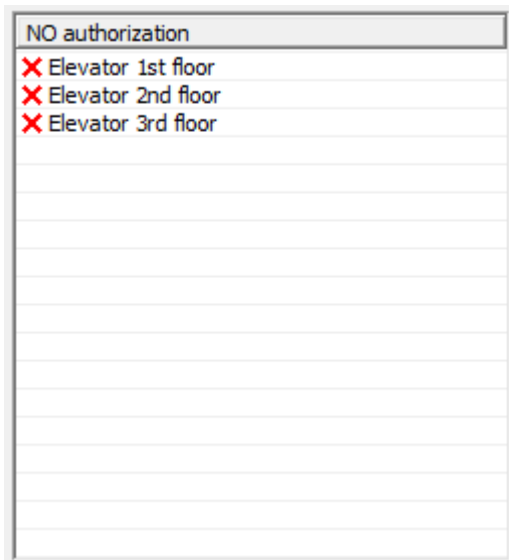
Oprócz tego można daną grupę uprawnień zdefiniować jako **default authorization** (uprawnienia domyślne) dla **personnel group** (grupy personelu) (np. pracownicy lub goście). Grupa uprawnień dostępu zostanie następnie automatycznie przyporządkowana podczas wprowadzania do wybranej grupy osób nowej osoby,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

9.2 Uprawnienia specjalne

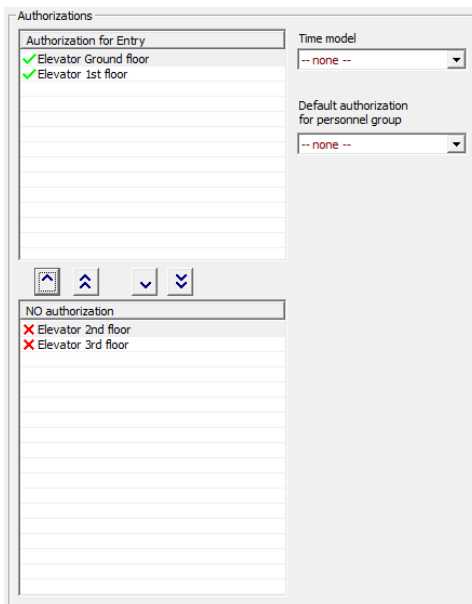
Modele drzwi 07 i 14 do **konfiguracji** wymagają podania dodatkowych informacji (*Modele drzwi z ustawieniami specjalnymi, Strona 55*). Różnią się jednak od innych modeli drzwi także w zakresie przydzielania i użytkowania.

Model drzwi 07: winda

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

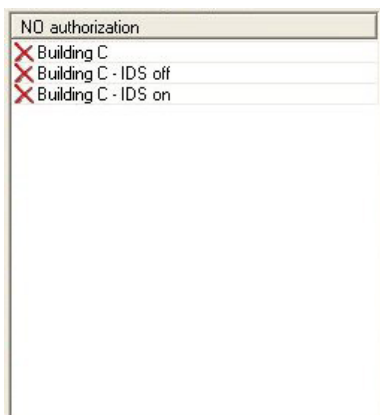


Podczas tworzenia grup uprawnień powinien zostać przydzielony jeden czytnik dla **windy** i **co najmniej jedna kondygnacja**.



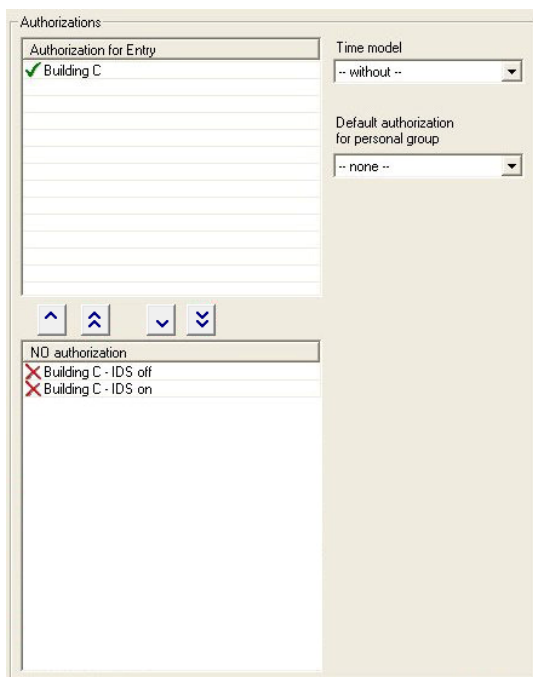
Model drzwi 14: Ponowne uzbrajanie systemu sygnalizacji włamania

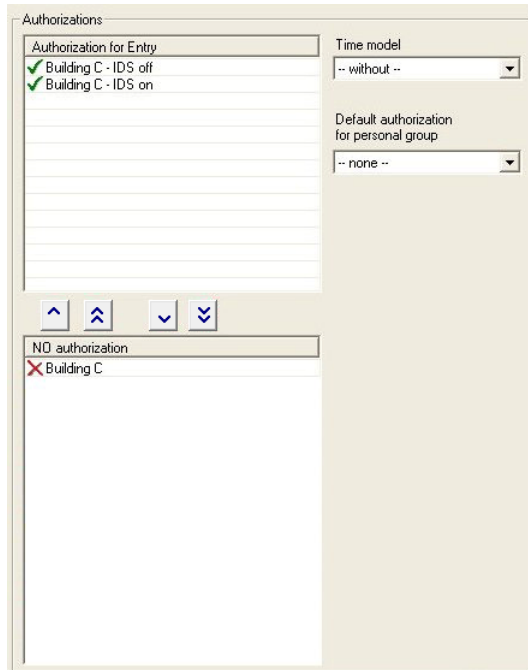
Lista dostępnych uprawnień zawiera oddzielny element dla wejścia, jak również dla uzbrojenia i rozbrojenia systemu alarmowego.



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.





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 systemie Access PE zdefiniowana jest pewna liczba typowych świąt. W zależności od lokalizacji można je zmieniać, dodając lub usuwając 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.*
Ulis Special	21.09.2016

Deactivated

Categorie Holiday

Priority higher than weekend

Date

01.01.*

active for offline locking system



Uwaga!

Liczba elementów dla systemu blokowania offline jest ograniczona do ##.

Wzdłuż górnej krawędzi pola listy znajdują się następujące przyciski:



Create (Utwórz): tworzenie nowego dnia świątecznego/specjalnego



Modify (Modyfikuj): modyfikowanie dnia świątecznego/specjalnego



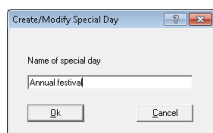
Delete (Usuń): usuwanie dnia świątecznego/specjalnego



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 nowej lub zmienionej nazwy. Po prawej stronie obok pola listy należy zdefiniować parametry elementu zaznaczonego na liście.

Nieaktywny	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 przypisać do poszczególnych kategorii 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 to pole wyboru jest zaznaczone, również w soboty/niedziele obowiązywać będzie model dzienny dnia świątecznego, a w przeciwnym razie pierwszeństwo ma model dzienny soboty/niedzieli.
Date (Data)	W przypadku dnia świątecznego powtarzającego się corocznie 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.

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

periods

1st period

start 07:00

end 16:00

2nd period

start

end

3rd period

start

end

Po lewej stronie znajduje się lista wszystkich utworzonych dotychczas modeli dziennych. Wzdłuż górnej krawędzi pola listy znajdują się następujące przyciski:





Utwórz nowy model dzienny

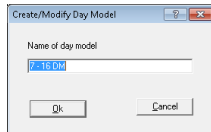


Edytuj zaznaczony model dzienny



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 49*) 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.

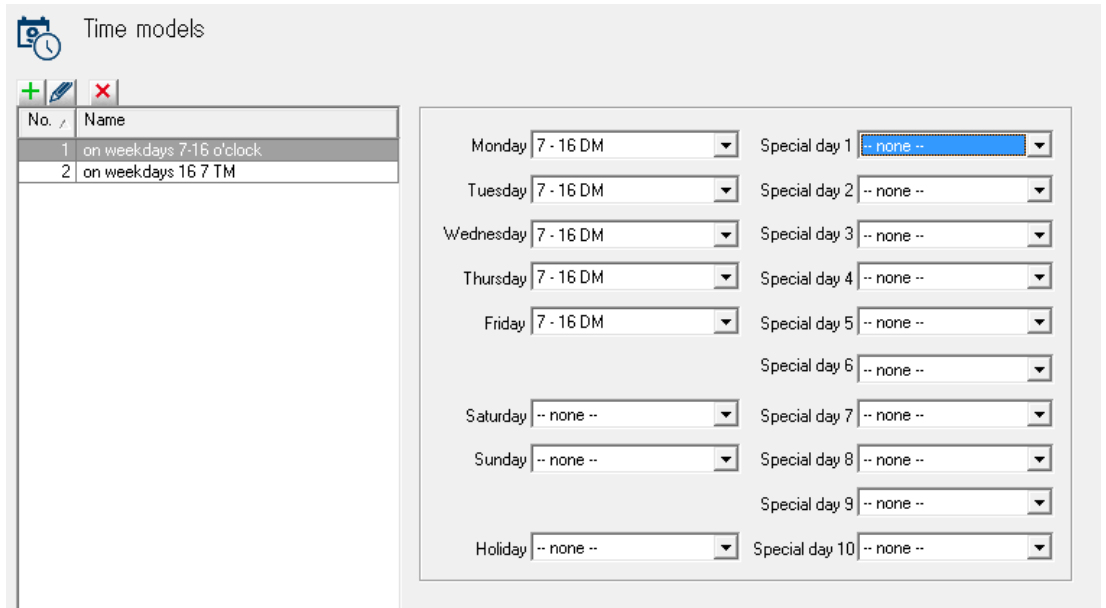
Przykład:**Osoba otrzymuje następujące uprawnienia:**

- 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 służy do tworzenia i modyfikowania modeli czasowych, które zależnie do zastosowania uaktywniają pewne elementy systemu.



Po lewej stronie znajduje się lista wszystkich utworzonych dotychczas modeli czasowych. Wzdłuż górnej krawędzi pola listy znajdują się następujące przyciski:





Create (Utwórz): tworzenie nowego modelu czasowego

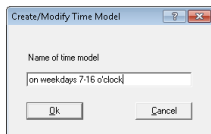


Modify (Modyfikuj): modyfikowanie zaznaczonego modelu czasowego



Delete (Usuń): usuwanie zaznaczonego modelu czasowego

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 stworzonych przy wybieraniu języka aplikacji.

13.1 Displaytexts (Wyświetlany tekst)

	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: _



Uwaga!

Dla piętra wpisz jedną cyfrę, jeżeli liczba pięter zawiera się w zakresie 1–9. W przypadku 10 lub więcej pięter wpisz liczbę dwucyfrową.

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 „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 przestawione 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


	!	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:@@ Cor:@@ 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 kolumnie **Category** (Kategoria), w którym ma zostać wprowadzona zmiana, 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
		IDS armed	14	New address assigned
		IDS not armed	15	Address not assigned
		Program Startup	16	Personnel data initialized
		Program Shutdown	17	Invalid parameter received
		Operator action	18	Program download OK
		Error	19	Error on program download
		Arriving	20	Access
		No access	21	Authorized but no entry

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

	Event log unavailable (Dziennik zdarzeń niedostępny)
	Information (Informacje)
	Message (Komunikat)
	Error (Błąd)
	Alarm
	Arriving (Przybycie)
	Leaving (Opuszczenie)
	No access (Brak dostępu)
	No authorization (Brak autoryzacji)
	Malfunction (Usterka)
	OK
	IDS armed (System sygnalizacji włamania uzbrojony)
	IDS not armed (System sygnalizacji włamania nieuzbrojony)
	Program startup (Uruchomienie programu)
	Program shutdown (Zakończenie działania programu)
	Operator action (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).

Odpowiedni tekst można zmodyfikować po dwukrotnym kliknięciu pola w kolumnie **Log text** (Tekst dziennika), w którym ma zostać wprowadzona zmiana.

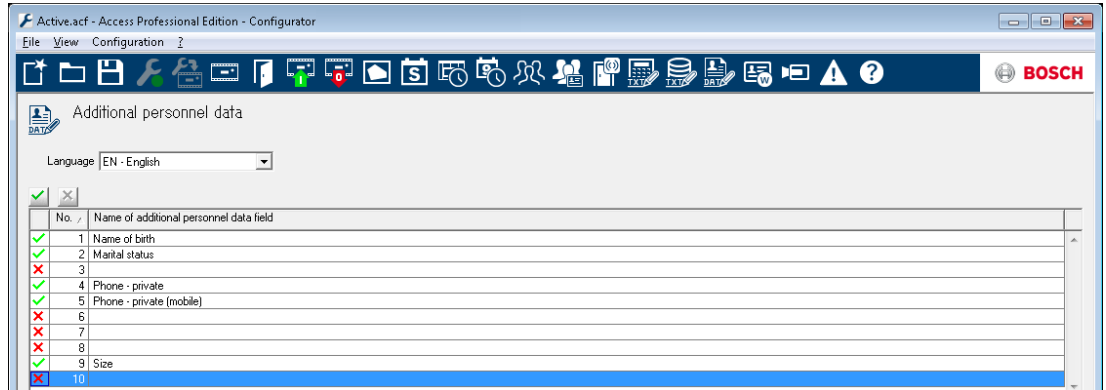
	!	Category	No. /	Log text
		Information	1	Cold start (Boot)
		Information	2	Program start
		Alarm	3	Sabotage contact opened
		Message	4	Sabotage contact closed
		Error	5	Power fail
		Message	6	Power ok
		Error	7	Hardware error: @@@@
		Message	8	LAC online
		Error	9	LAC offline
		OK	10	online (ready)
		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 przestawione na jego język.

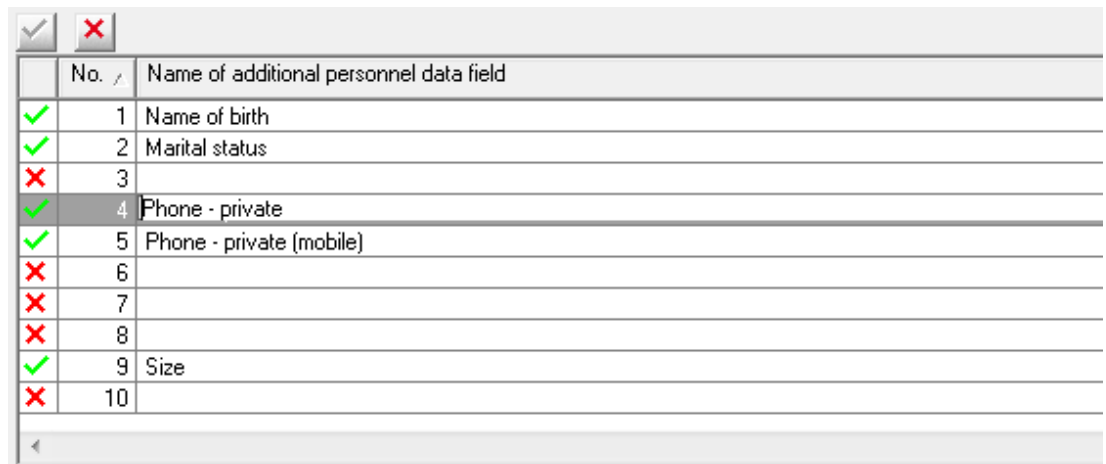
14

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.

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 Zarządzanie urządzeniami wizyjnymi

15.1 Otwieranie aplikacji Configurator


Istnieją trzy możliwe sposoby otwierania aplikacji Configurator (konfigurator):

Opcja 1



1. Kliknij dwukrotnie ikonę aplikacji Configurator na pulpicie
 - Aplikacja Configurator zostanie otwarta.

Opcja 2

1. Otwórz aplikację **Access PE Personnel Management**.
2. Na pasku menu aplikacji **Access PE Personnel Management** kliknij przycisk .
 - Aplikacja Configurator zostanie otwarta.


Opcja 3

1. Otwórz aplikację **Access PE Personnel Management**.
2. Na pasku menu wybierz pozycję **Tools** (Narzędzia).
3. Na liście rozwijanej wybierz pozycję **Execute Configurator** (Uruchom konfigurator).
 - Aplikacja Configurator zostanie otwarta.

15.2 Znajdowanie urządzeń wizyjnych

Warunki wstępne:


- Zainstaluj i skonfiguruj wszystkie urządzenia wizyjne.
- Otwórz aplikację Configurator.

1. Na pasku menu aplikacji Access Professional Edition Configurator kliknij przycisk .
2. Kliknij przycisk **Browse new devices** (Przeglądaj nowe urządzenia), aby wyszukać urządzenia wizyjne.
 - Podczas wyszukiwania nazwa przycisku zmienia się na **End searching** (Zakończ wyszukiwanie), aby można było w dowolnym momencie przerwać wyszukiwanie.
 - Wszystkie urządzenia wizyjne obsługiwane przez narzędzie Bosch Video SDK zostaną wykryte i wyświetlone w polu listy w prawym dolnym rogu okna dialogowego aplikacji Configurator.

Więcej informacji

- *Otwieranie aplikacji Configurator, Strona 88*

15.3 Dodawanie urządzenia wizyjnego do systemu kontroli dostępu

1. Otwórz aplikację Configurator.
2. Na pasku menu aplikacji Access Professional Edition Configurator kliknij przycisk .
3. Kliknij przycisk **Browse new devices** (Przeglądaj nowe urządzenia), aby wyszukać urządzenia wizyjne.
 - Podczas wyszukiwania nazwa przycisku zmienia się na **End searching** (Zakończ wyszukiwanie), aby można było w dowolnym momencie przerwać wyszukiwanie.

- Wszystkie urządzenia wizyjne obsługiwane przez narzędzie Bosch Video SDK zostaną wykryte i wyświetlone w polu listy w prawym dolnym rogu okna dialogowego aplikacji Configurator.
- Po uruchomieniu wideo przycisk aktywacji zostanie wyłączony.
- 4. Wybierz urządzenie wizyjne w polu listy w prawym dolnym rogu okna dialogowego aplikacji Configurator.
- 5. Kliknij przycisk **Activate device** (Aktywuj urządzenie).
- Wybrane urządzenie wideo zostanie przeniesione do pola listy po lewej stronie okna dialogowego aplikacji Configurator.

**Uwaga!**

Można przenosić tylko urządzenia oznaczone zielonym znacznikiem wyboru. Należy najpierw udostępnić chronione hasłem pozycje na liście (oznaczone czerwonym krzyżykiem), klikając przycisk **Change Connection Data** (Zmień dane połączenia).

**Uwaga!**

Liczba urządzeń, które można przenieść może być ograniczona licencją.


Więcej informacji

- *Otwieranie aplikacji Configurator, Strona 88*

15.4

Zmianie danych połączenia

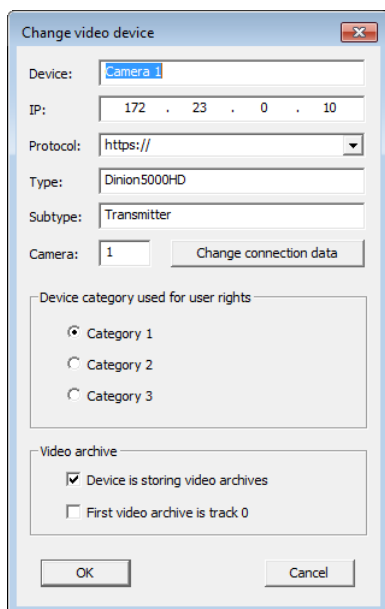
Opcja 1

1. Otwórz aplikację Configurator.
2. Na pasku menu aplikacji Access Professional Edition Configurator kliknij przycisk .
3. Kliknij przycisk **Browse new devices** (Przeglądaj nowe urządzenia), aby wyszukać urządzenia wizyjne.
 - Podczas wyszukiwania nazwa przycisku zmienia się na **End searching** (Zakończ wyszukiwanie), aby można było w dowolnym momencie przerwać wyszukiwanie.
 - Wszystkie urządzenia wizyjne obsługiwane przez narzędzie Bosch Video SDK zostaną wykryte i wyświetlone w polu listy w prawym dolnym rogu okna dialogowego aplikacji Configurator.
4. Wybierz urządzenie wizyjne w polu listy w prawym dolnym rogu okna dialogowego aplikacji Configurator.
5. Kliknij przycisk **Change Connection Data** (Zmień dane połączenia).
 - Otworzy się okno dialogowe o nazwie **Change connection parameters** (Zmień parametry połączenia).
6. Wprowadź nazwę użytkownika i hasło.
 - Upewnij się, że korzystasz z konta użytkownika z uprawnieniami.
7. Kliknij **OK**.

Opcja 2

1. Otwórz aplikację Configurator.
2. W polu listy po lewej stronie okna dialogowego aplikacji Configurator kliknij dwukrotnie urządzenie wizyjne.
 - Aby łatwiej było zidentyfikować pojedyncze urządzenia, zobacz pozycje nadajnika (nr, nazwa, adres, kamera i typ).

- Otworzy się okno dialogowe **Change video device** (Zmień urządzenie wizyjne).
- 3. Kliknij przycisk **Change Connection Data** (Zmień dane połączenia).
- 4. Wprowadź nazwę użytkownika i hasło.
 - Upewnij się, że korzystasz z konta użytkownika z uprawnieniami.
 - Dane dostępu samego urządzenia wizyjnego można zmienić tylko za pomocą jego oprogramowania.
- 5. Kliknij **OK**.




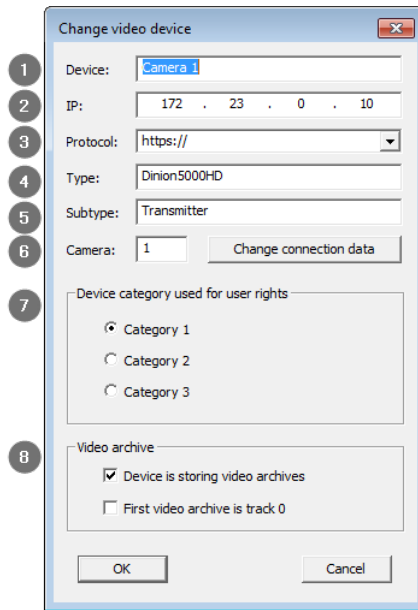
Więcej informacji

- Otwieranie aplikacji Configurator, Strona 88

15.5

Zmiana danych urządzenia wizyjnego

1. Otwórz aplikację Configurator.
2. Na pasku menu aplikacji Access Professional Edition Configurator kliknij przycisk .
3. Aby otworzyć okno dialogowe **Zmień urządzenie wizyjne**:
 - W polu listy po lewej stronie okna dialogowego aplikacji Configurator kliknij dwukrotnie urządzenie wizyjne.
 - Kliknij zieloną ikonę Plus nad polem listy po lewej stronie okna dialogowego aplikacji Configurator.
4. Wprowadź lub zmień dane urządzenia wizyjnego zgodnie z poniższymi możliwościami.
5. Kliknij **OK**.




1	Wprowadź lub zmień nazwę urządzenia wizyjnego.
2	Wprowadź lub zmień adres IP urządzenia wizyjnego.
3	Domyślnie urządzenia wizyjne są połączone za pomocą protokołu HTTPS. Jeśli wybrane urządzenie wizyjne nie obsługuje protokołu HTTPS, na liście rozwijanej wybierz opcję None (Brak).
4	Wprowadź lub zmień typ urządzenia wizyjnego.
5	Wprowadź lub zmień podtyp urządzenia wizyjnego.
6	Zmień dane połączenia.
7	Przypisz jedną z trzech kategorii uprawnień użytkownika, aby tylko wybrani użytkownicy mogli obsługiwać określone kamery.
8	Zaznacz lub wyczyść pola wyboru zależnie od tego, jak chcesz archiwizować pliki wideo.

Więcej informacji

- Otwieranie aplikacji Configurator, Strona 88

15.6

Wyświetlanie obrazu na żywo

1. Otwórz aplikację Configurator.
2. Na pasku menu aplikacji Access Professional Edition Configurator kliknij przycisk .
 - W polu listy po lewej stronie okna dialogowego aplikacji Configurator wybierz urządzenie wizyjne.
 - Kliknij przycisk **Show video** (Wyświetl wideo).


Więcej informacji

- Otwieranie aplikacji Configurator, Strona 88

15.7

Wyświetlanie zapisów archiwalnych

1. Otwórz aplikację Configurator.

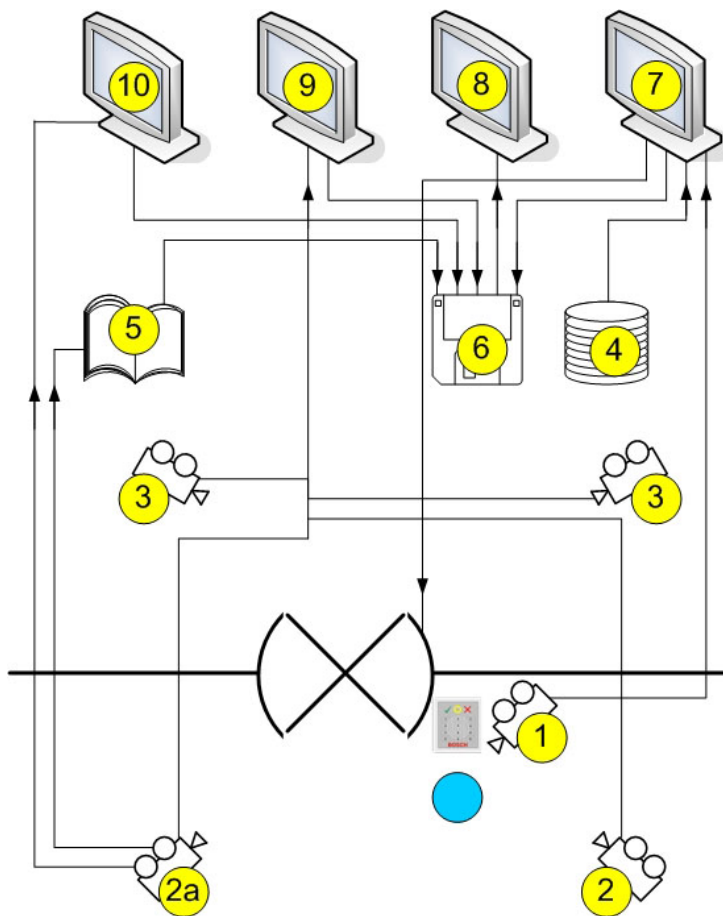
2. Na pasku menu aplikacji Access Professional Edition Configurator kliknij przycisk .
3. W polu listy po lewej stronie okna dialogowego aplikacji Configurator wybierz urządzenie wizyjne.
4. Kliknij przycisk Show playback (Pokaż odtwarzanie).
 - Otworzy się okno dialogowe o nazwie Rozpoczynanie odtwarzania.
5. Zdefiniuj punkt czasowy, od którego chcesz rozpocząć oglądanie nagrania.
6. Kliknij **OK**.

Więcej informacji

- Otwieranie aplikacji Configurator, Strona 88

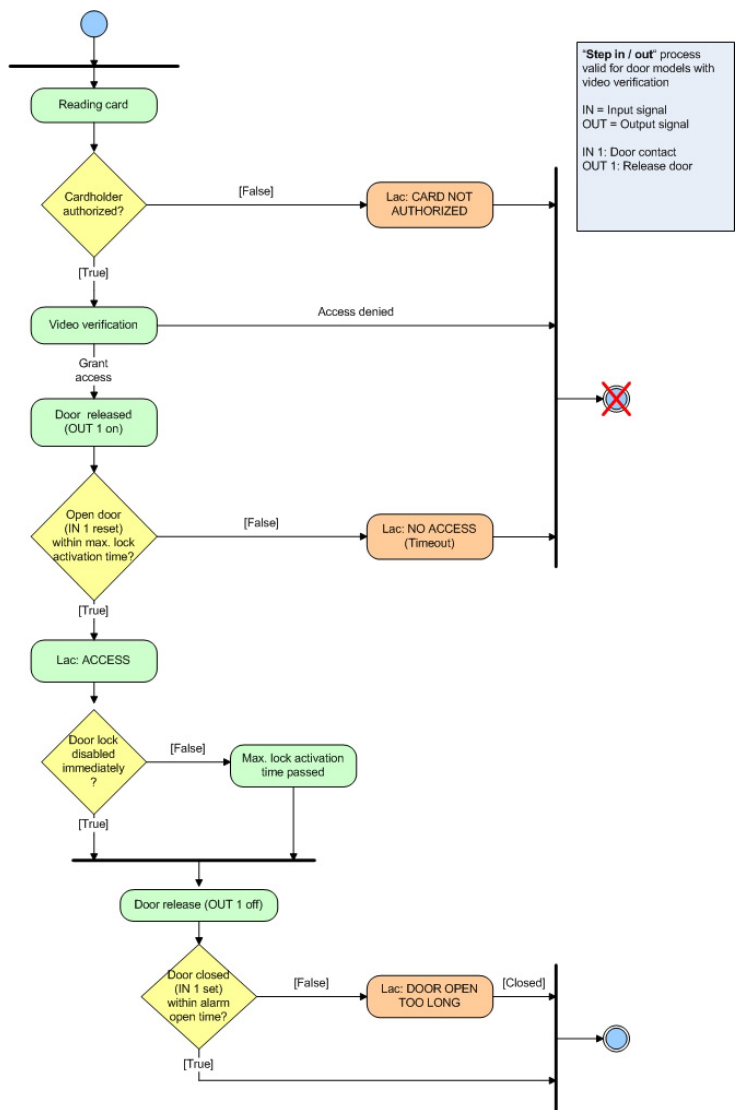
15.8

Wyświetlacze i procesy



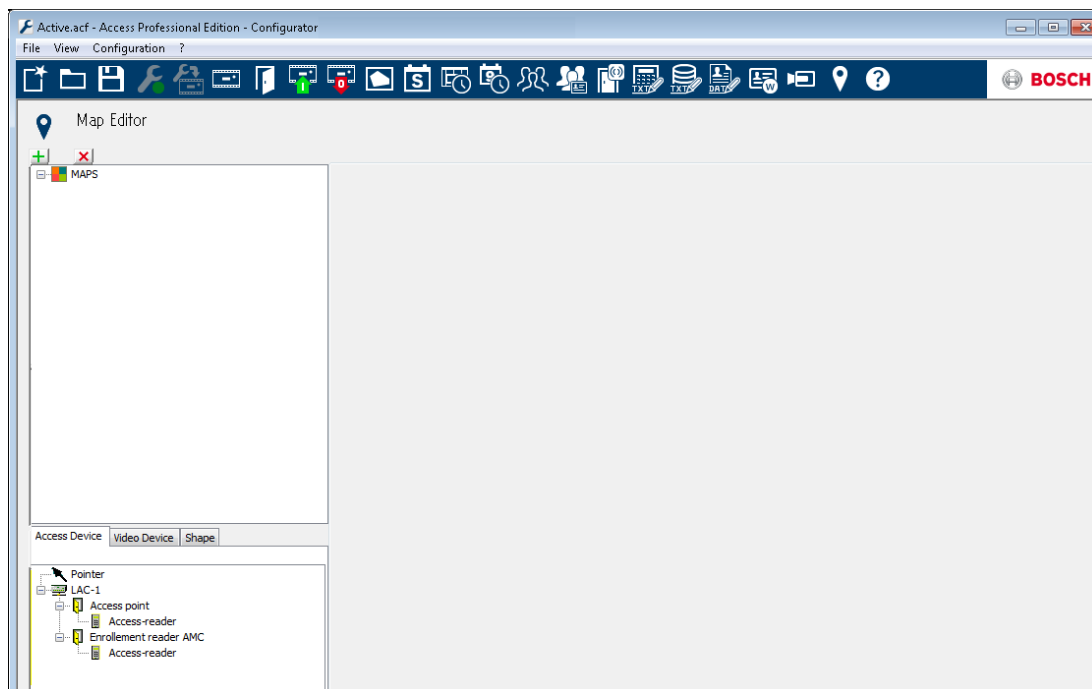
1 =	Kamera identyfikacyjna Gdy pojawia się żądanie dostępu, obraz z tej kamery jest wyświetlany w oknie dialogowym Video verification (Weryfikacja wideo) (7).
2 =	Kamery nadzorujące – strefa tylna
2a =	Kamera alarmowa i rejestracyjna Wybierz jedną z kamer 1, 2 lub 3
3 =	Kamery nadzorujące – strefa przednia
4 =	Baza danych Podczas weryfikacji danych (7) obraz z bazy danych jest zestawiany z obrazem na żywo pochodzącym z kamery identyfikacyjnej (1) w celu porównania.


5 =	<p>Dziennik</p> <p>Po skonfigurowaniu kamery alarmowej i rejestracyjnej (2a) obrazy związane z alarmami będą zapisywane.</p>
6 =	<p>Lokalny dysk twardy/nośnik danych</p> <p>Można zapisać pliki lokalne z okien dialogowych Video verification (Weryfikacja wideo) (7), Video panel (Panel wideo) (9) i Alarm Management (Zarządzanie alarmami) (10), a także z obrazów komunikatów dziennika (5). Nagrania wideo (format .vxx) mogą być odtwarzane za pomocą odtwarzacza Bosch Video Player (8).</p>
7 =	<p>Weryfikacja wideo</p> <ul style="list-style-type: none">– Porównywanie obrazów na żywo pochodzących z kamery identyfikacyjnej (1) z obrazami z bazy danych (4).– Zwalnianie/blokowanie drzwi za pomocą przycisku w oknie dialogowym.– Przechowywanie obrazów w pamięci lokalnej (6).
8 =	<p>Bosch Video Player (Odtwarzacz wideo firmy Bosch)</p> <p>Nagrania .vxx przechowywane w pamięci lokalnej (6) mogą być odtwarzane w tym oknie dialogowym.</p>
9 =	<p>Panel wideo</p> <ul style="list-style-type: none">– W tym widoku można wyświetlać obrazy z maksymalnie czterech kamer jednocześnie.– Tworzenie lokalnych zapisów (6) jest możliwe w przypadku każdej kamery.
10 =	<p>Zarządzanie alarmami</p> <p>Jeśli kamera alarmowa i rejestracyjna (2a) zostały skonfigurowane, można też wyświetlać obrazy wideo do komunikatów alarmowych z odpowiedniego wejścia. Można utworzyć kopie lokalne (6) tych obrazów i wyświetlać je za pomocą odtwarzacza Video Player (8).</p>

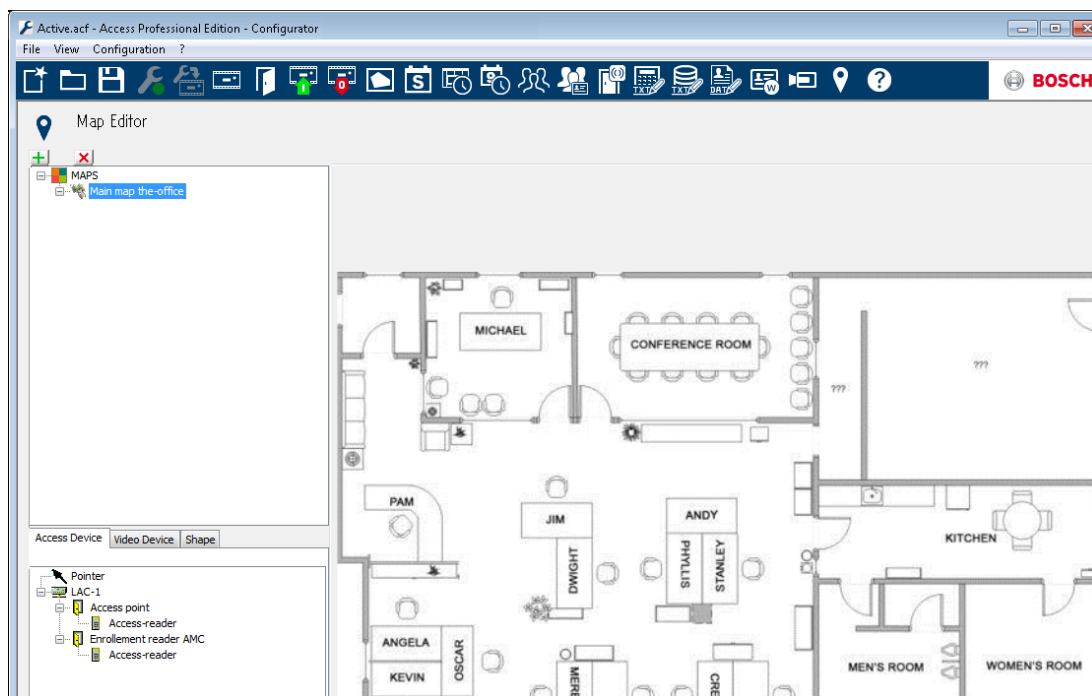


16 Konfigurowanie mapy

Uruchom Edytor map



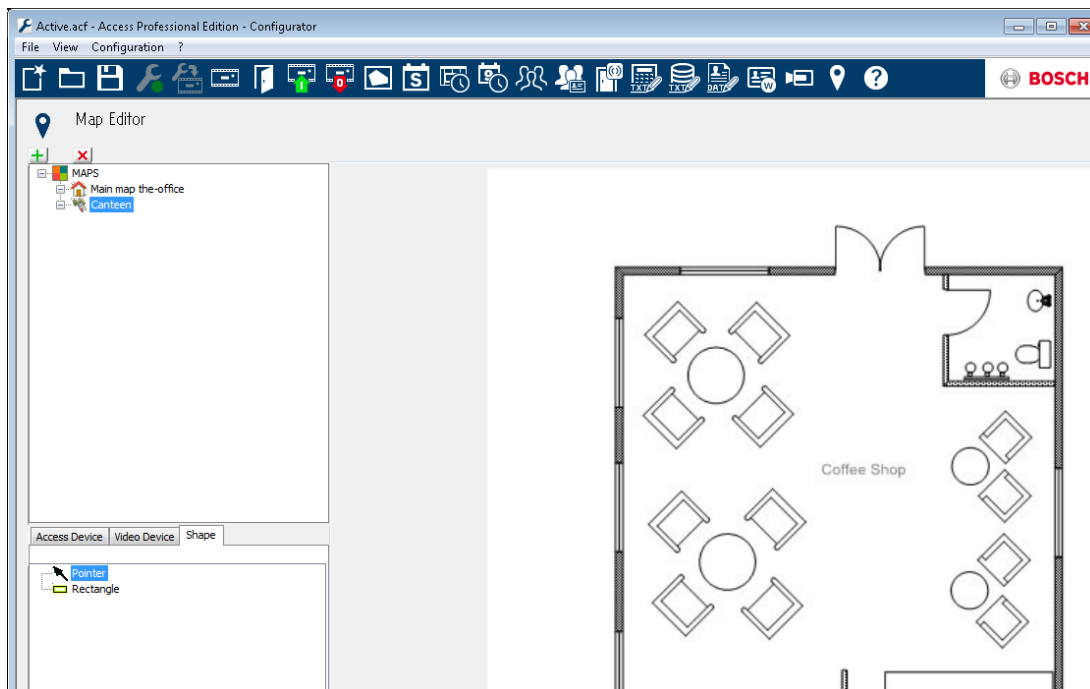
Aby dodać mapę, kliknij przycisk  .



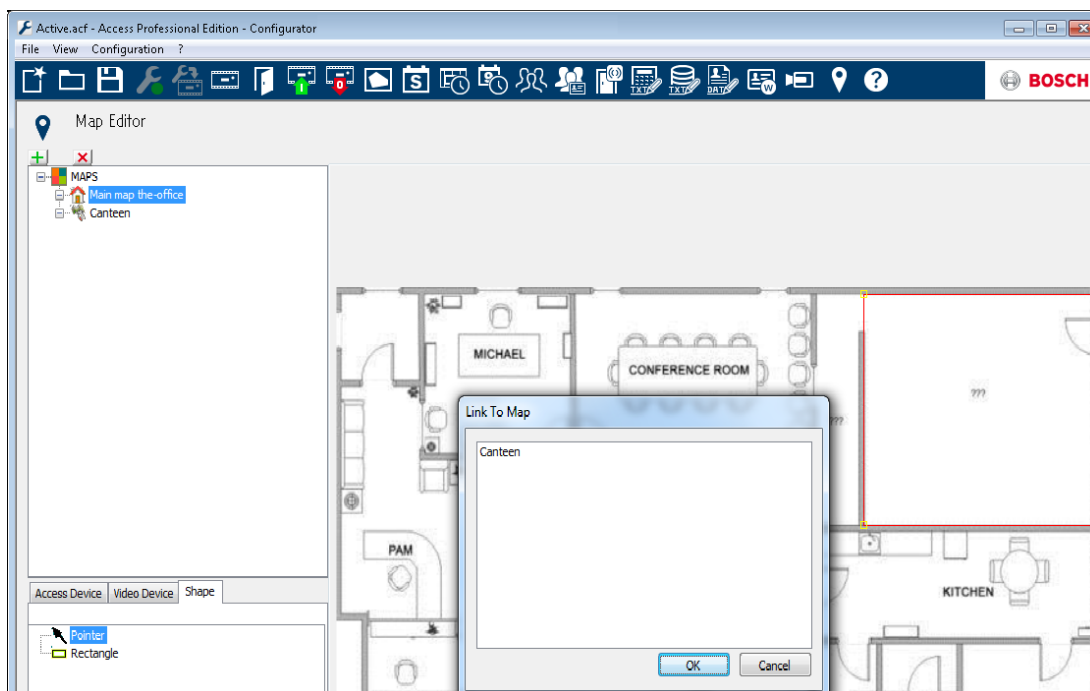
Mapa będzie wyświetlana w oknie dialogowym

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

Dodaj do drzewa map widok szczegółowy np. widok stołówki.



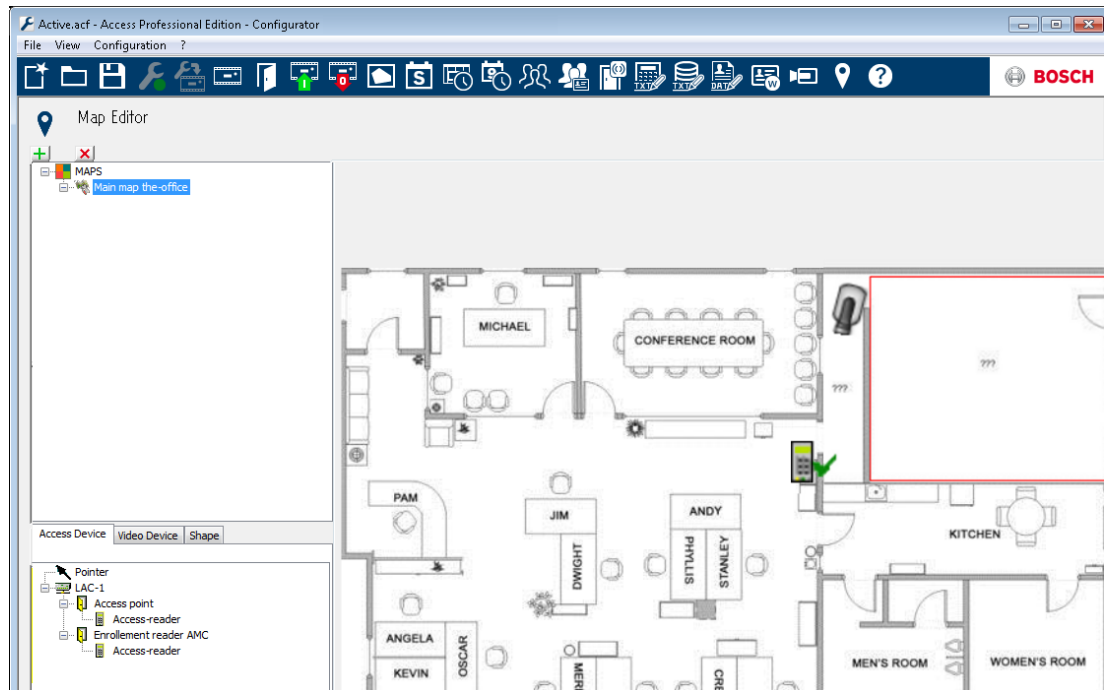
- Aby połączyć nową **Mapę stołówki** z mapą główną, należy przejść do zakładki **Kształt** i wybrać pozycję **Prostokąt**.
- Umieścić prostokąt nad obszarem mapy, który ma być wyświetlany jako widok szczegółowy (w przykładzie poniżej pokazany jako czerwony prostokąt).
- Wybierz na wyświetlaczu **Łącze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



17 Dodawanie urządzenia do mapy

Wybierz kartę **Device** (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
	Drzwi
	Czytnik
	Kamera

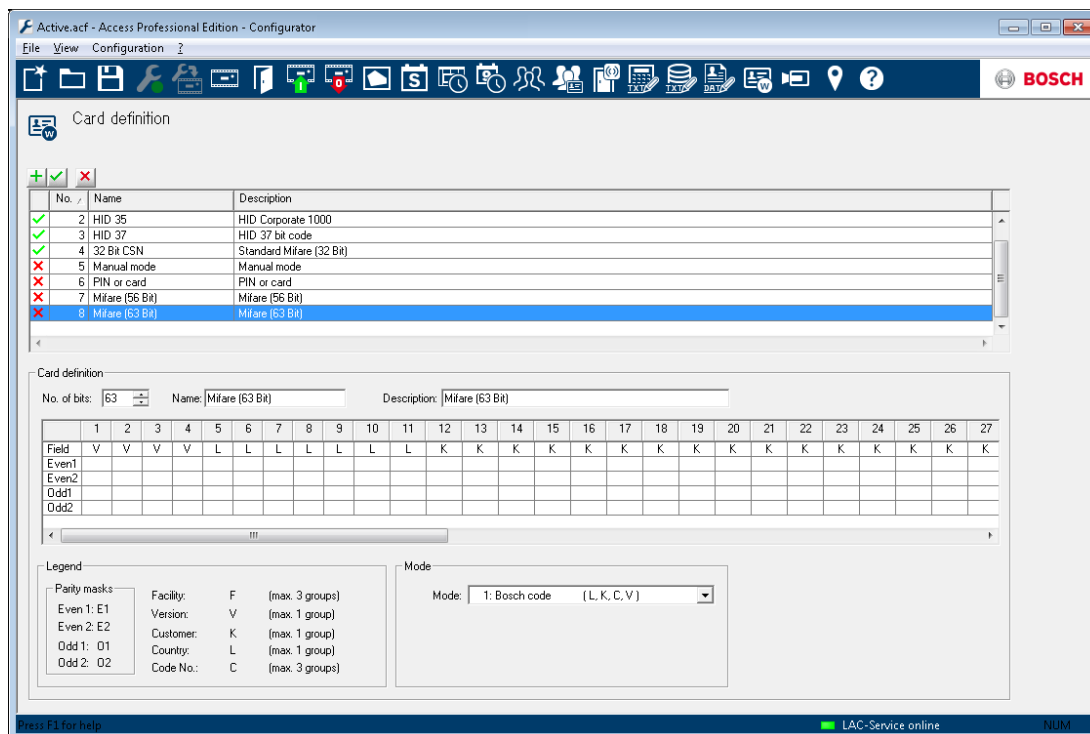
Typy urządzeń	Alarmy
Access Point (Entrance) (Punkt dostępu (przejście))	
	Drzwi otwarte bez autoryzacji
	Drzwi otwarte zbyt długo
	(Wszystkie alarmy czytników są takie same, jak alarmy wejść*)
Reader (Czytnik)	Błąd czytnika

Typy urządzeń	Alarmy
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). Dwukrotne kliknięcie w drugiej kolumnie spowoduje uaktywnienie alarmu.

18 Definicja karty

W tym oknie można określić, jakie dane ma przekazywać czytnik, aby również w późniejszym czasie 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 **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).



Uwaga!

Należy upewnić się, że aktywne są tylko 4 typy kart, ponieważ maksymalna liczba prawidłowych typów kart to 4.

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	Sprawdzane 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?).

19 Konfigurowanie alertów zagrożenia

Wstęp

Zagrożenie jest to sytuacja krytyczna, która wymaga natychmiastowej i równoczesnej reakcji na niektórych lub wszystkich wejściach w systemie kontroli dostępu.

Threat alert (Alert zagrożenia) to alarm w reakcji na zagrożenie. Zależnie od ustawień wejść w aplikacji Access PE Configurator są możliwe różne sposoby reagowania na alerty zagrożenia. Odpowiednio uprawnione osoby mogą dokonywać alertu zagrożenia z jedną akcją, np. za pośrednictwem interfejsu użytkownika aplikacji Access PE, naciskając przycisk lub przedstawiając specjalną kartę identyfikacyjną przed dowolnym czytnikiem.



Uwaga!

Należy zawsze przestrzegać lokalnych przepisów bezpieczeństwa dotyczących wejść w sytuacjach awaryjnych.

Dla wejść jest zwykle przewidziany bezpieczny tryb awaryjny.

19.1 Konfigurowanie sprzętu do obsługi alarmów zagrożenia

Przegląd

- Przypisz sygnał wejściowy AMC w celu propagacji alertów zagrożenia
- Zdefiniuj odpowiedź poszczególnych wejść na alarm zagrożenia

Przypisywanie sygnału wejściowego do alertów zagrożenia

1. W aplikacji Access PE Configurator wybierz **Input signals** (Sygnały wejściowe).
2. W wierszu odpowiadającym pożądanemu sygnałowi wejściowemu kliknij dwukrotnie kolumnę **Threat alert** (Alarm zagrożenia) lub zaznacz pole wyboru **Activate threat alert** (Aktywuj alert zagrożenia).

W komórce pojawi się ikona głośnika.



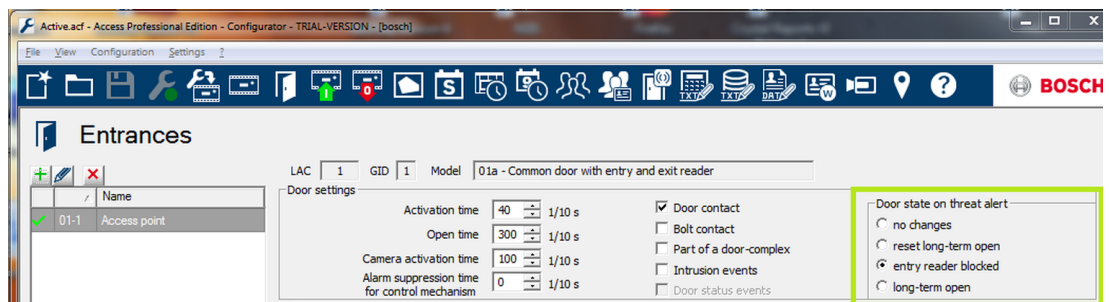
Board	Signal	Signal Name	Message	.. in time model	R serial	R par.	Threat alert
0	1	Signal 0-1			
0	2	Signal 0-2			
0	3	Signal 0-3			
0	4	Signal 0-4			
0	5	Signal 0-5			
0	6	Signal 0-6			
0	7	Signal 0-7			
0	8	Signal 0-8			

Definiowanie odpowiedzi wejść na alert zagrożenia

1. W aplikacji Access PE Configurator wybierz **Entrances** (Wejścia).
2. Na liście wejść wybierz wejście, które ma reagować na alerty o zagrożeniu



3. Ustaw parametr **Door state on threat alert** (Stan drzwi w momencie alertu zagrożenia) w jeden z następujących sposobów:
 - **no changes:** (bez zmian) wejście nie może zmieniać stanu w odpowiedzi na alert zagrożenia.
 - **reset long-term open:** (resetuj otwarcie długoterminowe) kończy okres nieblokowanego wejścia i drzwi zaczynają pracować w normalnym trybie. Oznacza to, że drzwi będą teraz odblokowane tylko w przypadku prawidłowego uwierzytelnienia.
 - **door blocked:** (drzwi zablokowane) drzwi są zablokowane i zabezpieczone. Tryb normalny jest zawieszony.
 - **long-term open:** (otwarcie długoterminowe) drzwi są odblokowane i dopuszczają dostęp niekontrolowany.
4. Powtórz tę procedurę dla wszystkich wejść, które reagują na alerty zagrożenia.



Należy pamiętać, że skutki alertu związanego z zagrożeniem pozostają trwałe, do czasu, aż alert o zagrożeniu zostanie wyraźnie cofnięty za pośrednictwem interfejsu użytkownika w systemie kontroli dostępu. Informacje na ten temat można znaleźć w pomocy online aplikacji APE Personal Management, sekcja: **Using the Set/Deactivate Threat Alert buttons** (Używanie przycisków Ustaw/Dezaktywuj alert zagrożenia).

Uwaga!

Drzwi zablokowane (zabezpieczone)

Po dezaktywowaniu alertu przyciskiem **Deactivate Threat Alert** (Dezaktywuj alert zagrożenia) drzwi, które zostały jawnie ustawione w stan **drzwi zablokowane** (zabezpieczone) pozostaną nadal zabezpieczone. W celu uniknięcia dodatkowych naruszeń zabezpieczeń po wystąpieniu alertów o zagrożeniu, konieczne jest jawne dezaktywowanie stanu zabezpieczenia drzwi.

Ścieżka dostępu:

ekran główny aplikacji Personnel Management > drzewo **Device states** (Stany drzwi) >

kliknij w menu kontekstowym prawym przyciskiem myszy zabezpieczone wejście (oznaczone za pomocą kłódki).



20

20.1

Dodatek

Sygnaly

Lista dostępnych sygnałów wejściowych i wyjściowych.

Sygnaly 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	Sygnal sabotażu z kontrolera zewnętrznego.
Bramka obrotowa w pozycji normalnej	Bramka obrotowa jest zamknięta.
Przejście zakończone	Przejście zostało z powodzeniem zakończone. Jest to impuls z kontrolera zewnętrznego.
System sygnalizacji włamania gotowy do uzbrojenia	Zostanie użyty przez system sygnalizacji włamania, jeśli wszystkie czujki znajdują się w spoczynku i system może zostać uzbrojony.
System sygnalizacji włamania jest uzbrojony	System sygnalizacji włamania jest uzbrojony.
Przycisk żądania uzbrojenia systemu sygnalizacji włamania	Przycisk uzbrajania systemu sygnalizacji włamania.
Włączenie otwarcia lokalnego	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 służby	Zamyka drzwi z przeciwnej strony służby. 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.
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.

20.2 Domyślne modele drzwi

Standardowe modele drzwi

Dostępne są następujące domyślne modele drzwi:

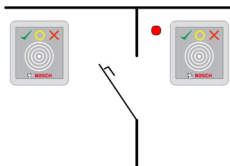
01a Pojedyncze drzwi z czytnikiem wejścia i wyjścia

- 01b Pojedyncze drzwi z czytnikiem wejścia i przyciskiem otwierania drzwi
- 01c Pojedyncze drzwi z czytnikiem wejścia
- 01r Jeden czytnik wyłącznie w celu rejestracji osób w miejscu zbiórki, na przykład w przypadku ewakuacji. Brak blokad fizycznych, żadne sygnały nie będą generowane.
- 03b Kontrolowana bramka obrotowa z czytnikiem wejścia i przyciskiem otwierania
- 03c Kontrolowana bramka obrotowa z czytnikiem wejścia
- 06c Rejestracja przez AMC – brak kontroli wejść!
- 07a Winda obsługująca maksymalnie 16 pięter
- 07b Winda obsługująca maksymalnie 16 pięter
- 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

20.3 Model drzwi 01

Drzwi pojedyncze



Sygnały:

Sygnały wejściowe	Sygnały wyjściowe
Czujnik drzwi	Automat do otwierania drzwi
Przycisk otwierania drzwi: drzwi otwarte	Śluza: blokada przeciwnych drzwi
Czujnik rygla	Wyciszenie alarmu
Wejście zablokowane	Aktywacja kamery
Sygnał sabotażu	Drzwi są otwarte zbyt długo
Włączenie otwarcia lokalnego	

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
- 01r Jeden czytnik wyłącznie w celu rejestracji osób w miejscu zbiórki, na przykład w przypadku ewakuacji. W tym modelu drzwi brak jest blokad fizycznych, żadne sygnały nie będą generowane.

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.

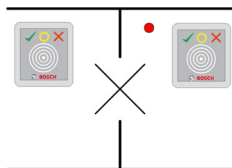
Istnieje możliwość dołączenia dodatkowych czytników kart identyfikacyjnych. Dzięki zastosowaniu drugich drzwi z funkcją blokowania można stworzyć służę pozwalającą na zabezpieczenie wejścia/wyjścia personelu. Jest to korzystne w przypadku przejazdów dla samochodów, zalecany jest jednak montaż dodatkowego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

**Uwaga!**

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

20.4 Model drzwi 03

Kontrolowana bramka obrotowa



Sygnały:

Sygnały wejściowe	Sygnały 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	Śluza: blokada przeciwnych drzwi
Sygnal 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:

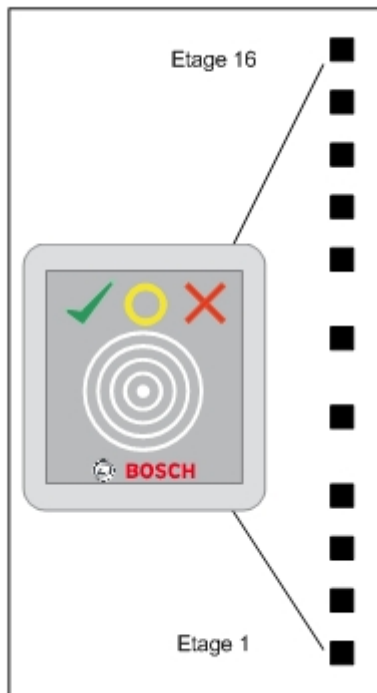
Zablokowanie śluzy jest możliwe tylko wtedy, gdy drzwi są skonfigurowane jako część śluzy. Jeśli drzwi nie są częścią śluzy, sygnał wejściowy 03 jest interpretowany jako blokada czytnika. W takim przypadku w chwili pojawienia się sygnału wejściowego 03 czytnik zostaje zablokowany.

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

20.5 Model drzwi 06c

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

20.6 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)

Sygnaly wejścia modelu 07a:

Sygnaly wejściowe	Sygnaly 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.

Sygnaly wejścia modelu 07b:

Sygnaly wejściowe	Sygnaly 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:

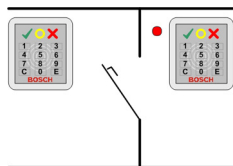
Najpierw posiadacz karty przywołuje windę. Może tego dokonać za pośrednictwem przycisku windy lub za pośrednictwem czytnika kart (np. model drzwi 01c).

W windzie posiadacz karty przesuwają 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.

20.7

Model drzwi 10

Pojedyncze drzwi z funkcją uzbrojenia/rozbrojenia systemu 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 (włamania)
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:

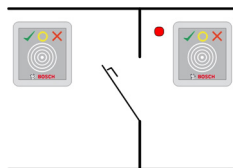
Za pomocą przycisku **E** na czytniku wejścia można uzbroić system sygnalizacji włamania. W tym przypadku niezbędna jest również karta z uprawnieniami oraz wprowadzenie kodu PIN. Rozbrojenie systemu sygnalizacji włamania następuje po pierwszym uprawnionym wejściu, przy czym w takim wypadku też konieczna 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.

20.8

Model drzwi 14

Drzwi ze sterowaniem systemem 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:

- 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

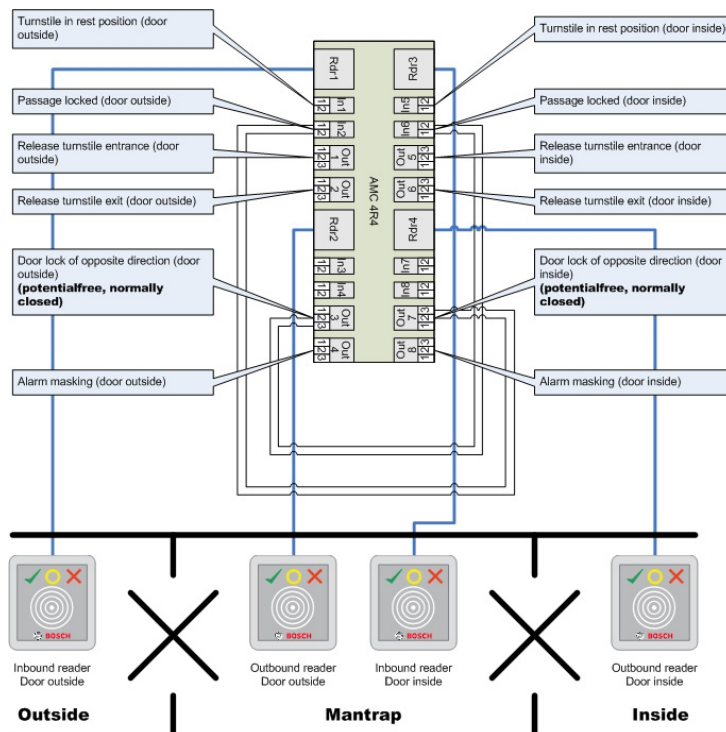
Zbliżenie identyfikatora z uprawnieniami spowoduje uzbrojenie systemu sygnalizacji włamania. Rozbrojenie następuje w wyniku naciśnięcia przycisku i zbliżenia identyfikatora z uprawnieniami.

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

20.9 Przykłady konfiguracji śluz 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 śluzi osobowej z dwoma bramkami obrotowymi (DM 03a)



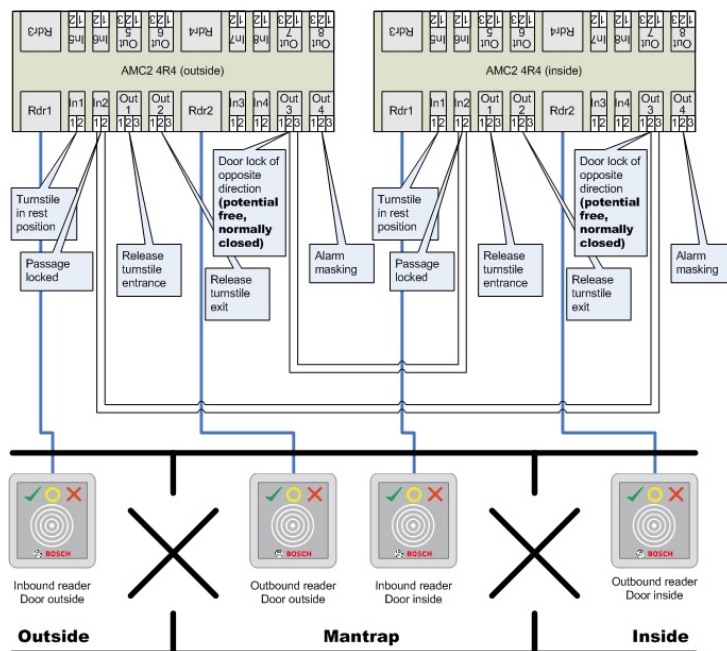
Połączenia do blokady drzwi dla kierunku przeciwnego zapewniają, że w danym momencie można otworzyć tylko jedną bramkę obrotową.



Uwaga!

Sygnal wyjściowy (Out 3 (Wyjście 3)) powinien zostać ustawiony jako beznapięciowy (tryb suchy). Sygnal „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.

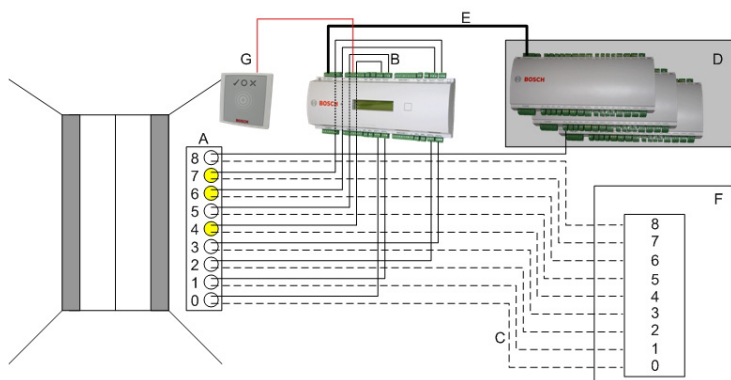


Uwaga!

Sygnal wyjściowy (Out 3 (Wyjście 3)) powinien zostać ustawiony jako beznapięciowy (tryb suchy). Sygnal „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).

20.10 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

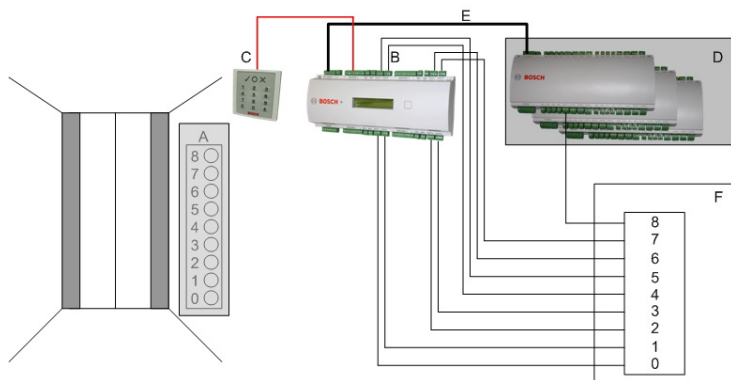
D = Można przyłączyć moduł rozszerzeń WE/WY (AMC2 8I-8O-EXT, AMC2 16I-EXT lub AMC2 16I-16O-EXT)

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)



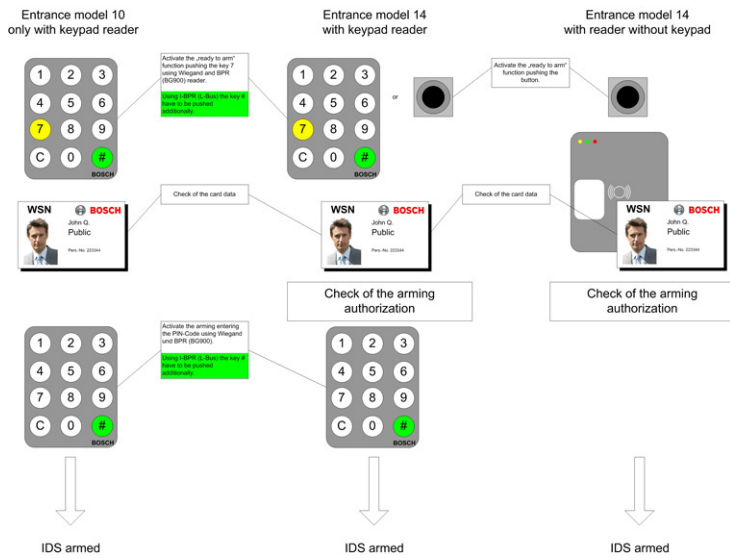
Uwaga!

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.

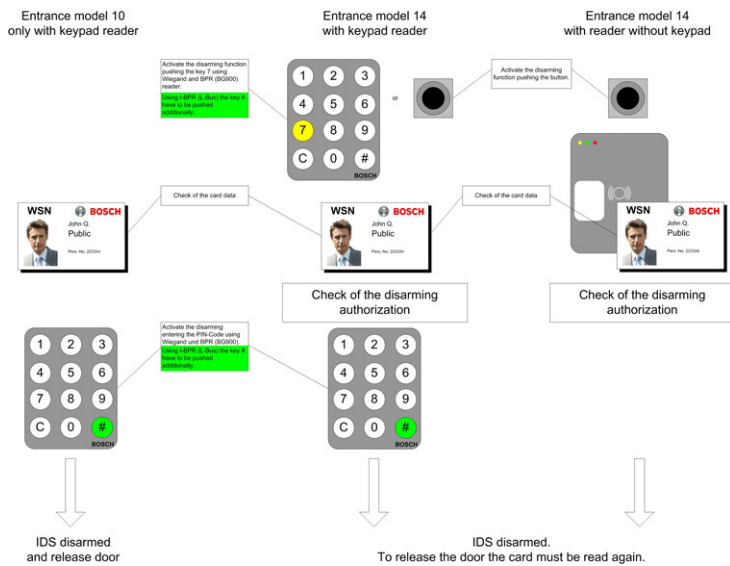
20.11

Instrukcje dotyczące uzbrajania/rozbrajania

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



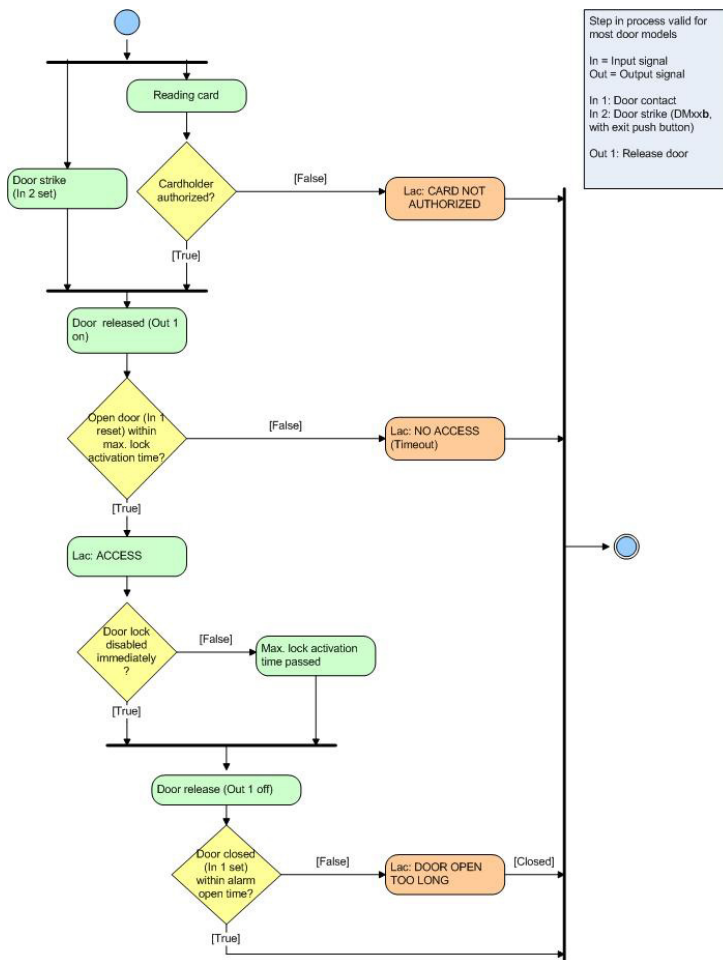
Porównanie **rozbrajania** systemu alarmowego na wejściu (drzwiach) w modelach 10 i 14.



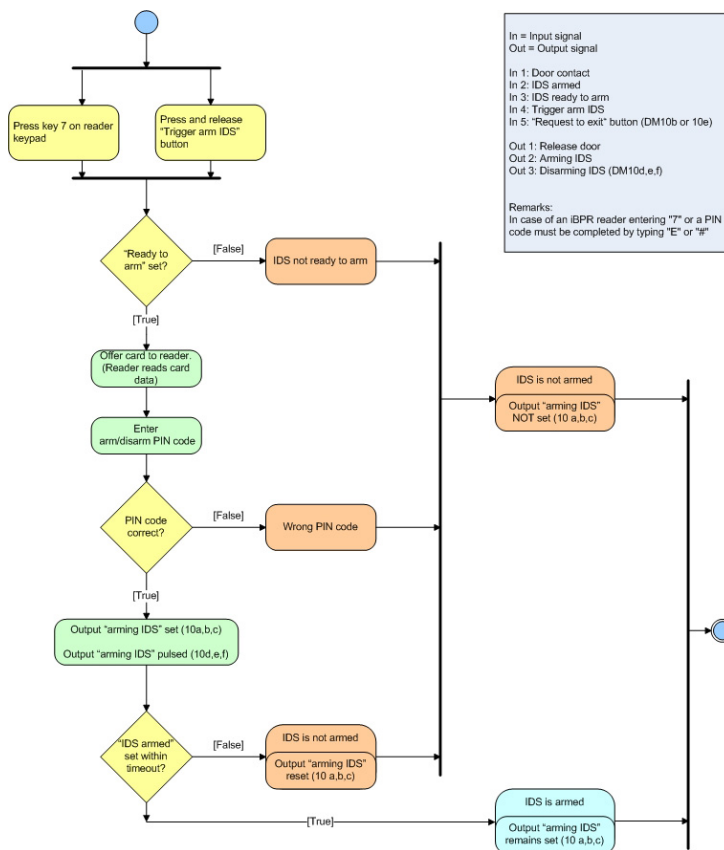
20.12 Procedury kontroli dostępu

Schematy procedur kontroli dostępu

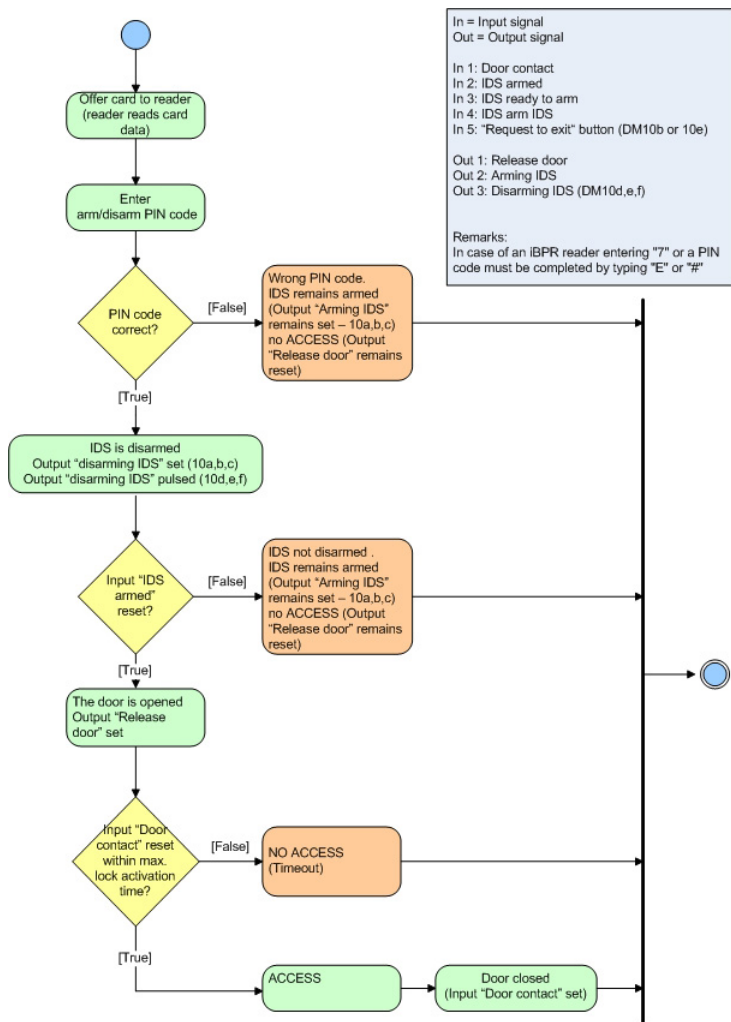
Model drzwi DM01



Model drzwi DM10 - uzbrajanie



Model drzwi DM10 - rozbrajanie



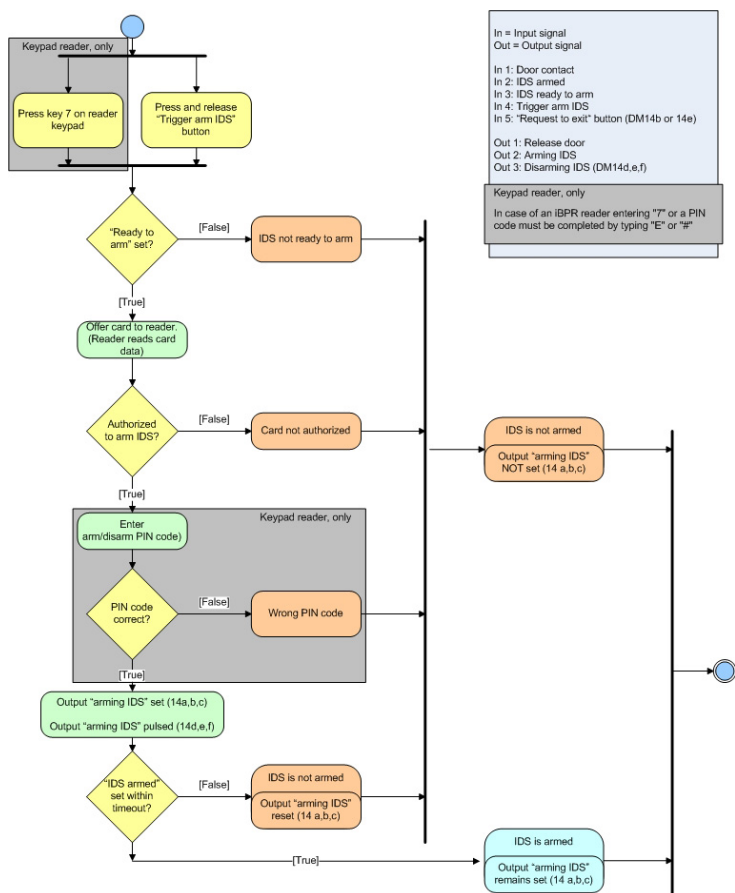
In = Input signal
Out = Output signal

In 1: Door contact
In 2: IDS armed
In 3: IDS ready to arm
In 4: IDS arm IDS
In 5: "Request to exit" button (DM10b or 10e)

Out 1: Release door
Out 2: Arming IDS
Out 3: Disarming IDS (DM10d,e,f)

Remarks:
In case of an IBPR reader entering "7" or a PIN code must be completed by typing "E" or "#"

Model drzwi DM14 - uzbrajanie



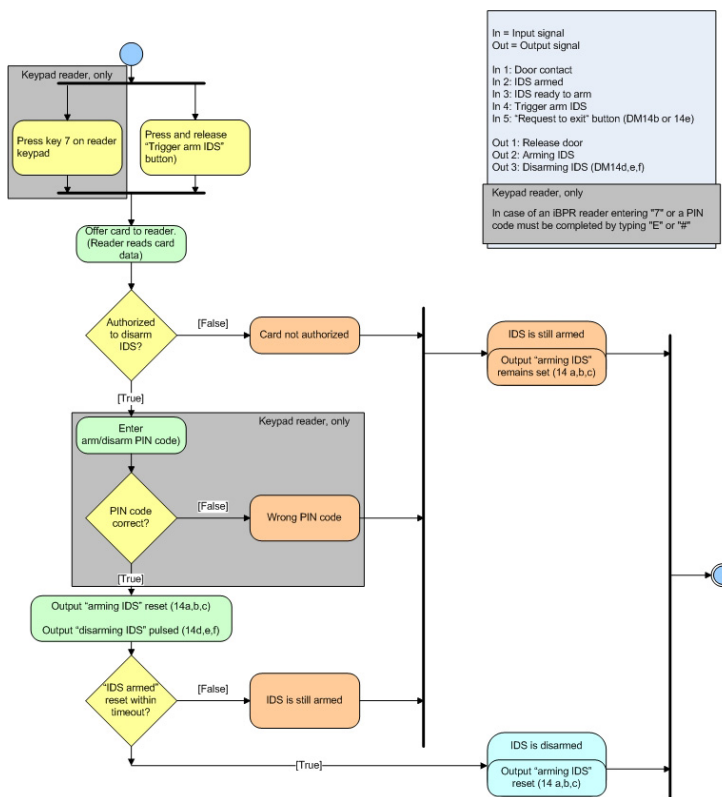
In = Input signal
Out = Output signal

In 1: Door contact
In 2: IDS armed
In 3: IDS ready to arm
In 4: Trigger arm IDS
In 5: "Request to exit" button (DM14b or 14e)

Out 1: Release door
Out 2: Arming IDS
Out 3: Disarming IDS (DM14d,e,f)

Keypad reader, only
In case of an IBPR reader entering "7" or a PIN code must be completed by typing "E" or "#".

Model drzwi DM14 - rozbrajanie



20.13

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

21 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 (blokady, 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.

22

Wymagania normy UL 294

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

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

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



Bosch Security Systems B.V.

Torenallee 49
5617 BA Eindhoven
Netherlands

www.boschsecurity.com

© Bosch Security Systems B.V., 2019