Access Professional Edition

Video Verification

BOSCH

pl Operation Manual

Spis treści

1 Przegląd

2 Informacje ogólne

2.1 Logowanie użytkownika

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

Zarządzanie personelem

Konfigurator

Analiza dziennika

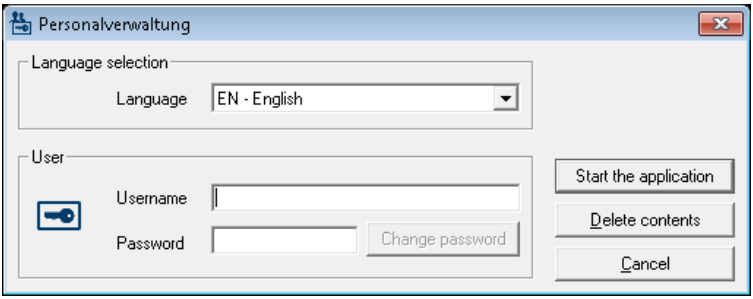
Zarządzanie mapami i alarmami

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”.

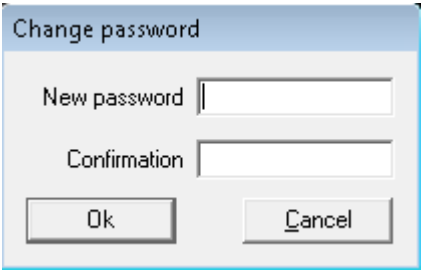
Na górnej liście rozwijanej można wybrać odpowiedni **język**. Domyślnie stosowany jest język wybrany podczas instalowania aplikacji. W przypadku zmiany użytkownika bez restartowania aplikacji zachowany zostanie ostatnio używany język. Z tego powodu okno logowania może się wyświetlić się w nieprawidłowym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

Aplikacje systemu Access PE można uruchomiać 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:



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!).

3 Video Verification (Weryfikacja wideo)

Weryfikacja wideo służy do sprawdzania, czy osoba żądająca dostępu rzeczywiście jest właścicielem karty. W tym celu należy sprawdzić dane karty i uprawnień.

Uwaga!
Jeśli funkcja weryfikacji wideo zostanie uaktywniona w przypadku co najmniej jednego wejścia (PE Configurator > Entrances > Select the entrance you want to edit > Video configuration (Konfigurator PE > Wejścia > Wybierz wejście, które chcesz edytować > Konfiguracja wideo)), należy też otworzyć okno dialogowe weryfikacji wideo na co najmniej jednej stacji roboczej. W przeciwnym razie **wszystkie** żądania dostępu zostaną odrzucone.

Po zainstalowaniu systemu wizyjnego w aplikacji Personnel Management (Zarządzanie personelem) aktywne są dodatkowe funkcje, które zwiększają użyteczność i wszechstronność systemu wizyjnego.

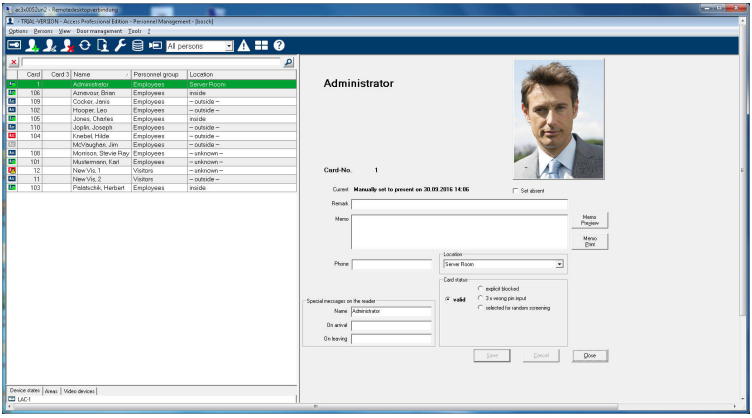
Więcej informacji

– *Weryfikacja wideo, Strona 9*

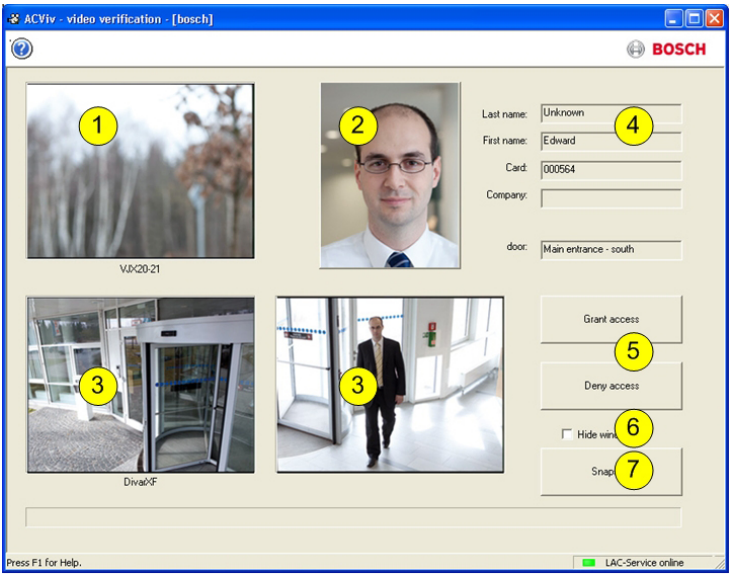
3.1 Weryfikacja wideo

Opis okien dialogowych

Aplikację należy uruchomić, klikając przycisk  w oknie dialogowym Personnel Management (Zarządzanie personelem).



Jeśli nie będzie aktualnie żadnych żądań dostępu, okno dialogowe wyświetli stronę domyślną. Gdy uprawniona osoba skanuje swoją kartę przy wejściu, okno dialogowe przełącza się na widoki obrazów pochodzących z odpowiednich kamer.
Jeśli użytkownik stacji roboczej jest w danym momencie zajęty innymi czynnościami, każde żądanie dostępu spowoduje wyświetlenie okna dialogowego weryfikacji wideo na pierwszym planie.



1 =	**Kamera identyfikacyjna** – przesyła obraz na żywo osoby żądającej dostępu.
2 =	**Obraz z bazy danych** – zdjęcie z archiwum jest wyświetlane w celu porównania go z obrazem na żywo.
3 =	**Kamery nadzorujące** – najpierw przedstawiony jest widok z kamery pokazującej strefę tylną, a następnie, po odblokowaniu drzwi, ekran przełącza się do widoku z kamery monitorującej strefę przednią.
4 =	**Dane osobowe** – wyświetlenie danych odpowiadających zeskanowanemu numerowi karty, przechowywanych w bazie danych.
5 =	**Grant access** (Zezwolenie na dostęp)/**Deny access** (Odmowa dostępu) – przyciski zwalniania lub blokowania konkretnych drzwi.

6 =	**Hide window** (Ukryj okno) – zamyka okno dialogowe po pomyślnym zakończeniu weryfikacji wideo, aby ponownie wyświetlić je na pierwszym planie w przypadku kolejnego żądania dostępu.
7 =	**Snapshot** (Pojedyncze ujęcie) – obrazy zatrzymane pochodzące ze wszystkich trzech widoków z kamer są przechowywane w pamięci lokalnej.

Wymagania

Aby można było przeprowadzić kontrolę polegającą na porównywaniu obrazu na żywo ze zdjęciem z archiwum, muszą zostać spełnione następujące warunki.

- Zdjęcia posiadacza karty są przechowywane w bazie danych.
- Kamera jest zainstalowana w taki sposób, że pokazuje twarz osoby żądającej dostępu.
- Maksymalnie dwie kamery obserwujące obszar znajdujący się za osobą żądającą dostępu – opcjonalnie.
- Maksymalnie dwie kamery rejestrujące obraz w samym przejściu – opcjonalnie.
- Door configuration (Konfiguracja drzwi)
  - Zaznacz jako **Entrance with video verification** (Wejście z funkcją weryfikacji wideo).
  - Ustaw funkcję weryfikacji wideo na **Active** (Aktywna).
  - Wybierz urządzenie, które będzie pełniło funkcję kamery identyfikacyjnej (**Identification camera**).
  - Opcjonalnie – inne kamery do monitoringu strefy tylnej lub przedniej.
- Co najmniej jedna stacja robocza ze stałą obsługą przez personel, na której jest zainstalowana i uruchomiona aplikacja **Video Verification** (Weryfikacja wideo).
  Może ona działać na kilku stacjach roboczych jednocześnie. Napływające żądania dostępu są jednak przesyłane tylko do jednej stacji roboczej, aby uniknąć podwójnej czy nawet sprzecznej procedury.

Procedura dostępu w przypadku osoby uprawnionej

1. Osoba skanuje kartę
   - Sprawdzenie danych karty
   - Sprawdzenie uprawnień
2. Połączenie z aplikacji Video Verification (Weryfikacja wideo)
   Jeśli dostępne i skonfigurowane:
   - Na górze po lewej stronie: obraz na żywo z kamery identyfikacyjnej
   - Obok, po prawej stronie: zdjęcie posiadacza karty przechowywane w archiwum
   - Obok, po prawej stronie: dane posiadacza karty – nazwisko, imię, numer karty, nazwa firmy wraz z nazwą wejścia, przy którym czeka dana osoba
   - Na dole, po lewej stronie: obraz na żywo pochodzący z pierwszej kamery nadzorującej tylną strefę
   - Obok, po prawej stronie: obraz na żywo pochodzący z drugiej kamery nadzorującej tylną strefę
3. Użytkownik stacji roboczej:
   - upewnia się, czy obraz na żywo jest zgodny ze zdjęciem z archiwum, i sprawdza zapis z kamer nadzorujących;
   - zezwala/nie zezwala na dostęp w zależności od wyniku porównania i czynności kontrolnych.
4. Aplikacja Video Verification (Weryfikacja wideo)
   - Kiedy drzwi zostają odblokowane, dwa dolne okna kamer nadzorujących przełączają się do wyświetlania obrazu z kamer monitorujących strefę przednią. Ten obraz pozostaje na ekranie do czasu zamknięcia drzwi.

Uwaga!

W pamięci lokalnej można zawsze przechowywać dowolną liczbę obrazów zatrzymanych z wyświetlanych przez kamery obrazów. Naciśnięcie przycisku **Snapshot** (Pojedyncze ujęcie) spowoduje zapisanie obrazu z każdego strumienia wideo.

Uaktywnienie okna dialogowego
Po wyświetleniu okna dialogowego Video verification (Weryfikacja wideo) przełącza się ono na obraz domyślny. Kiedy okno znajduje się w tym stanie, nie można edytować danych ani przeprowadzać żadnych procedur. Kiedy **upoważniona** osoba żąda dostępu przy wejściu, które jest **skonfigurowane** i **aktywowane** do weryfikacji wideo, wówczas ekran pokazuje obrazy z zainstalowanych kamer i odpowiednie dane z bazy danych.
Jeśli w chwili przedstawienia żądania dostępu na stacji roboczej używane były inne aplikacje, co spowodowało ustawienie okna dialogowego w tle, to w tym momencie okno zostaje automatycznie wysunięte na pierwszy plan.
Po zakończeniu procedury związanej z żądaniem dostępu widok okna ponownie przełącza się na domyślny obraz, ale pozostaje na pierwszym planie.
Jeśli praca z takimi ustawieniami nie odpowiada użytkownikowi, może wybrać opcję **Hide window** (Ukryj okno), która po zakończeniu każdego procesu weryfikacji automatycznie zminimalizuje okno dialogowe (do postaci ikony na pasku zadań). Opcja ta powoduje też wysunięcie okna dialogowego na pierwszy plan za każdym razem, gdy pojawi się nowe żądanie dostępu.

3.1.1 Włączanie/wyłączanie weryfikacji wideo

W menu kontekstowym wejść/czytników [na liście stanu urządzeń] również znajduje się funkcja **Deactivate video verification** (Wyłącz weryfikację wideo).
Umożliwia to np. tymczasowe skrócenie procesu żądania dostępu lub, przeciwnie, szybkie aktywowanie weryfikacji wideo bez potrzeby zmian w konfiguracji.
Po wyłączeniu weryfikacji wideo odpowiednia pozycja w menu kontekstowym jest oznaczana haczykiem.

Funkcja jest dostępna wyłącznie dla wejść, dla których weryfikacja wideo została aktywowana w danych konfiguracji. Aktywacja/dezaktywacja jest sterowana przez usługę LAC. Rozdziela ona informacje do wszystkich stacji roboczych, co umożliwia modyfikację ustawień z dowolnej z nich.

4 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 Access Systems GmbH
Charlottenburger Allee 50
52068 Aachen
Germany
www.boschsecurity.com