Credential Management V5.5

Z Mobile Access

pl Instrukcja obsługi

Spis treści

1 Bezpieczeństwo

Użyj najnowszego oprogramowania

Przed pierwszym uruchomieniem urządzenia upewnij się, że zainstalowano najnowszą i właściwą wersję oprogramowania. Aby zapewnić spójną funkcjonalność, zgodność, wydajność i bezpieczeństwo, należy regularnie aktualizować oprogramowanie przez cały okres eksploatacji urządzenia. Postępuj zgodnie z instrukcjami dotyczącymi aktualizacji oprogramowania zawartymi w dokumentacji produktu.

Więcej informacji można znaleźć na stronach poniżej:

– Informacje ogólne: https://www.boschsecurity.com/xc/en/support/product-security/
– Zalecenia dotyczące bezpieczeństwa, czyli lista zidentyfikowanych luk i proponowanych rozwiązań: https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

Firma Bosch nie ponosi żadnej odpowiedzialności za jakiekolwiek szkody spowodowane korzystaniem z jej produktów w połączeniu z nieaktualnym oprogramowaniem.

2 Wstęp

2.1 Informacje o narzędziach Credential and Visitor Management

Oprogramowanie Credential Management, zwane dalej CredMgmt, to narzędzie obsługiwane przez przeglądarkę internetową, które współpracuje z systemami kontroli dostępu (ACS) firmy Bosch. Dzięki prostemu i intuicyjnemu interfejsowi użytkownika oprogramowanie umożliwia nawet stosunkowo niedoświadczonym operatorom zarządzanie uprawnieniami dostępu pracowników i personelu zewnętrznego. Same poświadczenia mogą mieć postać kart fizycznych lub poświadczeń mobilnych.

Zarządzanie poświadczeniami

Za pomocą programu CredMgmt operatorzy ACS mogą zarządzać zarówno poświadczeniami, jak i rekordami pracowników, do których te poświadczenia należą.

Jednostka	Dodawanie	Zmiana	Usuń	Przypisywanie/ Cofanie przypisania
Poświadczenia w formie fizycznej				Tak
Wirtualne poświadczenia „mobilne” (jeśli zainstalowany jest program Mobile Access)	Tak		Tak	Tak
Uprawnienia				Tak
Dokumentacja posiadacza karty	Tak	Tak	Tak	

Visitor Management

Program VisMgmt pozwala operatorom ACS zarządzać poświadczeniami, rejestrami gości i rejestrami wizyt.

Jednostka	Dodawanie	Zmiana	Usuń	Przypisywanie/ Cofanie przypisania
Poświadczenia w formie fizycznej				Tak
Wirtualne poświadczenia „mobilne” (jeśli zainstalowany jest program Mobile Access)	Tak			Tak
Rejestry gości	Tak	Tak	Tak	
Rejestry wizyt	Tak	Tak	Tak	

2.2 Informacje o oprogramowaniu Mobile Access

Mobile Access to aplikacja do kontroli dostępu osób za pomocą wirtualnych poświadczeń przechowywanych na urządzeniu mobilnym, takim jak smartfon danej osoby. Wirtualne poświadczenia są przechowywane w podstawowym systemie kontroli dostępu (ang. Access Control System, ACS).

- Operatorzy ACS generują, przypisują i wysyłają wirtualne poświadczenia do osób za pośrednictwem aplikacji internetowej typu plug-in.
- Posiadacze mobilnych poświadczeń używają czytników kontroli dostępu przez Bluetooth, za pomocą aplikacji Mobile Access na urządzeniach mobilnych.
- Instalatorzy systemów Mobile Access konfigurują czytniki kontroli dostępu przez Bluetooth za pomocą specjalnej aplikacji na urządzeniach mobilnych.
- System nie przechowuje na urządzeniach mobilnych żadnych danych osobowych.

3 Instalowanie i odinstalowywanie

3.1 Wymagania wstępne dotyczące oprogramowania

Serwer CredMgmt należy zainstalować na tym samym komputerze, co główny system kontroli dostępu (ACS). Obowiązują te same wymagania programowe i sprzętowe.
Jeśli podstawowy system kontroli dostępu nie jest jeszcze zainstalowany, pamiętaj o przygotowaniu go przed instalacją Credential Management.
W przypadku pierwszej instalacji lub aktualizacji kolejność instalacji powinna być następująca:

1. Główny system kontroli dostępu — Access Management System.
2. Credential Management i/lub Visitor Management.
3. Mobile Access.

Programy konfiguracyjne CredMgmt i Mobile Access posiadają własne nośniki instalacyjne, oddzielne od ACS. Można je pobrać z internetowych katalogów produktów firmy Bosch.

Uwaga!
Konieczność posiadania stabilnego certyfikatu głównego
Przed przystąpieniem do poniższych instalacji należy upewnić się, że instalacja systemu ACS jest kompletna i ma wszystkie licencje. Obejmuje to ostateczną decyzję o certyfikacie głównym serwera ACS (czy jest samopodpisany, czy oparty na CA) oraz potwierdzenie jego stabilnego wdrożenia. Późniejsze zmiany w certyfikacie głównym serwera ACS będą wymagać ponownej konfiguracji certyfikatów na wszystkich komputerach i czytnikach dostępu mobilnego należących do danego systemu kontroli dostępu.

Wymagania dotyczące serwera
Serwer to komputer, na którym działa system ACS i aplikacja CredMgmt.

Systemy operacyjne	– Windows 11 Professional i Enterprise 23H2; – Windows Server 2019 (Version 1809) (64bit, Standard, Datacenter); – Windows Server 2022 (64-bitowy, Standard, Datacenter)
Systemy zarządzania bazami danych	– MS SQL Server 2019 and later Należy zawsze używać tego samego wystąpienia bazy danych jak w przypadku systemu ACS (głównego systemu kontroli dostępu)
Minimalna rozdzielczość monitora	Full HD 1920x1080
Obsługiwane przeglądarki	Google Chrome, Mozilla Firefox, Microsoft Edge (na bazie Chromium) Należy użyć najnowszej wersji przeglądarki przeznaczonej do systemu operacyjnego Windows.

Wymagania dotyczące urządzeń klienckich

Wymagania	**Opis**
Minimalna rozdzielczość monitora	Full HD 1920x1080

Wymagania	Opis
Obsługiwane przeglądarki	Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium based) Należy użyć najnowszej wersji przeglądarki przeznaczonej do systemu operacyjnego Windows.

3.2 Wymagania sprzętowe

Czytnik rejestracji

CredMgmt wymaga co najmniej jednego czytnika rejestracji do rejestracji kart fizycznych. Czytniki rejestracji są zwykle instalowane na stacjach roboczych klienta. Stacja robocza klienta komunikuje się ze sprzętem peryferyjnym za pośrednictwem programu `BoschPeripheralDeviceAddon.exe`. Jego instalację opisano poniżej.
Obsługiwane są następujące czytniki rejestracji i formaty kart.

	MIFARE DESFire EV1 Bosch Code	MIFARE DESFire EV1 CSN	MIFARE Classic CSN	HID Prox 26 bit	iCLASS 26 bit	iCLASS 35 bit	iCLASS 37 bit	iCLASS 48 bit	EM 26 bit
LECTUS enroll ARD-EDMCV002-USB	X								
OMNIKEY 5427 CK		X	X	X	X	X	X	X	X

3.2.1 Konfigurowanie dodatku na urządzenia peryferyjne

Dodatek Peripheral Devices jest wymagany tylko na tych komputerach klienckich, które łączą się z czytnikami rejestracji, skanerami lub innymi urządzeniami peryferyjnymi. Powtórz poniższą procedurę na każdym komputerze klienckim, który jest objęty tym wymaganiem.

1. Na docelowym komputerze klienckim zaloguj się jako administrator i z nośnika instalacyjnego uruchom program `BoschPeripheralDeviceAddon.exe`.
   - Zostaną wyświetlone podstawowe składniki, czyli oprogramowanie klienckie i oprogramowanie typowych urządzeń peryferyjnych. Zalecamy zainstalowanie wszystkich wyszczególnionych składników, nawet jeśli obecnie konkretne urządzenia nie będą instalowane.
2. Kliknij przycisk **Dalej**, aby zaakceptować domyślne pakiety instalacyjne.
3. W oknie **Konfiguracja klienta**

- **Katalog instalacyjny:** zaakceptuj domyślny (zalecane) lub zmień zgodnie z wymaganiami.
- **Port COM:**
  - W przypadku korzystania z czytnika rejestracji LECTUS, wprowadzić numer portu COM, na przykład `COM3`, do którego podłączony jest czytnik rejestracji. Sprawdź tę wartość w Menedżerze urządzeń systemu Windows.
  - Jeśli używany jest czytnik HID OMNIKEY, należy pozostawić to pole puste.

  - Kamera, skaner podpisów i skaner dokumentów są urządzeniami typu „plug-and-play” i nie wymagają podawania portu COM. Kliknij przycisk **Zezwól**, gdy w przeglądarce pojawi się monit o zezwolenie na połączenie.
- **Adres serwera** i **port:**
  - Wpisz nazwę dowolnego serwera (domyślnie co najmniej głównego serwera ACS) oraz numery portów stosownie do wszystkich usług backendowych, które muszą kontrolować urządzenia peryferyjne.
    Niezależnie od wyboru, kliknij polecenie **Testuj połączenie** i poczekaj na potwierdzenie.
    Kliknij polecenie **Dodaj**, aby dodać kolejne serwery.
    Kliknij polecenie **Usuń**, aby usunąć serwery.
  - Domyślne porty dla zwykłych usług backendowych to:
    `5806` dla CredMgmt
    `5706` dla VisMgmt

4. Kliknij przycisk **Dalej**, a zostanie wyświetlone podsumowanie składników do zainstalowania.
5. Kliknij przycisk **Instaluj**, aby rozpocząć instalację.
6. Kliknij przycisk **Zakończ**, aby zakończyć instalację.
7. Po zakończeniu instalacji uruchom ponownie komputer.

3.3 Instalowanie programu Credential Management

Wstęp

CredMgmt działa jako aplikacja internetowa w połączeniu z systemem kontroli dostępu firmy Bosch (ACS). W poniższych sekcjach opisano instalację składnika backendowego, który odpowiada za działanie aplikacji internetowej.

- Można go zainstalować tak, aby korzystał albo z lokalnej, albo zdalnej bazy danych.

W przypadku uruchomionego środowiska AMS, Visitor Management, Credential Management, Mobile Access w środowisku sieci korporacyjnej, zalecamy korzystanie z certyfikatów wydanych przez korporacyjny urząd certyfikacji (CA). Certyfikaty należy przygotować przed instalacją któregokolwiek z systemów backendowych. Zapoznaj się z sekcją *Korzystanie z certyfikatów niestandardowych* w podręczniku instalacji AMS.

3.3.1 Wymagania wstępne oprogramowania CredMgmt

Specjalny użytkownik dla zdalnej bazy danych (jeśli z niej korzystasz)

Użytkownik `CMUser` otwierający bazę danych ACS na rzecz aplikacji CredMgmt.
Jeśli CredMgmt ma korzystać ze zdalnej bazy danych, wykonaj poniższą procedurę.
WAŻNE: nie należy uruchamiać konfiguracji CredMgmt przed ukończeniem tej procedury.

1. Na serwerze zdalnej bazy danych utwórz użytkownika systemu Windows należącego do tej samej domeny, co ACS. Użyj następujących ustawień:

- **Nazwa użytkownika** (w samej nazwie użytkownika rozróżniana jest wielkość liter): <ACS-Domain>\`CMUser`
- **Hasło**: ustaw hasło zgodnie z zasadami zabezpieczeń, które mają zastosowanie do wszystkich komputerów. Należy o tym pamiętać, ponieważ będzie to wymagane do konfiguracji CredMgmt.
- **Użytkownik musi zmienić hasło przy następnym logowaniu**: `NO`
- **Użytkownik nie może zmienić hasła**: `YES`

– **Hasło nigdy nie wygasa**: YES
– **Logowanie jako usługa**: YES
– **Konto jest wyłączone**: NO

Następnie dodaj CMUser jako login do zdalnego serwera SQL w następujący sposób:

1. Otwórz SQL Management Studio
2. Połącz ze zdalną instancją SQL
3. Przejdź do **Security** (Zabezpieczenia) > **Login**
4. W okienku **Select a page** (Wybierz stronę) wybierz opcję **General** (Ogólne).
5. Wybierz użytkownika CMUser.
6. W okienku **Select a page** (Wybierz stronę) wybierz opcję **Server roles** (Role serwera).
7. Zaznacz pola wyboru public i dbcreator.

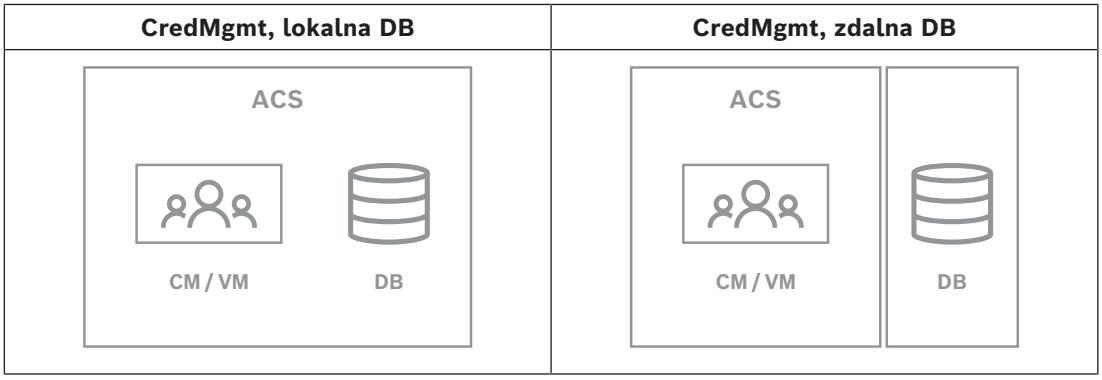
Specjalny użytkownik dla lokalnej bazy danych (jeśli z niej korzystasz)

Użytkownik CMUser otwierający bazę danych ACS na rzecz aplikacji CredMgmt.
NIE musisz tworzyć tego użytkownika, jeśli CredMgmt ma używać lokalnej bazy danych — program instalacyjny CredMgmt tworzy automatycznie użytkownika Windows CMUser na serwerze ACS.

Specjalny użytkownik w ACS

1. W ACS utwórz użytkownika i aktywuj dla niego funkcję **nieograniczonego** dostępu do **interfejsów API**.
   – Ścierzka postępowania dla AMS: **Configuration** (Konfiguracja) > **Operators and Workstations** (Operatorzy i stacje robocze) > **User rights** (Uprawnienia użytkownika) > karta **User account** (Kontrola dostępu) > **API Access rights control (Interfejs API do kontroli dostępu).**
     Wybierz z listy opcję Unlimited access.
   – Ścieżka postępowania w systemie BIS: **Configuration** (Konfiguracja) **Browser** (Przeglądarka) > **Administration** (Administracja) > **Operators** (Operatorzy) > wybierz operatora > karta: **ACE API Access rights (Uprawnienia dostępu ACE API)**
     Wybierz opcję Unlimited access.
   – Bardziej szczegółowe informacje na ten temat podano w rozdziale **Przydzielanie profili użytkowników (operatorów)** w instrukcji operatora głównego systemu kontroli dostępu.
2. Zapamiętaj lub zanotuj nazwę użytkownika i hasło, ponieważ będzie ich wymagał kreator instalacji aplikacji internetowej.

3.3.2 Procedura instalacji



Procedura

1. Na serwerze ACS uruchom program `BoschCredentialManagementServer.exe` jako administrator.

– Otworzy się program instalacyjny.

2. Na ekranie **Core components** (Komponenty podstawowe) wybierz opcję `Bosch Credential Management` i kliknij polecenie **Next** (Dalej).
3. Przeczytaj uważnie Umowę licencyjną użytkownika końcowego (EULA) i, jeśli wyrażasz na nią zgodę, kliknij polecenie **Accept** (Akceptuj). Bez wyrażenia zgody instalacja nie będzie możliwa.
4. Wybierz folder docelowy instalacji lub zaakceptuj domyślny (zalecane), a następnie kliknij polecenie **Next** (Dalej).
5. Na ekranie **SQL Server** (Serwer SQL) wybierz jedną z dwóch alternatywnych lokalizacji bazy danych. Dalsza konfiguracja ma dwa możliwe przebiegi. Wybierz jedną alternatywę dla następnego kroku:

– ALTERNATYWA 1 Opcja **z lokalną bazą danych**:
  – Program instalacyjny odnajduje lokalną bazę danych i dokonuje jej wstępnego wyboru.
  – Wpisz hasło SQL użytkownika admin (domyślne: `sa`).
  – Kliknij przycisk **Test Connection** (Testuj połączenie).
  – Kliknij przycisk **Dalej>**.
– ALTERNATYWA 2 Opcja **ze zdalną bazą danych**:
  – Wpisz nazwę serwera SQL znajdującego się w sieci.
  – Wpisz nazwę tej instancji bazy danych SQL.
  – Wpisz hasło SQL użytkownika admin (domyślne: `sa`).
  – Kliknij przycisk **Test Connection** (Testuj połączenie).
  – Zaznacz nazwę użytkownika i podaj hasło użytkownika administratora systemu Windows i serwera SQL, który utworzono do zdalnego korzystania z bazy danych (patrz wyżej: Wymagania wstępne)
  – Kliknij przycisk **Dalej>**.

6. Na ekranie **ACS access configuration** (Konfiguracja dostępu przez ACS):

– Wprowadź nazwę hosta dla serwera ACS.
– Wpisz nazwę użytkownika ACS z nieograniczonym dostępem do interfejsu API (patrz wyżej: Wymagania wstępne).
– Wpisz hasło ACS dla tego użytkownika ACS i potwierdź je.

7. Kliknij przycisk **Next** (Dalej).
8. W oknie **Identity server configuration** (Konfiguracja serwera tożsamości)

– Domyślnym serwerem tożsamości (wstępnie wybranym) jest podstawowy serwer ACS z portem `44333` `https://<nazwaserweraACS>:44333`
– Kliknij przycisk **Test Connection** (Testuj połączenie).

– Jeśli test się nie powiedzie, sprawdź ponownie dostępność serwera tożsamości.
– Kliknij przycisk **Next** (Dalej).

9. Na ekranie **Core components** (Komponenty podstawowe) potwierdź, że wybrano opcję CredMgmt, i kliknij polecenie **Install** (Instaluj).
10. Po zakończeniu instalacji uruchom program CredMgmt, wpisując następujący adres URL:

`https://` <nazwa_serwera_ACS>`:5806`

3.4 Instalowanie programu Mobile Access

Wstęp

Usługa backendowa Mobile Access zapewnia obsługę dostępu mobilnego zarówno dla aplikacji Credential Management, jak i Visitor Management.
Upewnij się, że masz najnowszą wersję głównego systemu kontroli dostępu i najnowszą wersję backendu Mobile Access.
UWAGA: jeśli używasz zarówno CredMgmt, jak i VisMgmt, program Mobile Access wystarczy zainstalować jeden raz.

– Można zainstalować go na tym samym serwerze, co ACS (instalacja współdzielona), lub na oddzielnym serwerze (instalacja rozproszona).
– Można go zainstalować tak, aby korzystał albo z lokalnej, albo zdalnej bazy danych.

Dostępność usługi backendu Mobile Access

Usługa backendu Mobile Access musi być stale dostępna dla urządzeń mobilnych.
Ze względów bezpieczeństwa jest bardzo mało prawdopodobne, aby urządzenia mobilne miały dostęp sieciowy do serwera ACS. Dlatego zalecana jest instalacja rozproszona. Pozwala to na uruchomienie usługi backendu Mobile Access na szerzej dostępnym serwerze „w chmurze”.

3.4.1 Przegląd instalacji, konfiguracji i użytkowania

Mobile Access wymaga współpracy kilku komponentów. Poniżej wymieniamy poszczególne etapy i opisujemy odpowiednie warunki wstępne i procedury w kolejnych częściach tego rozdziału:

Konfiguracja serwera ACS

1. Zainstalowany oraz uruchomiony serwer ACS z kompletem licencji, z trwałym certyfikatem głównym i zgodnymi czytnikami dostępu. Zdefiniowani w nim operatorzy z uprawnieniami do zarządzania programem Mobile Access.

Konfigurowanie programu Mobile Access

1. Administrator systemu instaluje jedną lub dwie aplikacje internetowe korzystające z usługi Mobile Access — albo Credential Management, albo Visitor Management w systemie ACS.
2. Administrator systemu instaluje backend Mobile Access.
3. Administrator systemu aktywuje Mobile Access w zainstalowanych aplikacjach internetowych.

Konfiguracja czytników

1. Administrator systemu tworzy w CredMgmt aplikacji instalatora (osobę uprawnioną do konfiguracji czytników Mobile Access).

2. Instalator pobiera aplikację instalatora ("Setup Access") na swoje urządzenie mobilne ze zwykłego sklepu z aplikacjami.
3. Administrator systemu wysyła zaproszenie do wskazanego instalatora.
4. Instalator akceptuje zaproszenie w aplikacji instalatora. To zaproszenie upoważnia instalatora do konfigurowania czytników dostępu dla Mobile Access.
5. Instalator konfiguruje czytniki za pomocą aplikacji instalacyjnej.

Używanie aplikacji Mobile Access

1. Uprawnieni posiadacze poświadczeń pobierają aplikację posiadacza poświadczeń („Mobile Access”) na swoje urządzenia mobilne ze zwykłego sklepu z aplikacjami.
2. Operatorzy CredMgmt i/lub VisMgmt wysyłają mobilne poświadczenia za pomocą kodu QR lub poczty elektronicznej do ich uprawnionych posiadaczy.
3. Posiadacze poświadczeń odczytują kod QR lub e-mail w aplikacji Mobile Access. Dzięki temu ich urządzenie mobilne może zacząć działać jako przedmiot uwierzytelniający podczas działania aplikacji.

3.4.2 Wymagania sprzętowe oprogramowania Mobile Access

Mobile Access wymaga czytników dostępu z modułem BLE. Odpowiednie są następujące czytniki Bosch:

ARD-SELECT -BOM, -WOM, -BOKM, -WOKM

- Litery B i W oznaczają kolor, odpowiednio czarny lub biały.
- O oznacza protokół OSDP.
- K wskazuje na obecność klawiatury
- M oznacza współpracę z aplikacją Mobile Access.

3.4.3 Wymagania wstępne konfiguracji oprogramowania Mobile Access

Specjalny użytkownik dla zdalnej bazy danych (jeśli z niej korzystasz)

Jeśli Mobile Access ma korzystać ze zdalnej bazy danych, utwórz i skonfiguruj na tym zdalnym serwerze użytkownika-administratora o nazwie `MAUser` — zarówno w systemie Windows, jak i na serwerze SQL Server. Następnie podczas poniższej konfiguracji wybierz opcję komputera zdalnego serwera bazy danych i wpisać hasło zdefiniowane powyżej dla `MAUser`.

WAŻNE: nie należy uruchamiać konfiguracji Mobile Access przed ukończeniem tej procedury.

Procedura

1. Na serwerze zdalnej bazy danych utwórz użytkownika systemu Windows należącego do tej samej domeny, co ACS. Użyj następujących ustawień:

- **Nazwa użytkownika** (w samej nazwie użytkownika rozróżniana jest wielkość liter): <ACS-Domain>\`MAUser`
- **Hasło**: ustaw hasło zgodnie z zasadami zabezpieczeń, które mają zastosowanie do wszystkich komputerów. Należy o tym pamiętać, ponieważ będzie to wymagane do konfiguracji Mobile Access.
- **Użytkownik musi zmienić hasło przy następnym logowaniu**: `NO`
- **Użytkownik nie może zmienić hasła**: `YES`
- **Hasło nigdy nie wygasa**: `YES`
- **Logowanie jako usługa**: `YES`
- **Konto jest wyłączone**: `NO`

Następnie dodaj `MAUser` jako login do zdalnego serwera SQL w następujący sposób:

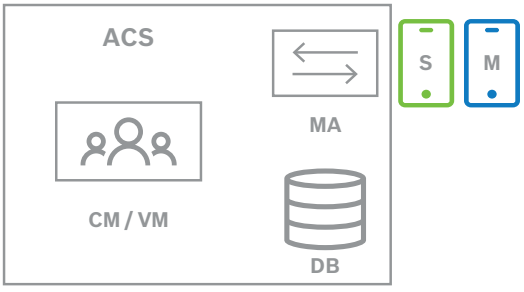
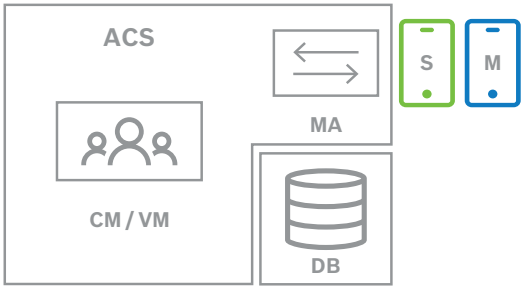
1. Otwórz SQL Management Studio

2. Połącz ze zdalną instancją SQL
3. Przejdź do **Security** (Zabezpieczenia) > **Login**
4. W okienku **Select a page** (Wybierz stronę) wybierz opcję **General** (Ogólne).
5. Wybierz użytkownika `MAUser`.
6. W okienku **Select a page** (Wybierz stronę) wybierz opcję **Server roles** (Role serwera).
7. Zaznacz pola wyboru `public` i `dbcreator`.

Specjalny użytkownik dla lokalnej bazy danych (jeśli z niej korzystasz)
Użytkownik `MAUser` otwierający bazę danych ACS na rzecz aplikacji Mobile Access.
NIE musisz tworzyć tego użytkownika, jeśli ma używać lokalnej bazy danych. Program instalacyjny Mobile Access tworzy automatycznie użytkownika Windows `MAUser` na serwerze ACS.

3.4.4 Procedura dla instalacji współdzielonej

Instalacja kolokowana oznacza, że usługa backendu Mobile Access działa na tym samym serwerze, co ACS.
Instalacja rozproszona oznacza, że usługa backendu Mobile Access działa na innym serwerze, na przykład „w chmurze”.
W przypadku opcji rozproszonej należy zapoznać się z następną sekcją **Procedura instalacji rozproszonej**.

Kolokacja z lokalną bazą danych	Kolokacja ze zdalną bazą danych
	

Klucz	Znaczenie
ACS	Główny system kontroli dostępu, AMS lub BIS-ACE
CM/VM	Backend aplikacji internetowej: Credential Management lub Visitor Management
DB	Główna baza danych ACS
MA	Backend Mobile Access
S	Aplikacja Setup Access dla urządzeń mobilnych instalatorów i konfiguratorów systemu
M	Aplikacja Mobile Access dla urządzeń mobilnych zwykłych posiadaczy poświadczeń.

Procedura
1. Na serwerze ACS, który w przypadku instalacji kolokowanych jest także serwerem Mobile Access, uruchom program `BoschMobileAccessBackend.exe` jako administrator.
– Otworzy się program instalacyjny.
2. Na ekranie **Location** (Lokalizacja) wybierz typ konfiguracji: **Co-located** (Współdzielona).

3. Na ekranie **Components** (Komponenty) sprawdź, czy wybrano opcję `Bosch Mobile Access`, i kliknij polecenie **Next** (Dalej).
4. Na ekranie **EULA** przeczytaj uważnie Umowę licencyjną użytkownika końcowego (EULA) i, jeśli wyrażasz na nią zgodę, kliknij polecenie **Accept** (Akceptuj). Bez wyrażenia zgody instalacja nie będzie możliwa.
5. Na ekranie **Installation directory** (Katalog instalacji):

– Wybierz folder docelowy instalacji lub zaakceptuj domyślny (zalecane).
– Wpisz nazwę swojej firmy taką, jaka ma być wyświetlana w aplikacji mobilnej oraz w szablonach wiadomości e-mail w formacie HTML
– Kliknij przycisk **Next** (Dalej).

6. Na ekranie **Certificate** (Certyfikat)

– Wpisz nazwę hosta, na którym ma być uruchomiony backend Mobile Access.
– W razie potrzeby lub jeśli sieć nie umożliwia ustalania nazwy hosta, wpisz adres IP tego hosta
– Kliknij przycisk **Dalej>**.

7. Na ekranie **SQL Server** (Serwer SQL) wybierz jedną z dwóch alternatywnych lokalizacji bazy danych. Dalsza konfiguracja ma dwa możliwe przebiegi. Wybierz jedną alternatywę dla następnego kroku:

– ALTERNATYWA 1 Opcja **z lokalną bazą danych**:
  – Program instalacyjny odnajduje lokalną bazę danych i dokonuje jej wstępnego wyboru.
  – Wpisz hasło SQL użytkownika admin (domyślne: `sa`).
  – Kliknij przycisk **Test Connection** (Testuj połączenie).
  – Kliknij przycisk **Dalej>**.
– ALTERNATYWA 2 Opcja **ze zdalną bazą danych**:
  – Wpisz nazwę serwera SQL znajdującego się w sieci.
  – Wpisz nazwę tej instancji bazy danych SQL.
  – Wpisz hasło SQL użytkownika admin (domyślne: `sa`).
  – Kliknij przycisk **Test Connection** (Testuj połączenie).
  – Zaznacz nazwę użytkownika i podaj hasło użytkownika administratora systemu Windows i serwera SQL, który utworzono do zdalnego korzystania z bazy danych (patrz wyżej: Wymagania wstępne)
  – Kliknij przycisk **Dalej>**.

8. W oknie **Identity server configuration** (Konfiguracja serwera tożsamości)

– Domyślnym serwerem tożsamości (wstępnie wybranym) jest podstawowy serwer ACS z portem `44333` `https://`<nazwaserweraACS>`:44333`
– Kliknij przycisk **Test Connection** (Testuj połączenie).
– Jeśli test się nie powiedzie, sprawdź ponownie dostępność serwera tożsamości.
– Kliknij przycisk **Next** (Dalej).

9. Na ekranie **Core components** (Komponenty podstawowe) potwierdź, że wybrano opcję **Bosch Mobile Access** i kliknij przycisk **Install** (Instaluj)

– Kreator instalacji zostanie zamknięty.

10. Kliknij przycisk **Dalej>**.
11. Na ekranie **Core components** (Komponenty podstawowe) sprawdź, czy instalacja została pomyślnie wykonana, i kliknij polecenie **Finish** (Zakończ).
12. W aplikacji `Services` w systemie Windows sprawdź, czy usługa `Bosch Mobile Access` jest uruchomiona.

3.4.5 Procedura dla instalacji rozproszonej

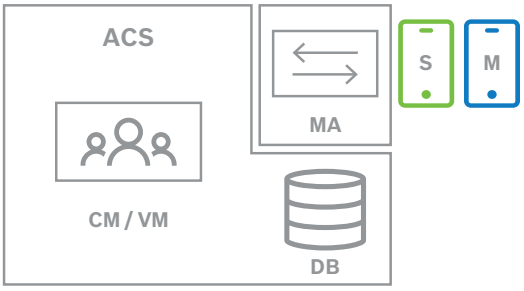
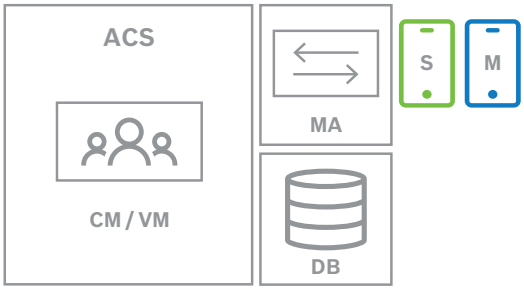
Instalacja kolokowana oznacza, że usługa backendu Mobile Access działa na tym samym serwerze, co ACS.

Instalacja rozproszona oznacza, że usługa backendu Mobile Access działa na innym serwerze, na przykład „w chmurze”.

W przypadku opcji współdzielonej zapoznaj się z poprzednią sekcją **Procedura instalacji współdzielonej**.

Na rozproszonym serwerze backendowym Mobile Access przed instalacją Mobile Access lub aktualizacją systemu wymagane jest spełnienie następującego warunku wstępnego. Nie jest to wymagane w środowisku kolokowanym:

– Przed uruchomieniem instalatora Mobile Access zainstaluj pakiet **ASP.NET Core 8.0 Runtime (v8.0.2) Hosting Bundle** na rozproszonym serwerze backendowym Mobile Access.
– Użyj poniższego łącza, aby pobrać wymagany pakiet hostingowy: https://dotnet.microsoft.com/en-us/download/dotnet/thank-you/runtime-aspnetcore-8.0.2-windows-hosting-bundle-installer.

Rozproszona z lokalną bazą danych	Rozproszona ze zdalną bazą danych
	

Klucz	Znaczenie
ACS	Główny system kontroli dostępu, AMS lub BIS-ACE
CM/VM	Backend aplikacji internetowej: Credential Management lub Visitor Management
DB	Główna baza danych ACS
MA	Backend Mobile Access
S	Aplikacja Setup Access dla urządzeń mobilnych instalatorów i konfiguratorów systemu
M	Aplikacja Mobile Access dla urządzeń mobilnych zwykłych posiadaczy poświadczeń.

Procedura

Upewnij się, że masz najnowszą wersję głównego systemu kontroli dostępu.

1. Na serwerze backendu Mobile Access uruchom program `BoschMobileAccessBackend.exe` jako administrator.

– Otworzy się program instalacyjny.

2. Na ekranie **Location** (Lokalizacja) wybierz typ konfiguracji: **Distributed** (Rozproszona).
3. Na ekranie **Host** wybierz opcję **Mobile Access Backend** i kliknij przycisk **Dalej**

– Uwaga: opcja **ACS** zostanie użyta w dalszej części procedury, przy instalacji aplikacji Mobile Access na serwerze ACS.

4. Na ekranie **Components** (Komponenty) sprawdź, czy wybrano opcję **BoschMobile Access** i kliknij przycisk **Next** (Dalej)
5. Na ekranie **EULA** przeczytaj uważnie Umowę licencyjną użytkownika końcowego (EULA) i, jeśli wyrażasz na nią zgodę, kliknij polecenie **Accept** (Akceptuj). Bez wyrażenia zgody instalacja nie będzie możliwa.
6. Na ekranie **Installation directory** (Katalog instalacji):

– Wybierz folder docelowy instalacji lub zaakceptuj domyślny (zalecane).
– Wpisz nazwę swojej firmy taką, jaka ma być wyświetlana w aplikacji mobilnej oraz w szablonach wiadomości e-mail w formacie HTML
– Kliknij przycisk **Dalej>**.

7. Na ekranie **SQL Server** (Serwer SQL) wybierz jedną z dwóch alternatywnych lokalizacji bazy danych. Dalsza konfiguracja ma dwa możliwe przebiegi. Wybierz jedną alternatywę dla następnego kroku:

– ALTERNATYWA 1 Opcja **z lokalną bazą danych**:
  – Program instalacyjny odnajduje lokalną bazę danych i dokonuje jej wstępnego wyboru.
  – Wpisz hasło SQL użytkownika admin (domyślne: `sa`).
  – Kliknij przycisk **Test Connection** (Testuj połączenie).
  – Kliknij przycisk **Dalej>**.
– ALTERNATYWA 2 Opcja **ze zdalną bazą danych**:
  – Wpisz nazwę serwera SQL znajdującego się w sieci.
  – Wpisz nazwę tej instancji bazy danych SQL.
  – Wpisz hasło SQL użytkownika admin (domyślne: `sa`).
  – Kliknij przycisk **Test Connection** (Testuj połączenie).
  – Zaznacz nazwę użytkownika i podaj hasło użytkownika administratora systemu Windows i serwera SQL, który utworzono do zdalnego korzystania z bazy danych (patrz wyżej: Wymagania wstępne)
  – Kliknij przycisk **Dalej>**.

Na tym etapie instalacji rozproszonej należy przełączyć się na komputer, na którym działa serwer ACS, i skonfigurować na nim aplikację Mobile Access. *Pozwoli to na dalszą komunikację z backendem* Mobile Access *na komputerze lokalnym.*
Po wykonaniu wskazanych czynności program instalacyjny poprowadzi Cię z powrotem do lokalnego serwera w celu potwierdzenia i kontynuacji.

1. Na serwerze ACS uruchom program `BoschMobileAccessBackend.exe` jako administrator.

– Otworzy się program instalacyjny.

2. Na ekranie **Location** (Lokalizacja) wybierz typ konfiguracji: **Distributed** (Rozproszona).
3. Na ekranie **Host** wybierz opcję **ACS** i kliknij polecenie **Next** (Dalej).
4. Na ekranie kreatora **Companion** przeczytaj wyjaśnienie i kliknij przycisk **Next** (Dalej).
5. Na ekranie **Certificate** (Certyfikat)

– Wpisz nazwę hosta, na którym ma być uruchomiony backend Mobile Access.
– W razie potrzeby lub jeśli sieć nie umożliwia ustalania nazwy hosta, wpisz adres IP tego hosta
– Kliknij przycisk **Dalej>**.

6. W oknie **Identity server configuration** (Konfiguracja serwera tożsamości)

– Domyślnym serwerem tożsamości (wstępnie wybranym) jest podstawowy serwer ACS z portem `44333` `https://`<nazwaserweraACS>`:44333`

– Kliknij przycisk **Test Connection** (Testuj połączenie).
– Jeśli test się nie powiedzie, sprawdź ponownie dostępność serwera tożsamości.
– Kliknij przycisk **Next** (Dalej).
7. Na ekranie **Create file** (Utwórz plik)
W tym miejscu tworzymy plik konfiguracyjny w formie zabezpieczonego hasłem pliku ZIP, który zostanie udostępniony backendowi Mobile Access.
– **User password** (Hasło użytkownika): wprowadź hasło do pliku ZIP.
– **Configuration file** (Plik konfiguracyjny): wpisz lub wybierz folder, w którym zapiszesz plik ZIP. Pamiętaj, że folder ten powinien być dostępny z komputera, na którym uruchomiono backend Mobile Access. Jeśli nie, musisz w inny sposób przenieść plik ZIP na ten komputer.
– Kliknij polecenie przycisk **Create configuration file (Utwórz plik konfiguracyjny)**.
– Kliknij przycisk **Dalej>**.
8. Na ekranie **Switch machine** (Przełącz urządzenie)
Kroki instalacji na serwerze ACS zostały zakończone.
– Kliknij **Confirm (Potwierdź)**, aby zakończyć procedurę.

W tym kroku instalacji rozproszonej wrócić do programu instalacyjnego, na komputerze z backendem oprogramowania Mobile Access.

1. Wróć do programu instalacyjnego `BoschMobileAccessBackend.exe` na komputerze z serwerem Bosch Mobile Access.
2. Na stronie **Switch machine** (Przełącz urządzenie)
– zaznacz pole wyboru z opisem **I have already completed the required steps on the ACS machine** (Wymagane kroki na maszynie ACS zostały już wykonane).
– Kliknij przycisk **Dalej>**.
3. Na ekranie **Upload file** (Przesyłanie pliku)
– **Upload configuration file** (Prześlij plik konfiguracyjny): wybierz plik konfiguracyjny utworzony na serwerze ACS.
– **Password verification** (Weryfikacja hasła): wpisz hasło do pliku ZIP ustawione na serwerze ACS.
– Po wpisaniu prawidłowego hasła kliknij przycisk **Next** (Dalej), aby odczytać plik konfiguracyjny
4. Na ekranie **Core components** (Komponenty podstawowe) potwierdź, że wybrano opcję **Bosch Mobile Access** i kliknij przycisk **Install** (Instaluj)
– Kreator instalacji zostanie zamknięty.
5. Kliknij przycisk **Dalej>**.
6. Na ekranie **Core components** (Komponenty podstawowe) sprawdź, czy instalacja została pomyślnie wykonana, i kliknij polecenie **Finish** (Zakończ).
7. W aplikacji `Services` w systemie Windows sprawdź, czy usługa `Bosch Mobile Access` jest uruchomiona.

3.5 Certyfikaty do bezpiecznej komunikacji

Aby zapewnić bezpieczną komunikację między przeglądarką na komputerze klienckim i serwerem ACS, skopiuj poniższy certyfikat z serwera ACS do komputerów klienckich. Aby go zainstalować, należy użyć konta z uprawnieniami administratora systemu Windows.
Typowa ścieżka dostępu do certyfikatu:

– <installation drive>:
`\Bosch Sicherheitssysteme\Access Management System\Certificates\Bosch Security System Internal CA - BISAMS.cer`

Uwaga: po zwinięciu certyfikatu należy ponownie uruchomić aplikację backendową Mobile Access lub usługę Bosch Credential Management i usługę Bosch Visitor Management.

Przegląd transferów certyfikatów

Do → **Od ↓**	**ACS**	**MA** Backend Mobile Access	**DB** Baza danych	**S** Instalator	**M** Aplikacja dostępowa właściciela karty	**R** Czytnik
ACS	/	Przesłane przez kreatora instalacji (za pomocą narzędzia cert)	/	/	/	/
MA Backend Mobile Access	Przeniesione przez kreatora konfiguracji MA	/	/	Przeniesione przez rejestrację kodem QR Zaktualizowane powiadomieniem push	Przeniesione przez rejestrację kodem QR Zaktualizowane powiadomieniem push	/
DB Baza danych	/	/	/	/	/	/
S Instalator	/	Przeniesione przez rejestrację kodem QR	/	/	/	/
M Aplikacja dostępowa właściciela karty	/	Przeniesione przez rejestrację kodem QR	/	/	/	/

3.5.1 Certyfikaty dla przeglądarki Firefox

Można zignorować tę sekcję, jeśli nie korzysta się z przeglądarki Firefox.

Przeglądarka Firefox obsługuje certyfikaty główne w inny sposób: Firefox nie konsultuje przechowywania certyfikatu Windows zaufanych certyfikatów głównych. Zamiast tego każdy profil przeglądarki zachowuje swój własny magazyn certyfikatów głównych. Więcej informacji na ten temat można znaleźć w łączu https://support.mozilla.org/en-US/kb/setting-certificate-authorities-firefox
W tej witrynie internetowej znajdują się również instrukcje dotyczące wymuszania przez przeglądarkę Firefox przechowywania certyfikatu Windows dla wszystkich użytkowników. Można również importować certyfikaty domyślne zgodnie z poniższym opisem. Uwaga:
– Należy zaimportować certyfikaty dla każdego użytkownika i profilu Firefox.
– Opisany poniżej certyfikat serwera jest domyślnym certyfikatem utworzonym podczas instalacji. Jeśli użytkownik posiada certyfikat zakupiony od organu certyfikacji, może go użyć zamiast tego.

Importowanie certyfikatów do magazynu certyfikatów w przeglądarce Firefox
Aby uzyskać dostęp do serwera ACS z przeglądarki Firefox na komputerze klienckim VisMgmt, można zaimportować z serwera następujący certyfikat domyślny:
– <installation drive>:
`\Bosch Sicherheitssysteme\Access Management System\Certificates\Bosch Security System Internal CA - BISAMS.cer`
W przypadku systemu BIS ACE można też pobrać certyfikat za pośrednictwem sieci Web:
– `HTTP://`<Hostname>`/`<Hostname>`.cer`

Urządzenia peryferyjne: aby uzyskać dostęp do podłączonego urządzenia peryferyjnego, takiego jak skaner dokumentów lub podpisów, z przeglądarki Firefox na komputerze klienckim, można użyć domyślnego certyfikatu. Można go znaleźć na komputerze klienckim w następującej lokalizacji:
<installation drive>`:\Program Files (x86)\Bosch Sicherheitssysteme\Bosch Peripheral Device Addon\BoschAcePeripheralDeviceAddonHardware CA.cer`

Procedura (powtarzanie w przypadku każdego certyfikatu i profilu przeglądarki Firefox):
Aby zainstalować wymagane certyfikaty, należy na komputerze klienckim wykonać następującą procedurę:
1. Zlokalizować certyfikat, który ma zostać zainstalowany.
2. Otworzyć przeglądarkę Firefox i wpisać `about:preferences` w pasku adresu.
– Pojawi się strona opcji.
3. W polu **Znajdź w ustawieniach** wpisz `certificate`
– Na stronie pojawi się przycisk **Wyświetl certyfikaty**.
4. Kliknij przycisk **Wyświetl certyfikaty**.
– Otworzy się okno dialogowe **Menadżer certyfikatów** z kilkoma kartami.
5. Wybierz kartę **Organy certyfikacji**.
6. Kliknij przycisk **Importuj**...
– Pojawi się okno dialogowe wyboru certyfikatu.
7. Wybierz certyfikat zlokalizowany w kroku 1 i kliknij przycisk **Otwórz**.
– Otworzy się okno dialogowe **Pobieranie certyfikatu**.
8. Wybierz opcję **Zaufaj temu CA przy identyfikacji witryn internetowych** i kliknij przycisk **OK**.
– Okno dialogowe **Pobieranie certyfikatu** zamknie się
9. W oknie dialogowym **menadżer certyfikatów** kliknij **OK**.
– Procedura importowania certyfikatu została zakończona.

3.5.2 Certyfikaty dla przeglądarki Chrome

Możesz zignorować tę sekcję, jeśli nie używasz przeglądarki Chrome.
Informacje o zmianach w obsłudze certyfikatów w przeglądarce Chrome można znaleźć w uwagach do wydania systemu ACS.
Aby zainstalować certyfikat w przeglądarce Chrome w systemie Microsoft Windows:

1. Pobierz plik z certyfikatem.
2. Przejdź do strony ustawień przeglądarki Chrome (`chrome://settings`) i kliknij polecenie **Zaawansowane**.
3. W obszarze **Prywatność i bezpieczeństwo** kliknij opcję **Zarządzaj certyfikatami**.
4. Na karcie **Twoje certyfikaty** kliknij przycisk **Importuj**, aby rozpocząć proces instalacji certyfikatu:

– Zostanie otwarty Kreator importu.

5. Wybierz plik certyfikatu i zakończ pracę kreatora.
6. Zainstalowany certyfikat zostanie wyświetlony na karcie **Zaufane główne urzędy certyfikacji**.

3.5.3 Instalowanie aplikacji Mobile Access

Wstęp

Do obsługi systemu Mobile Access Bosch udostępnia następujące aplikacje

– Bosch Mobile Access: aplikacja do przechowywania wirtualnych poświadczeń i przesyłania ich przez Bluetooth do tych czytników, które są skonfigurowane do pracy z systemem Mobile Access. Czytnik następnie przyznaje dostęp lub odmawia go w zależności od tego, czy przechowywane poświadczenia na to pozwalają.
– Bosch Setup Access: aplikacja instalacyjna do skanowania i konfigurowania czytników przez Bluetooth.

Upoważnieni operatorzy Visitor Management i Credential Management mogą wysyłać wirtualne dane uwierzytelniające zarówno dla aplikacji posiadacza karty, jak i aplikacji instalatora.

Dopóki aplikacja posiadacza karty jest uruchomiona, a na urządzeniu mobilnym aktywna jest funkcja Bluetooth, można z niej korzystać tak, jak z karty fizycznej. Nie ma potrzeby wydawania poleceń z aplikacji, ani nawet odblokowywania ekranu.

Uwaga!
WAŻNE: nie należy jednocześnie używać aplikacji posiadacza karty i aplikacji instalatora. Upewnij się, że gdy aplikacja posiadacza karty jest w użyciu nikt nie używa aplikacji instalatora i odwrotnie.

Procedura

Aplikacje Bosch Mobile Access można pobrać ze sklepów z aplikacjami Google i Apple oraz zainstalować w zwykły sposób. Ich nazwy w sklepach z aplikacjami to:

– Bosch Mobile Access
– Bosch Setup Access

3.6 Naprawa instalacji aplikacji Mobile Access

Wstęp

Aby zaktualizować pliki binarne lub odtworzyć certyfikat Mobile Access, możesz uruchomić instalator bieżącej lub nowszej wersji Mobile Access na istniejącej instalacji:

Procedura

1. Na serwerze backendu Mobile Access uruchom program `BoschMobileAccessBackend.exe` jako administrator.

– Zwróć uwagę, że w przypadku instalacji kolokowanych serwer backendu Mobile Access oprogramowania jest taki sam, co serwer ACS.

2. Postępuj zgodnie z kreatorem instalacji, wprowadzając te same ustawienia, co w instalacji pierwotnej.

– Aby ponownie utworzyć certyfikat, na ekranie **Certificates** (Certyfikaty) wybierz przycisk radiowy **Re-create certificate** (Utwórz ponownie certyfikat).

3. Po zakończeniu pracy programu instalacyjnego uruchom ponownie serwer.
4. Uruchom nową sesję logowania w każdej aplikacji internetowej, która korzysta z aplikacji Mobile Access (CredMgmt lub VisMgmt lub obu z nich).

– Aplikacja internetowa zacznie używać nowych plików binarnych.
– Jeśli wybrano opcję **Re-create certificate** (Utwórz ponownie certyfikat), dalsze zaproszenia wysyłane do użytkowników i instalatorów Mobile Access będą oparte na nowym certyfikacie Mobile Access.

3.7 Odinstalowanie oprogramowania

Aby odinstalować oprogramowanie z serwera lub klienta:

1. Jako administrator systemu Windows uruchom program **Dodaj lub usuń programy** w systemie Windows.
2. Wybierz program (serwer lub klient) i kliknij polecenie **Uninstall** (Odinstaluj).
3. (W zakresie zarządzania gośćmi i tylko na serwerze) Wybierz, czy chcesz usunąć bazę danych zarządzania gośćmi oraz sam program.

– **Uwaga**: baza danych zawiera zapisy wszystkich wizyt, które zostały zarejestrowane w czasie działania programu. Możesz zarchiwizować bazę danych lub przenieść ją do innej instalacji.

4. Wybierz, czy chcesz usunąć pliki dziennika.
5. Zakończ usuwanie w zwykły sposób.
6. (Zalecane) Uruchom ponownie komputer, aby upewnić się, że rejestr systemu Windows został w pełni zmodyfikowany.

Uwaga: Po odinstalowaniu backendu Mobile Access następujące ślady konfiguracji powinny zostać usunięte w razie potrzeby ręcznie:

– **MAUser** – ten użytkownik pozostaje mimo dezinstalacji. Administrator musi usunąć go ręcznie.
– **Certyfikaty** – użyj opcji *Zarządzaj certyfikatami komputera*, aby ręcznie usunąć wszystkie certyfikaty zainstalowane w związku z instalacją programu Mobile Access.
– **Konfiguracja serwera ID dla dostępu mobilnego** – plik *appsettings.Extension.MobileAccessBackend* nie jest kasowany po dezinstalacji backendu. Usuń go ręcznie.

4 Przegląd informacji o aplikacji Credential Management

Poniżej przedstawiono możliwe topologie instalacji zarządzania poświadczeniami, zarówno z oprogramowaniem Mobile Access, jak i bez niego. Każda ramka reprezentuje osobny komputer.

Klucz	Znaczenie
ACS	Główny system kontroli dostępu, AMS lub BIS-ACE
CM/VM	Backend aplikacji internetowej: Credential Management lub Visitor Management
DB	Główna baza danych ACS
MA	Backend Mobile Access
S	Aplikacja Setup Access dla urządzeń mobilnych instalatorów i konfiguratorów systemu
M	Aplikacja Mobile Access dla urządzeń mobilnych zwykłych posiadaczy poświadczeń.

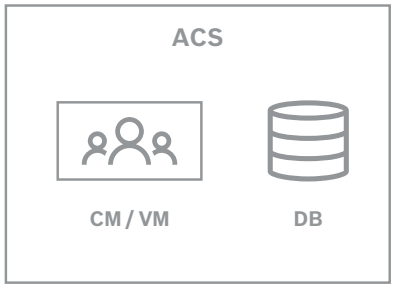
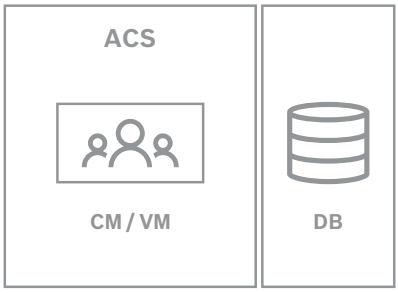
Credential Management, lokalna DB	Credential Management, zdalna DB
	

Tabela 4.1: Topologie aplikacji Credential Management

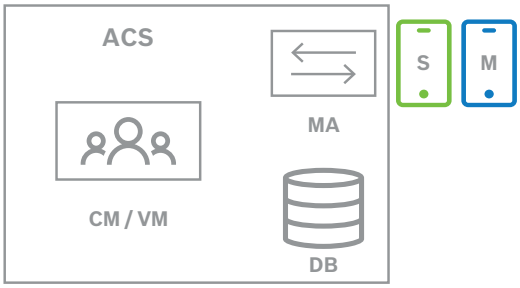
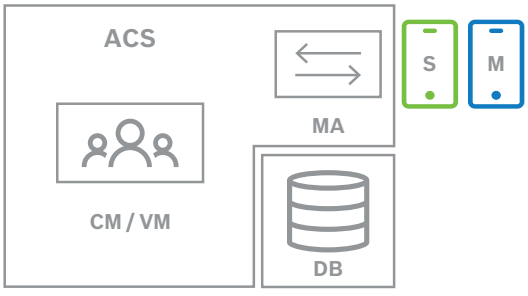
Mobile Access, kolokowane, lokalna DB	Mobile Access, kolokowane, zdalna DB
	

Tabela 4.2: Mobile Access, topologie współdzielone

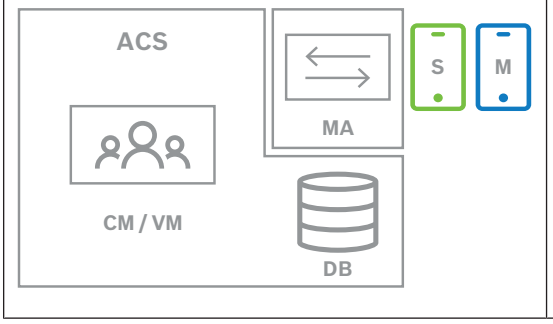
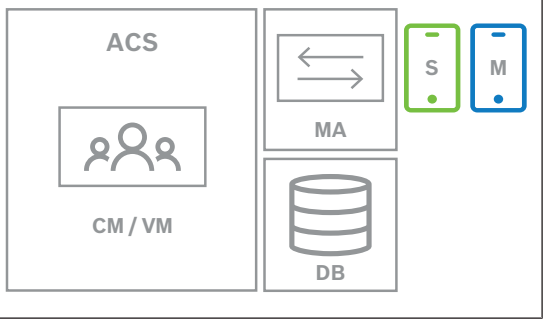
Mobile Access, rozproszone, lokalna DB	Mobile Access, rozproszone, zdalna DB
	

Tabela 4.3: Mobile Access, topologie rozproszone

Zgodne wersje powiązanego oprogramowania

W poniższej tabeli wymieniono wersje narzędzi programów pomocniczych zgodne z tą wersją systemu.

Element	Wersja	Lokalizacja
Access Management System (AMS)	5.5 (zawiera rozszerzenie Mobile Access)	Download Store / katalog produktów
Visitor Management (VisMgmt)	5.5 (zawiera rozszerzenie Mobile Access)	Download Store / katalog produktów

Uwaga!

Dywizji

Programy Credential Management, Visitor Management i Mobile Access nie obsługują funkcji „stref” w systemach kontroli dostępu firmy Bosch, w których jedno ACS zarządza kontrolą dostępu u wielu niezależnych dzierżawców.

5 Konfiguracja

5.1 Tworzenie użytkowników Credential Management w ACS

W systemie ACS (ACE lub AMS) każdy użytkownik Credential Management musi być posiadaczem karty z oddzielną definicją operatora.

Te definicje operatorów zawierają specjalne uprawnienia do korzystania z programu CredMgmt przedstawione w formie **profili użytkowników**.
Należy zdefiniować osobnego operatora dla każdego posiadacza karty, który pracuje w programie CredMgmt. Temu samemu operatorowi nie można przypisywać wielu posiadaczy kart.
Szczegółowe informacje i instrukcje dotyczące **Profili użytkowników** można znaleźć w pomocy ekranowej usługi ACS.
Użytkownicy aplikacji Credential Management muszą zostać utworzeni w AMS:

Ścieżka w oknie dialogowym
Configuration > **Operators and Workstations** > **User profiles** (Konfiguracja > Operatorzy i stacje robocze > Profile użytkownika).

Procedura

1. Kliknij przycisk  , aby utworzyć nowy profil.
2. Wprowadź nazwę profilu w polu **Nazwa profilu** (obowiązkowe).
3. Wprowadź opis profilu w polu **Description** (Opis) (opcjonalnie, ale zalecane).
4. Kliknij przycisk  lub **Zastosuj**, aby zapisać zmiany.
5. Wybierz funkcję w zależności od typu profilu:
   - W panelu listy wybierz funkcje (pierwsza kolumna) i możliwości wewnątrz funkcji (**Execute** [Wykonywanie], **Change** [Zmiana], **Add** [Dodawanie], **Delete** [Usuwanie]), które mają być dostępne w tym profilu. Kliknij dwukrotnie te elementy, aby przełączyć wartości ich ustawień na `Yes`.
   - Podobnie upewnij się, że we wszystkich funkcjach, które mają być niedostępne, ustawiono wartość `No`.
6. Kliknij przycisk  lub **Zastosuj**, aby zapisać zmiany.

Aby uzyskać więcej informacji na temat ról użytkowników w aplikacji Credential Management, zapoznaj się z sekcją *Przegląd ról użytkowników*.

5.2 Logowanie w celu wykonania zadań konfiguracyjnych

Do wykonywania zadań administracyjnych i konfiguracyjnych należy używać komputera, który jest fizycznie chroniony przed nieuprawnionym dostępem.

1. W przeglądarce internetowej wprowadź adres HTTPS serwera programu CredMgmt, a następnie dwukropek i numer portu (domyślnie `5806`)
   `https://`<mój_serwer_CredMgmt>`:5806`
   Pojawi się ekran **Login**.
2. Zaloguj się jako użytkownik o statusie **Administrator** dla programu CredMgmt.
3. Kliknij przycisk  , a zostanie otwarte menu **Ustawienia**.

5.3 Konfigurowanie za pomocą menu Ustawienia

Informacje ogólne	– **Retention period (days)** (Okres przechowywania (dni)): to ustawienie określa sposób obsługi rekordów wizyt. – Po jednokrotnym upłynięciu tego czasu aplikacja anonimizuje rekord. – Po dwukrotnym upłynięciu tego czasu aplikacja usuwa rekord. Wartością domyślną jest `365`. Aby całkowicie wyłączyć okres przechowywania, ustaw 0. Rekordy wizyt będą wówczas przechowywane bezterminowo. – **Logo**: zaznacz lub wyczyść pole wyboru, które reguluje, czy okna dialogowe wyświetlają niestandardowe logo, czy logo domyślne. – Aby zapoznać się z kryteriami dotyczącymi niestandardowych plików logo, patrz: *Dostosowywanie firmowego logo, Strona 30* – **Supergraphic** (Supergrafika): zaznacz lub wyłącz to pole wyboru, które reguluje, czy w oknach dialogowych wyświetlana jest supergrafika Bosch. – **Języki**: wybierz, które języki mają być dostępne w interfejsie użytkownika, wraz z ich preferowanymi formatami **daty** i **godziny**. – **Mail server** (Serwer poczty e-mail): wpisz adres IP, numer portu i szczegóły konta swojego serwera poczty e-mail, aby umożliwić wysyłanie wiadomości e-mail z aplikacji. Jeśli zewnętrzny serwer pocztowy wymaga dodatkowego certyfikatu SSL/TSL, zaimportuj go na maszynę, na której działa backend dostępu mobilnego. Po imporcie wymagane jest ponowne uruchomienie środowiska `VisitorManagerServer`. – **Szablony poczty e-mail** Dostępnych jest kilka szablonów wiadomości e-mail w formacie HTML, które zazwyczaj dostosowuje się do własnych wymagań. Szczegółowe informacje na ten temat można znaleźć w oddzielnej sekcji **Szablony poczty e-mail** poniżej. – **Mobile Access** Zaznacz pole wyboru **Mobile Access**, aby włączyć dostęp mobilny.Mobile Access. **Connection** (Połączenia): wprowadź adres serwera Mobile Access (adres serwera rejestracji). `https://`<mój_serwer_backendu_MyMobile>`:5700` Użyj ustawienia (FQDN), aby wprowadzić ten <mój_serwer_backendu_MyMobile>w środowisko wielodomenowym. **Uwaga:** aby użyć adresu IP zamiast FQDN, musisz wprowadzić ten adres IP w obszarze **Certificate creation** (Tworzenie certyfikatu) podczas uruchamiania kreatora konfiguracji backendu Mobile Access.

	Rejestracja instalatora (Installer onboarding): wybierz informacje, których wymagasz od instalatorów, aby mogli skonfigurować czytniki dostępu mobilnego za pomocą aplikacji Bosch Setup Access. Wyloguj się z aplikacji internetowej i zaloguj ponownie, aby natychmiast korzystać z funkcji Mobile Access.

5.3.1 Szablony wiadomości e-mail

Dostępnych jest kilka szablonów wiadomości e-mail w formacie HTML, które zazwyczaj dostosowuje się do wymagań własnej firmy. W każdym szablonie możliwe jest przechowywanie adresów pocztowych DW, UDW i odbiorcy testowego, do którego można natychmiast wysłać testową wiadomość e-mail.
Szablony pobrane z menu **Settings** (Ustawienia) są zapisywane w domyślnym folderze pobierania w przeglądarce.

- `MobileAccess.html` Zaproszenie dla posiadacza karty do korzystania z poświadczeń na smartfonie.
- `SetupAccess.html` Zaproszenie dla instalatora służące do konfigurowania czytników na potrzeby aplikacji Mobile Access.

Symbole zastępcze wykorzystywane w szablonach wiadomości e-mail

Szablony wiadomości e-mail zawierają kilka tekstów symboli zastępczych służących do dołączania pól bazy danych w tekście. Te symbole zastępcze zostały opisane w poniższych tabelach w odniesieniu do szablonów, w których można ich używać.

Mobile Access

Wiadomość e-mail wysyłana do posiadacza karty (w przypadku aplikacji Mobile Access) po udzieleniu dostępu mobilnego

Symbol zastępczy	Opis
`{{Title}}`	tytuł osoby (pan, pani, dr.)
`{{FirstName}}`	imię osoby
`{{LastName}}`	nazwisko osoby
`{{CompanyName}}`	firma osoby
`{{QrcodeLink}}`	Kod QR odpowiadający linkowi, który oferuje posiadaczowi karty mobilny dostęp za pośrednictwem aplikacji
`{{InviteLink}}`	link oferujący posiadaczowi karty mobilny dostęp za pośrednictwem aplikacji

Setup Access

Wiadomość e-mail wysyłana do instalatora aplikacji Mobile Access (do aplikacji Setup Access) po udzieleniu dostępu do konfiguracji czytników

Symbol zastępczy	Opis
`{{Title}}`	tytuł instalatora (pan, pani, dr.)

Symbol zastępczy	Opis
{{FirstName}}	imię instalatora
{{LastName}}	nazwisko instalatora
{{CompanyName}}	firma instalatora
{{QrcodeLink}}	Kod QR odpowiadający linkowi, który oferuje instalatorowi mobilny dostęp za pośrednictwem aplikacji Setup Access
{{InviteLink}}	link, który oferuje instalatorowi mobilny dostęp za pośrednictwem aplikacji Setup Access

5.3.2 Szablony dokumentów

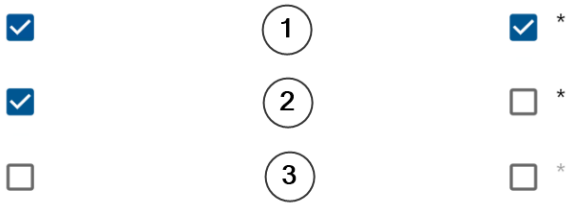
W przypadku różnych dokumentów i wiadomości e-mail możesz pobrać szablony i przesłać ich dostosowane wersje. Pozwala na to okno dialogowe **Pulpit** > **Ustawienia > Ogólne**.

5.4 Dostosowywanie interfejsu użytkownika

Interfejs użytkownika dostosowuje się w oknie dialogowym Pulpit nawigacyjny > **Settings** (Ustawienia).

5.4.1 Ustawianie opcji jako widocznych, niewidocznych i obowiązkowych

Określ, które pola danych będą widoczne w oknach dialogowych, a które z tych danych będą dodatkowo obowiązkowe.
Przykład:



- (1) jest widoczne i obowiązkowe,
- (2) jest widoczne, ale nieobowiązkowe,
- (3) jest niewidoczne.

5.4.2 Dostosowywanie tekstów interfejsu użytkownika do lokalizacji

Teksty interfejsu użytkownika można łatwo dostosować w zależności od języka.
Domyślnie pole **lokalnego tekstu** zawiera standardowe nagłówki bloków pól danych w oknach dialogowych zbierania danych.
Aby dostosować te nagłówki do wymagań lokalnych:

1. Wybierz język interfejsu użytkownika z listy.
2. Zastąp tekst w polu tekstowym.
   Można używać tagów HTML do prostego formatowania, np.:
   ```
   <b>this text will appear bold </b>
   <i>italics</i>
   <u>underline</u>
   ```

5.4.3 Dostosowywanie firmowego logo

Przesyłane pliki graficzne z logo firmy muszą spełniać następujące kryteria:

Obsługiwane formaty	PNG, JPEG, JPG
Dokładna szerokość (w pikselach)	125
Dokładna wysokość (w pikselach)	63
Maksymalny rozmiar (MB)	1

5.5 Ustawienia zapory sieciowej

Dodaj dodatkowe aplikacje do konfiguracji zapory na komputerach serwera i klientów:

1. Uruchom Zaporę systemu Windows: kliknij kolejno Start > **Panel sterowania** > **Zapora systemu Windows**
2. Kliknij opcję **Ustawienia zaawansowane**
3. Kliknij opcję **Reguły przychodzące**
4. W okienku **Akcje** kliknij opcję **Nowa reguła...**
5. W oknie dialogowym **Typ reguły** zaznacz opcję **Port** i kliknij przycisk **Dalej >**
6. Na następnej stronie zaznacz opcje **TCP i Określone porty lokalne**
7. Zezwól na komunikację przez następujące porty:

– Na serwerze lub komputerach

<nazwa_serwera>:44333 — używany przez serwer tożsamości AMS **(*)**

<nazwa_serwera> :5706 — używany przez serwer VisMgmt

<nazwa_serwera> :5806 — używany przez serwer CredMgmt

<nazwa_serwera> :5701 — używany przez serwer backendu Mobile Access

– Na komputerach klienckich

localhost:5707— używany przez dodatek Bosch na urządzenia peryferyjne

(*) Używamy serwerów tożsamości AMS i BIS zgodnie z ich instrukcjami instalacji.

Wykorzystanie portów w systemie

Serwer wychodzący	Port wychodzący	Serwer przychodzący	Port przychodzący	Protokół	Uwagi
VisMgmt lub CredMgmt	*	Backend Mobile Access	5701	HTTPS	Polecenia z aplikacji internetowej służące do tworzenia i/lub usuwania poświadczeń mobilnych
Urządzenia mobilne z Internetu	*	Backend Mobile Access	5701	HTTPS	Urządzenia mobilne otrzymują poświadczenia mobilne przez Internet.

Serwer wychodzący	Port wychodzący	Serwer przychodzący	Port przychodzący	Protokół	Uwagi
Backend Mobile Access	*	Google Firebase (Internet)	*	HTTPS	Urządzenia mobilne otrzymują powiadomienia push; zapoznaj się z dokumentacją Google Firebase dotyczącą ustawień zapór. https://firebase.google.com/docs/cloud-messaging/concept-options
Komputer kliencki użytkownika VisMgmt	*	Backend VisMgmt	5706	HTTPS	Polecenia z komputera klienckiego VisMgmt do backendu VisMgmt
Komputer kliencki użytkownika CredMgmt	*	Backend CredMgmt	5806	HTTPS	Polecenia z komputera klienckiego CreMgmt do backendu CredMgmt
Komputer administratora	*	Backend Mobile Access	3389	Pulpit zdalny (RDP)	Ze względów bezpieczeństwa dostęp do komputera z backendem Mobile Access należy przydzielać tylko tymczasowo.

Uwaga!
Należy pamiętać, że Mobile Access i ACS nie mają bezpośredniego połączenia, ani przychodzącego, ani wychodzącego.

5.5.1 Programy i usługi jako wyjątki w zaporze

Zaporę można również skonfigurować, dodając programy i usługi jako wyjątki.

1. Uruchom interfejs Zapory systemu Windows: kliknij kolejno **Start > Ustawienia > Panel sterowania > Zapora systemu Windows**.
2. Wybierz kartę **Zezwól aplikacji lub funkcji na dostęp przez Zaporę systemu Windows**.
3. Wybierz opcję **Zezwalaj na dostęp innej aplikacji** (jeśli przycisk jest wyszarzony, włącz go, wybierając polecenie **Zmień ustawienia**).
4. Możesz dodać następujące programy:

Programy

Domyślna ścieżka instalacji to `C:\Program Files (x86)\Bosch Sicherheitssysteme\`

Program	Lokalizacja pliku
acsp.exe	[ścieżka instalacyjna]\AccessEngine**AC**\BIN

Program	**Lokalizacja pliku**
ACTA-3.exe	[ścieżka instalacyjna]\AccessEngine**AC**\BIN
BioVerify.exe	[ścieżka instalacyjna]\AccessEngine**AC**\BIN
BioIdentify.exe	[ścieżka instalacyjna]\AccessEngine**AC**\BIN
Bosch.Ace.CredentialManagement.exe	[ścieżka instalacyjna]\Bosch Credential Management
Bosch.Access.MobileAccessBackend.exe	[ścieżka instalacyjna]\Bosch Mobile Access
Bosch.Ace.VisitorManagement.exe	[ścieżka instalacyjna]\Bosch Visitor Management
CalTa-3.exe	[ścieżka instalacyjna]\AccessEngine**AC**\BIN
CDTA-1.exe	[ścieżka instalacyjna]\AccessEngine**AC**\BIN
EMDP.exe	[ścieżka instalacyjna]\AccessEngine**AC**\BIN
KCKemas.exe	[ścieżka instalacyjna]\AccessEngine**AC**\BIN
KCS.exe	[ścieżka instalacyjna]\AccessEngine**AC**\BIN
Loggifier-2.exe	[ścieżka instalacyjna]\AccessEngine**AC**\BIN
PictureServer.exe	[ścieżka instalacyjna]\AccessEngine**AC**\BIN
ReplServer.exe	[ścieżka instalacyjna]\AccessEngine**AC**\BIN
reps.exe	[ścieżka instalacyjna]\AccessEngine**AC**\BIN
TAccExc.exe	[ścieżka instalacyjna]\AccessEngine**AC**\BIN
EMAILSP.exe	[ścieżka instalacyjna]\AccessEngine**AC**\BIN
master-3.exe	[ścieżka instalacyjna]\AccessEngine**AC**\BIN
querySrv-2.exe	[ścieżka instalacyjna]\AccessEngine**AC**\BIN
webSrv-1.exe	[ścieżka instalacyjna]\AccessEngine**AC**\BIN
LicenseGateway.exe	[ścieżka instalacyjna]\AccessEngine**AC**\BIN
DMS.exe	[ścieżka instalacyjna]\AccessEngine**MAC**\BIN
lac.exe	[ścieżka instalacyjna]\AccessEngine**MAC**\BIN

Services

Domyślna ścieżka instalacji to `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System`

Usługa	**Lokalizacja pliku**
Bosch.States.Api	[ścieżka instalacyjna]\States API
Bosch.Map.Api	[ścieżka instalacyjna]\Map API
Bosch.MapView.Api	[ścieżka instalacyjna]\Map View API
Bosch.Events.Api	[ścieżka instalacyjna]\Events API

Usługa	Lokalizacja pliku
Bosch.Alarms.Api	[ścieżka instalacyjna]\Alarms API
Bosch.Ace.IdentityServer	[ścieżka instalacyjna]\Identity Server
Bosch.Ace.Api	[ścieżka instalacyjna]\Access API
Bosch.DialogManager.Api	[ścieżka instalacyjna]\Dialog Manager API
Bosch.Intrusion.Api	[ścieżka instalacyjna]\Intrusion API
Bosch Ace Visitor Management	[ścieżka instalacyjna VM]\
Bosch Ace Visitor Management Client	[ścieżka instalacyjna klienta VM]\
Bosch.OSS-SO	[ścieżka instalacyjna]\OSS-SO
Bosch.OSS-SO.Configurator	[ścieżka instalacyjna]\OSS-SO.Configurator
Bosch.Access.ProductApi.Api	[ścieżka instalacyjna]\ProductApi
Bosch.MUM	[ścieżka-instalacyjna-MUM]\

5.5.2 Mobile Access API

Od wersji Mobile Access 5.2 i nowszych, Credential Management 5.2 i nowszych oraz Visitor Management 5.2 i nowszych interfejs API Mobile Access Backend został podzielony na część dla kanału przedniego i część dla kanału tylnego. Kanał przedni ma komunikować się z telefonami komórkowymi, a kanał tylny — ze środowiskami Credential Management i/lub Visitor Management.
Umożliwia to ustawienie reguł i tras firewalla w celu kontrolowania ruchu sieciowego i wzmocnienia bezpieczeństwa sieci. Podział interfejsu API obejmuje dwa oddzielne numery portów. Oznacza to, że port dla telefonów komórkowych ma numer 5700, a port dla środowisk Credential Management i Visitor Management — 5701.
Zarówno Credential Management, jak i Visitor Management mają dwa osobne ustawienia — odpowiednio dla adresu URL kanału przedniego i adresu URL kanału tylnego. Interfejs użytkownika nazywa je „adresem usługi administracyjnej” (kanał tylny) i „adresem usługi rejestracyjnej” (kanał przedni).
Domyślny port dla „adresu usług administracyjnych” (kanał tylny) to 5701. Zgodnie z regułą firewalla u klienta port ten powinien być skonfigurowany tylko do komunikacji z komputerem, na którym działa backend Credential Management i/lub Visitor Management. W większości przypadków jest to serwer AMS.
Domyślnym portem dla „adresu usługi rejestracji” (kanału przedniego) to 5700. Zgodnie z regułą firewalla u klienta port ten powinien być skonfigurowany tak, by był dostępny dla aplikacji Mobile Access. W wielu scenariuszach ten punkt końcowy byłby dostępny z zewnątrz. Zależy to jednak w dużym stopniu od scenariusza klienta.
Jeśli klient dokonuje aktualizacji z wcześniejszej do najnowszej wersji systemu AMS, należy dostosować ustawienia funkcji Credential Management i Visitor Management. To ustawienie na stronie ustawień jest dostępne w zakresie funkcji Visitor Management i Credential Management dla roli administratora.
Kanał tylny powinien być zabezpieczony tak, aby nie był dostępny publicznie z Internetu ani żadnej nieautoryzowanej sieci.

5.6 Bezpieczeństwo IT

Bezpieczeństwo systemów kontroli dostępu organizacji ma kluczowe znaczenie dla kondycji jej infrastruktury. Bosch rekomenduje ścisłe przestrzeganie wytycznych w zakresie bezpieczeństwa informatycznego wypracowanych w kraju instalacji.
Organizacja obsługująca system kontroli dostępu jest odpowiedzialna co najmniej za następujące zadania:

5.6.1 Obowiązki w zakresie sprzętu

- Zapobieganie nieuprawnionemu fizycznemu dostępowi do składników sieciowych, takich jak porty RJ45.
  - Napastnicy chcący prowadzać ataki typu man-in-the-middle potrzebują fizycznego dostępu.
- Zapobieganie nieuprawnionemu fizycznemu dostępowi do urządzeń kontrolerów AMC2.
- Używanie dedykowanej sieci do systemów kontroli dostępu.
  - Napastnicy mogą uzyskać dostęp z innych urządzeń należących do tej samej sieci.
- Używanie bezpiecznych poświadczeń, takich jak **DESFire** z kodem Bosch czy uwierzytelnianie wieloskładnikowe z odczytem biometrycznym.
- Szybkie rejestrowanie przez aplikację **Setup Access** mobilnych czytników dostępu z modułami BLE (Bluetooth Low Energy). Niezarejestrowane, włączone czytniki są podatne na przejęcie przez podmioty zewnętrzne. Aby tego uniknąć, zapoznaj się z instrukcją instalacji czytnika i uzyskaj informację o sposobie przywrócenia ustawień fabrycznych.
- Zapewnienie mechanizmu awaryjnego i zapasowego zasilania dla systemu kontroli dostępu.
- Śledzenie i wyłączanie poświadczeń, które zgłoszono jako utracone lub zagubione.
- Prawidłowe likwidowanie sprzętu, który nie jest już używany, w szczególności jego resetowanie do domyślnych ustawień fabrycznych oraz usuwanie danych osobowych i informacji dostępowych.

5.6.2 Obowiązki w zakresie oprogramowania

- Prawidłowe utrzymywanie, aktualizowanie i użytkowanie zapory sieciowej systemu kontroli dostępu.
- Monitorowanie alarmów wskazujących, kiedy składniki sprzętowe, np. czytniki kart lub kontrolery AMC2, przechodzą do trybu offline.
  - Alarmy te mogą wskazywać na próbę wymiany komponentów sprzętowych.
- Monitorowanie alarmów sabotażowych wywołanych przez styki elektryczne w urządzeniach kontroli dostępu, np. kontrolerach, czytnikach i szafkach.
- Ograniczanie emisji wykorzystujących protokół UDP wewnątrz dedykowanej sieci.
- Instalowanie aktualizacji, zwłaszcza aktualizacji zabezpieczeń i poprawek, w oprogramowaniu kontroli dostępu.
- Instalowanie aktualizacji, zwłaszcza aktualizacji zabezpieczeń i poprawek, w oprogramowaniu układowym urządzeń.
  - Należy pamiętać, że nawet świeżo dostarczone urządzenia mogą wymagać aktualizacji oprogramowania układowego. Opisy procedur znajdują się w instrukcjach obsługi konkretnych urządzeń.
  - Bosch nie ponosi odpowiedzialności za szkody spowodowane przez produkty włączone do eksploatacji bez aktualnego oprogramowania układowego.
- Szyfrowanie komunikacji protokołem OSDPv2 Secure-Channel.
- Używanie silnych haseł o odpowiednio skomplikowanych wyrażeniach.

- Egzekwowanie *zasady najniższych uprawnień*, która stanowi, iż indywidualni użytkownicy mają dostęp tylko do tych zasobów, których potrzebują do uzasadnionych celów.
- Prawidłowe przypisywanie i skonfigurowanie profili użytkowników dla operatorów pozwala uniknąć sytuacji, w której zwykli operatorzy przypisują wysokie uprawnienia bezpieczeństwa z pominięciem zasady dwóch osób.

5.6.3 Bezpieczna obsługa poświadczeń mobilnych

- Niepozostawianie nieskonfigurowanych czytników Mobile Access bez ochrony.
  - Napastnik może przejąć czytnik na rzecz innego ACS. Wymagałoby to realizacji kosztownej procedury przywracania ustawień fabrycznych.
- Jeśli urządzenie mobilne z poświadczeniami mobilnymi zostanie zgubione lub skradzione, należy je potraktować tak, jak zgubioną kartę: należy je zablokować lub usunąć wszystkie jego mobilne poświadczenia tak szybko, jak to możliwe.
- W środowiskach wymagających wysokiego poziomu bezpieczeństwa Bosch zaleca uwierzytelnianie dwuskładnikowe. Wymaga to odblokowania urządzenia mobilnego przed użyciem go jako poświadczenia.
- Przywrócenie zawartości telefonu z kopii zapasowej nie powoduje przywrócenia poświadczeń mobilnych. Jeśli użytkownik mobilnego poświadczenia otrzyma nowe urządzenie, musisz ponownie wysłać wszystkie obowiązujące zaproszenia.
- Niektórzy napastnicy mogą próbować użyć zagłuszacza do zablokowania komunikacji z czytnikami dostępu mobilnego. Pracownicy, których prawo dostępu jest niezbędne, powinni nosić zapasowo poświadczenia fizyczne.
  - W roli kopii zapasowej do rozwiązania Mobile Access należy używać wyłącznie kart fizycznych z bezpiecznym kodowaniem (np. z kodem Bosch).
- Chroń serwer Mobile Access przed nieautoryzowanym fizycznym dostępem. Firma Bosch zaleca dodatkowe środki, takie jak na przykład szyfrowanie dysku funkcją BitLocker.
- Zabezpiecz serwer Mobile Access przed atakami typu Blokada Usług (DoS). Serwer musi być częścią chronionego środowiska sieciowego, które zapewnia zabezpieczenia — takie jak ogranicznik prędkości połączeń przychodzących.
- Traktuj kody QR z zaproszeniem dla instalatora jako poświadczenia administratora. Skradziony telefon instalatora z aktywnymi poświadczeniami może umożliwić napastnikowi złośliwą rekonfigurację czytników Mobile Access.
  - Wyślij zaproszenia do instalatorów bezpośrednio przed konfiguracją czytnika i upewnij się, że po zakończeniu konfiguracji poświadczenia zostały usunięte.
  - Zamiast zaproszeń wysyłanych e-mailem użyj funkcji skanowania kodów QR z ekranu. Upewnij się, że instalator natychmiast wprowadza poświadczenia.

5.7 Prywatność i ochrona danych w firmie Bosch

Wstęp

We wszystkich procesach biznesowych, zgodnie z obowiązującymi wymogami przepisami prawa, zapewniamy ochronę prywatności, ochronę danych osobowych i bezpieczeństwo informacji biznesowych. W technicznym i organizacyjnym zakresie, w tym w szczególności w ramach ochrony przed nieuprawnionym dostępem i utratą danych, stosujemy odpowiednie standardy odzwierciedlające aktualny stan wiedzy i uwzględniające powiązane ryzyka. Podczas opracowywania produktów Bosch i nowych modeli biznesowych dbamy o to, aby już na wczesnym etapie uwzględniać wymogi prawne dotyczące ochrony danych i bezpieczeństwa informacji.

Poza działem zgodności i działem prawnym głównym kontaktem w przypadku pytań dotyczących prawidłowego postępowania z danymi jest inspektor bezpieczeństwa danych.

Przetwarzanie danych osobowych w aplikacji Mobile Access i w backendzie oprogramowania Mobile Access

- Kategorie danych osobowych
  - Aplikacje Mobile Access zawierają dane osobowe. Są nimi informacje o numerze karty służącej do uzyskiwania dostępu do czytników. Dostęp do rzeczywistych danych prawdziwych osób jest możliwy tylko przez dodatkowe wykorzystanie programów AMS, ACE lub Visitor Management.
  - Procedura rejestracji instalatora w menu **Settings** (Ustawienia) nie wymaga przechowywania danych osobowych. Niemniej jednak opcjonalnie mogą być przechowywane niektóre informacje o użytkowniku, takie jak adresy e-mail.
  - Serwer backendu oprogramowania Mobile Access w celu zarządzania danymi uwierzytelniającymi musi przechowywać dane osobowe.
- Transfer danych
  - W celu kontroli dostępu do czytników poświadczenia są przekazywane między backendem, aplikacją Mobile Access i systemem Visitor Management.
- Rejestrowanie danych
  - Aplikacja Mobile Access prowadzi dzienniki techniczne. Te dzienniki są przechowywane lokalnie na urządzeniu mobilnym i w razie potrzeby mogą być wysyłane do stron trzecich, takich jak pomoc techniczna.
  - Serwer backendowy przechowuje ponadto dzienniki techniczne. Dane są przechowywane lokalnie w systemie serwerowym.
  - Domyślnie serwer backendowy nie usuwa automatycznie plików dziennika. Można jednak skonfigurować automatyczne usuwanie na podstawie pozostałej pojemności pamięci lub na podstawie harmonogramu czasowego.

Co zrobiliśmy, aby nasz produkt skutecznie chronił dane?

Systemy kontroli dostępu firmy Bosch zarządzają prawami dostępu posiadanymi przez inne osoby. Aby chronić te osoby, firma Bosch podejmuje działania mające na celu zintegrowanie wymagań RODO z rozwojem produktu, zgodnie z zasadą „privacy by design”.

- Stosujemy najnowocześniejsze szyfrowanie.
- Dane poświadczeń są pseudonimizowane.
- Użytkownik aplikacji do otrzymania wirtualnych poświadczeń za pośrednictwem kodu QR lub poczty nie musi podawać danych osobowych.
- Możliwe jest usunięcie poświadczeń z aplikacji Mobile Access, z podstawowych systemów kontroli dostępu oraz z aplikacji pomocniczych, takich jak Visitor Management i Credential Management.
- Poświadczenia mogą w każdej chwili uprawnienia zostać zablokowane przez operatorów podstawowych systemów kontroli dostępu oraz aplikacji pomocniczych.
- Dane telemetryczne są z założenia anonimizowane.
- Pliki dziennika nie są przekazywane z urządzeń mobilnych do innych podmiotów, takich jak wsparcia technicznego, bez aktywnej zgody i współpracy użytkownika.
- W głównym systemie kontroli dostępu można skonfigurować zaplanowane automatyczne usuwanie plików dziennika.
- Bosch nie wymaga rejestracji w sklepie z aplikacjami ani w samej aplikacji. Sklep z aplikacjami nie przekazuje firmie Bosch żadnych danych osobowych.
- Aplikacja wymaga do działania Bluetooth, ale wysyła monit o jego ręczną aktywację.

Masz dodatkowe pytania?

Aby uzyskać więcej informacji na temat prywatności danych, zapoznaj się z informacją o prywatności danych w aplikacji Mobile Access lub skontaktuj z zespołem firmy Bosch.

5.8 Autoryzacje o wysokim poziomie bezpieczeństwa

5.8.1 Zasada dwóch osób

Od wersji AMS 5.5 możliwe jest włączenie zasady dwóch osób. Głównym celem tej funkcji jest zwiększenie bezpieczeństwa przy nadawaniu uprawnień poprzez dodanie osoby zatwierdzającej. W Credential Management operator może przypisać do jednej osoby jedną lub więcej autoryzacji. W przeciwieństwie do typowego przypisania autoryzacji, w którym jest ona natychmiast przypisywana do osoby, autoryzacje z włączoną zasadą dwóch osób są wysyłane jako żądanie do innego operatora, który ma prawo zatwierdzić lub odrzucić to żądanie. Zapobiegnie to błędnym przypisaniom, gdyż może służyć do ochrony uprawnień do obszarów wrażliwych, czyli uprawnień, które można przypisać pracownikowi tylko wtedy, gdy zgodzi się na to dwóch operatorów (osoba żądająca i osoba zatwierdzająca).

5.8.2 Konfigurowanie autoryzacji o wysokim poziomie bezpieczeństwa

Aby możliwe było wprowadzenie zasady dwóch osób, należy zrealizować następujące wymagania:

– AMS zaktualizowany do najnowszej wersji.
– Bycie administratorem AMS.

Tworzenie uprawnień dostępu z zasadą dwóch osób

W głównym systemie kontroli dostępu:

Ścieżka w oknie dialogowym

Menu główne AMS > **System data** > **Authorizations** (Dane systemowe > Autoryzacje)

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

   Alternatywnie kliknij przycisk **Kopiuj**  , aby utworzyć nową autoryzację na podstawie istniejącej.
2. Nadaj uprawnieniu niepowtarzalną nazwę.
3. (Opcjonalnie) Wprowadź opis.
4. (Opcjonalnie) Wybierz model czasowy mający sterować tym uprawnieniem.
5. (Opcjonalnie) Wybierz z listy ustawienie opcji **Inactivity limit** (Limit braku aktywności).
6. (Obowiązkowe) Przydziel co najmniej jedno ustawienie **Entrance** (Wejście).
7. Zaznacz pole wyboru **Approval required** (Wymagana akceptacja) — włącza to zasadę dwóch osób.
8. Kliknij przycisk Zapisz  , aby zapisać autoryzację.

Uwaga!

Rekomendacje bezpieczeństwa

Ta funkcja jest dostępna tylko dla Credential Management. W systemie AMS administratorzy muszą prawidłowo przypisać i skonfigurować profile użytkowników dla operatorów, tak aby okna dialogowe były niedostępne. Pozwoli to uniknąć sytuacji, w której zwykli operatorzy przypisują wysokie uprawnienia bezpieczeństwa z pominięciem zasady dwóch osób.

Więcej informacji można znaleźć w najnowszej wersji podręcznika *konfiguracji i obsługi* oprogramowania *Access Management System*.

6 Obsługa

6.1 Omówienie ról użytkowników

Możliwości użytkowników Credential Management są określone przez ich profile użytkownika w systemie ACS:

Typ użytkownika	Wykonywane czynności
Administrator	Konfigurowanie ustawień globalnych Dostosowywanie działania narzędzia i interfejsu użytkownika plus Wszystkie przypadki użycia przynależne dla operatora
Operator	Przydzielanie i cofanie przydziału fizycznych kart dostępu oraz poświadczeń wirtualnych w ramach dostępu mobilnego
Zasada dwóch osób: osoba żądająca	Żądanie autoryzacji o wysokim poziomie bezpieczeństwa
Zasada dwóch osób: osoba zatwierdzająca	Zatwierdzanie lub odrzucanie autoryzacji o wysokim poziomie bezpieczeństwa Usuwanie normalnych autoryzacji

Patrz

– *Tworzenie użytkowników Credential Management w ACS, Strona 26*

6.2 Korzystanie z pulpitu nawigacyjnego

Pulpit nawigacyjny jest ekranem głównym — centralnym oknem dialogowym prowadzącym do innych okien dialogowych.

Ogólne informacje o spisie pracowników

Każdy wiersz w tabeli reprezentuje osobę. Są to pracownicy wewnętrzni lub zewnętrzni, którzy wymagają poświadczeń pozwalających im na dostęp do pomieszczeń.

- Możesz wybierać osoby pojedynczo albo wybrać kilka osób jednocześnie, używając mechanizmów z klawiaturą i myszą:
  - Naciśnij klawisz Ctrl i kliknij, aby wybrać jeden z wybranych wierszy.
  - Naciśnij klawisz Shift i kliknij już wybrany wiersz, aby usunąć go z zaznaczenia.
  - Naciśnij klawisze Shift + Ctrl i kliknij, aby wybrać kilka kolejnych wierszy.
- Możesz dodawać nowe osoby do tabeli
- Możesz przypisywać poświadczenia i cofać ich przypisanie, klikając przyciski działań
  - Przypisywanie poświadczenia fizycznego
  - Przypisywanie poświadczenia wirtualnego (dla dostępu mobilnego)
  - Edytuj dane osoby
- Możesz wyeksportować wszystkie dane do pliku CSV lub XLSX. Jeśli potrzebne są tylko określone dane, użyj funkcji filtrowania. Nie ma możliwości wyeksportowania żądanych danych poprzez ich wybranie. Do pliku CSV lub XLSX można wyeksportować tylko aktualnie odfiltrowane linie.

Funkcje pulpitu nawigacyjnego

Etykieta	Funkcja
(1) N **pozycji**	Łączna liczba N osób (każda osoba to wiersz w tabeli).
(2) **Wyszukaj**	Wyszukiwanie dowolnego tekstu wśród osób w tabeli.
(3) 	Wybranie wszystkich pozycji z listy.
(4)  **Usuń**	Usunięcie wybranych pozycji.
(5)  **Najnowsze**	Wyświetlanie najnowszych osób dodanych do tabeli.
(6)  **Resetuj**	Przywracanie domyślnego widoku tabeli i domyślnych wartości wszystkich filtrów.
(7)  **Cofnij przypisanie karty**	Otwieranie okna dialogowego, w którym można odebrać przydzielone karty za pomocą podłączonego czytnika rejestracji.
(8) **. . .**	Kliknij wielokropek, aby wyświetlić menu umożliwiające wyeksportowanie osób lub dokumentów do różnych formatów plików, np. `CSV` oraz `.XLSX`.. Należy pamiętać, że z przyczyn bezpieczeństwa danych eksport można przeprowadzać tylko wtedy, gdy klient pracuje w zabezpieczonym połączeniu HTTPS z certyfikatem.
(9) 	Otwarcie okna dialogowego umożliwiającego utworzenie nowej osoby

Kolumny pulpitu nawigacyjnego

Kolumna	Opis
Imię i nazwisko	Kliknięcie hiperłącza spowoduje wyświetlenie szczegółowych informacji o osobie.
E-mail	
Dział	
Pozycja	
Firma	
Numery kart	Numery kart przydzielonych tej osobie.
Działania	Patrz osobna tabela poniżej

Czynności do wykonania na rekordach personelu w tabeli pulpitu nawigacyjnego

Ikona	Działania
	**Przypisanie** jednej lub więcej kart fizycznych do osoby
	**Przypisywanie** osobie poświadczenia wirtualnego (dla dostępu mobilnego)
	**Edycja** danych osoby. Zmiany są propagowane do systemu ACS. Zmiany wprowadzone do systemu ACS są propagowane do aplikacji CredMgmt.

6.2.1 Strona przeglądowa osoby

Kliknij imię i nazwisko danej osoby. Pojawi się okno dialogowe z jej danymi osobowymi. W tym oknie dialogowym znajdują się pola, w których można wyświetlać i edytować główne informacje o osobie. Jednak podstawowe dane osobowe są stale wyświetlane po lewej stronie okna dialogowego.

Informacje o wpisach na czarnej liście, jeśli istnieją, pojawią się na dole tej kolumny z podstawowymi danymi osobowymi.

Wskazówka: w polu **Tytuł** obok opcji dostępnych na liście rozwijanej można wpisać dowolny tekst.

W tym samym oknie dialogowym są trzy karty z oddzielnym widokiem **View (Szczegóły), Credentials (Poświadczenia), Authorizations (Uprawnienia)**.

W Credential Management jeśli osoba jest zablokowana, pojawi się pomarańczowe powiadomienie z napisem **Blacklisted** (Czarna lista). Pojawi się także przyczyna wpisania na czarną listę i nazwisko osoby, która to zrobiła.

Administrator i operator z właściwymi uprawnieniami może zablokować daną osobę, klikając przycisk **Blacklist (Czarna lista).**

– Otworzy się okno z ostrzeżeniem

1. Kliknij przycisk **Yes** (Tak).
2. W kreatorze **powodów** wpisz powód i kliknij **Save** (Zapisz) > OK.

Uwaga: osoba dopisana do czarnej listy zachowuje przypisane uprawnienia. Nie będzie jednak w stanie otworzyć wejścia/drzwi.

Aby usunąć osobę z czarnej listy, kliknij przycisk **X Remove from blacklist** (X Usuń z czarnej listy).
Skonfiguruj prawidłowo uprawnienia. Więcej informacji na temat uprawnień użytkownika można znaleźć w *podręczniku konfiguracji i obsługi oprogramowania Access Management System*.

Details (Szczegóły)
Na tej karcie możliwe jest wprowadzenie danych osobowych, które nie muszą być stale widoczne.

PIN
Na karcie **Details** (Szczegóły) można przeglądać i zmieniać kody PIN (weryfikacyjne kody PIN)[1] posiadacza karty. Podczas zmiany kodu PIN możliwe jest określenie daty jego wygaśnięcia.
Uwaga: jeśli kod PIN ulegnie zmianie lub zmienią się jego ustawienia, konieczne będzie potwierdzenie zmian przez ponowne wpisanie kodu.
Jeżeli dla poświadczeń wybranej osoby istnieje co najmniej jedna blokada **kodu PIN**, na dole kolumny z podstawowymi danymi osobowymi pojawi się odpowiednia informacja. Kliknięcie przez operatora tego powiadomienia powoduje wybranie zakładki **Credentials** (Poświadczenia) i uzyskanie przez operatora dodatkowych informacji na temat blokady **kodu PIN**.
Pamiętaj, że jeśli na karcie wystąpi błąd sprawdzania poprawności, wybranie innej strony przed jego usunięciem nie będzie możliwe.
[1]Credential Management obsługuje tylko standardowy kod PIN. Identyfikacyjne kody PIN ORAZ oddzielne kody PIN IDS/zazbrojenia nie są obsługiwane.
Więcej informacji na temat **kodów PIN** można znaleźć w podręczniku *konfiguracji i obsługi oprogramowania Access Management System*.

Poświadczenia
Na tej karcie zakładce można przypisać kartę fizyczną, klikając przycisk **Read card** (Odczytaj kartę), lub przypisać poświadczenie mobilne, klikając przycisk **Add mobile access** (Dodaj dostęp mobilny). Aby uzyskać więcej informacji, przejdź do sekcji *Przypisywanie poświadczeń mobilnych* i *Przypisywanie poświadczeń fizycznych*.
Uwaga: jeśli na ikonie telefonu pojawi się pomarańczowa kropka, oznacza to, że dane uwierzytelniające znajdują się już na telefonie komórkowym, ale wymagają zatwierdzenia z backendu dostępu mobilnego. Kropka zmieni kolor na zielony po tym zatwierdzeniu.

Uprawnienia
Na tej karcie można przejrzeć wszystkie nadane uprawnienia oraz je zmienić. Więcej informacji znajduje się w sekcji *Przypisywanie informacji ze strony z danymi osobowymi*.
Zwracamy uwagę, że w dowolnym oknie dialogowym z kartami przycisk **Save & Close** (Zapisz i zamknij) przekierowuje do okna dialogowego **Pulpit nawigacyjny** (Dashboard).

6.3 Przypisywanie uprawnień

Przypisywanie uprawnień ze strony z danymi osobowymi.
– W oknie dialogowym pulpitu nawigacyjnego pojawi się lista osób.
1. Kliknij imię i nazwisko osoby.

– Pojawi się okno dialogowe z danymi o osobie.
1. W prawym górnym rogu okna dialogowego kliknij kartę **Authorizations (Autoryzacje)**.

2. Aby przypisać nową autoryzację, kliknij opcję **Modify authorizations** (Modyfikuj autoryzację).

Pojawi się kreator z listą wszystkich autoryzacji. Wszystkie autoryzacje zostały wcześniej skonfigurowane w systemie Access Management System. Od tego kroku zacznij wybierać, które uprawnienia chcesz przypisać.

1. Kliknij  > **Confirm** > **Save** (Potwierdź > Zapisz).

Uwaga: autoryzacje o wysokim poziomie bezpieczeństwa, tj. z włączoną funkcją Zasada dwóch osób, są wyświetlane z ikoną  .

Zostanie otwarte okno dialogowe pulpitu nawigacyjnego. Jeżeli osobie nadano zwykłą autoryzację, można to sprawdzić, klikając jej imię i nazwisko osoby i przechodząc na kartę **Authorizations** (Uprawnienia).
Jeśli nadano autoryzację z zasadą dwóch osób, wynik jest inny. Autoryzacja nie będzie aktywna natychmiast po zapisaniu, a jedynie zostanie zażądana. W kolumnach **Authorizations** (Autoryzacje) i **Actions (Działania)** można sprawdzić, kto zażądał autoryzacji. Na karcie **Authorizations** (Autoryzacje) autoryzacje, dla których włączono zasadę dwóch osób, mogą być zatwierdzone lub odrzucone. Możliwe jest sprawdzenie, kto i kiedy złożył żądanie o potwierdzenie autoryzacji, ustawiając kursor myszy nad jej nazwą. Pojawi się podpowiedź.

W zależności od typu autoryzacji oraz roli i uprawnień użytkownika, wyświetlane mogą być następujące przyciski **działań**:

Żądanie
Retract (Cofnij): anuluj moje własne żądania przypisania autoryzacji, które nie zostało jeszcze zatwierdzone.
Approve (Zatwierdź): zatwierdź żądanie nadania autoryzacji przez innego operatora.
Deny (Odrzuć): odrzuć żądanie przypisania autoryzacji przez innego operatora.
Remove (Usuń): usuń przypisaną autoryzację. Dotyczy to autoryzacji normalnych i o wysokim poziomie bezpieczeństwa.

Uwaga: samo kliknięcie przycisku działania nie uruchamia go. Należy zawsze kliknąć przycisk **Save** (Zapisz).
Aby uzyskać więcej informacji, zapoznaj się z sekcją *Przegląd ról użytkowników*.

W systemie AMS **profile użytkowników** powinny być odpowiednio skonfigurowane z dostępnymi uprawnieniami dla zasady dwuosobowej:
– Administrator
– Operator
– Zasada dwóch osób: osoba żądająca
– Zasada dwóch osób: osoba zatwierdzająca

Więcej informacji na temat konfiguracji **profili użytkownika** można znaleźć w najnowszej wersji podręcznika *konfiguracji i obsługi* oprogramowania Access Management System.

Oczekujące żądania autoryzacji

Operator z uprawnieniami do zatwierdzania lub wnioskowania oraz administrator wybrać z menu opcję **Authorization Requests** (Żądania autoryzacji). W tym oknie dialogowym można wyświetlić wszystkie **oczekujące żądania autoryzacji** bez konieczności przechodzenia do każdej nazwy osoby.
Operator może w tym oknie zatwierdzać żądania, a administrator może wycofywać autoryzacje. Operator żądający może jedynie przeglądać oczekujące autoryzacje. Operator bez uprawnień osoby zatwierdzającej i żądającej nie może wyświetlić tego okna dialogowego.
Uwaga: samo kliknięcie przycisku działania nie uruchamia go. Kliknięty przycisk działania zmienia kolor na szary. Należy jeszcze kliknąć przycisk **Save** (Zapisz).

6.4 Przydzielanie poświadczeń fizycznych

Wymagania wstępne
Zdecydowanie zalecamy przypisanie nowych poświadczeń nowemu personelowi przy użyciu nowej karty, drukarki kart i czytnika rejestrującego.

Przypisywanie karty (wymaga czytnika rejestracji)
Procedura
Przypisanie karty jest możliwe bezpośrednio z pulpitu nawigacyjnego lub ze strony przeglądowej osoby.
Na **pulpicie nawigacyjnym**:
1. Przygotuj fizyczną kartę dostępu do przyłożenia do czytnika rejestracji.
2. Wybierz wiersz osoby i kliknij 
3. Postępuj zgodnie z instrukcjami posługiwania się czytnikiem rejestracji wyświetlanymi w wyskakującym oknie.

Ze strony przeglądowej osoby:
1. Na **pulpicie nawigacyjnym** wybierz imię i nazwisko osoby. Pojawi się strona przeglądowa tej osoby.
2. wybierz kartę **Credential** > **Read Card** (Poświadczenia > Odczyt karty).

Przydzielanie karty w edytorze poświadczeń (wymaga czytnika rejestracji)

1. W pulpicie nawigacyjnym, w tabeli osób wybierz osobę i kliknij przycisk  . Umożliwi to zmodyfikowanie poświadczeń tej osoby.
2. Kliknij przycisk **Read card** (Odczytaj kartę) i postępuj zgodnie z instrukcjami w oknie dialogowym dotyczącymi korzystania z czytnika rejestracji.
– W razie potrzeby powtórz ostatnie kroki, aby przypisać kolejne karty.
3. Kliknij przycisk **Save** (Zapisz). Informacje o osobie i jej przydziałach kart zostaną zapisane.

6.5 Przydzielanie poświadczeń mobilnych

Wymagania wstępne
– Aplikacja Mobile Access jest zainstalowana i skonfigurowana w systemie.
  – Odpowiednie instrukcje znajdują się w części tego dokumentu dotyczącej instalacji.

– Osoba, który odbiera autoryzację, ma zainstalowany program Mobile Access i uruchomiła go na swoim urządzeniu.
  – Odpowiednie instrukcje znajdują się w części tego dokumentu dotyczącej instalacji.

Procedura

Możliwe jest przypisanie poświadczeń mobilnych bezpośrednio z pulpitu nawigacyjnego lub ze strony przeglądowej osoby.

Na **pulpicie nawigacyjnym**:

1. Wybierz wiersz osoby, która ma otrzymać mobilne poświadczenia.
2. W wybranym wierszu kliknij  .

Ze strony przeglądowej osoby:

1. Na **pulpicie nawigacyjnym** wybierz imię i nazwisko osoby. Pojawi się strona przeglądowa tej osoby.
2. Wybierz kartę **Credential** > **Add mobile access** (Poświadczenia > Dodaj dostęp mobilny).

Postępuj zgodnie z poniższymi instrukcjami:

1. Wybierz jedną z dużych ikon z dostępnymi opcjami:

– **kod QR**
  lub
– **e-mail z zaproszeniem**

2. W przypadku wybrania opcji z **kodem QR**:

– System wyświetla kod QR.
– Osoba skanuje kod QR na swoim urządzeniu mobilnym za pomocą aplikacji Mobile Access.
– Aby poświadczenia zaczęły działać, musisz **zatwierdzić** wizytę.
  Odpowiednie instrukcje znajdują się w rozdziale Zatwierdzanie i odrzucanie wniosków o wizyty
– Urządzenie mobilne z uruchomioną aplikacją może działać jak fizyczna karta dostępu.

3. W przypadku wybrania opcji z **e-mailem z zaproszeniem**:

– Domyślnie program wybiera adres e-mail zdefiniowany dla wybranej osoby. W razie potrzeby wprowadź alternatywny adres e-mail.
– System wyśle wiadomość e-mail na wybrany adres.
– Osoba odbiera e-mail na swoim urządzeniu mobilnym z uruchomioną aplikacją Mobile Access.
– Odbiorca wiadomości wywołuje umieszczony w niej odnośnik.
– Aby poświadczenia zaczęły działać, musisz **zatwierdzić** wizytę.
  Odpowiednie instrukcje znajdują się w rozdziale Zatwierdzanie i odrzucanie wniosków o wizyty
– Urządzenie mobilne z uruchomioną aplikacją może działać jak fizyczna karta dostępu.

Procedura w oknach edycji

1. Wybierz wiersz osoby, która ma otrzymać mobilne poświadczenia.
2. W wybranym wierszu kliknij  .

– Zostanie otwarte okno dialogowe edycji.

3. W programie VisMgmt kliknij przycisk **Next** (Dalej), aby przejść do ekranu **szczegółów wizyty**.
4. Kliknij przycisk **Add** (Dodaj).**Mobile Access**

5. Wybierz jedną z dużych ikon z dostępnymi opcjami:
– **kod QR**
lub
– **e-mail z zaproszeniem**
6. W przypadku wybrania opcji z **kodem QR**:
– System wyświetla kod QR.
– Osoba skanuje kod QR na swoim urządzeniu mobilnym za pomocą aplikacji Mobile Access.
– Aby poświadczenia zaczęły działać, musisz **zatwierdzić** wizytę.
Odpowiednie instrukcje znajdują się w rozdziale Zatwierdzanie i odrzucanie wniosków o wizyty
– Urządzenie mobilne z uruchomioną aplikacją może działać jak fizyczna karta dostępu.
7. W przypadku wybrania opcji z **e-mailem z zaproszeniem**:
– Domyślnie program wybiera adres e-mail zdefiniowany dla wybranej osoby. W razie potrzeby wprowadź alternatywny adres e-mail.
– System wyśle wiadomość e-mail na wybrany adres.
– Osoba odbiera e-mail na swoim urządzeniu mobilnym z uruchomioną aplikacją Mobile Access.
– Odbiorca wiadomości wywołuje umieszczony w niej odnośnik.
– Aby poświadczenia zaczęły działać, musisz **zatwierdzić** wizytę.
Odpowiednie instrukcje znajdują się w rozdziale Zatwierdzanie i odrzucanie wniosków o wizyty
– Urządzenie mobilne z uruchomioną aplikacją może działać jak fizyczna karta dostępu.

Patrz
– *Instalowanie programu Mobile Access, Strona 13*
– *Instalowanie aplikacji Mobile Access, Strona 22*

6.6 Cofanie przydzielania poświadczeń

Odbieranie karty w pulpicie nawigacyjnym (wymaga czytnika rejestracji)
1. Odbierz fizyczną kartę od posiadacza i przygotuj ją do przyłożenia do czytnika rejestracji.
2. Na pasku narzędzi kliknij opcję **Odbierz kartę**. 
3. Postępuj zgodnie z instrukcjami posługiwania się czytnikiem rejestracji wyświetlanymi w wyskakującym oknie.

Cofanie przydzielenia karty w edytorze poświadczeń
1. Aby zmodyfikować właściciela karty, w pulpicie nawigacyjnym, w głównej tabeli zaznacz wiersz i kliknij przycisk  .
2. W oknieedycji, w kolumnie **Employee cards** (Karty pracowników) kliknij przycisk  znajdujący się obok karty, której przydział chcesz cofnąć, a następnie potwierdź działanie w wyskakującym oknie.
Powtarzaj tę czynność aż do cofnięcia przydziału wszystkich potrzebnych kart.

3. Kliknij przycisk **Zapisz**, co spowoduje zapisanie obecnej wizyty z przydziałami kart.

6.7 Autoryzacja instalatorów czytników Mobile Access

Wstęp

Instalatorzy czytników Mobile Access w celu wyszukania i skonfigurowania czytników z wykorzystaniem technologii BLE potrzebują użyć aplikacji Bosch Setup Access. Upoważnieni operatorzy aplikacji **Credential Management** i **Visitor Management** mogą wysyłać wirtualne poświadczenia do aplikacji instalatora, upoważniając go do pracy. W tej części opisano tę procedurę.

Wymagania wstępne

- Aplikacja Mobile Access jest zainstalowana i skonfigurowana w systemie.
  - Odpowiednie instrukcje znajdują się w części tego dokumentu dotyczącej instalacji.
- Upewnij się, że instalator, który odbiera autoryzację, ma zainstalowany program Bosch Setup Access i uruchomił go na swoim urządzeniu.
  - Odpowiednie instrukcje znajdują się w części tego dokumentu dotyczącej instalacji.

Procedura

1. W menu głównym kliknij przycisk  , aby otworzyć okno dialogowe **Installer onboarding** (Rejestracja instalatora).

2. Kliknij przycisk **Add** (Dodaj), aby dodać instalatora do listy, lub  , aby usunąć istniejącego instalatora.
- Zostanie wyświetlone wyskakujące okno **Add installer** (Dodawanie instalatora).
3. W oknie **dodawania instalatora** wpisz potrzebne informacje, na przykład:
- imiona i nazwiska, nazwę firmy, adres e-mail, numer telefonu
- Uwaga: kliknij  , aby później zmodyfikować szczegóły wybranego instalatora.
4. Kliknij przycisk **Dalej>**.
5. Wybierz jedną z dużych ikon z dostępnymi opcjami:
- **kod QR**
  lub
- **e-mail z zaproszeniem**
6. W przypadku wybrania opcji z **kodem QR**:
- System wyświetla kod QR.
- Osoba skanuje kod QR na swoim urządzeniu mobilnym za pomocą aplikacji Mobile Access.
- Zamyka to proces rejestracji instalatora.
- Dzięki temu urządzenie mobilne z uruchomioną aplikacją może wyszukiwać czytniki Mobile Access i konfigurować je za pomocą technologii BLE.
7. W przypadku wybrania opcji z **e-mailem z zaproszeniem**:
- Domyślnie program wybiera adres e-mail zdefiniowany dla wybranej osoby. W razie potrzeby wprowadź alternatywny adres e-mail.
- System wyśle wiadomość e-mail na wybrany adres.
- Osoba odbiera e-mail na swoim urządzeniu mobilnym z uruchomioną aplikacją Bosch Setup Access.
- Odbiorca wiadomości wywołuje umieszczony w niej odnośnik.
- Zamyka to proces rejestracji instalatora.

– Dzięki temu urządzenie mobilne z uruchomioną aplikacją może wyszukiwać czytniki Mobile Access i konfigurować je za pomocą technologii BLE.

Ponowne wysyłanie zaproszeń

1. W oknie dialogowym rejestracji instalatora wybierz żądanego instalatora
2. Kliknij  w tym samym wierszu, aby ponownie wysłać autoryzację do wybranego instalatora za pomocą kodu QR lub wiadomości e-mail.
   UWAGA: autoryzację można wysłać ponownie tylko wtedy, gdy instalator jeszcze jej nie aktywował.

6.7.1 Resetowanie czytników Mobile Access

Aby umożliwić ponowną konfigurację czytników dostępu, może okazać się konieczne przywrócenie domyślnych ustawień fabrycznych.
Taka sytuacją zachodzi na przykład wtedy, gdy instalator musi ponownie skonfigurować czytniki Mobile Access skonfigurowane wcześniej dla innego obiektu.
Opis sposobu resetowania czytnika za pomocą przełączników DIP znajduje się w instrukcji obsługi czytnika LECTUS select.

6.8 Używanie aplikacji Mobile Access na urządzeniach mobilnych

UWAGA: używanie aplikacji Bosch zostało Mobile Access szczegółowo opisane w oddzielnych **skróconych instrukcjach obsługi** dla różnych grup użytkowników. Dokumenty te są dostępne w internetowym katalogu produktów firmy Bosch.

Wstęp

Do obsługi systemu Mobile Access Bosch udostępnia następujące aplikacje

– Bosch Mobile Access: aplikacja do przechowywania wirtualnych poświadczeń i przesyłania ich przez Bluetooth do tych czytników, które są skonfigurowane do pracy z systemem Mobile Access. Czytnik następnie przyznaje dostęp lub odmawia go w zależności od tego, czy przechowywane poświadczenia na to pozwalają.
– Bosch Setup Access: aplikacja instalacyjna do skanowania i konfigurowania czytników przez Bluetooth.

Upoważnieni operatorzy Visitor Management i Credential Management mogą wysyłać wirtualne dane uwierzytelniające zarówno dla aplikacji posiadacza karty, jak i aplikacji instalatora.

Uwaga!
WAŻNE: nie należy jednocześnie używać aplikacji posiadacza karty i aplikacji instalatora. Upewnij się, że gdy aplikacja posiadacza karty jest w użyciu nikt nie używa aplikacji instalatora i odwrotnie.

6.8.1 Ustawianie progów RSSI w aplikacji Setup Access

Wstęp

Próg RSSI i zasięg BLE w kontekście aplikacji Bosch Mobile Access można uznać za mniej więcej równoważne pojęcia.

Mobilne urządzenia dostępowe przesyłają sygnały BLE do pobliskich czytników. Ważnym elementem konfiguracji czytników jest ustawienie progu RSSI dla każdego czytnika. Próg to minimalna siła sygnału BLE mierzona w dBm, którą czytnik (R) ma zaakceptować jako żądanie kontroli wejścia. Wszystkie słabsze sygnały BLE mają być ignorowane.

Wartości RSSI mogą się znacznie różnić w zależności od wielu czynników, w tym rodzaju urządzenia nadawczego, poziomu naładowania baterii oraz materiału i grubości pobliskich ścian. Nie ma liniowej zależności między wartością RSSI a odległością między nadajnikiem a odbiornikiem.

Dlatego aplikacja Setup Access zapewnia narzędzie do pomiaru RSSI czytnika z aktualnej pozycji urządzenia mobilnego. Poniższa procedura opisuje sposób korzystania z tego narzędzia.

Po znalezieniu odpowiedniej wartości progowej dla zakresu BLE użyj aplikacji Setup Access, aby zapisać tę wartość w konfiguracji czytnika.

Procedura

Skonfiguruj wartość opcji **BLE range** (Zasięg BLE), używając jednej z poniższych opcji, A lub B:

A: wykorzystanie wartości RSSI odzwierciedlonych przez czytnik

1. Ustaw się przed czytnikiem, w miejscu, w którym spodziewasz się, że znajdzie się użytkownik uwierzytelniający się urządzeniem mobilnym.
2. Stuknij polecenie **Check and use current range** (Sprawdź bieżący zakres i użyj go).

– Pojawi się wyskakujące okienko. Stuknij przycisk **OK**.

3. Pojawi się wartość RSSI.

– Zalecane: powtórz ten krok kilka razy z tego samego miejsca, aby uzyskać wrażenie stopnia zróżnicowania postrzeganej siły sygnału.

4. Po znalezieniu odpowiedniej wartości progowej, dotknij polecenia **Save** (Zapisz).

B: ręczne ustawianie progu RSSI

1. Wprowadź wartość progu RSSI.
   Poniżej pokazano tabelę z typowymi progami
2. Stuknij przycisk **Save** (Zapisz).

Typowe wartości progów (w przybliżeniu):

Przewidywana odległość od urządzenia mobilnego do czytnika	Sugerowany próg RSSI
Bliska (5–10 cm)	–30 – –40 dBm
Średnia (0,5–2 m)	–50 – –60 dBm
Daleka (>2 m)	–70 – –90 dBm

Uwaga!
Wartości RSSI mogą się znacznie różnić w zależności od wielu czynników, w tym rodzaju urządzenia nadawczego, poziomu naładowania baterii oraz materiału i grubości pobliskich ścian.

Słowniczek

ACS

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

BLE

Bluetooth Low Energy to technologia sieci bezprzewodowej, która zapewnia podobny zasięg komunikacji jak Bluetooth, ale przy niższym zużyciu energii.

FQDN

Pełna jednoznaczna nazwa domenowa to nazwa domeny sieciowej, która wyraża jej bezwzględną lokalizację w hierarchii systemu nazw domen (DNS).

GDPR (RODO)

Ogólne rozporządzenie o ochronie danych (RODO) to prawo dotyczące prywatności i bezpieczeństwa, które zostało ustanowione przez Unię Europejską (UE) i weszło w życie w 2018 r. Prawo to nakłada obowiązki na organizacje gromadzące dane dotyczące osób w UE w dowolnym miejscu.

Mobile Access

to aplikacja do kontroli dostępu osób za pomocą wirtualnych poświadczeń przechowywanych na urządzeniu mobilnym, takim jak smartfon danej osoby.

OSDP

Open Supervised Device Protocol to standard komunikacji w zakresie kontroli dostępu wprowadzony w 2011 roku przez Security Industry Association (SIA). Oferuje on przewagę w stosunku do starszych protokołów w zakresie szyfrowania, biometrii, łatwości użycia i interoperacyjności.

RSSI

Wskaźnik siły sygnału odbieranego (ang. Received Signal Strength Indicator, RSSI) to mierzona w dBm siła sygnału odbieranego przez urządzenie odbiorcze. Urządzenia mobilne zazwyczaj wyświetlają RSSI w postaci wykresu słupkowego siły sygnału.

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

Rozwiązania do budynków podnoszące jakość życia

202405132118