Visitor 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 rozwiązaniu Bosch Visitor Management

Oprogramowanie Visitor Management, zwane dalej VisMgmt, to narzędzie obsługiwane przez przeglądarkę internetową, które współpracuje z systemami kontroli dostępu Bosch. Zarządza odwiedzinami gości w obiekcie o kontrolowanym dostępie, w tym planowaniem wizyt, informacjami służbowymi gości, powiązanymi dokumentami i umowami oraz przypisywaniem tymczasowych poświadczeń.
Interfejs użytkownika jest konfigurowalny, a każdy użytkownik może zmieniać język interfejsu w trakcie pracy, bez wylogowywania.
Narzędzie przewiduje następujące podstawowe rodzaje użytkowników i czynności, które będą wykonywać:

Typ użytkownika	Wykonywane czynności
Recepcjonista	Rejestrowanie nowych wizyt i gości Zatwierdzanie i odrzucanie wniosków o wizyty Umieszczanie gości na czarnej liście Przydzielanie i odbieranie kart gościom Zarządzanie powiązanymi dokumentami Monitorowanie liczby gości w obiekcie
Visitor (Goście)	Samodzielna i rejestracja wstępna Tworzenie profil gości i zarządzanie tymi profilami Podpisywanie dokumentów
Gospodarz	Zarządzanie harmonogramami oraz listami odwiedzin i gości Wstępne rejestrowanie wizyt
Administrator	Konfigurowanie ustawień globalnych Dostosowywanie działania narzędzia i jego interfejsu użytkownika Plus: Wszystkie czynności wykonywane przez recepcjonistę

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.

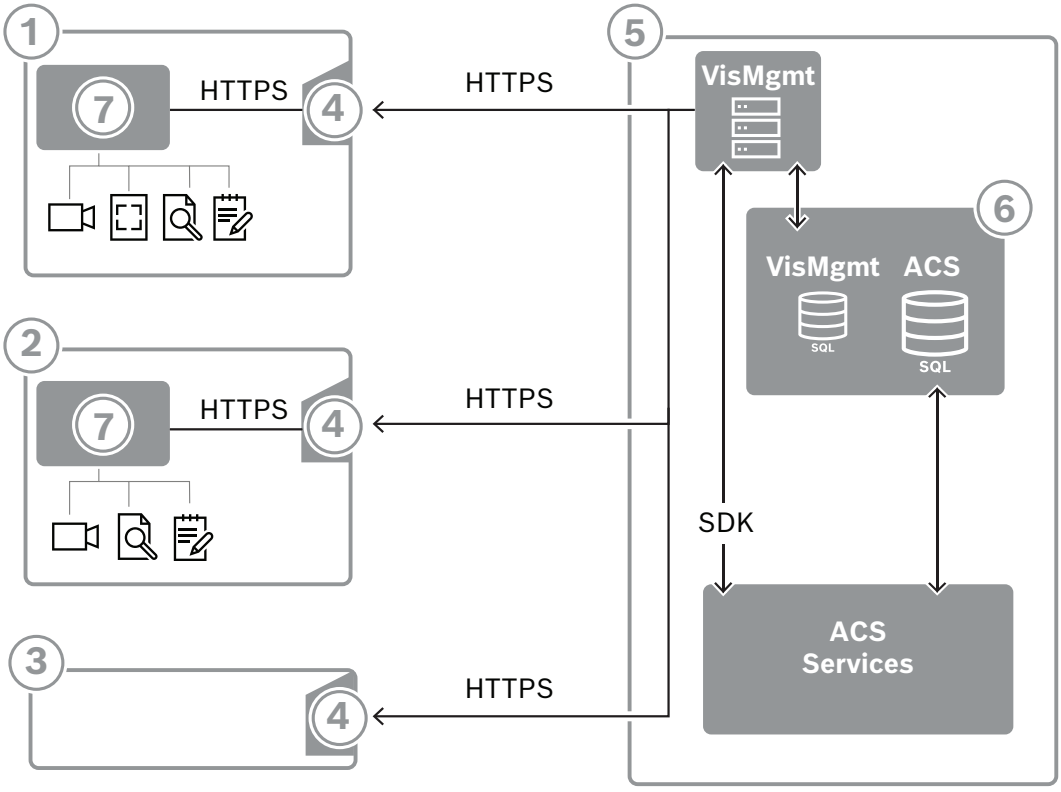
2.3 Docelowi odbiorcy

- Instalatorzy i administratorzy oprogramowania Visitor Management
- Główne typy użytkowników Visitor Management

2.4 Sposób korzystania z tego dokumentu

- Funkcja **Wyszukaj** w przeglądarce pomocy umożliwia znajdowanie żądanych treści.
- Sekcje **Przegląd systemu, Instalacja** i **Konfiguracja** są kierowane przede wszystkim dla administratorów systemu.
- Sekcje **Obsługa** są adresowane przede wszystkim do użytkowników systemu.

3 Przegląd i topologia systemu



Etykieta	Opis
1	Stacja robocza **Recepcjonista**. Stacja robocza może być wyposażona w opcjonalny sprzęt peryferyjny, np. czytnik rejestracji, kamerę internetową i skaner do podpisów i dokumentów.
2	Stacja robocza typu kiosk **Gość** z obsługiwaną przeglądarką działającą w trybie kiosk. Stacja robocza może być wyposażona w opcjonalny sprzęt peryferyjny, np. kamerę internetową i skanery do podpisów i dokumentów.
3	Stacja robocza **Gospodarz**, czyli stacja robocza pracownika, który przyjmuje gościa.
4	Obsługiwana przeglądarka z witryną internetową VisMgmt
5	Serwer ACS (BIS lub AMS)
6	Instancja bazy danych serwera ACS (może znajdować się na osobnym komputerze).
7	Opcjonalny **dodatek Bosch na urządzenia peryferyjne**, które zarządza komunikacją między przeglądarką a sprzętem peryferyjnym.

W zalecanej topologii systemu serwer programu VisMgmt znajduje się na tym samym komputerze, co główny system kontroli dostępu, a jego baza danych w tej samej instancji systemu bazodanowego.

Dodatek Bosch na urządzenia peryferyjne jest instalowany tylko na stacjach roboczych, które wymagają dostępu do urządzeń peryferyjnych.

Stacja robocza gospodarza zazwyczaj wymaga tylko dostępu do serwera programu VisMgmt przez przeglądarkę.

4 Instalowanie i odinstalowywanie

4.1 Wymagania programowe i sprzętowe

Zainstaluj serwer VisMgmt na tym samym komputerze, na którym znajduje się główny system kontroli dostępu, z zachowaniem tych samych wymagań w zakresie oprogramowania i sprzętu.
Jeśli główny system kontroli dostępu nie jest jeszcze zainstalowany, pamiętaj o przygotowaniu go przed instalacją Visitor 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.

Wymagania dotyczące serwera

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 dodatku Bosch na urządzenia peryferyjne
Dodatek na urządzenia peryferyjne Bosch to program obsługujący komunikację elektroniczną między przeglądarką a urządzeniami peryferyjnymi, np. czytnikiem rejestracji, kamerą internetową, skanerem podpisów i skanerem dokumentów.
Komputer kliencki to komputer, który jest fizycznie podłączony do urządzenia peryferyjnego. Uruchamia również przeglądarkę, która łączy się z serwerem VisMgmt.
Chociaż instalacja urządzeń peryferyjne nie jest bezwzględnie wymagania, zdecydowanie warto je dodać, ponieważ znacznie usprawniają one proces rejestracji gości.

Wymagania	**Opis**
Minimalna rozdzielczość monitora	Full HD 1920x1080
Obsługiwane przeglądarki	Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium based) Należy użyć najnowszej wersji przeglądarki przeznaczonej do systemu operacyjnego Windows.

4.1.1 Główny system kontroli dostępu

Bez aplikacji Mobile Access

Jeśli aplikacja Mobile Access nie jest wymagana, VisMgmt w wersji 5.5 współpracuje z następującymi systemami kontroli dostępu firmy Bosch:

– Access Management System (AMS) w wersjach 5.5 i nowszych

Z aplikacją Mobile Access

Jeśli jako licencję dodatkową wybrano Mobile Access, VisMgmt w wersji 5.5 współpracuje z następującymi systemami kontroli dostępu Bosch:

– Access Management System (AMS) w wersji 5.5 (zawiera rozszerzenie Mobile Access) i nowsze

Przed przystąpieniem do instalacji programu VisMgmt należy zainstalować w całości główny system kontroli dostępu i sprawdzić poprawność instalacji zgodnie z jego instrukcjami instalacji.

4.1.2 Instancja systemu bazodanowego do obsługi bazy danych systemu Visitor Manager.

Instalacja głównego systemu kontroli dostępu tworzy instancję bazy danych, której można używać do obsługi bazy danych VisMgmt, `dbVisitorManagement`.
Domyślna nazwa tej instancji zmienia się w zależności od usługi ACS

– W przypadku AMS nazwa to `ACE`
– W przypadku BIS ACE nazwa to `BIS_ACE`

4.1.3 Dedykowany użytkownik z lokalnym dostępem do bazy danych

Użytkownik `VMUser` pracuje w bazie danych systemu Visitor Manager w imieniu aplikacji VisMgmt.
Instalator serwera programu VisMgmt tworzy użytkownika VisMgmt systemu Windows na serwerze `VMUser`.

4.1.4 Dedykowany użytkownik ze zdalnym dostępem do bazy danych

Jeśli VisMgmt służy do korzystania z bazy danych na zdalnym serwerze baz danych, utwórz i skonfiguruj użytkownika `VMUser` w systemie Windows i na serwerze SQL, postępując zgodnie z poniższym opisem.
WAŻNE: nie należy uruchamiać konfiguracji VisMgmt przed ukończeniem tej procedury.

1. Na zdalnym serwerze bazy danych utwórz użytkownika systemu Windows z następującymi ustawieniami:

– **Nazwa użytkownika** (z uwzględnieniem wielkości liter): `VMUser`
– **Hasło**: ustaw hasło zgodnie z zasadami zabezpieczeń, które mają zastosowanie do wszystkich komputerów. Należy o tym pamiętać, ponieważ będzie to wymagane do konfiguracji VisMgmt.
– **Członek grupy**: `Administrators`
– **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`

(Dodaj `VMUser` jako logowanie zdalne do serwera SQL)

1. Otwórz SQL Management Studio
2. Połącz ze zdalną instancją SQL
3. Przejdź do **Security** (Zabezpieczenia) > **Login** (Zaloguj)
4. Dodaj użytkownika `VMUser` pełniącego na serwerze rolę `sysadmin`

Następnie po wykonaniu konfiguracji VisMgmt na serwerze VisMgmt należy wybrać opcję komputera **zdalnego serwera bazy danych** i wpisać hasło zdefiniowane powyżej dla `VMUser`.

4.1.5 Dedykowany użytkownik w głównym systemie kontroli dostępu

1. W głównym systemie kontroli dostępu utwórz użytkownika i aktywuj dla niego funkcję **Nieograniczone używanie interfejsów API**.
   Szczegółowe informacje na ten temat można znaleźć w rozdziale **Przypisywanie profili użytkowników (operatorów)** w instrukcji operatora głównego systemu kontroli dostępu.
2. W przypadku korzystania z BIS ACE należy zalogować się w systemie BIS lub za pomocą programu Smart Client, aby ustawić hasło.
3. Zapamiętaj lub zanotuj nazwę użytkownika i hasło, ponieważ kreator instalacji programu VisMgmt będzie ich wymagał.

4.2 Instalowanie serwera

Program instalacyjny można uruchomić dopiero po spełnieniu wszystkich wymagań programowych.
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.

4.2.1 Uruchamianie programu instalacyjnego serwera

1. Na komputerze, który ma pełnić rolę serwera programu VisMgmt, zaloguj się jako administrator i uruchom program `BoschVisitorManagementServer.exe`.
2. Kliknij przycisk **Dalej**, aby zaakceptować domyślny pakiet instalacyjny.
3. W przypadku wyrażenia zgody na umowę licencyjną użytkownika oprogramowania (EULA) zaakceptuj ją i kliknij przycisk **Dalej**.
4. Wybierz docelowy folder instalacji. Zalecamy użycie domyślnego folderu.

– W oknie **Konfiguracja serwera SQL**

5. Określ, czy chcesz utworzyć bazę danych w lokalnej instancji serwera SQL, czyli w instancji na serwerze VisMgmt, czy też na zdalnym komputerze serwera bazy danych.
   – **Uwaga:** W przypadku wybrania opcji zdalnego serwera bazy danych program instalacyjny wyświetli monit o podanie hasła użytkownika `VMUser`, czyli użytkownika z prawami administratora, który został skonfigurowany na zdalnym serwerze baz danych (patrz podrozdział Wymagania programowe).
6. Sprawdź i w razie potrzeby zmodyfikuj wartości następujących parametrów:

Serwer SQL	Nazwa komputera z serwerem bazy danych

Instancja SQL	Nazwa instancji głównej bazy danych ACS. W takim przypadku tworzona jest baza danych gości. W przypadku AMS nazwa to `ACE` W przypadku BIS ACE nazwa to `BIS_ACE`
Nazwa użytkownika SQL	Nazwa użytkownika z prawami administratora w instancji, zazwyczaj `sa`
Hasło SQL	Hasło tego użytkownika będącego administratorem.

7. Kliknij przycisk **Testuj połączenie**, aby sprawdzić, czy można uzyskać dostęp do instancji systemu bazodanowego przy użyciu wprowadzonych wartości parametrów. W razie niepowodzenia testu sprawdź jeszcze raz parametry.
8. Aby kontynuować, kliknij **Dalej**.

– W oknie **Konfiguracja dostępu przez ACS** (gdzie ACS odnosi się do głównego systemu kontroli dostępu — AMS lub ACE)

9. Wprowadź wartości następujących parametrów:

Nazwa hosta ACS	Nazwa komputera, na którym uruchomiony jest system ACS
Nazwa użytkownika ACS	Nazwa dedykowanego użytkownika systemu ACS mającego nieograniczonym prawa do korzystania z interfejsów API. Patrz podrozdział Wymagania programowe.
Hasło ACS	Hasło tego dedykowanego użytkownika systemu ACS.

10. Aby kontynuować, kliknij **Dalej**.

– W oknie **Konfiguracja serwera tożsamości**

11. Wprowadź identyfikator URI odpowiedniego serwera tożsamości ACS:
    – AMS: `HTTPS://`<NameOfACSserver>`:44333`
    – BIS: `HTTPS://`<NameOfACSserver>`/BisIdServer`
12. Kliknij przycisk **Testuj połączenie**, aby sprawdzić, czy serwer tożsamości jest dostępny.
13. W oknie podsumowania kliknij przycisk **Dalej**, a następnie kliknij przycisk **Instaluj**, aby rozpocząć instalowanie serwera programu VisMgmt.
14. Po zakończeniu instalacji uruchom ponownie komputer.

4.2.2 Plik JSON AppSettings

Wiele parametrów konfiguracyjnych serwera programu VisMgmt jest przechowywanych w pliku `.JSON`:

`<installation drive>:\Program Files (x86)\Bosch Sicherheitssysteme\Bosch Visitor Management\appsettings.json`

Zazwyczaj nie trzeba zmieniać wartości domyślnych, natomiast w sekcji **Settings** tego pliku znajdują się ustawienia, które czasami warto dostosować. W przypadku dostosowywania parametrów należy najpierw utworzyć kopię zapasową pliku. Kopia zapasowa pomoże szybko cofnąć zmiany, jeśli spowodują one awarię.

Aby zmodyfikowane parametry zaczęły obowiązywać, zapisz zmiany i uruchom ponownie usługę systemu Windows dotyczącą programu VisMgmt. Nazwa usługi to `Bosch Visitor Management`.

Nazwa parametru	Wartość domyślna	Opis
PageSizeNumberOfVisit	20	Maksymalna liczba rekordów wizyt wyświetlanych jednocześnie na ekranie. Gdy użytkownik przewija zawartość, każda nowa strona jest wypełniana tą liczbą rekordów wczytywanych z bazy danych.
MaximumUploadFileSizeBytes	31457289	Maksymalna liczba bajtów, jaką może zawierać przesłany plik.
StartoverTimeoutAskSeconds	300	Jeśli użytkownik zatrzyma się w trakcie wpisywania danych logowania, aplikacja poczeka tę liczbę sekund, po czym wyświetli monit o wprowadzenie danych.
StartoverTimeoutResetSeconds	60	Po wyświetleniu monitu aplikacja czeka tę liczbę sekund, zanim zresetuje ekran logowania.

4.3 Konfigurowanie komputera klienckiego VisMgmt

Dodatek na urządzenia peryferyjne Bosch można zainstalować na komputerze serwera, ale zazwyczaj umieszcza się go na komputerze klienckim w tej samej sieci. Jeśli tak, skopiuj certyfikat HTTPS z serwera ACS i zainstaluj go również na komputerze klienckim. Instrukcje znajdują się poniżej w punkcie *Certyfikaty do bezpiecznej komunikacji, Strona 15*.
Dodatek na urządzenia peryferyjne Bosch to oprogramowanie do nawiązywania połączeń z urządzeniami, np. czytnikami rejestracji i skanerami. Jeśli takie urządzenia nie są wymagane, na przykład dla użytkownika będącego gospodarzem, do zalogowania się w aplikacji VisMgmt i jej używania wystarczy przeglądarka internetowa.

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

Patrz

– *Certyfikaty do bezpiecznej komunikacji, Strona 15*

4.3.1 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.

4.3.2 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	/	/	/	/

4.3.2.1 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.

4.3.2.2 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**.

4.3.2.3 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

4.3.3 Plik JSON AppSettings

Wiele parametrów konfiguracyjnych komputera klienckiego programu VisMgmt jest przechowywanych w pliku `.JSON`:

<installation drive>:`\Program Files (x86)\Bosch Sicherheitssysteme\Bosch Visitor Management\appsettings.json`

Zazwyczaj nie trzeba zmieniać wartości domyślnych, natomiast w sekcji **AppSettings** tego pliku znajdują się ustawienia, które czasami warto dostosować.

Aby zmodyfikowane parametry zaczęły obowiązywać, zapisz zmiany i uruchom ponownie usługę systemu Windows dotyczącą programu VisMgmt. Nazwa usługi to `Bosch Ace Visitor Management Client`.

Nazwa parametru	Przykład	Opis
`CorseOrigins`	`"https://my-vm-server:5706"`	Adres i numer portu serwera programu Visitor Management.
`CardReaderPort`	`"com3"`	Numer portu COM, do którego podłączony jest czytnik rejestracji LECTUS. W przypadku czytników HID OMNIKEY ten parametr może być pusty.

4.4 Weryfikowanie instalacji serwera

Na komputerze w tej samej sieci, używając z jednej z obsługiwanych przeglądarek, otwórz następujący adres URL:

`https://`<VisMgmt server computer>`:5706/main`

Jeśli serwer jest uruchomiony, wyświetli stronę logowania do aplikacji.

4.5 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”.

4.5.1 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.

4.5.2 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.

4.5.3 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)

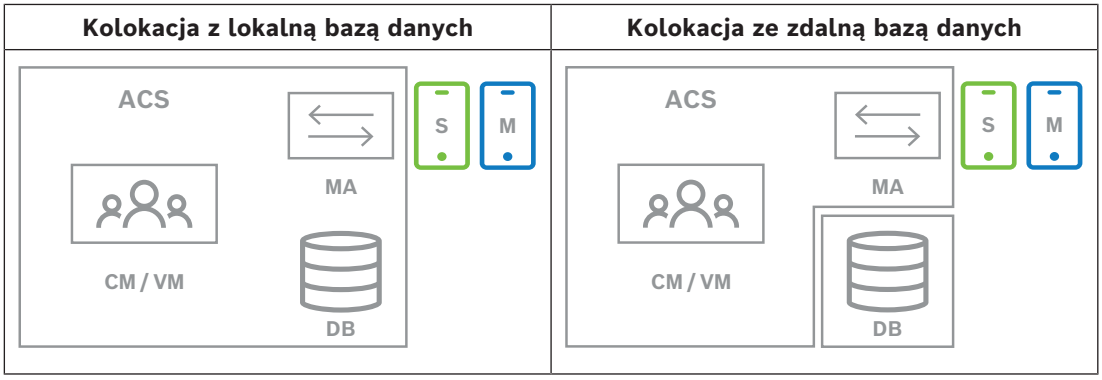
Użytkownik `MAUser` otwierający bazę danych ACS na rzecz aplikacji Mobile Access.
NIE musisz tworzyć tego użytkownika, jeśli ma używać lokalnej bazy danych. Program instalacyjny Mobile Access tworzy automatycznie użytkownika Windows `MAUser` na serwerze ACS.

4.5.4 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**.



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.

4.5.5 Procedura dla instalacji rozproszonej

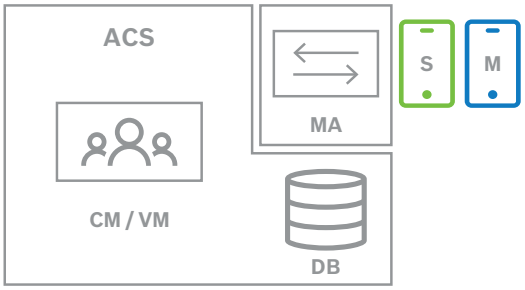
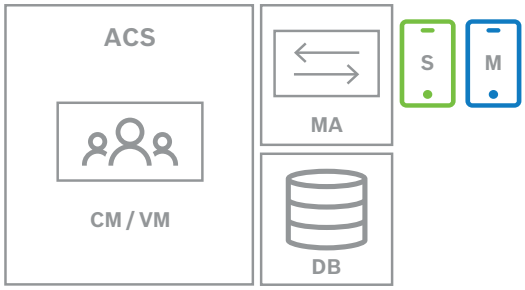
Instalacja kolokowana oznacza, że usługa backendu Mobile Access działa na tym samym serwerze, co ACS.

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.

4.6 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

4.7 Urządzenia peryferyjne

W momencie pisania tego tekstu przetestowane i zatwierdzone do użytku z VisMgmt oraz CredMgmt zostały następujące peryferyjne urządzenia USB. Regularnie aktualizowany spis zgodnych urządzeń znajduje się w specjalnym arkuszu danych głównego systemu kontroli dostępu.

Czytnik rejestracji kart	LECTUS enroll ARD-EDMCV002-USB, HID OMNIKEY 5427 CK
Skaner dokumentów identyfikacyjnych	ARH Combo, ARH Osmond
Skaner podpisów	signotec LITE, signotec Omega

Aby podłączyć te urządzenia do komputerów klienckich, postępuj zgodnie z instrukcjami producenta.

Czytnik rejestrujący
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

4.7.1 Rejestrowanie urządzeń peryferyjnych w komputerze klienckim

Aby zarejestrować urządzenie peryferyjne na komputerze klienckim programu VisMgmt, uruchomić program instalacyjny Bosch na urządzenia peryferyjne, `BoschPeripheralDeviceAddon.exe`, na komputerze klienckim. Instrukcje można znaleźć w temacie *Konfigurowanie dodatku na urządzenia peryferyjne, Strona 15*.

Patrz
– *Konfigurowanie dodatku na urządzenia peryferyjne, Strona 15*

4.8 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.

4.9 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.

5 Konfiguracja

5.1 Tworzenie użytkowników programu Visitor Management w systemie ACS

Wstęp

Każdy administrator, recepcjonista lub gospodarz korzystający z programu VisMgmt musi być posiadaczem karty z odrębną definicją operatora w systemie ACS, czyli głównym systemie kontroli dostępu (access control system).

Te definicje operatorów zawierają specjalne uprawnienia do korzystania z programu VisMgmt przedstawione w formie **profili użytkowników**. Szczegółowe informacje i instrukcje dotyczące **Profili użytkowników** można znaleźć w pomocy ekranowej usługi ACS.

– Należy zdefiniować osobnego operatora dla każdego posiadacza karty, który zajmuje się zarządzaniem gośćmi. Temu samemu operatorowi nie można przypisywać wielu posiadaczy kart.

Uwaga!

Zabezpieczenia IT i kont użytkowników

Zgodnie z najlepszymi wskazówkami dotyczącymi zabezpieczeń IT zaleca się, aby każdy użytkownik typu recepcjonista, gospodarz i administrator miał swoje własne konto w systemie Windows.

Tworzenie profili użytkowników na potrzeby zarządzania gośćmi

1. Zaloguj się w głównym systemie kontroli dostępu przy użyciu uprawnień administratora.
2. Utwórz dla użytkowników programu VisMgmt jeden lub więcej profili użytkowników (operatorów).
   Ścieżka w oknie dialogowym:
– **Konfiguracja > Operatorzy i stacje robocze** > **Profile użytkownika**
– Przeglądarka konfiguracji > **Administracja** > **Profile użytkowników ACE**
3. Przypisz tym profilom jedno z następujących uprawnień użytkowników.
– Administrator: `Visitor Management > Administrator`
– Gospodarz: `Visitor Management > Host`
– Recepcjonista: `Visitor Management > Receptionist`

Po utworzeniu profili użytkowników potrzebnych dla różnych ról w programie VisMgmt (administrator, recepcjonista, gospodarz) można przypisać każdy profil wielu operatorom.

Przypisywanie profili użytkowników operatorom systemu ACS i posiadaczom kart

Ścieżka w oknie dialogowym:

– **Konfiguracja** > **Operatorzy i stacje robocze** > **Uprawnienia użytkownika**
– Przeglądarka konfiguracji > **Administracja** > **Operatorzy**

1. Dodaj nowy typ operatora (kliknij  lub  w zależności od systemu ACS) i nadaj mu nazwę, która jasno odnosi się do jednej z ról w programie VisMgmt (administrator, gospodarz lub recepcjonista).
2. Na karcie **Ogólne ustawienia operatora** wybierz z listy uprawnień opcję `Operator ACE`.
3. Na karcie **Ustawienia operatora systemu ACE** za pomocą przycisków strzałek przypisz operatorowi utworzony wcześniej **profil użytkownika systemu ACE**.
   Należy odznaczyć profil domyślny `UP-Administrator`, z wyjątkiem mało prawdopodobnej sytuacji, w której posiadacz karty musi mieć ogólne uprawnienia administratora w systemie ACS.

4. Nadal na karcie **Ustawienia operatora systemu ACE** w okienku **Przypisz osobę** znajdź w systemie posiadacza karty, który ma pełnić daną rolę w programie VisMgmt.
5. Kliknij przycisk **Przypisz osobę**, aby zakończyć przypisywanie roli wybranemu posiadaczowi karty.

– Należy zdefiniować osobnego operatora dla każdego posiadacza karty, który zajmuje się zarządzaniem gośćmi. Temu samemu operatorowi nie można przypisywać wielu posiadaczy kart.

5.2 Tworzenie autoryzacji i profili gości w ACS

Wstęp

Pracownik recepcji lub administrator systemu VisMgmt wybiera dla każdego nowego gościa **Typ gościa**. Ten typ gościa jest oparty na wcześniej zdefiniowanym **Typie osoby** o nazwie **Gość** w głównym systemie kontroli dostępu (ACS) lub na podtypie **Gościa** utworzonym przez administratorów systemu ACS.

Administratorzy muszą również skonfigurować Typ Osoby **Gość** oraz jego podtypy w systemie ACS z profilami dostępu. Za pomocą tych profili dostępu osoby w poszczególnych kategoriach mogą używać prawdziwych przejść na terenie obiektu.

5.3 Konfigurowanie komputera recepcjonisty

Komputer recepcjonisty zawiera dodatek **Bosch na urządzenia peryferyjne**, który umożliwia fizyczne podłączanie urządzeń peryferyjnych w celu odczytywania kart, skanowania dokumentów identyfikacyjnych i skanowania podpisów.

Przed zainstalowaniem oprogramowania klienckiego podłącz wszystkie wymagane urządzenia peryferyjne.

Upewnij się, że komputer i jego urządzenia peryferyjne są odpowiednio zabezpieczone przed nieuprawnionym dostępem.

5.4 Konfigurowanie komputera typu Kiosk dla gości

Wstęp

Goście zwykle rejestrują swoje odwiedziny i tworzą własne profile na komputerze, który jest powszechnie dostępny w strefie recepcji obiektu o kontrolowanym dostępie. Z względów bezpieczeństwa przeglądarka internetowa komputera działa w trybie kiosku, który umożliwia dostęp tylko do programu VisMgmt. Użytkownik nie może przejść do innych kart, ustawień przeglądarki ani systemu operacyjnego komputera. Wszystkie obsługiwane przeglądarki mają funkcjonalność trybu kiosku, ale jego dokładna konfiguracja zależy od przeglądarki.

Komputer kioskowy zawiera dodatek **Bosch na urządzenia peryferyjne**, który umożliwia fizyczne podłączanie urządzeń peryferyjnych w celu skanowania dokumentów identyfikacyjnych i podpisów.

– Adres URL trybu kiosk to `https://`<Mój_serwer_programu_VisMgmt>`:5706`

Konfigurowanie trybu kiosk w przeglądarkach

Poniższe łącza prowadzą do procedur konfigurowania trybu kiosk w przeglądarkach internetowych obsługiwanych przez program VisMgmt.

	Instrukcje konfigurowania trybu kiosk
Chrome	https://support.google.com/chrome/a/answer/9273974
Firefox	https://support.mozilla.org/en-US/kb/firefox-enterprise-kiosk-mode

	Instrukcje konfigurowania trybu kiosk
Edge	https://docs.microsoft.com/en-us/deployedge/microsoft-edge-configure-kiosk-mode

Uwaga!
Ze względów bezpieczeństwa wyłącz na stałe opcję automatycznego zapisywania haseł w przeglądarce.

5.5 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 VisMgmt, a następnie dwukropek i numer portu (domyślnie `5706`)
   `https://`<My_VisMgmt_server>`:5706/main`
   Zostanie wyświetlony ekran **logowania**
2. Zaloguj się jako użytkownik o statusie **Administrator** dla programu VisMgmt.
3. Kliknij przycisk  , a zostanie otwarte menu **Ustawienia**.

5.6 Konfigurowanie za pomocą menu Ustawienia

W menu **Ustawienia** znajdują się podsekcje umożliwiające wykonywanie następujących czynności konfiguracyjnych:

Ustawienia ogólne	– **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.
	– **Tryb przechowywania dokumentów**: wybierz, czy dokumenty mają być przechowywane jako pliki papierowe czy cyfrowe.
	– **Maksymalna liczba gości**, którzy mogą jednocześnie przebywać w obiekcie.
	Wartością domyślną jest `100`.
	Aby całkowicie wyłączyć licznik gości na pulpicie, ustaw `0`.
	– **Okres ostrzeżenia o wygaśnięciu dokumentu (w dniach)**: określ okres ostrzeżenia o wygaśnięciu dokumentów, takich jak umowy o zachowaniu poufności (NDA) czy warunki użytkowania. Ten okres dotyczy zarówno plików papierowych, jak i cyfrowych.
	Po tym okresie dokumenty są oznaczane w profilu gościa jako wygasłe (ikona zegara z czerwoną kropką).
	Wartością domyślną jest `365`

- **Okres ostrzeżenia o wygaśnięciu dokumentu (w dniach)**: określ długość okresu ostrzeżenia o wygaśnięciu dokumentu.
  Podczas tego okresu ostrzegawczego dokumenty są oznaczane w profilu gościa (ikona zegara z pomarańczową kropką). Przed upływem okresu ostrzegawczego ikona zegara ma zieloną kropkę.
- **Logo:** zaznacz lub usuń zaznaczenie pól wyboru, które określają, czy w oknach dialogowych ma być wyświetlane logo niestandardowe, czy logo domyślne, oraz czy ma być wyświetlana **grafika** Bosch.
  - Aby zapoznać się z kryteriami dotyczącymi niestandardowych plików logo, patrz: *Dostosowywanie firmowego logo, Strona 37*
- Kliknięcie przycisku **Podgląd** spowoduje wyświetlenie strony okna dialogowego w postaci, w jakiej będzie wyglądać z tymi ustawieniami. Aby uzyskać więcej informacji na temat trybu podglądu, przejdź do następnej sekcji.
- **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.

Recepcjonista	– Ten ekran ustawień zawiera 2 pola wyboru dla każdego pola danych znajdującego się w oknach dialogowych rejestrowania gości przez recepcjonistę.
	  – Zaznacz lub wyczyść pierwsze pole wyboru, aby określić, czy pole danych ma być **widoczne** we wszystkich oknach dialogowych rejestracji.
	  – Zaznacz lub wyczyść drugie pole wyboru (oznaczone gwiazdką), aby określić, czy pole danych jest **obowiązkowe**.
	– Dostosuj domyślny tekst nagłówków w oknach dialogowych zbierania danych.
	Dokładniejsze informacje znajdują się pod spodem w temacie *Dostosowywanie interfejsu użytkownika, Strona 36*.

	Opcja specjalna: włączanie meldowanie/wymeldowywanie bez karty Jeśli goście są ściśle chronieni lub przebywają w przestrzeniach ogólnodostępnych, pojedyncze karty gości mogą nie być potrzebne. W takich przypadkach istnieje możliwość meldowania i wymeldowania gości bez użycia kart. Ta opcja jest domyślnie wyłączona ze względów bezpieczeństwa. Aby ją włączyć, należy zaznaczyć to pole wyboru: – **Uwaga:** jeśli ta opcja jest włączona, każdy **gość**, który dokonuje rejestracji automatycznej na komputerze kioskowym, w jednym momencie automatycznie potwierdzi odwiedziny i zamelduje się. – W rozdziale **Obsługa** *Meldowanie i wymeldowanie bez użycia karty, Strona 54* tego dokumentu znajdują się szczegółowe informacje na temat tego, w jaki sposób użytkownik typu **Recepcjonista** obsługuje gości bez użycia kart.
Gospodarz **Gość**	Ustawienia użytkowników **Gospodarz** i **Gość** pozostają tylko do odczytu do czasu, aż zmodyfikujesz i zapiszesz ustawienia użytkownika **Recepcjonista**. Pola, które oznaczysz jako niewidoczne w ustawieniach użytkownika **Recepcjonista**, automatycznie stają się niewidoczne w ustawieniach użytkowników **Gospodarz** i **Gość**. Potem procedura konfiguracji jest już taka sama.

Patrz

- *Przydzielanie poświadczeń fizycznych, Strona 50*
- *Dostosowywanie interfejsu użytkownika, Strona 36*

5.6.1 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. Pobrany szablon do edycji jest zapisywany w domyślnym folderze Pobrane w Twojej 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.
- `VisitorInvite.html` Zaproszenie do odwiedzenia obiektu z wykorzystaniem opcji dodawania pliku iCalendar do wiadomości e-mail.
- `InformHostAboutCheckin.html` Wiadomość e-mail informująca gospodarza o przybyciu gościa.

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.)
`{{FirstName}}`	imię instalatora
`{{LastName}}`	nazwisko instalatora
`{{CompanyName}}`	firma instalatora
`{{QrcodeLink}}`	Kod QR odpowiadający linkowi, który oferuje instalatorowi mobilny dostęp za pośrednictwem aplikacji Setup Access

Symbol zastępczy	Opis
{{InviteLink}}	link, który oferuje instalatorowi mobilny dostęp za pośrednictwem aplikacji Setup Access

Zaproszenie dla gości
E-mail, który jest wysyłany do gości przy tworzeniu lub edycji wizyty.

Symbol zastępczy	Opis
{{VisitorID}}	kod identyfikacyjny gościa wygenerowany przez aplikację VisMgmt
{{Title}}	tytuł gościa (pan, pani, dr itd.)
{{FirstName}}	imię gościa
{{LastName}}	nazwisko gościa
{{CompanyName}}	firma gościa
{{HostFirstName}}	imię gospodarza
{{HostLastName}}	nazwisko gospodarza
{{ExpArrivalDate}}	planowana data odwiedzin

Gość dotarł
E-mail, który jest wysyłany do gospodarza, gdy recepcja zatwierdzi wizytę.

Symbol zastępczy	Opis
{{VisitorID}}	kod identyfikacyjny gościa wygenerowany przez aplikację VisMgmt
{{Title}}	tytuł gościa (pan, pani, dr itd.)
{{FirstName}}	imię gościa
{{LastName}}	nazwisko gościa
{{CompanyName}}	firma gościa
{{HostFirstName}}	imię gospodarza
{{HostLastName}}	nazwisko gospodarza
{{ExpArrivalDate}}	planowana data odwiedzin
{{ArrivalDate}}	rzeczywista data odwiedzin

Przepustka gościa
Dokument, który można wydrukować i wręczyć gościowi. Może zawierać mapę budynku lub listę kontrolną.

Symbol zastępczy	Opis
{{VisitorID}}	kod identyfikacyjny gościa wygenerowany przez aplikację VisMgmt

Symbol zastępczy	Opis
{{Title}}	tytuł gościa (pan, pani, dr itd.)
{{FirstName}}	imię gościa
{{LastName}}	nazwisko gościa
{{CompanyName}}	firma gościa
{{HostFirstName}}	imię gospodarza
{{HostLastName}}	nazwisko gospodarza
{{ExpArrivalDate}}	planowana data odwiedzin
{{ArrivalDate}}	rzeczywista data odwiedzin

5.6.2 Tryb podglądu

Obok niektórych zbiorów opcji znajduje się przycisk **Podgląd**, który uaktywnia tryb podglądu. Pozwala on wyświetlić okna dialogowe w postaci, w jakiej będą wyglądać po ustawieniu tych opcji.

W trybie podglądu obowiązują następujące ograniczenia:

– U góry pulpitu nawigacyjnego pojawia się baner.

– Zmiany wprowadzone w pulpicie nawigacyjnym i menu **nie są** zapisywane.
– Aby zamknąć tryb podglądu, kliknij przycisk **Zamknij tryb podglądu** znajdujący się wewnątrz banera.
– Użyj listy **Change role** (Zmień rolę) dostępnej wewnątrz banera, aby wyświetlić podgląd interfejsu u różnych typów użytkowników.

5.6.3 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**.

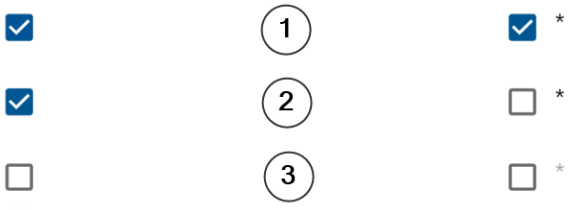
5.7 Dostosowywanie interfejsu użytkownika

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

5.7.1 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.

5.7.2 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>
   ```

5.7.3 Dostosowywanie trybu kiosku

Jeśli w obiekcie brakuje co najmniej jednego z urządzeń peryferyjnych, na przykład skanera dokumentów, możesz dostosować proces autorejestracji gości w trybie kiosku, usuwając zaznaczenie pól wyboru przy odpowiednich krokach rejestracji.

5.7.4 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

5.8 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.
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.

5.8.1 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
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

Program	Lokalizacja pliku
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
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]\

5.8.2 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.

5.9 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:

5.9.1 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.

5.9.2 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.

5.9.3 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.

5.10 Tworzenie kopii zapasowej systemu

VisMgmt to pomocnicza aplikacja internetowa do głównego systemu kontroli dostępu. Informacje o tworzeniu zapasowych kopii systemowych baz danych znajdują się w dokumentacji głównego systemu kontroli dostępu.

6 Obsługa

6.1 Omówienie ról użytkowników

Typ użytkownika	Wykonywane czynności
Recepcjonista	Rejestrowanie nowych wizyt i gości Zatwierdzanie i odrzucanie wniosków o wizyty Umieszczanie gości na czarnej liście Przydzielanie i odbieranie kart gościom Zarządzanie powiązanymi dokumentami Monitorowanie liczby gości w obiekcie
Visitor (Goście)	Samodzielna i rejestracja wstępna Tworzenie profil gości i zarządzanie tymi profilami Podpisywanie dokumentów
Gospodarz	Zarządzanie harmonogramami oraz listami odwiedzin i gości Wstępne rejestrowanie wizyt
Administrator	Konfigurowanie ustawień globalnych Dostosowywanie działania narzędzia i jego interfejsu użytkownika Plus: Wszystkie czynności wykonywane przez recepcjonistę

6.2 Korzystanie z pulpitu nawigacyjnego

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

Przegląd i szybkie filtry

U góry pulpitu nawigacyjnego znajduje skrócony przegląd dziennych odwiedzin. Pozwala on użytkownikowi łatwo monitorować liczby gości w obiekcie.

Goście oczekiwani dzisiaj: _%	Goście zarejestrowani: _%	Goście nadal do wyrejestrowania dzisiaj	Goście, których czas wymeldowania minął
`<current count> / <total capacity>`	`<current count> / <total capacity>`	`<current count>`	`<current count>`

Kliknięcie nagłówka spowoduje wyfiltrowanie tabeli odwiedzin zgodnie ze znaczeniem nagłówka. Na przykład po kliknięciu nagłówka **Goście zarejestrowani** zobaczysz tylko tych gości, którym przydzielono karty.

`<total capacity>` to ustawienie konfiguracyjne, którego wartość ustawia administrator systemu. Patrz *Konfigurowanie za pomocą menu Ustawienia, Strona 31*.

6.2.1 Strona przeglądowa osoby

W pulpicie nawigacyjnym kliknij imię i nazwisko danej osoby. Pojawi się okno dialogowe z jej danymi osobowymi. Dane zostaną otwarte. Na stronie przeglądowej osoby są cztery sekcje z danymi osobowymi:

- Obraz identyfikacyjny
- Dokument tożsamości
- Informacje ogólne

– Dokumenty

6.2.2 Tabela odwiedzin

Każdy wiersz w tabeli reprezentuje umówienie wizyty.

– Tabelę można posortować według dowolnej z kolumn, klikając nagłówek kolumny.
– Można wybrać pojedyncze odwiedziny lub kilka odwiedzin naraz za pomocą klawiatury i myszy:
  – 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.
– Do tabeli można dodawać nowe wizyty
– Można przetwarzać dane wizyt i gości, klikając przyciski działań
  – Zatwierdzanie odwiedzin
  – Odrzucanie wizyty
  – Przydzielanie kart gościom
  – Wprowadzanie wizyt i danych gości
– 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.

Poziomy pasek narzędzi zawiera następujące funkcje:

Etykieta	Funkcja
1 N **pozycji**	Łączna liczba N odwiedzin (każda wizyta to wiersz w tabeli).
2 **Wyszukaj**	Wyszukiwanie dowolnego tekstu wśród rekordów wizyt w tabeli
3	Wyświetlanie najnowszych wizyt dodanych do tabeli.
4	Otwieranie okna dialogowego, w którym można wybrać kryteria filtrowania
5	Przywracanie domyślnego widoku tabeli i domyślnych wartości wszystkich filtrów.
6 **Odbierz kartę**	Otwieranie okna dialogowego, w którym można odebrać przydzielone karty za pomocą podłączonego czytnika rejestracji.

Etykieta	Funkcja
	Otwieranie okna dialogowego, w którym można utworzyć nowy wpis odwiedzin do tabeli
...	Kliknięcie symbolu wielokropka w menu powoduje wyeksportowanie aktualnie odfiltrowanych odwiedzin, a także dokumentów do różnych formatów plików, np.: `CSV` i `.XLSX` Należy pamiętać, że z przyczyn bezpieczeństwa danych eksport można przeprowadzać tylko wtedy, gdy klient pracuje w zabezpieczonym połączeniu HTTPS z certyfikatem.

6.2.3 Kolumny tabeli i działania

Kolumny

Kolumna	Wartość	Opis
Stan	 Wizyta oczekiwana  Wizyta zatwierdzona  Wizyta odrzucona  Karta przydzielona  Upłynął okres ważności karty  Wizyta zakończona (gość już nie posiada kart i opuścił obiekt)	Ikona odzwierciedlająca status odwiedzin
Imię i nazwisko	Hiperłącze z imieniem i nazwiskiem gościa	Kliknięcie hiperłącza spowoduje wyświetlenie szczegółowych informacji o gościu i jego obecnej wizycie.
Spodziewane wejście	Data i godzina	Przewidywana data i godzina przybycia gościa

Kolumna	Wartość	Opis
Spodziewane wyjście	Data i godzina	Przewidywana data i godzina opuszczenia obiektu przez gościa
Zarejestrowany	Data i godzina	Data i godzina przydzielenia gościowi pierwszej karty.
Wyrejestrowany	Data i godzina	Data i godzina odebrania gościowi ostatniej karty.
Numery kart	Liczbowe	Numery kart przydzielonych temu gościowi.
Działania	Ikony	Patrz osobna tabela poniżej

Działania

Ikona	Funkcja
	**Zatwierdzanie** wizyty. UWAGA: Nie można przydzielać kart gościom umieszczonym na czarnej liście. Najpierw należy usunąć gościa z czarnej listy albo tymczasowo wyłączyć go z restrykcji. Patrz *Dodawanie, usuwanie i wyłączanie z czarnej listy, Strona 55*.
	**Odrzucanie** wizyty. Ten przycisk jest dezaktywowany po zarejestrowaniu się gościa, czyli wtedy, gdy ma on już kartę.
	**Przydzielanie** gościowi jednej lub kilku kart
	**Edytowanie** zdarzenia odwiedzin i/lub poświadczeń gościa

6.3 Recepcjonista

6.3.1 Logowanie do roli recepcjonisty

1. W przeglądarce otwórz `https://<My_VisMgmt_server>:5706/main/` w odniesieniu do ekranu logowania.
2. Wprowadź nazwę użytkownika odpowiadającą kontu z uprawnieniami wymaganymi do przewidzianej roli.
   Jeśli nie masz konta, skontaktuj się z administratorem systemu.
3. Wprowadź hasło.
4. Kliknij przycisk **Zaloguj się**.

6.3.2 Wyszukiwanie i filtrowanie odwiedzin

W pulpicie nawigacyjnym programu VisMgmt na pasku narzędzi nad tabelą wizyt jest dostępnych kilka opcji.

Wyszukaj

Aby szukać imiona i nazwiska gości i gospodarczy, wprowadź tekst alfanumeryczny w polu wyszukiwania, a następnie naciśnij klawisz Enter.

Filtrowanie

- Aby zobaczyć wizyty najbliższe obecnej godzinie, kliknij przycisk **Najnowsze**.
- Aby skonstruować złożony filtr obejmujący stany odwiedzin, daty zarejestrowania i wyrejestrowania oraz numery kart, kliknij przycisk **Filtr**.
  - W wyskakującym oknie dialogowym wprowadź żądane kryteria filtrowania.
  - Kliknij przycisk **Zastosuj**
    . System zredukuje tabelę wizyt tylko do tych umówień, które spełniają kryteria filtrowania.
- Aby usunąć wszystkie kryteria filtrowania, kliknij przycisk **Resetuj**.

6.3.3 Rejestrowanie wizyt

Wstęp

Recepcjonista ma do dyspozycji dwa podstawowe scenariusze rejestrowania wizyt:

- **A:** Jeśli gość za pomocą stacji Kiosk utworzy własny identyfikator gościa i prześle dokumenty, recepcjonista musi tylko uzupełnić niezbędne brakujące informacje i podpisy, po czym przydzielić kartę gościowi.
- **B:** Gdy gość pomija stację Kiosk i podchodzi bezpośrednio do recepcji, recepcjonista może zarejestrować wizytę od podstaw: zebrać wymagane informacje, uzyskać podpisy na wymaganych dokumentach, a następnie przydzielić kartę gościowi.

Scenariusz **A** jest podzbiorem scenariusza **B**, dlatego poniżej opisujemy kompletny scenariusz **B**. Używanie trybu kiosku przez gościa opisano w osobnym podrozdziale. Patrz *Wprowadzenie do trybu kiosku, Strona 58*.

Procedura

W pulpicie nawigacyjnym programu VisMgmt na pasku narzędzi nad tabelą wizyt jest dostępnych kilka opcji.

1. Kliknij przycisk  , aby dodać umówienie wizyty do tabeli odwiedzin.
2. W oknie dialogowym **Dane osobowe** wprowadź dane, których administratorzy obiektu wymagają od gości. Pola obowiązkowe są oznaczone gwiazdką (*).
   Dane można wprowadzić ręcznie, ale szybszy i dokładniejszy będzie skaner dokumentów, o ile jest dostępny na stacji roboczej recepcjonisty. Szczegółowe informacje o obsługiwanych urządzeniach peryferyjnych zawiera punkt *Urządzenia peryferyjne, Strona 27*.

- **Informacje ogólne**
  - Odszukaj i wczytaj cały profil gościa utworzony w trakcie poprzednich odwiedzin.
    W tym celu kliknij ikonę  (Wyszukaj) znajdującą się w polu **Nazwisko***.
    Podczas tworzenia profilu gościa jest mu nadawany unikatowy kod alfanumeryczny, który gość powinien zachować, ponieważ przyspieszy on proces rejestracji przy kolejnych wizytach.
  - W przeciwnym razie wprowadź dane ręcznie.
- **Zdjęcia identyfikacyjne**
  - **Prześlij** zdjęcie z systemu plików.
  - **Zrób** zdjęcie gościowi za pomocą podłączonej kamery internetowej.
- **Dokumenty identyfikacyjne**
  - Kliknij przycisk **Skanuj dokument**, aby sczytać dane ze skanera dokumentów (o ile jest dostępny) i automatycznie wypełnić odpowiednie pola danych w oknie dialogowym.
  - Jeżeli system nie zawiera skanera dokumentów, uzupełnij informacje ręcznie.

- **Dokumenty prawne**
  - Wczytaj dokumenty, które gość podpisał elektronicznie w kiosku.
  - Jeśli system nie zawiera kiosku dla gości, wydrukuj wymagane dokumenty w formacie PDF przechowywane w systemie plików, daj je gościowi do podpisu, a następnie zarchiwizuj w systemie.

3. Kliknij przycisk **Dalej**, aby przejść do okna dialogowego **Wizyty**.
4. W oknie dialogowym **Wizyty** w okienku **Bieżąca wizyta** wprowadź dane wymagane przez administratorów obiektu. Pola obowiązkowe są oznaczone gwiazdką (*).

- Wybierz odpowiednią wartość w polu **Typ gościa**.
  Może to być **Gość** (domyślnie) lub spersonalizowana podklasa typu **Gość**, definiowana w polu **Typ osoby** w głównym systemie kontroli dostępu.
- W polu **Gospodarz** wybierz imię i nazwisko odwiedzanego pracownika.
  - Uwaga: można wybrać tylko posiadaczy kart zapisanych w głównym systemie kontroli dostępu.
  - W polu wskazówki można wyświetlić adres e-mail danej osoby jako pomoc w identyfikacji.
- Jeśli gość wymaga eskorty na terenie obiektu, w polu **Eskorta** zaznacz imię i nazwisko pracownika, który będzie pełnił tę rolę.
  - Uwaga: można wybrać tylko posiadaczy kart zapisanych w głównym systemie kontroli dostępu.
  - W polu wskazówki można wyświetlić adres e-mail danej osoby jako pomoc w identyfikacji.
- Jeżeli gość potrzebuje dodatkowego czasu na przechodzenie przez drzwi, zaznacz pole wyboru **Rozszerzony czas otwierania drzwi**.

5. Kliknij przycisk **Zapisz**.
   Pamiętaj, że dane będzie można zapisać dopiero po uzupełnieniu wszystkich obowiązkowych pól.

Patrz
- *Urządzenia peryferyjne, Strona 27*

6.3.4 Zatwierdzanie i odrzucanie wniosków o wizyty

Kontekst: zatwierdzanie kart fizycznych
Przed przypisaniem karty do gościa musisz zatwierdzić wizytę.

Kontekst: zatwierdzanie poświadczeń mobilnych
Poświadczenia mobilne możesz utworzyć i udostępnić w dniu wizyty, podobnie jak przypisanie karty fizycznej.
- **Uwaga:** poświadczenia mobilne będą nieaktywne do momentu zatwierdzenia wizyty.

Można też utworzyć poświadczenia mobilne i udostępnić je z wyprzedzeniem. Po przybyciu gościa do recepcji należy zatwierdzić wizytę według poniższego opisu. Pozwoli to aktywować poświadczenia mobilne.
- **Uwaga:** poświadczenia mobilne będą nieaktywne do momentu zatwierdzenia wizyty.
- Jeśli ustalono przewidywaną godzinę zakończenia wizyty, będzie ona obowiązywać.
- Jeśli nie ustawiono takiej godziny, zostanie użyta domyślna liczba godzin (8). Administratorzy mogą zmienić to domyślne ustawienie w menu **Ustawienia**.

Procedury zatwierdzania i odrzucania
Wizyty można zatwierdzać i odrzucać w dwóch miejscach:

– w tabeli wizyt w pulpicie nawigacyjnym
– w edytorze wizyt

W tabeli wizyt w pulpicie nawigacyjnym:

– **Zatwierdź**: W tabeli wizyt zaznacz wiersz i kliknij przycisk  . Pojawi się okno potwierdzenia, a następnie ikona zmieni kolor na szary, co oznacza, że odwiedziny zostały zaaprobowane.

– **Odrzuć**: W tabeli wizyt zaznacz wiersz i kliknij przycisk  . Pojawi się okno potwierdzenia, a ikona **Zatwierdź** zmieni kolor na niebieski. Oznacza, że wizyta nadal musi zostać zatwierdzona.

W edytorze wizyt:

1. W pulpicie nawigacyjnym w tabeli odwiedzin zaznacz wiersz i kliknij przycisk  , co umożliwi zmodyfikowanie wizyty.
2. W oknie dialogowym **Dane osobowe** kliknij przycisk **Dalej**.
3. W oknie dialogowym **Wizyty** kliknij przycisk **Zatwierdź** lub **Odrzuć**.
4. Potwierdź operację w wyskakującym oknie.

6.3.5 Przydzielanie poświadczeń fizycznych

Wstęp

Każdemu gościowi, który ma otrzymać pozwolenie wejścia na teren obiektu, należy przydzielić kartę. W razie potrzeby jednej osobie można przypisać kilka kart.

– Godzina **rejestracji** odwiedzin to moment, w którym przydzielono pierwszą kartę.
– Godzina **wyrejestrowania** odwiedzin to moment odebrania ostatniej karty od gościa.

Recepcjonista może łatwo przydzielać i odbierać karty z pulpitu nawigacyjnego, o ile tylko czytnik kart rejestracyjnych jest podłączony do komputera recepcjonisty.
Na wypadek braku takiego czytnika edytor wizyt umożliwia przypisywanie numerów kart.

Uwaga!
Osoby na czarnej liście nie mogą otrzymywać kart
Nie można przydzielać kart gościom figurującym na czarnej liście. Aby wręczyć kartę takiej osobie, należy usunąć ją z czarnej listy albo utworzyć dla niej tymczasowe wyłączenie.

Przydzielanie karty w pulpicie nawigacyjnym (wymaga czytnika rejestracji)

1. Przygotuj fizyczną kartę gościa do przyłożenia do czytnika rejestracji.
2. W tabeli odwiedzin zatwierdź wizytę. Patrz *Zatwierdzanie i odrzucanie wniosków o wizyty, Strona 49*.
3. Zaznacz wiersz odwiedzin i kliknij przycisk  .

4. Postępuj zgodnie z instrukcjami posługiwania się czytnikiem rejestracji wyświetlanymi w wyskakującym oknie.

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.

Przydzielanie karty w edytorze wizyt

1. W pulpicie nawigacyjnym w tabeli odwiedzin zaznacz wiersz i kliknij przycisk  , co umożliwi zmodyfikowanie wizyty.
2. W oknie dialogowym **Dane osobowe** kliknij przycisk **Dalej**.
3. W oknie dialogowym **Wizyty** kliknij przycisk **Zatwierdź**, jeśli odwiedziny nie zostały jeszcze zatwierdzone.
4. Jeśli masz podłączony czytnik rejestracji, kliknij przycisk **Read card** (Odczyt karty) i postępuj zgodnie z instrukcjami posługiwania się czytnikiem rejestracji wyświetlanymi w wyskakującym oknie. W przeciwnym razie:

– W przeciwnym razie kliknij opcję **Show free cards** (Pokaż wolne karty), aby wyświetlić listę kart gości, które nie zostały jeszcze przydzielone.
Ewentualnie, jeśli dysponujesz nieposortowanymi kartami fizycznymi z nadrukowanymi numerami, należy wybrać dowolną kartę i użyć narzędzia **Search** (Szukaj), aby szybko znaleźć jej numer na liście.
– Kliknij przycisk  obok numeru karty, a karta zostanie przypisana do obecnego gościa.
– W razie potrzeby powtórz ostatnie kroki, aby przypisać kolejne karty.

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

Odbieranie karty w edytorze wizyt

1. W pulpicie nawigacyjnym w tabeli odwiedzin zaznacz wiersz i kliknij przycisk  , co umożliwi zmodyfikowanie wizyty.
2. W oknie dialogowym **Dane osobowe** kliknij przycisk **Dalej**.
3. W oknie dialogowym **Wizyty** w okienku Karty gości kliknij przycisk  znajdujący się obok karty, którą chcesz odebrać, a następnie potwierdź operację w wyskakującym oknie.
Powtarzaj tę czynność, aż do odebrania wszystkich żądanych kart.
4. Kliknij przycisk **Zapisz**, co spowoduje zapisanie obecnej wizyty z przydziałami kart.

5. Po odebraniu ostatniej karty przydzielonej gościowi system odnotuje tę datę i godzinę jako czas wyrejestrowania gościa.

W tabeli wizyt stan tego rekordu odwiedzin zmieni wartość na .

Patrz
- *Konfigurowanie za pomocą menu Ustawienia, Strona 31*
- *Rejestrowanie wizyt, Strona 48*
- *Zatwierdzanie i odrzucanie wniosków o wizyty, Strona 49*

6.3.6 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, Strona 49*
- 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, Strona 49*
– 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, Strona 49*
– 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, Strona 49*
– Urządzenie mobilne z uruchomioną aplikacją może działać jak fizyczna karta dostępu.

Patrz

– *Instalowanie programu Mobile Access, Strona 19*
– *Instalowanie aplikacji Mobile Access, Strona 18*

6.3.7 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.

6.3.8 Meldowanie i wymeldowanie bez użycia karty

Wstęp

Jeśli goście są ściśle chronieni lub przebywają w przestrzeniach ogólnodostępnych, pojedyncze karty gości mogą nie być potrzebne. W takich przypadkach istnieje możliwość meldowania i wymeldowania gości bez użycia kart. Ta opcja jest domyślnie wyłączona ze względów bezpieczeństwa.

Wymaganie wstępne.

Administrator systemu włącza specjalną opcję **Zameldowanie/wymeldowanie bez karty** w oknie dialogowym **Ustawienia** > **Recepcjonista > Wizyty**. Zobacz instrukcje w rozdziale dotyczącym konfiguracji *Konfigurowanie za pomocą menu Ustawienia, Strona 31*.

Proces

Kiedy ta opcja jest włączona, należy wykonać następujące czynności:

– Każdy z gości, którzy rejestrują się samodzielnie na komputerze kioskowym, w tym samym czasie automatycznie potwierdza odwiedziny i melduje się.
– System ustawia datę i godzinę zameldowania w chwili rejestracji.
– Przycisk **Zamelduj/wymelduj się bez karty** pojawia się w edytorze odwiedzin i na pulpicie nawigacyjnym tych samych odwiedzin.

Procedura: meldowanie gościa bez karty

Jeśli gość nie może sam zarejestrować się w kiosku, ale ma być zameldowany bez karty:

1. zarejestrować odwiedziny ręcznie w sposób opisany w rozdziale *Rejestrowanie wizyt, Strona 48*
2. Na pulpicie nawigacyjnym w tabeli odwiedzin kliknij nazwisko gościa w tabeli lub kliknij  , aby edytować te odwiedziny.
3. W oknie dialogowym **Dane osobowe** kliknij przycisk **Dalej**.
4. W oknie dialogowym **Wizyty** w okienku **Karty gości** kliknij przycisk **Zamelduj bez karty**

Procedura: wymeldowanie gościa bez karty

Jeśli gość bez karty opuszcza obiekt:

1. Na pulpicie nawigacyjnym w tabeli odwiedzin kliknij nazwisko gościa w tabeli lub kliknij  , aby edytować te odwiedziny.
2. W oknie dialogowym **Dane osobowe** kliknij przycisk **Dalej**.
3. W oknie dialogowym **Wizyty** w okienku **Karty gości** kliknij przycisk **Wymelduj bez karty**

Patrz

– *Rejestrowanie wizyt, Strona 48*

6.3.9 Dodawanie, usuwanie i wyłączanie z czarnej listy

Osoby niemile widziane w obiekcie można umieszczać na czarnej liście. Dopóki gość znajduje się na tej liście, nie można mu przydzielić karty. W każdej chwili można usunąć gościa z czarnej listy albo przyznać mu tymczasowe wyłączenie, co pozwoli przydzielić kartę.

Umieszczanie na czarnej liście

1. W pulpicie nawigacyjnym w tabeli odwiedzin zaznacz wiersz i kliknij przycisk  , co umożliwi zmodyfikowanie wizyty.
2. W oknie dialogowym **Dane osobowe** kliknij przycisk **Czarna lista**.
3. W wyskakującym oknie potwierdź, że naprawdę chcesz dodać wybraną osobę do czarnej listy.
4. W następnym oknie wprowadź przyczynę umieszczenia na czarnej liście, a następnie potwierdź.

– W edytorze wizyt pojawi się baner **Na czarnej liście**:

– Pod banerem widać dwa przyciski: jeden umożliwiający usunięcie gościa z czarnej listy, a drugi do przyznania czasowego wyłączenia.
– W tabeli wizyt obok imienia i nazwiska każdego gościa umieszczonego na czarnej liście widać trójkąt ostrzegawczy. Na przykład: 

Usuwanie i wyłączanie z czarnej listy

1. W pulpicie nawigacyjnym w tabeli odwiedzin zaznacz wiersz, w którym gość jest oznaczony jako figurujący na czarnej liście, i kliknij przycisk  , co umożliwi zmodyfikowanie wizyty.
2. W oknie dialogowym **Dane osobowe** kliknij jedną z następujących opcji:

– **Usuń**, aby trwale usunąć gościa z czarnej listy.
– **Odstąp**, aby pozostawić gościa na czarnej liście, ale pozwolić na przydzielenie mu karty tylko na tę wizytę.

3. Potwierdź operację w wyskakującym oknie.

6.3.10 Zarządzanie profilami gości

System przechowuje profile gości do czasu, aż sam goście, recepcjoniści lub administratorzy je usuną.
Po upływie okresu przechowywania zdefiniowanego w ustawieniach systemu (domyślnie 12 miesięcy) system usuwa rekord odwiedzin.
Gdy gość lub recepcjonista tworzy nowy profil gościa, profil otrzymuje unikatowy kod alfanumeryczny. Za pomocą tego kodu goście mogą się logować w kiosku dla gości i w ten sposób samodzielnie zarządzać swoimi profilami.

Uwaga!
Chroń identyfikatory gości
Chroń identyfikatory gości przed nieuprawnionym dostępem, ponieważ otwierają one dostęp do danych osobowych.

6.3.11 Przeglądanie rekordów wizyt

1. W pulpicie nawigacyjnym w tabeli odwiedzin zaznacz wiersz i kliknij przycisk  , co umożliwi zmodyfikowanie wizyty.
2. W oknie dialogowym **Dane osobowe** kliknij przycisk **Dalej**.
3. W oknie dialogowym **Bieżąca wizyta** kliknij przycisk **Pokaż wszystkie wizyty** . W oknie dialogowym **Bieżąca wizyta** pojawi się lista poprzednich odwiedzin.

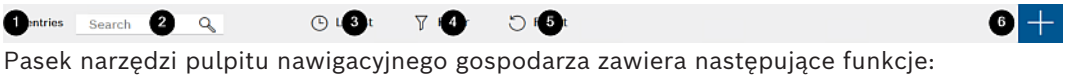
6.4 Gospodarz

Gospodarze to pracownicy, do których przychodzą goście. Mogą oni rejestrować swoje własne umówione wizyty, a także przeglądać system w poszukiwaniu informacji o gościach i rekordów ich odwiedzin: przeszłych, obecnych i przyszłych.

6.4.1 Logowanie do roli gospodarza

1. W przeglądarce otwórz `https://<My_VisMgmt_server>:5706/main/` w odniesieniu do ekranu logowania.
2. Wprowadź nazwę użytkownika odpowiadającą kontu z uprawnieniami wymaganymi do przewidzianej roli.
   Jeśli nie masz konta, skontaktuj się z administratorem systemu.
3. Wprowadź hasło.
4. Kliknij przycisk **Zaloguj się**.

6.4.2 Wyszukiwanie i filtrowanie



Pasek narzędzi pulpitu nawigacyjnego gospodarza zawiera następujące funkcje:

Etykieta	Funkcja
 N **pozycji**	Łączna liczba N odwiedzin (każda wizyta to wiersz w tabeli).

Etykieta	Funkcja
2 **Wyszukaj**	Wyszukiwanie dowolnego tekstu wśród rekordów wizyt w tabeli
3 	Wyświetlanie najnowszych wizyt dodanych do tabeli.
4 	Otwieranie okna dialogowego, w którym można wybrać kryteria filtrowania
5 	Przywracanie domyślnego widoku tabeli i domyślnych wartości wszystkich filtrów.
6 	Otwieranie okna dialogowego, w którym można utworzyć nowy wpis odwiedzin do tabeli

Wyszukaj

Aby szukać imiona i nazwiska gości i gospodarczy, wprowadź tekst alfanumeryczny w polu wyszukiwania, a następnie naciśnij klawisz Enter.

Filtrowanie

- Aby zobaczyć wizyty najbliższe obecnej godzinie, kliknij przycisk **Najnowsze**.
- Aby skonstruować złożony filtr obejmujący stany odwiedzin, daty zarejestrowania i wyrejestrowania oraz numery kart, kliknij przycisk **Filtr**.
  - W wyskakującym oknie dialogowym wprowadź żądane kryteria filtrowania.
  - Kliknij przycisk **Zastosuj**
    . System zredukuje tabelę wizyt tylko do tych umówień, które spełniają kryteria filtrowania.
- Aby usunąć wszystkie kryteria filtrowania, kliknij przycisk **Resetuj**.

6.4.3 Rejestrowanie wizyt

Aby zarejestrować umówienie wizyty dla nowego gościa:
W pulpicie nawigacyjnym programu VisMgmt na pasku narzędzi nad tabelą wizyt jest dostępnych kilka opcji.

1. Kliknij przycisk  , co spowoduje dodanie wiersza do tabeli odwiedzin.
2. W oknie dialogowym **Dane osobowe** w sekcji **Dane ogólne** wprowadź dane osobowe, których administratorzy obiektu wymagają od gości.
3. W sekcji **Szczegóły wizyty** uzupełnij wymagane informacje. Zazwyczaj są to spodziewane godziny wejścia i wyjścia oraz przyczyna odwiedzin.
4. Kliknij przycisk **Zapisz**, aby zapisać umówienie wizyty.
   Odwiedziny pojawią się w pulpicie nawigacyjnym jako wiersz w tabeli wizyt.

6.4.4 Kopiowanie umówień wizyt

Aby zaplanować kolejną wizytę tego samego gościa:

1. W pulpicie nawigacyjnym programu VisMgmt odszukaj istniejącą umówioną wizytę tego samego gościa w tabeli odwiedzin.
2. Kliknij mniejszą ikonę  na końcu wiersza.
3. W oknie dialogowym **Dane osobowe** w sekcji **Szczegóły wizyty** uzupełnij wymagane informacje. Zazwyczaj są to spodziewane godziny wejścia i wyjścia oraz przyczyna odwiedzin.
4. Kliknij przycisk **Zapisz**, aby zapisać umówienie wizyty.
   Odwiedziny pojawią się w pulpicie nawigacyjnym jako wiersz w tabeli wizyt.

6.5 Gość

Goście mogą na terenie obiektu skorzystać z systemu w trybie kiosku i utworzyć własne profile gości oraz podpisać wymagane dokumenty, po czym udać się do recepcji i odebrać gotowe karty gości.

6.5.1 Wprowadzenie do trybu kiosku

Goście zwykle rejestrują swoje odwiedziny i tworzą własne profile na komputerze, który jest powszechnie dostępny w strefie recepcji obiektu o kontrolowanym dostępie. Z względów bezpieczeństwa przeglądarka internetowa komputera działa w trybie kiosku, który umożliwia dostęp tylko do programu VisMgmt. Użytkownik nie może przejść do innych kart, ustawień przeglądarki ani systemu operacyjnego komputera. Wszystkie obsługiwane przeglądarki mają funkcjonalność trybu kiosku, ale jego dokładna konfiguracja zależy od przeglądarki.
Komputer kioskowy zawiera dodatek **Bosch na urządzenia peryferyjne**, który umożliwia fizyczne podłączanie urządzeń peryferyjnych w celu skanowania dokumentów identyfikacyjnych i podpisów.

- Adres URL trybu kiosk to `https://`<Mój_serwer_programu_VisMgmt>`:5706`
- Adres URL do zalogowania się jako Administrator, Recepcjonista lub Gospodarz: `https://`<My_VisMgmt_server>`:5706/main/`

6.5.2 Tworzenie profilu gościa: Samodzielna rejestracja

Nowi goście

Należy pamiętać, że dokładna procedura zależy od tego, jakie urządzenia peryferyjne, czyli np. skanery dokumentów i podpisów oraz aparaty fotograficzne, są podłączone do komputera kioskowego.

1. Na komputerze Kiosk na ekranie powitalnym kliknij opcję **Kontynuuj bez identyfikatora gościa**.
2. Na następnym ekranie kliknij opcję **Samodzielna rejestracja**.
3. Na kolejny ekranie kliknij opcję **Skanuj dokument**.
4. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie, które wskazują wymagania w tym konkretnym obiekcie, na przykład:

- zeskanowanie dokumentów identyfikacyjnych,
- podpisanie wszelkich innych wymaganych dokumentów prawnych,
- zrobienie zdjęcia.

5. System wyświetli zebrane informacje, które można wtedy poprawić i uzupełnić.
6. System zapyta, czy potrzebujesz specjalnych uprawnień dostępu, i w razie potrzeby przekaże tę informację do recepcji.

7. Na koniec procesu rejestracji na ekranie zobaczysz swój niepowtarzalny identyfikator gościa.
   Zabierz go do recepcji, gdzie otrzymasz kartę gościa.

Uwaga!
Unikatowy identyfikator gościa
Starannie zapisz swój identyfikator gościa i nie pokazuj osobom postronnym. Umożliwia on dostęp do Twojego profilu gościa. Za jego pomocą możesz się logować na komputerze kioskowym i w ten sposób szybciej rejestrować przy kolejnych odwiedzinach.

Wracający goście

1. Zaloguj się w kiosku przy użyciu swojego niepowtarzalnego identyfikatora gościa.
2. System wyświetli zebrane informacje, które w razie potrzeby możesz poprawić i uzupełnić.
3. Przejdź do recepcji i odbierz kartę gościa.

6.6 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.

6.6.1 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.

6.7 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.

6.7.1 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).

gospodarz

W kontekście zarządzania gośćmi gospodarzem jest osoba, która przyjmuje gościa.

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.

tryb kiosku

Tryb korzystania z przeglądarki internetowej obłożony rygorystycznymi ograniczeniami. Zazwyczaj umożliwia dostęp tylko do jednej aplikacji internetowej, tzn. użytkownik nie może przejść do ustawień przeglądarki, innych kart ani systemu operacyjnego komputera.

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

Rozwiązania do budynków podnoszące jakość życia

202405131939