



**BOSCH**

# Access Management System

**pl**

Instrukcja instalacji



## Spis treści

<b>1</b>	<b>Informacje o tym dokumencie</b>	<b>4</b>
<b>2</b>	<b>Przegląd systemu AMS</b>	<b>5</b>
<b>3</b>	<b>Instalacja</b>	<b>6</b>
3.1	Wymagania systemowe	6
3.2	Instalowanie serwera	7
3.3	Wyłączanie zapory	9
3.4	Instalowanie klienckich stacji roboczych	9
3.5	Sprawdzanie, czy system jest zainstalowany	13
3.6	Używanie niestandardowych certyfikatów	13
3.6.1	Warunki wstępne	13
3.6.2	Używanie niestandardowych certyfikatów	13
3.7	Rozwiązywanie problemów	17
3.8	Aktualizowanie systemu	17
3.9	Odinstalowanie	20
<b>4</b>	<b>Dane techniczne</b>	<b>22</b>

# 1 Informacje o tym dokumencie

To jest główny podręcznik instalacji oprogramowania Access Management System.

## **Pokrewna dokumentacja**

Następujące zagadnienia omówiono w osobnych dokumentach:

- Konfiguracja i obsługa systemu AMS oraz jego programów pomocniczych.
- Obsługa programu AMS - Map View.

## 2 Przegląd systemu AMS

Access Management System to zaawansowany, specjalistyczny system kontroli dostępu, który pracuje niezależnie lub we współpracy z BVMS — flagowym systemem Bosch do zarządzania danymi wizyjnymi.

Jego siła wynika z wyjątkowego połączenia najnowocześniejszych technologii z technologiami już sprawdzonymi:

- Zaprojektowany z myślą o użyteczności: praktyczny interfejs użytkownika z aplikacją Map View obsługującą metodę „przeciągnij i upuść” oraz zoptymalizowane okna dialogowe rejestracji biometrycznej.
- Zaprojektowany z myślą o bezpieczeństwie danych: obsługuje najnowsze standardy (EU-GDPR 2018), systemy operacyjne, systemy bazodanowe i szyfrowane interfejsy systemowe.
- Zaprojektowany z myślą o odporności na błędy: główne kontrolery dostępu działające w warstwie pośredniej zapewniają automatyczne przełączanie awaryjne i uzupełnianie funkcjonalności lokalnych kontrolerów dostępu w przypadku awarii sieci.
- Zaprojektowany z myślą o przyszłości: regularne aktualizacje i innowacyjne ulepszenia.
- Zaprojektowany pod kątem skalowalności: można go skonfigurować do obsługi małej i dużej liczby użytkowników.
- Zaprojektowany pod kątem współdziałania: interfejsy API typu RESTful umożliwiające współpracę z systemem Bosch do zarządzania danymi wizyjnymi, systemami obsługi zdarzeń i specjalistycznymi rozwiązaniami naszych partnerów.
- Zaprojektowany z myślą o ochronie inwestycji: może pracować na bazie zainstalowanych urządzeń kontroli dostępu, przy okazji poprawiając ich efektywność.

## 3 Instalacja

### Ogólna procedura

Instalacja systemu obejmuje użycie dwóch oddzielnych instalatorów: serwera i klienta.

Ogólna kolejność instalacji jest następująca:

1. Sprawdzenie wymagań systemowych.
2. Przed zainstalowaniem wszystkich klienckich stacji roboczych:
  - Zainstaluj oprogramowanie na serwerze i sprawdź poprawność instalacji.
  - Utwórz na serwerze co najmniej jedną autoryzację stacji roboczej na potrzeby klienckich stacji roboczych i dostosuj ustawienia zapory, aby umożliwić połączenia klient-serwer.
3. Zainstaluj certyfikat HTTPS na każdym komputerze klienckim.
4. Zainstaluj klientów.

### Patrz

- *Importowanie certyfikatu HTTPS, Strona 10*
- *Sprawdzanie, czy system jest zainstalowany, Strona 13*

## 3.1 Wymagania systemowe

### Minimalne wymagania techniczne serwera systemu AMS

Server	
Obsługiwane systemy operacyjne. Instalacje w innych systemach operacyjnych mogą zakończyć się powodzeniem, ale nie są objęte gwarancją.	<ul style="list-style-type: none"> <li>– Windows Server 2016 (64-bitowy, Standard, Datacenter)</li> <li>– Windows 10, version 1809 (LTSC)</li> <li>– <b>Należy upewnić się, że zainstalowane są najnowsze aktualizacje oprogramowania.</b></li> <li>– <b>Uwaga:</b> domyślny system bazodanowy dostarczany z tą wersją systemu to SQL Server 2017 Express z usługami zaawansowanymi</li> </ul>
Minimalne wymagania sprzętowe	<ul style="list-style-type: none"> <li>– Procesor Intel i5 z co najmniej 4 rdzeniami fizycznymi</li> <li>– 8 GB RAM (32 GB — zalecane)</li> <li>– 200 GB wolnego miejsca na dysku twardym (zalecane dyski SSD)</li> <li>– Karta graficzna               <ul style="list-style-type: none"> <li>– 256 MB pamięci RAM</li> <li>– Rozdzielczość 1280x1024 (jeśli chcesz uruchomić klienta Map View na serwerze AMS, zastosuj rozdzielczość graficzną zalecaną dla tego klienta).</li> <li>– Co najmniej 32 tys. kolorów</li> </ul> </li> <li>– Karta Ethernet 1 Gbit/s</li> <li>– Wolny port USB lub udział sieciowy na pliki instalacyjne</li> </ul>

### Minimalne wymagania techniczne klienta systemu AMS

Klient, w tym klient aplikacji Map View	
Obsługiwane systemy operacyjne.	<ul style="list-style-type: none"> <li>– Windows 10, wersja 1809 (LTSC)</li> </ul>

<b>Klient, w tym klient aplikacji Map View</b>	
Instalacje w innych systemach operacyjnych mogą zakończyć się powodzeniem, ale nie są objęte gwarancją.	<ul style="list-style-type: none"> <li>- <b>Należy upewnić się, że zainstalowane są najnowsze aktualizacje oprogramowania.</b></li> </ul>
Minimalne wymagania sprzętowe	<ul style="list-style-type: none"> <li>- Intel i5 lub nowszy</li> <li>- 8 GB RAM (16 GB — zalecane)</li> <li>- 20 GB wolnego miejsca na dysku twardym</li> <li>- Karta graficzna               <ul style="list-style-type: none"> <li>- 256 MB pamięci RAM</li> <li>- Do korzystania z menedżera okien dialogowych AMS wystarcza rozdzielczość 1280x1024.</li> <li>- W przypadku aplikacji AMS Map View wymagana jest rozdzielczość 1920x1080 (Full HD).</li> <li>- Co najmniej 32 tys. kolorów</li> </ul> </li> <li>- DirectX® 11</li> <li>- Karta Ethernet 1 Gbit/s</li> <li>- Wolny port USB lub udział sieciowy na pliki instalacyjne</li> </ul>

#### Minimalne wymagania techniczne dodatkowego kontrolera MAC

<b>Serwer kontrolera MAC</b>	
Obsługiwane systemy operacyjne. Instalacje w innych systemach operacyjnych mogą zakończyć się powodzeniem, ale nie są objęte gwarancją.	<ul style="list-style-type: none"> <li>- Windows Server 2016 (64-bitowy, Standard, Datacenter)</li> <li>- Windows 10, version 1809 (LTSC)</li> <li>- <b>Należy upewnić się, że zainstalowane są najnowsze aktualizacje oprogramowania.</b></li> </ul>
Minimalne wymagania sprzętowe	<ul style="list-style-type: none"> <li>- Intel i5 lub nowszy</li> <li>- 8 GB RAM (16 GB — zalecane)</li> <li>- 20 GB wolnego miejsca na dysku twardym</li> <li>- Karta graficzna               <ul style="list-style-type: none"> <li>- 256 MB pamięci RAM</li> <li>- Rozdzielczość 1280x1024</li> <li>- Co najmniej 32 tys. kolorów</li> </ul> </li> <li>- Karta Ethernet 1 Gbit/s</li> </ul>

## 3.2 Instalowanie serwera

### Zanim zaczniesz

1. Upewnij się, że nazwa hosta odpowiedniego żądanego serwera odpowiada regułom określonym w poniższym polu.
2. Upewnij się, że system nie jest już zainstalowany (patrz **Sprawdzanie, czy system jest zainstalowany**).

3. Skopiuj pakiet instalacyjny na serwer.

**Uwaga!**

Do nazw komputerów stosuje się konwencje NETBIOS, np.:

- Nazwa jest nie dłuższa niż 15 znaków.
- Nazwa **nie** zaczyna się od cyfry [0–9].
- Nazwa zawiera tylko znaki łacińskie, bez znaków diakrytycznych.
- Więcej informacji można znaleźć pod adresem <https://support.microsoft.com/en-us/help/909264/naming-conventions-in-active-directory-for-computers-domains-sites-and>.

**Rozpoczęcie instalacji serwera**

1. Kliknij dwukrotnie pakiet instalacyjny oprogramowania.
2. Kliknij dwukrotnie pozycję **Serwer**.
3. Kliknij prawym przyciskiem myszy plik **AMS Server Setup.exe** i z menu kontekstowego wybierz opcję **Uruchom jako administrator**.
  - Spowoduje to wyświetlenie okna kreatora przygotowania do instalacji. Postępuj zgodnie z instrukcjami wyświetlanymi w kreatorze.
4. Zaznacz składniki, które chcesz zainstalować, i kliknij przycisk **Dalej>**.
  - Zależnie od składników, które są już zainstalowane, kreator wyświetli listę oprogramowania, które zostanie zainstalowane:
  - Jeśli widzisz jakieś nieobowiązkowe składniki, których nie potrzebujesz, anuluj ich wybór na tym etapie.
5. Przeczytaj **Umowę licencyjną z użytkownikiem końcowym** i kliknij przycisk **Akceptuj**. Jeśli nie akceptujesz warunków umowy, kliknij przycisk **Odrzuć**, aby przerwać instalację.
6. Wprowadź dane konfiguracyjne serwera baz danych SQL.
  - Dane konfiguracyjne serwera baz danych SQL:
    - Serwer SQL: nazwa hosta, na którym będzie działało wystąpienie programu SQL Server. Użyj lokalnego komputera.
    - Instancja SQL: nazwa wystąpienia serwera SQL
    - Baza danych AMS: nazwa bazy danych
    - Nazwa użytkownika SQL: nazwa logowania umożliwiająca dostęp do programu SQL Server
7. Kliknij przycisk **Dalej>**.
8. Jeśli domyślna ścieżka instalacji serwera jest akceptowalna, kliknij przycisk **Dalej>**. Jeśli chcesz wybrać inną ścieżkę instalacji (tylko na dyskach lokalnych), kliknij przycisk **Przeglądaj**.
  - Zaleca się używanie domyślnej ścieżki instalacji *C:\Program Files (86)*, ponieważ wtedy pliki mogą być modyfikowane tylko przez administratorów systemu.
  - Jeśli wybierzesz inną ścieżkę instalacji, upewnij się, że jest ona odpowiednio chroniona przed nielegalnym dostępem.
9. Aby kontynuować, kliknij przycisk **Dalej>**.
  - Na tej stronie konfiguruje się nazwę hosta interfejsu API.
10. Sprawdź podsumowanie informacji przedinstalacyjnych i kliknij przycisk **Zainstaluj**.
  - Zostanie wyświetlone podsumowanie zawierające wszystkie składniki wybrane do zainstalowania.
11. Obserwuj pasek postępu instalacji.
  - Gdy ruchomy zielony pasek dotrze do mniej więcej środka paska postępu, minie kilka minut, zanim znów zacznie się ruszać. Poczekaj cierpliwie.



- Zostanie otwarte inne okno dialogowe służące do konfiguracji bazy danych AMS.
  - Jeśli baza danych jest już zainstalowana, zostanie zaktualizowana.
  - W przeciwnym razie zostanie utworzona nowa baza danych i konieczne będzie utworzenie nowego hasła do konta *sa*. **WAŻNE:** przechowuj hasło bezpiecznie, ponieważ będzie wymagane przy aktualizacji i innych operacjach. Tworzenie bazy danych może potrwać kilka minut. Poczekaj na zamknięcie okna dialogowego.
- 12. Po zakończeniu operacji kliknij przycisk **Dalej>** i sprawdź podsumowanie informacji poinstalacyjnych.
  - Zostanie wyświetlone podsumowanie ze wszystkimi zainstalowanymi składnikami.
- 13. Kliknij przycisk **Zakończ**, aby zakończyć instalację.
  - Zostanie otwarte okno dialogowe z prośbą o ponowne uruchomienie. Ponowne uruchomienie komputera jest niezbędne do ukończenia instalacji systemu.
- 14. Kliknij przycisk **Tak**, aby ponownie uruchomić komputer.
  - Komputer uruchomi się ponownie.
- 15. Sprawdź, czy system jest poprawnie zainstalowany (patrz **Sprawdzanie, czy system jest zainstalowany**).
  - Jeśli tak, pierwsza instalacja aplikacji systemowej została zakończona. Ikona systemu pojawi się na pulpicie.

#### Logowanie po raz pierwszy

1. Kliknij dwukrotnie ikonę aplikacji systemu na pulpicie.
2. Wprowadź domyślną nazwę użytkownika i hasło.
  - Domyślna nazwa użytkownika i hasło to **Administrator**. Należy pamiętać, że w hasle rozróżnia się wielkość liter, natomiast w nazwie użytkownika już nie.
3. Kliknij przycisk **Logowanie**.
  - Pojawi się okno dialogowe z prośbą o zmianę hasła.
  - Podczas logowania po raz pierwszy musisz w wyskakującym oknie dialogowym zmienić hasło.
4. Kliknij przycisk **OK**, aby się zalogować.

#### Patrz

- *Sprawdzanie, czy system jest zainstalowany, Strona 13*
- *Rozpoczęcie aktualizacji serwera, Strona 17*

## 3.3

### Wyłączanie zapory

Po pomyślnym zainstalowaniu serwera, a przed zainstalowaniem klienckich stacji roboczych, należy zdezaktywować zaporę. Umożliwia to klienckim stacjom roboczym i zewnętrznym komputerom kontrolerów MAC łatwe łączenie z serwerem podczas wstępnej konfiguracji.

## 3.4

### Instalowanie klienckich stacji roboczych

#### Zanim zaczniesz

1. Upewnij się, że nazwa hosta odpowiedniego docelowego serwera klienckiego odpowiada regułom określonym w poniższym polu.
2. Skopiuj pakiet instalacyjny na docelową stację roboczą klienta.

**Uwaga!**

Do nazw komputerów stosuje się konwencje NETBIOS, np.:

- Nazwa jest nie dłuższa niż 15 znaków.
- Nazwa **nie** zaczyna się od cyfry [0–9].
- Nazwa zawiera tylko znaki łacińskie, bez znaków diakrytycznych.
- Więcej informacji można znaleźć pod adresem <https://support.microsoft.com/en-us/help/909264/naming-conventions-in-active-directory-for-computers-domains-sites-and>.

**Certyfikaty HTTPS dla klienckich stacji roboczych**

Serwer systemu obsługuje kilka interfejsów API. Te interfejsy API komunikują się za pośrednictwem protokołu HTTPS i używają certyfikatu z podpisem własnym. Program konfiguracyjny serwera tworzy ten certyfikat z podpisem własnym i zainstaluje go na serwerze. Aby umożliwić bezpieczną komunikację między serwerem i klientami, certyfikat z serwera musi być kopiowany i importowany ręcznie na każdym komputerze klienckim (patrz **Importowanie certyfikatu HTTPS**).

**Importowanie certyfikatu HTTPS**

1. Przejdź do pliku *C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates\Access Management System Internal CA.cer*
2. Skopiuj certyfikat do komputera klienta.
3. Na komputerze klienckim kliknij dwukrotnie certyfikat.
  - Zostanie wyświetlone okno dialogowe certyfikatu.
4. Kliknij przycisk **Zainstaluj certyfikat**.
  - Otworzy się Kreator importu certyfikatów.
5. Zaznacz opcję **Komputer lokalny** (zalecane) i kliknij przycisk **Dalej>**.
6. Zaznacz opcję **Umieść wszystkie certyfikaty w następującym magazynie** i określ lokalizację dla certyfikatu (zalecane).
7. Kliknij przycisk **Przeglądaj**.
  - Otworzy się okno dialogowe wyboru magazynu certyfikatów.
8. Zaznacz opcję *Trusted Root Certification Authorities* i kliknij przycisk **OK** (zalecane).
  - Okno dialogowe wyboru magazynu certyfikatów zostanie zamknięte.
9. W Kreatorze importu certyfikatów kliknij przycisk **Dalej>**.
10. Kliknij przycisk **Zakończ**, aby zaimportować certyfikat.
  - Proces importowania certyfikatu został zakończony.

**Uwaga!**

Jeśli certyfikat HTTPS nie jest zainstalowany, nie będzie można uruchomić aplikacji.

Pamiętaj, że nie musisz importować certyfikatu do komputera serwera, ponieważ odbywa się to automatycznie podczas instalacji serwera. Dotyczy to tylko samodzielnych klienckich stacji roboczych.

## Integracja interfejsu API AMS z systemem BVMS

Aby zintegrować interfejs AMS API z systemem BVMS (Bosch Video Management System) w wersji 10.1 lub nowszej, zaimportuj certyfikat z podpisem własnym na komputer z zainstalowanym oprogramowaniem BVMS (patrz **Importowanie certyfikatu HTTPS**).

### Rozpoczęcie instalacji klienta

1. Kliknij dwukrotnie pakiet instalacyjny oprogramowania.
2. Kliknij dwukrotnie pozycję **Klient**.
3. Kliknij dwukrotnie plik **AMS Client Setup.exe**.
  - Spowoduje to wyświetlenie okna kreatora przygotowania do instalacji. Postępuj zgodnie z instrukcjami wyświetlanymi w kreatorze.
4. Zaznacz składniki, które chcesz zainstalować, i kliknij przycisk **Dalej>**.
  - W zależności od tego, co jest już dostępne w systemie, kreator wybierze wymagane pakiety Microsoft dla Visual C++ i .NET.
  - Składniki opcjonalne:
    - Klient
    - Map View
5. Przeczytaj **Umowę licencyjną z użytkownikiem końcowym** i kliknij przycisk **Akceptuj**. Jeśli nie akceptujesz umowy, kliknij przycisk **Odrzuć**, a operacja zostanie anulowana.
6. Jeśli domyślna ścieżka instalacji na klienckiej stacji roboczej jest akceptowalna, kliknij przycisk **Dalej>**. Jeśli chcesz wybrać inną ścieżkę instalacji (tylko na dyskach lokalnych), kliknij przycisk **Przeglądaj**.
7. Wprowadź adres serwera. Format adresu: `<hostname>:4999/tcp`
  - Domyślnie kreator instalacji zainstaluje klienta systemu na dysku lokalnym w folderze `C:\Program Files (86)` (zalecane).
  - Pliki instalowane w lokalnym folderze `C:\Program Files (86)` mogą być modyfikowane tylko przez użytkowników mających uprawnienia administratora, więc zaleca się używanie tego domyślnego folderu.
8. Jeśli domyślna ścieżka instalacji aplikacji Map View jest akceptowalna, kliknij przycisk **Dalej>**.
9. Jeśli chcesz wybrać inną ścieżkę instalacji (tylko na dyskach lokalnych), kliknij przycisk **Przeglądaj**.
10. Wprowadź adres wykrywania.
  - Domyślnie kreator instalacji instaluje aplikację Map View na dysku lokalnym w ścieżce `C:\Program Files (86)` (zalecane).
  - Aplikacja Map View połączy się z lokalizacją pod adresem wykrywania, aby wykryć punkty końcowe systemu. Ten adres jest adresem URL zawierającym nazwę serwera i numer portu punktu końcowego wykrywania.
11. Sprawdź podsumowanie informacji przedinstalacyjnych i kliknij przycisk **Zainstaluj**.
  - Zostanie wyświetlone podsumowanie zawierające wszystkie składniki wybrane do zainstalowania.
12. Obserwuj pasek postępu instalacji.
  - Poczekaj, aż operacja zostanie zakończona.
13. Po zakończeniu operacji kliknij przycisk **Dalej>** i sprawdź podsumowanie informacji poinstalacyjnych.
  - Wyświetli się wykaz wszystkich zainstalowanych składników.
14. Kliknij przycisk **Zakończ**, aby zakończyć instalację.
15. Ponownie uruchom komputer.

16. Sprawdź, czy system jest zainstalowany (patrz **Sprawdzanie, czy system jest zainstalowany**).
  - Po zakończeniu instalacji klienta AMS i aplikacji Map View, obie ikony aplikacji pojawiają się na pulpicie. Domyślna nazwa użytkownika i hasło to **Administrator**. Należy pamiętać, że w hasle rozróżnia się wielkość liter, natomiast w nazwie użytkownika już nie.

#### Przed uruchomieniem klienta

Przed zalogowaniem się na kliencie należy skonfigurować kliencką stację roboczą na serwerze.

Wykonaj poniższą procedurę:

1. Uruchom klienta na komputerze serwera.
2. Kliknij kolejno opcje **Konfiguracja > Dane urządzenia**.
  - Otworzy się nowe okno dialogowe.
3. Na górnym pasku narzędzi kliknij ikonę **Stacje robocze**.
4. Na górnym pasku narzędzi kliknij ikonę **Nowy**.
5. Na karcie **Stacja robocza** wypełnij puste pola.
  - Pola:
    - **Nazwa**: wstaw nazwę hosta klienckiej stacji roboczej (obowiązkowe).
    - **Opis**: wstaw opis (opcjonalnie).
    - **Logowanie za pomocą czytnika**: wykonaj logowanie za pomocą czytnika (opcjonalnie).
    - **Automatyczne wylogowanie po: X sekundach** (opcjonalnie). Ustaw automatyczne wylogowywanie, jeśli chcesz, aby aplikacja wylogowywała Cię automatycznie po określonym czasie.
  - Zwróć uwagę, że podkreślone pola są obowiązkowe.
6. Na górnym pasku narzędzi kliknij ikonę **Zapisz**, aby zapisać zmiany.
  - Teraz możesz się logować z klienckiej stacji roboczej.

#### Logowanie po raz pierwszy

1. Kliknij dwukrotnie ikonę aplikacji na pulpicie.
2. Wprowadź domyślną nazwę użytkownika i hasło.
  - Domyślną nazwą użytkownika i hasłem dla obu aplikacji klienckich jest **Administrator**. Należy pamiętać, że w hasle rozróżnia się wielkość liter, natomiast w nazwie użytkownika już nie.
3. Kliknij przycisk **Logowanie**.
  - Podczas logowania po raz pierwszy musisz zmienić hasło. Wyświetli się okno dialogowe.
4. Kliknij przycisk **OK**, aby wprowadzić nowe hasło w następnym oknie dialogowym.
  - Należy używać silnych haseł o długości co najmniej 8 znaków.
5. Wprowadź nowe hasło i kliknij przycisk **Zmień**. Jeśli chcesz zrezygnować ze zmiany hasła, kliknij przycisk **Anuluj**.
  - Wyświetli się okno dialogowe potwierdzające zmianę hasła.
6. Kliknij przycisk **OK**, aby się zalogować.



#### Uwaga!

Na kliencie i serwerze musi być zainstalowana ta sama wersja klienta AMS. Nie próbuj uzyskiwać dostępu do serwera z innej wersji klienta AMS.

#### Patrz

- *Sprawdzanie, czy system jest zainstalowany, Strona 13*

- *Importowanie certyfikatu HTTPS, Strona 10*

## 3.5 Sprawdzenie, czy system jest zainstalowany

### Sprawdzenie, czy system jest zainstalowany

System jest zainstalowany, jeśli:

- Ikony systemu są widoczne na pulpicie.
- Następujące usługi znajdują się w aplikacji Usługi systemu Windows (**Start > Wyszukaj > `service.msc`**): DMS, MAC, Interfejs API dostępu, Usługa tożsamości, Interfejs API mapy, Interfejs API stanów.
- System znajduje się w domyślnej ścieżce instalacji: `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\`

## 3.6 Używanie niestandardowych certyfikatów

W interfejsach API systemu AMS można skonfigurować korzystanie z certyfikatów innych niż certyfikaty z podpisem własnym tworzone automatycznie podczas instalacji.

Jest to przydatne, gdy organizacja ma już infrastrukturę klucza publicznego (PKI) z własnym urzędem certyfikacji (CA).

### 3.6.1 Warunki wstępne

- Posiadanie zaufanego pliku certyfikatu głównego.
- Publiczne i prywatne części certyfikatu muszą być umieszczone w katalogu serwera AMS `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates`

Przykłady publicznych i prywatnych części certyfikatu:

- `Access Management System Test CA.cer` (część publiczna)
- `CustomRootTestCA.pfx` (część prywatna)

### 3.6.2 Używanie niestandardowych certyfikatów

#### Otwarcie sesji narzędzia PowerShell

Uruchom jako administrator program PowerShell na serwerze AMS w folderze: `C:`

```
\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates
```

#### Usunięcie zainstalowanych certyfikatów

1. Usuń certyfikaty zainstalowane podczas instalacji systemu AMS.
2. Wykonaj polecenie `"RemoveAceApiCertificates.ps1"` w otwartej sesji narzędzia PowerShell.

#### Edytowanie skryptu tworzenia certyfikatów interfejsów API

1. Otwórz plik programu PowerShell `"CreateAceApiCertificatesFromOwnRoot.ps1"` w edytorze tekstów i zmień następujące nazwy plików na nazwy swoich certyfikatów:
  - `CustomRootTestCA.pfx`
  - `Access Management System Test CA.cer`

- Należy pamiętać, że każda nazwa pliku występuje tylko raz w skrypcie.
2. Zapisz zmiany.

#### Uruchomienie skryptu tworzenia certyfikatów interfejsów API

1. Wykonaj polecenie `CreateAceApiCertificatesFromOwnRoot.ps1` w sesji PowerShell otwartej powyżej.
2. Wprowadź hasło prywatnego certyfikatu.
  - Zostaną utworzone i zainstalowane niezbędne certyfikaty API:
  - Certyfikat główny jest zainstalowany.

#### Sprawdzenie instalacji certyfikatów wśród certyfikatów systemu Windows dla bieżącego użytkownika i komputera lokalnego

Certyfikat jest zainstalowany, jeśli:

- Certyfikat główny jest zainstalowany na listach *Current User Personal Certificates*, *Trusted Root Certificates* i *Local Computer Trusted Root Certificates*
- Certyfikaty interfejsów API są zainstalowane na liście *Local Computer Personal Certificates*

#### Zaktualizowanie ustawień aplikacji Thumbprint dla każdego interfejsu API

Dla każdego interfejsu API należy zaktualizować odcisk palca.

Interfejs API dostępu	<ol style="list-style-type: none"> <li>1. Otwórz folder <code>C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Access API</code>.</li> <li>2. Zamień wartości w pliku <code>appsettings.json</code>, wiersz <code>"Thumbprint"</code>:</li> <li>3. Otwórz folder <b>Certyfikaty na komputerze lokalnym &gt; Osobiste &gt; Certyfikaty &gt; Przyjazna nazwa: Access Management System Access API</b>.</li> <li>4. Zaznacz i otwórz zainstalowany certyfikat <code>"Access Management System Access API"</code> &gt; <b>Szczegóły</b>.</li> <li>5. Przewiń listę w dół do pozycji <code>"Thumbprint"</code>.</li> <li>6. Zaznacz opcję <code>Thumbprint</code>.</li> <li>7. Skopiuj wyświetlany odcisk palca (np. <code>"da"</code>).</li> <li>8. Wklej odcisk palca bez spacji do pliku <code>appsettings.json</code> w folderze <code>C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Access API</code>.           <ul style="list-style-type: none"> <li>- (np. <code>"Thumbprint": "53d3588285bd570c9799e883b27ef1b139ba28da"</code>)</li> </ul> </li> </ol>
-----------------------	---

Interfejs API mapy	<ol style="list-style-type: none"> <li>1. Otwórz folder <code>C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Map API</code>.</li> <li>2. Zamień wartości w pliku <code>appsettings.json</code>, wiersz <code>"Thumbprint"</code>:</li> </ol>
--------------------	--

	<ol style="list-style-type: none"> <li>3. Otwórz folder <b>Certyfikaty na komputerze lokalnym &gt; Osobiste&gt; Certyfikaty &gt; Przyjazna nazwa:</b> <i>Access Management System Map API</i>.</li> <li>4. Zaznacz i otwórz zainstalowany certyfikat "<i>Access Management System Map API</i>" &gt; <b>Szczegóły</b>.</li> <li>5. Przewiń listę w dół do pozycji "<i>Thumbprint</i>".</li> <li>6. Zaznacz opcję <i>Thumbprint</i>.</li> <li>7. Skopiuj wyświetlany odcisk palca (np. "<i>e8</i>").</li> <li>8. Wklej odcisk palca bez spacji do pliku <i>appsettings.json</i> w folderze <i>C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Map API</i> .</li> </ol> <p>– (np. "<i>Thumbprint</i>": "<i>3cef0c43be36ee01d8a6ea2f59f170cde96168e8</i>")</p>
--	---

Interfejs API stanów	<ol style="list-style-type: none"> <li>1. Otwórz folder <i>C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\States API</i>.</li> <li>2. Zamień wartości w pliku <i>appsettings.json</i>, wiersz „<i>Thumbprint</i>”:</li> <li>3. Otwórz folder <b>Certyfikaty na komputerze lokalnym &gt; Osobiste&gt; Certyfikaty &gt; Przyjazna nazwa:</b> <i>Access Management System States API</i>.</li> <li>4. Zaznacz i otwórz zainstalowany certyfikat "<i>Access Management System States API</i>" &gt; <b>Szczegóły</b>.</li> <li>5. Przewiń listę w dół do pozycji "<i>Thumbprint</i>"..</li> <li>6. Zaznacz opcję <i>Thumbprint</i>.</li> <li>7. Skopiuj wyświetlany odcisk palca (np. "<i>e2</i>").</li> <li>8. Wklej odcisk palca bez spacji do pliku <i>appsettings.json</i> w folderze <i>C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\States API</i>.</li> </ol> <p>– (np. "<i>Thumbprint</i>": "<i>37c0bb09d4cab985b620da1c667597ef43b5f8e2</i>")</p>
----------------------	---

Serwer tożsamości:	<ol style="list-style-type: none"> <li>1. Otwórz folder <i>C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Identity Server</i>.</li> <li>2. Zamień wartości w pliku <i>appsettings.json</i>, wiersz "<i>Thumbprint</i>":</li> <li>3. Otwórz folder <b>Certyfikaty na komputerze lokalnym &gt; Osobiste&gt; Certyfikaty &gt; Przyjazna nazwa:</b> <i>Access Management System Identity Server</i>.</li> <li>4. Zaznacz i otwórz zainstalowany certyfikat "<i>Access Management Identity Server</i>" &gt; <b>Szczegóły</b>.</li> <li>5. Przewiń listę w dół do pozycji "<i>Thumbprint</i>"..</li> <li>6. Zaznacz opcję <i>Thumbprint</i>.</li> </ol>
--------------------	---

7. Skopiuj wyświetlany odcisk palca.
8. Wklej odcisk palca bez spacji do pliku `appsettings.json` w folderze `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Identity Server`.
9. Wklej odciski palca pozostałych interfejsów API w odpowiednich miejscach w tym pliku.
  - Przykład:
    - Dla `"Name": "AccessApi"`  
`"Thumbprint":`  
`"53d3588285bd570c9799e883b27ef1b139ba28da"`
    - Dla `"Name": "MapApi"`  
`"Thumbprint":`  
`"3cef0c43be36ee01d8a6ea2f59f170cde96168e8"`
    - Dla `"Name": "StatesApi"`  
`"Thumbprint":`  
`"37c0bb09d4cab985b620da1c667597ef43b5f8e2"`

#### Zatrzymywanie i uruchamianie usług

1. Otwórz usługi systemu Windows.
2. Kliknij prawym przyciskiem myszy następujące usługi i dla każdej z nich wybierz polecenie „Zatrzymaj”:
  - Interfejs Access API do systemu Access Management System
  - Serwer tożsamości w systemie Access Management System
  - Interfejs Map API w systemie Access Management System
  - Interfejs Stanów API w systemie Access Management System
    - Po zatrzymaniu wszystkich czterech usług kliknij je ponownie prawym przyciskiem myszy i wybierz polecenie **Uruchom**.

#### Instalowanie certyfikatu głównego na komputerze klienckim

1. Za pomocą Menedżera plików systemu Windows skopiuj certyfikat główny `"Access Management System Test CA.cer"` i wklej go na komputerze klienckim, gdzie są zainstalowane aplikacje klienckie „Map View” i „AMS” (Menedżer okien dialogowych). Na przykład wklej go w folderze Pobrane.
2. Zainstaluj certyfikat główny:
  - W Menedżerze plików kliknij prawym przyciskiem myszy **plik certyfikatu** i wybierz kolejno opcje **Zainstaluj certyfikat > Bieżący użytkownik > Dalej>**. Wybierz kolejno opcje **Umieść wszystkie certyfikaty w następującym magazynie > Przeglądaj>**. Wybierz kolejno opcje **Zaufane główne urzędy certyfikacji > Dalej > Zakończ > OK**.

#### Testowanie certyfikatów interfejsów API na komputerze klienckim.

Certyfikaty interfejsów API należy przetestować na komputerze klienta, gdzie są zainstalowane aplikacje klienckie Map View i AMS (Menedżer okien dialogowych).

Na komputerze klienckim uruchom przeglądarkę Google Chrome.

- Aby przetestować działanie serwera tożsamości, wprowadź następujący adres: `https://[ServerHostname]:44333/.well-known/openid-configuration`



- Kliknij prawym przyciskiem ikonę blokady informacji w witrynie > sprawdź, czy widać podpis „Certyfikat (ważny)”, oraz sprawdź, czy w sekcji „Wystawiony przez” jest używany właściwy certyfikat.
- Aby przetestować działanie interfejsu Access API, wprowadź następujący adres:  
`https://[ServerHostname]:44347/swagger`
  - Kliknij prawym przyciskiem ikonę blokady informacji w witrynie > sprawdź, czy widać podpis „Certyfikat (ważny)”, oraz sprawdź, czy w sekcji „Wystawiony przez” jest używany właściwy certyfikat.
- Aby przetestować działanie interfejsu API stanów, wprowadź następujący adres:  
`https://[ServerHostname]:62901/swagger`
  - Kliknij prawym przyciskiem ikonę blokady informacji w witrynie > sprawdź, czy widać podpis „Certyfikat (ważny)”, oraz sprawdź, czy w sekcji „Wystawiony przez” jest używany właściwy certyfikat.
- Aby przetestować działanie interfejsu Map API, wprowadź następujący adres: `https://[ServerHostname]:61801/$metadata`
  - Kliknij prawym przyciskiem myszy na pasku adresu ikonę kłódki i sprawdź, czy widać podpis „Certificate (Valid)” [Certyfikat (ważny)], oraz sprawdź, czy wartość w polu „Issued by” (Wystawiony przez) jest prawidłowa.

#### Użycie certyfikatu w systemie AMS.

Na komputerze klienckim uruchom aplikację Map View i się zaloguj.

## 3.7 Rozwiązywanie problemów

W razie niepowodzenia instalacji pasek postępu zmienia kolor na czerwony. Może się też pojawić dodatkowy opis błędu.

Kliknij przycisk **Dalej**, aby przejść do strony podsumowania, gdzie znajdują się informacje o składniku, w którym wystąpił błąd.

## 3.8 Aktualizowanie systemu

#### Zanim zaczniesz

1. Zaloguj się na komputerze serwera.
2. Sprawdź, czy jest zainstalowana poprzednia wersja systemu (patrz **Sprawdzenie, czy system jest zainstalowany**).
3. Skopiuj nowy pakiet instalacyjny do komputera serwera.



#### Uwaga!

Na kliencie i serwerze musi być zainstalowana ta sama wersja klienta AMS. Nie próbuj uzyskiwać dostępu do serwera z innej wersji klienta AMS.

#### Rozpoczęcie aktualizacji serwera

1. Kliknij dwukrotnie nową wersję pakietu instalacyjnego oprogramowania.
2. Wybierz język interfejsu.
3. Kliknij dwukrotnie pozycję **Serwer**.

4. Kliknij prawym przyciskiem myszy plik **AMS Server Setup.exe** i z menu kontekstowego wybierz opcję **Uruchom jako administrator**.
  - Spowoduje to wyświetlenie okna kreatora przygotowania do instalacji.
  - Wybierz składnik, który chcesz zaktualizować, i kliknij przycisk **Dalej>**.
  - Zależnie od składników, które są już zainstalowane, kreator zaznaczy składniki, które mogą zostać zaktualizowane domyślnie.
  - Możesz wybrać zaktualizowanie lub pominięcie aktualizacji składników.
  - Komponenty, których nie można zaktualizować, zostaną domyślnie oznaczone podpisem **Pomiń**.
5. Przeczytaj **Umowę licencyjną z użytkownikiem końcowym** i kliknij przycisk **Akceptuj**. Jeśli nie akceptujesz umowy, kliknij przycisk **Odrzuć**, a operacja zostanie anulowana.
6. Wprowadź dane konfiguracyjne serwera baz danych SQL.
  - Dane konfiguracyjne serwera baz danych SQL:
    - Serwer SQL: nazwa hosta, na którym działa wystąpienie programu SQL Server, np. Komputer lokalny (zalecane)
    - Instancja SQL: nazwa wystąpienia serwera SQL
    - Baza danych AMS: nazwa bazy danych
    - Nazwa użytkownika SQL: nazwa logowania umożliwiająca dostęp do programu SQL Server
7. Kliknij przycisk **Dalej>**.
  - Następne okno pokazuje ścieżkę instalacji, w której będzie przechowywany serwer systemu.
  - Domyślnie kreator instalacji zainstaluje serwer systemu na dysku lokalnym w ścieżce *C:\Program Files (86)* (zalecane).
  - Pliki zainstalowane na dysku lokalnym w folderze *C:\Program Files (86)* mogą być modyfikowane tylko przez użytkowników z uprawnieniami administratora. Zapewnia to bezpieczeństwo, ponieważ użytkownicy nieposiadający uprawnień administratora nie mogą modyfikować plików związanych z systemem.
8. Aby kontynuować, kliknij przycisk **Dalej>**.
9. Sprawdź podsumowanie informacji przedaktualizacyjnych i kliknij przycisk **Zainstaluj**.
  - Zostanie wyświetlone podsumowanie zawierające wszystkie składniki wybrane do zaktualizowania.
10. Obserwuj pasek postępu instalacji.
  - Gdy ruchomy zielony pasek dotrze do mniej więcej środka paska postępu, minie kilka minut, zanim znów zaczną się ruszać. Poczekaj cierpliwie.
  - Zostanie otwarte inne okno dialogowe służące do konfiguracji bazy danych AMS.
    - Jeśli baza danych jest już zainstalowana, zostanie zaktualizowana.
    - W przeciwnym razie zostanie utworzona nowa baza danych i konieczne będzie utworzenie nowego hasła do konta *sa*. **WAŻNE:** przechowuj hasło bezpiecznie, ponieważ będzie wymagane przy aktualizacji i innych operacjach. Tworzenie bazy danych może potrwać kilka minut. Poczekaj na zamknięcie okna dialogowego.
11. Po zakończeniu operacji kliknij przycisk **Dalej>** i sprawdź podsumowanie informacji poaktualizacyjnych.
  - Zostanie wyświetlone podsumowanie ze wszystkimi zaktualizowanymi składnikami.
12. Kliknij przycisk **Zakończ**, aby dokończyć instalowanie zaktualizowanej wersji systemu.
13. Uruchom ponownie komputer (zalecane).
  - Komputer uruchomi się ponownie.

14. Sprawdź, czy system jest zainstalowany (patrz **Sprawdzanie, czy system jest zainstalowany**).
  - Jeśli tak, instalacja zaktualizowanej wersji aplikacji systemowej została zakończona.
  - Domyślna nazwa użytkownika i hasło to **Administrator**. Należy pamiętać, że w hasle rozróżnia się wielkość liter, natomiast w nazwie użytkownika już nie.

#### Rozpoczęcie aktualizacji klienta

1. Kliknij dwukrotnie nową wersję pakietu instalacyjnego oprogramowania.
2. Wybierz język interfejsu.
3. Kliknij dwukrotnie pozycję **Klient**.
4. Kliknij prawym przyciskiem myszy plik **AMS Client Setup.exe** i wybierz opcję **Uruchom jako administrator** z menu kontekstowego.
  - Spowoduje to wyświetlenie okna kreatora przygotowania do instalacji.
  - Wybierz składnik, który chcesz zaktualizować, i kliknij przycisk **Dalej>**.
  - Zależnie od składników, które są już zainstalowane, kreator zaznaczy składniki, które mogą zostać zaktualizowane domyślnie.
  - Możesz wybrać zaktualizowanie lub pominięcie aktualizacji składników:
  - Komponenty, których nie można zaktualizować, zostaną domyślnie oznaczone podpisem **Pomiń**.
5. Przeczytaj **Umowę licencyjną z użytkownikiem końcowym** i kliknij przycisk **Akceptuj**. Jeśli nie akceptujesz umowy, kliknij przycisk **Odrzuć**, a operacja zostanie anulowana.
  - Następne okno pokazuje ścieżkę instalacji, w której będzie przechowywany klient systemu.
  - Domyślnie kreator instalacji zainstaluje klienta systemu na dysku lokalnym w ścieżce *C:\Program Files (86)* (zalecane).
  - Pliki zainstalowane na dysku lokalnym w folderze *C:\Program Files (86)* mogą być modyfikowane tylko przez użytkowników z uprawnieniami administratora.
6. Wprowadź adres serwera. Format adresu: *<hostname>:4999/tcp*
7. Aby kontynuować, kliknij przycisk **Dalej>**.
  - Następne okno pokazuje ścieżkę instalacji, w której będzie przechowywana aplikacja Map View wchodząca w skład systemu.
  - Domyślnie kreator instalacji instaluje systemową aplikację Map View na dysku lokalnym w ścieżce *C:\Program Files (86)* (zalecane).
8. Wprowadź adres wykrywania.
  - Aplikacja Map View połączy się z lokalizacją pod adresem wykrywania, aby wykryć punkty końcowe systemu. Ten adres jest adresem URL zawierającym nazwę serwera i numer portu punktu końcowego wykrywania.
9. Sprawdź podsumowanie informacji przedaktualizacyjnych i kliknij przycisk **Zainstaluj**.
  - Zostanie wyświetlone podsumowanie zawierające wszystkie składniki wybrane do zaktualizowania.
10. Obserwuj pasek postępu instalacji.
  - Poczekaj, aż operacja zostanie zakończona.
11. Po zakończeniu operacji kliknij przycisk **Dalej>** i sprawdź podsumowanie informacji poaktualizacyjnych.
  - Zostanie wyświetlone podsumowanie ze wszystkimi zaktualizowanymi składnikami.
12. Kliknij przycisk **Zakończ**, aby dokończyć instalowanie zaktualizowanej wersji systemu.
13. Uruchom ponownie komputer (zalecane).
  - Komputer uruchomi się ponownie.

14. Sprawdź, czy system jest zainstalowany (patrz **Sprawdzanie, czy system jest zainstalowany**).
  - Jeśli tak, instalacja zaktualizowanej wersji aplikacji systemowej została zakończona.
  - Domyślna nazwa użytkownika i hasło to **Administrator**. Należy pamiętać, że w hasle różni się wielkość liter, natomiast w nazwie użytkownika już nie.

**Patrz**

- *Sprawdzanie, czy system jest zainstalowany, Strona 13*

## 3.9 Odinstalowanie

Aby całkowicie usunąć oprogramowanie systemu, wykonaj następujące czynności:

### Odinstalowywanie serwera

1. W systemie Windows kliknij przycisk **Start**.
2. Poszukaj pozycji **Panel sterowania** i kliknij ją dwukrotnie, a zostanie otwarta.
3. Wybierz kolejno opcje **Programy > Programy i funkcje > Odinstaluj program**.
  - Otworzy się lista zainstalowanych programów.
4. Kliknij prawym przyciskiem myszy pozycję **Access Management System - serwer** i z menu kontekstowego wybierz polecenie **Odinstaluj**.
  - Otworzy się kreator deinstalacji systemu.
5. Zaznacz składniki, które chcesz odinstalować, i kliknij przycisk **Dalej>**. Aby zrezygnować z odinstalowywania, kliknij przycisk **Anuluj**.
  - Możesz wskazać, czy chcesz odinstalować, czy pominąć komponenty. Większość składników jest obowiązkowa i nie można ich pominąć.
6. Zaznacz składniki, które chcesz odinstalować, i kliknij przycisk **Dalej>**. Po wprowadzeniu hasła w polu **Hasło SQL** kliknij przycisk **Testuj serwer**.
  - Dane konfiguracyjne serwera baz danych SQL:
    - Serwer SQL: nazwa hosta, na którym działa program SQL Server, np. Komputer lokalny.
    - Instancja SQL: nazwa wystąpienia serwera SQL.
    - Baza danych AMS: nazwa utworzonej bazy danych.
    - Nazwa użytkownika SQL: utworzona nazwa logowania umożliwiająca dostęp do programu SQL Server.
    - Hasło SQL: hasło użytkownika utworzone dla nazwy logowania do programu SQL Server.
7. Kliknij przycisk **Dalej>**.
8. Obserwuj pasek postępu odinstalowywania.
9. Po zakończeniu operacji kliknij przycisk **Dalej>** i sprawdź podsumowanie informacji podeinstalacyjnych.
  - Zostanie wyświetlone podsumowanie zawierające wszystkie składniki, które zostały odinstalowane lub pominięte.
10. Kliknij przycisk **Zakończ**, aby dokończyć odinstalowywanie serwera.
  - Kreator deinstalacji zostanie zamknięty.
  - System zniknie z listy zainstalowanych programów.
  - Ikona systemu zniknie z pulpitu.

### Odinstalowywanie klienta

1. W systemie Windows kliknij przycisk **Start**.

2. Poszukaj pozycji **Panel sterowania** i kliknij ją dwukrotnie, a zostanie otwarta.
3. Wybierz kolejno opcje **Programy > Programy i funkcje > Odinstaluj program**.
  - Otworzy się lista zainstalowanych programów.
4. Kliknij prawym przyciskiem myszy pozycję **Access Management System - klient** i z menu kontekstowego wybierz polecenie **Odinstaluj**.
  - Otworzy się kreator deinstalacji systemu.
5. Zaznacz składniki, które chcesz odinstalować, i kliknij przycisk **Dalej>**. Aby zrezygnować z odinstalowywania, kliknij przycisk **Anuluj**.
  - Możesz wskazać, czy chcesz odinstalować, czy pominąć komponenty. Większość składników jest obowiązkowa i nie można ich pominąć.
6. Obserwuj pasek postępu odinstalowywania.
7. Po zakończeniu operacji kliknij przycisk **Dalej>** i sprawdź podsumowanie informacji podeinstalacyjnych.
  - Zostanie wyświetlone podsumowanie zawierające wszystkie składniki, które zostały odinstalowane lub pominięte.
8. Kliknij przycisk **Zakończ**, aby dokończyć odinstalowywanie klienta.
  - Kreator instalacji zostanie zamknięty.
  - System zniknie z listy programów.
  - Ikona systemu zniknie z pulpitu.

Aby zakończyć proces odinstalowywania, usuń folder C:

```
\Program Files (x86)\Bosch Sicherheitssysteme\
```

---

## 4 Dane techniczne

---

**Uwaga!**

Na kliencie i serwerze musi być zainstalowana ta sama wersja klienta AMS. Nie próbuj uzyskiwać dostępu do serwera z innej wersji klienta AMS.

---











**Bosch Security Systems B.V.**

Torenallee 49  
5617 BA Eindhoven  
Netherlands

**[www.boschsecurity.com](http://www.boschsecurity.com)**

© Bosch Security Systems B.V., 2020