# Credential Management V5.5

Mit Mobile Access

**de** Bedienungsanleitung

# Inhaltsverzeichnis

# 1 Sicherheit

**Verwendung aktueller Software**

Vor der Inbetriebnahme des Geräts sollten Sie sicherstellen, dass Sie die aktuelle Softwareversion installiert haben. Aktualisieren Sie die Software regelmäßig während der gesamten Betriebsdauer des Geräts, um die durchgängige Funktionalität, Kompatibilität, Leistung und Sicherheit zu gewährleisten. Befolgen Sie die Anweisungen zu Softwareaktualisierungen in der Produktdokumentation.

Unter den folgenden Links finden Sie weitere Informationen:

- Allgemeine Informationen: https://www.boschsecurity.com/xc/en/support/product-security/
- Sicherheitshinweise, d. h. eine Liste identifizierter Schwachstellen und Lösungsvorschläge: https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

Bosch übernimmt keinerlei Haftung für Schäden, die durch Produkte entstehen, die mit veralteten Softwarekomponenten in Betrieb genommen wurden.

# 2 Einführung

## 2.1 Über Credential und Visitor Management

Credential Management, im Folgenden als CredMgmt bezeichnet, ist ein browserbasiertes Softwaretool, das in Verbindung mit einem Bosch-Zutrittskontrollsystem (ACS) arbeitet. Mit einer einfachen und intuitiven Benutzeroberfläche ermöglicht es auch relativ unerfahrenen Bedienern, die Anmeldedaten von Mitarbeitern und externen Personen zu verwalten. Bei den Anmeldedaten kann es sich entweder um physische Ausweise oder mobile Anmeldedaten handeln.

**Credential Management**

Im CredMgmt können ACS-Nutzer sowohl die Anmeldedaten als auch die Datensätze der Mitarbeiter verwalten, zu denen die Anmeldedaten gehören.

| Entität | Hinzufügen | Ändern | Löschen | Zuweisen/ Zuweisung aufheben |
|---|---|---|---|---|
| Physische Anmeldedaten | | | | Ja |
| Virtuelle „Mobile“ Ausweise (falls Mobile Access installiert) | Ja | | Ja | Ja |
| Autorisierungen | | | | Ja |
| Ausweisinhaber Datensätze | Ja | Ja | Ja | |

**Visitor Management**

Im VisMgmt verwalten die ACS-Nutzer Anmeldedaten, Besucherdaten und Besuchsdaten.

| Entität | Hinzufügen | Ändern | Löschen | Zuweisen/ Zuweisung aufheben |
|---|---|---|---|---|
| Physische Anmeldedaten | | | | Ja |
| Virtuelle „Mobile“ Ausweise (falls Mobile Access installiert) | Ja | | | Ja |
| Besucherdatensätze | Ja | Ja | Ja | |
| Besuchsdatensätze | Ja | Ja | Ja | |

## 2.2 Über Mobile Access

Mobile Access ist eine Zutrittskontrolle von Personen mit Hilfe von virtuellen Anmeldedaten, die auf einem mobilen Gerät, z. B. dem Smartphone der Person, gespeichert sind. Die virtuellen Anmeldedaten werden im primären Zutrittskontrollsystem (ACS) verwaltet.

- Die Bediener des ACS generieren diese virtuellen Berechtigungen, weisen sie zu und senden sie über eine entsprechende Webanwendung an Personen.
- Die Inhaber mobiler Anmeldedaten bedienen die Zutrittskontrollleser über Bluetooth von einer Mobile Access-App auf ihren mobilen Geräten aus.

- Installationstechniker von Mobile Access konfigurieren Zutrittskontrollleser über Bluetooth mit einer speziellen Setup-App auf ihren mobilen Geräten.
- Das System speichert keine persönlichen Daten auf mobilen Geräten.

# 3 Installieren und Deinstallieren

## 3.1 Softwarevoraussetzungen

CredMgmt-Server installieren Sie auf demselben Computer wie das ACS (das primäre Zutrittskontrollsystem). Es gelten dieselben Software- und Hardwareanforderungen.
Wenn das primäre Zutrittskontrollsystem noch nicht installiert wurde, müssen Sie es zuerst installieren, bevor Sie Credential Management installieren.
Bei der ersten Installation oder bei Aktualisierungen sollte die Installationsreihenfolge wie folgt sein:

1. Haupt-Zutrittskontrollsystem – Access Management System.
2. Credential Management und/oder Visitor Management.
3. Mobile Access.

Die Installationsprogramme für CredMgmt und Mobile Access verfügen über eigene Installationsmedien, die von ACS getrennt sind. Sie können aus den Online-Produktkatalogen von Bosch heruntergeladen werden.

**Hinweis!**
Notwendigkeit eines stabilen Stammzertifikats
Bevor Sie mit den nachstehenden Installationen fortfahren, vergewissern Sie sich, dass die Installation des ACS vollständig und gemäß der zugehörigen Installationsanleitung lizenziert ist. Dazu gehört eine endgültige Entscheidung über das Stammzertifikat des ACS-Servers (ob selbstsigniert oder CA-basiert) und seine stabile Implementierung. Post-hoc-Änderungen am Stammzertifikat des ACS-Servers würden eine Neukonfiguration der Zertifikate auf allen Computern und mobilen Lesern erfordern, die Teil des Zutrittskontrollsystems sind.

**Serveranforderungen**
Der Server ist der Computer, auf dem das ACS und die CredMgmt-Anwendung laufen.

| | |
|---|---|
| Betriebssysteme | – Windows 11 Professional und Enterprise 23H2;<br>– Windows Server 2019 (Version 1809) (64bit, Standard, Datacenter);<br>– Windows Server 2022(64 Bit, Standard, Datacenter) |
| Datenbankmanagementsysteme | – MS SQL Server 2019 and later<br>Verwenden Sie immer dieselbe Datenbankinstanz wie die des ACS (des primären Zutrittskontrollsystems) |
| Minimale Monitorauflösung | Full HD 1920 x 1080 |
| Unterstützte Browser | Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium-basiert)<br>Verwenden Sie die neueste Version des Browsers für Ihr Windows-Betriebssystem. |

**Client-Anforderungen**

| Anforderung | Description (Beschreibung) |
|---|---|
| Minimale Monitorauflösung | Full HD 1920x1080 |
| Unterstützte Browser | Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium based) Verwenden Sie die neueste Version des Browsers für Ihr Windows-Betriebssystem. |

## 3.2 Hardwarevoraussetzungen

**Registrierungsleser**

CredMgmt benötigt mindestens einen Bekanntmachungsleser, um physische Ausweise zu erfassen. Die Registrierungsleser werden in der Regel auf den Arbeitsplätzen der Kunden installiert. Die Client-Workstation kommuniziert mit der Peripherie-Hardware über ein `BoschPeripheralDeviceAddon.exe`-Programm. Die Installation dieses Programms wird im Folgenden beschrieben.

Die folgenden Bekanntmachungsleser und Ausweisformate werden unterstützt.

| | 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-Registrierung ARD-EDMCV002-USB | X | | | | | | | | |
| OMNIKEY 5427 CK | | X | X | X | X | X | X | X | X |

### 3.2.1 Einrichten des Add-ons für Peripheriegeräte

Das Add-on für Peripheriegeräte ist nur auf den Client-Computern erforderlich, die eine Verbindung mit Registrierungslesern, Scannern oder anderen Peripheriegeräten herstellen. Wiederholen Sie das folgende Verfahren auf jedem Client-Computer, der diese Anforderung erfüllt.

1. Führen Sie auf dem gewünschten Client-Computer als Administrator `BoschPeripheralDeviceAddon.exe` vom Installationsmedium aus.
   - Die Kernkomponenten werden aufgeführt, also die Client-Software und die Software für die üblichen Peripheriegeräte. Es wird empfohlen, alle aufgeführten Komponenten zu installieren, selbst wenn die Hardware derzeit nicht verfügbar ist.
2. Klicken Sie auf **Weiter**, um die Standard-Installationspakete zu akzeptieren.
3. Auf dem Bildschirm **Client-Konfiguration**

- **Installationsverzeichnis:** Übernehmen Sie die Standardeinstellung (empfohlen), oder ändern Sie sie nach Bedarf.
- **COM-Port:**

  - Wenn Sie einen LECTUS Enroll Reader verwenden, geben Sie die Nummer des COM-Ports ein, z. B. `COM3`, an den der Enroll Reader angeschlossen ist. Überprüfen Sie diesen Wert im Windows-Geräte-Manager.
  - Wenn Sie einen HID OMNIKEY Leser verwenden, lassen Sie dieses Feld leer.
  - Die Kamera, das Signopad und der Dokumentenscanner sind „plug-and-play“ und benötigen keinen COM-Port. Klicken Sie auf **Zulassen**, wenn der Browser die Berechtigung zum Herstellen einer Verbindung anfordert.
- **Serveradresse** und **Port:**
  - Geben Sie den Namen aller Server-Computer (standardmäßig mindestens den primären ACS-Server Computer) sowie die Portnummern für alle Backend-Dienste ein, die die Peripheriegeräte steuern müssen.
    Klicken Sie in jedem Fall auf **Verbindung testen**, und warten Sie auf Bestätigung.
    Klicken Sie auf **Hinzufügen**, um weitere Server hinzuzufügen.
    Klicken Sie auf **Löschen**, um Server zu entfernen.
  - Die Standard-Ports für die üblichen Backend-Dienste sind:
    `5806` für CredMgmt
    `5706` für VisMgmt

4. Klicken Sie auf **Weiter**, um eine Zusammenfassung der zu installierenden Komponenten zu erhalten.
5. Klicken Sie auf **Installieren**, um die Installation zu starten.
6. Klicken Sie auf **Fertigstellen**, um die Installation abzuschließen.
7. Starten Sie den Computer nach der Installation neu.

## 3.3 Installation von Credential Management

**Einführung**

CredMgmt läuft als Webanwendung in Verbindung mit einem Bosch Zutrittskontrollsystem (ACS). In den folgenden Abschnitten wird die Installation der Backend-Komponente beschrieben, die diese Webanwendung steuert.

- Sie können es so installieren, dass es entweder eine lokale oder eine Remote-Datenbank verwendet.

Bei Verwendung von AMS , Visitor Management, Credential Management und Mobile Access in einer Unternehmensnetzwerkumgebung wird die Verwendung von Zertifikaten empfohlen, die von einer Unternehmens-CA (Zertifizierungsstelle) ausgestellt werden. Zertifikate sollten vor der Installation all dieser Backend-Systeme ausgestellt werden. Weitere Informationen finden Sie im Abschnitt *Verwenden von benutzerdefinierten Zertifikaten* im AMS Installationshandbuch.

### 3.3.1 CredMgmt-Voraussetzungen

**Dedizierter Benutzer für eine entfernte Datenbank (nur wenn Sie eine Remote-Datenbank verwenden)**

Der Benutzer `CMUser` greift stellvertretend für die CredMgmt-Anwendung auf die ACS-Datenbank zu.

Wenn CredMgmteine Datenbank auf einem Remote-Datenbankserver verwenden soll, gehen Sie wie folgt vor.

WICHTIG: Führen Sie die CredMgmt-Installation nicht aus, bevor Sie diesen Vorgang abgeschlossen haben.

1. Erstellen Sie auf dem Remote-Datenbankserver einen Domänen-Windows-Benutzer in derselben Domäne wie der ACS . Verwenden Sie die folgenden Einstellungen:

– **Benutzername** (beim Benutzernamen wird zwischen Groß- und Kleinschreibung unterschieden): <ACS-Domäne>\CMUser
– **Kennwort**: Legen Sie das Kennwort entsprechend den Sicherheitsrichtlinien fest, die für alle Computer gelten. Notieren Sie es sorgfältig, da es für die CredMgmt-Installation benötigt wird.
– **Benutzer muss Kennwort bei der nächsten Anmeldung ändern**: NO
– **Benutzer kann Kennwort nicht ändern**: YES
– **Kennwort läuft nie ab**: YES
– **Anmeldung als Service**: YES
– **Konto ist deaktiviert**: NO

Fügen Sie dann CMUser als Login für den SQL Server wie folgt hinzu:

1. SQL Management Studio öffnen
2. Mit der Remote-SQL-Instanz verbinden
3. Zu **Sicherheit** > **Login** navigieren
4. Wählen Sie im Fensterbereich **Seite auswählen** die Option **Allgemein**
5. Wählen Sie CMUser als Benutzer
6. Wählen Sie im Fensterbereich **Seite auswählen** die Option **Serverrollen**
7. Aktivieren Sie die Kontrollkästchen public und dbcreator

**Dedizierter Benutzer für die lokale Datenbank (nur wenn Sie eine lokale Datenbank verwenden)**

Der Benutzer CMUser greift stellvertretend für die CredMgmt-Anwendung auf die ACS-Datenbank zu.

Sie müssen diesen Benutzer NICHT anlegen, wenn CredMgmt eine lokale Datenbank verwenden soll, da das CredMgmt Setup-Programm automatisch einen Windows-Benutzer CMUser auf dem ACS-Server anlegt.

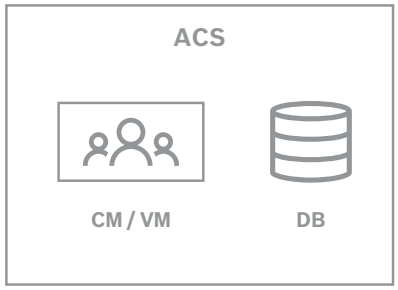
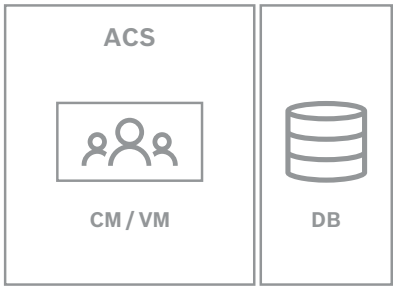
**Ein eigener Benutzer im ACS**

1. Erstellen Sie im ACS einen Benutzer, der die Funktion **unbegrenzte API-Nutzung** hat.

– Dialog Pfad in AMS: **Konfiguration** > **Bediener und Bedienplätze** > **Benutzerrechte** > Registerkarte: **Benutzerkonto** > **API-Zutrittsrechte.**
  Wählen Sie Unlimited access aus der Liste.
– Dialogpfad im BIS: **Konfiguration Browser** > **Administration** > **Bediener** > Bediener auswählen > Registerkarte: **ACE API-Zugriffsrechte.**
  Wählen Sie Unlimited access.
– Ausführlichere Anweisungen finden Sie im Kapitel **Zuweisung von Benutzerprofilen (Bedienerprofilen)** im Bedienerhandbuch des ACS.

2. Notieren Sie sich den Benutzernamen und das Passwort sorgfältig, da der Installationsassistent der Webanwendung sie benötigt.

### 3.3.2 Installationsvorgang

| CredMgmt mit lokaler DB | CredMgmt mit Remote-DB |
|---|---|
|  |  |



**Vorgehensweise**

1. Führen Sie `BoschCredentialManagementServer.exe` auf dem ACS-Server als Administrator aus.

– Das Installationsprogramm wird geöffnet.

2. Wählen Sie auf dem Bildschirm **Kernkomponenten** `Bosch Credential Management` und klicken Sie auf **Weiter**
3. Lesen Sie sorgfältig und klicken Sie auf **Accept** (Akzeptieren), wenn Sie die Endbenutzer-Lizenzvereinbarung (EULA) akzeptieren möchten. Nur wenn Sie dies tun, kann die Installation fortgesetzt werden.
4. Wählen Sie einen Zielordner für die Installation aus, oder übernehmen Sie die Standardeinstellung (empfohlen), und klicken Sie auf **Weiter.**
5. Wählen Sie auf dem Bildschirm **SQL-Server** eine von zwei Alternativen für den Speicherort der Datenbank aus. Die Konfigurationen sind leicht unterschiedlich. Wählen Sie eine Alternative für den nächsten Schritt:

– ALTERNATIVE 1 **Lokale Datenbank**-Option:
  – Das Setup-Programm findet die lokale Datenbank und trifft eine Vorauswahl.
  – Geben Sie das SQL-Passwort für einen Admin-Benutzer ein (die Voreinstellung ist `sa`).
  – Klicken Sie auf **Verbindung testen**
  – Klicken Sie auf **Next** (Weiter).
– ALTERNATIVE 2 **Remote-Datenbank**-Option
  – Geben Sie den Namen des SQL-Servers ein, der sich im Netzwerk befindet.
  – Geben Sie den Namen der SQL-Instanz ein
  – Geben Sie das SQL-Passwort für einen Admin-Benutzer ein (die Voreinstellung ist `sa`).
  – Klicken Sie auf **Verbindung testen**
  – Überprüfen Sie den Benutzernamen und geben Sie das Kennwort des Windows- und SQL-Administrator-Benutzers ein, den Sie für die Remote-Datenbanknutzung erstellt haben (siehe Voraussetzungen oben).
  – Klicken Sie auf **Next** (Weiter).

6. Auf dem Bildschirm für die **ACS-Zutrittskonfiguration**:

– Geben Sie den Hostnamen des ACS-Servers ein.
– Geben Sie den Namen eines ACS-Benutzers mit unbegrenzter API-Nutzung ein (siehe Voraussetzungen oben).
– Geben Sie das ACS-Passwort für diesen ACS-Benutzer ein und bestätigen Sie es.

7. Klicken Sie auf **Next** (Weiter).
8. Auf dem Bildschirm **Identity server configuration** (Identitätsserver-Konfiguration):

– Der Standard-Identitätsserver (voreingestellt) ist der primäre ACS-Server mit Port `44333`: `https://`<NameOfACSserver>`:44333`

– Klicken Sie auf **Test Connection** (Verbindung testen).
– Wenn der Test fehlschlägt, überprüfen Sie die Verfügbarkeit des Identitätsservers erneut.
– Klicken Sie auf **Next** (Weiter).

9. Bestätigen Sie auf dem Bildschirm **Kernkomponenten**, dass CredMgmt ausgewählt ist, und klicken Sie auf **Installieren**
10. Wenn die Installation abgeschlossen ist, starten Sie CredMgmt mit der folgenden URL: `https://` <NameOfACSserver>`:5806`

## 3.4 Installieren von Mobile Access

**Einführung**

Der Mobile Access-Backend-Dienst bietet Mobile Access-Funktionen sowohl für Credential Management als auch für Visitor Management.

Verwenden Sie unbedingt die neueste Version des Zutrittskontrollsystems und des Mobile Access-Backends.

**HINWEIS:** Wenn Sie sowohl CredMgmt als auch VisMgmt verwenden, müssen Sie Mobile Access nur einmal installieren.

– Sie können es auf demselben Server wie das ACS (gemeinsame Installation) oder auf einem separaten Server (verteilte Installation) installieren.
– Sie können es so installieren, dass es entweder eine lokale oder eine Remote-Datenbank verwendet.

**Erreichbarkeit des Mobile Access Backend-Dienstes**

Der Mobile Access-Backend Dienst muss für die mobilen Endgeräte ständig erreichbar sein. Aus Sicherheitsgründen ist es sehr unwahrscheinlich, dass mobile Geräte Netzzugang zu einem ACS-Server haben. Daher wird eine verteilte Installation empfohlen. Dadurch können Sie den Mobile Access-Dienst auf einem weithin verfügbaren „Cloud“-Server ausführen.

### 3.4.1 Überblick über Installation, Konfiguration und Verwendung

Für Mobile Access müssen mehrere Komponenten zusammenarbeiten. Wir führen hier die einzelnen Phasen auf und beschreiben ihre jeweiligen Voraussetzungen und Verfahren in den folgenden Abschnitten dieses Kapitels:

**Einrichten des ACS-Servers**

1. Ein ACS ist installiert, lizenziert und läuft mit einem permanenten Stammzertifikat und kompatiblen Zutrittslesern. Darin werden Bediener mit Berechtigungen zur Verwaltung von Mobile Access definiert.

**Mobile Access einrichten**

1. Ein Systemadministrator installiert eine oder beide der Webanwendungen, die Mobile Access verwenden, entweder Credential Management oder Visitor Management auf dem ACS.
2. Ein Systemadministrator installiert das Mobile Access-Backend.
3. Ein Systemadministrator aktiviert Mobile Access in den Webanwendungen, die installiert sind.

**Einrichten des Lesers.**

1. Ein Systemadministrator (eine Person, die berechtigt ist, Mobile Access-Leser zu konfigurieren) erstellt in der CredMgmt-Anwendung einen Installationstechniker.

2. Der Installationstechniker lädt die Installer-App („Setup Access“) über den üblichen öffentlichen App Store des Geräts auf sein Mobilgerät herunter.
3. Ein Systemadministrator sendet eine Einladung an den vorgesehenen Installationstechniker.
4. Der Installationstechniker nimmt die Einladung in der Installer-App an. Mit dieser Einladung wird der Installationstechniker ermächtigt, Zutrittsleser für Mobile Access zu konfigurieren.
5. Das Installationsprogramm konfiguriert die Leser mit Hilfe der Installer-App.

**Mobile Access verwenden**

1. Berechtigungsinhaber, die zur Nutzung von Mobile Access berechtigt sind, laden die Berechtigungsinhaber-App („Mobile Access”) aus dem üblichen öffentlichen App-Store des Geräts auf ihr mobiles Gerät herunter.
2. CredMgmt und/oder VisMgmt Bediener senden mobile Berechtigungen per QR-Code oder E-Mail an die berechtigten Berechtigungsinhaber.
3. Die Berechtigungsinhaber lesen den QR-Code oder die E-Mail in ihrer Berechtigungsinhaber-App („Mobile Access”). Dadurch kann ihr mobiles Gerät als physischer Ausweis fungieren, wenn die App ausgeführt wird.

### 3.4.2 Hardware-Voraussetzungen für Mobile Access

Mobile Access erfordert Zutrittsleser mit einem BLE-Modul. Die folgenden Bosch-Leser sind geeignet:

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

- B und W stehen für die Farbe, schwarz oder weiß
- O bedeutet OSDP
- K steht für das Vorhandensein eines Tastenfeldes
- M steht für die Eignung für Mobile Access

### 3.4.3 Voraussetzungen für die Konfiguration von Mobile Access

**Dedizierter Benutzer für eine Remote-Datenbank (wenn Sie eine entfernte Datenbank verwenden)**

Wenn Mobile Access eine Datenbank auf einem Remote-Datenbankserver verwenden soll, erstellen und konfigurieren Sie einen Administratorbenutzer mit dem Namen `MAUser` auf diesem Remote-Server, sowohl in Windows als auch auf dem SQL-Server. Wählen Sie bei der unten beschriebenen Einrichtung die Option für den Remote-Datenbankserver und geben Sie das Passwort ein, das Sie für `MAUser` festgelegt haben.

WICHTIG: Führen Sie die Mobile Access-Installation nicht aus, bevor Sie diesen Vorgang abgeschlossen haben.

**Vorgehensweise**

1. Erstellen Sie auf dem Remote-Datenbankserver einen Domänen-Windows-Benutzer in derselben Domäne wie der ACS . Verwenden Sie die folgenden Einstellungen:

- **Benutzername** (beim Benutzernamen wird zwischen Groß- und Kleinschreibung unterschieden): <ACS-Domäne>\`MAUser`
- **Kennwort**: Legen Sie das Kennwort entsprechend den Sicherheitsrichtlinien fest, die für alle Computer gelten. Notieren Sie sie sorgfältig, da sie für die Mobile Access-Installation benötigt wird.
- **Benutzer muss Kennwort bei der nächsten Anmeldung ändern**: `NO`
- **Benutzer kann Kennwort nicht ändern**: `YES`

- **Kennwort läuft nie ab**: YES
- **Anmeldung als Service**: YES
- **Konto ist deaktiviert**: NO

Fügen Sie dann MAUser als Login für den SQL Server wie folgt hinzu:

1. SQL Management Studio öffnen
2. Mit der Remote-SQL-Instanz verbinden
3. Zu **Sicherheit** > **Login** navigieren
4. Wählen Sie im Fensterbereich **Seite auswählen** die Option **Allgemein**
5. Wählen Sie MAUser als Benutzer
6. Wählen Sie im Fensterbereich **Seite auswählen** die Option **Serverrollen**
7. Aktivieren Sie die Kontrollkästchen public und dbcreator

**Ein dedizierter Benutzer für die lokale Datenbank (nur wenn Sie eine lokale Datenbank verwenden)**

Der Benutzer MAUser greift stellvertretend für die Mobile Access-Anwendung auf die ACS-Datenbank zu.

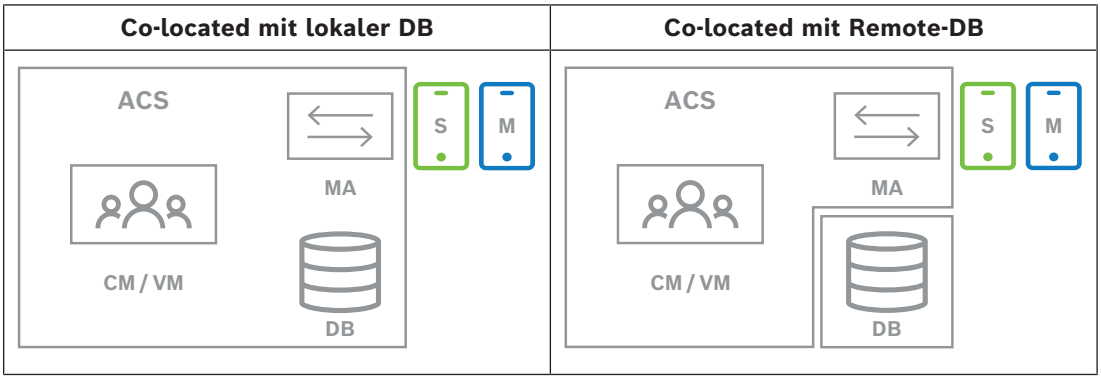
Sie müssen diesen Benutzer NICHT anlegen, wenn Sie eine lokale Datenbank verwenden. Das Mobile Access-Setup-Programm erstellt automatisch einen Windows-Benutzer MAUser auf dem ACS-Server.

### 3.4.4 Verfahren für die Installation an einem Ort

**Co-located Installation** bedeutet, dass der Mobile Access-Backend-Dienst auf demselben Server läuft wie der ACS.

**Verteilte Installation** bedeutet, dass der Mobile Access-Backend-Dienst auf einem anderen Server läuft, zum Beispiel auf einem „Cloud-Server".

Für die Option der verteilten Installation lesen Sie bitte den nächsten Abschnitt **Vorgehensweise bei der verteilten Installation**.




| Schlüssel | Bedeutung |
|---|---|
| ACS | Das primäre Zutrittskontrollsystem, AMS oder BIS-ACE |
| CM/VM | Backend für die Webanwendung: Credential Management oder Visitor Management |
| DB | ACS-Hauptdatenbank |
| MA | Mobile Access-Backend |

| Schlüssel | Bedeutung |
|---|---|
| S | „Setup Access” Installer-App für mobile Geräte von Systeminstallationstechnikern und -konfiguratoren |
| M | „Mobile Access“-Zutritts-App für mobile Geräte von Inhabern normaler Anmeldedaten. |

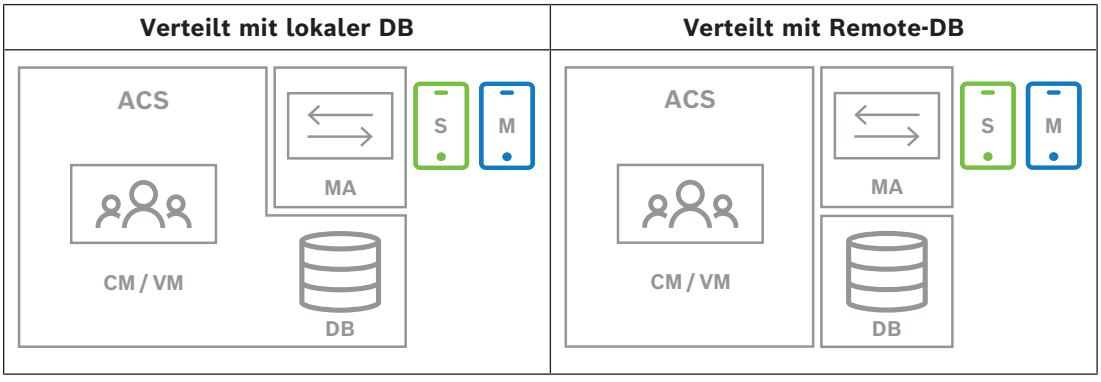
**Vorgehensweise**

1. Führen Sie auf dem ACS-Server, der bei standortgleichen Installationen auch der Mobile Access-Server ist, `BoschMobileAccessBackend.exe` als Administrator aus
– Das Setup-Programm öffnet sich
2. Wählen Sie auf dem Bildschirm **Standort** die Art der Einrichtung aus: **Co-located**
3. Überprüfen Sie auf dem Bildschirm **Komponenten**, ob die Option `Bosch Mobile Access` ausgewählt ist, und klicken Sie auf **Weiter**
4. Lesen Sie den Bildschirm **EULA** sorgfältig durch und klicken Sie auf **Akzeptieren**, wenn Sie die Endbenutzer-Lizenzvereinbarung (EULA) akzeptieren möchten. Nur wenn Sie dies tun, kann die Installation fortgesetzt werden.
5. Auf dem Bildschirm **Installationsverzeichnis**:
– Wählen Sie einen Zielordner für die Installation aus, oder akzeptieren Sie die Standardeinstellung (empfohlen).
– Geben Sie Ihren Firmennamen ein, wie er in der mobilen App und in HTML-E-Mail-Vorlagen angezeigt werden soll
– Klicken Sie auf **Next** (Weiter).
6. Auf dem Bildschirm **Zertifikat**
– Geben Sie den Hostnamen ein, auf dem das Mobile Access-Backend laufen soll.
– Falls gewünscht, oder falls das Netzwerk keine Hostnamenauflösung bietet, geben Sie die IP-Adresse des Hosts ein
– Klicken Sie auf **Next** (Weiter).
7. Wählen Sie auf dem Bildschirm **SQL-Server** eine von zwei Alternativen für den Speicherort der Datenbank aus. Die Konfigurationen sind leicht unterschiedlich. Wählen Sie eine Alternative für den nächsten Schritt:
– ALTERNATIVE 1 **Lokale Datenbank**-Option:
  – Das Setup-Programm findet die lokale Datenbank und trifft eine Vorauswahl.
  – Geben Sie das SQL-Passwort für einen Admin-Benutzer ein (die Voreinstellung ist `sa`).
  – Klicken Sie auf **Verbindung testen**
  – Klicken Sie auf **Next** (Weiter).
– ALTERNATIVE 2 **Remote-Datenbank**-Option
  – Geben Sie den Namen des SQL-Servers ein, der sich im Netzwerk befindet.
  – Geben Sie den Namen der SQL-Instanz ein
  – Geben Sie das SQL-Passwort für einen Admin-Benutzer ein (die Voreinstellung ist `sa`).
  – Klicken Sie auf **Verbindung testen**
  – Überprüfen Sie den Benutzernamen und geben Sie das Kennwort des Windows- und SQL-Administrator-Benutzers ein, den Sie für die Remote-Datenbanknutzung erstellt haben (siehe Voraussetzungen oben).
  – Klicken Sie auf **Next** (Weiter).
8. Auf dem Bildschirm **Identity server configuration** (Identitätsserver-Konfiguration):

– Der Standard-Identitätsserver (voreingestellt) ist der primäre ACS-Server mit Port `44333`: `https://<NameOfACSserver>:44333`
– Klicken Sie auf **Test Connection** (Verbindung testen).
– Wenn der Test fehlschlägt, überprüfen Sie die Verfügbarkeit des Identitätsservers erneut.
– Klicken Sie auf **Next** (Weiter).
9. Bestätigen Sie auf dem Bildschirm **Kernkomponenten**, dass **BoschMobile Access** ausgewählt ist und klicken Sie auf **Installieren**
– Der Installationsassistent wird abgeschlossen
10. Klicken Sie auf **Next** (Weiter).
11. Überprüfen Sie auf dem Bildschirm **Kernkomponenten**, ob die Installation erfolgreich abgeschlossen wurde, und klicken Sie auf **Fertigstellen**
12. Überprüfen Sie in der Windows-Anwendung `Services`, ob der Dienst `Bosch Mobile Access` ausgeführt wird.

### 3.4.5 Verfahren für die verteilte Installation

**Co-located Installation** bedeutet, dass der Mobile Access-Backend-Dienst auf demselben Server läuft wie der ACS.
**Verteilte Installation** bedeutet, dass der Mobile Access-Backend-Dienst auf einem anderen Server läuft, zum Beispiel auf einem „Cloud-Server".
Für die Option der gleichzeitigen Installation lesen Sie bitte den vorherigen Abschnitt **Vorgehensweise bei der gleichzeitigen Installation**.
Auf einem verteilten Mobile Access-Backend-Server muss vor dem Start einer Mobile Access-Installation oder bei der Aktualisierung des Systems die folgende Voraussetzung erfüllt sein. Dies ist in einer „co-located" Umgebung nicht erforderlich:
– Installieren Sie das **ASP.NET Core 8.0 Runtime (v8.0.2) Hosting-Bundle** auf dem verteilten Mobile Access-Backend-Server, bevor Sie das Installationsprogramm für Mobile Access ausführen.
– Laden das erforderliche Hosting-Bundle unter dem folgenden Link herunter: https://dotnet.microsoft.com/en-us/download/dotnet/thank-you/runtime-aspnetcore-8.0.2-windows-hosting-bundle-installer.




| Schlüssel | Bedeutung |
|---|---|
| ACS | Das primäre Zutrittskontrollsystem, AMS oder BIS-ACE |
| CM/VM | Backend für die Webanwendung: Credential Management oder Visitor Management |

| Schlüssel | Bedeutung |
|---|---|
| DB | ACS-Hauptdatenbank |
| MA | Mobile Access-Backend |
| S | „Setup Access” Installer-App für mobile Geräte von Systeminstallationstechnikern und -konfiguratoren |
| M | „Mobile Access“-Zutritts-App für mobile Geräte von Inhabern normaler Anmeldedaten. |

**Vorgehensweise**

Stellen Sie sicher, dass die aktuelle Version des Haupt-Zutrittskontrollsystems installiert ist.

1. Führen Sie auf dem Mobile Access-Backend Server `BoschMobileAccessBackend.exe` als Administrator aus
– Das Setup-Programm öffnet sich
2. Wählen Sie auf dem Bildschirm **Standort** die Art der Einrichtung aus: **Verteilt**
3. Wählen Sie auf dem Bildschirm **Host** die Option **Mobile Access**-**Backend** und klicken Sie auf **Weiter**
– Hinweis: Die **ACS**-Option wird später in diesem Verfahren verwendet, wenn wir Mobile Access auf dem ACS-Server installieren.
4. Vergewissern Sie sich auf dem Bildschirm **Komponenten**, dass **BoschMobile Access** ausgewählt ist, und klicken Sie auf **Weiter.**
5. Lesen Sie den Bildschirm **EULA** sorgfältig durch und klicken Sie auf **Akzeptieren**, wenn Sie die Endbenutzer-Lizenzvereinbarung (EULA) akzeptieren möchten. Nur wenn Sie dies tun, kann die Installation fortgesetzt werden.
6. Auf dem Bildschirm **Installationsverzeichnis**:
– Wählen Sie einen Zielordner für die Installation aus, oder akzeptieren Sie die Standardeinstellung (empfohlen).
– Geben Sie Ihren Firmennamen ein, wie er in der mobilen App und in HTML-E-Mail-Vorlagen angezeigt werden soll
– Klicken Sie auf **Next** (Weiter).
7. Wählen Sie auf dem Bildschirm **SQL-Server** eine von zwei Alternativen für den Speicherort der Datenbank aus. Die Konfigurationen sind leicht unterschiedlich. Wählen Sie eine Alternative für den nächsten Schritt:
– ALTERNATIVE 1 **Lokale Datenbank**-Option:
  – Das Setup-Programm findet die lokale Datenbank und trifft eine Vorauswahl.
  – Geben Sie das SQL-Passwort für einen Admin-Benutzer ein (die Voreinstellung ist `sa`).
  – Klicken Sie auf **Verbindung testen**
  – Klicken Sie auf **Next** (Weiter).
– ALTERNATIVE 2 **Remote-Datenbank**-Option
  – Geben Sie den Namen des SQL-Servers ein, der sich im Netzwerk befindet.
  – Geben Sie den Namen der SQL-Instanz ein
  – Geben Sie das SQL-Passwort für einen Admin-Benutzer ein (die Voreinstellung ist `sa`).
  – Klicken Sie auf **Verbindung testen**
  – Überprüfen Sie den Benutzernamen und geben Sie das Kennwort des Windows- und SQL-Administrator-Benutzers ein, den Sie für die Remote-Datenbanknutzung erstellt haben (siehe Voraussetzungen oben).

– Klicken Sie auf **Next** (Weiter).

*An diesem Punkt der verteilten Installation müssen Sie zu dem Computer wechseln, auf dem der ACS-Server läuft, und dort* Mobile Access *konfigurieren, damit er später mit dem Backend für* Mobile Access *auf dem lokalen Computer kommunizieren kann.*
*Nachdem Sie die dort angegebenen Schritte durchgeführt haben, führt Sie das Setup-Programm zurück zum lokalen Server, um zu bestätigen und fortzufahren.*

1. Führen Sie auf dem ACS-Server-Computer `BoschMobileAccessBackend.exe` als Administrator aus
– Das Setup-Programm öffnet sich
2. Wählen Sie auf dem Bildschirm **Standort** die Art der Einrichtung aus: **Verteilt**
3. Wählen Sie auf dem Bildschirm **Host** die Option **ACS** und klicken Sie auf **Weiter**
4. Lesen Sie auf dem Bildschirm des **Companion-Assistenten** den erläuternden Text und klicken Sie auf **Weiter**
5. Auf dem Bildschirm **Zertifikat**
– Geben Sie den Hostnamen ein, auf dem das Mobile Access-Backend laufen soll.
– Falls gewünscht, oder falls das Netzwerk keine Hostnamenauflösung bietet, geben Sie die IP-Adresse des Hosts ein
– Klicken Sie auf **Next** (Weiter).
6. Auf dem Bildschirm **Identity server configuration** (Identitätsserver-Konfiguration):
– Der Standard-Identitätsserver (voreingestellt) ist der primäre ACS-Server mit Port `44333`: `https://`<NameOfACSserver>`:44333`
– Klicken Sie auf **Test Connection** (Verbindung testen).
– Wenn der Test fehlschlägt, überprüfen Sie die Verfügbarkeit des Identitätsservers erneut.
– Klicken Sie auf **Next** (Weiter).
7. Auf dem Bildschirm **Datei erstellen**
Hier erstellen wir eine Konfigurationsdatei in einer passwortgeschützten ZIP-Datei und stellen sie dem Mobile Access-Backend zur Verfügung.
– **Benutzerpasswort**: Geben Sie ein Passwort für die ZIP-Datei ein
– **Konfigurationsdatei**: Geben Sie einen Ordner ein, in dem die ZIP-Datei gespeichert werden soll, oder suchen Sie ihn. Beachten Sie, dass dieser Ordner für den Computer zugänglich sein muss, auf dem das Mobile Access-Backend ausgeführt wird. Ist dies nicht der Fall, müssen Sie die ZIP-Datei auf andere Weise auf diesen Computer übertragen.
– Klicken Sie auf **Konfigurationsdatei erstellen**
– Klicken Sie auf **Next** (Weiter).
8. Auf dem Bildschirm **Rechner wechseln**
Die Installationsschritte auf dem ACS-Server sind nun abgeschlossen.
– Klicken Sie auf **Bestätigen**, um die Prozedur zu beenden

*An diesem Punkt der verteilten Installation kehren Sie zum Setup-Programm auf dem* Mobile Access*-Backend Computer zurück.*

1. Kehren Sie zum Setup-Programm `BoschMobileAccessBackend.exe` auf dem Bosch Mobile Access-Server Computer zurück.
2. Auf der Seite **Rechner wechseln**

– Aktivieren Sie das Kontrollkästchen **Ich habe die erforderlichen Schritte auf dem ACS-Rechner bereits abgeschlossen**
– Klicken Sie auf **Next** (Weiter).

3. Auf dem Bildschirm **Datei hochladen**
– **Konfigurationsdatei hochladen:** Wählen Sie die Konfigurationsdatei, die Sie auf dem ACS-Server erstellt haben
– **Passwort-Überprüfung:** Geben Sie das Passwort ein, das Sie für die ZIP-Datei auf dem ACS-Server festgelegt haben.
– Wenn Sie das richtige Passwort eingegeben haben, können Sie auf **Weiter** klicken, um die Konfigurationsdatei zu lesen
4. Bestätigen Sie auf dem Bildschirm **Kernkomponenten**, dass **BoschMobile Access** ausgewählt ist und klicken Sie auf **Installieren**
– Der Installationsassistent wird abgeschlossen
5. Klicken Sie auf **Next** (Weiter).
6. Überprüfen Sie auf dem Bildschirm **Kernkomponenten**, ob die Installation erfolgreich abgeschlossen wurde, und klicken Sie auf **Fertigstellen**
7. Überprüfen Sie in der Windows-Anwendung `Services`, ob der Dienst `Bosch Mobile Access` ausgeführt wird.

## 3.5 Zertifikate für sichere Kommunikation

Für eine sichere Kommunikation zwischen dem Browser auf dem Client-Rechner und dem ACS-Server kopieren Sie das folgende Zertifikat vom ACS-Server auf die Client-Computer. Verwenden Sie ein Konto mit Windows-Administratorrechten, um es zu installieren.
Der übliche Pfad zum Zertifikat lautet:

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

**Hinweis:** Starten Sie nach dem Zertifikatsrollout entweder das Mobile Access-Backend oder den Bosch Credential Management Service und den Bosch Visitor Management Service neu.

**Übersicht der Zertifikatsübertragungen**

| **Auf →**<br>**Von ↓** | **ACS** | **MA**<br>Mobile Access-Backend | **DB**<br>Daten-bank | **S**<br>Setup-App | **M**<br>App für den Zutritt von Ausweisinhabern | **R**<br>Leser |
|---|---|---|---|---|---|---|
| **ACS** | / | Übertragen durch den Einrichtungsassistenten (mit Hilfe des Cert-Tools) | / | / | / | / |

| | | | | | | |
|---|---|---|---|---|---|---|
| **MA**<br>Mobile Access-Backend | Übertragen durch den MA-Einrichtungsassistenten | / | / | Übertragen per QR-Code Registrierung<br><br>Aktualisierung per Push-Benachrichtigung | Übertragen per QR-Code Registrierung<br><br>Aktualisierung per Push-Benachrichtigung | / |
| **DB**<br>Datenbank | / | / | / | / | / | / |
| **S**<br>Setup -App | / | Übertragen durch QR-Code Registrierung | / | / | / | / |
| **M**<br>App für den Zutritt von Ausweisinhabern | / | Übertragen durch QR-Code Registrierung | / | / | / | / |

### 3.5.1 Zertifikate für den Firefox-Browser

Sie können diesen Abschnitt ignorieren, wenn Sie nicht den Firefox-Browser verwenden.

Der Firefox-Browser geht mit Stammzertifikaten anders um: Firefox konsultiert nicht den Windows-Zertifikatspeicher für vertrauenswürdige Stammzertifikate. Stattdessen verwaltet jedes Browserprofil seinen eigenen Stammzertifikatspeicher. Weitere Einzelheiten finden Sie unter https://support.mozilla.org/en-US/kb/setting-certificate-authorities-firefox
Auf dieser Webseite finden Sie auch Anweisungen, wie Sie Firefox zwingen können, den Windows-Zertifikatspeicher für alle Benutzer zu verwenden.
Alternativ können Sie auch die Standardzertifikate wie unten beschrieben importieren.
Hinweis:

- Sie müssen die Zertifikate für jeden Benutzer und jedes Firefox-Profil importieren.
- Das unten beschriebene Serverzertifikat ist das Standardzertifikat, das bei der Installation erstellt wird. Wenn Sie Ihr eigenes Zertifikat bei einer Zertifizierungsstelle erworben haben, können Sie dieses stattdessen verwenden.

**Importieren von Zertifikaten in den Firefox-Zertifikatspeicher**

Um von Firefox auf dem Client-Computer auf den ACS-Server zuzugreifen, können Sie das folgende Standardzertifikat vom Server importieren:

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

Für BIS ACE können Sie das Zertifikat auch über das Internet herunterladen:

- `HTTP://`<Hostname>`/`<Hostname>`.cer`

**Peripheriegeräte:** Für den Zutritt auf ein angeschlossenes Peripheriegerät, z. B. einen Dokumenten- oder Unterschriftenscanner, von Firefox auf dem Client-Computer aus, können Sie das Standardzertifikat verwenden. Sie finden es auf dem Client-Computer an folgender Stelle:
<Installationslaufwerk>:\Program Files (x86)\Bosch Sicherheitssysteme\Bosch Peripheral Device Addon\BoschAcePeripheralDeviceAddonHardware CA.cer

**Verfahren (für jedes Zertifikat und Firefox-Profil wiederholen):**
Gehen Sie auf dem Client-Computer wie folgt vor, um die benötigten Zertifikate zu installieren:

1. Suchen Sie das Zertifikat, das Sie installieren möchten.
2. Öffnen Sie den Firefox-Browser und geben Sie `about:preferences` in die Adressleiste ein.
– Eine Optionsseite wird geöffnet.
3. Geben Sie in das Feld **Suchen in Optionen** `certificate` ein
– Auf der Seite wird die Schaltfläche **Zertifikate anzeigen** angezeigt.
4. Klicken Sie auf die Schaltfläche **Zertifikate anzeigen**.
– Das Dialogfeld **Zertifikatsmanager** wird mit mehreren Registerkarten geöffnet
5. Wählen Sie die Registerkarte **Behörden**.
6. Klicken Sie auf **Importieren** ...
– Es öffnet sich ein Dialogfeld zur Auswahl des Zertifikats.
7. Wählen Sie das in Schritt 1 gefundene Zertifikat aus, und klicken Sie auf **Öffnen**.
– Das Dialogfeld **Zertifikat herunterladen** wird geöffnet.
8. Wählen Sie die Option **Dieser CA zur Identifizierung von Websites vertrauen** und klicken Sie auf **OK**.
– Das Dialogfeld **Zertifikat herunterladen** wird geschlossen.
9. Klicken Sie im Dialogfeld **Zertifikatsmanager** auf **OK**.
– Der Vorgang des Zertifikatsimports ist abgeschlossen.

### 3.5.2 Zertifikate für den Chrome-Browser

Sie können diesen Abschnitt ignorieren, wenn Sie nicht den Chrome-Browser verwenden.
In den Release Notes des ACS finden Sie Informationen zur Änderung der Handhabung von Zertifikaten im Chrome Browser.
So installieren Sie ein Zertifikat im Chrome-Browser unter Microsoft Windows:

1. Laden Sie die Zertifikatsdatei herunter.
2. Gehen Sie zur Einstellungsseite von Chrome (`chrome://settings`) und klicken Sie auf **Erweitert**.
3. Klicken Sie unter **Privatsphäre und Sicherheit** auf **Zertifikate verwalten**
4. Klicken Sie auf der Registerkarte **Ihre Zertifikate** auf **Importieren**, um den Zertifikat Installationsvorgang zu starten:
– Ein Zertifikatimport-Assistent wird angezeigt.
5. Wählen Sie die Zertifikatsdatei aus, und schließen Sie den Assistenten ab.
6. Das installierte Zertifikat wird auf der Registerkarte **Vertrauenswürdige Stammzertifizierungsstellen** angezeigt.

### 3.5.3 Installieren der Mobile Access-Apps

**Einführung**

Bosch bietet die folgenden Apps für Mobile Access

- Bosch Mobile Access: Eine Ausweisinhaber-App zum Speichern virtueller Anmeldedaten und zur Übertragung über Bluetooth an die Leser, die für Mobile Access konfiguriert sind. Ein solcher Leser gewährt oder verweigert dann den Zutritt, je nachdem, ob eine der gespeicherten Anmeldedaten der App für ihn gültig ist.
- Bosch Setup Access: Eine Installations-App zum Scannen und Konfigurieren der Leser über Bluetooth.

Autorisierte Bediener von Visitor Management und Credential Management können virtuelle Berechtigungen sowohl für Ausweisinhaber- als auch für Installer-Apps senden.

Solange die Ausweisinhaber-App läuft und Bluetooth auf dem mobilen Gerät aktiviert ist, können Sie sie wie einen physischen Ausweis verwenden. Es ist nicht erforderlich, Befehle über die App zu erteilen oder gar den Bildschirm zu entsperren.

**Hinweis!**
WICHTIG: Betreiben Sie die Ausweisinhaber- und die Installer-App nicht gleichzeitig. Stellen Sie sicher, dass niemand die Installer-App verwendet, wenn die Ausweisinhaber-App in Gebrauch ist, und umgekehrt.

**Vorgehensweise**

Die Apps für Bosch Mobile Access können in den App-Stores von Google und Apple heruntergeladen und wie gewohnt installiert werden. Ihre Namen in den App Stores sind:

- Bosch Mobile Access
- Bosch Setup Access

## 3.6 Reparieren von Installationen von Mobile Access

**Einführung**

Um die Binärdateien zu aktualisieren oder das Mobile Access-Zertifikat neu zu erstellen, können Sie das Installationsprogramm der aktuellen oder neueren Version von Mobile Access über eine vorhandene Installation ausführen:

**Vorgehensweise**

1. Führen Sie auf dem Mobile Access-Backend Server die neue Version von `BoschMobileAccessBackend.exe` als Administrator aus.
- Beachten Sie, dass der Mobile Access-Backend Server bei „co-located” Installationen mit dem ACS-Server identisch ist.
2. Folgen Sie dem Einrichtungsassistenten und nehmen Sie die gleichen Einstellungen wie bei der ursprünglichen Installation vor.
- Um das Zertifikat erneut zu erstellen, wählen Sie auf dem Bildschirm **Zertifikate** das Optionsfeld **Zertifikat erneut erstellen** aus.
3. Starten Sie den Server nach dem Abschluss des Setup-Programms neu.
4. Starten Sie eine neue Anmeldesitzung auf jeder Webanwendung, die Mobile Access (CredMgmt, VisMgmt oder beides) verwendet.
- Die Webanwendung wird die neuen Binärdateien verwenden.

– Wenn Sie **Zertifikat erneut erstellen** ausgewählt haben, basieren alle weiteren Einladungen, die Sie an Mobile Access-Benutzer und -Installationsprogramme senden, auf dem neuen Mobile Access-Zertifikat.

## 3.7 Deinstallieren der Software

So deinstallieren Sie die Software vom Server oder Client:

1. Starten Sie das Windows-Programm **Programm hinzufügen oder entfernen** mit Windows-Administratorrechten.
2. Wählen Sie das Programm (Server oder Client) und klicken Sie auf **Deinstallieren**.
3. (Nur für die Besucherverwaltung und auf dem Server) Wählen Sie aus, ob Sie sowohl die Visitor Management-Datenbank als auch das Programm entfernen möchten.

– **Hinweis**: Die Datenbank enthält die Datensätze aller Besuche, die während der Verwendung des Programms registriert wurden. Möglicherweise sollten Sie die Datenbank archivieren oder zu einer anderen Installation übertragen.

4. Wählen Sie aus, ob die Protokolldateien entfernt werden sollen.
5. Schließen Sie die Deinstallation auf die übliche Weise ab.
6. (Empfohlen) Starten Sie den Computer neu, um sicherzustellen, dass die Änderungen in der Windows-Registrierung durchgeführt wurden.

**Hinweis:** Nach der Deinstallation des Mobile Access-Backends können die folgenden Konfigurationen auf Wunsch manuell entfernt werden:

– **MAUser**: Dieser Benutzer bleibt nach der Deinstallation erhalten. Ein Administrator muss ihn manuell entfernen.
– **Zertifikate**: Verwenden Sie *Manage computer certificates* (Computerzertifikate verwalten), um alle Zertifikate manuell zu entfernen, die aufgrund der Mobile Access-Installation installiert wurden.
– **ID-Server-Konfiguration für Mobile Access**: Die Datei *appsettings.Extension.MobileAccessBackend* bleibt nach der Deinstallation des Backends erhalten. Löschen Sie sie manuell.

# 4 Überblick über das Credential Management

Im Folgenden werden mögliche Topologien von Credential Management-Installationen sowohl mit als auch ohne Mobile Access dargestellt. Jedes umschließende Kästchen steht für einen separaten Computer.

| Schlüssel | Bedeutung |
|---|---|
| ACS | Das primäre Zutrittskontrollsystem, AMS oder BIS-ACE |
| CM/VM | Backend für die Webanwendung: Credential Management oder Visitor Management |
| DB | ACS-Hauptdatenbank |
| MA | Mobile Access-Backend |
| S | „Setup Access" Installer-App für mobile Geräte von Systeminstallationstechnikern und -konfiguratoren |
| M | „Mobile Access"-Zutritts-App für mobile Geräte von Inhabern normaler Anmeldedaten. |

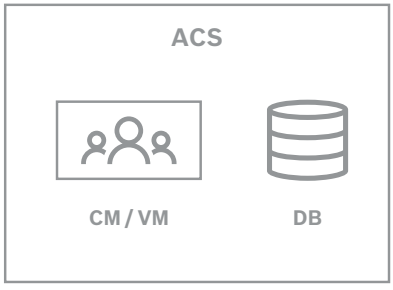
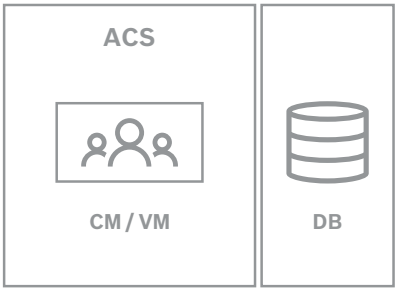
| Credential Management, lokale DB | Credential Management, remote DB |
|---|---|
|  |  |



**Tabelle 4.1:** Topologien von Credential Management

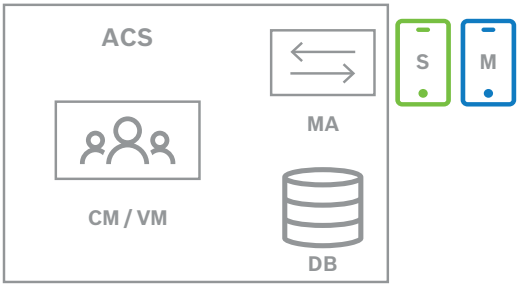
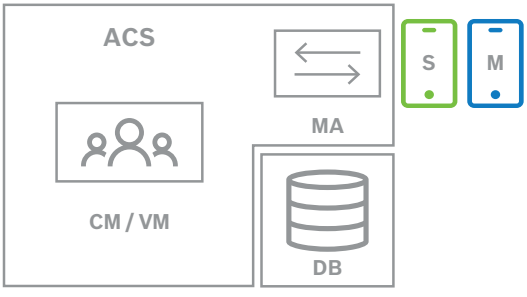
| Mobile Access Co-located, lokale DB | Mobile Access, Co-located, Remote-DB |
|---|---|
|  |  |



**Tabelle 4.2:** Zusammen gelegene Mobile Access-Topologien

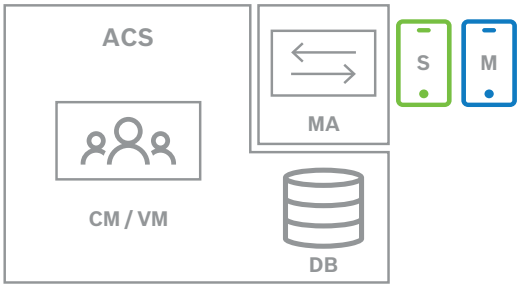
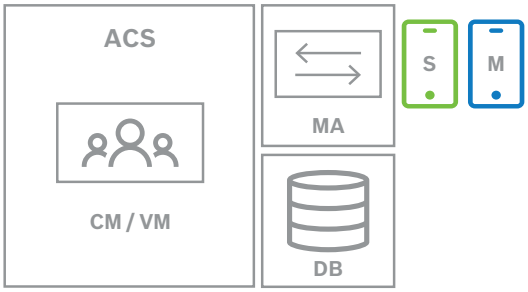
| Mobile Access, verteilt, lokale DB | Mobile Access, verteilt, Remote-DB |
|---|---|
|  |  |



**Tabelle 4.3:** Mobile Access – verteilte Topologien

**Kompatible Versionen der zugehörigen Software**

In der folgenden Tabelle sind die Versionen der Hilfsprogramme aufgeführt, die mit dieser Version des Systems kompatibel sind.

| Komponente | Version | Location (Standort) |
|---|---|---|
| Access Management System (AMS) | 5.5 (mit Mobile Access-Erweiterung) | Download Store/ Produktkatalog |
| Visitor Management (VisMgmt) | 5.5 (mit Mobile Access-Erweiterung) | Download Store/ Produktkatalog |

**Hinweis!**

Divisions

Credential Management, Visitor Management und Mobile Access unterstützen nicht die „Divisions"-Funktion von Bosch Zutrittskontrollsystemen, bei der einer (ACS) die Zutrittskontrolle mehrerer unabhängiger Mandanten verwaltet.

# 5 Konfiguration

## 5.1 Erstellen von Credential Management-Benutzern im ACS

In ACS (ACE oder AMS) muss jeder Benutzer von Credential Management ein Ausweisinhaber mit einer eigenen Bediener-Definition sein.

Diese Bediener-Definitionen umfassen spezielle CredMgmt-Rechte in Form von **Benutzerprofilen**.
Sie müssen für jeden Ausweisinhaber, der im CredMgmt arbeitet, einen separaten Bediener definieren. Einem Bediener können nicht mehrere Ausweisinhaber zugewiesen werden.
Detaillierte Informationen und Anleitungen zu den **Benutzerprofilen** finden Sie in der Online-Hilfe in Ihrem ACS.
Credential Management-Benutzer müssen im AMS erstellt werden:

**Dialogpfad**
**Configuration** > **Operators and workstations** > **User profiles** (Konfiguration > Bediener und Bedienstationen > Benutzerprofile)

**Vorgehensweise**

1. Wenn Sie ein neues Profil erstellen möchten, klicken Sie auf 
2. Geben Sie einen Profilnamen im Feld **Profile Name** (Profilname) (obligatorisch) ein
3. Geben Sie eine Profilbeschreibung in das Feld **Description** (Beschreibung) ein (optional, aber empfohlen).
4. Klicken Sie auf  oder **Apply** (Anwenden), um Ihre Änderungen zu speichern
5. Wählen Sie die Funktion je nach Profiltyp aus:
   - Wählen Sie im Listenbereich die Funktionen (erste Spalte) und die Funktionen innerhalb dieser Funktion (**Execute** [Ausführen], **Change** [Ändern], **Add** [Hinzufügen], **Delete** [Löschen]), die für dieses Profil zugänglich sein sollen. Doppelklicken Sie auf diese, um ihre Einstellungen in `Yes` zu ändern.
   - Stellen Sie ebenfalls sicher, dass alle Funktionen, auf die nicht zugegriffen werden soll, auf `No` festgelegt sind.
6. Klicken Sie auf  oder **Apply** (Anwenden), um Ihre Änderungen zu speichern

Weitere Informationen über Benutzerrollen für Credential Management finden Sie unter *Übersicht über die Benutzerrollen*.

## 5.2 Anmelden für Konfigurationsaufgaben

Verwenden Sie für Konfigurations- und Administrationsaufgaben einen Computer, der physisch vor unberechtigtem Zutritt geschützt ist.

1. Geben Sie im Browser die HTTPS-Adresse des CredMgmt Servers ein, gefolgt von einem Doppelpunkt und der Portnummer (standardmäßig `5806`)
   `https://`<My_CredMgmt_server>`:5806`
   . Anschließend wird der Bildschirm **Login** (Anmeldung) angezeigt.
2. Melden Sie sich als CredMgmt **Administratorbenutzer** an.
3. Klicken Sie  , um das Menü **Einstellungen** zu öffnen.

## 5.3 Verwenden des Einstellungsmenüs zur Konfiguration

| | |
|---|---|
| **Allgemein** | – **Aufbewahrungszeitraum (Tage)** Diese Einstellung regelt die Bearbeitung von Personendatensätzen.<br>– Wenn der Zeitraum zum ersten Mal abläuft, wird der Datensatz durch die Anwendung anonymisiert.<br>– Wenn der Zeitraum zum zweiten Mal abläuft, wird der Datensatz durch die Anwendung gelöscht.<br>Der Standardwert ist `365`.<br>Legen Sie 0 fest, um die Beibehaltungsdauer vollständig zu deaktivieren. In diesem Fall werden Datensätze für unbestimmte Zeit aufbewahrt.<br>– **Logo**: Aktivieren oder deaktivieren Sie das Kontrollkästchen, das bestimmt, ob in den Dialogen ein benutzerdefiniertes Logo oder das Standardlogo angezeigt wird.<br>– Kriterien für angepasste Logo-Dateien finden Sie unter: *Anpassen des Firmenlogos, Seite 31*<br>– **Supergrafik:** Aktivieren oder deaktivieren Sie das Kontrollkästchen, das steuert, ob in den Dialogen die Bosch-Supergrafik angezeigt wird.<br>– **Languages** (Sprachen):<br>Wählen Sie die Sprachen, die in der Benutzeroberfläche verfügbar sein sollen, und die bevorzugten Formate für **Datum** und **Uhrzeit** aus.<br>– **Mail-Server**<br>Geben Sie die IP-Adresse, die Portnummer und die Kontodaten Ihres E-Mail-Servers ein, um den Versand von E-Mails über die Anwendung zu ermöglichen. Falls der externe E-Mail-Server ein zusätzliches SSL/TSL-Zertifikat benötigt, importieren Sie es auf der Maschine, auf der das Mobile Access-Backend ausgeführt wird. Nach dem Import muss der `VisitorManagerServer` neu gestartet werden.<br>– **E-Mail-Vorlagen**<br>Es werden mehrere HTML-E-Mail-Vorlagen bereitgestellt, die Sie in der Regel an Ihre eigenen Anforderungen anpassen können. Weitere Informationen finden Sie im Abschnitt **E-Mail-Vorlagen** weiter unten.<br>– **Mobile Access**<br>Aktivieren Sie das Kontrollkästchen **Mobile Access**, um Mobile Access zu aktivieren.<br><br>**Verbindung**: Geben Sie die Adresse des Mobile Access-Servers (Adresse des Registrierungsdienstes) ein.<br>`https://`<MyMobileAccessBackendServer>`:5700`<br>Verwenden Sie ein (FQDN) für <MyMobileAccessBackendServer> in Multi-Domain-Umgebungen.<br><br>**Hinweis:** um eine IP-Adresse anstelle eines FQDN zu verwenden, |

| | |
|---|---|
| | müssen Sie diese IP-Adresse unter **Zertifikaterstellung** eingeben, wenn Sie den Einrichtungsassistenten für das Mobile Access-Backend ausführen.<br><br>**Onboarding von Installationstechnikern:** Wählen Sie die Informationen aus, die Sie von den Installationstechnikern benötigen, damit diese die Mobile Access-Leser mit dem Bosch Setup Access konfigurieren können.<br><br>Melden Sie sich von der Webanwendung ab und melden Sie sich erneut an, um die Funktion Mobile Access sofort nutzen zu können. |

### 5.3.1 E-Mail-Vorlagen

Es werden mehrere HTML-E-Mail-Vorlagen bereitgestellt, die Sie in der Regel an die Anforderungen Ihres Unternehmens anpassen können. Für jede Vorlage können Sie E-Mail-Adressen für CC, BCC und einen Testempfänger hinterlegen, an den Sie sofort eine Test-E-Mail senden können.
Nachdem Sie sie über das Menü **Einstellungen** heruntergeladen haben, werden die Vorlagen im Standard-Download-Ordner Ihres Browsers gespeichert.

- `MobileAccess.html` Eine Aufforderung an einen Ausweisinhaber, Smartphone-basierte Anmeldeinformationen zu verwenden.
- `SetupAccess.html` Eine Aufforderung an einen Techniker, Leser für Mobile Access zu konfigurieren.

**Platzhalter zur Verwendung in E-Mail-Vorlagen**

Die E-Mail-Vorlagen bieten mehrere Textplatzhalter für die Aufnahme von Datenbankfeldern in den Text. Diese Platzhalter werden in den folgenden Tabellen beschrieben, je nachdem, in welchen Vorlagen sie verwendet werden können.

**Mobile Access**

E-Mail, die an einen Karteninhaber (für die Mobile Access-App) gesendet wird, wenn ihm Mobile Access gewährt wird

| Platzhalter | Description (Beschreibung) |
|---|---|
| `{{Title}}` | Titel der Person (Herr, Frau, Dr., etc.) |
| `{{FirstName}}` | Vorname der Person |
| `{{LastName}}` | Nachname der Person |
| `{{CompanyName}}` | Unternehmen der Person |
| `{{QrcodeLink}}` | QR-Code, der dem Link entspricht, der dem Ausweisinhaber den mobilen Zutritt über die App ermöglicht |
| `{{InviteLink}}` | Link, der dem Ausweisinhaber einen mobilen Zutritt über die APP bietet |

**Setup Access**

E-Mail, die an einen Mobile Access Installationstechniker (für die Setup Access-App) gesendet wird, wenn ihm der mobile Zutritt für die Einrichtung von Lesern gewährt wird.

| Platzhalter | Description (Beschreibung) |
|---|---|
| {{Title}} | Titel des Installationstechnikers (Herr, Frau, Dr. etc.) |
| {{FirstName}} | Vorname des Einrichters |
| {{LastName}} | Nachname des Einrichters |
| {{CompanyName}} | Unternehmen des Einrichters |
| {{QrcodeLink}} | QR-Code, der dem Link entspricht, der dem Installationstechniker einen mobilen Zutritt zur Einrichtung von Lesegeräten über die Setup Access-App bietet |
| {{InviteLink}} | Link, der dem Installationstechniker über die Setup Access-App mobilen Zutritt zur Einrichtung von Lesern bietet |

### 5.3.2 Dokumentenvorlagen

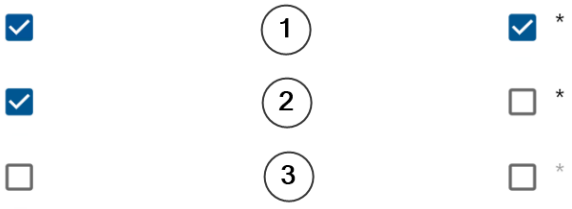
Für die verschiedenen Dokumente und E-Mails können Sie Vorlagen herunterladen und angepasste Versionen dieser Vorlagen im Dialog **Dashboard** > **Einstellungen > Allgemein** hochladen.

## 5.4 Anpassen der Benutzeroberfläche

Passen Sie die Benutzeroberfläche in den Dialogen Dashboard > **Einstellungen** an.

### 5.4.1 Optionen auf sichtbar, unsichtbar und obligatorisch einstellen

Wählen Sie aus, welche Datenfelder in den Dialogen sichtbar und welche dieser Daten dabei obligatorisch sein sollen.
Beispiel:




- (1) ist sichtbar und obligatorisch,
- (2) ist sichtbar, aber nicht obligatorisch
- (3) ist nicht sichtbar.

### 5.4.2 Anpassen von Texten der Benutzeroberfläche für die Lokalisierung

Sie können die Texte der Benutzeroberfläche für jede Sprache auf einfache Weise anpassen. Standardmäßig enthält der **lokalisierbare Text** die Standardüberschriften für Datenfeldblöcke in den Datenerfassungsdialogen.
So passen Sie diese Überschriften an die lokalen Anforderungen an:

1. Wählen Sie in der Liste eine Sprache für die Benutzeroberfläche aus.
2. Überschreiben Sie die Texte im Textfeld.
   Sie können für eine einfache Formatierung HTML-Tags verwenden, zum Beispiel:
   ```
   <b>this text will appear bold </b>
   <i>italics</i>
   <u>underline</u>
   ```

### 5.4.3 Anpassen des Firmenlogos

Grafikdateien, die Sie für Ihr Firmenlogo hochladen, müssen die folgenden Kriterien erfüllen:

| | |
|---|---|
| Unterstützte Formate | PNG, JPEG, JPG |
| Genaue Breite (Pixel) | 125 |
| Genaue Höhe (Pixel) | 63 |
| Max. Größe (MB) | 1 |

## 5.5 Firewall-Einstellungen

Fügen Sie Zusatzanwendungen zur Firewall-Konfiguration von Server- und Client-Computern hinzu:

1. Öffnen Sie die Windows-Firewall, indem Sie „Start > **Systemsteuerung** > **Windows-Firewall**“ klicken
2. Wählen Sie **Erweiterte Einstellungen** aus
3. Wählen Sie **Eingehende Regeln** aus
4. Wählen Sie im Bereich **Aktionen Neue Regel...** aus
5. Wählen Sie im Dialog **Regeltyp Port** aus und klicken Sie auf **Weiter >**
6. Wählen Sie auf der nächsten Seite **TCP und bestimmte lokale Ports** aus
7. Lassen Sie die Kommunikation über die folgenden Ports zu:

– Auf dem Server-Computer oder den Computern

<Servername>:44333 – vom AMS Identity Server verwendet **(*)**

<Servername>:5706 – vom VisMgmt-Server verwendet

<Servername>:5806 – vom CredMgmt-Server verwendet

<server name>:5701 – vom Mobile Access-Backend Server verwendet

– Auf Client-Computern

localhost:5707 – verwendet vom Bosch Peripheriegeräte-Add-on

**(*)** Wir verwenden die AMS- und BIS-Identitätsserver wie in den jeweiligen Installationshandbüchern beschrieben.

**Portnutzung innerhalb des Systems**

| Server ausgehend | Port Ausgang | Server eingehend | Port Eingang | Protokoll | Kommentare |
|---|---|---|---|---|---|
| VisMgmt oder CredMgmt | * | Mobile Access-Backend | 5701 | HTTPS | Befehle aus der Webanwendung zum Erstellen und/oder Löschen mobiler Anmeldedaten |
| Mobile Geräte aus dem Internet | * | Mobile Access-Backend | 5701 | HTTPS | Mobile Geräte erhalten mobile Anmeldedaten über das Internet |

| Server ausgehend | Port Ausgang | Server eingehend | Port Eingang | Protokoll | Kommentare |
|---|---|---|---|---|---|
| Mobile Access-Backend | * | Google Firebase (Internet) | * | HTTPS | Mobile Geräte erhalten Push-Benachrichtigungen. Bitte lesen Sie die Dokumentation von Google Firebase zu den Firewall-Einstellungen.<br><br>https://firebase.google.com/docs/cloud-messaging/concept-options |
| Client-Computer des VisMgmt-Benutzers | * | VisMgmt-Backend | 5706 | HTTPS | Befehle vom VisMgmt-Client-Computer an das VisMgmt-Backend |
| Client-Computer des CredMgmt-Benutzers | * | CredMgmt-Backend | 5806 | HTTPS | Befehle vom CreMgmt-Client-Computer an das CredMgmt-Backend |
| Admin-Computer | * | Mobile Access-Backend | 3389 | Remote Desktop (RDP) | Aus Sicherheitsgründen sollten Sie den Administratorzutritt auf den Mobile Access-Backend-Computer nur vorübergehend zulassen. |

**Hinweis!**
Beachten Sie, dass Mobile Access und der ACS keine direkte Verbindung haben, weder inbound noch outbound.

### 5.5.1 Programme und Dienste als Firewall-Ausnahmen

Sie können die Firewall auch konfigurieren, indem Sie Programme und Dienste als Ausnahmen hinzufügen

1. Starten Sie die Windows-Firewall-Benutzeroberfläche, wählen Sie **Start > Einstellungen > Systemsteuerung > Windows-Firewall**.
2. Wählen Sie die Registerkarte **Eine App oder Funktion durch die Windows Firewall zulassen**.
3. Wählen Sie **Andere App zulassen** (falls ausgegraut, aktivieren Sie die Schaltfläche, indem Sie **Einstellungen ändern** wählen).
4. Sie können die folgenden Programme hinzufügen:

**Programme**
Der Standardinstallationspfad lautet `C:\Program Files (x86)\Bosch Sicherheitssysteme\`

| Program (Programm) | Dateispeicherort |
|---|---|
| acsp.exe | [Install-path]\AccessEngine**AC**\BIN |
| ACTA-3.exe | [Install-path]\AccessEngine**AC**\BIN |
| BioVerify.exe | [Install-path]\AccessEngine**AC**\BIN |
| BioIdentify.exe | [Install-path]\AccessEngine**AC**\BIN |
| Bosch.Ace.CredentialManagement.exe | [Installationspfad]\Bosch Credential Management |
| Bosch.Access.MobileAccessBackend.exe | [Install-path]\Bosch Mobile Access |
| Bosch.Ace.VisitorManagement.exe | [Installationspfad]\Bosch Visitor Management |
| CalTa-3.exe | [Install-path]\AccessEngine**AC**\BIN |
| CDTA-1.exe | [Install-path]\AccessEngine**AC**\BIN |
| EMDP.exe | [Install-path]\AccessEngine**AC**\BIN |
| KCKemas.exe | [Install-path]\AccessEngine**AC**\BIN |
| KCS.exe | [Install-path]\AccessEngine**AC**\BIN |
| Loggifier-2.exe | [Install-path]\AccessEngine**AC**\BIN |
| PictureServer.exe | [Install-path]\AccessEngine**AC**\BIN |
| ReplServer.exe | [Install-path]\AccessEngine**AC**\BIN |
| reps.exe | [Install-path]\AccessEngine**AC**\BIN |
| TAccExc.exe | [Install-path]\AccessEngine**AC**\BIN |
| EMAILSP.exe | [Install-path]\AccessEngine**AC**\BIN |
| master-3.exe | [Install-path]\AccessEngine**AC**\BIN |
| querySrv-2.exe | [Install-path]\AccessEngine**AC**\BIN |
| webSrv-1.exe | [Install-path]\AccessEngine**AC**\BIN |
| LicenseGateway.exe | [Install-path]\AccessEngine**AC**\BIN |
| DMS.exe | [install-path]\AccessEngine**MAC**\BIN |
| lac.exe | [install-path]\AccessEngine**MAC**\BIN |

**Dienste**

Der Standardinstallationspfad lautet `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System`

| Service | Dateispeicherort |
|---|---|
| Bosch.States.Api | [install-path]\States API |
| Bosch.Map.Api | [install-path]\Map API |
| Bosch.MapView.Api | [install-path]\Map View API |
| Bosch.Events.Api | [install-path]\Events API |

| Service | Dateispeicherort |
|---|---|
| Bosch.Alarms.Api | [install-path]\Alarms API |
| Bosch.Ace.IdentityServer | [install-path]\Identity Server |
| Bosch.Ace.Api | [install-path]\Access API |
| Bosch.DialogManager.Api | [install-path]\Dialog Manager API |
| Bosch.Intrusion.Api | [install-path]\Intrusion API |
| Bosch Ace Visitor Management | [VM-install-path]\ |
| Bosch Ace Visitor Management Client | [VM-client-install-path]\ |
| Bosch.OSS-SO | [install-path]\OSS-SO |
| Bosch.OSS-SO.Configurator | [install-path]\OSS-SO.Configurator |
| Bosch.Access.ProductApi.Api | [install-path]\ProductApi |
| Bosch.MUM | [MUM-install-path]\ |

### 5.5.2 Mobiler Zutritt API

Ab der Veröffentlichung von Mobile Access 5.2, Credential Management 5.2 und Visitor Management 5.2 wurde die API des Mobile Access-Backends in einen Front-Channel-Teil und einen Back-Channel-Teil aufgeteilt. Der Front-Channel dient zur Kommunikation mit Mobiltelefonen, während der Back-Channel mit Credential Management und/oder Visitor Management kommuniziert.
Dies ermöglicht das Festlegen von Firewallregeln und Routen zur Regulierung des Netzwerkverkehrs, um die IT-Sicherheit zu stärken. Die Aufteilung der API geht mit zwei separaten Portnummern einher. Der Port für das Mobiltelefon ist 5700, während der Port für Credential Management und Visitor Management 5701 ist.
Sowohl Credential Management als auch Visitor Management haben zwei separate Einstellungen für die Front-Channel-URL und die Back-Channel-URL. In der Benutzeroberfläche werden sie „Administrative service address“ (Back-Channel) und „Registration service address“ (Front-Channel) genannt.
Der Standardport für „Administrative service address“ (Back-Channel) ist 5701. In einer kundenspezifischen Firewallregel sollte dieser Port nur für die Kommunikation mit der Maschine konfiguriert werden, auf der das Backend von Credential Management und/oder Visitor Management ausgeführt wird, was in den meisten Fällen der AMS-Server ist.
Der Standardport für die „Registration service address“ (Front-Channel) ist 5700. In einer kundenspezifischen Firewallregel sollte dieser Port so konfiguriert werden, dass er über die Mobile Access-Apps erreichbar ist. In vielen Szenarien ist dieser Endpunkt von außen zugänglich. Dies hängt jedoch in hohem Maße vom Kundenszenario ab.
Wenn der Kunde von einer früheren Version auf die neueste AMS-Version aktualisiert, müssen die Einstellungen von Credential Management und Visitor Management angepasst werden. Diese Einstellung ist für die Administrator-Rolle für Visitor Management und Credential Management auf der Einstellungsseite zugänglich.
Der Back-Channel sollte so gesichert werden, dass er nicht aus dem öffentlichen Internet oder einem beliebigen unbefugten Netzwerk erreichbar ist.

## 5.6 IT-Sicherheit

Die Sicherheit des Zutrittskontrollsystems einer Organisation ist ein entscheidender Teil ihrer Infrastruktur. Bosch rät zur strikten Einhaltung der IT-Sicherheitsrichtlinien, die für das Land gelten, in dem die Installation durchgeführt wurde.
Die Organisation, die das Zutrittskontrollsystem betreibt, ist mindestens für die folgenden Punkte verantwortlich:

### 5.6.1 Verantwortlichkeit für die Hardware

- Verhinderung des unberechtigten physischen Zugriffs auf Netzwerkkomponenten wie z. B. RJ45-Verbindungen.
  - Angreifer benötigen physischen Zutritt, um Man-in-the-Middle-Angriffe durchzuführen.
- Die Verhinderung des unberechtigten physischen Zugriffs auf die AMC2-Controller-Hardware.
- Verwendung eines dedizierten Netzwerks für die Zutrittskontrolle.
  - Angreifer können über andere Geräte innerhalb desselben Netzwerks Zutritt erlangen.
- Die Verwendung von sicheren Anmeldeinformationen wie **DESFire** mit Code von Bosch und mehrstufiger Authentifizierung durch Biometrie.
- Die Aufforderung zur Registrierung über die **Setup Access**-App der Mobiler Zutritt-Leser mit BLE-Modulen (Bluetooth Low Energy). Nicht registrierte, eingeschaltete Leser sind anfällig für Missbrauch durch Drittanbieter. Um einen solchen Missbrauch zu verhindern, lesen Sie im Installationshandbuch des Leser nach, wie Sie die Werkseinstellungen zurücksetzen können.
- Bereitstellung einer Ausfallsicherung und einer Notstromversorgung für das Zutrittskontrollsystem
- Das Nachverfolgen und Deaktivieren von Anmeldeinformationen, die angeblich verloren gegangen sind oder verlegt wurden.
- Die ordnungsgemäße Stilllegung von Hardware, die nicht mehr verwendet wird, insbesondere ihre Zurücksetzung auf die Werkseinstellungen und die Löschung von personenbezogenen Daten und Sicherheitsinformationen.

### 5.6.2 Verantwortlichkeiten für die Software

- Die ordnungsgemäße Wartung, Aktualisierung und Funktionstüchtigkeit der Firewall des Zutrittskontroll-Netzwerks.
- Die Überwachung von Alarmen, die darauf hinweisen, wann Hardwarekomponenten, z. B. Ausweisleser oder AMC2-Controller, offline gehen.
  - Diese Alarme können auf einen Versuch hindeuten, Hardwarekomponenten auszutauschen.
- Überwachung von Alarmen zur Manipulationserkennung, die durch elektrische Kontakte in der Zutrittskontroll-Hardware ausgelöst werden, wie beispielsweise Controllern, Lesern und Schaltschränken.
- Die Beschränkung von UDP-Broadcasts im dedizierten Netzwerk.
- Aktualisierungen der Zutrittskontrollsoftware, insbesondere Sicherheitsupdates und Patches.
- Aktualisierungen der Firmware der Hardware, insbesondere Sicherheitsupdates und Patches.

  - Beachten Sie, dass selbst bei kürzlich gelieferter Hardware möglicherweise ein Firmware-Update erforderlich ist. Anweisungen hierzu finden Sie im Handbuch zur Hardware.
  - Bosch übernimmt keinerlei Haftung für Schäden, die durch Produkte entstehen, die mit veralteter Firmware in Betrieb genommen wurden.
- Die Verwendung von OSDPv2 Secure Channel-Kommunikation.
- Die Verwendung starker Passwort-Sätze.
- Die Durchsetzung des *Prinzips der geringsten Rechte*, um sicherzustellen, dass einzelne Benutzer nur auf die Ressourcen zugreifen können, die sie für ihren legitimen Bedarf benötigen.
- Die ordnungsgemäße Zuweisung und Konfiguration von Benutzerprofilen für Bediener, um zu vermeiden, dass normale Benutzer Hochsicherheitsberechtigungen ohne das Zwei-Personen-Prinzip zuweisen.

### 5.6.3 Sicherer Umgang mit mobilen Anmeldedaten

- Lassen Sie unkonfigurierte Mobile Access-Leser nicht unbewacht.
  - Ein Angreifer könnte das Lesegerät für einen anderen ACS missbrauchen. Dies würde einen kostspieligen Werksreset erfordern.
- Wenn ein mobiles Gerät mit mobilen Anmeldedaten verloren geht oder gestohlen wird, behandeln Sie dieses Gerät wie einen verlorenen Ausweis: Sperren oder löschen Sie alle mobilen Anmeldedaten so schnell wie möglich.
- Für hochsichere Umgebungen empfiehlt Bosch eine Zwei-Faktor-Authentifizierung. Dies erfordert, dass der Inhaber des Berechtigungsnachweises das mobile Gerät entsperrt, bevor er es als Anmeldedaten verwendet.
- Mobile Anmeldedaten werden nicht wiederhergestellt, wenn ein Smartphone aus einem Backup wiederhergestellt wird. Wenn ein Inhaber einer mobilen Berechtigung ein neues mobiles Gerät erhält, müssen Sie alle aktuellen Einladungen erneut versenden.
- Ein Angreifer könnte einen Störsender verwenden, um die Kommunikation mit mobilen Lesegeräten zu blockieren. Mitarbeiter, deren Zutritt zu bestimmten Bereichen unerlässlich ist, sollten einen physischen Ausweis als Backup mit sich führen.
  - Verwenden Sie als Backup für Mobile Access nur physische Ausweise mit einer sicheren Kodierung (z. B. Bosch-Code).
- Schützen Sie den Mobile Access-Server vor unbefugtem physischen Zutritt. Bosch empfiehlt zusätzliche Maßnahmen wie z. B. die BitLocker-Festplattenverschlüsselung.
- Schützen Sie den Mobile Access vor DoS-Angriffen (Denial of Service). Es muss Teil einer sicheren Netzwerkumgebung sein, die Schutzmaßnahmen wie einen Rate-Limiter bietet.
- Behandeln Sie QR-Codes für Einladungen zur Installation als Administrator-Anmeldedaten. Ein gestohlenes Telefon eines Installationstechnikers mit aktiven Anmeldedaten dieses Installationstechnikers könnte es einem Angreifer ermöglichen, Mobile Access-Leser böswillig neu zu konfigurieren.
  - Schicken Sie die Einladungen an die Installationstechniker rechtzeitig vor der Einrichtung des Lesers und stellen Sie sicher, dass sie die Anmeldedaten löschen, sobald die Einrichtung abgeschlossen ist.
  - Verwenden Sie die Funktion „QR-Codes vom Bildschirm scannen“, anstatt Einladungen per E-Mail zu verschicken. Stellen Sie sicher, dass der vorgesehene Installationstechniker die Anmeldedaten sofort lädt.

## 5.7 Privatsphäre und Datenschutz bei Bosch

**Einführung**

In allen Geschäftsprozessen und in Übereinstimmung mit den geltenden gesetzlichen Bestimmungen stellen wir sicher, dass die Privatsphäre gewahrt wird, persönliche Daten geschützt werden und Geschäftsinformationen sicher aufbewahrt werden. Technisch und organisatorisch, insbesondere beim Schutz vor unberechtigtem Zutritt und Verlust, wenden wir einen angemessenen Standard an, der dem Stand der Technik entspricht und die damit verbundenen Risiken berücksichtigt. Bei der Entwicklung von Bosch-Produkten und neuen Geschäftsmodellen stellen wir sicher, dass die gesetzlichen Anforderungen an Datenschutz und Informationssicherheit frühzeitig berücksichtigt werden.
Neben der Compliance-Organisation und der Rechtsabteilung ist der Datenschutzbeauftragte der erste Ansprechpartner für Fragen zum richtigen Umgang mit Daten.

**Verarbeitung personenbezogener Daten in der Mobile Access-App und im Mobile Access Backend-System**

- Kategorien von personenbezogenen Daten
  - Die Mobile Access-Apps enthalten personenbeziehbare Daten. Dies ist die Ausweisnummer, die verwendet wird, um Zutritt an den Lesern zu erhalten. Der Zutritt auf die tatsächlichen Daten von realen Personen ist nur durch die zusätzliche Verwendung der Programme AMS, ACE oder Visitor Management möglich.
  - Bei der Registrierung des Installationstechnikers im Menü **Einstellungen** müssen keine persönlichen Daten gespeichert werden. Dennoch können einige Benutzerinformationen, wie z. B. E-Mail-Adressen, optional gespeichert werden.
  - Der Backend-Server für die Mobile Access-App speichert personenbezogene Daten für das Credential Management.
- Datenübertragung
  - Die Ausweisdaten werden zwischen dem Backend-System, der Mobile Access-App und dem Visitor Management-System übertragen, um den Zutritt an den Lesern zu kontrollieren.
- Protokollierung von Daten
  - Die Mobile Access-App führt technische Protokolle. Diese Protokolle werden lokal auf dem mobilen Gerät gespeichert und können bei Bedarf an Dritte, z. B. den technischen Support, gesendet werden.
  - Der Backend-Server führt auch technische Protokolle. Die Daten werden lokal auf dem Serversystem gespeichert.
  - In der Standardeinstellung löscht der Backend-Server die Protokolldateien nicht automatisch. Die automatische Löschung kann jedoch auf der Grundlage der verbleibenden Speicherkapazität oder eines Zeitplans konfiguriert werden.

**Was haben wir getan, um das Produkt datenschutzfreundlich zu gestalten?**

Bosch Zutrittskontrollsysteme verwalten die Zutrittsrechte von Personen. Um diese Personen zu schützen, ergreift Bosch Maßnahmen, um die Anforderungen der Datenschutzgrundverordnung direkt in die Produktentwicklung zu integrieren und verfolgt dabei einen „Privacy by Design“-Ansatz.

- Es wird eine hochmoderne Verschlüsselung verwendet.
- Die Anmeldedaten sind pseudonymisiert.
- Der Benutzer der App muss keine persönlichen Daten eingeben, um virtuelle Anmeldedaten per QR-Code oder E-Mail zu erhalten.

- Das Löschen von Anmeldedaten ist aus den Mobile Access-Apps, aus den primären Zutrittskontrollsystemen und aus Zusatzanwendungen wie der Visitor- und Credential Management möglich.
- Berechtigungsnachweise können von den Bedienern der primären Zutrittskontrollsysteme und der Zusatzanwendungen jederzeit gesperrt werden.
- Telemetriedaten sind von vornherein anonymisiert.
- Logdateien werden von mobilen Geräten nicht ohne die aktive Zustimmung und Mitarbeit des Nutzers an andere Parteien, wie z. B. den technischen Support, übertragen.
- Die geplante automatische Löschung von Protokolldateien ist im primären Zutrittskontrollsystem konfigurierbar.
- Bosch erfordert keine Registrierung im App Store oder in der App. Der App Store gibt keine persönlichen Daten an Bosch weiter.
- Die App benötigt Bluetooth, um zu funktionieren, fordert aber den Benutzer auf, Bluetooth manuell zu aktivieren.

**Weitere Fragen**

Weitere Informationen zum Datenschutz finden Sie in den Datenschutzhinweisen in der Mobile Access-App, oder wenden Sie sich an Ihr Bosch Projektteam.

## 5.8 Hochsicherheitsberechtigungen

### 5.8.1 Zwei-Personen-Prinzip

Ab AMS 5.5 ist die Aktivierung des Zwei-Personen-Prinzips möglich. Das Hauptziel dieser Funktion besteht in einer höheren Sicherheit beim Zuweisen von Berechtigungen, indem ein Genehmiger hinzugefügt wird. In Credential Management kann ein Bediener einer ausgewählten Person eine oder mehrere Berechtigungen zuweisen. Im Gegensatz zu einer typischen Berechtigungszuweisung, bei der eine Berechtigung sofort dem Benutzer zugewiesen wird, werden Berechtigungen bei aktiviertem Zwei-Personen-Prinzip zunächst als Anforderung an einen anderen Bediener gesendet, der die Berechtigungsanforderung genehmigen oder ablehnen kann. Auf diese Weise können falsche Zuweisungen vermieden werden, um sensible Bereiche besser zu schützen, d. h. Berechtigungen können einem Mitarbeiter nur zugewiesen werden, wenn zwei Bediener (Anforderer und Genehmiger) zustimmen.

### 5.8.2 Konfigurieren von Hochsicherheitsberechtigungen

Zum Aktivieren des Zwei-Personen-Prinzips sind die folgenden Voraussetzungen erforderlich:

- Installiertes AMS mit der neuesten Version.
- Konto mit AMS-Administratorrechten.

**Erstellen von Zutrittsberechtigungen mit Zwei-Personen-Prinzip**

Im Haupt-Zutrittskontrollsystem:

**Dialogpfad**

AMS Main menu > **System data** > **Authorizations** (AMS Hauptmenü > Systemdaten > Berechtigungen)

1. Klicken Sie in der Symbolleiste auf **New** (Neu)  , um den Inhalt der Eingabefelder zu löschen.

   Alternativ klicken Sie auf **Copy** (Kopieren)  , um eine neue Berechtigung basierend auf einer bestehenden zu erstellen.
2. Geben Sie einen eindeutigen Namen für die Berechtigung ein.
3. (Optional) Geben Sie eine Beschreibung ein
4. (Optional) Wählen Sie ein Zeitmodell, um diese Berechtigung zu regeln
5. (Optional) Wählen Sie ein **Inaktivitätslimit** aus der Liste aus.
6. (Obligatorisch) Weisen Sie mindestens einen **Eingang** zu.
7. Aktivieren Sie das Kontrollkästchen **Approval required** (Genehmigung erforderlich), um das Zwei-Personen-Prinzip zu aktivieren.
8. Klicken Sie auf "Save" (Speichern)  , um die Berechtigung zu speichern.

**Hinweis!**
Sicherheitsempfehlung
Diese Funktion gilt nur für Credential Management. In AMS müssen Administratoren Benutzerprofile für Bediener korrekt zuweisen und konfigurieren, damit Dialoge nicht mehr zugänglich sind. Dadurch wird verhindert, dass normale Bediener Hochsicherheitsberechtigungen ohne das Zwei-Personen-Prinzip zuweisen können.

Weitere Informationen finden Sie in der aktuellen Version des Softwarehandbuchs für *Access Management System Konfiguration und Betrieb*.

# 6 Bedienung

## 6.1 Übersicht über die Benutzerrollen

Die Fähigkeiten der Benutzer im Credential Management werden durch ihre Benutzerprofile im ACS bestimmt:

| Benutzertyp | Anwendungsfälle |
|---|---|
| Administrator | Vornahme globaler Einstellungen<br>Anpassen des Verhaltens des Tools und seiner Benutzeroberfläche<br>plus<br>Alle Anwendungsfälle von Bedienern |
| Bediener | Zuweisung und Aufhebung der Zuweisung von physischen Zutrittsausweise und virtuellen Anmeldedaten für den mobilen Zutritt |
| Zwei-Personen-Prinzip: Anforderer | Anfordern von Hochsicherheitsberechtigungen |
| Zwei-Personen-Prinzip: Genehmiger | Genehmigen oder verweigern von Hochsicherheitsberechtigungen<br>Entfernen normaler Berechtigungen |

**Siehe**

– *Erstellen von Credential Management-Benutzern im ACS, Seite 27*

## 6.2 Verwendung des Dashboards

Das Dashboard ist der Startbildschirm – ein zentraler Dialog, der zu allen anderen Dialogen führt.

**Allgemeine Verwendung der Personaltabelle**

Jede Zeile in der Tabelle steht für eine Person. Dabei handelt es sich um interne oder externe Mitarbeiter, die Anmeldedaten für den Zutritt zu den Räumlichkeiten benötigen.

- Sie können einzelne Personen oder mehrere Personen auf einmal auswählen, indem Sie die Tastatur-Maus-Idiome verwenden:
  - Strg + Klick zur Mehrfachauswahl einzelner Zeilen.
  - Umschalt + Klick auf eine bereits ausgewählte Zeile, um sie aus der Auswahl zu entfernen.
  - Umschalt + Klick für Mehrfachauswahl von zusammenhängenden Zeilen.
- Sie können neue Personen hinzufügen
- Sie können Anmeldedaten zuweisen und ihre Zuweisung aufheben, indem Sie auf die Aktionsschaltflächen klicken
  - Einen physischen Berechtigungsnachweis zuweisen
  - Zuweisen virtueller Anmeldedaten (für den mobilen Zutritt)
  - Details zur Person bearbeiten
- Sie können alle Daten in eine .CSV- oder .XLSX-Datei exportieren. Verwenden Sie die Filterfunktion, wenn nur bestimmte Daten gewünscht werden. Es ist nicht möglich, die gewünschten Daten nur durch ihre Auswahl zu exportieren. Es können nur die aktuell gefilterten Linien in eine .CSV- oder .XLSX-Datei exportiert werden.

**Die Funktionen des Dashboards**


| Beschriftung | Funktion |
|---|---|
| (1)<br>N **Einträge** | Die Gesamtzahl N der Personen (jede Person ist eine Zeile in der Tabelle). |
| (2)<br>**Suchen** | Suche nach beliebigem Text unter den Personen in der Tabelle |
| (3)  | Wählen Sie alle Objekte in der Liste aus |
| (4)  <br>**Löschen** | Löscht die ausgewählten Elemente |
| (5)  <br>**Letzte** | Zeigen Sie die Personen an, die der Tabelle zuletzt hinzugefügt wurden. |
| (6)  <br>**Zurücksetzen** | Die Tabelle auf die Standardansicht zurücksetzen und alle Filter wiederherstellen. |
| (7)  <br>**Zuweisung eines Ausweises aufheben** | Öffnen Sie einen Dialog, um die Zuweisung von Ausweisen mithilfe eines verbundenen Bekanntmachungslesers aufzuheben. |
| (8) **. . .** | Klicken Sie auf das Ellipsen-Symbol, um das Menü zu öffnen, mit dem Sie Personen und Dokumente in verschiedene Dateiformate exportieren können, zum Beispiel `.CSV` und `.XLSX`.<br><br>Beachten Sie, dass Sie aus Gründen der Datensicherheit nur exportieren können, wenn Ihr Client über eine gesicherte HTTPS-Verbindung mit einem Zertifikat läuft. |
| (9)  | Öffnet ein Dialogfeld zum Anlegen einer neuen Person |

**Die Spalten des Dashboards**

| Spalte | Description (Beschreibung) |
|---|---|
| **Name** | Klicken Sie auf den Hyperlink, um die Details der Person anzuzeigen. |
| **E-Mail** | |
| **Department** (Abteilung) | |
| **Position** | |
| **Company** (Unternehmen) | |
| **Ausweisnummer** | Die Nummern der Ausweise, die dieser Person zugewiesen sind. |
| **Aktionen** | Siehe separate Tabelle unten |

**Aktionen, die Sie für Personaldatensätze in der Dashboard-Tabelle durchführen können**

| Symbol | Aktionen |
|---|---|
|  | **Zuweisen** einer oder mehrerer physischen Ausweise an die Person |
|  | **Zuweisen** von Mobile Access Anmeldedaten |
|  | **Bearbeiten** der persönlichen Daten der Person.<br>Änderungen werden an den ACS weitergegeben. Die im ACS vorgenommenen Änderungen werden an die CredMgmt-Anwendung weitergegeben. |

### 6.2.1 Übersichtsseite der Person

Durch Klicken auf den Namen einer Person öffnet sich ein Dialogfeld mit den personenbezogenen Daten. In diesem Dialog werden die wichtigsten Informationen der Person in Feldern angezeigt und können bearbeitet werden. Grundlegende Informationen werden dauerhaft auf der linken Seite des Dialogs angezeigt.
Informationen über Sperrlisteneinträge (falls vorhanden) werden am unteren Rand dieser Spalte mit grundlegenden personenbezogenen Informationen angezeigt.
**Tipp**: Das Feld **Title** (Titel) bietet neben den in der Dropdown-Liste verfügbaren Möglichkeiten auch Freitext.
Im selben Dialog gibt es drei Registerkarten mit einer eigenen Ansicht: **Details, Credentials, Authorizations** (Details, Anmeldedaten, Berechtigungen).
Wenn diese Person gesperrt ist, wird in Credential Management ein orangefarbener Hinweis mit dem Wort **Blacklisted** angezeigt. Dort wird auch angezeigt, wieso und von wem die Person gesperrt wurde.
Ein Administrator und ein Bediener mit den entsprechenden Rechten kann die Person durch einen Klick auf die Schaltfläche **Blacklist** (Sperren) sperren.

– Ein Warnfenster wird geöffnet.

1. Klicken Sie auf **Yes** (Ja).

2. Geben Sie im Assistent **Reason** (Grund) den Grund ein und wählen Sie dann **Save > Ok** (Speichern > OK) aus.

Beachten Sie, dass eine gesperrte Person die ihr zugewiesenen Berechtigungen weiterhin behält. Diese Person kann jedoch keine Eingänge/Türen mehr öffnen.
Wenn die Sperre der Person aufgehoben werden soll, klicken Sie einfach auf die Schaltfläche **X Remove from blacklist** (X Sperre aufheben).
Konfigurieren Sie die Rechte ordnungsgemäß. Weitere Informationen zu **Benutzerrechten** finden Sie im Softwarehandbuch für *Access Management System Konfiguration und Betrieb*.

**Details**
In dieser Registerkarte können Sie personenbezogene Daten eingeben, die nicht ständig sichtbar sein müssen.

**PIN**
Auf dieser Registerkarte **Details** können PINs (Verifikations-PIN)[1] für einen Ausweisinhaber angezeigt und geändert werden. Beim Ändern der PIN kann ein Ablaufdatum festgelegt werden.
**Hinweis**: Wenn die PIN oder ihre Einstellungen geändert werden, muss die PIN zur Bestätigung erneut eingeben werden.
Wenn eine oder mehrere **PIN-Sperren** für die Anmeldedaten der gewählten Person vorhanden sind, wird unten in der Spalte mit den grundlegenden personenbezogenen Daten ein Hinweis angezeigt. Wenn der Bediener auf diesen Hinweis klickt, wird die Registerkarte **Credentials** (Anmeldedaten) ausgewählt, und der Bediener kann weitere Informationen zur **PIN-Sperre** anzeigen.
Beachten Sie, dass bei einem Validierungsfehler auf einer Registerkarte keine andere Seite ausgewählt werden kann, bis der Fehler behoben wurde.
[1] Credential Management unterstützt nur Standard-PINs. Identifikations-PINs und separate EMA-PINs/Scharfschalte-PINs werden nicht unterstützt.
Weitere Informationen zu **PINs** finden Sie im Softwarehandbuch für *Access Management System Konfiguration und Betrieb*.

**Berechtigungsnachweis**
In dieser Registerkarte können Sie mit der Schaltfläche **Read card** (Ausweis lesen) einen physischen Ausweis bzw. mit der Schaltfläche **Add mobile access** (Mobilen Zutritt hinzufügen) mobile Anmeldedaten zuweisen. Weitere Informationen finden Sie unter *Zuweisen von mobilen Anmeldedaten* und *Zuweisen von physischen Anmeldedaten*.
**Hinweis**: Ein orangefarbener Punkt auf dem Telefonsymbol weist darauf hin, dass die Anmeldedaten bereits auf dem Mobiltelefon vorhanden sind, aber noch im Mobile Access-Backend freigegeben werden müssen. Erst nach dieser Freigabe wird der Punkt grün.

**Autorisierungen**
In dieser Registerkarte können alle zugewiesenen Berechtigungen angezeigt und geändert werden. Weitere Informationen finden Sie unter *Zuweisen von Berechtigungen auf der Seite mit Personeninformationen*.
Beachten Sie, dass die Schaltfläche **Save & Close** (Speichern und schließen) in allen Registerkartendialogen Sie zum **Dashboard**-Dialog weiterleitet.

## 6.3 Zuweisen von Berechtigungen

**Zuweisen von Berechtigungen auf der Seite mit Personeninformationen**
– Im Dashboard-Dialog wird eine Liste von Personen angezeigt.
1. Klicken Sie auf den Namen einer Person.

– Der Dialog mit Personeninformationen wird geöffnet.
1. Klicken Sie rechts oben im Dialog auf die Registerkarte **Authorizations** (Berechtigungen).
2. Klicken Sie zum Zuweisen einer neuen Berechtigung auf **Modify authorizations** (Berechtigungen ändern).

Ein Assistent mit einer Liste aller Berechtigungen wird angezeigt. Alle diese Berechtigungen wurden zuvor im Access Management System konfiguriert. Wählen Sie ab diesem Schritt, welche Berechtigungen Sie zuweisen möchten.

1. Navigieren Sie zu  > **Confirm** > **Save** (Bestätigen > Speichern).

**Hinweis**: Hochsicherheitsberechtigungen, d. h. die Funktionalität bei aktiviertem Zwei-Personen-Prinzip, erscheinen mit  .

Der Dashboard-Dialog wird geöffnet. Wenn eine normale Berechtigung zugewiesen wurde, kann durch erneuten Klick auf den Personennamen und Prüfung der Registerkarte **Authorizations** (Berechtigungen) überprüft werden, ob die Berechtigung tatsächlich zugewiesen wurde.
Wenn die Berechtigung mit Zwei-Personen-Prinzip zugewiesen wurde, ist der Vorgang anders. In diesem Fall ist die Berechtigung nicht sofort nach dem Speichern aktiv, sondern wird zunächst angefordert. In den Spalten **Authorizations** (Berechtigungen) und **Actions** (Aktionen) wird ersichtlich, wer die Berechtigung angefordert hat.
Auf der Registerkarte **Authorizations** (Berechtigungen) werden die Berechtigungen mit Zwei-Personen-Prinzip entweder als genehmigt oder verweigert angezeigt. Wenn Sie den Cursor über Berechtigungsnamen bewegen, zeigt ein Tooltip an, wann und von wem die Berechtigung angefordert wurde.

Je nach Berechtigungsart und abhängig von der Benutzerrolle und Benutzerrechten können die angezeigten **Aktionsschaltflächen** folgende sein:

**Request** (Anforderung)
**Retract** (Zurückziehen): Die eigene Anforderung auf Berechtigungszuweisung stornieren, die noch nicht genehmigt wurde.
**Approve** (Genehmigen): Die Berechtigungsanforderung eines anderen Bedieners genehmigen.
**Deny** (Verweigern): Die Berechtigungsanforderung eines anderen Bedieners ablehnen.
**Remove** (Entfernen): Zugewiesene Berechtigung entfernen. Dies gilt für normale und Hochsicherheitsberechtigungen.

**Hinweis:** Aktionen werden nicht nur durch das Klicken auf die Aktionsschaltfläche aktiviert. Sie müssen immer auch auf **Save** (Speichern) klicken.
Weitere Informationen finden Sie unter *Übersicht über die Benutzerrollen*.

Im AMS sollten die **Benutzerprofile** ordnungsgemäß mit den verfügbaren Rechten für das Zwei-Personen-Prinzip konfiguriert werden:
– Administrator
– Bediener
– Zwei-Personen-Prinzip: Anforderer

– Zwei-Personen-Prinzip: Genehmiger

Weitere Informationen zur Konfiguration von **Benutzerprofilen** finden Sie in der aktuellen Version des Softwarehandbuchs für *Access Management System Konfiguration und Betrieb*.

**Ausstehende Berechtigungsanforderungen**
Ein Bediener mit Genehmiger- oder Anfordererrechten und ein Administrator können die **Berechtigungsanforderungen** im Menü anzeigen. In diesem Dialog können alle **ausstehenden Berechtigungsanforderungen** in einer Ansicht angezeigt werden, ohne dass durch jeden Personennamen navigieren werden muss.
Ein Bediener-Genehmiger kann Berechtigungen über diesen Dialog genehmigen und ein Administrator kann Berechtigungen zurückziehen. Ein Bediener-Anforderer kann nur die ausstehenden Berechtigungsanforderungen anzeigen. Ein Bediener ohne Genehmiger- und Anfordererrechte kann diesen Dialog nicht anzeigen.
**Hinweis:** Aktionen werden nicht nur durch das Klicken auf die Aktionsschaltfläche aktiviert. Nach einem Klick auf die Aktionsschaltfläche wird sie grau. Klicken Sie dann auf **Save** (Speichern).

## 6.4 Zuweisung von physischen Anmeldedaten

**Voraussetzungen**
Es wird dringend empfohlen, neuen Mitarbeitern neue Anmeldedaten zuzuweisen, und zwar mit einem neuen Ausweis, einem Ausweisdrucker und einem Bekanntmachungsleser.

**Zuweisen eines Ausweises (erfordert einen Bekanntmachungsleser)**
**Vorgehensweise**
Ein Ausweis kann entweder direkt vom Dashboard-Symbol oder aus der Übersichtsseite der Person zugeordnet werden.
Auf dem **Dashboard**:
1. Halten Sie einen physischen Zutrittsausweis bereit, den Sie dem Bekanntmachungsleser vorlegen.
2. Wählen Sie die Zeile der Person und klicken Sie auf 
3. Befolgen Sie die Anweisungen in der Popup-Benachrichtigung zur Verwendung des Bekanntmachungslesers.

Auf der Übersichtsseite der Person:
1. Wählen Sie auf dem **Dashboard** den Namen der Person aus. Die Übersichtsseite der Person wird geöffnet.
2. Navigieren Sie zur Registerkarte **Credential** > **Read card** (Anmeldedaten > Ausweis lesen).

**Zuweisen eines Ausweises im Anmeldedaten-Editor (erfordert einen Bekanntmachungsleser)**
1. Wählen Sie auf dem Dashboard in der Personentabelle eine Person aus und klicken Sie auf  , um die Anmeldedaten dieser Person zu bearbeiten.
2. Klicken Sie auf **Ausweis lesen** und befolgen Sie die Anweisungen im Popup-Fenster zur Verwendung des Bekanntmachungslesers.

– Wiederholen Sie die letzten Schritte, um bei Bedarf weitere Ausweise zuzuweisen.
3. Klicken Sie auf **Speichern**, um die aktuellen Person mit den Ausweiszuweisungen zu speichern.

## 6.5 Zuweisen von mobilen Anmeldedaten

**Voraussetzungen**

– Mobile Access ist auf Ihrem System installiert und konfiguriert.
  – Anweisungen dazu finden Sie im entsprechenden Abschnitt im Kapitel über die Installation in diesem Dokument.
– Die empfangende Person hat die Mobile Access-App installiert und sie läuft auf ihrem Smartgerät.
  – Anweisungen dazu finden Sie im entsprechenden Abschnitt im Kapitel über die Installation in diesem Dokument.

**Vorgehensweise**

Mobile Anmeldedaten können entweder direkt vom Dashboard-Symbol oder aus der Übersichtsseite der Person zugeordnet werden.

Auf dem **Dashboard**:

1. Wählen Sie die Zeile der Person aus, die mobile Anmeldedaten erhalten soll
2. Klicken Sie in der ausgewählten Zeile auf 

Auf der Übersichtsseite der Person:

1. Wählen Sie auf dem **Dashboard** den Namen der Person aus. Die Übersichtsseite der Person wird geöffnet.
2. Navigieren Sie zur Registerkarte **Credential** > **Add mobile access** (Anmeldedaten > Mobilen Zutritt hinzufügen).

Fahren Sie mit den folgenden Anweisungen fort:

1. Wählen Sie eines der großen Symbole für die Optionen:

– **QR-Code**
  oder
– **Einladungsmail**

2. Wenn Sie die Option **QR-Code** wählen:

– Das System zeigt einen QR-Code an
– Die Person scannt den QR-Code mit der Mobile Access-App auf ihrem Mobilgerät
– Sie müssen den Besuch **genehmigen**, damit die Berechtigungen funktionieren. Weitere Informationen finden Sie im Abschnitt Genehmigung und Ablehnung von Besuchen
– Das Mobilgerät funktioniert wie ein physischer Zutrittsausweis, solange die App läuft

3. Wenn Sie die Option **Einladungsmail** wählen:

– Standardmäßig wählt das Programm die E-Mail-Adresse aus, die für die ausgewählte Person definiert wurde. Geben Sie bei Bedarf eine alternative E-Mail-Adresse ein
– Das System sendet eine E-Mail an die ausgewählte Adresse
– Die Person empfängt die E-Mail auf ihrem mobilen Gerät, auf dem Mobile Access ausgeführt wird
– Die Person öffnet den Link in der E-Mail
– Sie müssen den Besuch **genehmigen**, damit die Berechtigungen funktionieren. Weitere Informationen finden Sie im Abschnitt Genehmigung und Ablehnung von Besuchen

– Das Mobilgerät funktioniert wie ein physischer Zutrittsausweis, solange die App läuft

**Vorgehensweise in den Bearbeitungsdialogen**

1. Wählen Sie die Zeile der Person aus, die mobile Anmeldedaten erhalten soll
2. Klicken Sie in der ausgewählten Zeile auf 
– Der Dialog bearbeiten wird geöffnet.
3. Klicken Sie in VisMgmt auf **Weiter**, um zum Bildschirm mit den **Besuchsdetails** zu gelangen.
4. Klicken Sie auf die Schaltfläche **HinzufügenMobile Access**
5. Wählen Sie eines der großen Symbole für die Optionen:
– **QR-Code**
oder
– **Einladungsmail**
6. Wenn Sie die Option **QR-Code** wählen:
– Das System zeigt einen QR-Code an
– Die Person scannt den QR-Code mit der Mobile Access-App auf ihrem Mobilgerät
– Sie müssen den Besuch **genehmigen**, damit die Berechtigungen funktionieren. Weitere Informationen finden Sie im Abschnitt Genehmigung und Ablehnung von Besuchen
– Das Mobilgerät funktioniert wie ein physischer Zutrittsausweis, solange die App läuft
7. Wenn Sie die Option **Einladungsmail** wählen:
– Standardmäßig wählt das Programm die E-Mail-Adresse aus, die für die ausgewählte Person definiert wurde. Geben Sie bei Bedarf eine alternative E-Mail-Adresse ein
– Das System sendet eine E-Mail an die ausgewählte Adresse
– Die Person empfängt die E-Mail auf ihrem mobilen Gerät, auf dem Mobile Access ausgeführt wird
– Die Person öffnet den Link in der E-Mail
– Sie müssen den Besuch **genehmigen**, damit die Berechtigungen funktionieren. Weitere Informationen finden Sie im Abschnitt Genehmigung und Ablehnung von Besuchen
– Das Mobilgerät funktioniert wie ein physischer Zutrittsausweis, solange die App läuft

**Siehe**

– *Installieren von Mobile Access, Seite 13*
– *Installieren der Mobile Access-Apps, Seite 23*

## 6.6 Anmeldedaten freigeben

**Aufheben der Zuweisung eines Ausweises über das Dashboard (erfordert einen Bekanntmachungsleser)**

1. Sammeln Sie den physischen Ausweis vom Ausweisinhaber ein und halten Sie sie zur Vorlage beim Bekanntmachungsleser bereit.
2. Klicken Sie in der Symbolleiste auf **Zuweisung von Ausweis aufheben**. 
3. Befolgen Sie die Anweisungen in der Popup-Benachrichtigung zur Verwendung des Bekanntmachungslesers.

**Aufheben der Zuweisung eines Ausweises im Anmeldedaten-Editor**

1. Wählen Sie auf dem Dashboard in der Haupttabelle eine Zeile aus und klicken Sie auf  , um diesen Ausweisinhaber zu bearbeiten.
2. Klicken Sie im Dialog **Bearbeitung** in der Spalte **Mitarbeiterausweise** auf  neben dem Ausweis, den Sie nicht mehr zuordnen möchten, und bestätigen Sie Ihre Aktion im Popup-Fenster.
   Wiederholen Sie diesen Schritt, bis Sie alle Ausweise, die Sie freigeben möchten, freigegeben haben.
3. Klicken Sie auf **Speichern**, um den aktuellen Besuch mit den Ausweiszuweisungen zu speichern.

## 6.7 Autorisierung von Installationstechnikern von Mobile Access Lesern

**Einführung**

Die Installationstechniker von Mobile Access Lesern verwenden die Bosch Setup Access-App zum Scannen und Konfigurieren der Leser über BLE.

Autorisierte Bediener von **Credential Management** und **Visitor Management** senden virtuelle Anmeldedaten an die Installer-App, um den Installationstechniker zu autorisieren. Dieser Abschnitt beschreibt dieses Verfahren.

**Voraussetzungen**

- Mobile Access ist auf Ihrem System installiert und konfiguriert.
  - Anweisungen dazu finden Sie im entsprechenden Abschnitt im Kapitel über die Installation in diesem Dokument.
- Vergewissern Sie sich, dass der Installationstechniker, der die Autorisierung erhält, Bosch Setup Access installiert hat und dass er auf seinem Smart Device läuft.
  - Anweisungen dazu finden Sie im entsprechenden Abschnitt im Kapitel über die Installation in diesem Dokument.

**Vorgehensweise**

1. Klicken Sie im Hauptmenü auf  , um das Dialogfeld **Onboarding von Installationstechnikern** zu öffnen.
2. Klicken Sie auf **Hinzufügen**, um einen Installationstechniker zur Liste hinzuzufügen, oder auf  , um einen vorhandenen Installationstechniker zu löschen.
- Das Popup-Fenster **Installationstechniker hinzufügen** erscheint.
3. Geben Sie im Popup-Fenster **Installationstechniker hinzufügen** die gewünschten Details ein, zum Beispiel:
- Persönliche Namen, Firmenname, E-Mail-Adresse, Telefonnummer
- Hinweis: Sie können auf  klicken, um die Details für ein ausgewähltes Installationsprogramm zu einem späteren Zeitpunkt zu ändern.
4. Klicken Sie auf **Next** (Weiter).
5. Wählen Sie eines der großen Symbole für die Optionen:

– **QR-Code**
oder
– **Einladungsmail**

6. Wenn Sie die Option **QR-Code** wählen:
– Das System zeigt einen QR-Code an
– Die Person scannt den QR-Code mit der Mobile Access-App auf ihrem Mobilgerät
– Damit ist der Registrierungsprozess des Installationstechnikers abgeschlossen
– Sie ermöglicht es dem mobilen Gerät, nach Mobile Access Lesern zu scannen und sie per BLE zu konfigurieren, solange die App läuft.
7. Wenn Sie die Option **Einladungsmail** wählen:
– Standardmäßig wählt das Programm die E-Mail-Adresse aus, die für die ausgewählte Person definiert wurde. Geben Sie bei Bedarf eine alternative E-Mail-Adresse ein
– Das System sendet eine E-Mail an die ausgewählte Adresse
– Die Person empfängt die E-Mail auf ihrem mobilen Gerät, auf dem Bosch Setup Access ausgeführt wird
– Die Person öffnet den Link in der E-Mail
– Damit ist der Registrierungsprozess des Installationstechnikers abgeschlossen
– Sie ermöglicht es dem mobilen Gerät, nach Mobile Access Lesern zu scannen und sie per BLE zu konfigurieren, solange die App läuft.

**Einladungen erneut senden**

1. Wählen Sie im Dialogfeld für das Onboarding den gewünschten Installationstechniker aus
2. Klicken Sie in der gleichen Zeile auf  , um die Autorisierung per QR-Code oder E-Mail erneut an den ausgewählten Installationstechniker zu senden.
**HINWEIS:** Sie können die Berechtigung nur erneut senden, wenn Sie vom Installationstechniker noch nicht aktiviert wurde.

### 6.7.1 Mobile Access-Leser zurücksetzen

Es kann notwendig sein, die Zutrittsleser auf die Werkseinstellungen zurückzusetzen, damit sie neu konfiguriert werden können.
Wenn ein Installationstechniker zum Beispiel Mobile Access-Leser, die bereits für einen anderen Standort konfiguriert wurden, neu konfigurieren muss, müssen diese Leser zurückgesetzt werden.
Im Handbuch des LECTUS select-Lesegeräts finden Sie eine Beschreibung, wie Sie das Lesegerät mit Hilfe der DIP-Schalter zurücksetzen können.

## 6.8 Verwendung der Mobile Access-Apps auf mobilen Geräten

**HINWEIS:** Die Verwendung der Bosch Mobile Access-Apps wird für die jeweiligen Benutzer in separaten **Kurzanleitungen** detailliert beschrieben. Diese Dokumente finden Sie im Bosch Online-Produktkatalog.

**Einführung**

Bosch bietet die folgenden Apps für Mobile Access

– Bosch Mobile Access: Eine Ausweisinhaber-App zum Speichern virtueller Anmeldedaten und zur Übertragung über Bluetooth an die Leser, die für Mobile Access konfiguriert sind. Ein solcher Leser gewährt oder verweigert dann den Zutritt, je nachdem, ob eine der gespeicherten Anmeldedaten der App für ihn gültig ist.
– Bosch Setup Access: Eine Installations-App zum Scannen und Konfigurieren der Leser über Bluetooth.

Autorisierte Bediener von Visitor Management und Credential Management können virtuelle Berechtigungen sowohl für Ausweisinhaber- als auch für Installer-Apps senden.

**Hinweis!**
WICHTIG: Betreiben Sie die Ausweisinhaber- und die Installer-App nicht gleichzeitig. Stellen Sie sicher, dass niemand die Installer-App verwendet, wenn die Ausweisinhaber-App in Gebrauch ist, und umgekehrt.

### 6.8.1 Einstellen von RSSI-Schwellenwerten in der Setup Access-App

**Einführung**

RSSI-Schwellenwert und BLE-Reichweite können im Zusammenhang mit Bosch Mobile Access als ungefähr gleichwertige Konzepte betrachtet werden.
Mobile Zutrittsgeräte senden BLE-Signale an Leser in der Nähe. Ein wichtiger Teil der Leser-Konfiguration ist die Einstellung eines RSSI-Schwellenwerts für jeden Leser. Dieser Schwellenwert ist die minimale BLE-Signalstärke, gemessen in dBm, die den Leser (R) als Aufforderung zum Betreten akzeptieren soll. Der Leser soll alle schwächeren BLE-Signale ignorieren.


Die RSSI-Werte können stark variieren, was von vielen Faktoren abhängt, z. B. von der Art des Sendegeräts, dem Batteriestand sowie dem Material und der Dicke der Wände in der Nähe. Es gibt keine lineare Beziehung zwischen dem RSSI-Wert und der Entfernung zwischen Sender und Empfänger.
Aus diesem Grund bietet die Setup Access-App ein Tool zur Messung des RSSI des Lesers anhand der aktuellen Position des mobilen Geräts. Im Folgenden wird beschrieben, wie Sie dieses Tool verwenden.
Wenn Sie einen geeigneten Schwellenwert für den BLE-Bereich gefunden haben, verwenden Sie die Setup Access-App, um diesen Wert in der Konfiguration des Lesers zu speichern.

**Vorgehensweise**

Konfigurieren Sie den **BLE-Bereich** mit einer der folgenden Optionen A oder B:
**A:** Verwenden von RSSI-Werten, die vom Leser reflektiert werden

1. Positionieren Sie sich vor dem Leser an der Stelle, an der Sie den Mobile Access-Benutzer erwarten.
2. Tippen Sie auf **Aktuelle Reichweite prüfen und nutzen**

– Eine Pop-up-Meldung wird angezeigt. Tippen Sie auf **OK**

3. Ein RSSI-Wert wird angezeigt.

– Empfohlen: Wiederholen Sie diesen Schritt einige Male von der gleichen Position aus, um einen Eindruck vom Grad der Abweichung der wahrgenommenen Signalstärke zu erhalten.

4. Wenn Sie einen geeigneten Schwellenwert gefunden haben, tippen Sie auf **Speichern**.

**B:** Manuelles Einstellen des RSSI-Schwellwerts

1. Geben Sie einen Wert für den RSSI-Schwellenwert ein.
   Siehe die nachstehende Tabelle mit typischen Schwellenwerten
2. Tippen Sie auf **Speichern**

**Typische Schwellenwerte (nur Richtwerte):**

| **Erwartete Entfernung vom mobilen Gerät zum Leser** | **Empfohlener RSSI-Schwellenwert** |
|---|---|
| Nah (5 cm – 10 cm) | -30 ... -40 dBm |
| Mittel (0,5 m – 2 m) | -50 ... -60 dBm |
| Weit (> 2 m) | -70 ... -90 dBm |

**Hinweis!**
Die RSSI-Werte können stark variieren, was von vielen Faktoren abhängt, z. B. von der Art des Sendegeräts, dem Batteriestand sowie dem Material und der Dicke der Wände in der Nähe.

# Glossar

**ACS**

Allgemeiner Begriff für ein Bosch Zutrittskontrollsystem, z. B. AMS (Access Management System) oder ACE (BIS Access Engine).

**BLE**

Bluetooth Low Energy ist eine drahtlose Netzwerktechnologie, die eine ähnliche Kommunikationsreichweite wie Bluetooth bietet, aber weniger Energie verbraucht.

**DSGVO**

Die Allgemeine Datenschutzverordnung (GDPR) ist ein Datenschutz- und Sicherheitsgesetz, das von der Europäischen Union (EU) erlassen wurde und 2018 in Kraft getreten ist. Es erlegt Organisationen überall dort Verpflichtungen auf, wo Daten von Menschen in der EU gesammelt werden.

**FQDN**

Ein voll qualifizierter Domänenname ist ein Netzwerkdomänenname, der seine absolute Position in der Hierarchie des Domänennamensystems (DNS) ausdrückt.

**Mobile Access**

Zutrittskontrolle von Personen mit Hilfe von virtuellen Anmeldedaten, die auf einem mobilen Gerät, z. B. dem Smartphone der Person, gespeichert sind.

**OSDP**

Open Supervised Device Protocol ist ein Kommunikationsstandard für die Zutrittskontrolle, der 2011 von der Security Industry Association (SIA) eingeführt wurde. Es bietet gegenüber älteren Protokollen Vorteile in den Bereichen Verschlüsselung, Biometrie, Benutzerfreundlichkeit und Interoperabilität.

**RSSI**

der Received Signal Strength Indicator (RSSI) ist die von einem Empfangsgerät wahrgenommene Signalstärke, gemessen in dBm. Mobile Geräte zeigen RSSI in der Regel in Form einer Balkengrafik an.

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


**Gebäudelösungen für ein besseres Leben**

202405132115