

# Visitor Management V5.0.1

Mit Mobile Access



# Inhaltsverzeichnis

<b>1</b>	<b>Einführung</b>	<b>5</b>
1.1	Protokoll der Funktionsänderungen	5
1.2	Über das Besuchermanagement von Bosch	5
1.3	Über Mobile Access	6
1.4	Zielgruppen	6
1.5	Verwenden dieser Dokumentation	6
<b>2</b>	<b>Systemübersicht und Topologie</b>	<b>7</b>
<b>3</b>	<b>Installieren und Deinstallieren</b>	<b>9</b>
3.1	Software- und Hardwareanforderungen	9
3.1.1	Das Haupt-Zutrittskontrollsystem	9
3.1.2	Eine Datenbankinstanz zum Hosten der Besuchermanager-Datenbank	10
3.1.3	Ein eigener Benutzer für den lokalen Datenbankzugriff	10
3.1.4	Ein dedizierter Benutzer für den Remote-Datenbankzugriff	10
3.1.5	Ein dedizierter Nutzer im Haupt-Zutrittskontrollsystem	11
3.2	Installieren des Servers	11
3.2.1	Ausführen des Setup-Programms für den Server	11
3.2.2	Appsettings JSON-Datei	12
3.3	Einrichten des VisMgmt Client-Computers	13
3.3.1	Einrichten des Add-ons für Peripheriegeräte	13
3.3.2	Zertifikate für sichere Kommunikation	14
3.3.3	Appsettings JSON-Datei	16
3.4	Überprüfen der Server-Installation	17
3.5	Installieren von Mobile Access	17
3.5.1	Überblick über Installation, Konfiguration und Verwendung	17
3.5.2	Hardware-Voraussetzungen für Mobile Access	18
3.5.3	Voraussetzungen für die Konfiguration von Mobile Access	18
3.5.4	Verfahren für die Installation an einem Ort	19
3.5.5	Verfahren für die verteilte Installation	21
3.6	Installieren der Mobile Access-Apps	24
3.7	Peripheriehardware	24
3.7.1	Registrierung von Peripheriegeräten auf dem Client-Computer	25
3.8	Reparieren von Installationen von Mobile Access	25
3.9	Deinstallieren der Software	26
<b>4</b>	<b>Konfiguration</b>	<b>27</b>
4.1	Besuchermanagement-Benutzer im ACS erstellen	27
4.2	Erstellen von Besucherberechtigungen und -profilen im ACS	28
4.3	Einrichten des Computers für das Empfangspersonal	28
4.4	Einrichten eines Kioskcomputers für Besucher	28
4.5	Anmelden für Konfigurationsaufgaben	29
4.6	Verwenden des Einstellungsmenüs zur Konfiguration	29
4.6.1	E-Mail-Vorlagen	32
4.6.2	Vorschaumodus	34
4.6.3	Dokumentenvorlagen	34
4.7	Anpassen der Benutzeroberfläche	34
4.7.1	Optionen auf sichtbar, unsichtbar und obligatorisch einstellen	34
4.7.2	Anpassen des Kioskmodus	35
4.7.3	Anpassen des Firmenlogos	35
4.8	Firewall-Einstellungen	35

4.8.1	Programme und Dienste als Firewall-Ausnahmen	36
4.9	IT-Sicherheit	38
4.9.1	Verantwortlichkeit für die Hardware	38
4.9.2	Verantwortlichkeiten für die Software	39
4.9.3	Sicherer Umgang mit mobilen Anmeldedaten	39
4.10	Sicherung des Systems	40
5	<b>Bedienung</b>	<b>41</b>
5.1	Übersicht über die Benutzerrollen	41
5.2	Verwendung des Dashboards	41
5.2.1	Die Besuche-Tabelle	41
5.2.2	Tabellenspalten und Aktionen	43
5.3	Empfangspersonal	44
5.3.1	Anmelden als Empfangspersonal	44
5.3.2	Suchen und Filtern von Besuchen	44
5.3.3	Registrierung von Besuchen	45
5.3.4	Genehmigung und Ablehnung von Besuchen	46
5.3.5	Zuweisen von physischen Berechtigungen	47
5.3.6	Zuweisen von mobilen Anmeldedaten	49
5.3.7	Anmeldedaten freigeben	51
5.3.8	Ein- und Auschecken ohne Ausweis	51
5.3.9	Zur Sperrliste hinzufügen, entfernen oder davon ausnehmen	52
5.3.10	Besucherprofile pflegen	53
5.3.11	Anzeigen von Besuchsdatensätzen	53
5.4	Gastgeber	53
5.4.1	Anmelden der Gastgeberrolle	54
5.4.2	Suchen und Filtern	54
5.4.3	Registrierung von Besuchen	55
5.4.4	Kopieren von Besuchsterminen	55
5.5	Besucher	55
5.5.1	Einführung in den Kioskmodus	55
5.5.2	Erstellen eines Besucherprofils: Selbständiges Einchecken	56
5.6	Autorisierung von Installationstechnikern von mobilen Zutrittslesern	56
5.6.1	Mobile Access-Leser zurücksetzen	58
5.7	Verwendung der Mobile Access-Apps auf mobilen Geräten	58
5.7.1	Einstellen von RSSI-Schwellenwerten in der App Setup Access	58
	<b>Glossar</b>	<b>61</b>

# 1 Einführung

## 1.1 Protokoll der Funktionsänderungen

VisMgmt Version	Hinzugefügte Funktionalitäten	AMS-Version	BIS-Version
1.0	n. z.	3.0.1	4.9
1.0.1	Ein- und Auschecken von Besuchern ohne Ausweis Suche nach der Anzahl der freien Ausweise Unterscheidung zwischen verschiedenen Gastgebern mit demselben Namen (Leistungsverbesserung) Feinere Granularität der Dialogaktualisierung	4.0	4.9.1
5.0	Unterstützung für E-Mail-Server Unterstützung für HID OMNIKEY-Leser Anpassbare Firmenlogos	5.0	k. A.
5.0.1	Unterstützung für Mobiler Zutritt Zuweisen von mobilen Anmeldedaten	5.0.1	k. A.

## 1.2 Über das Besuchermanagement von Bosch

Visitor Management, im Folgenden bezeichnet als VisMgmt, ist ein browserbasiertes Softwaretool, das mit den Zutrittskontrollsystemen von Bosch zusammenarbeitet. Er verwaltet die Besuche an Standorten mit Zutrittskontrolle. Das beinhaltet auch die Zeitplanung der Besuche, berufliche Informationen zu den Besuchern samt zugehöriger Dokumente oder Verträge sowie die Zuweisung von temporären Zugangsberechtigungen.

Die Benutzeroberfläche ist anpassbar und jeder Anwender kann spontan und ohne sich abzumelden die Sprache wechseln.

Die hauptsächlichen Nutzer und ihre jeweiligen Anwendungsfälle sind:

Art der Benutzer	Anwendungsfälle
Empfangspersonal	Registrierung neuer Besuche und Besucher Genehmigung und Ablehnung von Besuchen Besucher sperren Besucherausweise zuweisen und deren Gültigkeit aufheben Verwalten von zugehörigen Dokumenten Überwachung der Anzahl der Besucher am Standort
Visitor (Besucher)	Selbständige oder Vorabregistrierung Erstellen und pflegen eines Besucherprofils Unterzeichnen von Dokumenten
Gastgeber	Verwalten von Zeitplänen und Listen von Besuchen und Besuchern Vorregistrierung von Besuchen
Administrator	Vornahme globaler Einstellungen

Art der Benutzer	Anwendungsfälle
	Anpassen des Verhaltens des Tools und seiner Benutzeroberfläche Plus: Alle Anwendungsfälle des Empfangsmitarbeiters

### 1.3 Über Mobile Access

Mobiler Zutritt ist die App zur Verifizierung der Zutrittskontrolle von Personen mithilfe virtueller Berechtigungen, die auf einem mobilen Gerät, z. B. dem Smartphone der Person, gespeichert sind. Die virtuellen Berechtigungen werden im primären Zutrittskontrollsystem (ACS) verwaltet.

- Die Bediener des ACS generieren diese virtuellen Berechtigungen, weisen sie zu und senden sie über eine entsprechende Webanwendung wie Credential Management oder Visitor Management an Personen.
- Die Inhaber mobiler Berechtigungen bedienen die Zutrittskontrollleser über Bluetooth von einer Mobile Access-App auf ihren mobilen Geräten aus.
- Installationstechniker von mobilen Zutrittssystemen konfigurieren Zutrittskontrollleser über Bluetooth von einer speziellen Setup-App auf Ihren mobilen Geräten.
- Das System speichert keine persönlichen Daten auf mobilen Geräten.

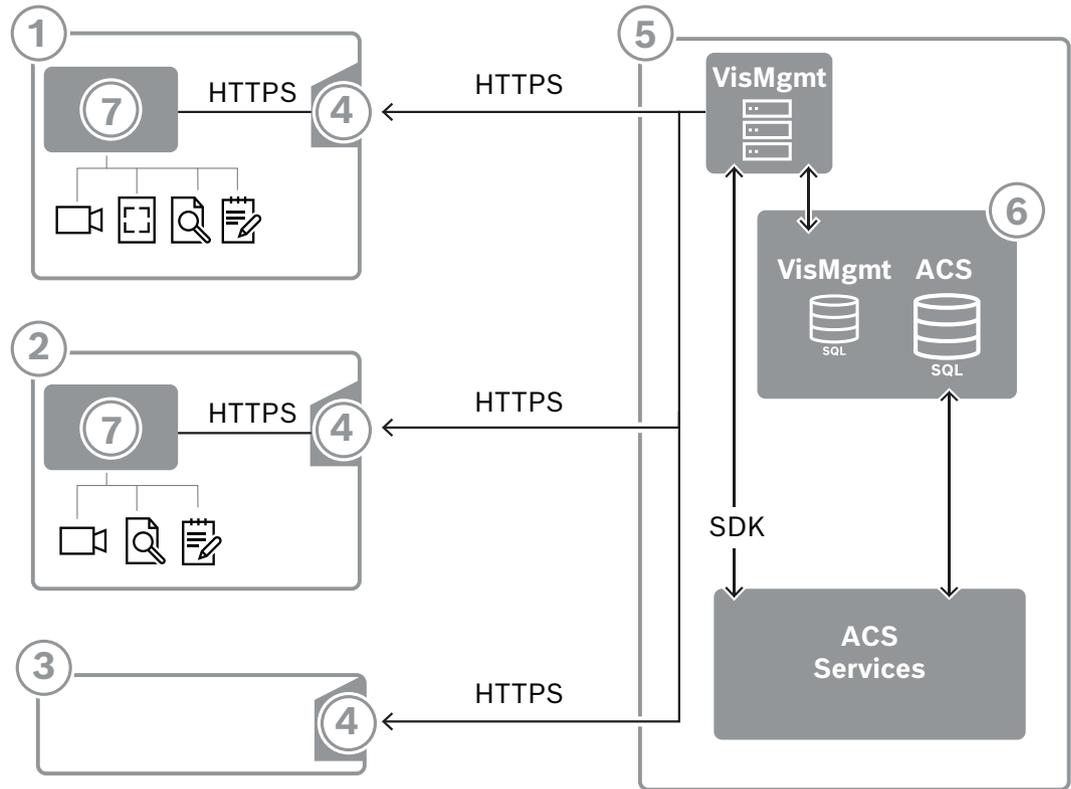
### 1.4 Zielgruppen

- Einrichter und Administratoren von VisMgmt
- Die Arten von Hauptbenutzern des VisMgmt

### 1.5 Verwenden dieser Dokumentation

- Verwenden Sie die **Suchfunktion** Ihrer Hilfeanzeige, um relevante Inhalte zu finden.
- Die Abschnitte zur **Systemübersicht, Installation** und **Konfiguration** sind hauptsächlich für Systemadministratoren von Interesse.
- Die Abschnitte zum **Betrieb** sind hauptsächlich für Systembenutzer relevant.

## 2 Systemübersicht und Topologie



Beschriftung	Beschreibung
1	Die Arbeitsstation des <b>Empfangsmitarbeiters</b> . Diese Arbeitsstation kann mit optionaler Peripherie-Hardware ausgestattet werden, z. B. mit einem Einschreibegerät, einer Webkamera und Scannern für Unterschriften und Dokumente.
2	Die <b>Besucherkiosk-Bedienstation</b> mit einem Browser im Kioskmodus. Diese Arbeitsstation kann mit optionaler Peripherie-Hardware ausgestattet werden, z. B. mit einer Webkamera und Scannern für Unterschriften und Dokumente.
3	Die <b>Gastgeber</b> -Arbeitsstation d. h. die Arbeitsstation des Mitarbeiters, der den Besucher empfängt.
4	Unterstützte Browser mit der VisMgmt Website
5	Der ACS Server (BIS oder AMS)
6	Die Datenbankinstanz des ACS-Servers (Diese kann sich auf einem separaten Computer befinden).
7	Das optionale <b>Bosch Peripheriegeräte-Add-on</b> , das die Kommunikation zwischen dem Browser und der Peripherie-Hardware verwaltet.

Bei der empfohlenen Systemtopologie befindet sich der VisMgmt Server auf demselben Computer wie der des Haupt-Zutrittskontrollsystems und seine Datenbank auf derselben Datenbankinstanz.

Das Bosch Peripheriegeräte-Add-on wird nur auf den Arbeitsstationen installiert, die Zugriff auf Peripheriegeräte benötigen.

Die Gastgeber-Bedienstation erfordert in der Regel nur einen Browser-Zugriff auf den VisMgmt Server.

# 3 Installieren und Deinstallieren

## 3.1 Software- und Hardwareanforderungen

Sie installieren den VisMgmt Server auf demselben Computer wie das Haupt-Zutrittskontrollsystem. Es gelten dieselben Software- und Hardwareanforderungen.

### Serveranforderungen

Betriebssysteme	Windows 10, Windows Server 2016, Windows Server 2019
Database Management Systeme	MS SQL Server 2019 and later Verwenden Sie immer dieselbe Datenbankinstanz wie die des ACS (des primären Zutrittskontrollsystems)
Unterstützte Browser	Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium based) Verwenden Sie die neueste Version des Browsers für Ihr Windows-Betriebssystem.
Minimale Monitoraufösung (zur Verwendung der Nutzeroberfläche der Anwendung)	Full HD 1920x1080

### Anforderungen für das Bosch Peripheriegeräte-Add-on

Das **Bosch Peripheriegeräte-Add-on** ist das Programm, das die elektronische Kommunikation zwischen dem Browser und Peripheriegeräten wie Einschreibeleser, Webkamera, Unterschriftenscanner und Dokumentenscanner übernimmt.

Der Client-Computer ist der Computer, der physisch mit der Peripherie-Hardware verbunden ist. Auf ihm läuft auch der Browser, der die Verbindung zum VisMgmt-Server herstellt.

Auch wenn die Peripheriegeräte für die Installation nicht strikt erforderlich sind, werden Sie dennoch dringend empfohlen, da sie die Effizienz des Registrierungsprozesses für Besucher erheblich erhöhen.

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

### 3.1.1 Das Haupt-Zutrittskontrollsystem

#### Ohne Mobiler Zutritt

Wenn Mobiler Zutritt nicht erforderlich ist, funktioniert VisMgmt Version 5.0.1 mit den folgenden Zutrittskontrollsystemen von Bosch:

- Access Management System (AMS) Versionen 5.0 und höher

#### Mit Mobiler Zutritt

Wenn Mobiler Zutritt erforderlich ist, funktioniert VisMgmt Version 5.0.1 mit den folgenden Zutrittskontrollsystemen von Bosch:

- Access Management System (AMS) Versions 5.0.1 (mit einer Mobiler Zutritt-Erweiterung) und höher

Vervollständigen und überprüfen Sie die Installation des Haupt-Zutrittskontrollsystems gemäß der zugehörigen Installationsanleitung, bevor Sie mit der Installation von VisMgmt fortfahren.

### 3.1.2 Eine Datenbankinstanz zum Hosten der Besuchermanager-Datenbank

Bei der Installation des Haupt-Zutrittskontrollsystems wird eine Datenbankinstanz erstellt, die Sie als Gastgeber für die VisMgmt-Datenbank, *dbVisitorManagement*, verwenden können. Der Standardname dieser Instanz variiert je nach ACS

- Für AMS lautet der Name *ACE*
- Für BIS ACE lautet der Name *BIS\_ACE*

### 3.1.3 Ein eigener Benutzer für den lokalen Datenbankzugriff

Der Benutzer *VMUser* greift im Namen der VisMgmt-Anwendung auf die Besuchermanager-Datenbank zu.

Das VisMgmt-Server-Installationsprogramm erstellt den Windows-Benutzer *VMUser* auf dem VisMgmt-Server.

### 3.1.4 Ein dedizierter Benutzer für den Remote-Datenbankzugriff

Wenn VisMgmt eine Datenbank auf einem entfernten Datenbankserver verwenden soll, erstellen und konfigurieren Sie den *VMUser*-Benutzer in Windows und auf dem SQL-Server wie unten beschrieben.

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

1. Legen Sie auf dem entfernten Datenbankserver einen Windows-Benutzer mit den folgenden Einstellungen an:
  - **Benutzername** (Groß- und Kleinschreibung wird berücksichtigt): *VMUser*
  - **Kennwort**: Legen Sie das Kennwort entsprechend den Sicherheitsrichtlinien fest, die für alle Computer gelten. Notieren Sie sie sorgfältig, da sie für die VisMgmt-Installation benötigt wird.
  - **Mitglied von Gruppe**: *Administrators*
  - **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 *VMUser* als Login hinzu, um den SQL-Server fernzusteuern)

1. SQL Management Studio öffnen
2. Mit der Remote-SQL-Instanz verbinden
3. Zu **Sicherheit** > **Login** navigieren
4. Hinzufügen des *VMUser*-Benutzers mit der Serverrolle *sysadmin*

Wenn Sie später die VisMgmt-Installation auf dem VisMgmt-Server ausführen, wählen Sie die Option für den **Remote-Datenbankserver**-Computer und geben das Kennwort ein, das Sie oben für *VMUser* definiert haben.

### 3.1.5 Ein dedizierter Nutzer im Haupt-Zutrittskontrollsystem

1. Erstellen Sie im Haupt-Zutrittskontrollsystem einen Benutzer mit **unbegrenzter API-Nutzung**. Ausführliche Anweisungen finden Sie im Kapitel **Benutzer-/Bedienerprofile zuweisen** des Bedienungshandbuchs zum Haupt-Zutrittskontrollsystem.
2. Achten Sie sorgfältig auf den Benutzernamen und das Passwort, da diese vom VisMgmt Installationsassistenten benötigt werden.

## 3.2 Installieren des Servers

Starten Sie das Setup-Programm erst, wenn alle Softwareanforderungen erfüllt sind.

### 3.2.1 Ausführen des Setup-Programms für den Server

1. Führen Sie auf dem gewünschten VisMgmt Server *BoschVisitorManagementServer.exe* als Administrator aus.
2. Klicken Sie auf **Weiter**, um das Standard-Installationspaket zu akzeptieren.
3. Wenn Sie mit dem Endbenutzer-Lizenzvertrag (EULA) einverstanden sind, akzeptieren Sie ihn und klicken Sie auf **Weiter**.
4. Wählen Sie den Zielordner für die Installation aus. Es wird empfohlen, den Standardordner zu verwenden.
  - Auf dem Bildschirm **SQL-Serverkonfiguration**
5. Wählen Sie aus, ob Sie die Datenbank auf der lokalen SQL-Server-Instanz erstellen möchten, die sich auf der Datenbankinstanz auf dem VisMgmt Server befindet, oder auf einem Remote-Datenbank-Servercomputer.
  - **Hinweis:** Wenn Sie einen Remote-Datenbankserver auswählen, werden Sie vom Setup-Programm aufgefordert, das Passwort zu *VMUser* einzugeben, dem Administratorbenutzer, den Sie auf dem Remote-Datenbankserver eingerichtet haben (siehe Abschnitt „Softwarevoraussetzungen“).
6. Überprüfen Sie die Werte für die folgenden Parameter und ändern Sie sie gegebenenfalls:

<b>SQL-Server</b>	Name des Datenbank-Servercomputers
<b>SQL-Instanz</b>	Der Name der Instanz der ACS-Hauptdatenbank. Hier wird die Besucherdatenbank erstellt. Für AMS lautet der Name <i>ACE</i> Für BIS ACE lautet der Name <i>BIS_ACE</i>
<b>SQL-Benutzername</b>	Üblicherweise der Name eines Administratorbenutzers der Instanz <i>sa</i>
<b>SQL-Passwort</b>	Das Passwort dieses Administratorbenutzers.

7. Klicken Sie auf **Verbindung testen**, um zu prüfen, ob die Datenbankinstanz mit den eingegebenen Parameterwerten erreicht werden kann. Überprüfen Sie die Parameter erneut, falls der Test fehlschlägt.
8. Klicken Sie zum Fortfahren auf **Weiter**
  - Auf dem Bildschirm **ACS-Zutrittskonfiguration** (ACS verweist auf das Haupt-Zutrittskontrollsystem, AMS oder ACE)
9. Geben Sie Werte für die folgenden Parameter ein:

<b>ACS-Hostname</b>	Der Name des Computers, auf dem ACS ausgeführt wird
<b>ACS-Benutzername</b>	Der Name des dedizierten Benutzers des ACS mit unbegrenzter API-Verwendung. Siehe Abschnitt „Softwareanforderungen“.

<b>ACS-Passwort</b>	Das Passwort dieses dedizierten ACS-Benutzers.
---------------------	--

10. Klicken Sie zum Fortfahren auf **Weiter**
  - Auf dem Bildschirm **Serverkonfiguration**
11. Geben Sie den URI des entsprechenden ACS-Identitätsservers ein:
  - AMS: `HTTPS://<Name des ACS-Servers>:44333`
  - BIS: `HTTPS://<Name des ACS-Servers>/BisIdServer`
12. Klicken Sie auf **Verbindung testen**, um zu prüfen, ob der Identity Server erreichbar ist.
13. Klicken Sie **Weiter**, um auf den Übersichtsbildschirm zu gelangen und klicken Sie anschließend auf **Installieren**, um die Installation des VisMgmt Servers zu starten.
14. Fahren Sie den Computer nach der Installation neu hoch.

### 3.2.2

#### Appsettings JSON-Datei

Eine Reihe von Konfigurationsparametern für den VisMgmt Server werden in der folgenden `.JSON`-Datei gespeichert:

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

Es ist im Allgemeinen nicht erforderlich, die Standardwerte zu ändern. Aber es kann vorteilhaft sein, die folgenden Parameter im Abschnitt **Einstellungen** der Datei anzupassen. Wenn Sie Parameter anpassen, erstellen Sie zunächst eine Sicherungskopie der Datei. Die Sicherungskopie hilft Ihnen, Änderungen schnell rückgängig zu machen, falls diese eine Fehlfunktion verursachen.

Speichern Sie Ihre Änderungen und starten Sie den VisMgmt Windows-Dienst neu, um die geänderten Parameter anzuwenden. Der Name des Diensts lautet

```
Bosch Visitor Management.
```

Parametername	Standardwert	Beschreibung
<code>PageSizeNumberOfVisit</code>	20	Die maximale Anzahl an Besuchsdatensätzen, die auf dem Bildschirm gleichzeitig angezeigt werden. Wenn der Benutzer einen Bildlauf durchführt, wird jede neue Seite mit dieser Anzahl von Datensätzen gefüllt, die aus der Datenbank geladen werden.
<code>MaximumUploadFileSizeBytes</code>	31457289	Die maximale Anzahl von Bytes, die eine hochgeladene Datei enthalten kann.
<code>StartoverTimeoutAskSeconds</code>	300	Die Anwendung wartet diese Anzahl von Sekunden, wenn der Benutzer die Eingabe von Anmeldeinformationen unterbricht. Dann fordert sie diesen zur Eingabe auf.

Parametername	Standardwert	Beschreibung
<i>StartoverTimeoutResetSeconds</i>	60	Nach der Aufforderung wartet die Anwendung diese Anzahl von Sekunden, bevor der Anmeldebildschirm zurückgesetzt wird.

### 3.3 Einrichten des VisMgmt Client-Computers

Das Bosch Peripheriegeräte-Add-on kann auf dem Server-Computer installiert werden, wird aber normalerweise auf einem Client-Computer im selben Netzwerk installiert. Kopieren Sie in diesem Fall das HTTPS-Zertifikat vom ACS-Server, und installieren Sie es ebenfalls auf dem Client-Computer. Ziehen Sie dazu die untenstehenden *Zertifikate für sichere Kommunikation, Seite 14* zu Rate.

Das Bosch Peripheriegeräte-Add-on ist die Verbindungssoftware für Geräte wie Einschreibeleser und Scanner. Wenn solche Geräte nicht erforderlich sind, z. B. für den Gastgeber-Benutzer, dann reicht der Browser-Zugang aus, um sich anzumelden und die VisMgmt-Anwendung auszuführen.

Die folgenden Registrierungsleser und Ausweisformate werden unterstützt.

	MIFARE DESfire Ev1 Bosch Code	MIFARE DESfire Ev1 CSN	MIFARE Classic CSN	iCLAS S 26 Bit	iCLAS S 35 Bit	iCLAS S 37 Bit	iCLAS S 48 Bit	HID Prox 26 Bit	EM 26 Bit
LECTUS-Registrierung ARD-EDMCV002-USB	X								
OMNIKEY 5427 CK		X	X	X	X	X	X	X	X

**Siehe**

- *Zertifikate für sichere Kommunikation, Seite 14*

#### 3.3.1 Einrichten des Add-ons für Peripheriegeräte

Das Add-on für Peripheriegeräte ist nur auf diesen 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. Fahren Sie den Computer nach der Installation neu hoch.

### 3.3.2

#### 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*

#### Übersicht der Zertifikatsübertragungen

Auf → Von ↓	ACS	MA Mobile Access Backend	DB Daten- bank	S Setup-App	M App für den Zutritt von Ausweisinhab ern	R Leser
<b>ACS</b>	/	Übertragen durch den Einrichtungs	/	/	/	/

		assistenten (mit Hilfe des Cert- Tools)				
<b>MA</b> Mobile Access Backend	Übertragen durch den MA- Einrichtungs- assistenten	/	/	Übertragen per QR-Code Registrierung	Übertragen per QR-Code Registrierung	/
				Aktualisierung per Push- Benachrichti- gung	Aktualisierung per Push- Benachrichtig- ung	
<b>DB</b> Datenbank	/	/	/	/	/	/
<b>S</b> Setup -App	/	Übertragen durch QR- Code Registrierung	/	/	/	/
<b>M</b> App für den Zutritt von Ausweisin- habern	/	Übertragen durch QR- Code Registrierung	/	/	/	/

### 3.3.2.1

#### 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.

### **3.3.2.2 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.

### **3.3.3 Appsettings JSON-Datei**

Eine Reihe von Konfigurationsparametern für den VisMgmt-Client-Computer sind in der folgenden `.JSON`-Datei gespeichert:

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

Es ist im Allgemeinen nicht erforderlich, die Standardwerte zu ändern. Aber es kann vorteilhaft sein, die folgenden Parameter im Abschnitt **AppSettings** der Datei anzupassen.

Speichern Sie Ihre Änderungen und starten Sie den VisMgmt Windows-Dienst neu, um die geänderten Parameter anzuwenden. Der Name des Diensts lautet

```
Bosch Ace Visitor Management Client
```

Parametername	Beispiel	Beschreibung
<i>CorseOrigins</i>	<code>"https://my-vm-server:5706"</code>	Die Adresse und die Portnummer des Besuchsmanagementservers.
<i>CardReaderPort</i>	<code>"com3"</code>	Die Nummer des COM-Ports, an den ein LECTUS-Anmeldeleser angeschlossen ist. Bei HID OMNIKEY-Lesern kann dieser Parameter leer sein.

### 3.4 Überprüfen der Server-Installation

Öffnen Sie auf einem Computer im gleichen Netzwerk mit einem der unterstützten Browser die folgende URL:

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

Wenn der Server ausgeführt wird, wird die Anmeldeseite der Anwendung angezeigt.

### 3.5 Installieren von Mobile Access

#### Einführung

Der Bosch Mobiler Zutritt Backend-Dienst bietet mobile Zutrittsfunktionen für Credential Management und Visitor Management.

**HINWEIS:** Wenn Sie CredMgmt und VisMgmt verwenden, müssen Sie Mobiler Zutritt 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 entfernte Datenbank verwendet.

#### Erreichbarkeit des Mobile Access Backend-Dienstes

Der Mobile Access Backend Service 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 Backend-Dienst auf einem weithin verfügbaren „Cloud“-Server ausführen.

#### 3.5.1 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 Mobiler Zutritt definiert.

##### Einrichten von Mobiler Zutritt

1. Ein Systemadministrator installiert eine oder beide der Webanwendungen, die Mobiler Zutritt verwenden, entweder Credential Management oder Visitor Management auf dem ACS.
2. Ein Systemadministrator installiert das Mobiler Zutritt-+Backend.

3. Ein System Administrator aktiviert Mobiler Zutritt in den installierten Web-Anwendungen.

#### **Einrichten des Lesers**

1. Ein Systemadministrator erstellt in der Anwendung CredMgmt einen Installationstechniker (eine Person, die berechtigt ist, Mobiler Zutritt-Leser zu konfigurieren).
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 Mobiler Zutritt zu konfigurieren.
5. Der Installationstechniker konfiguriert die Leser mithilfe der Installer-App.

#### **Verwenden von Mobiler Zutritt**

1. Ausweisinhaber, die zur Nutzung des mobilen Zutritts berechtigt sind, laden die Ausweisinhaber-App („Mobile Access“) über den üblichen öffentlichen App Store des Geräts auf ihr Mobilgerät 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.

### **3.5.2**

#### **Hardware-Voraussetzungen für Mobile Access**

Mobile Access erfordert Zutrittsleser mit einem BLE-Modul. Die folgenden Bosch-Lesegeräte 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 bedeutet Eignung für Mobile Access

### **3.5.3**

#### **Voraussetzungen für die Konfiguration von Mobile Access**

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

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

**3.5.4**

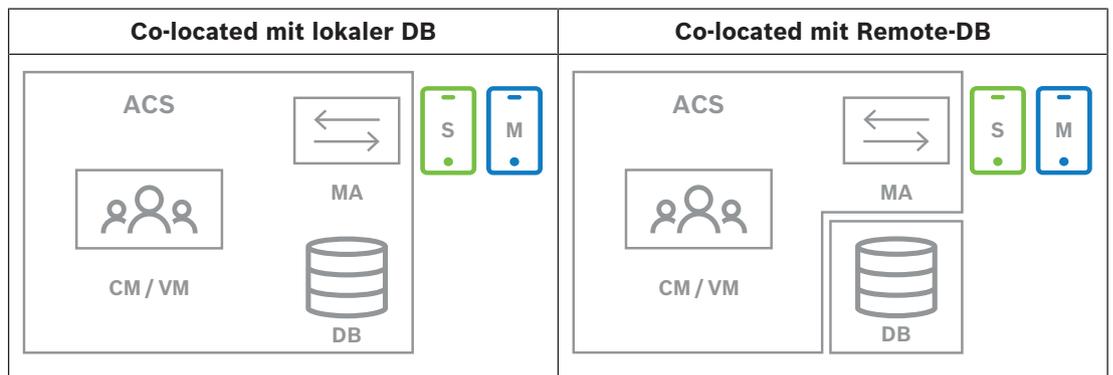
**Verfahren für die Installation an einem Ort**

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

**Verteilte Installation** bedeutet, dass der Mobile Access Backend-Dienst auf einem anderen Server, z. B. einem „Cloud Server“, läuft.

Für die Option der verteilten Installation lesen Sie bitte den nächsten Abschnitt

**Vorgehensweise bei der verteilten Installation.**



Taste	Bedeutung
ACS	Das primäre Zutrittskontrollsystem, AMS oder BIS-ACE

Taste	Bedeutung
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 Ausweise.

### Vorgehensweise

1. Führen Sie auf dem ACS-Server, der bei „co-located“ 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-Servere** 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 **Serverkonfiguration**
  - Der Standard-Identitätsserver (voreingestellt) ist der primäre ACS-Server mit Port 44333  
`https://<NameOfACSserver>:44333`
  - Klicken Sie auf **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 **Bosch Mobile 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.

### 3.5.5

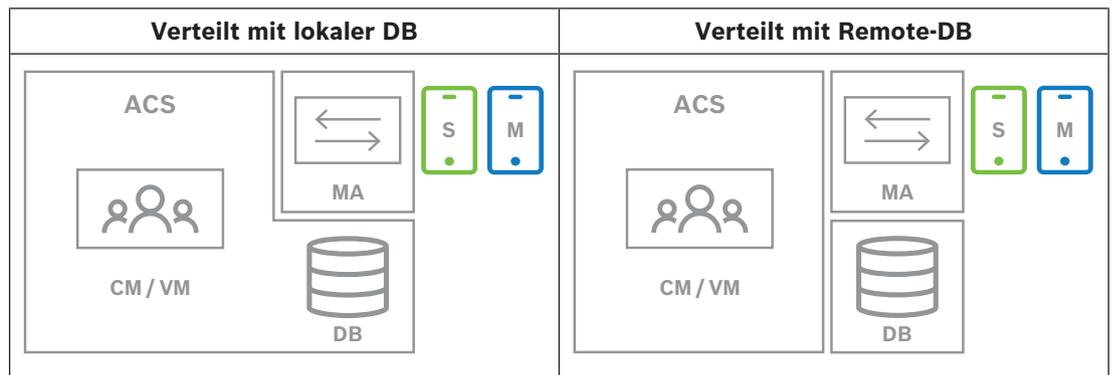
#### Verfahren für die verteilte Installation

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

**Verteilte Installation** bedeutet, dass der Mobile Access Backend-Dienst auf einem anderen Server, z. B. einem „Cloud Server“, läuft.

Für die Option der gleichzeitigen Installation lesen Sie bitte den vorherigen Abschnitt

#### Vorgehensweise bei der gleichzeitigen Installation.



Taste	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 Ausweise.

**Vorgehensweise**

1. Führen Sie auf dem Mobiler Zutritt-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 **Mobiler Zutritt-Backend** , und klicken Sie auf **Weiter**
  - Hinweis: Die **ACS**-Option wird später in diesem Verfahren verwendet, wenn wir den mobilen Zutritt auf dem ACS-Server installieren.
4. Überprüfen Sie auf dem Bildschirm **Komponenten**, ob die Option **Bosch Mobiler Zutritt** 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 den mobilen Zutritt konfigurieren, damit er später mit dem Backend für den mobilen Zutritt 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 **Serverkonfiguration**
  - Der Standard-Identitätsserver (voreingestellt) ist der primäre ACS-Server mit Port `44333`  
`https://<NameOfACSserver>:44333`
  - Klicken Sie auf **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 **Bosch Mobile 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.

## 3.6 Installieren der Mobile Access-Apps

### Einführung

Bosch bietet die folgenden Apps für den mobilen Zutritt

- Bosch Mobile Access: Eine Ausweisinhaber-App zum Speichern virtueller Anmeldedaten und zur Übertragung über Bluetooth an die Leser, die für den mobilen Zutritt konfiguriert sind. Ein solcher Leser gewährt oder verweigert dann den Zutritt, je nachdem, ob einer der gespeicherten Berechtigungen in 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 den mobilen Zutritt von Bosch 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

## 3.7 Peripheriehardware

Die folgenden Peripherie-USB-Geräte wurden getestet und zum Zeitpunkt der Erstellung dieses Dokuments für die Verwendung mit VisMgmt und CredMgmt genehmigt. Eine ständig aktualisierte Liste kompatibler Geräte finden Sie im Datenblatt des Haupt-Zutrittskontrollsystems.

Ausweis-Bekanntmachungsleser	LECTUS enroll ARD-EDMCV002-USB, HID OMNIKEY 5427 CK
Scanner für Ausweisdokumente	ARH Combo, ARH Osmond
Unterschriftenscanner	signotec LITE, signotec Omega

Folgen Sie den Anweisungen des Herstellers, um diese Geräte mit Ihren Client-Computern zu verbinden.

**Bekanntmachungsleser**

Die folgenden Registrierungsleser und Ausweisformate werden unterstützt.

	MIFARE DESfire Ev1 Bosch Code	MIFARE DESfire Ev1 CSN	MIFARE Classic CSN	iCLAS S 26 Bit	iCLAS S 35 Bit	iCLAS S 37 Bit	iCLAS S 48 Bit	HID Prox 26 Bit	EM 26 Bit
LECTUS- Registrierung ARD- EDMCV0 02-USB	X								
OMNIKEY 5427 CK		X	X	X	X	X	X	X	X

**3.7.1**

**Registrierung von Peripheriegeräten auf dem Client-Computer**

Um Peripheriegeräte auf dem VisMgmt-Client-Computer zu registrieren, führen Sie das Bosch Peripheriegeräte-Installationsprogramm, *BoschPeripheralDeviceAddon.exe*, auf dem Client aus. Anweisungen finden Sie unter *Einrichten des Add-ons für Peripheriegeräte, Seite 13*.

**Siehe**

- *Einrichten des Add-ons für Peripheriegeräte, Seite 13*

**3.8**

**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 nach Abschluss des Setup-Programms eine neue Anmeldesitzung bei jeder Webanwendung, die Mobile Access verwendet (CredMgmt oder VisMgmt oder beide).
  - 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.

## 3.9 Deinstallieren der Software

So deinstallieren Sie die Software vom Server oder Client:

1. Starten Sie mit Windows-Administratorrechten das Windows-Programm **Programm hinzufügen oder entfernen**.
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 Änderung in der Windows-Registrierung durchgeführt wurden.

## 4 Konfiguration

### 4.1 Besuchermanagement-Benutzer im ACS erstellen

#### Einführung

Jeder Administrator, Empfangsmitarbeiter oder Benutzer in der Rolle des Gastgebers in VisMgmt muss ein Ausweisinhaber mit einer separaten Operator-Definition im ACS, dem Haupt-Zutrittskontrollsystem, sein.

Diese Bediener-Definitionen umfassen spezielle VisMgmt-Rechte in Form von

**Benutzerprofilen**. Detaillierte Informationen und Anleitungen zu den **Benutzerprofilen** finden Sie in der Online-Hilfe in Ihrem ACS.

- Sie müssen für jeden Ausweisinhaber, der im Besuchermanagement arbeitet, einen separaten Bediener definieren. Einem Bediener können nicht mehrere Ausweisinhaber zugewiesen werden.



#### Hinweis!

IT-Sicherheit und Benutzerkonten

In Übereinstimmung mit den besten Praktiken für die IT-Sicherheit empfehlen wir, dass jeder Empfangsmitarbeiter, der Gastgeber und der Administrator unter seinem eigenen Windows-Konto arbeiten.

#### Erstellen von Benutzerprofilen für die Besucherverwaltung

1. Melden Sie sich mit Administratorrechten im Haupt-Zutrittskontrollsystem an.
2. Erstellen Sie ein oder mehrere Benutzerprofile (Bediener) für VisMgmt Benutzer.  
Dialogpfad:
3. Weisen Sie diesen Profilen eines der folgenden Benutzerrechte zu.
  - Administrator: *Visitor Management > Administrator*
  - Gastgeber: *Visitor Management > Host*
  - Empfangspersonal: *Visitor Management > Receptionist*

Wenn Sie die Benutzerprofile erstellt haben, die Sie für die verschiedenen VisMgmt-Rollen (Administrator, Empfangsmitarbeiter, Gastgeber) benötigen, können Sie jedes dieser Profile mehreren Bedienern zuweisen.

#### Zuweisen von Benutzerprofilen zu ACS-Bedienern und Ausweisinhabern

Dialogpfad:

1. Fügen Sie einen neuen Bedientyp hinzu (klicken Sie – je nach ACS – auf  oder ) , und geben Sie ihm einen Namen, der eindeutig im Zusammenhang mit einer der VisMgmt-Rollen (Administrator, Gastgeber oder Empfangsmitarbeiter) steht.
2. Wählen Sie aus der Liste „Autorisierung“ auf der Registerkarte **Allgemeine Bedienerereinstellungen** die Option *Operator ACE* aus.
3. Verwenden Sie auf der Registerkarte **ACE-Bedienerereinstellungen** die Pfeil-Schaltflächen, um das zuvor erstellte **ACE-Benutzerprofil** zuzuweisen.  
Heben Sie die Zuweisung des Standardprofils *UP-Administrator* auf (außer in dem unwahrscheinlichen Fall, dass der Ausweisinhaber allumfassende Administratorrechte im ACS benötigt).
4. Bleiben Sie auf der Registerkarte **ACE-Bedienerereinstellungen**, und lokalisieren Sie im Bereich **Person zuweisen** den Ausweisinhaber im System, dem die VisMgmt-Rolle zugewiesen werden soll.

5. Klicken Sie auf **Person zuweisen**, um die Zuweisung zum ausgewählten Ausweisinhaber durchzuführen.
  - Sie müssen für jeden Ausweisinhaber, der im Besuchermanagement arbeitet, einen separaten Bediener definieren. Einem Bediener können nicht mehrere Ausweisinhaber zugewiesen werden.

## 4.2 Erstellen von Besucherberechtigungen und -profilen im ACS

### Einführung

Die Empfangsmitarbeiter oder Administratoren des VisMgmt Systems wählen für jeden neuen Besucher einen **Visitor type** (Besuchertyp) aus. Dieser Besuchertyp basiert auf einem vordefinierten **Person type** (Personentyp) mit dem Namen **Visitor** (Besucher) im Haupt-Zutrittskontrollsystem (Access Control System, ACS) oder auf einem Untertyp von **Visitor** (Besucher), der von den ACS-Administratoren erstellt wurde.

Diese Administratoren müssen im ACS auch den Personentyp **Visitor** (Besucher) und dessen Untertypen mit Zutrittsprofilen konfigurieren. Die Zutrittsprofile ermöglichen diesen Personentypen die Bedienung physischer Türen am Standort.

## 4.3 Einrichten des Computers für das Empfangspersonal

Auf dem Computer der Empfangsdame läuft das **Bosch Peripheriegeräte-Add-on**, das physische Verbindungen zu Peripheriegeräten für das Lesen von Ausweisen, das Scannen von Ausweisdokumenten und das Scannen von Unterschriften ermöglicht.

Schließen Sie alle erforderlichen Peripheriegeräte an, bevor Sie die Client-Software installieren.

Stellen Sie sicher, dass der Computer und seine Peripheriegeräte ausreichend vor unberechtigtem Zugriff geschützt sind.

## 4.4 Einrichten eines Kioskcomputers für Besucher

### Einführung

In der Regel registrieren Besucher Ihre Besuche oder erstellen Ihre eigenen Profile selbst an einem Computer, der im Empfangsbereich des Standortes frei zugänglich ist. Aus Sicherheitsgründen wird der Webbrowser des Computers im Kioskmodus ausgeführt, sodass nur der Zugriff auf VisMgmt möglich ist und nicht auf verschiedene Registerkarten, Browsereinstellungen oder das Betriebssystem des Computers. Alle unterstützten Browser bieten den Kioskmodus an, aber seine genaue Konfiguration hängt vom jeweiligen Browser ab. Auf dem Kioskcomputer läuft das **Bosch Peripheriegeräte-Add-on**, das physische Verbindungen zu Peripheriegeräten zum Scannen von Ausweisdokumenten und Unterschriften ermöglicht.

- Die URL für den Kioskmodus ist `https://<My_VisMgmt_server>:5706`

### Konfigurieren von Browsern für den Kioskmodus

Die folgenden Links beschreiben die Konfiguration des Kioskmodus für Browser, die von VisMgmt unterstützt werden

	Anleitung zum Einrichten des Kioskmodus
<b>Chrome</b>	<a href="https://support.google.com/chrome/a/answer/9273974">https://support.google.com/chrome/a/answer/9273974</a>
<b>Firefox</b>	<a href="https://support.mozilla.org/en-US/kb/firefox-enterprise-kiosk-mode">https://support.mozilla.org/en-US/kb/firefox-enterprise-kiosk-mode</a>
<b>Edge</b>	<a href="https://docs.microsoft.com/en-us/deployedge/microsoft-edge-configure-kiosk-mode">https://docs.microsoft.com/en-us/deployedge/microsoft-edge-configure-kiosk-mode</a>



**Hinweis!**

Deaktivieren Sie aus Sicherheitsgründen stets die Browseroption zum automatischen Speichern von Passwörtern.

## 4.5 Anmelden für Konfigurationsaufgaben

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

1. Geben Sie im Browser die HTTPS-Adresse des VisMgmt Servers ein, gefolgt von einem Doppelpunkt und der Portnummer (standardmäßig 5706)

```
https://<My_VisMgmt_server>:5706/main
```

. Anschließend wird der Bildschirm **Login** (Anmeldung) angezeigt.

2. Melden Sie sich als VisMgmt **Administratorbenutzer** an.



3. Klicken Sie , um das Menü **Einstellungen** zu öffnen.

## 4.6 Verwenden des Einstellungsmenüs zur Konfiguration

Das Menü **Einstellungen** enthält Unterabschnitte, mit denen Sie die folgenden Konfigurationsschritte ausführen können:

<b>Allgemeine Einstellungen</b>	<ul style="list-style-type: none"> <li>- <b>Retention period (days)</b> (Aufbewahrungszeitraum (Tage): Diese Einstellung regelt die Bearbeitung von Besuchsdatensätzen.                         <ul style="list-style-type: none"> <li>- Wenn der Zeitraum zum ersten Mal abläuft, wird der Datensatz durch die Anwendung anonymisiert.</li> <li>- Wenn der Zeitraum zum zweiten Mal abläuft, wird der Datensatz durch die Anwendung gelöscht. Der Standardwert ist 365. Legen Sie 0 fest, um die Beibehaltungsdauer vollständig zu deaktivieren. In diesem Fall werden Besuchsdatensätze für unbestimmte Zeit aufbewahrt.</li> </ul> </li> <li>- <b>Document storage mode</b> (Dokumentspeichermodus): Wählen Sie aus, ob Dokumente auf Papier oder als digitale Dateien gespeichert werden sollen.</li> <li>- <b>Maximum number of visitors</b> (Maximal zulässige Anzahl von Besuchern): Die maximale Anzahl von Besuchern, die gleichzeitig am Standort zulässig ist. Der Standardwert ist 100. Legen Sie 0 fest, um die Besucherzähler im Dashboard vollständig zu deaktivieren.</li> <li>- <b>Document expiry period (days)</b> (Ablaufzeitraum für das Dokument (Tage): Geben Sie an, wie lange hochgeladene Dokumente gültig bleiben sollen, z. B. Geheimhaltungsvereinbarungen (NDA) und Nutzungsbedingungen. Der Zeitraum gilt für Datensätze auf Papier und in Form digitaler Dateien.</li> </ul>
---------------------------------	--

Nach diesem Zeitraum werden die Dokumente im Profil des Besuchers (Uhrensymbol mit rotem Punkt) als abgelaufen markiert. Der Standardwert ist 365.

- **Document expiry warning period (days)** (Warnzeitraum für den Dokumentablauf): Geben Sie die Dauer des Warnzeitraums vor dem Ablaufdatum ein.  
Während dieses Warnzeitraums werden Dokumente im Profil des Besuchers gekennzeichnet (Uhrensymbol mit orangefarbenem Punkt). Vor dem Warnzeitraum weist das Uhrensymbol einen grünen Punkt auf.
- **Logo:** Aktivieren oder deaktivieren Sie die Kontrollkästchen, die festlegen, ob in den Dialogen ein benutzerdefiniertes oder das Standard-Logo angezeigt wird und ob die Bosch **Supergrafik** angezeigt werden soll.
  - Kriterien für angepasste Logo-Dateien finden Sie unter:  
*Anpassen des Firmenlogos, Seite 35*
- Klicken Sie auf **Vorschau**, um die Dialogseite so anzuzeigen, wie Sie mit diesen Einstellungen dargestellt wird. Weitere Informationen zum Vorschaumodus finden Sie im nächsten Abschnitt.
- **Languages** (Sprachen):  
Wählen Sie die Sprachen, die in der Benutzeroberfläche verfügbar sein sollen, und die bevorzugten Formate für **Datum** und **Uhrzeit** aus.
- **Mail-Server**  
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.
- **E-Mail-Vorlagen**  
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.
- **Mobiler Zutritt**  
Aktivieren Sie das Kontrollkästchen **Mobiler Zutritt**, um mobilen Zutritt zu aktivieren.

**Verbindung:** Geben Sie die Adresse des mobilen Zutrittservers (Adresse des Registrierungsdienstes) ein.

`https://<MyMobileAccessBackendServer>:5700`

Verwenden Sie ein (FQDN) für <MyMobileAccessBackendServer> in Multi-Domain-Umgebungen.

**Hinweis:** eine IP-Adresse anstelle eines FQDN verwenden möchten, müssen Sie unter **Zertifikaterstellung** diese IP-Adresse eingeben, wenn Sie den Einrichtungsassistenten für das Mobiler Zutritt-Backend ausführen.

**Onboarding von Installationstechnikern:** Wählen Sie die Informationen aus, die Sie von den Installationstechnikern benötigen, damit diese die mobilen Zutrittsleser mit dem Bosch

	<p>Setup Access konfigurieren können.</p> <p>Melden Sie sich von der Webanwendung ab und melden Sie sich erneut an, um die Funktion „Mobiler Zutritt“ sofort nutzen zu können.</p>
<p><b>Empfangspersonal</b></p>	<ul style="list-style-type: none"> <li>- Dieser Einstellungsbildschirm enthält zwei Kontrollkästchen für jedes der Datenfelder im Besucherregistrierungsdialog für das Empfangspersonal.             <ul style="list-style-type: none"> <li>- Deaktivieren oder aktivieren Sie das erste Kontrollkästchen, um festzulegen, ob das Datenfeld in allen Registrierungsdialogen <b>sichtbar</b> sein soll.</li> <li>- Deaktivieren oder aktivieren Sie das zweite Kontrollkästchen (markiert mit einem Sternchen), um zu bestimmen, ob das Datenfeld <b>obligatorisch</b> sein soll.</li> </ul> </li> <li>- Passen Sie die Standardtexte für die Überschriften in den Datenerfassungsdialogen an.</li> </ul> <p>Weitere Einzelheiten finden Sie unter <i>Anpassen der Benutzeroberfläche, Seite 34</i>.</p> <p><b>Besondere Option: Check-in/Check-out ohne Ausweis ermöglichen</b></p> <p>Wenn Besucher eine enge Begleitung haben oder sich nur in öffentlichen Räumen aufhalten dürfen, sind individuelle Besucherausweise möglicherweise überflüssig. Für solche Fälle gibt es die Möglichkeit, Besucher ohne Ausweise ein- und auszuchecken. Aus Sicherheitsgründen ist diese Option standardmäßig deaktiviert. Aktivieren Sie das Kontrollkästchen, um es zu aktivieren:</p> <ul style="list-style-type: none"> <li>- <b>Hinweis:</b> Wenn die Option aktiviert ist, wird jeder <b>Besucher</b>, der sich selbst am Kioskcomputer anmeldet, automatisch genehmigt und sein eigener Besuch gleichzeitig eingecheckt.</li> <li>- Im Kapitel <b>Betrieb</b> dieses Dokuments unter <i>Ein- und Auschecken ohne Ausweis, Seite 51</i> erfahren Sie, wie ein <b>Empfangsmitarbeiter</b> Besucher ohne Ausweise bearbeitet.</li> </ul>
<p><b>Gastgeber</b></p>	<p>Die Einstellungen für die <b>Host-</b> und <b>Besucher-</b>Benutzer bleiben solange schreibgeschützt, bis Sie die Einstellungen für das <b>Empfangspersonal</b> bearbeitet und abgespeichert haben.</p>
<p><b>Besucher</b></p>	<p>Felder, die Sie in den Einstellungen für das <b>Empfangspersonal</b> als nicht sichtbar markieren, werden automatisch für <b>Gastgeber</b> und <b>Besucher</b> als nicht sichtbar markiert.</p> <p>Im Anschluss daran ist der Konfigurationsvorgang identisch.</p>

**Siehe**

- *Zuweisen von physischen Berechtigungen, Seite 47*
- *Anpassen der Benutzeroberfläche, Seite 34*

## 4.6.1

### 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. Wenn Sie eine Vorlage zum Bearbeiten herunterladen, wird Sie in den Standard-Download-Ordner Ihres Browsers kopiert.

- *MobileAccess.html* Eine Aufforderung an einen Ausweisinhaber, Smartphone-basierte Anmeldeinformationen zu verwenden.
- *SetupAccess.html* Eine Aufforderung an einen Einrichter, Leser für den mobilen Zutritt zu konfigurieren.
- *VisitorInvite.html* Eine Einladung zum Besuch Ihrer Website mit der Option, eine iCalendar-Datei an die E-Mail anzuhängen.
- *InformHostAboutCheckin.html* Eine E-Mail, die den Gastgeber darüber informiert, dass ein Besucher eingetroffen ist.

#### 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.

#### Mobiler Zutritt

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

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

#### Zutritt einrichten

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

Platzhalter	Description (Beschreibung)
<code>{{Title}}</code>	Titel des Installationstechnikers (Herr, Frau, Dr. etc.)
<code>{{FirstName}}</code>	Vorname des Einrichters
<code>{{LastName}}</code>	Nachname des Einrichters
<code>{{CompanyName}}</code>	Unternehmen des Einrichters

Platzhalter	Description (Beschreibung)
{{QrcodeLink}}	QR-Code, der dem Link entspricht, der dem Installationstechniker einen mobilen Zutritt zur Einrichtung von Lesegeräten über die App Setup Access bietet
{{InviteLink}}	Link, der dem Installationstechniker über die App Setup Access mobilen Zutritt zur Einrichtung von Lesegeräten bietet

**Besuchereinladung**

E-Mail, die an den Besucher gesendet wird, wenn ein Besuch angelegt oder bearbeitet wird.

Platzhalter	Description (Beschreibung)
{{VisitorID}}	der ID-Code des Besuchers, wie er von der VisMgmt-Anwendung generiert wird
{{Title}}	Titel des Besuchers (Herr, Frau, Dr., etc.)
{{FirstName}}	Vorname des Besuchers
{{LastName}}	Nachname des Besuchers
{{CompanyName}}	Unternehmen des Besuchers
{{HostFirstName}}	Vorname des Gastgebers
{{HostLastName}}	Nachname des Gastgebers
{{ExpArrivalDate}}	geplantes Besuchsdatum

**Besucher angekommen**

E-Mail, die an den Host gesendet wird, wenn das Empfangspersonal den Besuch genehmigt

Platzhalter	Description (Beschreibung)
{{VisitorID}}	der ID-Code des Besuchers, wie er von der VisMgmt-Anwendung generiert wird
{{Title}}	Titel des Besuchers (Herr, Frau, Dr., etc.)
{{FirstName}}	Vorname des Besuchers
{{LastName}}	Nachname des Besuchers
{{CompanyName}}	Unternehmen des Besuchers
{{HostFirstName}}	Vorname des Gastgebers
{{HostLastName}}	Nachname des Gastgebers
{{ExpArrivalDate}}	geplantes Besuchsdatum
{{ArrivalDate}}	tatsächliches Besuchsdatum

**Besucherausweis**

Dokument, das ausgedruckt und einem Besucher ausgehändigt werden kann. Diese könnte eine Karte des Gebäudes oder eine Checkliste enthalten.

Platzhalter	Beschreibung
{{VisitorID}}	der ID-Code des Besuchers, wie er von der VisMgmt-Anwendung generiert wird
{{Title}}	Titel des Besuchers (Herr, Frau, Dr., etc.)
{{FirstName}}	Vorname des Besuchers
{{LastName}}	Nachname des Besuchers
{{CompanyName}}	Unternehmen des Besuchers
{{HostFirstName}}	Vorname des Gastgebers
{{HostLastName}}	Nachname des Gastgebers
{{ExpArrivalDate}}	geplantes Besuchsdatum
{{ArrivalDate}}	tatsächliches Besuchsdatum

## 4.6.2

### Vorschaumodus

Bestimmte Optionssätze stellen eine Schaltfläche **Vorschau** zur Verfügung, die den Vorschaumodus aktiviert, sodass Sie die Dialoge so sehen können, wie Sie im Anschluss an die Festlegung dieser Optionen angezeigt werden.

Im Vorschaumodus gelten die folgenden Bedingungen:

- Ein Banner wird am oberen Rand des Dashboards angezeigt.

 **Preview mode. Any changes will not be applied. Close preview-mode or change role** 

- Im Dashboard oder in den Menüs vorgenommene Änderungen werden **nicht** gespeichert.
- Klicken Sie im Banner auf **Vorschaumodus schließen**, um den Vorschaumodus zu beenden
- Verwenden Sie die Liste **Rolle ändern** im Banner, um eine Vorschau der Darstellung der Schnittstelle für die verschiedenen Benutzergruppen anzuzeigen: Rezeptionist, Gastgeber, Besucher.

## 4.6.3

### Dokumentenvorlagen

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

## 4.7

### Anpassen der Benutzeroberfläche

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

### 4.7.1

#### 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:

<input checked="" type="checkbox"/>	①	<input checked="" type="checkbox"/> *
<input checked="" type="checkbox"/>	②	<input type="checkbox"/> *
<input type="checkbox"/>	③	<input type="checkbox"/> *

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

### 4.7.2 Anpassen des Kioskmodus

Wenn auf Ihrer Website ein oder mehrere Peripheriegeräte fehlen, z. B. ein Dokumentscanner, können Sie den Selbstregistrierungsprozess für Besucher im Kioskmodus entsprechend anpassen, indem Sie die Kontrollkästchen für die entsprechenden Registrierungsschritte deaktivieren.

### 4.7.3 Anpassen des Firmenlogos

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

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

## 4.8 Firewall-Einstellungen

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

1. Öffnen Sie die Windows-Firewall, indem Sie „Start > **Zentrale** > **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
    - <Servername> : 5700 – vom Mobile Access Backend-Server verwendet
  - Auf Client-Computern
    - localhost:5707 – verwendet vom Bosch Peripheriegeräte-Add-on

#### Portnutzung innerhalb des Systems

Server ausgehend	Port Ausgang	Server eingehend	Port Eingang	Protokoll	Kommentare
VisMgmt oder CredMgmt	*	Mobile Access Backend	5700	HTTPS	Befehle aus der Webanwendung zum Erstellen und/oder Löschen mobiler Anmeldedaten

Server ausgehend	Port Ausgang	Server eingehend	Port Eingang	Protokoll	Kommentare
Mobile Geräte aus dem Internet	*	Mobile Access Backend	5700	HTTPS	Mobile Geräte erhalten mobile Anmeldedaten über das Internet
Mobile Access Backend	*	Google Firebase (Internet)	*	HTTPS	Mobile Geräte erhalten Push-Benachrichtigungen. Bitte lesen Sie die Dokumentation von Google Firebase zu den Firewall-Einstellungen.  <a href="https://firebase.google.com/docs/cloud-messaging/concept-options">https://firebase.google.com/docs/cloud-messaging/concept-options</a>
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 CredMgmt-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.

### 4.8.1

#### 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 > Zentrale > 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\net6.0
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

Service	Dateispeicherort
Bosch.Events.Api	[install-path]\Events API
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

## 4.9

### 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:

#### 4.9.1

#### 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.

## 4.9.2 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.

## 4.9.3 Sicherer Umgang mit mobilen Anmeldedaten

- Lassen Sie unkonfigurierte Mobiler Zutritt-Leser nicht unbewacht.
  - Ein Angreifer könnte das Leser für einen anderen ACS missbrauchen. Dies würde einen kostspieligen Werksreset erfordern.
- Wenn ein mobiles Gerät mit mobilen Berechtigungen verloren geht oder gestohlen wird, behandeln Sie dieses Gerät wie einen verlorenen Ausweis: Sperren oder löschen Sie alle mobilen Berechtigungen so schnell wie möglich.
- Für hochsichere Umgebungen empfiehlt Bosch eine Zwei-Faktor-Authentifizierung. Dies erfordert, dass der Berechtigungsinhaber das mobile Gerät entsperrt, bevor er es als Berechtigungsausweis verwendet.
- Mobile Berechtigungen 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 Mobiler Zutritt nur physische Ausweise mit einer sicheren Kodierung (z. B. Bosch-Code).
- Schützen Sie den Mobiler Zutritt-Server vor unbefugtem physischen Zutritt. Bosch empfiehlt zusätzliche Maßnahmen wie z. B. die BitLocker-Festplattenverschlüsselung.
- Schützen Sie den Mobiler Zutritt-Server vor DoS-Angriffen (Denial of Service). Es muss Teil einer sicheren Netzwerkumgebung sein, die Schutzmaßnahmen wie einen Rate-Limiter bietet.

- Rollen Sie die mobilen "Installer"-Berechtigungen mittels QR-Codes- Einladungen als Administrator aus. Ein gestohlenen Telefon eines Installationstechnikers mit aktiven Berechtigungen dieses Installationstechnikers könnte es einem Angreifer ermöglichen, Mobiler Zutritt-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 Berechtigungen 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 Berechtigungen sofort lädt.

## 4.10 **Sicherung des Systems**

VisMgmt ist eine Web-Zusatzanwendung für ein Haupt-Zutrittskontrollsystem. Ziehen Sie bezüglich der Sicherung von Systemdatenbanken die Dokumentation des Haupt-Zutrittskontrollsystems zu Rate.

## 5

## Bedienung

### 5.1

### Übersicht über die Benutzerrollen

Art der Benutzer	Anwendungsfälle
Empfangspersonal	Registrierung neuer Besuche und Besucher Genehmigung und Ablehnung von Besuchen Besucher sperren Besucherausweise zuweisen und deren Gültigkeit aufheben Verwalten von zugehörigen Dokumenten Überwachung der Anzahl der Besucher am Standort
Visitor (Besucher)	Selbständige oder Vorabregistrierung Erstellen und pflegen eines Besucherprofils Unterzeichnen von Dokumenten
Gastgeber	Verwalten von Zeitplänen und Listen von Besuchen und Besuchern Vorregistrierung von Besuchen
Administrator	Vornahme globaler Einstellungen Anpassen des Verhaltens des Tools und seiner Benutzeroberfläche Plus: Alle Anwendungsfälle des Empfangsmitarbeiters

### 5.2

### Verwendung des Dashboards

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

#### Übersicht und Schnellfilter

Der obere Rand des Dashboards enthält einen schnellen Überblick über die Besuche des Tages. Auf diese Weise kann der Benutzer die Besucheranzahl am Standort problemlos überwachen.

<b>Besucher erwartet heute: _%</b>	<b>Besucher eingeeckht: _%</b>	<b>Besucher, die noch heute auschecken sollen</b>	<b>Besucher, deren Auschecken überfällig ist</b>
<code>&lt;current count&gt;</code> <code>/ &lt;total capacity&gt;</code>	<code>&lt;current count&gt;</code> <code>/ &lt;total capacity&gt;</code>	<code>&lt;current count&gt;</code>	<code>&lt;current count&gt;</code>

Klicken Sie auf eine der Kopfzeilen, um die Besuche-Tabelle entsprechend der Bedeutung der Kopfzeile zu filtern. Klicken Sie beispielsweise auf **Besucher eingeeckht**, um nur die Besucher anzuzeigen, denen ein Ausweis zugewiesen ist.

Der Wert für `<total capacity>` ist eine Konfigurationseinstellung, die vom Systemadministrator vorgenommen wird. Siehe *Verwenden des Einstellungsmenüs zur Konfiguration, Seite 29*.

#### 5.2.1

#### Die Besuche-Tabelle

Jede Zeile in der Tabelle repräsentiert einen Termin für einen Besuch.

- Sie können die Tabelle nach jeder beliebigen Spalte sortieren, indem Sie auf die Spaltenüberschrift klicken.

- Sie können einzelne Besuche oder mehrere Besuche auf einmal auswählen, indem Sie die Tastatur-Maus-Idiome verwenden:
  - Strg-Klick zur Mehrfachauswahl einzelner Zeilen.
  - Klicken Sie mit der Strg-Taste auf eine bereits ausgewählte Zeile, um sie aus der Auswahl zu entfernen.
  - Umschalt-Taste für Mehrfachauswahl von zusammenhängenden Zeilen
- Sie können der Tabelle neue Besuche hinzufügen
- Sie können Einzelheiten zu Besuchen und Besuchern bearbeiten, indem Sie auf die Aktionsschaltflächen klicken
  - Besuch genehmigen
  - Besuch ablehnen
  - Dem Besucher einen Ausweis zuweisen
  - Einzelheiten zu Besuchen und Besuchern bearbeiten
- Sie können die aktuell gefilterten Zeilen in eine *.CSV* - oder *.XLSX*-Datei exportieren.

Die horizontale Symbolleiste hat folgende Funktionen:



Beschriftung	Funktion
<b>1</b> N Einträge	Die Gesamtzahl N der Besuche (jeder Besuch ist eine Zeile in der Tabelle).
<b>2</b> Suchen	Suche nach beliebigem Text in den Besuchen in der Tabelle
<b>3</b> 	Zeigt die Besuche an, die zuletzt der Tabelle hinzugefügt wurden.
<b>4</b> 	Dialog zur Auswahl von Filterkriterien öffnen
<b>5</b> 	Die Tabelle auf die Standardansicht zurücksetzen und alle Filter wiederherstellen.
<b>6</b> Zuweisung eines Ausweises aufheben	Öffnen Sie einen Dialog, um die Zuweisung von Ausweisen mithilfe eines verbundenen Bekanntmachungslesers aufzuheben.
<b>7</b> 	Dialog öffnen zum Erstellen eines neuen Besuchseintrags in der Tabelle
...	Klicken Sie auf das Ellipsen-Symbol für ein Menü, um die aktuell gefilterten Besuche und auch Dokumente in verschiedene Dateiformate zu exportieren, zum Beispiel <i>CSV</i> und <i>.XLSX</i>

Beschriftung	Funktion
	Beachten Sie, dass Sie aus Gründen der Datensicherheit nur exportieren können, wenn Ihr Client über eine gesicherte HTTPS-Verbindung mit einem Zertifikat läuft.

## 5.2.2 Tabellenspalten und Aktionen

### Spalten

Spalte	Wert	Beschreibung
<b>Status</b>	 Besuch erwartet  Besuch genehmigt  Besuch abgelehnt  Ausweis zugewiesen  Ausweis abgelaufen  Besuch beendet (Besucher verfügt nicht mehr über Ausweise und hat das Gelände verlassen)	Ein Symbol, das den Status des Besuchs wiedergibt
<b>Name</b>	Name des Besuchers als Hyperlink	Klicken Sie auf den Hyperlink, um Einzelheiten zum Besucher und seinem aktuellen Besuch anzuzeigen.
<b>Erw. Ankunft</b>	Datum und Uhrzeit	Datum und Uhrzeit der voraussichtlichen Ankunft des Besuchers
<b>Erw. Abreise</b>	Datum und Uhrzeit	Datum und Uhrzeit der voraussichtlichen Abreise des Besuchers
<b>Eingecheckt</b>	Datum und Uhrzeit	Datum und Uhrzeit der Zuweisung des ersten Ausweises an den Besucher.
<b>Ausgecheckt</b>	Datum und Uhrzeit	Datum und Uhrzeit der Aufhebung der Zuweisung des letzten Ausweises des Besuchers.

Spalte	Wert	Beschreibung
<b>Ausweisnummer</b>	Nummerisch	Die Nummern der Ausweise, die diesem Besucher zugewiesen wurden.
<b>Aktionen</b>	Symbole	Siehe separate Tabelle unten

#### Aktionen

Symbol	Funktion
	<b>Genehmigen</b> des Besuchs. HINWEIS: Es ist nicht möglich, einem Besucher auf der Sperrliste einen Ausweis zuzuweisen. Sie müssen den Besucher zuerst von der Sperrliste nehmen oder ihn vorübergehend davon ausnehmen. Siehe <i>Zur Sperrliste hinzufügen, entfernen oder davon ausnehmen, Seite 52</i>
	<b>Ablehnen</b> des Besuchs. Diese Schaltfläche wird deaktiviert, nachdem der Besucher eing_checked hat, also dann, wenn er bereits über einen Ausweis verfügt.
	<b>Zuweisen</b> von einem oder mehreren Ausweisen zum Besucher
	<b>Bearbeiten</b> des Besuchereignisses und/oder der Anmeldedaten des Besuchers

## 5.3 Empfangspersonal

### 5.3.1 Anmelden als Empfangspersonal

1. Öffnen Sie im Browser `https://<My_VisMgmt_server>:5706/main/`, um zum Anmeldebildschirm zu gelangen.
2. Geben Sie den Benutzernamen eines Kontos mit den erforderlichen Rechten für ihre Rolle ein.  
Wenden Sie sich an Ihren Systemadministrator, falls Sie über kein Konto verfügen.
3. Geben Sie das Passwort ein.
4. Klicken Sie auf **Anmelden**.

### 5.3.2 Suchen und Filtern von Besuchen

Im VisMgmt Dashboard in der Symbolleiste oberhalb der Besuche-Tabelle.

#### Suchen

Geben Sie einen alphanumerischen Text in das Suchfeld ein und drücken Sie die Eingabetaste, um nach Namen und Gastgebern zu suchen.

#### Filtern

- Um die Besuche anzuzeigen, die der aktuellen Uhrzeit am nächsten sind, klicken Sie auf **Aktuell**
- Klicken Sie auf **Filter**, um einen komplexen Filter aus dem Besuchsstatus, den Ein- und Auscheckdaten und den Ausweisnummern zu erstellen.
  - Geben Sie im Popup-Dialog die gewünschten Filterkriterien ein.

- Klicken Sie auf **Anwendungen**
  - Das System reduziert dann die Besuche-Tabelle auf die Besuchstermine, die den Filterkriterien entsprechen.
- Um alle Filterkriterien zu löschen, klicken Sie auf **Zurücksetzen**

### 5.3.3

## Registrierung von Besuchen

### Einführung

Für das Empfangspersonal gibt es zwei grundlegende Szenarios bei der Registrierung von Besuchen:

- **A:** Wenn ein Besucher den Besucherkiosk verwendet, um seine eigene Besucherkennung zu erstellen und Dokumente zu hochzuladen, muss das Empfangspersonal nur alle erforderlichen Informationen und Unterschriften eintragen, die noch fehlen, und dem Besucher einen Ausweis zuweisen.
- **B:** Wenn ein Besucher den Besucherkiosk nicht nutzt und sich direkt an der Rezeption anmeldet, kann der Rezeptionist den Besuch von Grund auf neu anmelden: die erforderlichen Informationen erfassen, Unterschriften für erforderliche Dokumente einholen und dem Besucher einen Ausweis zuweisen.

Szenario **A** ist eine Teilmenge von Szenario **B**. Deswegen wird hier das vollständige Szenario **B** beschrieben. Die Verwendung des Kioskmodus durch einen Besucher wird in einem eigenen Abschnitt beschrieben. Siehe *Einführung in den Kioskmodus, Seite 55*.

### Vorgehensweise

Im VisMgmt Dashboard in der Symbolleiste oberhalb der Besuche-Tabelle.

1. Klicken Sie , um einen Besuchstermin zur Besuche-Tabelle hinzuzufügen.
  2. Geben Sie die Daten, die Ihr Standort von Besuchern benötigt, im Dialog **Persönliche Daten** ein. Pflichtfelder sind mit einem Sternchen (\*) gekennzeichnet. Sie können Daten manuell eingeben, jedoch schneller und präziser geht dies über einen Dokumentenscanner, sofern diese an der Bedienstation des Empfangspersonals verfügbar sind. Weitere Informationen zu den unterstützten Peripheriegeräten finden Sie unter *Peripheriehardware, Seite 24*.
- **Allgemeine Informationen**
    - Suchen und laden Sie ein vollständiges Besucherprofil, das bei einem vorherigen Besuch erstellt wurde. Klicken Sie zum Suchen von Profilen auf das  (Suchen)-Symbol, das sich im Feld **Nachname\*** befindet. Wenn ein Besucherprofil erstellt wird, wird ihm ein eindeutiger alphanumerischer Code zugeordnet, den der Besucher sorgfältig speichern sollte, um den Registrierungsvorgang für zukünftige Besuche zu beschleunigen.
    - Geben Sie andernfalls die Daten per Hand ein.
  - **Ausweisfotos**
    - Ein Foto aus dem Dateisystem **Hochladen**.
    - Fotos des Besuchers über eine verbundene Web-Kamera **Erfassen**.
  - **Ausweisdokumente**
    - Klicken Sie auf **Dokument scannen**, um Daten von einem Dokumentenscanner einzulesen (sofern verfügbar) und automatisch die relevanten Datenfelder im Dialog auszufüllen.
    - Geben Sie ansonsten den Text manuell ein, falls Ihr System über keinen Dokumentenscanner verfügt.
  - **Rechtsdokumente**

- Laden Sie die Dokumente, die der Besucher elektronisch am Kiosk unterschrieben hat.
  - Wenn Ihr System nicht über einen Besucherkiosk verfügt, drucken Sie die erforderlichen PDF-Dokumente aus und speichern Sie sie (mit Unterschrift des Besuchers) auf dem Dateisystem.
3. Klicken Sie auf **Weiter**, um mit dem Dialog **Besuche** fortzufahren.
  4. Geben Sie im Dialog **Besuche** im Bereich **Aktueller Besuch** die Daten, die für Ihren Standort erforderlich sind, ein. Pflichtfelder sind mit einem Sternchen (\*) gekennzeichnet.
    - Wählen Sie einen **Besuchertyp** aus.  
Dabei handelt es sich entweder um **Besucher** (Standard) oder eine angepasste Unterklasse von **Besucher**, die als **Personentyp** im Haupt-Zutrittskontrollsystem definiert ist.
    - Wählen Sie unter **Gastgeber** den Namen des zu besuchenden Mitarbeiters.
      - Beachten Sie, dass Sie nur Ausweisinhaber des Haupt-Zutrittskontrollsystems auswählen können.
      - Ein Tooltip zeigt die E-Mail-Adresse der Person an, um die Identifizierung zu erleichtern.
    - Wenn der Besucher eine Begleitperson durch das Gelände benötigt, wählen Sie den Namen des begleitenden Mitarbeiters unter **Begleitung** aus.
      - Beachten Sie, dass Sie nur Ausweisinhaber des Haupt-Zutrittskontrollsystems auswählen können.
      - Ein Tooltip zeigt die E-Mail-Adresse der Person an, um die Identifizierung zu erleichtern.
    - Wenn der Besucher zusätzliche Zeit benötigt, um durch eine Tür zu gehen, wählen Sie das Kontrollkästchen **Verlängerte Türöffnungszeit** aus
  5. Klicken Sie auf **Speichern**.  
Beachten Sie, dass Sie die Daten erst dann speichern können, wenn Sie alle Pflichtfelder ausgefüllt haben.

#### Siehe

- *Peripheriehardware, Seite 24*

## 5.3.4

### Genehmigung und Ablehnung von Besuchen

#### Hintergrund: Genehmigen von physischen Ausweisen

Sie müssen einen Besuch genehmigen, bevor Sie einem Besucher Ausweise zuweisen können.

#### Hintergrund: Genehmigen von mobilen Berechtigungen

Sie können mobile Berechtigungen am Tag des Besuchs erstellen und ausgeben, ähnlich wie beim Zuweisen eines physischen Ausweises.

- **Hinweis:** Die mobilen Berechtigungen können erst verwendet werden, wenn Sie den Besuch genehmigen.

*Alternativ* können Sie die mobilen Berechtigungen auch erstellen und im Voraus ausgeben. Wenn der Besucher an der Rezeption eintrifft, genehmigen Sie den Besuch wie unten beschrieben, um die Berechtigungen endgültig zu aktivieren.

- **Hinweis:** Die mobilen Berechtigungen können erst verwendet werden, wenn Sie den Besuch genehmigen.
- Wenn Sie eine voraussichtliche Abreisezeit für den Besuch festgelegt haben, dann gilt diese Zeit.

- Wenn Sie keine voraussichtliche Abreisezeit festgelegt haben, wird eine Standardanzahl von Stunden (8) angewendet. Administratoren können diese Standardeinstellung im Menü **Einstellungen** ändern.

### Verfahren für die Genehmigung und Ablehnung

Es gibt zwei Möglichkeiten, einen Besuch zu genehmigen oder abzulehnen:

- in der Besuche-Tabelle auf dem Dashboard
- im Besuche-Editor

#### in der Besuche-Tabelle auf dem Dashboard:

- **Genehmigen:** Wählen Sie in der Tabelle „Besuche“ eine Zeile aus und klicken Sie auf



. Nach einer Popup-Bestätigung wird das Symbol grau angezeigt, um zu signalisieren, dass der Besuch genehmigt wurde.

- **Ablehnen:** Wählen Sie in der Tabelle „Besuche“ eine Zeile aus und klicken Sie auf



. Nach einem Bestätigungs-Popup wird das Symbol **Genehmigen** wieder auf Blau zurückgesetzt, um zu zeigen, dass der Besuch noch genehmigt werden muss.

#### im Besuche-Editor:

1. Wählen Sie im Dashboard in der Besuche-Tabelle eine Zeile aus und klicken Sie auf



, um den Besuch zu bearbeiten.

2. Klicken Sie im Dialog **Persönliche Daten** auf **Weiter**.
3. Klicken Sie im Dialog **Besuche** auf die Schaltfläche **Genehmigen** oder **Ablehnen**.
4. Bestätigen Sie Ihre Aktion im Popup-Fenster.

## 5.3.5

### Zuweisen von physischen Berechtigungen

#### Einführung

Weisen Sie jedem Besucher, den Sie auf das Gelände lassen, einen Besucherausweis zu. Sie können einem einzelnen Besucher bei Bedarf mehrere Ausweise zuweisen.

- Die **ingecheckte** Zeit eines Besuchs ist die Zeit ab der Zuweisung des ersten Ausweises.
- Die **ausgecheckte** Zeit eines Besuchs ist die Zeit, ab der die Zuweisung des letzten Ausweises, der dem Besucher noch zugewiesen wurde, aufgehoben wurde.

Das Empfangspersonal kann Ausweise problemlos über das Dashboard zuweisen und oder die Zuweisung aufheben, sofern ein Bekanntmachungsleser für Ausweise mit dem Computer des Empfangspersonals verbunden ist.

Dennoch bietet auch der Besuche-Editor eine Möglichkeit, Ausweisnummern zuzuweisen, wenn kein solcher Leser verfügbar ist.



#### Hinweis!

Gesperrte Personen können keine Ausweise erhalten

Es ist nicht möglich, Ausweise Besuchern zuzuweisen, die sich auf der Sperrliste befinden.

Entfernen Sie den Besucher von der Sperrliste oder legen Sie für den Besucher eine vorübergehende Ausnahme fest, bevor Sie versuchen, diesem einen Ausweis zuzuweisen.

### Zuweisen eines Ausweises über das Dashboard (erfordert einen Bekanntmachungsleser)

1. Halten Sie einen physischen Besucherausweis für den Bekanntmachungsleser bereit.
2. Genehmigen Sie den Besuch in der Besuche-Tabelle. Siehe *Genehmigung und Ablehnung von Besuchen*, Seite 46



3. Wählen Sie die Zeile des Besuchs aus und klicken Sie auf
4. Befolgen Sie die Anweisungen in der Popup-Benachrichtigung zur Verwendung des Bekanntmachungslesers.

### 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 Registrierungsleser 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.

### Zuweisen eines Ausweises im Besuche-Editor

1. Wählen Sie im Dashboard in der Besuche-Tabelle eine Zeile aus und klicken Sie auf



, um diesen Besuch zu bearbeiten.

2. Klicken Sie im Dialog **Persönliche Daten** auf **Weiter**.
3. Klicken Sie im Dialog **Besuche** auf **Genehmigen**, falls der Besuch noch nicht genehmigt wurde.
4. Wenn ein Bekanntmachungsleser angeschlossen ist, klicken Sie auf **Ausweis lesen**, und folgen Sie den Anweisungen in der Popup-Benachrichtigung zur Verwendung des Bekanntmachungslesers.
- Klicken Sie andernfalls auf **Freie Ausweise anzeigen**, um eine Liste der noch verfügbaren Besucherausweise anzuzeigen.  
Wenn Sie über unsortierte physische Ausweise mit aufgedruckten Nummern verfügen, können Sie auch einen beliebigen Ausweis auswählen und die **Such**-Funktion verwenden, um ihre Nummer schnell in der Liste zu finden.



- Klicken Sie auf neben einer Ausweisnummer, um diesen Ausweis dem aktuellen Besucher zuzuweisen.
- Wiederholen Sie die letzten Schritte, um bei Bedarf weitere Ausweise zuzuweisen.
5. Klicken Sie auf **Speichern**, um den aktuellen Besuch mit den Ausweiszweisungen zu speichern.

### Aufheben der Zuweisung eines Ausweises im Besuche-Editor

1. Wählen Sie im Dashboard in der Besuche-Tabelle eine Zeile aus und klicken Sie auf



, um diesen Besuch zu bearbeiten.

2. Klicken Sie im Dialog **Persönliche Daten** auf **Weiter**.
3. Klicken Sie im Bereich „Besucherausweise“ auf den Dialog **Besuche**, klicken Sie auf



neben dem Ausweis, dessen Zuweisung Sie aufheben möchten und bestätigen Sie die Aktion im Popup-Fenster.

Wiederholen Sie diesen Schritt, bis Sie die alle gewünschten Ausweiszweisungen aufgehoben haben.

4. Klicken Sie auf **Speichern**, um den aktuellen Besuch mit den Ausweiszweisungen zu speichern.
5. Wenn Sie die Zuweisung des letzten Ausweises, der dem Besucher zugewiesen wurde, aufheben, zeichnet das System dieses Datum und die Uhrzeit als Auscheckzeit des Besuchers auf.



In der Besuche-Tabelle wird der Status dieses Besuchsdatensatzes zu \_\_\_\_\_

### Siehe

- *Verwenden des Einstellungsmenüs zur Konfiguration, Seite 29*
- *Registrierung von Besuchen, Seite 45*
- *Genehmigung und Ablehnung von Besuchen, Seite 46*

## 5.3.6

### 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 im Dashboard

1. Wählen Sie die Zeile der Person aus, die mobile Anmeldedaten erhalten soll



2. Klicken Sie in der ausgewählten Zeile auf
3. Wählen Sie eines der großen Symbole für die Optionen:

- **QR-Code**

oder

- **Einladungsmail**

4. 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, Seite 46*
- Das Mobilgerät funktioniert wie ein physischer Zutrittsausweis, solange die App läuft
- 5. 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 nimmt die E-Mail auf ihrem mobilen Gerät entgegen, auf dem die Mobile Access-App läuft
  - 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, Seite 46*
  - 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 **Mobilien Zutritt hinzufügen**
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, Seite 46*
  - 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 nimmt die E-Mail auf ihrem mobilen Gerät entgegen, auf dem die Mobile Access-App läuft
  - 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, Seite 46*
  - Das Mobilgerät funktioniert wie ein physischer Zutrittsausweis, solange die App läuft

**Siehe**

- *Installieren von Mobile Access, Seite 17*
- *Installieren der Mobile Access-Apps, Seite 24*

**5.3.7****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 Registrierungsleser 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 Ausweiszweisungen zu speichern.

**5.3.8****Ein- und Auschecken ohne Ausweis****Einführung**

Wenn Besucher eine enge Begleitung haben oder sich nur in öffentlichen Räumen aufhalten dürfen, sind individuelle Besucherausweise möglicherweise überflüssig. Für solche Fälle gibt es die Möglichkeit, Besucher ohne Ausweise ein- und auszuchecken. Aus Sicherheitsgründen ist diese Option standardmäßig deaktiviert.

**Voraussetzung.**

Ihr Systemadministrator hat im Dialog **Einstellungen > Empfangsmitarbeiter > Besuche** die spezielle Option **Check-in/Check-out ohne Ausweis** aktiviert. Anweisungen dazu finden Sie im Kapitel *Verwenden des Einstellungsmenüs zur Konfiguration, Seite 29* über die Konfiguration.

**Verfahren**

Wenn die Option aktiviert ist, geschieht Folgendes:

- Jeder Besucher, der sich selbst am Kioskcomputer anmeldet, wird automatisch für den Besuch zugelassen und checkt gleichzeitig ein.
- Das System setzt das Check-in-Datum und die Check-in-Zeit auf den Zeitpunkt der Anmeldung.

- Die Umschalttaste **Check-in/out ohne Ausweis** erscheint im Besuchseditor und im Dashboard für denselben Besuch.

#### Verfahren: Einchecken eines Besuchers ohne Ausweis

Wenn ein Besucher sich nicht selbst am Kiosk anmelden kann, sondern ohne Ausweis einchecken soll:

1. Den Besuch manuell registrieren, wie im Kapitel *Registrierung von Besuchen, Seite 45* beschrieben
2. Klicken Sie im Dashboard in der Besuchstabelle auf den Namen des Besuchers in der



Tabelle oder auf , um den Besuch zu bearbeiten.

3. Klicken Sie im Dialog **Persönliche Daten** auf **Weiter**.
4. Klicken Sie im Dialogfeld **Besuche** im Bereich **Besucherausweise** auf **Einchecken ohne Ausweis**

#### Verfahren: Auschecken eines Besuchers ohne Ausweis

Wenn ein Besucher ohne Ausweis das Gelände verlässt:

1. Klicken Sie im Dashboard in der Besuchstabelle auf den Namen des Besuchers in der



Tabelle oder auf , um den Besuch zu bearbeiten.

2. Klicken Sie im Dialog **Persönliche Daten** auf **Weiter**.
3. Klicken Sie im Dialogfeld **Besuche** im Bereich **Besucherausweise** auf **Auschecken ohne Ausweis**

#### Siehe

- *Registrierung von Besuchen, Seite 45*

### 5.3.9

#### Zur Sperrliste hinzufügen, entfernen oder davon ausnehmen

Besucher, die am Standort nicht willkommen sind, können auf eine Sperrliste gesetzt werden. Solange sich ein Besucher auf der Sperrliste befindet, können Sie dieser Person keinen Ausweis zuweisen. Sie können den Besucher jederzeit von der Sperrliste entfernen oder eine vorübergehende Ausnahme gewähren, um ihm einen Ausweis zuzuweisen.

#### Sperrliste

1. Wählen Sie im Dashboard in der Besuche-Tabelle eine Zeile aus und klicken Sie auf



, um einen Besuch zu bearbeiten.

2. Klicken Sie im Dialog **Persönliche Daten** auf **Sperrliste**.
3. Bestätigen Sie im Popup-Fenster, dass diese Person wirklich gesperrt werden soll.
4. Geben Sie im nächsten Popup-Fenster einen Grund für die Sperrung ein und bestätigen Sie.

- Ein Banner **Gesperrt** wird im Besuche-Editor angezeigt,

 **Blacklisted**

- Unter dem Banner werden zwei Schaltflächen angezeigt: eine für das Entfernen des Besuchers von der Sperrliste und eine für die Gewährung einer temporären Ausnahme.

- In der Besuche-Tabelle wird der Name jedes gesperrten Besuchers mit einem



Warndreieck angezeigt. Zum Beispiel:

#### Entfernen und Ausnahme gewähren

1. Wählen Sie im Dashboard in der Besuche-Tabelle eine Zeile aus, in welcher der Besucher



als gesperrt markiert ist, und klicken Sie auf , um den Besuch zu bearbeiten.

2. Klicken Sie im Dialog **Persönliche Daten** auf eine der folgenden Optionen:
  - **Entfernen**, um den Besucher dauerhaft von der Sperrliste zu entfernen.
  - **Ausnahme machen**, um den Besucher auf der Sperrliste zu belassen, aber für diesen Besuch die Zuweisung eines Ausweises zu ermöglichen.
3. Bestätigen Sie Ihre Aktion im Popup-Fenster.

### 5.3.10

#### Besucherprofile pflegen

Das System speichert Besucherprofile, bis die Besucher selbst, das Empfangspersonal oder die Administratoren sie löschen.

Nach einer in den Systemeinstellungen definierten Aufbewahrungsfrist (Standardwert 12 Monate) löscht das System die Datensätze des Besuchs.

Wenn ein Besucher oder ein Mitarbeiter des Empfangspersonals ein neues Besucherprofil erstellt, erhält das Profil einen eindeutigen alphanumerischen Code. Besucher können sich mit diesem Code am Besucherkiosk anmelden und so Zugriff zur Pflege ihrer eigenen Profile erhalten.



#### Hinweis!

Besucherausweise schützen

Schützen Sie Besucherausweise sorgfältig vor unberechtigtem Zugriff, da Sie den Zugang zu personenbezogenen Daten ermöglichen.

### 5.3.11

#### Anzeigen von Besuchsdatensätzen

1. Wählen Sie im Dashboard in der Besuche-Tabelle eine Zeile aus und klicken Sie auf



, um diesen Besuch zu bearbeiten.

2. Klicken Sie im Dialog **Persönliche Daten** auf **Weiter**
3. Klicken Sie im Dialog **Aktueller Besuch** auf **Alle Besuche anzeigen**
  - . Der Dialog **Aktueller Besuch** zeigt dann eine Liste der vorherigen Besuche an.

## 5.4

### Gastgeber

Gastgeber sind Mitarbeiter, die Besuche empfangen. Sie können ihre eigenen Termine anmelden und das System nach Details zu den Besuchern und Aufzeichnungen ihrer früheren Besuche durchsuchen: Vergangenheit, Gegenwart und Zukunft.

### 5.4.1

#### Anmelden der Gastgeberrolle

1. Öffnen Sie im Browser `https://<My_VisMgmt_server>:5706/main/`, um zum Anmeldebildschirm zu gelangen.
2. Geben Sie den Benutzernamen eines Kontos mit den erforderlichen Rechten für ihre Rolle ein.  
Wenden Sie sich an Ihren Systemadministrator, falls Sie über kein Konto verfügen.
3. Geben Sie das Passwort ein.
4. Klicken Sie auf **Anmelden**.

### 5.4.2

#### Suchen und Filtern



Die Symbolleiste für das Gastgeber-Dashboard enthält die folgenden Funktionen:

Beschriftung	Funktion
 N Einträge	Die Gesamtzahl N der Besuche (jeder Besuch ist eine Zeile in der Tabelle).
 Suchen	Suche nach beliebigem Text in den Besuchen in der Tabelle
 3	Zeigt die Besuche an, die zuletzt der Tabelle hinzugefügt wurden.
 4	Dialog zur Auswahl von Filterkriterien öffnen
 5	Die Tabelle auf die Standardansicht zurücksetzen und alle Filter wiederherstellen.
 6	Dialog öffnen zum Erstellen eines neuen Besuchseintrags in der Tabelle

#### Suchen

Geben Sie einen alphanumerischen Text in das Suchfeld ein und drücken Sie die Eingabetaste, um nach Namen und Gastgebern zu suchen.

#### Filtern

- Um die Besuche anzuzeigen, die der aktuellen Uhrzeit am nächsten sind, klicken Sie auf **Aktuell**
- Klicken Sie auf **Filter**, um einen komplexen Filter aus dem Besuchsstatus, den Ein- und Auscheckdaten und den Ausweisnummern zu erstellen.
  - Geben Sie im Popup-Dialog die gewünschten Filterkriterien ein.
  - Klicken Sie auf **Anwendungen**
    - Das System reduziert dann die Besuche-Tabelle auf die Besuchstermine, die den Filterkriterien entsprechen.

- Um alle Filterkriterien zu löschen, klicken Sie auf **Zurücksetzen**

### 5.4.3 Registrierung von Besuchen

So melden Sie einen Besuchstermin bei einem erstmaligen Besucher an:  
Im VisMgmt Dashboard in der Symbolleiste oberhalb der Besuche-Tabelle.



1. Klicken Sie , um eine Zeile zur Besuche-Tabelle hinzuzufügen.
2. Geben Sie im Dialog **Persönliche Daten** im Abschnitt **Allgemeine Informationen** die personenbezogenen Daten ein, die Ihr Standort für Besucher benötigt.
3. Geben Sie im Abschnitt **Besuchsdetails** die erforderlichen Details ein. Das sind in der Regel die erwartete Ankunfts- und Abreisezeit sowie ein Grund für den Besuch.
4. Klicken Sie auf **Speichern**, um den Besuchstermin zu speichern.  
Der Besuch wird auf dem Dashboard als Zeile in der Besuche-Tabelle angezeigt.

### 5.4.4 Kopieren von Besuchsterminen

Festlegen eines weiteren Termins mit demselben Besucher

1. Auf dem VisMgmt Dashboard finden Sie einen bereits vorhandenen Termin mit demselben Besucher in der Besuche-Tabelle.



2. Klicken Sie auf das kleinere -Symbol am Ende der Zeile.
3. Geben Sie im Dialog **Persönliche Daten** im Abschnitt **Besuchsdetails** die erforderlichen Informationen ein, in der Regel die erwarteten Ankunfts- und Abreisezeiten sowie einen Grund für den Besuch.
4. Klicken Sie auf **Speichern**, um den Besuchstermin zu speichern.  
Der Besuch wird auf dem Dashboard als Zeile in der Besuche-Tabelle angezeigt.

## 5.5 Besucher

Besucher können das System im Kioskmodus auf dem Gelände verwenden, um ihre eigenen Besucherprofile zu erstellen und die erforderlichen Dokumente zu unterzeichnen, bevor Sie zur Rezeption gehen, um Ihre Besucherausweise abzuholen.

### 5.5.1 Einführung in den Kioskmodus

In der Regel registrieren Besucher Ihre Besuche oder erstellen Ihre eigenen Profile selbst an einem Computer, der im Empfangsbereich des Standortes frei zugänglich ist. Aus Sicherheitsgründen wird der Webbrowser des Computers im Kioskmodus ausgeführt, sodass nur der Zugriff auf VisMgmt möglich ist und nicht auf verschiedene Registerkarten, Browsereinstellungen oder das Betriebssystem des Computers. Alle unterstützten Browser bieten den Kioskmodus an, aber seine genaue Konfiguration hängt vom jeweiligen Browser ab. Auf dem Kioskcomputer läuft das **Bosch Peripheriegeräte-Add-on**, das physische Verbindungen zu Peripheriegeräten zum Scannen von Ausweisdokumenten und Unterschriften ermöglicht.

- Die URL für den Kioskmodus ist `https://<My_VisMgmt_server>:5706`

- Im Gegensatz hierzu ist die URL für die Anmeldung als Administrator, Empfangsmitarbeiter oder Gastgeber `https://<My_VisMgmt_server>:5706/main/`.

## 5.5.2

### Erstellen eines Besucherprofils: Selbständiges Einchecken

#### Erstmalige Besucher

Beachten Sie, dass die genaue Vorgehensweise davon abhängt, welche Peripheriegeräte, wie Dokumenten- und Unterschriftenscanner oder Fotokameras, dem Kioskcomputer zur Verfügung stehen.

1. Klicken Sie auf dem Begrüßungsbildschirm des Kioskcomputers auf **Ohne Besuchererkennung fortfahren**.
2. Klicken Sie auf dem nächsten Bildschirm auf **Selbständiges Einchecken**.
3. Wählen Sie auf dem nächsten Bildschirm die Option **Dokument scannen**.
4. Folgen Sie den Anweisungen auf dem Bildschirm in Bezug auf standortspezifische Anforderungen wie z. B.:
  - Scannen von Ausweisdokumenten
  - Unterzeichnung sonstiger erforderlicher Rechtsdokumente,
  - Aufnehmen eines Fotos.
5. Das System zeigt die erfassten Informationen an, damit Sie diese korrigieren und vervollständigen können.
6. Das System fragt, ob Sie spezielle Zutrittsberechtigungen benötigen, und gibt dies gegebenenfalls an die Rezeption weiter.
7. Am Ende des Eincheckvorgangs wird auf dem Bildschirm eine eindeutige Besuchererkennung angezeigt.  
Gehen Sie mit dieser Kennung an die Rezeption, um Ihren Besucherausweis zu erhalten.

#### Hinweis!



Ihre einzigartige Besuchererkennung

Notieren Sie Ihre Besuchererkennung sorgfältig und schützen Sie sie vor unberechtigter Verwendung. Durch sie erhalten Sie Zugang zu Ihrem Besucherprofil. Sie können sie verwenden, um sich am Kioskcomputer anzumelden und so Ihr nächstes Einchecken zu beschleunigen.

#### Wiederkehrende Besucher

1. Melden Sie sich am Kiosk mit ihrer eindeutigen Besuchererkennung an.
2. Das System zeigt die erfassten Informationen an, damit Sie diese korrigieren und gegebenenfalls vervollständigen können.
3. Gehen Sie zur Rezeption, um Ihren Besucherausweis entgegenzunehmen.

## 5.6

### Autorisierung von Installationstechnikern von mobilen Zutrittslesern

#### Einführung

Die Installationstechniker von mobilen Zutrittslesern verwenden den Bosch Setup Access 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, den 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 mobilen Zutrittslesern 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 mobilen Zutrittslesern 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.

### 5.6.1 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-Lesegeräte, die bereits für einen anderen Standort konfiguriert wurden, neu konfigurieren muss, müssen diese Lesegeräte zurückgesetzt werden.

Im Handbuch des LECTUS select-Lesegeräts finden Sie eine Beschreibung, wie Sie das Lesegerät mit Hilfe der DIP-Schalter zurücksetzen können.

## 5.7 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 den mobilen Zutritt

- Bosch Mobile Access: Eine Ausweisinhaber-App zum Speichern virtueller Anmeldedaten und zur Übertragung über Bluetooth an die Leser, die für den mobilen Zutritt konfiguriert sind. Ein solcher Leser gewährt oder verweigert dann den Zutritt, je nachdem, ob einer der gespeicherten Berechtigungen in 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.

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

#### Einführung

RSSI-Schwelle und BLE-Reichweite können im Zusammenhang mit Bosch Mobile Access als ungefähr gleichwertige Konzepte betrachtet werden.

Mobile Zutrittsgeräte senden BLE-Signale an Lesegeräte 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 das Lesegerät (R) als Aufforderung zum Betreten akzeptieren soll. Das Lesegerät 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 App Setup Access ein Tool zur Messung des RSSI des Lesegeräts 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 App Setup Access, 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 Benutzer der mobilen Berechtigungen 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-Schwellenwerts

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

**Typische Schwellenwerte (nur Richtwerte):**

Erwartete Entfernung vom mobilen Gerät zum Leser	Empfohlener RSSI-Schwellenwert
Nah (5–10 cm)	-30 ... -40 dBm
Mittel (0,5–2 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.

## FQDN

---

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

## Gastgeber

---

Im Kontext der Besucherverwaltung ist der Gastgeber der Besuchte, d. h. die Person, die den Besuch empfängt.

## Kioskmodus

---

Ein stark eingeschränkter Browser-Modus, der in der Regel nur auf eine einzelne Webanwendung zugreifen kann, nicht jedoch auf Browsereinstellungen, mehrere Registerkarten oder auf das Betriebssystem des Computers.

## Mobiler Zutritt

---

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.bosch-sicherheitssysteme.de](http://www.bosch-sicherheitssysteme.de)**

© Bosch Security Systems B.V., 2023

**Building solutions for a better life.**

202302171342