



BOSCH

Access Management System

de Installationshandbuch

Inhaltsverzeichnis

1	Über diese Dokumentation	4
2	AMS-Systemübersicht	5
3	Installation	6
3.1	Systemanforderungen	6
3.2	Serverinstallation	7
3.3	Die Firewall deaktivieren	9
3.4	Client-Installation	9
3.5	Überprüfen, ob das System installiert ist	13
3.6	Verwenden von benutzerdefinierten Zertifikaten	13
3.6.1	Voraussetzungen	13
3.6.2	Verwenden von benutzerdefinierten Zertifikaten	13
3.7	Fehlerbehebung	17
3.8	Aktualisieren des Systems	17
3.9	Deinstallieren	20
4	Technische Daten	23

1 Über diese Dokumentation

Dies ist das Hauptinstallationshandbuch für den Access Management System.

Dazugehörige Dokumentation

Folgendes ist separat dokumentiert:

- Die Konfiguration und Bedienung von AMS und seinen Hilfsprogrammen.
- Der Betrieb von AMS - Map View.

2 AMS-Systemübersicht

Access Management System ist ein leistungsfähiges, reines Zutrittskontrollsystem, das allein oder in Verbindung mit BVMS, dem Vorseige-Videomanagementsystem von Bosch, funktioniert. Seine Stärke beruht auf der einzigartigen Kombination aus führenden und bewährten Technologien:

- Konzipiert für Benutzerfreundlichkeit: praktische Benutzeroberfläche mit Drag-and-Drop-Kartenansicht und optimierten biometrischen Registrierungsdialogen.
- Konzipiert für die Datensicherheit: Unterstützung der neuesten Standards (EU-DSGVO 2018), Betriebssysteme, Datenbanken und verschlüsselten Systemschnittstellen.
- Konzipiert für hohe Stabilität: Middle Layer-Main Access Controller bieten automatisches Failover und Wiederherstellung von lokalen Zutrittskontrollzentralen bei einem Netzwerkausfall.
- Konzipiert für die Zukunft: regelmäßige Updates und eine Pipeline voller innovativer Erweiterungen.
- Konzipiert für Skalierbarkeit: Niedrige bis hohe Einstiegslevel.
- Konzipiert für Interoperabilität: RESTful APIs mit Schnittstellen zu Bosch Videomanagement, Event-Handling und spezialisierten Partnerlösungen.
- Konzipiert für Investitionsschutz: Damit können Sie Ihre installierte Hardware für die Zutrittskontrolle weiter ausbauen und gleichzeitig die Effizienz steigern.

3 Installation

Gesamtverfahren

Die Installation des Systems besteht aus zwei separaten Installationsprogrammen: dem Server und dem Client.

Die Gesamtreihenfolge der Installation lautet wie folgt:

1. Überprüfen der Systemanforderungen
2. Installieren der Software auf dem Server und Überprüfen der korrekten Installation vor dem Installieren von Clients
3. Installieren des HTTPS-Zertifikats auf dem Clientrechner
4. Installieren des Client

Siehe

- *Importieren des HTTPS-Zertifikats, Seite 9*
- *Überprüfen, ob das System installiert ist, Seite 13*

3.1 Systemanforderungen

Technische Mindestanforderungen für einen AMS-Server

Server	
Unterstützte Betriebssysteme. AMS kann möglicherweise auch auf anderen Betriebssystemen installiert werden, hierfür besteht jedoch keinerlei Garantie.	<ul style="list-style-type: none"> – Windows Server 2016(64 Bit, Standard, Datacenter) – Windows 10, version 1903 (LTSB, LTSC) – Hinweis: Die mit diesem System ausgelieferte Standard-Datenbank ist SQL Server 2017 Express Edition mit Advanced Services
Hardware-Mindestanforderungen	<ul style="list-style-type: none"> – Intel i5 Prozessor mit mindestens 4 Kernen – 8 GB RAM (32 GB empfohlen) – 200GB freier Festplattenspeicher (SSD-Datenträger empfohlen) – Grafikkarte mit <ul style="list-style-type: none"> – 256 MB RAM – einer Auflösung von 1280x1024 – mindestens 32K Farben – Ethernet-Karte mit 1 Gbit/s – Ein freier USB-Anschluss oder Netzwerkfreigabe für Installationsdateien

Technische Mindestanforderungen für einen AMS-Client

Client	
Unterstützte Betriebssysteme.	<ul style="list-style-type: none"> – Windows 10, Version 1803 (LTSB, LTSC)

Client	
AMS kann möglicherweise auch auf anderen Betriebssystemen installiert werden, hierfür besteht jedoch keinerlei Garantie.	
Hardware-Mindestanforderungen	<ul style="list-style-type: none"> - Intel i5 oder höher - 8 GB RAM (16 GB empfohlen) - 20 GB freier Festplattenspeicher - Grafikkarte mit <ul style="list-style-type: none"> - 256 MB RAM - einer Auflösung von 1920x1080 - mindestens 32K Farben - DirectX® 11 - Ethernet-Karte mit 1 Gbit/s - Ein freier USB-Anschluss oder Netzwerkfreigabe für Installationsdateien

Technische Mindestanforderungen für einen zusätzlichen MAC

MAC-Server	
Hardware-Mindestanforderungen	<ul style="list-style-type: none"> - Intel i5 oder höher - 8 GB RAM (16 GB empfohlen) - 20 GB freier Festplattenspeicher - Grafikkarte mit <ul style="list-style-type: none"> - 256 MB RAM - einer Auflösung von 1280x1024 - mindestens 32K Farben - Ethernet-Karte mit 1 Gbit/s

3.2 Serverinstallation

Vor dem Start

1. Melden Sie sich beim Serverrechner an.
2. Überprüfen Sie, ob das System bereits installiert ist (siehe **Überprüfen, ob das System installiert ist**). Wenn nicht, fahren Sie mit der Installation fort.
3. Kopieren Sie das Installationspaket auf Ihren Serverrechner.

Mit der Serverinstallation beginnen

1. Doppelklicken Sie auf das Software-Installationspaket.
2. Doppelklicken Sie auf **Server**.
3. Wählen Sie **AMS Server Setup.exe** mit einem Rechtsklick aus und wählen Sie dann **Run as administrator** (Als Administrator ausführen) aus dem Kontextmenü aus.
 - Der Preparation Wizard wird geöffnet. Befolgen Sie die Schritte des Preparation Wizard.
4. Wählen Sie die erforderlichen Komponenten aus, die installiert werden sollen, und klicken Sie auf **Next>** (Weiter>).

- Je nachdem, was bereits installiert ist, zeigt der Assistent eine Liste der Software an, die installiert werden muss:
- Wenn es nicht obligatorische Komponenten gibt, die nicht benötigt werden, heben Sie ihre Auswahl an dieser Stelle auf.
- 5. Lesen Sie die **Bedingungen des Endbenutzer-Lizenzvertrags** und klicken Sie auf **Accept** (Akzeptieren), um fortzufahren. Wenn Sie nicht einverstanden sind, klicken Sie auf **Decline** (Ablehnen), um die Installation abzubrechen.
- 6. Geben Sie die Konfigurationsdaten für den SQL Database Server ein.
 - SQL Database Server-Konfigurationsdaten:
 - SQL Server: Der Name des Hosts, auf dem die SQL Server-Instanz ausgeführt wird. Es wird empfohlen, den lokalen Rechner zu verwenden.
 - SQL-Instanz: Der SQL-Instanzname
 - AMS-Datenbank: Der Name der Datenbank
 - SQL-Benutzername: Die SQL-Anmeldung
 - SQL-Passwort: Das SQL-Passwort für die SQL-Anmeldung. Das **Standardpasswort lautet: sa_s3k_pw**
- 7. Nachdem Sie das SQL-Passwort eingegeben haben, klicken Sie auf **Test Server** (Server testen).
 - Wenn der Test erfolgreich ist, wird eine Nachricht mit einem grünen Hintergrund unter dem SQL-Passwortfeld angezeigt.
- 8. Klicken Sie auf **Next>** (Weiter>).
- 9. Wenn der Standardinstallationspfad für den Server akzeptabel ist, klicken Sie auf **Next>** (Weiter>). Wenn Sie einen anderen Installationspfad auswählen möchten (nur lokale Laufwerke), klicken Sie auf **Browse** (Durchsuchen).
 - Der Standardinstallationspfad `C:\Program Files` wird empfohlen, da die Dateien nur von Systemadministratoren geändert werden können.
 - Wenn Sie einen anderen Installationspfad auswählen, stellen Sie sicher, dass der Pfad ausreichend vor unberechtigtem Zutritt geschützt ist.
- 10. Klicken Sie zum Fortfahren auf **Next>** (Weiter>).
 - Auf dieser Seite wird der API-Hostname konfiguriert.
 - Der Servername darf nicht länger als **16** Zeichen sein. Der Standardwert (empfohlen) ist der Hostname des aktuellen Computers, auf dem das Installationsprogramm ausgeführt wird.
- 11. Überprüfen Sie die Zusammenfassung vor der Installation, und klicken Sie auf **Install** (Installieren).
 - Eine Zusammenfassung mit allen Komponenten, die Sie installieren möchten, wird angezeigt.
- 12. Beachten Sie die Fortschrittsleiste der Installation.
 - Sobald die sich bewegende grüne Leiste ungefähr die Mitte der Fortschrittsleiste erreicht, dauert es einige Minuten, bis sie sich wieder bewegt. Bitte warten Sie.
 - Ein weiteres Dialogfeld bezüglich der Access Engine-Datenbankeinrichtung (ACE) wird geöffnet. Diese Einrichtung aktualisiert die ACE-Datenbank. Wenn die Datenbank bereits installiert ist, wird sie aktualisiert. Andernfalls wird eine neue Datenbank erstellt. Dies kann einige Minuten dauern. Warten Sie, bis das Dialogfeld geschlossen wird.
- 13. Wenn der Vorgang abgeschlossen ist, klicken Sie auf **Next> (Weiter>)** und überprüfen Sie die Zusammenfassung nach der Installation.
 - Es wird eine Zusammenfassung mit allen installierten Komponenten angezeigt.
- 14. Klicken Sie auf **Finish** (Fertigstellen), um die Installation abzuschließen.

- Ein Dialogfeld, das einen Neustart anfordert, wird geöffnet. Sie müssen den Computer neu starten, um die Installation des Systems abzuschließen.
- 15. Klicken Sie auf **Yes** (Ja), um den PC neu zu starten.
- Der PC wird neu gestartet.
- 16. Überprüfen Sie, ob das System korrekt installiert ist (siehe **Überprüfen, ob das System installiert ist**).
- Falls ja, ist die Erstinstallation der Systemanwendung abgeschlossen. Ein Symbol für das System wird auf dem Desktop angezeigt.

Erstmaliges Anmelden

1. Doppelklicken Sie auf das Anwendungssymbol des Systems auf Ihrem Desktop.
2. Geben Sie den Standardbenutzernamen und das Standardkennwort ein.
 - Standardbenutzername und -passwort lauten **Administrator**. Beim Passwort (jedoch nicht beim Benutzernamen) wird zwischen Groß- und Kleinschreibung unterschieden.
3. Klicken Sie auf **Log in** (Einloggen).
 - Ein Dialogfeld mit der Aufforderung zum Ändern des Passworts wird angezeigt.
 - Bei der ersten Anmeldung müssen Sie das Passwort im Popup-Dialogfeld ändern.
4. Klicken Sie zum Anmelden auf **OK**.

Siehe

- *Überprüfen, ob das System installiert ist, Seite 13*
- *Das Serverupdate starten, Seite 18*

3.3 Die Firewall deaktivieren

Deaktivieren Sie nach erfolgreicher Installation des Servers und vor der Installation von Client-Dialogstationen die Firewall. Dadurch können Client-Dialogstationen und externe MAC-Computer während der Erstkonfiguration problemlos eine Verbindung zum Server herstellen.

3.4 Client-Installation

HTTPS-Zertifikat für Client

Der Server des Systems hostet mehrere APIs, nämlich: Access API, Map API und States API. Diese APIs kommunizieren über HTTPS und verwenden ein selbstsigniertes Zertifikat, um Vertrauen aufzubauen. Das selbstsignierte Zertifikat wird vom Server-Installationsprogramm erstellt und auf dem Serverrechner installiert.

Der Map-Client verwendet diese APIs, um ordnungsgemäß zu funktionieren, und erfordert daher, dass der Clientrechner den APIs vertraut. Um dies zu ermöglichen, muss ein Zertifikat vom Server kopiert und manuell auf den Clientrechner importiert werden (siehe **Importieren des HTTPS-Zertifikats**).

Importieren des HTTPS-Zertifikats

1. Gehen Sie zu `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates\Access Management System Internal CA.cer`
2. Kopieren Sie das Zertifikat auf den Clientrechner.
3. Doppelklicken Sie auf dem Clientrechner auf das Zertifikat.
 - Ein Zertifikat-Dialogfeld wird angezeigt.
4. Klicken Sie auf **Install Certificate** (Zertifikat installieren).
 - Der Zertifikats-Importassistent wird geöffnet.

5. Wählen **Local Machine** (Lokaler Rechner) (empfohlen) und klicken Sie auf **Next>** (Weiter>).
6. Wählen Sie **Place all certificates in the following store** (Alle Zertifikate im folgenden Speicher platzieren), um einen Speicherort für das Zertifikat anzugeben (empfohlen).
7. Klicken Sie auf **Browse** (Durchsuchen).
 - Ein Dialogfeld zum Auswählen des Zertifikatspeichers wird geöffnet.
8. Wählen Sie `Trusted Root Certification Authorities` aus und klicken Sie auf **OK** (empfohlen).
 - Das Dialogfeld zum Auswählen des Zertifikatspeichers wird geschlossen.
9. Klicken Sie auf **Next>** (Weiter>) im Zertifikats-Importassistenten.
10. Klicken Sie auf **Finish** (Fertigstellen), um das Zertifikat zu importieren.
 - Der Zertifikat-Importprozess ist abgeschlossen.

**Hinweis!**

Wenn das HTTPS-Zertifikat nicht installiert ist, kann die Anwendung nicht gestartet werden.

Beachten Sie, dass Sie das Zertifikat nicht auf den Serverrechner importieren müssen, da dies während der Serverinstallation automatisch erfolgt. Dies gilt nur für separate Client-Dialogstationen.

Access API-Integration mit BVMS

Um die AMS Access API in das BVMS (Bosch Video Management System) – Version 9.1 oder höher – zu integrieren, importieren Sie das im letzten Abschnitt beschriebene Zertifikat in den BVMS-Rechner (siehe **Importieren des HTTPS-Zertifikats**).

Unterstütztes Betriebssystem

Das unterstützte Betriebssystem für den Client ist **Windows 10, Version 1803 (LTSC, LTSC)**.

**Hinweis!**

Die Installation des Client außerhalb dieses Bereichs kann zu Kompatibilitätsproblemen führen.

Die Client-Installation starten

1. Doppelklicken Sie auf das Software-Installationspaket.
2. Doppelklicken Sie auf **Client**.
3. Doppelklicken Sie auf **AMS Client Setup.exe**.
 - Der Preparation Wizard wird geöffnet. Befolgen Sie die Schritte des Preparation Wizard.
4. Wählen Sie die Komponenten aus, die Sie installieren möchten, und klicken Sie auf **Next>** (Weiter>).
 - Je nach bereits verfügbarer Software markiert der Assistent die folgende verpflichtende, erforderliche Software:
 - Microsoft Visual C++ 2010 Redistributable

- Microsoft Visual C++ 2015 Redistributable
- Microsoft Visual C++ 2017 Redistributable
- .NET 4.8
- Optionale Komponenten:
 - Client
 - Kartenansicht
- Sie können für jede optionale Komponente auswählen, ob sie installiert oder übersprungen werden soll.
- 5. Lesen Sie die **Bedingungen des Endbenutzer-Lizenzvertrags** und klicken Sie auf **Accept** (Akzeptieren), um fortzufahren. Wenn Sie nicht einverstanden sind, klicken Sie auf **Decline** (Ablehnen), um zurückzugehen und den Vorgang abzubrechen.
- 6. Wenn der Standardinstallationspfad für die Client-Dialogstation akzeptabel ist, klicken Sie auf **Next>** (Weiter>). Wenn Sie einen anderen Installationspfad auswählen möchten (nur lokale Laufwerke), klicken Sie auf **Browse** (Durchsuchen).
- 7. Geben Sie die Serveradresse ein. Adressformat: Hostname:4999/tcp
 - Standardmäßig installiert der Installationsassistent den System-Client auf dem lokalen Laufwerk `C:/Program Files` (empfohlen).
 - Dateien, die unter dem lokalen Laufwerk `C:/Program Files` installiert sind, können nur von Benutzern mit Administratorrechten geändert werden. Dies bietet Sicherheit, indem sichergestellt wird, dass Benutzer ohne Administratorrechte keine mit dem System verbundenen Dateien ändern können.
 - Wenn Sie einen anderen Installationspfad wählen möchten, gehen die angebotenen Vorteile verloren.
- 8. Wenn der Standardinstallationspfad für die Kartenansicht-Anwendung akzeptabel ist, klicken Sie auf **Next>** (Weiter>).
- 9. Wenn Sie einen anderen Installationspfad auswählen möchten (nur lokale Laufwerke), klicken Sie auf **Browse** (Durchsuchen).
- 10. Geben Sie die Erkennungsadresse ein.
 - Standardmäßig installiert der Installationsassistent die Kartenansicht-Anwendung auf dem lokalen Laufwerk `C:/Program Files` (empfohlen).
 - Die Kartenansicht-Anwendung stellt eine Verbindung zur Ermittlungsadresse her, um die Endpunkte des Systems zu ermitteln. Diese Adresse ist eine URL, die den Servernamen und die Portnummer enthält, auf der der Erkennungsendpunkt gehostet wird.
- 11. Überprüfen Sie die Zusammenfassung vor der Installation und klicken Sie auf **Install** (Installieren).
 - Eine Zusammenfassung mit allen Komponenten, die Sie installieren möchten, wird angezeigt.
- 12. Beachten Sie die Fortschrittsleiste der Installation.
 - Warten Sie, bis der Vorgang abgeschlossen ist.
- 13. Wenn der Vorgang abgeschlossen ist, klicken Sie auf **Next> (Weiter>)** und überprüfen Sie die Zusammenfassung nach der Installation.
 - Es wird eine Zusammenfassung mit allen installierten Komponenten angezeigt.
- 14. Klicken Sie auf **Finish** (Fertigstellen), um die Installation abzuschließen.
- 15. Starten Sie Ihren PC neu (empfohlen).
- 16. Überprüfen Sie, ob das System installiert ist (siehe **Überprüfen, ob das System installiert ist**).

- Ist dies der Fall, ist die Installation des Clients und der Kartenansicht (optional) abgeschlossen. Beide Client-Anwendungssymbole werden auf dem Desktop angezeigt. Standardbenutzername und -passwort lauten **Administrator**. Beim Passwort (jedoch nicht beim Benutzernamen) wird zwischen Groß- und Kleinschreibung unterschieden.

Vor dem Start des Client

Bevor Sie sich beim Client anmelden, müssen Sie die Client-Dialogstation auf dem Server konfigurieren. Gehen Sie wie folgt vor:

1. Starten Sie den Client auf dem Serverrechner.
2. Klicken Sie auf **Configuration>Device Data** (Konfiguration>Gerätedaten).
 - Ein neues Dialogfeld wird geöffnet.
3. Wählen Sie in der oberen Symbolleiste das Symbol **Workstations** (Dialogstationen) aus.
4. Wählen Sie in der oberen Symbolleiste das Symbol **New** (Neu) aus.
5. Füllen Sie auf der Registerkarte "Workstation" (Dialogstation) die leeren Felder aus.
 - Die Felder:
 - Name: Geben Sie den Hostnamen der Client-Dialogstation ein (obligatorisch)
 - Beschreibung: Fügen Sie eine Beschreibung ein (optional)
 - Login über Leser: Führen Sie die Anmeldung über den Leser durch (optional)
 - Automatische Abmeldung nach: X Sekunden (optional). Legen Sie eine automatische Abmeldung fest, wenn die Anwendung nach einer bestimmten Zeit automatisch abgemeldet werden soll
 - Beachten Sie, dass die unterstrichenen Felder obligatorisch sind.
6. Klicken Sie in der oberen Symbolleiste auf das Symbol **Save** (Speichern), um die Änderungen zu speichern.
 - Sie können sich jetzt erfolgreich von der Client-Dialogstation aus anmelden.

Anmelden zum ersten Mal

1. Doppelklicken Sie auf das Systemanwendungssymbol auf Ihrem Desktop.
2. Geben Sie den Standardbenutzernamen und das Standardkennwort ein.
 - Standardbenutzername und -passwort für beide Client-Anwendungen lautet **Administrator**. Beim Passwort (jedoch nicht beim Benutzernamen) wird zwischen Groß- und Kleinschreibung unterschieden.
3. Klicken Sie auf **Log on** (Anmelden).
 - Ein Dialogfeld mit der Aufforderung zum Ändern des Passworts wird angezeigt.
 - Bei der ersten Anmeldung müssen Sie das Passwort ändern.
4. Klicken Sie auf **OK**, um im nächsten Dialogfeld ein neues Passwort einzugeben.
5. Geben Sie Ihr neues Passwort ein und klicken Sie auf **Change** (Ändern). Klicken Sie auf **Cancel** (Abbrechen), um die Passwortänderung abzubrechen.
 - Ein Dialogfeld zur Bestätigung der Passwortänderung wird angezeigt.
6. Klicken Sie zum Anmelden auf **OK**.



Hinweis!

Sowohl der Server als auch der Client müssen in derselben Version installiert sein. Versuchen Sie nicht, mit einer anderen Clientversion auf den Server zuzugreifen.

Siehe

- *Überprüfen, ob das System installiert ist, Seite 13*
- *Importieren des HTTPS-Zertifikats, Seite 9*

3.5 Überprüfen, ob das System installiert ist

Überprüfen, ob das System installiert ist

Das System wird installiert, wenn:

- Die Symbole des Systems sind auf dem Desktop sichtbar.
- Die folgenden Services sind in der Windows Services-Anwendung enthalten (**Start > Search** (Suchen) > `service.msc`): DMS, MAC Access PI, Identity service, MAP API, State API.
- Das System befindet sich im Standardinstallationspfad: `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\`

3.6 Verwenden von benutzerdefinierten Zertifikaten

AMS-APIs können so konfiguriert werden, dass sie unterschiedliche Zertifikate verwenden, anstatt die selbstsignierten Zertifikate zu verwenden, die während der Einrichtung automatisch erstellt werden.

Dies ist nützlich, wenn eine Organisation bereits über eine Public-Key-Infrastruktur (PKI) mit einer eigenen Zertifizierungsstelle verfügt.

3.6.1 Voraussetzungen

- Sie benötigen eine vertrauenswürdige Root-Zertifikatsdatei.
- Die öffentlichen und privaten Teile des Zertifikats müssen im AMS-Serververzeichnis `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates` abgelegt werden

Beispiele für öffentliche und private Teile eines Zertifikats:

- `Access Management System Test CA.cer` (öffentlicher Teil)
- `CustomRootTestCA.pfx` (privater Teil)

3.6.2 Verwenden von benutzerdefinierten Zertifikaten

Eine PowerShell-Sitzung öffnen

Öffnen Sie eine PowerShell-Sitzung auf dem AMS-Server im Verzeichnis `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates`

Die installierten Zertifikate entfernen

1. Entfernen Sie die Zertifikate, die während der AMS-Installation installiert wurden.
2. Ausführen: `"RemoveAceApiCertificates.ps1"` in der geöffneten PowerShell-Sitzung.

Das Skript für die Erstellung von API-Zertifikaten bearbeiten

1. Öffnen Sie die PowerShell-Datei `"CreateAceApiCertificatesFromOwnRoot.ps1"` in einem Texteditor und benennen Sie die folgenden Dateien in Ihre Dateinamen um:
 - `CustomRootTestCA.pfx`
 - 2. `Access Management System Test CA.cer`
 - Beachten Sie, dass die Dateinamen nur einmal im Skript angezeigt werden.
 - 3. Speichern Sie die Änderungen.

Das Skript für die Erstellung von API-Zertifikaten ausführen

1. Ausführen: "CreateAceApiCertificatesFromOwnRoot.ps1" in der PowerShell-Sitzung, die Sie in Schritt 1 geöffnet haben.
2. Geben Sie das Passwort für das private Zertifikat ein.
 - Die folgenden Sub-API-Zertifikate wurden erstellt und installiert:
 - Access Management System-Zugriffs-API
 - Access Management System-Identity Server
 - Access Management System-Map API
 - Access Management System-States API
 - Das Root-Zertifikat ist installiert.

Die Installation der Zertifikate in Windows-Zertifikaten für den aktuellen Benutzer und den lokalen Computer überprüfen

Das Zertifikat wird installiert, wenn:

- Das Root-Zertifikat ist unter Current User Personal Certificates, Trusted Root Certificates und unter Local Computer Trusted Root Certificates installiert
- Die API-Zertifikate sind unter Local Computer Personal Certificates installiert

Die Thumbprint-App-Einstellungen für jede API aktualisieren

Für jede API muss der Fingerabdruck aktualisiert werden.

Access API	<ol style="list-style-type: none"> 1. Öffnen Sie C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Access API 2. Tausche die Werte in der Datei appsettings.json, Zeile "Thumbprint" aus: 3. Öffnen Sie Certificates Local Computer (Zertifikate Lokaler Computer) > Personal (Persönlich) > Certificates (Zertifikate) > Friendly Name (Freundlicher Name): Access Management System Access API 4. Wählen und öffnen Sie das installierte Zertifikat "Access Management System Access API" > Details 5. Scrollen Sie in der Liste nach unten zu "Thumbprint" 6. Wählen Sie Thumbprint. 7. Kopieren Sie den angezeigten Fingerabdruck (z. B. "da"). 8. Fügen Sie den Fingerabdruck ohne Leerzeichen in die appsettings.json-Datei unter C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Access API ein <ul style="list-style-type: none"> - (z. B. "Thumbprint": "53d3588285bd570c9799e883b27ef1b139ba28da")
------------	--

Map API	<ol style="list-style-type: none"> 1. Öffnen Sie C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Map API
---------	--

	<ol style="list-style-type: none"> 2. Tausche die Werte in der Datei <code>appsettings.json</code>, Zeile <code>"Thumbprint"</code> aus: 3. Öffnen Sie Certificates Local Computer (Zertifikate Lokaler Computer) > Personal (Persönlich) > Certificates (Zertifikate) > Friendly Name (Freundlicher Name): Access Management System Map API 4. Wählen und öffnen Sie das installierte Zertifikat "Access Management System Map API"> Details 5. Scrollen Sie in der Liste nach unten zu "Thumbprint". 6. Wählen Sie Thumbprint. 7. Kopieren Sie den angezeigten Fingerabdruck (z. B. "e8"). 8. Fügen Sie den Fingerabdruck ohne Leerzeichen in die <code>appsettings.json</code>-Datei unter <code>C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Map API</code> ein – (z. B. <code>"Thumbprint": "3cef0c43be36ee01d8a6ea2f59f170cde96168e8"</code>)
--	--

States API	<ol style="list-style-type: none"> 1. Öffnen Sie <code>C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\States API</code> 2. Tausche die Werte in der Datei <code>appsettings.json</code>, Zeile <code>"Thumbprint"</code> aus: 3. Öffnen Sie Certificates Local Computer (Zertifikate Lokaler Computer) > Personal (Persönlich) > Certificates (Zertifikate) > Friendly Name (Freundlicher Name):Access Management System States API 4. Wählen und öffnen Sie das installierte Zertifikat "Access Management System States API"> Details 5. Scrollen Sie in der Liste nach unten zu "Thumbprint". 6. Wählen Sie Thumbprint. 7. Kopieren Sie den angezeigten Fingerabdruck (z. B. "e2"). 8. Fügen Sie den Fingerabdruck ohne Leerzeichen in die <code>appsettings.json</code>-Datei unter <code>C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\States API</code> ein – (z. B. <code>"Fingerabdruck": "37c0bb09d4cab985b620da1c667597ef43b5f8e2"</code>)
------------	---

Identity Server:	<ol style="list-style-type: none"> 1. Öffnen Sie <code>C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Identity Server</code> 2. Tausche die Werte in der Datei <code>appsettings.json</code>, Zeile <code>"Thumbprint"</code> aus:
------------------	--

3. Öffnen Sie **Certificates Local Computer (Zertifikate Lokaler Computer) > Personal (Persönlich) > Certificates (Zertifikate) > Friendly Name (Freundlicher Name):**Access Management System Identity Server
4. Wählen und öffnen Sie das installierte Zertifikat "Access Management Identity Server"> **Details**
5. Scrollen Sie in der Liste nach unten zu "Thumbprint".
6. Wählen Sie Thumbprint.
7. Kopieren Sie den angezeigten Fingerabdruck.
8. Fügen Sie den Fingerabdruck ohne Leerzeichen in die appsettings.json-Datei unter C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Identity Server ein
9. Fügen Sie die Fingerabdrücke der anderen APIs auch in die entsprechenden Fingerabdruck-Eingabefelder in dieser Datei ein.
 - Beispiel:
 - Für "Name": "AccessApi"


```
"Thumbprint":
"53d3588285bd570c9799e883b27ef1b139ba28da"
```
 - Für "Name": "MapApi"


```
"Thumbprint":
"3cef0c43be36ee01d8a6ea2f59f170cde96168e8"
```
 - Für "Name": "StatesApi"


```
"Thumbprint":
"37c0bb09d4cab985b620da1c667597ef43b5f8e2"
```

Dienste stoppen und starten

1. Öffnen Sie Windows-Dienste.
2. Klicken Sie mit der rechten Maustaste auf die folgenden Dienste und wählen Sie nach jeder dieser Optionen "Stop" (Stopp) aus:
 - Access Management System-Zugriffs-API
 - Access Management System-Identity Server
 - Access Management System-Map API
 - Access Management System-States API
 - Nachdem alle vier Dienste beendet wurden, klicken Sie erneut mit der rechten Maustaste auf die gleichen Dienste und wählen Sie nach jedem von ihnen **Start** (Starten).

Installieren des Root-Zertifikats auf dem Clientrechner

1. Verwenden Sie Windows File Manager, um Ihr Root-Zertifikat "Access Management System Test CA.cer" zu kopieren und es in den Clientrechner einzufügen, auf dem die Client-Anwendung "Map View" und "AMS" (Dialog Manager) installiert sind. Fügen Sie es zum Beispiel in den Downloads-Ordner ein.
2. Installieren Sie das Root-Zertifikat:

- Klicken Sie im File Manager mit der rechten Maustaste auf **certificate file** (Zertifikatsdatei) und wählen Sie **Install Certificate (Zertifikat installieren) > Current User (Aktueller Benutzer) > Next (Weiter) > Wählen Sie "Place all certificates in the following store" (Alle Zertifikate im folgenden Speicher platzieren) > Browse (Durchsuchen) > Wählen Sie "Trusted Root Certification Authorities" (Vertrauenswürdige Root-Zertifizierungsstellen) > Next (Weiter) > Finish (Fertigstellen) > OK**

Testen Sie die API-Zertifikate auf dem Clientrechner.

Die API-Zertifikate müssen auf dem Clientrechner getestet werden, auf dem die Client-Anwendung Kartenansicht und AMS (Dialog Manager) installiert sind.

Starten Sie auf dem Clientrechner den Google Chrome-Browser.

- Geben Sie die folgende Adresse ein, um den Identity Server zu testen: `https://[ServerHostname]:44333/.well-known/openid-configuration`
 - Klicken Sie mit der rechten Maustaste auf die Website-Informationen Sperren-Symbol > Verify "Certificate (Valid)" ("Zertifikat (Gültig)" überprüfen) und prüfen Sie, ob das korrekte Zertifikat unter "Issued by" (Ausgestellt von) verwendet wird
- Geben Sie die folgende Adresse ein, um die Access API zu testen: `https://[ServerHostname]:44347/swagger`
 - Klicken Sie mit der rechten Maustaste auf die Website-Informationen Sperren-Symbol > Verify "Certificate (Valid)" ("Zertifikat (Gültig)" überprüfen) und prüfen Sie, ob das korrekte Zertifikat unter "Issued by" (Ausgestellt von) verwendet wird
- Geben Sie die folgende Adresse ein, um die States API zu testen: `https://[ServerHostname]:62901/swagger`
 - Klicken Sie mit der rechten Maustaste auf die Website-Informationen Sperren-Symbol > Verify "Certificate (Valid)" ("Zertifikat (Gültig)" überprüfen) und prüfen Sie, ob das korrekte Zertifikat unter "Issued by" (Ausgestellt von) verwendet wird.
- Geben Sie die folgende Adresse ein, um die Map API zu testen: `https://[ServerHostname]:61801/odata/$metadata`
 - Klicken Sie mit der rechten Maustaste auf die Website-Informationen Sperren-Symbol > Verify "Certificate (Valid)" ("Zertifikat (Gültig)" überprüfen) und prüfen Sie, ob das korrekte Zertifikat unter "Issued by" (Ausgestellt von) verwendet wird

Verwenden Sie das Zertifikat in AMS.

Starten Sie die Anwendung "Kartenansicht" auf dem Clientrechner und melden Sie sich an.

3.7 Fehlerbehebung

Wenn die Installation fehlschlägt, wird die Fortschrittsanzeige in Rot angezeigt. Ggf. wird zusätzlicher Fehlertext angezeigt.

Klicken Sie auf **Next>** (Weiter>), um zur Übersichtsseite zu gelangen, auf der angezeigt wird, welche Komponente fehlgeschlagen ist.

3.8 Aktualisieren des Systems

Vor dem Start

1. Melden Sie sich beim Serverrechner an.
2. Überprüfen Sie, ob die vorherige Version des Systems installiert ist (siehe **Überprüfen, ob das System installiert ist**).
3. Kopieren Sie das neue Installationspaket auf Ihren Serverrechner.



Hinweis!

Sowohl der Server als auch der Client müssen in derselben Version installiert sein. Versuchen Sie nicht, mit einer anderen Clientversion auf den Server zuzugreifen.

Das Serverupdate starten

1. Doppelklicken Sie auf die neue Version des Software-Installationspakets.
2. Wählen Sie die Sprache der Benutzeroberfläche.
3. Doppelklicken Sie auf **Server**.
4. Wählen Sie **AMS Server Setup.exe** mit einem Rechtsklick aus und wählen Sie dann **Run as administrator** (Als Administrator ausführen) aus dem Kontextmenü aus.
 - Der Preparation Wizard wird geöffnet.
 - Wählen Sie die Komponenten aus, die Sie aktualisieren möchten, und klicken Sie auf **Next>** (Weiter>).
 - Je nachdem, was bereits verfügbar ist, markiert der Assistent die Komponenten, die standardmäßig aktualisiert werden können.
 - Sie können auswählen, ob die Aktualisierung von Komponenten aktualisiert oder übersprungen werden soll.
 - Komponenten, die nicht aktualisiert werden können, werden standardmäßig als **Skip** (Überspringen) markiert.
5. Lesen Sie die **Bedingungen des Endbenutzer-Lizenzvertrags** und klicken Sie auf **Accept** (Akzeptieren), um fortzufahren. Wenn Sie nicht einverstanden sind, klicken Sie auf **Decline** (Ablehnen), um zurückzugehen und den Vorgang abzubrechen.
6. Geben Sie die Konfigurationsdaten für den SQL Database Server ein.
 - SQL Database Server-Konfigurationsdaten:
 - SQL Server: Der Hostname, unter dem die SQL Server-Instanz ausgeführt wird, d. h. der lokale Rechner (empfohlen)
 - SQL-Instanz: Der SQL-Instanzname
 - AMS-Datenbank: Der Name der Datenbank
 - SQL-Benutzername: Die SQL-Anmeldung
 - SQL-Passwort: Das SQL-Passwort für die SQL-Anmeldung. Das Standardpasswort ist: `sa_s3k_pw`
7. Nachdem Sie das SQL-Passwort eingegeben haben, klicken Sie auf **Test Server** (Server testen).
 - Wenn der Test erfolgreich ist, wird eine Nachricht mit einem grünen Hintergrund unter dem SQL-Passwortfeld angezeigt.
 - Wenn die Datenbank bereits vorhanden ist, wird eine Migration versucht.
8. Klicken Sie auf **Next>** (Weiter>).
 - Der nächste Dialog zeigt den Installationspfad, in dem der Server des Systems aufbewahrt wird.
 - Standardmäßig installiert der Installationsassistent den Server des Systems im lokalen Laufwerk `C:\Program Files` (empfohlen).

- Dateien, die unter dem lokalen Laufwerk `C:\Program Files` installiert sind, können nur von Benutzern mit Administratorrechten geändert werden. Dies bietet Sicherheit, indem sichergestellt wird, dass Benutzer ohne Administratorrechte keine mit dem System verbundenen Dateien ändern können.
- 9. Klicken Sie zum Fortfahren auf **Next>** (Weiter>).
- 10. Überprüfen Sie die Zusammenfassung vor der Aktualisierung und klicken Sie auf **Install** (Installieren).
- Eine Zusammenfassung mit allen Komponenten, die Sie aktualisieren möchten, wird angezeigt.
- 11. Beachten Sie die Fortschrittsleiste der Installation.
 - Sobald die sich bewegende grüne Leiste ungefähr die Mitte der Fortschrittsleiste erreicht, dauert es einige Minuten, bis sie sich wieder bewegt. Bitte warten Sie.
 - Ein weiteres Dialogfeld bezüglich der Access Engine-Datenbankeinrichtung (ACE) wird geöffnet. Diese Einrichtung aktualisiert die ACE-Datenbank. Wenn die Datenbank bereits installiert ist, wird sie aktualisiert. Andernfalls wird eine neue Datenbank erstellt. Dies kann einige Minuten dauern. Warten Sie, bis das Dialogfeld geschlossen wird.
- 12. Wenn der Vorgang abgeschlossen ist, klicken Sie auf **Next> (Weiter>)** und überprüfen Sie die Zusammenfassung nach der Aktualisierung.
 - Es wird eine Zusammenfassung mit allen aktualisierten Komponenten angezeigt.
- 13. Klicken Sie auf **Finish** (Fertigstellen), um die Installation der aktualisierten Version des Systems abzuschließen.
- 14. Starten Sie den PC neu (empfohlen).
 - Der PC wird neu gestartet.
- 15. Überprüfen Sie, ob das System installiert ist (siehe **Überprüfen, ob das System installiert ist**).
 - Ist dies der Fall, ist die Installation der aktualisierten Version der Systemanwendung abgeschlossen.
 - Standardbenutzername und -passwort lauten **Administrator**. Beim Passwort (jedoch nicht beim Benutzernamen) wird zwischen Groß- und Kleinschreibung unterschieden.

Das Client-Update starten

1. Doppelklicken Sie auf die neue Version des Software-Installationspakets.
2. Wählen Sie die Sprache der Benutzeroberfläche.
3. Doppelklicken Sie auf **Client**.
4. Wählen Sie **AMS Client Setup.exe** mit einem Rechtsklick aus und wählen Sie dann **Run as administrator** (Als Administrator ausführen) aus dem Kontextmenü aus.
 - Der Preparation Wizard wird geöffnet.
 - Wählen Sie die Komponenten aus, die Sie aktualisieren möchten, und klicken Sie auf **Next>** (Weiter>).
 - Je nachdem, was bereits verfügbar ist, markiert der Assistent die Komponenten, die standardmäßig aktualisiert werden können.
 - Sie können auswählen, ob die Aktualisierung von Komponenten aktualisiert oder übersprungen werden soll:
 - Komponenten, die nicht aktualisiert werden können, werden standardmäßig als **Skip** (Überspringen) markiert.
5. Lesen Sie die **Bedingungen des Endbenutzer-Lizenzvertrags** und klicken Sie auf **Accept** (Akzeptieren), um fortzufahren. Wenn Sie nicht einverstanden sind, klicken Sie auf **Decline** (Ablehnen), um zurückzugehen und den Vorgang abubrechen.

- Der nächste Dialog zeigt den Installationspfad, in dem der Client des Systems aufbewahrt wird.
- Standardmäßig installiert der Installationsassistent den Client des Systems im lokalen Laufwerk `C:\Program Files` (empfohlen).
- Dateien, die unter dem lokalen Laufwerk `C:\Program Files` installiert sind, können nur von Benutzern mit Administratorrechten geändert werden. Dies bietet Sicherheit, indem sichergestellt wird, dass Benutzer ohne Administratorrechte keine mit dem System verbundenen Dateien ändern können.
- 6. Geben Sie die Serveradresse ein. Adressformat: `Hostname:4999/tcp`
- 7. Klicken Sie zum Fortfahren auf **Next>** (Weiter>).
 - Der nächste Dialog zeigt den Installationspfad, in dem die Anwendung "Kartenansicht" des Systems aufbewahrt wird.
 - Standardmäßig installiert der Installationsassistent die Kartenansicht-Anwendung des Systems im lokalen Laufwerk `C:\Program Files` (empfohlen).
- 8. Geben Sie die Erkennungsadresse ein.
 - Die Kartenansicht-Anwendung stellt eine Verbindung zur Ermittlungsadresse her, um die Endpunkte des Systems zu ermitteln. Diese Adresse ist eine URL, die den Servernamen und die Portnummer enthält, auf der der Erkennungsendpunkt gehostet wird.
- 9. Überprüfen Sie die Zusammenfassung vor der Aktualisierung und klicken Sie auf **Install** (Installieren).
 - Eine Zusammenfassung mit allen Komponenten, die Sie aktualisieren möchten, wird angezeigt.
- 10. Beachten Sie die Fortschrittsleiste der Installation.
 - Warten Sie, bis der Vorgang abgeschlossen ist.
- 11. Wenn der Vorgang abgeschlossen ist, klicken Sie auf **Next> (Weiter>)** und überprüfen Sie die Zusammenfassung nach der Aktualisierung.
 - Es wird eine Zusammenfassung mit allen aktualisierten Komponenten angezeigt.
- 12. Klicken Sie auf **Finish** (Fertigstellen), um die Installation der aktualisierten Version des Systems abzuschließen.
- 13. Starten Sie den PC neu (empfohlen).
 - Der PC wird neu gestartet.
- 14. Überprüfen Sie, ob das System installiert ist (siehe **Überprüfen, ob das System installiert ist**).
 - Ist dies der Fall, ist die Installation der aktualisierten Version der Systemanwendung abgeschlossen.
 - Standardbenutzername und -passwort lauten **Administrator**. Beim Passwort (jedoch nicht beim Benutzernamen) wird zwischen Groß- und Kleinschreibung unterschieden.

Siehe

- *Überprüfen, ob das System installiert ist, Seite 13*

3.9

Deinstallieren

Führen Sie die folgenden Schritte aus, um die Software des Systems vollständig zu deinstallieren:

Den Server deinstallieren

1. Klicken Sie auf die Windows-Schaltfläche **Start**.

2. Suchen Sie **Control Panel** (Systemsteuerung) und doppelklicken Sie darauf, um sie zu öffnen.
3. Folge dem Pfad: **Programms** (Programme) > **Programms and Features** (Programme und Funktionen) > **Uninstall a program** (Ein Programm deinstallieren)
 - Eine Liste der installierten Programme wird geöffnet.
4. Klicken Sie mit der rechten Maustaste auf **Access Management System - Server** und wählen Sie **Uninstall** (Deinstallieren) aus dem Kontextmenü.
 - Der Deinstallationsassistent des Systems wird geöffnet.
5. Wählen Sie die Komponenten aus, die Sie deinstallieren möchten, und klicken Sie auf **Next>** (Weiter>). Klicken Sie auf **Cancel** (Abbrechen), um den Vorgang abzubrechen.
 - Sie können wählen, ob Komponenten deinstalliert oder übersprungen werden sollen. Die meisten Komponenten sind obligatorisch und können nicht übersprungen werden.
6. Wählen Sie die Komponenten aus, die Sie deinstallieren möchten, und klicken Sie auf **Next>** (Weiter>). Nachdem Sie das **SQL-Passwort** eingegeben haben, klicken Sie auf **Test Server** (Server testen).
 - SQL Database Server-Konfigurationsdaten:
 - SQL Server: Der Hostname, unter dem SQL Server ausgeführt wird, d. h. der lokale Rechner
 - SQL-Instanz: Der SQL-Instanzname.
 - AMS-Datenbank: Der Name der Datenbank, die Sie erstellt haben.
 - SQL-Benutzername: Die von Ihnen erstellte SQL-Anmeldung.
 - SQL-Passwort: Das SQL-Passwort, das Sie für die SQL-Anmeldung erstellt haben.
7. Klicken Sie auf **Next>** (Weiter>).
8. Beachten Sie die Fortschrittsleiste der Deinstallation.
9. Wenn der Vorgang abgeschlossen ist, klicken Sie auf **Next> (Weiter>)** und überprüfen Sie die Zusammenfassung nach der Deinstallation.
 - Eine Zusammenfassung mit allen Komponenten, die deinstalliert oder übersprungen wurden, wird angezeigt.
10. Klicken Sie auf **Finish** (Fertigstellen), um die Deinstallation des Servers abzuschließen.
 - Der Deinstallationsassistent wird geschlossen.
 - Das System wird aus der Liste der installierten Programme entfernt.
 - Das Symbol des Systems wird aus dem Desktop entfernt.

Den Client deinstallieren

1. Klicken Sie auf die Windows-Schaltfläche **Start**.
2. Suchen Sie **Control Panel** (Systemsteuerung) und doppelklicken Sie darauf, um sie zu öffnen.
3. Folge dem Pfad: **Programms** (Programme) > **Programms and Features** (Programme und Funktionen) > **Uninstall a program** (Ein Programm deinstallieren)
 - Eine Liste der installierten Programme wird geöffnet.
4. Klicken Sie mit der rechten Maustaste auf **Access Management System - Client** und wählen Sie **Uninstall** (Deinstallieren) aus dem Kontextmenü.
 - Der Deinstallationsassistent des Systems wird geöffnet.
5. Wählen Sie die Komponenten aus, die Sie deinstallieren möchten, und klicken Sie auf **Next>** (Weiter>). Klicken Sie auf **Cancel** (Abbrechen), um den Vorgang abzubrechen.
 - Sie können wählen, ob Komponenten deinstalliert oder übersprungen werden sollen. Die meisten Komponenten sind obligatorisch und können nicht übersprungen werden.
6. Beachten Sie die Fortschrittsleiste der Deinstallation.

7. Wenn der Vorgang abgeschlossen ist, klicken Sie auf **Next> (Weiter>)** und überprüfen Sie die Zusammenfassung nach der Deinstallation.
 - Eine Zusammenfassung mit allen Komponenten, die deinstalliert oder übersprungen wurden, wird angezeigt.
8. Klicken Sie auf **Finish** (Fertigstellen), um die Deinstallation des Client abzuschließen.
 - Der Installationsassistent wird geschlossen.
 - Das System wird aus der Liste der Programme entfernt.
 - Das Symbol des Systems wird aus dem Desktop entfernt.

Um den Deinstallationsvorgang abzuschließen, gehen Sie zu `Program Files (x86)` in Ihrem lokalen Laufwerk `C:` und löschen Sie den Ordner `Bosch Sicherheitssysteme`.

4 Technische Daten

Server	
<p>Unterstützte Betriebssysteme. AMS kann möglicherweise auch auf anderen Betriebssystemen installiert werden, hierfür besteht jedoch keinerlei Garantie.</p>	<ul style="list-style-type: none"> - Windows Server 2016(64 Bit, Standard, Datacenter) - Windows 10, version 1903 (LTSB, LTSC) - Hinweis: Die mit diesem System ausgelieferte Standard-Datenbank ist SQL Server 2017 Express Edition mit Advanced Services
<p>Hardware-Mindestanforderungen</p>	<ul style="list-style-type: none"> - Intel i5 Prozessor mit mindestens 4 Kernen - 8 GB RAM (32 GB empfohlen) - 200GB freier Festplattenspeicher (SSD-Datenträger empfohlen) - Grafikkarte mit <ul style="list-style-type: none"> - 256 MB RAM - einer Auflösung von 1280x1024 - mindestens 32K Farben - Ethernet-Karte mit 1 Gbit/s - Ein freier USB-Anschluss oder Netzwerkfreigabe für Installationsdateien
Client	
<p>Unterstützte Betriebssysteme. AMS kann möglicherweise auch auf anderen Betriebssystemen installiert werden, hierfür besteht jedoch keinerlei Garantie.</p>	<ul style="list-style-type: none"> - Windows 10, Version 1803 (LTSB, LTSC)
<p>Hardware-Mindestanforderungen</p>	<ul style="list-style-type: none"> - Intel i5 oder höher - 8 GB RAM (16 GB empfohlen) - 20 GB freier Festplattenspeicher - Grafikkarte mit <ul style="list-style-type: none"> - 256 MB RAM - einer Auflösung von 1920x1080 - mindestens 32K Farben - DirectX® 11 - Ethernet-Karte mit 1 Gbit/s - Ein freier USB-Anschluss oder Netzwerkfreigabe für Installationsdateien
MAC-Server	
<p>Hardware-Mindestanforderungen</p>	<ul style="list-style-type: none"> - Intel i5 oder höher - 8 GB RAM (16 GB empfohlen) - 20 GB freier Festplattenspeicher - Grafikkarte mit <ul style="list-style-type: none"> - 256 MB RAM

MAC-Server	
	<ul style="list-style-type: none">- einer Auflösung von 1280x1024- mindestens 32K Farben- Ethernet-Karte mit 1 Gbit/s

**Hinweis!**

Sowohl der Server als auch der Client müssen in derselben Version installiert sein. Versuchen Sie nicht, mit einer anderen Clientversion auf den Server zuzugreifen.



Bosch Security Systems B.V.

Torenallee 49

5617 BA Eindhoven

Netherlands

www.boschsecurity.com

© Bosch Security Systems B.V., 2020