Access Management System

دليل التثبيت

ar

جدول المحتويات

1 حول هذه الوثائق

هذا هو دليل تثبيت Access Management System الرئيسي.

الوثائق ذات الصلة

تم توثيق العمليات التالية بشكل منفصل:

- تكوين وتشغيل AMS وبرامجه المساعدة.
- تشغيل AMS - Map View.

2 نظرة عامة على نظام AMS

إن Access Management System عبارة عن نظام تحكم في الوصول فعال وحقيقي، يعمل بمفرده أو بالتعاون مع BVMS، نظام إدارة الفيديو المميز من Bosch.
يستمد هذا النظام فعاليته من قدرته على الموازنة الفريدة بين التقنيات الرائدة والمثبتة الفعالية.

- مصمّم لقابلية الاستخدام: واجهة مستخدم عملية مزودة بتطبيق "طريقة عرض الخريطة" الذي يعمل بالسحب والإفلات ومربعات حوار التسجيل البيومتري المحسنة.
- مصمّم لتوفير أمان البيانات: يدعم أحدث المعايير (EU-GDPR 2018) وأنظمة التشغيل وقواعد البيانات وواجهات الأنظمة المشفرة.
- مصمّم لتحقيق المرونة. توفر وحدات التحكم في الوصول الرئيسية ذات الطبقة المتوسطة إمكانية تجاوز الفشل بشكل تلقائي وإعادة تزويد وحدات التحكم في الوصول المحلية في حال طرأ عطل في الشبكة.
- مصمّم للمستقبل: تحديثات منتظمة ومجموعة كبيرة من التحسينات المبتكرة.
- مصمّم لقابلية التوسع: يقدم مستويات تتراوح من منخفضة إلى مرتفعة.
- مصمّم لإمكانية التشغيل التفاعلي: واجهات برمجة تطبيقات RESTful، مع واجهات لنظام إدارة الفيديو من Bosch ومعالجة الأحداث بالإضافة إلى حلول تخصصية للشركاء.
- مصمّم لحماية الاستثمارات: يسمح لك بالبناء على أسس أجهزة التحكم في الوصول المثبتة، ولكن مع تعزيز فعاليتها.

3 التثبيت

الإجراء العام

تتكوّن عملية تثبيت النظام من برنامجي تثبيت منفصلين: الخادم والعميل.

وفيما يلي الترتيب الشامل لعملية التثبيت:

1. التحقق من متطلبات النظام.
2. قبل تثبيت أي محطات عمل خاصة بالعميل:
   - قم بتثبيت البرنامج على الخادم وتأكد من صحة عملية التثبيت.
   - على الخادم، أنشئ تخويل محطة عمل أو أكثر لمحطات العمل الخاصة بالعميل، وقم بتكييف إعدادات جدار الحماية للسماح بالاتصالات بين الخادم والعميل.
3. قم بتثبيت شهادة HTTPS على كل جهاز عميل.
4. قم بتثبيت أجهزة العميل.

راجع

- *استيراد شهادة HTTPS, الصفحة 9*
- *التأكد من تثبيت النظام, الصفحة 12*

3.1 متطلبات النظام

المتطلبات التقنية الدنيا لخادم AMS

الخادم	
أنظمة التشغيل المعتمدة. قد تنجح عمليات التثبيت على أنظمة تشغيل أخرى، ولكنها بكاملها غير مشمولة بضمان.	– Windows Server 2016 (إصدار 64 bit أو Standard أو Datacenter) – Windows 10, version 1809 (LTSC) – **تأكد من تثبيت آخر تحديثات البرامج.** – **ملاحظة:** قاعدة البيانات الافتراضية التي يتم توفيرها مع هذا النظام هي الإصدار SQL Server 2017 Express المزود بخدمات متقدمة
الحد الأدنى من متطلبات الأجهزة	– معالج Intel i5 مع 4 مراكز فعلية على الأقل – ذاكرة وصول عشوائي سعة 8 جيجابايت (السعة المستحسنة 32 جيجابايت) – مساحة خالية على القرص الثابت قدرها 200 جيجابايت (أقراص SSD مستحسنة) – محول رسومات مع – ذاكرة وصول عشوائي سعة 256 ميغابايت – دقة تبلغ 1280x1024 (استخدم دقة الرسومات الموصى بها للعميل إذا أردت تشغيل عميل Map View على خادم AMS). – 32 ألف لون على الأقل – بطاقة إيثرنت بسرعة 1 غيغابت في الثانية – منفذ USB خالٍ أو مساحة مشتركة على الشبكة لملفات التثبيت

المتطلبات التقنية الدنيا لعميل AMS

العميل، بما في ذلك عميل Map View	
أنظمة التشغيل المعتمدة.	– نظام التشغيل Windows 10، الإصدار 1809 (LTSC)

العميل، بما في ذلك عميل Map View	
قد تنجح عمليات التثبيت على أنظمة تشغيل أخرى، ولكنها بكاملها غير مشمولة بضمان.	– **تأكد من تثبيت آخر تحديثات البرامج.**
الحد الأدنى من متطلبات الأجهزة	– Intel i5 أو أعلى – ذاكرة وصول عشوائي سعة 8 جيجابايت (السعة المستحسنة 16 جيجابايت) – مساحة خالية على القرص الثابت قدرها 20 جيجابايت – محول رسومات – ذاكرة وصول عشوائي سعة 256 ميغابايت – لاستخدام مدير حوار AMS، تعتبر دقة من 1280x1024 كافية. – بالنسبة إلى AMS Map View، يجب أن تتوفر دقة من 1920x1080 (Full HD). – 32 ألف لون على الأقل – DirectX® 11 – بطاقة إيثرنت بسرعة 1 غيغابت في الثانية – منفذ USB خالٍ أو مساحة مشتركة على الشبكة لملفات التثبيت

المتطلبات التقنية الدنيا لوحدة MAC إضافية

خادم MAC	
أنظمة التشغيل المعتمدة. قد تنجح عمليات التثبيت على أنظمة تشغيل أخرى، ولكنها بكاملها غير مشمولة بضمان.	– Windows Server 2016 (إصدار 64 bit أو Standard أو Datacenter) – Windows 10, version 1809 (LTSC) – **تأكد من تثبيت آخر تحديثات البرامج.**
الحد الأدنى من متطلبات الأجهزة	– Intel i5 أو أعلى – ذاكرة وصول عشوائي سعة 8 جيجابايت (السعة المستحسنة 16 جيجابايت) – مساحة خالية على القرص الثابت قدرها 20 جيجابايت – محول رسومات مع – ذاكرة وصول عشوائي سعة 256 ميغابايت – دقة من 1280x1024 – 32 ألف لون على الأقل – بطاقة إيثرنت بسرعة 1 غيغابت في الثانية

3.2 تثبيت الخادم

قبل أن تبدأ

1. تأكد من أن اسم المضيف لجهاز الخادم المعني يتطابق مع القواعد المحددة في مربع الإشعار أدناه.
2. تأكد من أن النظام ليس مثبتًا (راجع **التأكد من تثبيت النظام**).
3. انسخ حزمة التثبيت إلى جهاز الخادم.

إشعار!
تنطبق اصطلاحات NETBIOS لأسماء أجهزة الكمبيوتر، على سبيل المثال:
- لا يتجاوز طول الاسم 15 حرفًا،
- **لا** يبدأ الاسم برقم [0-9].
- يتضمن الاسم أحرفًا لاتينية فقط، من دون علامات تشكيل.
- للاطلاع على التفاصيل، راجع: https://support.microsoft.com/en-us/help/909264/naming-conventions-in-active-directory-for-computers-domains-sites-and

بدء عملية تثبيت الخادم

1. انقر نقرًا مزدوجًا فوق حزمة تثبيت البرامج.
2. انقر نقرًا مزدوجًا فوق **الخادم**.
3. انقر بزر الماوس الأيمن فوق **AMS Server Setup.exe** وحدد **تشغيل كمسؤول** من قائمة السياق.
– يفتح معالج تحضير التثبيت. اتبع معالج تحضير التثبيت.
4. حدد المكونات المطلوبة التي يجب تثبيتها وانقر فوق **التالي>**.
– استنادًا إلى البرامج المُثبّتة بالفعل، يقدم المعالج قائمة بالبرامج التي سيقوم بتثبيتها:
– عند وجود مكونات غير إلزامية لا تحتاج إليها، يمكنك إلغاء تحديدها في هذه المرحلة.
5. اقرأ **اتفاقية ترخيص المستخدم النهائي** وانقر فوق **قبول** للمتابعة. إذا لم توافق، فانقر فوق **رفض** لإيقاف عملية التثبيت قبل اكتمالها.
6. أدخل بيانات تكوين SQL Database Server.
– بيانات تكوين SQL Database Server:
– SQL Server: اسم المضيف حيث سيتم تشغيل مثيل SQL Server. استخدم الجهاز المحلي.
– مثيل SQL: اسم مثيل SQL
– قاعدة بيانات AMS: اسم قاعدة البيانات
– اسم مستخدم SQL: اسم تسجيل الدخول إلى SQL
7. انقر فوق **التالي**.
8. إذا كان مسار التثبيت الافتراضي للخادم مقبولاً، فانقر فوق **التالي>**. إذا أردت اختيار مسار تثبيت آخر (محركات أقراص محلية فقط)، فانقر فوق **استعراض**.
– من المستحسن استخدام مسار التثبيت الافتراضي (C:\Program Files (86 لأنه لا يمكن تعديل الملفات إلا من قِبل مسؤولي النظام.
– إذا حددت مسار تثبيت مختلفًا، فتأكد من أن المسار مُزوَّد بحماية كافية من الوصول غير المشروع.
9. انقر فوق **التالي** للمتابعة
– تكوّن هذه الصفحة اسم مضيف واجهة API.
10. راجع ملخص ما قبل التثبيت، وانقر فوق **تثبيت**.
– يظهر ملخص يتضمن جميع المكونات التي اخترت تثبيتها.
11. راقب شريط تقدم التثبيت.
– عندما يصل الشريط الأخضر المتحرك إلى منتصف شريط التقدم، سيحتاج إلى عدة دقائق حتى يبدأ التحرك من جديد. يُرجى الانتظار.
– سيفتح مربع حوار آخر لإعداد قاعدة بيانات AMS.
– إذا كانت قاعدة البيانات مثبّتة، فسيتم تحديثها.
– وإلا، فسيتم إنشاء قاعدة بيانات جديدة، وستتم مطالبتك بإنشاء كلمة مرور جديدة لحساب sa.
مهم: من المستحسن تخزين كلمة المرور هذه بشكل آمن، إذ ستحتاج إليها لإجراء عمليات التحديث إلى جانب عمليات أخرى.
قد تستغرق عملية إنشاء قاعدة البيانات عدة دقائق. يُرجى الانتظار حتى إغلاق مربع الحوار.
12. بعد اكتمال العملية، انقر فوق **التالي** وراجع ملخص ما بعد التثبيت.
– يظهر ملخص يتضمن جميع المكونات التي تم تثبيتها.
13. انقر فوق **إنهاء** لإنهاء عملية التثبيت.
– سيفتح مربع حوار يطالبك بإعادة التشغيل. يجب إعادة تشغيل الكمبيوتر لإكمال عملية تثبيت النظام.
14. انقر فوق **نعم** لإعادة تشغيل الكمبيوتر.

– يبدأ تشغيل الكمبيوتر من جديد.

15. تأكد مما إذا كان النظام مثبتًا بشكل صحيح (راجع **التأكد من تثبيت النظام**).

– إذا كان الأمر كذلك، فهذا يعني أن عملية تثبيت تطبيق النظام للمرة الأولى قد اكتملت. تظهر أيقونة النظام على سطح المكتب.

تسجيل الدخول للمرة الأولى

1. انقر نقرًا مزدوجًا فوق أيقونة تطبيق النظام على سطح المكتب.
2. أدخل اسم المستخدم وكلمة المرور الافتراضيين.

– اسم المستخدم وكلمة المرور الافتراضيان هما **Administrator**. تذكّر أن كلمة المرور (وليس اسم المستخدم) حساسة لحالة الأحرف.

3. انقر فوق **تسجيل الدخول**.

– يظهر مربع حوار يطالبك بتغيير كلمة المرور.

– عند تسجيل الدخول للمرة الأولى، يجب تغيير كلمة المرور في مربع الحوار المنبثق.

4. انقر فوق **موافق** لتسجيل الدخول.

راجع

– *التأكد من تثبيت النظام, الصفحة 12*

– *بدء عملية تحديث الخادم, الصفحة 16*

3.3 إلغاء تنشيط جدار الحماية

بعد نجاح تثبيت الخادم وقبل تثبيت محطات العمل الخاصة بالعميل، ألغِ تنشيط جدار الحماية. سيتيح هذا لمحطات العمل الخاصة بالعميل وأجهزة كمبيوتر MAC الخارجية الاتصال بالخادم بسهولة خلال التكوين الأولي.

3.4 تثبيت محطات عمل العميل

قبل أن تبدأ

1. تأكد من أن اسم المضيف لمحطة عمل العميل المعنية يتطابق مع القواعد المحددة في مربع الإشعار أدناه.
2. انسخ حزمة التثبيت إلى محطة عمل العميل المعنية.

إشعار!

تنطبق اصطلاحات NETBIOS لأسماء أجهزة الكمبيوتر، على سبيل المثال:
- لا يتجاوز طول الاسم 15 حرفًا،
- **لا** يبدأ الاسم برقم [0-9].
- يتضمن الاسم أحرفًا لاتينية فقط، من دون علامات تشكيل.
- للاطلاع على التفاصيل، راجع: https://support.microsoft.com/en-us/help/909264/naming-conventions-in-active-directory-for-computers-domains-sites-and

شهادات HTTPS لمحطات عمل العميل

يستضيف خادم النظام عددًا كبيرًا من واجهات API. وتتصل واجهات API هذه عبر HTTPS وتستخدم شهادة موقّعة ذاتيًا. ينشئ برنامج إعداد الخادم هذه الشهادة الموقّعة ذاتيًا ويثبّتها على جهاز الخادم. ولتمكين الاتصال الآمن بين الخادم وأجهزة العميل، يجب نسخ الشهادة من الخادم واستيرادها يدويًا إلى كل جهاز عميل (راجع **استيراد شهادة HTTPS**).

استيراد شهادة HTTPS

1. انتقل إلى C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates\Access Management System Internal CA.cer
2. انسخ الشهادة إلى جهاز العميل.

3. في جهاز العميل، انقر نقرًا مزدوجًا فوق الشهادة.
   – يظهر مربع حوار الشهادة.
4. انقر فوق **تثبيت الشهادة**.
– يفتح معالج استيراد الشهادة.
5. حدد **الجهاز المحلي** (مستحسن) وانقر فوق **التالي>**.
6. حدد **وضع جميع الشهادات في المتجر التالي** لتحديد موقع للشهادة (مستحسن).
7. انقر فوق **استعراض**.
– يفتح مربع حوار يسمح لك بتحديد متجر الشهادات.
8. حدد `Trusted Root Certification Authorities` وانقر فوق **موافق** (مستحسن).
– يغلق مربع الحوار الذي يسمح لك بتحديد متجر الشهادات.
9. انقر فوق **التالي>** في معالج استيراد الشهادة.
10. انقر فوق **إنهاء** لاستيراد الشهادة.
   – تنتهي عملية استيراد الشهادة.

إشعار!
إذا لم يتم تثبيت شهادة HTTPS، سيتعذر بدء تشغيل التطبيق.

تذكر أنك لن تحتاج إلى استيراد الشهادة إلى جهاز الخادم، إذ تتم هذه العملية بشكل تلقائي أثناء تثبيت الخادم. ينطبق هذا الأمر فقط على محطات عمل منفصلة خاصة بالعميل.

تكامل AMS API مع BVMS

لتمكين تكامل AMS API مع BVMS (Bosch Video Management System)، الإصدار 10.1 أو إصدار لاحق، استورد الشهادة الموقّعة ذاتيًا من خادم AMS إلى جهاز BVMS (راجع **استيراد شهادة HTTPS**).

بدء عملية تثبيت العميل

1. انقر نقرًا مزدوجًا فوق حزمة تثبيت البرامج.
2. انقر نقرًا مزدوجًا فوق **العميل**.
3. انقر نقرًا مزدوجًا فوق **AMS Client Setup.exe**.
   – يفتح معالج تحضير التثبيت. اتبع معالج تحضير التثبيت.
4. حدد المكونات التي تريد تثبيتها وانقر فوق **التالي>**.
– يحدد المعالج حزم Microsoft المطلوبة لكل من Visual C++ وNET.، استنادًا إلى المكونات المتوفرة في النظام.
– المكونات الاختيارية:
   – العميل
   – Map View
5. اقرأ **اتفاقية ترخيص المستخدم النهائي** وانقر فوق **قبول** للمتابعة. إذا لم توافق، فانقر فوق **رفض** للعودة إلى الوراء وإلغاء العملية.
6. إذا كان مسار التثبيت الافتراضي الذي يتعلق بمحطة عمل العميل مقبولاً، فانقر فوق **التالي>**. إذا أردت اختيار مسار تثبيت آخر (محركات أقراص محلية فقط)، فانقر فوق **استعراض**.
7. أدخل عنوان الخادم. تنسيق العنوان: `<hostname>:4999/tcp`
– بشكل افتراضي، يقوم معالج التثبيت بتثبيت عميل النظام في مجلد `C:\Program Files (86)` المحلي.
– لا يمكن تعديل الملفات المثبتة ضمن مجلد `C:\Program Files (86)` المحلي إلا بواسطة مستخدمين لديهم حقوق المسؤول، وبالتالي ننصح بضرورة اختيار المجلد الافتراضي.
8. إذا كان مسار التثبيت الافتراضي الذي يتعلق بتطبيق Map View مقبولاً، فانقر فوق **التالي>**.
9. إذا أردت اختيار مسار تثبيت آخر (محركات أقراص محلية فقط)، فانقر فوق **استعراض**.

10. أدخل عنوان الاكتشاف.
– بشكل افتراضي، يقوم معالج التثبيت بتثبيت تطبيق Map View في محرك الأقراص C: المحلي (مستحسن) (Program Files (86\).
– سيتصل تطبيق Map View بعنوان الاكتشاف لاكتشاف نقاط نهاية النظام. هذا العنوان عبارة عن عنوان URL يحتوي على اسم الخادم ورقم المنفذ حيث تتم استضافة نقطة نهاية الاكتشاف.
11. راجع ملخص ما قبل التثبيت، وانقر فوق **تثبيت**.
– يظهر ملخص يتضمن جميع المكونات التي اخترت تثبيتها.
12. راقب شريط تقدم التثبيت.
– انتظر حتى استكمال العملية.
13. بعد اكتمال العملية، انقر فوق **التالي** وراجع ملخص ما بعد التثبيت.
– يظهر ملخص يتضمن جميع المكونات المثبّتة.
14. انقر فوق **إنهاء** لإنهاء عملية التثبيت.
15. أعد تشغيل الكمبيوتر.
16. تأكد مما إذا تم تثبيت النظام (راجع **التأكد من تثبيت النظام**).
– إذا اكتملت عملية تثبيت AMS Client وMap View، فسترى أيقونتي التطبيقين على سطح المكتب. اسم المستخدم وكلمة المرور الافتراضيان هما **Administrator**. تذكّر أن كلمة المرور (وليس اسم المستخدم) حساسة لحالة الأحرف.

قبل بدء تشغيل العميل

قبل تسجيل الدخول إلى العميل، ستحتاج إلى تكوين محطة عمل العميل على الخادم. اتبع الإجراء أدناه:

1. ابدأ تشغيل العميل على جهاز الخادم.
2. انقر فوق **تكوين>بيانات الجهاز**
– يظهر مربع حوار جديد.
3. في شريط الأدوات العلوي، حدد أيقونة **محطات العمل**.
4. في شريط الأدوات العلوي، حدد أيقونة **جديد**.
5. في علامة تبويب **محطة العمل**، قم بتعبئة الحقول الفارغة.
– الحقول:
  – **الاسم**: أدخل اسم المضيف لمحطة عمل العميل (إلزامي)
  – **الوصف**: أدخل وصفًا (اختياري)
  – **تسجيل الدخول عبر القارئ**: سجّل دخولك عبر القارئ (اختياري)
  – **تسجيل الخروج التلقائي بعد: X من الثواني** (اختياري). حدد تسجيل خروج تلقائي إذا أردت أن يسجل التطبيق خروجه تلقائيًا بعد مرور مدة زمنية محددة.
– لاحظ أن الحقول المُسطَّرة هي حقول إلزامية.
6. في شريط الأدوات العلوي، انقر فوق أيقونة **حفظ** لحفظ التغييرات.
– يمكنك الآن تسجيل الدخول من محطة عمل العميل.

تسجيل الدخول للمرة الأولى

1. انقر نقرًا مزدوجًا فوق أيقونة التطبيق على سطح المكتب.
2. أدخل اسم المستخدم وكلمة المرور الافتراضيين.
– اسم المستخدم وكلمة المرور الافتراضيان لتطبيقي العميل هما **Administrator**. تذكّر أن كلمة المرور (وليس اسم المستخدم) حساسة لحالة الأحرف.
3. انقر فوق **تسجيل الدخول**.
– عند تسجيل الدخول للمرة الأولى، يجب تغيير كلمة المرور. يظهر مربع حوار.
4. انقر فوق **موافق** لإدخال كلمة مرور جديدة في مربع الحوار التالي.
– استخدم كلمة مرور قوية مكوّنة من 8 أحرف على الأقل.
5. أدخل كلمة المرور الجديدة، وانقر فوق **تغيير**. انقر فوق **إلغاء** لإلغاء تغيير كلمة المرور.
– يظهر مربع حوار يؤكد تغيير كلمة المرور.
6. انقر فوق **موافق** لتسجيل الدخول.

إشعار!
لا تحاول الوصول إلى الخادم والعميل معًا من إصدار AMS نفسه. لا تحاول الوصول إلى الخادم من عميل من إصدار AMS مختلف.

راجع
- *التأكد من تثبيت النظام, الصفحة 12*
- *استيراد شهادة HTTPS, الصفحة 9*

3.5 التأكد من تثبيت النظام

التأكد من تثبيت النظام
يكون النظام مثبتًا:
- إذا ظهرت أيقونات النظام على سطح المكتب.
- إذا كانت الخدمات التالية موجودة في تطبيق خدمات Windows (**البدء** > **بحث** > `service.msc`):
  DMS وMAC Access Pl وخدمة الهوية وAPI الخريطة وAPI الحالات.
- إذا كان النظام في مسار التثبيت الافتراضي: `C:\Program Files (x86)\Bosch\Sicherheitssysteme\Access Management System\`

3.6 استخدام الشهادات المخصصة

يمكنك تكوين AMS API بحيث تستخدم شهادات مختلفة بدلاً من استخدام الشهادات الموقّعة ذاتيًا التي تنشأ تلقائيًا أثناء الإعداد.
ويُعتبر هذا الأمر مفيدًا إذا كان لدى المؤسسة بنية تحتية للمفتاح العام (PKI) لديها مصدر الشهادة (CA) الخاص بها.

3.6.1 الشروط المسبقة

- وجود شهادة جذر موثوقة.
- يجب وضع الأجزاء الخاصة والعامة للشهادة في دليل خادم AMS
  `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates\`

أمثلة عن الأجزاء العامة والخاصة للشهادة:
- `Access Management System Test CA.cer` (جزء عام)
- `CustomRootTestCA.pfx` (جزء خاص)

3.6.2 استخدام الشهادات المخصصة

فتح جلسة عمل PowerShell
قم بتشغيل PowerShell كمسؤول على خادم AMS في المجلد: `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates\`

إزالة الشهادات المثبتة
1. قم بإزالة الشهادات التي تم تثبيتها أثناء تثبيت AMS.
2. نفّذ: "`RemoveAceApiCertificates.ps1`" في جلسة عمل PowerShell المفتوحة.

تحرير البرنامج النصي لإنشاء شهادة API

1. افتح ملف PowerShell ""CreateAceApiCertificatesFromOwnRoot.ps1"" في برنامج لتحرير النص، وغيّر تسمية الملفات التالية إلى أسماء شهاداتك المخصصة:
   - CustomRootTestCA.pfx
   - Access Management System Test CA.cer
   - لاحظ ظهور كل اسم ملف مرة واحدة فقط في البرنامج النصي.
2. احفظ التغييرات.

تشغيل البرنامج النصي لإنشاء شهادة API

1. نفّذ: "CreateAceApiCertificatesFromOwnRoot.ps1" في جلسة عمل PowerShell التي فتحتها أعلاه.
2. أدخل كلمة مرور الشهادة الخاصة.
- يتم إنشاء وتثبيت شهادات واجهة API الضرورية التالية:
- تم تثبيت شهادة الجذر.

التحقق من تثبيت الشهادات في شهادات Windows للمستخدم الحالي والكمبيوتر المحلي

تكون الشهادة مثبتة:

- إذا كانت الشهادة الجذر مثبتة تحت Current User Personal Certificates, Trusted Root Certificates وتحت Local Computer Trusted Root Certificates
- إذا كانت شهادات API مثبتة تحت Local Computer Personal Certificates

تحديث إعدادات تطبيق بصمة الإبهام لكل واجهة API

يجب تحديث إعدادات بصمة الإبهام لكل واجهة API.

API الوصول	1. افتح C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Access API 2. بادل القيم الموجودة في الملف appsettings.json، السطر "Thumbprint": 3. افتح **الشهادات (الكمبيوتر المحلي) > شخصية > الشهادات > الاسم المألوف:** Access Management System Access API 4. حدد الشهادة المثبتة وافتحها "Access Management System Access API" **> تفاصيل** 5. قم بالتمرير للأسفل في القائمة وصولاً إلى "Thumbprint" 6. حدد Thumbprint. 7. انسخ بصمة الإبهام المعروضة (على سبيل المثال، "da"). 8. الصق بصمة الإبهام من دون مسافات في الملف appsettings.json، في C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Access API - (على سبيل المثال، "Thumbprint":""53d3588285bd570c9799e883b27ef1b139ba28da"")

API الخريطة	1. افتح C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Map API

	2. بادل القيم الموجودة في الملف appsettings.json، السطر "Thumbprint": 3. افتح **الشهادات (الكمبيوتر المحلي) > شخصية > الشهادات > الاسم المألوف:** Access Management System Map API 4. حدد الشهادة المثبتة وافتحها "Access Management System Map API" **> تفاصيل** 5. قم بالتمرير للأسفل في القائمة وصولاً إلى "Thumbprint" 6. حدد Thumbprint 7. انسخ بصمة الإبهام المعروضة (على سبيل المثال، "e8"). 8. الصق بصمة الإبهام من دون مسافات في الملف appsettings.json، في C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Map API – (على سبيل المثال، "Thumbprint":""3cef0c43be36ee01d8a6ea2f59f170cde96168e8"")
API الحالات	1. افتح C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\States API\ 2. بادل القيم الموجودة في الملف appsettings.json، السطر "Thumbprint": 3. افتح **الشهادات (الكمبيوتر المحلي) > شخصية > الشهادات > الاسم المألوف:** Access Management System States API 4. حدد الشهادة المثبتة وافتحها "Access Management System States API" **> تفاصيل** 5. قم بالتمرير للأسفل في القائمة وصولاً إلى "Thumbprint". 6. حدد Thumbprint. 7. انسخ بصمة الإبهام المعروضة (على سبيل المثال، "e2"). 8. الصق بصمة الإبهام من دون مسافات في الملف appsettings.json، في C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\States API – (على سبيل المثال، "Thumbprint":""37c0bb09d4cab985b620da1c667597ef43b5f8e2
Identity Server:	1. افتح C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Identity Server\ 2. بادل القيم الموجودة في الملف appsettings.json، السطر "Thumbprint": 3. افتح **الشهادات (الكمبيوتر المحلي) > شخصية > الشهادات > الاسم المألوف:** Access Management System Identity Server 4. حدد الشهادة المثبتة وافتحها "Access Management Identity Server" **> تفاصيل** 5. قم بالتمرير للأسفل في القائمة وصولاً إلى "Thumbprint". 6. حدد Thumbprint.

7. انسخ بصمة الإبهام المعروضة.
8. الصق بصمة الإبهام من دون مسافات في الملف appsettings.json، في C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Identity Server
9. الصق بصمات الإبهام لواجهات API الأخرى في حقول إدخال بصمة الإبهام المناظرة في هذا الملف أيضًا.

- مثال:
  - بالنسبة إلى ""Name": "AccessApi" "Thumbprint": ""53d3588285bd570c9799e883b27ef1b139ba28da
  - بالنسبة إلى ""Name": "MapApi" "Thumbprint": ""3cef0c43be36ee01d8a6ea2f59f170cde96168e8
  - بالنسبة إلى ""Name": "StatesApi" "Thumbprint": ""37c0bb09d4cab985b620da1c667597ef43b5f8e2

إيقاف الخدمات وبدء تشغيلها

1. افتح خدمات Windows.
2. انقر بزر الماوس الأيمن فوق الخدمات التالية، وحدد "إيقاف" بعد كل واحدة منها:
- Access Management System Access API
- Access Management System Identity Server
- Access Management System Map API
- Access Management System Sates API
- بعد أن تتوقف الخدمات الأربع كلها، انقر بزر الماوس الأيمن فوق الخدمات نفسها مرة أخرى، وحدد **بدء** بعد كل واحدة منها.

تثبيت شهادة الجذر على جهاز العميل

1. استخدم "إدارة الملفات" في Windows لنسخ شهادة الجذر "Access Management System Test CA.cer" والصقها في جهاز العميل، حيث تم تثبيت تطبيقي العميل "Map View" و"AMS" (مدير الحوار).
على سبيل المثال، يمكنك لصقها في مجلد التنزيلات.
2. ثبّت شهادة الجذر.
- في "إدارة الملفات"، انقر بزر الماوس الأيمن فوق **ملف الشهادة** ثم حدد **تثبيت الشهادة > المستخدم الحالي > التالي >** حدد **"وضع جميع الشهادات في المتجر التالي" > استعراض >** حدد **"الشهادات الجذر الموثوقة" > التالي > إنهاء > موافق**

اختبار شهادات واجهة API على جهاز العميل.

يجب أن تخضع شهادات API للاختبار على جهاز العميل، حيث تم تثبيت تطبيق العميل Map View وAMS (مدير الحوار).

على جهاز العميل، ابدأ تشغيل مستعرض Google Chrome.
- لاختبار Identity Server، أدخل العنوان التالي: https://[ServerHostname]:44333/.well-known/openid-configuration
- انقر بزر الماوس الأيمن فوق أيقونة قفل معلومات موقع الويب > تحقق من "شهادة (صالحة)" وتأكد من استخدام الشهادة الصحيحة ضمن "تم الإصدار من قبل"

- لاختبار API الوصول، أدخل العنوان التالي: https://[ServerHostname]:44347/swagger
  - انقر بزر الماوس الأيمن فوق أيقونة قفل معلومات موقع الويب > تحقق من "شهادة (صالحة)" وتأكد من استخدام الشهادة الصحيحة ضمن "تم الإصدار من قبل"
- لاختبار API الحالات، أدخل العنوان التالي: https://[ServerHostname]:62901/swagger
  - انقر بزر الماوس الأيمن فوق أيقونة قفل معلومات موقع الويب > تحقق من "شهادة (صالحة)" وتأكد من استخدام الشهادة الصحيحة ضمن "تم الإصدار من قبل".
- لاختبار API الخريطة، أدخل العنوان التالي: https://[ServerHostname]:61801/$metadata
  - انقر بزر الماوس الأيمن فوق أيقونة قفل معلومات موقع الويب > تحقق من "شهادة (صالحة)" وتأكد من استخدام الشهادة الصحيحة ضمن "تم الإصدار من قبل"

استخدام الشهادة في AMS.

ابدأ تشغيل تطبيق Map View على جهاز العميل، وسجّل دخولك.

3.7 استكشاف الأخطاء وإصلاحها

إذا فشل التثبيت، فسيتغير لون شريط التقدم إلى اللون الأحمر. قد يظهر نص رسالة خطأ إضافية.
انقر فوق **التالي>** للمتابعة إلى صفحة الملخص التي ستعرض المكونات التي فشل تثبيتها.

3.8 تحديث النظام

قبل أن تبدأ

1. سجّل دخولك إلى جهاز الخادم.
2. تأكد مما إذا كان الإصدار السابق من النظام مثبتًا بالفعل (راجع **التأكد من تثبيت النظام**).
3. انسخ حزمة التثبيت الجديدة إلى جهاز الخادم.

إشعار!

لا تحاول الوصول إلى الخادم والعميل معًا من إصدار AMS نفسه. لا تحاول الوصول إلى الخادم من عميل من إصدار AMS مختلف.

بدء عملية تحديث الخادم

1. انقر نقرًا مزدوجًا فوق الإصدار الجديد من حزمة تثبيت البرامج.
2. حدد لغة الواجهة.
3. انقر نقرًا مزدوجًا فوق **الخادم**.
4. انقر بزر الماوس الأيمن فوق **AMS Server Setup.exe** وحدد **تشغيل كمسؤول** من قائمة السياق.
   - يفتح معالج تحضير التثبيت.
   - حدد المكونات التي تريد تحديثها وانقر فوق **التالي>**.
   - استنادًا إلى المكونات المتوفرة، يضع المعالج علامة على المكونات التي يمكن تحديثها بشكل افتراضي.
   - يمكنك اختيار تحديث المكونات أو تخطي تحديثها.
   - ستوضع علامة **تخطي** بشكل افتراضي على المكونات التي لا يمكن تحديثها.
5. اقرأ **اتفاقية ترخيص المستخدم النهائي** وانقر فوق **قبول** للمتابعة. إذا لم توافق، فانقر فوق **رفض** للعودة إلى الوراء وإلغاء العملية.
6. أدخل بيانات تكوين SQL Database Server.
   - بيانات تكوين SQL Database Server:
     - SQL Server: اسم المضيف حيث يتم تشغيل مثيل SQL Server، أي الجهاز المحلي (مستحسن)
     - مثيل SQL: اسم مثيل SQL

- قاعدة بيانات AMS: اسم قاعدة البيانات
- اسم مستخدم SQL: اسم تسجيل الدخول إلى SQL

7. انقر فوق **التالي**.

- يعرض مربع الحوار التالي مسار التثبيت حيث سيتم الاحتفاظ بخادم النظام.
- بشكل افتراضي، يقوم معالج التثبيت بتثبيت خادم النظام في محرك الأقراص C:\Program Files (86) المحلي (مستحسن).
- لا يمكن تعديل الملفات المثبتة ضمن محرك الأقراص C:\Program Files (86) المحلي إلا بواسطة مستخدمين لديهم حقوق المسؤول. من شأن هذا الأمر أن يوفر الأمان من خلال ضمان عدم قدرة المستخدمين الذين ليس لديهم حقوق المسؤول على تعديل الملفات ذات الصلة بالنظام.

8. انقر فوق **التالي>** للمتابعة.
9. راجع ملخص ما قبل التحديث، وانقر فوق **تثبيت**.

- يظهر ملخص يتضمن جميع المكونات التي اخترت تحديثها.

10. راقب شريط تقدم التثبيت.

- عندما يصل الشريط الأخضر المتحرك إلى منتصف شريط التقدم، سيحتاج إلى عدة دقائق حتى يبدأ التحرك من جديد. يُرجى الانتظار.
- سيفتح مربع حوار آخر لإعداد قاعدة بيانات AMS.
  - إذا كانت قاعدة البيانات مثبّتة، فسيتم تحديثها.
  - وإلا، فسيتم إنشاء قاعدة بيانات جديدة، وستتم مطالبتك بإنشاء كلمة مرور جديدة لحساب sa.
    مهم: من المستحسن تخزين كلمة المرور هذه بشكل آمن، إذ ستحتاج إليها لإجراء عمليات التحديث إلى جانب عمليات أخرى.
    قد تستغرق عملية إنشاء قاعدة البيانات عدة دقائق. يُرجى الانتظار حتى إغلاق مربع الحوار.

11. بعد اكتمال العملية، انقر فوق **التالي** وراجع ملخص ما بعد التحديث.

- يظهر ملخص يتضمن جميع المكونات التي تم تحديثها.

12. انقر فوق **إنهاء** لإنهاء عملية تثبيت الإصدار المحدّث من النظام.
13. أعد تشغيل الكمبيوتر (مستحسن).

- يبدأ تشغيل الكمبيوتر من جديد.

14. تأكد مما إذا تم تثبيت النظام (راجع **التأكد من تثبيت النظام**).

- إذا كان الأمر كذلك، فهذا يعني أن عملية تثبيت الإصدار المحدّث من تطبيق النظام قد اكتملت.
- اسم المستخدم وكلمة المرور الافتراضيان هما **Administrator**. تذكّر أن كلمة المرور (وليس اسم المستخدم) حساسة لحالة الأحرف.

بدء عملية تحديث العميل

1. انقر نقرًا مزدوجًا فوق الإصدار الجديد من حزمة تثبيت البرامج.
2. حدد لغة الواجهة.
3. انقر نقرًا مزدوجًا فوق **العميل**.
4. انقر بزر الماوس الأيمن فوق **AMS Client Setup.exe** وحدد **تشغيل كمسؤول** من قائمة السياق.

- يفتح معالج تحضير التثبيت.
- حدد المكونات التي تريد تحديثها وانقر فوق **التالي>**.
- استنادًا إلى المكونات المتوفرة، يضع المعالج علامة على المكونات التي يمكن تحديثها بشكل افتراضي.
- يمكنك اختيار تحديث المكونات أو تخطي تحديثها:
- ستوضع علامة **تخطي** بشكل افتراضي على المكونات التي لا يمكن تحديثها.

5. اقرأ **اتفاقية ترخيص المستخدم النهائي** وانقر فوق **قبول** للمتابعة. إذا لم توافق، فانقر فوق **رفض** للعودة إلى الوراء وإلغاء العملية.

- يعرض مربع الحوار التالي مسار التثبيت حيث سيتم الاحتفاظ بعميل النظام.
- بشكل افتراضي، يثبّت معالج التثبيت عميل النظام في محرك الأقراص C:\Program Files (86) المحلي (مستحسن).

- لا يمكن تعديل الملفات المثبتة ضمن مجلد (C:\Program Files (86 المحلي إلا بواسطة مستخدمين لديهم حقوق المسؤول.

6. أدخل عنوان الخادم. تنسيق العنوان: <hostname>:4999/tcp>
7. انقر فوق **التالي>** للمتابعة.
- يعرض مربع الحوار التالي مسار التثبيت حيث سيتم الاحتفاظ بتطبيق Map View للنظام.
- بشكل افتراضي، يثبّت معالج التثبيت تطبيق Map View في محرك الأقراص :C (\Program Files (86 المحلي (مستحسن).

8. أدخل عنوان الاكتشاف.
- سيتصل تطبيق Map View بعنوان الاكتشاف لاكتشاف نقاط نهاية النظام. هذا العنوان عبارة عن عنوان URL يحتوي على اسم الخادم ورقم المنفذ حيث تتم استضافة نقطة نهاية الاكتشاف.

9. راجع ملخص ما قبل التحديث، وانقر فوق **تثبيت**.
- يظهر ملخص يتضمن جميع المكونات التي اخترت تحديثها.

10. راقب شريط تقدم التثبيت.
- انتظر حتى استكمال العملية.

11. بعد اكتمال العملية، انقر فوق **التالي** وراجع ملخص ما بعد التحديث.
- يظهر ملخص يتضمن جميع المكونات التي تم تحديثها.

12. انقر فوق **إنهاء** لإنهاء عملية تثبيت الإصدار المحدّث من النظام.
13. أعد تشغيل الكمبيوتر (مستحسن).
- يبدأ تشغيل الكمبيوتر من جديد.

14. تأكد مما إذا تم تثبيت النظام (راجع **التأكد من تثبيت النظام**).
- إذا كان الأمر كذلك، فهذا يعني أن عملية تثبيت الإصدار المحدّث من تطبيق النظام قد اكتملت.
- اسم المستخدم وكلمة المرور الافتراضيان هما **Administrator**. تذكّر أن كلمة المرور (وليس اسم المستخدم) حساسة لحالة الأحرف.

راجع

- *التأكد من تثبيت النظام, الصفحة 12*

3.9 إزالة التثبيت

لإزالة برنامج النظام، اتبع الخطوات أدناه:

إزالة تثبيت الخادم

1. انقر فوق زر **البدء** في Windows.
2. ابحث عن **لوحة التحكم** وانقر نقرًا مزدوجًا فوقها لفتحها.
3. اتبع المسار: **البرامج** > **البرامج والميزات** > **إزالة تثبيت برنامج**
- تظهر قائمة بالبرامج المثبتة.

4. انقر بزر الماوس الأيمن فوق **Access Management System** - **الخادم** وحدد **إزالة التثبيت** من قائمة السياق.
- يفتح معالج إزالة التثبيت التابع للنظام.

5. حدد المكونات التي تريد إزالة تثبيتها وانقر فوق **التالي>**. انقر فوق **إلغاء** لإلغاء العملية.
- يمكنك اختيار إلغاء تثبيت المكونات أو تخطيها. تعتبر معظم المكونات إلزامية ولا يمكن تخطيها.

6. حدد المكونات التي تريد إزالة تثبيتها وانقر فوق **التالي>**. بعد إدخال **كلمة مرور SQL**، انقر فوق **اختبار الخادم.**
- بيانات تكوين SQL Database Server:
  - SQL Server: اسم المضيف حيث يتم تشغيل SQL Server، أي الجهاز المحلي
  - مثيل SQL: اسم مثيل SQL.
  - قاعدة بيانات AMS: اسم قاعدة البيانات التي أنشأتها.
  - اسم مستخدم SQL: اسم تسجيل الدخول إلى SQL الذي أنشأته.
  - كلمة مرور SQL: كلمة مرور SQL التي أنشأتها لتسجيل الدخول إلى SQL.

7. انقر فوق **التالي**.
8. راقب شريط تقدم إزالة التثبيت.
9. بعد اكتمال العملية، انقر فوق **التالي**، وراجع ملخص ما بعد إزالة التثبيت.
– يظهر ملخص يتضمن جميع المكونات التي تمت إزالة تثبيتها أو تخطيها.
10. انقر فوق **إنهاء** لإنهاء عملية إزالة تثبيت الخادم.
– يغلق معالج إزالة التثبيت.
– يختفي النظام من قائمة البرامج المثبتة.
– تختفي أيقونة النظام من سطح المكتب.

إزالة تثبيت العميل

1. انقر فوق زر **البدء** في Windows.
2. ابحث عن **لوحة التحكم** وانقر نقرًا مزدوجًا فوقها لفتحها.
3. اتبع المسار: **البرامج** > **البرامج والميزات** > **إزالة تثبيت برنامج**
– تظهر قائمة بالبرامج المثبتة.
4. انقر بزر الماوس الأيمن فوق **Access Management System** - **العميل** وحدد **إزالة التثبيت** من قائمة السياق.
– يفتح معالج إزالة التثبيت التابع للنظام.
5. حدد المكونات التي تريد إزالة تثبيتها وانقر فوق **التالي>**. انقر فوق **إلغاء** لإلغاء العملية.
– يمكنك اختيار إلغاء تثبيت المكونات أو تخطيها. تعتبر معظم المكونات إلزامية ولا يمكن تخطيها.
6. راقب شريط تقدم إزالة التثبيت.
7. بعد اكتمال العملية، انقر فوق **التالي**، وراجع ملخص ما بعد إزالة التثبيت.
– يظهر ملخص يتضمن جميع المكونات التي تمت إزالة تثبيتها أو تخطيها.
8. انقر فوق **إنهاء** لإنهاء عملية إزالة تثبيت العميل.
– يغلق معالج التثبيت.
– يختفي النظام من قائمة البرامج.
– تختفي أيقونة النظام من سطح المكتب.

لإكمال عملية إزالة التثبيت، احذف المجلد :C
\Program Files (x86)\Bosch Sicherheitssysteme\

4 البيانات التقنية

إشعار!
لا تحاول الوصول إلى الخادم والعميل معًا من إصدار AMS نفسه. لا تحاول الوصول إلى الخادم من عميل من إصدار AMS مختلف.

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