



BOSCH

Access Management System

ar

دليل التثبيت

جدول المحتويات

4	حول هذه الوثائق	1
5	نظرة عامة على نظام AMS	2
6	التثبيت	3
6	متطلبات النظام	3.1
7	تثبيت الخادم	3.2
8	إلغاء تنشيط جدار الحماية	3.3
8	تثبيت العميل	3.4
11	التأكد من تثبيت النظام	3.5
11	استخدام الشهادات المخصصة	3.6
11	الشروط المسبقة	3.6.1
12	استخدام الشهادات المخصصة	3.6.2
15	استكشاف الأخطاء وإصلاحها	3.7
15	تحديث النظام	3.8
17	إزالة التثبيت	3.9
19	البيانات التقنية	4

حول هذه الوثائق

1

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.

نظرة عامة على نظام AMS

2

- 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 لتقابلية الاستخدام: واجهة مستخدم عملية مزودة بتطبيق "طريقة عرض الخريطة" الذي يعمل بالسحب والإفلات ومربعات حوار التسجيل البيوميترى 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 لتقابلية التوسع: يقدم مستويات تتراوح من منخفضة إلى مرتفعة.
 - مصمّم لإمكانية التشغيل التفاعلي: واجهات برمجية تطبيقات RESTful، مع واجهات لنظام إدارة الفيديو من Bosch ومعالجة الأحداث بالإضافة إلى حلول تخصيصية 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. تثبيت البرامج على الخادم والتأكد من صحة هذا التثبيت قبل تثبيت أي عملاء
3. تثبيت شهادة HTTPS على جهاز العميل
4. تثبيت العميل

- استيراد شهادة HTTPS, الصفحة 9
- التأكد من تثبيت النظام, الصفحة 11

متطلبات النظام

3.1

متطلبات النظام الدنيا لخادم AMS

الخادم	
<ul style="list-style-type: none"> - Windows Server 2016 (64 بت أو قياسي أو مركز البيانات) - (Windows 10, version 1903 (LTSC, LTSC - ملاحظة: قاعدة البيانات الافتراضية التي يتم توفيرها مع هذا النظام هي الإصدار SQL Server 2017 Express المزود بخدمات متقدمة 	<ul style="list-style-type: none"> - أنظمة التشغيل المعتمدة. - قد تنجح عمليات التثبيت على أنظمة تشغيل أخرى، ولكنها بكاملها غير مشمولة بضمان.
<ul style="list-style-type: none"> - 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 ميجابايت - دقة من 1280x1024 - 32 ألف لون على الأقل - بطاقة إيثرنت بسرعة 1 غيغابت في الثانية - منفذ USB خالٍ أو مساحة مشتركة على الشبكة لملفات التثبيت 	<ul style="list-style-type: none"> - الحد الأدنى من متطلبات الأجهزة

متطلبات النظام الدنيا لـ AMS Client

العميل	
<ul style="list-style-type: none"> - نظام التشغيل Windows 10، الإصدار (LTSC، LTSC) 1803 	<ul style="list-style-type: none"> - أنظمة التشغيل المعتمدة. - قد تنجح عمليات التثبيت على أنظمة تشغيل أخرى، ولكنها بكاملها غير مشمولة بضمان.
<ul style="list-style-type: none"> - 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 ميجابايت 	<ul style="list-style-type: none"> - الحد الأدنى من متطلبات الأجهزة

العميل	
-	دقة من 1920x1080
-	32 ألف لون على الأقل
-	DirectX® 11
-	بطاقة إيثرنت بسرعة 1 غيغابت في الثانية
-	منفذ USB خالٍ أو مساحة مشتركة على الشبكة للملفات التثبيت

متطلبات النظام الدنيا لوحدّة MAC إضافية

خادم MAC	
-	الحدا 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

تثبيت الخادم

3.2

قبل أن تبدأ

1. سجل دخولك إلى جهاز الخادم.
2. تأكد مما إذا كان النظام مثبتًا بالفعل (راجع التأكد من تثبيت النظام). إذا لم يكن مثبتًا، فتابع عملية التثبيت.
3. انسخ حزمة التثبيت إلى جهاز الخادم.

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.
- افتح معالج تحضير التثبيت. اتبع معالج تحضير التثبيت.
4. حدد المكونات المطلوبة التي يجب تثبيتها وانقر فوق التالي >.
- استنادًا إلى البرامج المثبتة بالفعل، يقدم المعالج قائمة بالبرامج التي سيقوم بتثبيتها:
- إذا كانت هناك أي مكونات غير إلزامية لا تحتاج إليها، فألغ 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. من المستحسن استخدام الجهاز المحلي.
- مثيل SQL: اسم مثيل SQL
- قاعدة بيانات AMS: اسم قاعدة البيانات
- اسم مستخدم SQL: اسم تسجيل الدخول إلى SQL
- كلمة مرور SQL: كلمة مرور SQL لتسجيل الدخول إلى SQL. كلمة المرور الافتراضية: sa_s3k_pw
7. بعد إدخال كلمة مرور SQL، انقر فوق اختبار الخادم.
- إذا نجحت عملية الاختبار، فستظهر رسالة مع خلفية خضراء تحت حقل "كلمة مرور SQL".

8. انقر فوق **التالي**.
9. 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 محرك الأقراص C:\Program Files لأنه لا يمكن تعديل الملفات إلا من قبل مسؤولي النظام.
- إذا حددت مسار تثبيت مختلفاً، فتأكد من أن المسار مُرُود بحماية كافية من الوصول غير المشروع.
10. انقر فوق **التالي** للمتابعة
- تكون هذه الصفحة اسم مضيف API.
- يجب ألا يزيد اسم الخادم عن **16** حرفاً. القيمة الافتراضية (المستحسنة) هي اسم المضيف للكمبيوتر الحالي حيث يتم تشغيل برنامج التثبيت.
11. راجع ملخص ما قبل التثبيت، وانقر فوق **تثبيت**.
- يظهر ملخص يتضمن جميع المكونات التي اخترت تثبيتها.
12. 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 يتعلق بإعداد Access Engine (ACE) Database. يقوم برنامج الإعداد هذا بتحديث قاعدة بيانات ACE. سيتم تحديث قاعدة البيانات إذا كانت مثبتة، وإلا فسيتم إنشاء قاعدة بيانات جديدة. قد يستغرق هذا الأمر عدة دقائق. يُرجى الانتظار حتى إغلاق مربع الحوار.
13. بعد اكتمال العملية، انقر فوق **التالي** وراجع ملخص ما بعد التثبيت.
- يظهر ملخص يتضمن جميع المكونات التي تم تثبيتها.
14. انقر فوق **إنهاء** لإنهاء عملية التثبيت.
- سيفتح مربع حوار يطالبك بإعادة التشغيل. يجب إعادة تشغيل الكمبيوتر لإكمال عملية تثبيت النظام.
15. انقر فوق **نعم** لإعادة تشغيل الكمبيوتر.
- يبدأ تشغيل الكمبيوتر من جديد.
16. تأكد مما إذا كان النظام مثبتاً 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**. تذكر 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.

- التأكد من تثبيت النظام، الصفحة 11

- بدء عملية تحديث الخادم، الصفحة 15

3.3 إلغاء تنشيط جدار الحماية

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

3.4 تثبيت العميل

شهادة HTTPS للعميل

يستضيف خادم النظام الكثير من واجهات برمجية التطبيقات (API)، وتحديداً: API الوصول، API الخريطة وAPI الحالات وتتواصل وواجهات برمجية التطبيقات (API) عبر HTTPS وتستخدم شهادة موقعة ذاتياً لتأسيس الثقة. ويتم إنشاء الشهادة الموقعة ذاتياً بواسطة برنامج تثبيت الخادم ويتم تثبيتها على جهاز الخادم. يستخدم عميل الخريطة وواجهات برمجية التطبيقات (API) هذه كي يعمل بشكل صحيح، ويتطلب بالتالي ثقة جهاز العميل بواجهات برمجية التطبيقات (API). ولتمكين هذا الأمر، يجب نسخ شهادة من الخادم واستيرادها يدوياً إلى جهاز العميل (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.
 - يظهر 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 API الوصول مع BVMS

لتمكين تكامل AMS Access API مع BVMS (Bosch Video Management System) - الإصدار 9.1 أو إصدار لاحق - ، استورد الشهادة كما ورد في القسم الأخير إلى جهاز BVMS (راجع استيراد شهادة HTTPS).

نظام التشغيل المعتمد

نظام التشغيل المعتمد للعميل هو Windows 10 ، الإصدار 1803 (LTSC, LTSB).

إشعار!

قد يؤدي تثبيت العميل خارج هذا النطاق إلى حدوث مشاكل في التوافق.

**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 >.
- استنادًا إلى المكونات المتوفرة، يضع المعالج علامة على البرامج الإلزامية المطلوبة مسبقًا التالية:
 - Microsoft Visual C++ 2010 Redistributable

- Microsoft Visual C++ 2015 Redistributable
- Microsoft Visual C++ 2017 Redistributable
- NET 4.8.
- المكونات الاختيارية:
 - العميل
 - Map View
- لكل مكون اختياري، يمكنك اختيار تثبيته أو تخطيه.
- 5. اقرأ اتفاقية ترخيص المستخدم النهائي وانقر فوق قبول للمتابعة. إذا لم توافق، فانقر فوق رفض للرجوع 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 محرك الأقراص C:/Program Files المحلي (مستحسن).
 - لا يمكن تعديل الملفات المثبتة ضمن محرك الأقراص C:/Program Files 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.
 - إذا أردت اختيار مسار تثبيت آخر، فستفقد الميزات المقدمة.
- 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:/Program Files المحلي (مستحسن).
 - سيتطلب 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 التي تم تثبيتها.
- 14. انقر فوق إنهاء لإنهاء عملية التثبيت.
- 15. أعد تشغيل الكمبيوتر (مستحسن).
- 16. تأكد مما إذا تم تثبيت النظام (راجع التأكد من تثبيت النظام).
- إذا كان الأمر كذلك، فهذا يعني أن عملية تثبيت العميل وتطبيق Map View (اختياري) قد اكتملت. تظهر أيقونة تطبيق العميل على سطح المكتب. اسم المستخدم وكلمة المرور الافتراضيان هما Administrator. تذكر 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"، املاً الحقول الفارغة.
 - الحقول:
 - الاسم: أدخل اسم المضيف لمحطة عمل العميل (الزامي)
 - الوصف: أدخل وصفاً (اختياري)
 - تسجيل الدخول عبر القارئ: سجل 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 المسطرة هي حقول إلزامية.
- 6. في شريط الأدوات العلوي، انقر فوق أيقونة **حفظ** لحفظ التغييرات.
- يمكنك الآن تسجيل الدخول بنجاح من محطة عمل العميل.

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 لتطبيقات العميل هما **Administrator**. تذكر أن كلمة المرور (وليس اسم المستخدم) تتحسس حالة الأحرف.
3. انقر فوق **تسجيل الدخول**.
- يظهر مربع حوار يطالبك بإدخال كلمة المرور.
- عند تسجيل الدخول للمرة الأولى، يجب تغيير كلمة المرور.
4. انقر فوق **موافق** لإدخال كلمة مرور جديدة في مربع الحوار التالي.
5. أدخل كلمة مرور جديدة، وانقر فوق **تغيير**. انقر فوق **إلغاء** لإلغاء تغيير كلمة المرور.
- يظهر مربع حوار يؤكد تغيير كلمة المرور.
6. انقر فوق **موافق** لتسجيل الدخول.

إشعار!

يجب تثبيت الخادم والعميل معًا في الإصدار نفسه. لا تحاول الوصول إلى الخادم باستخدام إصدار عميل مختلف.



- التأكد من تثبيت النظام، الصفحة 11

- استيراد شهادة HTTPS، الصفحة 9

التأكد من تثبيت النظام

3.5

التأكد من تثبيت النظام

يكون النظام مثبتًا:

- إذا ظهرت أيقونات النظام على سطح المكتب.
- إذا كانت الخدمات التالية موجودة في تطبيق خدمات Windows (البداية > بحث > service.msc): DMS و MAC Access PI وخدمة الهوية وAPI الخريطة وAPI الحالات.
- إذا كان النظام في مسار التثبيت الافتراضي: C:\Program Files (x86)\Bosch Sicherheitssysteme \\Access Management System

استخدام الشهادات المخصصة

3.6

يمكنك تكوين AMS API بحيث تستخدم شهادات مختلفة بدلاً من استخدام الشهادات الموقعة 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.

الشروط المسبقة

3.6.1

- 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 الخاصة والشهادة:

- Access Management System Test CA.cer (جزء عام)
- CustomRootTestCA.pfx (جزء خاص)

استخدام الشهادات المخصصة

3.6.2

فتح جلسة عمل PowerShell

افتح جلسة عمل PowerShell على خادم AMS في الدليل C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates

إزالة الشهادات المثبتة

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

تحرير البرنامج النصي لإنشاء شهادة

1. افتح ملف PowerShell "CreateAceApiCertificatesFromOwnRoot.ps1" في برنامج لتحرير النص، وأعد تسمية الملفات التالية إلى أسماء ملفاتك:
 - CustomRootTestCA.pfx
 - 2. Access Management System Test CA.cer
 - لاحظ أن أسماء الملفات تظهر مرة واحدة فقط في البرنامج النصي.
 - 3. احفظ التغييرات.

تشغيل البرنامج النصي لإنشاء شهادة

1. نفذ: "CreateAceApiCertificatesFromOwnRoot.ps1" في جلسة عمل PowerShell التي فتحتها في الخطوة 1.
2. أدخل كلمة مرور الشهادة الخاصة.
- تم إنشاء وتثبيت شهادات Sub-API التالية:
 - Access Management System Access API
 - Access Management System Identity Server
 - Access Management System Map API
 - Access Management System States API
- تم تثبيت شهادة الجذر.

التحقق من تثبيت الشهادات في شهادات Windows للمستخدم المحلي والكمبيوتر المحلي

تكون الشهادة مثبتة:

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

تحديث إعدادات تطبيق بصمة الإبهام لكل واجهة API

يجب تحديث إعدادات بصمة الإبهام لكل واجهة API.

افتح C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Access API	1.	API الوصول
بادل القيم الموجودة في الملف appsettings.json، السطر "Thumbprint"	2.	
افتح الشهادات (الكمبيوتر المحلي) < شخصية < الشهادات < الاسم المألوف: Access Management System Access API	3.	

<p>4. حدد الشهادة المثبتة وافتحها "Access Management System Access API" < تفاصيل</p> <p>5. قم بالتمرير للأسفل في القائمة وصولاً إلى "Thumbprint"</p> <p>6. حدد Thumbprint.</p> <p>7. انسخ بصمة الإبهام المعروضة (على سبيل المثال، "da").</p> <p>8. الصق بصمة الإبهام من دون مسافات في الملف appsettings.json، في C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Access API</p> <p>- (على سبيل المثال، "Thumbprint": "53d3588285bd570c9799e883b27ef1b139ba28da")</p>	
--	--

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

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

افتح C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Identity Server	1.	:Identity Server
بادل القيم الموجودة في الملف appsettings.json، السطر "Thumbprint":	2.	
افتح الشهادات (الكمبيوتر المحلي) < شخصية < الشهادات < الاسم المؤلف: Access Management System Identity Server	3.	
حدد الشهادة المثبتة وافتحها "Access Management Identity Server" < تفاصيل	4.	
قم بالتمرير للأسفل في القائمة وصولاً إلى "Thumbprint".	5.	
حدد Thumbprint.	6.	
انسخ بصمة الإيماء المعروضة.	7.	
الصق بصمة الإيماء من دون مسافات في الملف appsettings.json، في C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Identity Server	8.	
الصق بصمات الإيماء لواجهات API الأخرى في حقول إدخال بصمة الإيماء المناظرة في هذا الملف أيضاً.	9.	
مثال:	-	
بالنسبة إلى "AccessApi"	-	Name": "AccessApi"
"Thumbprint":		"Thumbprint":
"53d3588285bd570c9799e883b27ef1b139ba28da"		"53d3588285bd570c9799e883b27ef1b139ba28da"
بالنسبة إلى "MapApi"	-	Name": "MapApi"
"Thumbprint":		"Thumbprint":
"3cef0c43be36ee01d8a6ea2f59f170cde96168e8"		"3cef0c43be36ee01d8a6ea2f59f170cde96168e8"
بالنسبة إلى "StatesApi"	-	Name": "StatesApi"
"Thumbprint":		"Thumbprint":
"37c0bb09d4cab985b620da1c667597ef43b5f8e2"		"37c0bb09d4cab985b620da1c667597ef43b5f8e2"

إيقاف وبدء الخدمات

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 تطبيق العميل "Map View" و"AMS" (مدير مربع الحوار). على سبيل المثال، يمكنك لصقها في مجلد التنزيلات.
 2. ثبت 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 API على جهاز العميل.

يجب أن تخضع شهادات API للاختبار على جهاز العميل، حيث تم تثبيت تطبيق العميل "طريقة عرض الخريطة" و"AMS" (مدير مربع 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 Access API، 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/odata/$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 "طريقة عرض الخريطة" على جهاز العميل، وسجل دخولك.

استكشاف الأخطاء وإصلاحها

3.7

إذا فشل التثبيت، فستتغير 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.

تحديث النظام

3.8

قبل أن تبدأ

1. سجل 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!

يجب تثبيت الخادم والعميل معًا في الإصدار نفسه. لا تحاول الوصول إلى الخادم باستخدام إصدار عميل 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 <.

- استناداً 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** للرجوع 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
- كلمة مرور SQL: كلمة مرور SQL لتسجيل الدخول إلى SQL. كلمة المرور القياسية هي: sa_s3k_pw
- 7. بعد إدخال كلمة مرور SQL، انقر فوق **اختبار الخادم**.
- إذا نجحت عملية الاختبار، فستظهر رسالة مع خلفية خضراء تحت حقل "كلمة مرور SQL".
- إذا كانت قاعدة البيانات موجودة، فستجري محاولة تنفيذ عملية ترحيل.
- 8. 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 المحلي (مستحسن).
- يمكن تعديل الملفات المثبتة تحت محرك الأقراص C:\Program Files المحلي فقط 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.
- 9. انقر فوق **التالي** < للمتابعة.
- 10. راجع ملخص ما قبل التحديث، وانقر فوق **تثبيت**.
- يظهر ملخص يتضمن جميع المكونات التي اخترت تحديثها.
- 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 يتعلق بإعدادات Access Engine (ACE) Database. يقوم برنامج الإعدادات هذا بتحديث قاعدة بيانات ACE. سيتم تحديث قاعدة البيانات إذا كانت مثبتة، وإلا، سيتم إنشاء قاعدة بيانات جديدة. قد يستغرق هذا الأمر عدة دقائق. يُرجى الانتظار حتى إغلاق مربع الحوار.
- 12. بعد اكتمال العملية، انقر فوق **التالي**، وراجع ملخص ما بعد التحديث.
- يظهر ملخص يتضمن جميع المكونات التي تم تحديثها.
- 13. انقر فوق **إنهاء** لإنهاء عملية تثبيت الإصدار المحدث من النظام.
- 14. أعد تشغيل الكمبيوتر (مستحسن).
- يبدأ تشغيل الكمبيوتر من جديد.
- 15. تأكد مما إذا تم تثبيت النظام (راجع **التأكد من تثبيت النظام**).
- إذا كان الأمر كذلك، فهذا يعني أن عملية تثبيت الإصدار المحدث من تطبيق النظام قد اكتملت.
- اسم المستخدم وكلمة المرور الافتراضيان هما **Administrator**. تذكر أن كلمة المرور (وليس اسم المستخدم) تتحسس حالة 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**.
- استناداً 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 للرجوع وإلغاء العملية.
 - عرض مربع الحوار التالي مسار التثبيت حيث سيتم الاحتفاظ بعمل النظام.
 - بشكل افتراضي، يثبت معالج التثبيت عميل النظام في محرك الأقراص C:\Program Files المحلي (مستحسن).
 - لا يمكن تعديل الملفات المثبتة ضمن محرك الأقراص C:\Program Files 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.
6. أدخل عنوان الخادم. تنسيق العنوان: Hostname:4999/tcp
7. انقر فوق التالي > للمتابعة.
 - عرض مربع الحوار التالي مسار التثبيت حيث سيتم الاحتفاظ بتطبيق Map View للنظام.
 - بشكل افتراضي، يثبت معالج التثبيت تطبيق Map View في محرك الأقراص C:\Program Files المحلي (مستحسن).
8. أدخل عنوان الاكتشاف.
 - سيتم 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 المحدث 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 المحدث من تطبيق النظام قد اكتملت.
 - اسم المستخدم وكلمة المرور الافتراضيان هما Administrator. تذكر أن كلمة المرور (وليس اسم المستخدم) حساسة لحالة الأحرف.
- التأكد من تثبيت النظام، الصفحة 11

إزالة التثبيت

3.9

لإزالة تثبيت برامج النظام بشكل كامل، 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 تحطيمها. تعتبر معظم المكونات إلزامية ولا يمكن تحطيمها.
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
 - ميثيل SQL: اسم ميثيل 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 تحطيمها.

10. انقر فوق إنهاء لإنهاء عملية إزالة تثبيت الخادم.

– يعلق 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 تحطيمها. تعتبر معظم المكونات إلزامية ولا يمكن تحطيمها.

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 تحطيمها.

8. انقر فوق إنهاء لإنهاء عملية إزالة تثبيت العميل.

– يعلق معالج التثبيت.

– يختفي النظام من قائمة البرامج.

– تختفي أيقونة النظام من سطح المكتب.

لإكمال عملية إزالة التثبيت، انتقل إلى (x86) Program Files في محرك الأقراص C: المحلي واحذف المجلد Bosch

Sicherheitssysteme.

البيانات التقنية

4

الخادم	
<ul style="list-style-type: none"> - أنظمة التشغيل المعتمدة. - قد تنجح عمليات التثبيت على أنظمة تشغيل أخرى، ولكنها بأكملها غير مشمولة بضمان. 	<ul style="list-style-type: none"> - Windows Server 2016 (64 بت أو قياسي أو مركز البيانات) - (Windows 10, version 1903 (LTSB, LTSC - ملاحظة: قاعدة البيانات الافتراضية التي يتم توفيرها مع هذا النظام هي الإصدار SQL Server 2017 Express المزود بخدمات متقدمة
<ul style="list-style-type: none"> - الحد الأدنى من متطلبات الأجهزة 	<ul style="list-style-type: none"> - 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 من 1280x1024 - 32 ألف لون على الأقل - بطاقة إيثرنت بسرعة 1 غيغابت في الثانية - منفذ USB خالٍ أو مساحة مشتركة على الشبكة للملفات التثبيت
العميل	
<ul style="list-style-type: none"> - أنظمة التشغيل المعتمدة. - قد تنجح عمليات التثبيت على أنظمة تشغيل أخرى، ولكنها بأكملها غير مشمولة بضمان. 	<ul style="list-style-type: none"> - نظام التشغيل Windows 10، الإصدار (LTSC، LTSB) 1803
<ul style="list-style-type: none"> - الحد الأدنى من متطلبات الأجهزة 	<ul style="list-style-type: none"> - 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 1920x1080 - 32 ألف لون على الأقل - DirectX® 11 - بطاقة إيثرنت بسرعة 1 غيغابت في الثانية - منفذ USB خالٍ أو مساحة مشتركة على الشبكة للملفات التثبيت
خادم MAC	
<ul style="list-style-type: none"> - الحد الأدنى من متطلبات الأجهزة 	<ul style="list-style-type: none"> - 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

إشعاراً!

يجب تثبيت الخادم والعميل معاً في الإصدار نفسه. لا تحاول الوصول إلى الخادم باستخدام إصدار عميل مختلف.





.Bosch Security Systems B.V

Torenallee 49

BA Eindhoven 5617

Netherlands

www.boschsecurity.com

Bosch Security Systems B.V., 2020 ©