Credential Management V5.5

مع Mobile Access

ل التشغيل

ar

جدول المحتويات

1 الأمان

استخدام البرنامج الأحدث

قبل تشغيل الجهاز للمرة الأولى، تأكد من تثبيت الإصدار الأحدث القابل للتطبيق من البرنامج. لضمان التناسق على مستوى الوظائف والتوافق والأداء والأمان، عليك تحديث البرامج بشكل منتظم طوال فترة عمل الجهاز. اتبع الإرشادات الواردة في وثائق المنتج فيما يتعلق بتحديثات البرامج.

توفر الروابط التالية المزيد من المعلومات:

- معلومات عامة: https://www.boschsecurity.com/xc/en/support/product-security/
- التنبيهات الأمنية، وهي عبارة عن قائمة تتضمن نقاط الضعف التي تم التعرف عليها والحلول المقترحة: https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

لا تتحمل Bosch إطلاقًا مسؤولية أي ضرر ناتج عن تشغيل منتجاتها باستخدام مكونات برمجية قديمة.

2 المقدمة

2.1 حول Credential Management وVisitor Management

Credential Management، يُشار إليه في ما بعد باسم CredMgmt، عبارة عن أداة برمجية قائمة على المستعرض تعمل إلى جانب نظام التحكم في الوصول من Bosch أو ACS. تتميز هذه الأداة بواجهة مستخدم بسيطة وبديهية، وهي تسمح حتى للمشغلين عديمي الخبرة نسبيًا من إدارة بيانات اعتماد الوصول للموظفين في الشركة والموظفين الخارجيين. بإمكان بيانات الاعتماد بحد ذاتها أن تكون بطاقات مادية أو بيانات اعتماد المحمول.

Credential Management

في CredMgmt، بإمكان مشغلي ACS إدارة كل من بيانات الاعتماد وسجلات الموظفين الذين تنتمي إليهم بيانات الاعتماد.

الكيان	إضافة	تعديل	حذف	تعيين/ إلغاء التعيين
بيانات الاعتماد المادية				نعم
بيانات اعتماد "المحمول" الافتراضية (إذا تم تثبيت Mobile Access)	نعم		نعم	نعم
التصريحات				نعم
سجلات حاملي البطاقات	نعم	نعم	نعم	

Visitor Management

في VisMgmt، يقوم مشغلو ACS بإدارة بيانات الاعتماد وسجلات الزائرين وسجلات الزيارات.

الكيان	إضافة	تعديل	حذف	تعيين/ إلغاء التعيين
بيانات الاعتماد المادية				نعم
بيانات اعتماد "المحمول" الافتراضية (إذا تم تثبيت Mobile Access)	نعم			نعم
سجلات الزائرين	نعم	نعم	نعم	
سجلات الزيارات	نعم	نعم	نعم	

2.2 حول Mobile Access

Mobile Access هو التحكم في وصول الأشخاص الذين يستخدمون بيانات اعتماد افتراضية مخزنة على أحد الأجهزة المحمولة مثل الهاتف الذكي للشخص. يتم الاحتفاظ ببيانات الاعتماد الافتراضية في نظام التحكم في الوصول الأساسي أو ما يعرف اختصارًا باسم ACS.

- يقوم مشغلو ACS بإنشاء بيانات الاعتماد الافتراضية هذه وتعيينها وإرسالها إلى الأشخاص عبر تطبيق ويب تعاوني.
- يقوم أصحاب بيانات اعتماد المحمول بتشغيل أجهزة قراءة التحكم في الوصول عبر Bluetooth من تطبيق Mobile Access على أجهزتهم المحمولة.
- يقوم مثبتو أنظمة Mobile Access بتكوين أجهزة قراءة التحكم في الوصول عبر Bluetooth من تطبيق إعداد خاص على أجهزتهم المحمولة.
- لا يخزن النظام أي بيانات شخصية على الأجهزة المحمولة.

3 التثبيت وإلغاء التثبيت

3.1 المتطلبات الأساسية للبرنامج

تقوم بتثبيت خادم CredMgmt على الكمبيوتر نفسه حيث تم تثبيت ACS (نظام التحكم في الوصول الأساسي). تنطبق متطلبات البرامج والأجهزة نفسها.
إذا لم يكن نظام التحكم في الوصول الأساسي مثبتًا بعد، فتأكد من تثبيته أولاً قبل تثبيت Credential Management.
بالنسبة للتثبيت أو التحديثات لأول مرة، يجب أن يكون ترتيب التثبيت كما يلي:
1. نظام التحكم في الوصول الرئيسي - Access Management System.
2. Credential Management و/أو Visitor Management.
3. Mobile Access.

تتضمن برامج إعداد CredMgmt وMobile Access وسائط تثبيت خاصة بها، بشكل منفصل عن ACS. ويمكن تنزيلها من كتالوجات منتجات Bosch عبر الإنترنت.

إشعار!
ضرورة وجود شهادة جذر مستقرة
قبل متابعة عمليات التثبيت أدناه، تأكد من اكتمال تثبيت ACS وترخيصه، وفقًا لدليل التثبيت الخاص به. يتضمن ذلك قرارًا نهائيًا بشأن شهادة الجذر لخادم ACS (سواء كانت موقعة ذاتيًا أو مستندة إلى CA) وتنفيذها الثابت. قد تتطلب التغييرات اللاحقة على الشهادة الجذر لخادم ACS إعادة تكوين الشهادات على جميع أجهزة الكمبيوتر وأجهزة قراءة الوصول عبر المحمول المشاركة في نظام التحكم في الوصول الخاص به.

متطلبات الخادم
الخادم هو الكمبيوتر الذي يقوم بتشغيل ACS والتطبيق CredMgmt.

نظم التشغيل	– Windows 11 Professional وEnterprise 23H2؛ – Windows Server 2019 (Version 1809) (64bit, Standard, Datacenter)؛ – Windows Server 2022 (إصدار 64 bit أو Standard أو Datacenter)
نظم إدارة قاعدة البيانات	– MS SQL Server 2019 and later استخدم دائمًا مثيل قاعدة البيانات نفسها الذي يستخدمه ACS (نظام التحكم في الوصول الأساسي)
الحد الأدنى لدقة الشاشة	دقة عالية كاملة 1920×1080
المستعرضات المدعومة	Google Chrome، وMozilla Firefox، وMicrosoft Edge (قائم على Chromium) استخدم الإصدار الأحدث من المستعرض لنظام التشغيل Windows. نظام التشغيل.

متطلبات العميل

المتطلب	الوصف
الحد الأدنى لدقة وضوح الشاشة	Full HD 1920x1080
المستعرضات المدعومة	Google Chrome, Mozilla Firefox, Microsoft Edge (Chromium based) استخدم الإصدار الأحدث من المستعرض لنظام التشغيل Windows لديك.

3.2 متطلبات الأجهزة

أجهزة قراءة التسجيل
يحتاج CredMgmt إلى قارئ تسجيل واحد على الأقل لتسجيل البطاقات المادية. يتم عادةً تثبيت أجهزة قراءة التسجيل على محطات عمل العميل. تتواصل محطة عمل العميل مع الأجهزة الطرفية عبر برنامج يسمى BoschPeripheralDeviceAddon.exe. تجد أدناه وصفًا لعملية تثبيت هذا البرنامج.
يتم دعم أجهزة قراءة التسجيل وتنسيقات البطاقات التالية.

	كود MIFARE DESFire EV1 Bosch	MIFARE DESFire EV1 CSN	MIFARE Classic CSN	HID Prox 26 bit	iCLASS 26 bit	iCLASS 35 bit	iCLASS 37 bit	iCLASS 48 bit	EM 26 bit
LECTUS enroll ARD-EDMCV002-USB	X								
OMNIKEY 5427 CK		X	X	X	X	X	X	X	X

3.2.1 إعداد الوظيفة الإضافية Peripheral Devices

يجب توفير الوظيفة الإضافية Peripheral Devices فقط على أجهزة الكمبيوتر العميل التي تتصل بأجهزة قراءة التسجيل أو الماسحات الضوئية أو الأجهزة الطرفية الأخرى. كرر الإجراء أدناه على كل كمبيوتر عميل به هذا المطلب.

1. على كمبيوتر العميل المقصود، قم بتشغيل BoschPeripheralDeviceAddon.exe من وسيط التثبيت، باعتبارك المسؤول.
   - يتم إدراج المكونات الأساسية، وهي برامج العميل وبرامج الأجهزة الطرفية المعتادة. نوصي بأن تثبت جميع المكونات المدرجة، حتى لو لم تكن الأجهزة متاحة لك حاليًا.
2. انقر فوق **التالي** لقبول حزم التثبيت الافتراضية.
3. على شاشة **تكوين العميل**
   - **دليل التثبيت:** اقبل الإعدادات الافتراضية (موصى بها)، أو قم بتغييرها على النحو المطلوب.
   - **منفذ COM:**
     - إذا كنت تستخدم قارئ تسجيل LECTUS، فأدخل رقم منفذ COM، على سبيل المثال COM3، الذي يتصل به قارئ التسجيل. تحقق من هذه القيمة في إدارة الأجهزة في Windows.
     - إذا كنت تستخدم قارئ HID OMNIKEY، فاترك هذا الحقل فارغًا.
     - تعمل الكاميرا، وSignopad والماسح الضوئي للمستندات بنظام "التوصيل والتشغيل" ولا تحتاج إلى منفذ COM. انقر فوق **سماح** عندما يطالب المستعرض بإذن الاتصال.
   - **عنوان** الخادم **والمنفذ:**
     - أدخل اسم أي كمبيوتر خادم، وهو بصورة افتراضية على الأقل كمبيوتر خادم ACS الأساسي، وأرقام المنافذ لأي خدمات خلفية تحتاج إلى التحكم في الأجهزة الطرفية.
       في كل حالة، انقر فوق **اختبار الاتصال** وانتظر التأكيد.
       انقر فوق **إضافة** لإضافة المزيد من الخوادم.
       انقر فوق **حذف** لإزالة الخوادم.
     - المنافذ الافتراضية لخدمات الواجهة الخلفية المعتادة هي:
       5806 لـ CredMgmt
       5706 لـ VisMgmt
4. انقر فوق **التالي** للاطلاع على ملخص للمكونات المطلوب تثبيتها.

5. انقر فوق **تثبيت** لبدء عملية التثبيت.
6. انقر فوق **إنهاء** لإنهاء عملية التثبيت.
7. بعد التثبيت، أعد تمهيد الكمبيوتر.

3.3 تثبيت Credential Management

المقدمة

يتم تشغيل CredMgmt كتطبيق ويب جنبًا إلى جنب مع نظام التحكم في الوصول من Bosch (ACS).
تصف الأقسام التالية عملية تثبيت مكون الواجهة الخلفية الذي يقوم بتشغيل تطبيق الويب هذا.
– يمكنك تثبيته لاستخدام قاعدة بيانات محلية أو بعيدة.
عند استخدام AMS، Visitor Management، Credential Management، Mobile Access في بيئة شبكة شركة، يوصى باستخدام الشهادات الصادرة عن مرجع مصدق في الشركة. يجب ترتيب الشهادات قبل تثبيت أي من أنظمة الواجهة الخلفية. يرجى الرجوع إلى القسم استخدام الشهادات المخصصة في دليل تثبيت AMS.

3.3.1 متطلبات CredMgmt الأساسية

مستخدم مخصص لقاعدة بيانات بعيدة (فقط إذا كنت تستخدم قاعدة بيانات بعيدة)

يدخل المستخدم `CMUser` إلى قاعدة بيانات ACS بالنيابة عن تطبيق CredMgmt.
إذا كان CredMgmt سيستخدم قاعدة بيانات على خادم قاعدة بيانات بعيدة، فاستخدم الإجراء الموضح أدناه.
مهم: لا تقم بتشغيل إعداد CredMgmt قبل إكمال هذا الإجراء.

1. على خادم قاعدة البيانات البعيدة، قم بإنشاء مستخدم مجال Windows في نفس المجال حيث يوجد ACS. استخدم الإعدادات التالية:
– **اسم المستخدم** (اسم المستخدم بحد ذاته حساس لحالة الأحرف): <ACS-Domain>\`CMUser`
– **كلمة المرور**: قم بتعيين كلمة المرور وفقًا لسياسات الأمان التي تنطبق على جميع أجهزة الكمبيوتر لديك. سجّل كلمة المرور بتأنٍ لأنها ستكون مطلوبة لإعداد CredMgmt.
– **يجب على المستخدم تغيير كلمة المرور عند تسجيل الدخول التالي**: `NO`
– **يتعذر على المستخدم تغيير كلمة المرور**: `YES`
– **عدم انتهاء صلاحية كلمة المرور إطلاقًا**: `YES`
– **تسجيل الدخول كخدمة**: `YES`
– **الحساب معطل**: `NO`

ثم أضف `CMUser` كتسجيل الدخول عن بُعد إلى SQL Server على النحو التالي:
1. افتح SQL Management Studio
2. اتصل بمثيل SQL البعيد
3. انتقل إلى **الأمان** > **تسجيل الدخول**
4. في الجزء **تحديد صفحة**، حدد **عام**
5. حدد المستخدم `CMUser`
6. في الجزء **تحديد صفحة**، حدد **أدوار الخادم**
7. حدد خانتي الاختيار `public` و`dbcreator`

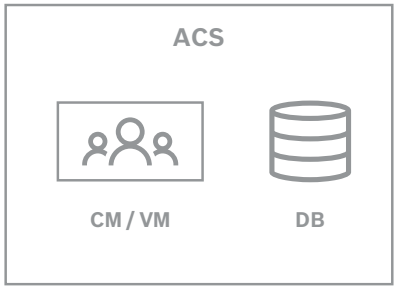
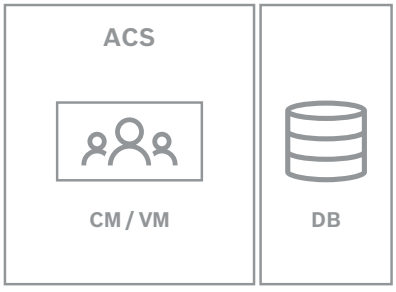
مستخدم مخصص لقاعدة البيانات المحلية (فقط إذا كنت تستخدم قاعدة بيانات محلية)

يدخل المستخدم `CMUser` إلى قاعدة بيانات ACS بالنيابة عن تطبيق CredMgmt.
لست بحاجة إلى إنشاء هذا المستخدم إذا كان CredMgmt سيستخدم قاعدة بيانات محلية، لأن برنامج إعداد CredMgmt ينشئ مستخدم `CMUser` Windows على خادم ACS بشكل تلقائي.

مستخدم مخصص في ACS

1. في ACS، أنشئ مستخدمًا يمتلك ميزة **استخدام واجهة برمجة التطبيقات (API) بشكل غير محدود**.
   - مسار الحوار في AMS: **التكوين** > **المشغّلون ومحطات العمل** > **حقوق المستخدم** > علامة التبويب: **حساب المستخدم** > **التحكم في حقوق الوصول إلى واجهة برمجة التطبيقات (API).** اختر `Unlimited access` من القائمة.
   - مسار الحوار في BIS: **التكوين المستعرض** > **الإدارة** > **المشغّلون** > اختيار المشغّل > علامة التبويب: **حقوق الوصول إلى واجهة برمجة التطبيقات (API) لتطبيق ACE.** حدد `Unlimited access`.
   - للحصول على تعليمات أكثر تفصيلاً، راجع الفصل **تعيين ملفات تعريف المستخدم (المشغّل)** في دليل مشغّل ACS.
2. دوّن اسم المستخدم وكلمة المرور بعناية، لأن معالج تثبيت تطبيق الويب سيطلب منك إدخالهما.

3.3.2 إجراء التثبيت

CredMgmt مع قاعدة بيانات محلية	CredMgmt مع قاعدة بيانات بعيدة
	

الإجراء

1. على خادم ACS، قم بتشغيل `BoschCredentialManagementServer.exe` كمسؤول.
   - يفتح برنامج التثبيت
2. على شاشة **المكونات الأساسية**، حدد `Bosch Credential Management` وانقر فوق **التالي**
3. اقرأ بعناية وانقر على **قبول** إذا كنت ترغب في قبول اتفاقية ترخيص المستخدم النهائي (EULA). يمكن متابعة التثبيت فقط إذا قمت بذلك.
4. استعرض وحدد مجلد وجهة للتثبيت، أو اقبل الوجهة الافتراضية (مستحسن)، وانقر فوق **التالي**.
5. في الشاشة **SQL Server**، حدد أحد بديلين لموقع قاعدة البيانات. التكوينات مختلفة قليلاً. اختر بديلًا للخطوة التالية:
   - البديل 1 خيار **قاعدة البيانات المحلية**:
     - يعثر برنامج الإعداد على قاعدة البيانات المحلية ويحددها مسبقًا.
     - أدخل كلمة مرور SQL لمستخدم مسؤول (القيمة الافتراضية هي `sa`)
     - انقر فوق **اختبار الاتصال**
     - انقر فوق **التالي**
   - البديل 2 خيار **قاعدة البيانات البعيدة**
     - أدخل اسم SQL Server الموجود على الشبكة
     - أدخل اسم مثيل SQL
     - أدخل كلمة مرور SQL لمستخدم مسؤول (القيمة الافتراضية هي `sa`)
     - انقر فوق **اختبار الاتصال**
     - تحقق من اسم المستخدم وأدخل كلمة مرور مستخدم مسؤول Windows وSQL التي أنشأتها لاستخدام قاعدة البيانات البعيدة (انظر المتطلبات الأساسية أعلاه)
     - انقر فوق **التالي**
6. على شاشة **تكوين الوصول إلى ACS**:

- أدخل اسم المضيف لخادم ACS.
- أدخل اسم مستخدم ACS مع استخدام غير محدود لواجهة برمجة التطبيقات (API) (راجع المتطلبات الأساسية أعلاه).
- أدخل كلمة مرور ACS لمستخدم ACS هذا وقم بتأكيدها.

7. انقر فوق **التالي**
8. على شاشة **تكوين خادم الهوية**
- خادم الهوية الافتراضي (المحدد مسبقًا) هو خادم ACS الأساسي مع المنفذ 44333 `https://<NameOfACSserver>:44333`
- انقر فوق **اختبار الاتصال**
- إذا فشل الاختبار، فأعد التحقق من توفر خادم الهوية.
- انقر فوق **التالي**

9. في شاشة **المكونات الأساسية**، تأكد من تحديد CredMgmt وانقر على **تثبيت**
10. عند اكتمال التثبيت، ابدأ تشغيل CredMgmt بعنوان URL التالي:
`https://<NameOfACSserver>:5806`

3.4 تثبيت Mobile Access

المقدمة

توفر خدمة الواجهة الخلفية لتطبيق Mobile Access وظيفة الوصول عبر المحمول لكل من Credential Management وVisitor Management.

احرص على استخدام الإصدار الأحدث من نظام التحكم في الوصول الرئيسي والإصدار الأحدث من الواجهة الخلفية لتطبيق Mobile Access.

ملاحظة: عند قيامك باستخدام كل من CredMgmt وVisMgmt، عليك تثبيت Mobile Access مرة واحدة فقط.

- يمكنك تثبيته على نفس الخادم حيث تم تثبيت ACS (التثبيت في نفس الموقع)، أو على خادم منفصل (التثبيت الموزع).
- يمكنك تثبيته لاستخدام قاعدة بيانات محلية أو بعيدة.

قابلية الوصول إلى خدمة الواجهة الخلفية Mobile Access

يجب أن يكون وصول الأجهزة المحمولة إلى خدمة الواجهة الخلفية لتطبيق Mobile Access ممكنًا بشكل مستمر.

لأسباب تتعلق بالأمان، من غير المرجح أن يتم منح الأجهزة المحمولة إمكانية الوصول إلى خادم ACS عبر الشبكة. وبالتالي، يوصى باستخدام التثبيت الموزع. يسمح لك ذلك بتشغيل خدمة الواجهة الخلفية لتطبيق Mobile Access على خادم "سحابي" متاح على نطاق واسع.

3.4.1 نظرة عامة على التثبيت والتكوين والاستخدام

يتطلب Mobile Access عدة مكونات للعمل بصورة متسقة. نسرد المراحل الإجمالية هنا، ونتناول المتطلبات والإجراءات الخاصة بكل منها في الأقسام التالية من هذا الفصل:

إعداد خادم ACS

1. يتم تثبيت ACS وترخيصه وتشغيله، مع شهادة جذر دائمة وأجهزة قراءة وصول متوافقة. يتم تعريف المشغلين فيه مع تصريحات لإدارة Mobile Access.

إعداد Mobile Access

1. يقوم مسؤول النظام بتثبيت تطبيق واحد أو كليهما من تطبيقات الويب التي تستخدم Mobile Access، إما Credential Management أو Visitor Management على ACS.
2. يقوم مسؤول النظام بتثبيت الواجهة الخلفية لتطبيق Mobile Access.
3. يقوم مسؤول النظام بتنشيط Mobile Access في تطبيقات الويب المثبتة هذه.

إعداد أجهزة القراءة

1. يقوم مسؤول النظام بإنشاء مثبت (شخص مصرح له بتكوين أجهزة قراءة Mobile Access) في التطبيق CredMgmt.
2. يقوم المثبت بتنزيل تطبيق المثبت ("Setup Access") على جهازه المحمول من App Store العام المعتاد على الجهاز.
3. يرسل مسؤول النظام دعوة إلى المثبت المعين.
4. يقبل المثبت الدعوة في تطبيق المثبت. تخوّل هذه الدعوة المثبت تكوين أجهزة قراءة الوصول لـ Mobile Access.
5. تقوم المثبت بتكوين أجهزة القراءة باستخدام تطبيق المثبت.

استخدام Mobile Access

1. يقوم حاملو بيانات الاعتماد المؤهلون لاستخدام Mobile Access بتنزيل تطبيق حامل بيانات الاعتماد ("Mobile Access") إلى أجهزتهم المحمولة من App Store العام المعتاد للجهاز.
2. يرسل المشغلون من CredMgmt و/ أو VisMgmt بيانات اعتماد الهاتف المحمول عن طريق رمز الاستجابة السريعة أو البريد الإلكتروني إلى حاملي بيانات الاعتماد المؤهلين.
3. يقرأ حاملو بيانات الاعتماد رمز الاستجابة السريعة أو البريد الإلكتروني في تطبيق حامل بيانات الاعتماد ("Mobile Access"). يمكّن ذلك أجهزتهم المحمولة من العمل كبيانات اعتماد فعلية عند تشغيل التطبيق.

3.4.2 المتطلبات الأساسية لأجهزة Mobile Access

يحتاج Mobile Access إلى أجهزة قراءة الوصول مع وحدة نمطية BLE. تعد أجهزة القراءة من Bosch التالية مناسبة:

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

- يشير B وW إلى اللونين، الأسود أو الأبيض
- يشير O إلى OSDP
- يشير K إلى وجود لوحة مفاتيح
- يعني الحرف M ملاءمة Mobile Access

3.4.3 المتطلبات الأساسية لتكوين Mobile Access

مستخدم مخصص لقاعدة بيانات بعيدة (إذا كنت تستخدم قاعدة بيانات بعيدة)

إذا كان Mobile Access سيستخدم قاعدة بيانات على خادم قاعدة بيانات بعيدة، فقم بإنشاء مستخدم مسؤول باسم `MAUser` وتكوينه على هذا الخادم البعيد، في كل من Windows وSQL Server. في أثناء الإعداد الموضح أدناه، حدد خيار خادم قاعدة البيانات البعيدة وأدخل كلمة المرور التي حددتها لـ `MAUser`.

مهم: لا تقم بتشغيل إعداد Mobile Access قبل إكمال هذا الإجراء.

الإجراء

1. على خادم قاعدة البيانات البعيدة، قم بإنشاء مستخدم مجال Windows في نفس المجال حيث يوجد ACS. استخدم الإعدادات التالية:

- **اسم المستخدم** (اسم المستخدم بحد ذاته حساس لحالة الأحرف): <ACS-Domain>\`MAUser`
- **كلمة المرور**: قم بتعيين كلمة المرور وفقًا لسياسات الأمان التي تنطبق على جميع أجهزة الكمبيوتر لديك. سجّل كلمة المرور بتأنٍ لأنها ستكون مطلوبة لإعداد Mobile Access.
- **يجب على المستخدم تغيير كلمة المرور عند تسجيل الدخول التالي**: `NO`
- **يتعذر على المستخدم تغيير كلمة المرور**: `YES`
- **عدم انتهاء صلاحية كلمة المرور إطلاقًا**: `YES`
- **تسجيل الدخول كخدمة**: `YES`
- **الحساب معطل**: `NO`

ثم أضف `MAUser` كتسجيل الدخول عن بُعد إلى SQL Server على النحو التالي:

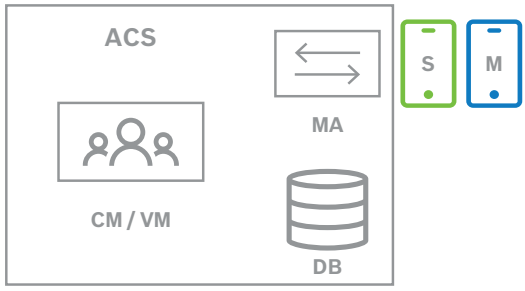
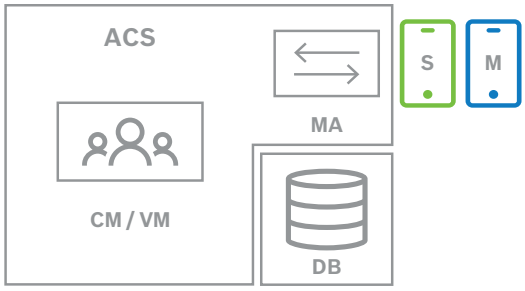
1. افتح SQL Management Studio

2. اتصل بمثيل SQL البعيد
3. انتقل إلى **الأمان** > **تسجيل الدخول**
4. في الجزء **تحديد صفحة**، حدد **عام**
5. حدد المستخدم `MAUser`
6. في الجزء **تحديد صفحة**، حدد **أدوار الخادم**
7. حدد خانتي الاختيار `public` و`dbcreator`

مستخدم مخصص لقاعدة البيانات المحلية (إذا كنت تستخدم قاعدة بيانات محلية)
يدخل المستخدم `MAUser` إلى قاعدة بيانات ACS بالنيابة عن تطبيق Mobile Access.
لست بحاجة إلى إنشاء هذا المستخدم إذا كنت تستخدم إحدى قواعد البيانات المحلية. يقوم برنامج إعداد Mobile Access بإنشاء مستخدم `MAUser` Windows على خادم ACS تلقائيًا.

3.4.4 إجراء التثبيت في نفس الموقع

يعني **التثبيت في نفس الموقع** أن خدمة الواجهة الخلفية لتطبيق Mobile Access تعمل على نفس الخادم، مثل ACS.
يعني **التثبيت الموزع** أن خدمة الواجهة الخلفية لتطبيق Mobile Access تعمل على خادم مختلف، على سبيل المثال "خادم سحابي".
بالنسبة لخيار التثبيت الموزع، راجع القسم التالي **إجراء للتثبيت الموزع**.

الموقع المشترك مع قاعدة البيانات المحلية	الموقع المشترك مع قاعدة البيانات البعيدة
	

المفتاح	المعنى
ACS	نظام التحكم في الوصول الأساسي AMS أو BIS-ACE
CM/VM	الواجهة الخلفية لتطبيق الويب: Credential Management أو Visitor Management
DB	قاعدة بيانات ACS الرئيسية
MA	الواجهة الخلفية لتطبيق Mobile Access
S	تطبيق مثبت "Setup Access" لمثبتي ومكوني النظام
M	تطبيق Mobile Access للأجهزة المحمولة لأصحاب بيانات الاعتماد العادية.

الإجراء

1. على خادم ACS، والذي يعتبر أيضًا خادم Mobile Access للتثبيت في نفس الموقع، قم بتشغيل `BoschMobileAccessBackend.exe` كمسؤول
   – يفتح برنامج الإعداد
2. على شاشة **الموقع**، حدد نوع الإعداد: **الموقع المشترك**
3. في شاشة **المكونات**، تحقق من تحديد `Bosch Mobile Access` وانقر فوق **التالي**
4. على شاشة **اتفاقية ترخيص المستخدم النهائي**، اقرأ بعناية وانقر فوق **قبول** إذا كنت ترغب في قبول اتفاقية ترخيص المستخدم النهائي (EULA). يمكن متابعة التثبيت فقط إذا قمت بذلك.
5. في الشاشة **دليل التثبيت**:

- استعرض وحدد مجلد وجهة للتثبيت، أو اقبل الوجهة الافتراضية (مستحسن)
- أدخل اسم شركتك كما سيتم عرضه في تطبيق الجوال وفي قوالب البريد الإلكتروني بتنسيق HTML
- انقر فوق **التالي**

6. على شاشة **الشهادة**
- أدخل اسم المضيف حيث سيتم تشغيل الواجهة الخلفية لتطبيق Mobile Access
- إذا رغبت في ذلك، أو إذا لم توفر الشبكة أي تحليل لاسم مضيف، فأدخل عنوان IP لهذا المضيف
- انقر فوق **التالي**

7. في الشاشة **SQL Server**، حدد أحد بديلين لموقع قاعدة البيانات. التكوينات مختلفة قليلاً. اختر بديلًا للخطوة التالية:
- البديل 1 خيار **قاعدة البيانات المحلية**:
  - يعثر برنامج الإعداد على قاعدة البيانات المحلية ويحددها مسبقًا.
  - أدخل كلمة مرور SQL لمستخدم مسؤول (القيمة الافتراضية هي sa)
  - انقر فوق **اختبار الاتصال**
  - انقر فوق **التالي**
- البديل 2 خيار **قاعدة البيانات البعيدة**
  - أدخل اسم SQL Server الموجود على الشبكة
  - أدخل اسم مثيل SQL
  - أدخل كلمة مرور SQL لمستخدم مسؤول (القيمة الافتراضية هي sa)
  - انقر فوق **اختبار الاتصال**
  - تحقق من اسم المستخدم وأدخل كلمة مرور مستخدم مسؤول Windows وSQL التي أنشأتها لاستخدام قاعدة البيانات البعيدة (انظر المتطلبات الأساسية أعلاه)
  - انقر فوق **التالي**

8. على شاشة **تكوين خادم الهوية**
- خادم الهوية الافتراضي (المحدد مسبقًا) هو خادم ACS الأساسي مع المنفذ 44333 https://<NameOfACSserver>:44333
- انقر فوق **اختبار الاتصال**
- إذا فشل الاختبار، فأعد التحقق من توفر خادم الهوية.
- انقر فوق **التالي**

9. على شاشة **المكونات الأساسية**، تأكد من تحديد **Bosch Mobile Access** وانقر فوق **تثبيت**
- يكتمل معالج التثبيت

10. انقر فوق **التالي**
11. في الشاشة **المكونات الأساسية**، تحقق من اكتمال التثبيت بنجاح، وانقر فوق **إنهاء**
12. في تطبيق Windows Services، تحقق من تشغيل الخدمة Bosch Mobile Access.

3.4.5 إجراء التثبيت الموزع

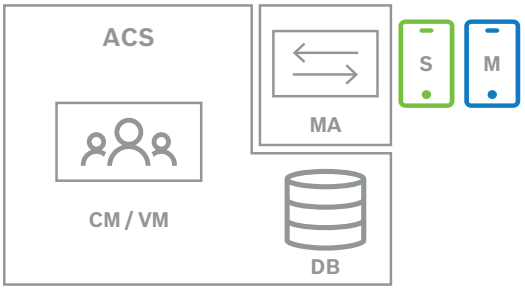
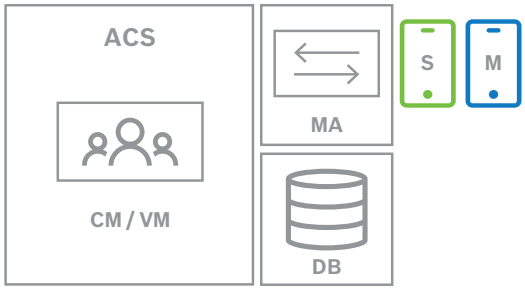
يعني **التثبيت في نفس الموقع** أن خدمة الواجهة الخلفية لتطبيق Mobile Access تعمل على نفس الخادم، مثل ACS.

يعني **التثبيت الموزع** أن خدمة الواجهة الخلفية لتطبيق Mobile Access تعمل على خادم مختلف، على سبيل المثال "خادم سحابي".

بالنسبة لخيار الموقع المشترك، راجع القسم السابق **إجراء التثبيت في نفس الموقع**.

على خادم الواجهة الخلفية الموزع لتطبيق Mobile Access، يلزم توفر المتطلبات الأساسية التالية قبل بدء تثبيت Mobile Access أو عند تحديث النظام. هذا غير مطلوب في البيئة ذات الموقع المشترك:

- ثبّت **ASP.NET Core 8.0 Runtime (v8.0.2) Hosting Bundle** على خادم الواجهة الخلفية الموزع لتطبيق Mobile Access قبل تشغيل مثبت Mobile Access.
- استخدم الرابط التالي لتنزيل حزمة الاستضافة المطلوبة: https://dotnet.microsoft.com/en-us/download/dotnet/thank-you/runtime-aspnetcore-8.0.2-windows-hosting-bundle-installer.

موزع مع قاعدة البيانات المحلية	موزع مع قاعدة البيانات البعيدة
	

المفتاح	المعنى
ACS	نظام التحكم في الوصول الأساسي AMS أو BIS-ACE
CM/VM	الواجهة الخلفية لتطبيق الويب: Credential Management أو Visitor Management
DB	قاعدة بيانات ACS الرئيسية
MA	الواجهة الخلفية لتطبيق Mobile Access
S	تطبيق مثبت "Setup Access" لمثبتي ومكوني النظام
M	تطبيق Mobile Access للأجهزة المحمولة لأصحاب بيانات الاعتماد العادية.

الإجراء

تأكد من أنك تستخدم الإصدار الأحدث من نظام التحكم في الوصول الرئيسي.

1. على خادم الواجهة الخلفية لتطبيق Mobile Access، قم بتشغيل `BoschMobileAccessBackend.exe` كمسؤول.
   - يفتح برنامج الإعداد
2. على الشاشة **الموقع**، حدد نوع الإعداد: **موزع**
3. على شاشة **المضيف**، حدد **Mobile Access الواجهة الخلفية** وانقر فوق **التالي**
   - ملاحظة: سيتم استخدام خيار **ACS** لاحقًا في هذا الإجراء، عندما نقوم بتثبيت Mobile Access على خادم ACS.
4. على شاشة **المكونات**، تأكد من تحديد **Bosch Mobile Access**، وانقر فوق **التالي**
5. على شاشة **اتفاقية ترخيص المستخدم النهائي**، اقرأ بعناية وانقر فوق **قبول** إذا كنت ترغب في قبول اتفاقية ترخيص المستخدم النهائي (EULA). يمكن متابعة التثبيت فقط إذا قمت بذلك.
6. في الشاشة **دليل التثبيت**:
   - استعرض وحدد مجلد وجهة للتثبيت، أو اقبل الوجهة الافتراضية (مستحسن)
   - أدخل اسم شركتك كما سيتم عرضه في تطبيق الجوال وفي قوالب البريد الإلكتروني بتنسيق HTML
   - انقر فوق **التالي**
7. في الشاشة **SQL Server**، حدد أحد بديلين لموقع قاعدة البيانات. التكوينات مختلفة قليلاً. اختر بديلًا للخطوة التالية:
   - البديل 1 خيار **قاعدة البيانات المحلية**:
     - يعثر برنامج الإعداد على قاعدة البيانات المحلية ويحددها مسبقًا.
     - أدخل كلمة مرور SQL لمستخدم مسؤول (القيمة الافتراضية هي `sa`)
     - انقر فوق **اختبار الاتصال**
     - انقر فوق **التالي**
   - البديل 2 خيار **قاعدة البيانات البعيدة**
     - أدخل اسم SQL Server الموجود على الشبكة
     - أدخل اسم مثيل SQL
     - أدخل كلمة مرور SQL لمستخدم مسؤول (القيمة الافتراضية هي `sa`)
     - انقر فوق **اختبار الاتصال**

- تحقق من اسم المستخدم وأدخل كلمة مرور مستخدم مسؤول Windows وSQL التي أنشأتها لاستخدام قاعدة البيانات البعيدة (انظر المتطلبات الأساسية أعلاه)
- انقر فوق **التالي**

في هذه المرحلة من التثبيت الموزع، يجب عليك التبديل إلى الكمبيوتر حيث يتم تشغيل خادم *ACS* وتكوين Mobile Access هناك، بحيث يمكنه الاتصال لاحقًا بالواجهة الخلفية لتطبيق Mobile Access على الكمبيوتر المحلي.
بعد الانتهاء من الخطوات المشار إليها هناك، سيرشدك برنامج الإعداد إلى الخادم المحلي للتأكيد والمتابعة.

1. على كمبيوتر خادم ACS، قم بتشغيل `BoschMobileAccessBackend.exe` كمسؤول
- يفتح برنامج الإعداد
2. على الشاشة **الموقع**، حدد نوع الإعداد: **موزع**
3. على شاشة **المضيف**، حدد **ACS** وانقر فوق **التالي**
4. في شاشة **معالج المرافق**، اقرأ النص التوضيحي وانقر فوق **التالي**
5. على شاشة **الشهادة**
- أدخل اسم المضيف حيث سيتم تشغيل الواجهة الخلفية لتطبيق Mobile Access
- إذا رغبت في ذلك، أو إذا لم توفر الشبكة أي تحليل لاسم مضيف، فأدخل عنوان IP لهذا المضيف
- انقر فوق **التالي**
6. على شاشة **تكوين خادم الهوية**
- خادم الهوية الافتراضي (المحدد مسبقًا) هو خادم ACS الأساسي مع المنفذ `https:// 44333` `<NameOfACSserver>:44333`
- انقر فوق **اختبار الاتصال**
- إذا فشل الاختبار، فأعد التحقق من توفر خادم الهوية.
- انقر فوق **التالي**
7. في الشاشة **إنشاء ملف**
، ننشئ ملف تكوين في ملف ZIP محمي بكلمة مرور، ونجعله متاحًا للواجهة الخلفية في Mobile Access.
- **كلمة مرور المستخدم**: أدخل كلمة مرور لملف ZIP
- **ملف التكوين**: أدخل مجلدًا أو استعرض وصولاً إلى مجلد لوضع ملف ZIP فيه. لاحظ أن هذا المجلد يجب أن يكون في متناول الكمبيوتر حيث يتم تشغيل الواجهة الخلفية لتطبيق Mobile Access. إذا لم يكن الأمر كذلك، فيجب عليك نقل الملف المضغوط بصيغة ZIP إلى هذا الكمبيوتر بوسائل أخرى.
- انقر فوق **إنشاء ملف التكوين**
- انقر فوق **التالي**
8. في الشاشة **تبديل الجهاز**، اكتملت الآن
خطوات التثبيت على خادم ACS.
- انقر فوق **تأكيد** لإنهاء الإجراء

في هذه المرحلة من التثبيت الموزع، ستعود إلى برنامج الإعداد على كمبيوتر الواجهة الخلفية لـ Mobile Access.

1. عد إلى برنامج الإعداد `BoschMobileAccessBackend.exe` على كمبيوتر خادم Bosch Mobile Access.
2. في صفحة **تبديل الجهاز**
- حدد خانة الاختيار باسم **لقد أكملتُ بالفعل الخطوات المطلوبة على جهاز ACS**
- انقر فوق **التالي**
3. في الشاشة **تحميل الملف**
- **تحميل ملف التكوين:** حدد ملف التكوين الذي قمت بإنشائه على خادم ACS
- **التحقق من كلمة المرور:** أدخل كلمة المرور التي قمت بتعيينها لملف ZIP على خادم ACS

- بعد إدخال كلمة المرور الصحيحة، يمكنك النقر فوق **التالي** لقراءة ملف التكوين
4. على شاشة **المكونات الأساسية**، تأكد من تحديد **Bosch Mobile Access** وانقر فوق **تثبيت**
- يكتمل معالج التثبيت
5. انقر فوق **التالي**
6. في الشاشة **المكونات الأساسية**، تحقق من اكتمال التثبيت بنجاح، وانقر فوق **إنهاء**
7. في تطبيق Windows Services، تحقق من تشغيل الخدمة Bosch Mobile Access.

3.5 شهادات الاتصال الآمن

لإنشاء اتصال آمن بين المستعرض على جهاز العميل وخادم ACS، انسخ الشهادة التالية من خادم ACS إلى أجهزة الكمبيوتر العميل. استخدم حسابًا يتمتع بحقوق مسؤول Windows لتثبيتها.

المسار المعتاد للشهادة هو:

- <محرك أقراص التثبيت>:

```
Bosch Sicherheitssysteme\Access Management System\Certificates\Bosch\
Security System Internal CA - BISAMS.cer
```

ملاحظة: بعد نشر الشهادة، أعد تشغيل إما خدمة الواجهة الخلفية لتطبيق Mobile Access أو خدمة Bosch Credential Management وخدمة Bosch Visitor Management.

نظرة عامة على تحويل الشهادات

إلى → **من** ↓	**ACS**	واجهة **MA** Mobile Access الخلفية	**DB** قاعدة البيانات	**S** تطبيق الإعداد	**M** تطبيق الوصول إلى حامل البطاقة	**R** القارئ
ACS	/	يتم التحويل بواسطة معالج الإعداد (عن طريق أداة الشهادة)	/	/	/	/
واجهة **MA** Mobile Access الخلفية	يتم التحويل بواسطة معالج إعداد MA	/	/	يتم التحويل عن طريق التسجيل في رمز الاستجابة السريعة، يتم التحديث عبر إشعار الدفع	يتم التحويل عن طريق التسجيل في رمز الاستجابة السريعة، يتم التحديث عبر إشعار الدفع	/
DB قاعدة البيانات	/	/	/	/	/	/
S تطبيق الإعداد	/	يتم التحويل عن طريق التسجيل باستخدام رمز الاستجابة السريعة	/	/	/	/

M تطبيق الوصول إلى حامل البطاقة	/	يتم التحويل عن طريق التسجيل باستخدام رمز الاستجابة السريعة	/	/	/	/

3.5.1 شهادات للمستعرض Firefox

يمكنك تجاهل هذا القسم إذا كنت لا تستخدم المستعرض Firefox.

يتعامل المستعرض Firefox مع شهادات الجذر بشكل مختلف: لا يستشير Firefox مخزن شهادات Windows للحصول على شهادات الجذر الموثوقة. بدلاً من ذلك، يحتفظ كل ملف تعريف مستعرض بمخزن خاص به للشهادات الجذر. لمزيد من التفاصيل، يرجى الرجوع إلى https://support.mozilla.org/en-US/kb/setting-certificate-authorities-firefox
تقدم صفحة الويب هذه أيضًا إرشادات تفرض على Firefox استخدام مخزن شهادات Windows لجميع المستخدمين.
بدلاً من ذلك، يمكنك استيراد الشهادات الافتراضية كما هو موضح أدناه. ملاحظة:

- يجب عليك استيراد الشهادات لكل مستخدم وملف تعريف Firefox.
- تُعد شهادة الخادم الموضحة أدناه الشهادة الافتراضية التي تم إنشاؤها بواسطة عملية التثبيت. إذا كنت قد اشتريت شهادتك الخاصة من مرجع مصدق، فيمكنك استخدامها بدلاً من ذلك.

استيراد الشهادات إلى مخزن شهادات Firefox

للوصول إلى خادم ACS من Firefox على الكمبيوتر العميل، يمكنك استيراد الشهادة الافتراضية التالية من الخادم:

- <محرك أقراص التثبيت>:

```
Bosch Sicherheitssysteme\Access Management System\Certificates\Bosch\
Security System Internal CA - BISAMS.cer
```

أو، بالنسبة إلى BIS ACE، يمكنك أيضًا تنزيل الشهادة من خلال الويب:

- `HTTP://:`<اسم المضيف>/<اسم المضيف>`.cer`

الأجهزة الطرفية: للوصول إلى جهاز طرفي متصل، مثل ماسح ضوئي للمستندات أو ماسح ضوئي التوقيعات، من Firefox على الكمبيوتر العميل، يمكنك استخدام الشهادة الافتراضية. يمكنك العثور عليه على الكمبيوتر العميل في الموقع التالي:

```
installation drive>:\Program Files (x86)\Bosch Sicherheitssysteme\<
Bosch Peripheral Device Addon\BoschAcePeripheralDeviceAddonHardware CA.cer
```

الإجراء (كرر لكل شهادة وملف تعريف Firefox):

استخدم الإجراء التالي على الكمبيوتر العميل لتثبيت الشهادات التي تحتاج إليها:

1. حدد موقع الشهادة التي تريد تثبيتها.
2. افتح المستعرض Firefox واكتب `about:preferences` في شريط العنوان.
   - تفتح صفحة خيارات.
3. في الحقل **بحث في الخيارات**، اكتب `certificate`
   - يظهر الزر **عرض الشهادات** على الصفحة.
4. انقر فوق الزر **عرض الشهادات**.
   - يفتح مربع الحوار **إدارة الشهادات** مع عدة علامات تبويب
5. حدد علامة التبويب **الشهادات**
6. انقر فوق **استيراد**...
   - يفتح مربع حوار محدد الشهادة.
7. حدد الشهادة التي حددتها في الخطوة 1، وانقر فوق **فتح**.

– يفتح مربع الحوار **تنزيل الشهادة**.
8. حدد **الثقة بالمرجع المصدق هذا لتحديد مواقع الويب** وانقر فوق **موافق**.
– يُغلق مربع الحوار **تنزيل الشهادة**
9. في مربع الحوار **مدير الشهادات**، انقر فوق **موافق**.
– انتهى إجراء استيراد الشهادة.

3.5.2 شهادات للمستعرض Chrome

يمكنك تجاهل هذا القسم إذا كنت لا تستخدم المستعرض Chrome.
يرجى الرجوع إلى ملاحظات الإصدار الخاصة بـ ACS لمعرفة التغييرات التي تم إجراؤها على معالجة الشهادة في المستعرض Chrome.
لتثبيت شهادة على المستعرض Chrome ضمن نوافذ Microsoft:

1. قم بتنزيل ملف الشهادة.
2. انتقل إلى صفحة إعدادات (`chrome://settings`) Chrome وانقر فوق **خيارات متقدمة**.
3. ضمن **الخصوصية والأمان**، انقر فوق **إدارة الشهادات**
4. في علامة التبويب **الشهادات الخاصة بك**، انقر فوق **استيراد** لبدء عملية تثبيت الشهادة:
– يظهر معالج استيراد الشهادة.
5. حدد ملف الشهادة وأكمل المعالج.
6. سيتم عرض الشهادة المثبتة في علامة التبويب **الشهادات الجذر الموثوقة**.

3.5.3 تثبيت تطبيقات Mobile Access

المقدمة

توفر Bosch التطبيقات التالية لتطبيق Mobile Access
– Bosch Mobile Access: تطبيق حامل البطاقة لتخزين بيانات الاعتماد الافتراضية ونقلها عبر Bluetooth إلى أجهزة القراءة التي تم تكوينها من أجل Mobile Access. ثم يمنح هذا القارئ الوصول أو يرفضه اعتمادًا على ما إذا كانت إحدى بيانات الاعتماد المخزنة للتطبيق صالحة له.
– Bosch Setup Access: تطبيق مثبت لفحص القراء وتكوينهم عبر Bluetooth.
بإمكان المشغلين المصرح لهم لكل من Visitor Management وCredential Management إرسال بيانات اعتماد افتراضية لكل من تطبيقات حامل البطاقة والمثبت.

طالما أن تطبيق حامل البطاقة قيد التشغيل ويتم تنشيط Bluetooth على الجهاز المحمول، يمكنك استخدامه كما لو كان بطاقة فعلية. لا حاجة لإعطاء أوامر من التطبيق أو حتى لفتح الشاشة.

إشعار!
هام: لا تقم بتشغيل تطبيقات حامل البطاقة والمثبت في الوقت ذاته
تأكد من عدم استخدام أي شخص لتطبيق المثبت عندما يكون تطبيق حامل البطاقة قيد الاستخدام، والعكس صحيح.

الإجراء

يمكن تنزيل تطبيقات Bosch Mobile Access من متاجر تطبيقات Google وApple وتثبيتها بالطريقة المعتادة. وأسماؤها في متاجر التطبيقات هي:
– Bosch Mobile Access
– Bosch Setup Access

3.6 إصلاح عمليات تثبيت Mobile Access

المقدمة

لتحديث الثنائيات، أو لإعادة إنشاء شهادة Mobile Access، يمكنك تشغيل مثبت الإصدار الحالي أو إصدار لاحق من Mobile Access، عبر عملية تثبيت حالية:

الإجراء

1. على خادم الواجهة الخلفية لتطبيق Mobile Access، قم بتشغيل الإصدار الجديد من `BoschMobileAccessBackend.exe` كمسؤول.

– لاحظ أنه بالنسبة لعمليات التثبيت في نفس الموقع، خادم الواجهة الخلفية لتطبيق Mobile Access هو نفسه خادم ACS.

2. اتبع معالج الإعداد، مع إجراء نفس الإعدادات كما في التثبيت الأصلي.

– لإعادة إنشاء الشهادة، في شاشة **الشهادات**، حدد زر الاختيار **إعادة إنشاء الشهادة**.

3. بعد أن ينهي برنامج الإعداد عمله، أعد تشغيل الخادم.
4. ابدأ جلسة تسجيل دخول جديدة على كل تطبيق ويب يستخدم Mobile Access (CredMgmt أو VisMgmt أو كليهما).

– سيستخدم تطبيق الويب الثنائيات الجديدة.

– إذا حددت **إعادة إنشاء الشهادة**، فستستند أي دعوات أخرى ترسلها إلى مستخدمي ومثبتي Mobile Access إلى شهادة Mobile Access الجديدة.

3.7 إزالة تثبيت البرامج

لإزالة تثبيت البرامج من الخادم أو العميل:

1. مع حقوق مسؤول Windows، ابدأ البرنامج الخاص بنظام Windows **إضافة البرامج أو إزالتها**.
2. حدد البرنامج (الخادم أو العميل) وانقر فوق **إلغاء التثبيت**.
3. (لـ Visitor Management وللخادم فقط) حدد ما إذا كنت تريد إزالة قاعدة بيانات إدارة الزائرين إلى جانب البرنامج.

– **ملاحظة**: تحتوي قاعدة البيانات على سجلات لكل الزيارات التي تم تسجيلها عندما كان البرنامج قيد الاستخدام. قد ترغب في أرشفة قاعدة البيانات أو نقلها إلى تثبيت آخر.

4. حدد ما إذا كنت تريد إزالة ملفات السجلات.
5. أكمل إزالة التثبيت بالطريقة المعتادة.
6. (موصى به) أعد تمهيد الكمبيوتر لتضمن التعديل الكامل لسجل Windows.

ملاحظة: بعد إلغاء تثبيت الواجهة الخلفية لتطبيق Mobile Access، يجب إزالة آثار التكوين التالية يدويًا إذا رغبت في ذلك:

– **MAUser** - يبقى هذا المستخدم موجودًا بعد إلغاء التثبيت. ويجب على المسؤول إزالته يدويًا.

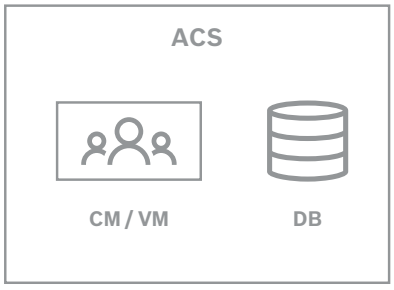
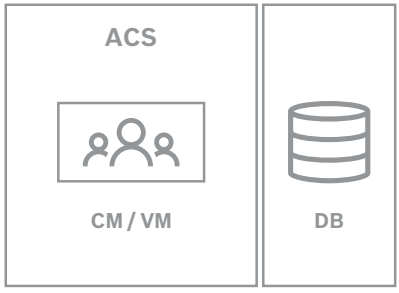
– **الشهادات** - استخدم إدارة شهادات الكمبيوتر لإزالة كافة الشهادات المثبتة يدويًا بسبب تثبيت Mobile Access.

– **تكوين خادم المعرف لـ Mobile Access** - يبقى الملف *appsettings.Extension.MobileAccessBackend* موجودًا بعد إلغاء تثبيت الواجهة الخلفية. احذفه يدويًا.

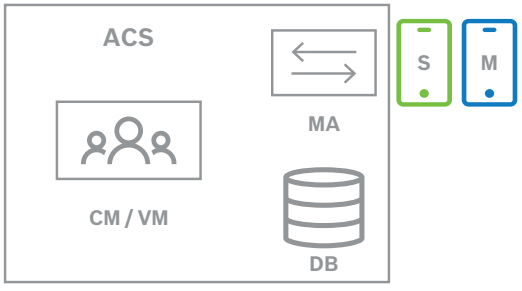
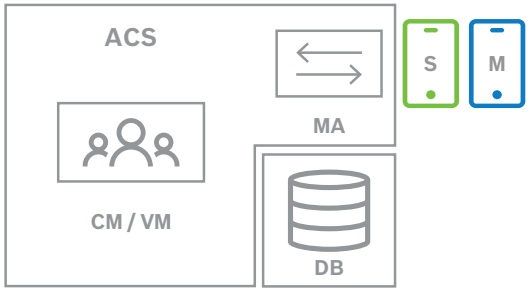
4 نظرة عامة على Credential Management

يوضح ما يلي الطبولوجيات المحتملة لعمليات تثبيت Credential Management، مع Mobile Access وبدونه. يمثل كل صندوق مرفق جهاز كمبيوتر منفصلاً.

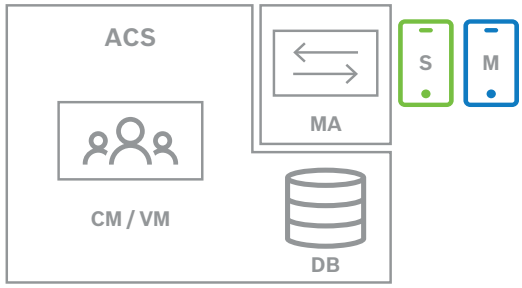
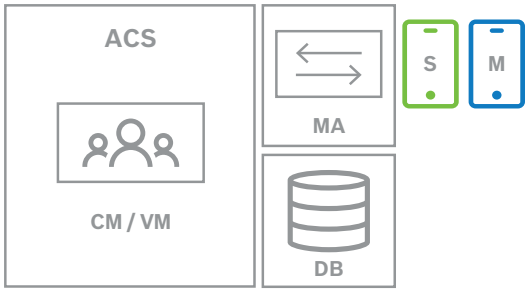
المفتاح	المعنى
ACS	نظام التحكم في الوصول الأساسي AMS أو BIS-ACE
CM/VM	الواجهة الخلفية لتطبيق الويب: Credential Management أو Visitor Management
DB	قاعدة بيانات ACS الرئيسية
MA	الواجهة الخلفية لتطبيق Mobile Access
S	تطبيق مثبت "Setup Access" لمثبتي ومكوني النظام
M	تطبيق Mobile Access للأجهزة المحمولة لأصحاب بيانات الاعتماد العادية.

طبولوجيات Credential Management، قاعدة البيانات المحلية	طبولوجيات Credential Management، قاعدة البيانات البعيدة
	

الجدول 4.1: طبولوجيات Credential Management

Mobile Access، في نفس الموقع، قاعدة بيانات محلية	Mobile Access، في نفس الموقع، قاعدة بيانات بعيدة
	

الجدول 4.2: طبولوجيات Mobile Access في نفس الموقع

Mobile Access، موزع، قاعدة بيانات محلية	Mobile Access، موزع، قاعدة بيانات بعيدة
	

الجدول 4.3: طبولوجيات Mobile Access الموزعة

الإصدارات المتوافقة من البرامج ذات الصلة

يسرد الجدول التالي إصدارات الأدوات البرمجية المساعدة المتوافقة مع هذا الإصدار من النظام.

المكون	الإصدار	الموقع
Access Management System (AMS)	5.5 (يتضمن ملحق Mobile Access)	متجر التنزيل /كتالوج المنتجات
Visitor Management (VisMgmt)	5.5 (يتضمن ملحق Mobile Access)	متجر التنزيل /كتالوج المنتجات

إشعار!

الأقسام

لا يدعم كل من Credential Management وVisitor Management وMobile Access ميزة "الأقسام" في أنظمة التحكم في الوصول من Bosch، حيث يتحكم شخص واحد (ACS) في وصول عدة مستأجرين مستقلين.

5 التكوين

5.1 إنشاء مستخدمي Credential Management في ACS

في ACS (ACE أو AMS)، يجب أن يكون كل مستخدم Credential Management حامل بطاقة مع تعريف مشغّل منفصل.

وتحتوي تعريفات المُشغّل هذه على حقوق CredMgmt خاصة تأتي في شكل **ملفات تعريف المستخدم**. يجب عليك تعريف مشغّل منفصل لكل حامل بطاقة يعمل في CredMgmt. لا يُمكنك تعيين حاملي بطاقات متعددين للمشغّل ذاته.
راجع المساعدة عبر الإنترنت في ACS للحصول على معلومات مفصلة وإرشادات بخصوص **ملفات تعريف المستخدم**.
يجب إنشاء مستخدمي Credential Management في AMS:

مسار مربع الحوار
التكوين > **المشغّلون ومحطات العمل** > **ملفات تعريف المستخدمين**

الإجراء

1. انقر فوق  لإنشاء ملف تعريف جديد
2. أدخل اسمًا لملف التعريف في الحقل **اسم ملف التعريف** (إلزامي)
3. أدخل وصفًا لملف التعريف في حقل **الوصف** (اختياري ولكن مستحسن)
4. انقر فوق  أو **تطبيق** لحفظ تغييراتك
5. اختر الوظيفة وفقًا لنوع ملف التعريف:
   - في جزء القائمة، حدد الوظائف (العمود الأول) والقدرات ضمن تلك الوظيفة (**التنفيذ** و**التغيير** و**الإضافة** و**الحذف**) التي يمكن لملف التعريف هذا الوصول إليها. انقر نقرًا مزدوجًا فوقها لتبديل إعداداتها إلى `Yes`.
   - تأكد أيضًا من أن الوظائف التي يجب ألا يكون الوصول إليها ممكنًا معيّنة إلى `No`.
6. انقر فوق  أو **تطبيق** لحفظ تغييراتك

لمزيد من المعلومات حول أدوار المستخدم في Credential Management، راجع نظرة عامة على أدوار المستخدم.

5.2 تسجيل الدخول لمهام التكوين

بالنسبة إلى مهام التكوين والإدارة، استخدم جهاز كمبيوتر محمي ماديًا من الوصول غير المصرح به.

1. من مستعرضك، قم بإدخال عنوان HTTPS لخادم CredMgmt ويليه نقطتان ورقم المنفذ (الافتراضي `5806`)
   `https://<My_CredMgmt_server>:5806`
   تظهر شاشة **تسجيل الدخول**
2. قم بتسجيل الدخول كمستخدم CredMgmt **مسؤول**.
3. انقر فوق  لفتح قائمة **الإعدادات**.

5.3 استخدام قائمة الإعدادات في التكوين

عام	– **فترة الاحتفاظ (بالأيام)**: يحكم هذا الإعداد طريقة التعامل مع سجلات الأشخاص. – عندما تنقضي الفترة لأول مرة، يقوم التطبيق بتحويل السجل إلى سجل مجهول الهوية.

	– عندما تنقضي الفترة لثاني مرة، يقوم التطبيق بحذف السجل. القيمة الافتراضية هي 365. قم بتعيين 0 لإلغاء تنشيط فترة الاحتفاظ بالكامل. في هذه الحالة، يتم الاحتفاظ بالسجلات إلى ما لا نهاية. – **الشعار**: حدد أو قم بإلغاء تحديد خانة الاختيار التي تتحكم فيما إذا كانت مربعات الحوار تعرض شعارًا مخصصًا أو الشعار الافتراضي. – لمعايير ملفات الشعار المخصصة، انظر: تخصيص شعار الشركة, الصفحة *26* – **Supergraphic:** حدد أو قم بإلغاء تحديد خانة الاختيار التي تتحكم فيما إذا كانت مربعات الحوار تعرض Supergraphic من Bosch. – **اللغات**: حدد اللغات التي ستتوفر في واجهة المستخدم إلى جانب تنسيقات **التاريخ** و**الوقت** المفضلة لديها. – **خادم البريد** أدخل عنوان IP ورقم المنفذ وتفاصيل حساب خادم البريد الإلكتروني الذي تستخدمه، من أجل تمكين إرسال رسائل البريد الإلكتروني من التطبيق. إذا احتاج خادم البريد الخارجي إلى شهادة SSL/TSL إضافية، فاستوردها إلى الجهاز الذي يقوم بتشغيل الواجهة الخلفية لتطبيق Mobile Access. بعد عملية الاستيراد، يجب إعادة تشغيل VisitorManagerServer. – **قوالب البريد الإلكتروني** يتم توفير عدد كبير من قوالب البريد الإلكتروني بتنسيق HTML، والتي تقوم عادةً بتخصيصها وفقًا لمتطلباتك الخاصة. للحصول على المزيد من التفاصيل، راجع القسم المنفصل **قوالب البريد الإلكتروني** أدناه. – **Mobile Access** حدد خانة الاختيار **Mobile Access** لتنشيط Mobile Access. **الاتصال**: أدخل عنوان خادم Mobile Access (عنوان خدمة التسجيل). https://<MyMobileAccessBackendServer>:5700 استخدم (FQDN) لـ <MyMobileAccessBackendServer> في بيئات متعددة المجالات. **ملاحظة:** لاستخدام عنوان IP بدلاً من FQDN، عليك إدخال عنوان IP ضمن **إنشاء الشهادة**، عندما تقوم بتشغيل معالج إعداد الواجهة الخلفية لـ Mobile Access. **إعداد المثبت:** حدد المعلومات التي تحتاج إليها من المثبتين، لتمكينهم من تكوين أجهزة قراءة الوصول عبر المحمول باستخدام Bosch Setup Access. سجل خروجك من تطبيق الويب، وسجل دخولك من جديد من أجل استخدام ميزة Mobile Access على الفور.

5.3.1 قوالب البريد الإلكتروني

يتم توفير عدد كبير من قوالب البريد الإلكتروني بتنسيق HTML، والتي تقوم عادةً بتخصيصها وفقًا لمتطلبات شركتك الخاصة. لكل قالب، يمكنك تخزين عناوين البريد لكل من النسخة (CC) والنسخة المخفية (BCC) ومستلم الاختبار، والذي يمكنك إرسال بريد إلكتروني تجريبي إليه على الفور.

بعد تنزيل القوالب من قائمة **الإعدادات**، يتم تخزينها في مجلد التنزيلات الافتراضي في المستعرض.

– MobileAccess.html دعوة لحامل بطاقة لاستخدام بيانات الاعتماد المستندة إلى الهاتف الذكي.
– SetupAccess.html دعوة لأحد المثبتين لتكوين أجهزة القراءة من أجل Mobile Access.

عناصر نائبة لاستخدامها في قوالب البريد الإلكتروني
توفر قوالب البريد الإلكتروني عددًا كبيرًا من العناصر النائبة للنص لتضمين حقول قاعدة البيانات في النص. يتم وصف هذه العناصر النائبة في الجداول التالية، وفقًا للقوالب التي يمكن استخدامها فيها.

Mobile Access
بريد إلكتروني مُرسل إلى حامل البطاقة (لتطبيق Mobile Access) عندما يتم منحه إمكانية الوصول عبر المحمول

العنصر النائب	الوصف
{{Title}}	لقب الشخص (السيد أو السيدة وغيرهما).
{{FirstName}}	الاسم الأول للشخص
{{LastName}}	لقب الشخص
{{CompanyName}}	شركة الشخص
{{QrcodeLink}}	رمز الاستجابة السريعة المناظر للرابط الذي يتيح لحامل البطاقة الوصول عبر المحمول من خلال التطبيق
{{InviteLink}}	الارتباط الذي يتيح لحامل البطاقة الوصول عبر المحمول من خلال التطبيق

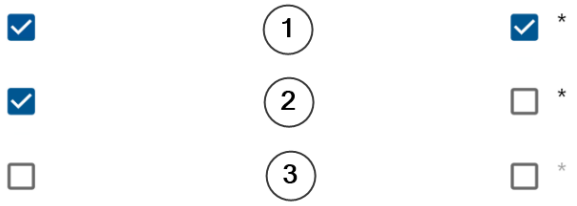
Setup Access
بريد إلكتروني مُرسل إلى مثبت Mobile Access (لتطبيق Setup Access) عندما يتم منحه حق الوصول عبر المحمول لإعداد أجهزة القراءة.

العنصر النائب	الوصف
{{Title}}	لقب المثبت (السيد أو السيدة أو الطبيب أو غيرها)
{{FirstName}}	الاسم الأول للمثبت
{{LastName}}	لقب المثبت
{{CompanyName}}	شركة المثبت
{{QrcodeLink}}	رمز الاستجابة السريعة المناظر للرابط الذي يوفر للمثبت الوصول عبر المحمول لإعداد أجهزة القراءة عبر تطبيق Setup Access
{{InviteLink}}	رابط يوفر الوصول عبر المحمول للمثبت لإعداد أجهزة القراءة عبر تطبيق Setup Access

5.3.2 قوالب المستندات
بالنسبة إلى المستندات ورسائل البريد الإلكتروني المختلفة، يمكنك تنزيل القوالب وتحميل إصدارات مخصصة من تلك القوالب، في مربع الحوار **لوحة المعلومات** > **الإعدادات** > **عام**.

5.4 تخصيص واجهة المستخدم
خصص واجهة المستخدم في مربعات حوار لوحة المعلومات > **الإعدادات**.

5.4.1 تكوين الخيارات التي ستكون ظاهرة وغير ظاهرة وإلزامية
حدد حقول البيانات التي ستكون ظاهرة في مربعات الحوار والبيانات التي تعتبر إلزامية.
مثال:



- (1) ظاهر وإلزامي،
- (2) ظاهر لكنه ليس إلزاميًا
- (3) غير ظاهر.

5.4.2 تخصيص نصوص واجهة المستخدم للتطويع اللغوي

يمكنك بسهولة تخصيص نصوص واجهة المستخدم على أساس كل لغة.

في الوضع الافتراضي، يحتوي **نص التطويع اللغوي** على العناوين القياسية لكتل حقول البيانات في مربعات حوار جمع البيانات.

لتخصيص هذه العناوين حسب المتطلبات المحلية:

1. حدد لغة واجهة مستخدم من القائمة.
2. اكتب فوق النصوص في مربع النص.

يمكنك استخدام علامات HTML للتنسيق البسيط مثل:

```
b>this text will appear bold </b>>
<i>italics</i>
<<u>underline</u
```

5.4.3 تخصيص شعار الشركة

يجب أن تستوفي الملفات الرسومية التي تقوم بتحميلها لشعار شركتك المعايير التالية:

التنسيقات المدعومة	PNG, JPEG, JPG
العرض الدقيق (بالبكسل)	125
الارتفاع الدقيق (بالبكسل)	63
الحد الأقصى للحجم (ميغابايت)	1

5.5 إعدادات جدار الحماية

أضف التطبيقات المساعدة إلى تكوين جدار الحماية لأجهزة الكمبيوتر العميل والخادم:

1. ابدأ تشغيل جدار الحماية في Windows. انقر فوق بدء > **لوحة التحكم** > **Windows-Firewall**
2. حدد **الإعدادات المتقدمة**
3. حدد **القواعد الداخلية**
4. في جزء **الإجراءات**، حدد **قاعدة جديدة...**
5. في مربع حوار **نوع القاعدة**، حدد **المنفذ** وانقر فوق **التالي >**
6. في الصفحة التالية، حدد **TCP ومنافذ محلية محددة**
7. اسمح بالاتصال عبر المنافذ التالية:

- على كمبيوتر الخادم أو أجهزة الكمبيوتر

<server name>:44333 - مستخدم بواسطة خادم هوية AMS **(*)**

<server name>:5706 - مستخدم بواسطة خادم VisMgmt

<server name>:5806 - مستخدم بواسطة خادم CredMgmt
<server name>:5701 - مستخدم بواسطة الواجهة الخلفية لتطبيق Mobile Access
– على أجهزة الكمبيوتر العميل
localhost:5707 - مستخدم بواسطة الوظيفة الإضافية Bosch Peripheral Devices

(*) نحن نستخدم خوادم هوية AMS وBIS كما هو موضح في أدلة التثبيت الخاصة بكل منهما.

استخدام المنفذ داخل النظام

الخادم الصادر	المنفذ للخارج	الخادم الوارد	المنفذ للداخل	البروتوكول	التعليقات
VisMgmt أو أو CredMgmt	*	الواجهة الخلفية لتطبيق Mobile Access	5701	HTTPS	أوامر من تطبيق الويب لإنشاء بيانات اعتماد الهاتف المحمول و/ أو حذفها
الأجهزة المحمولة من الإنترنت	*	الواجهة الخلفية لتطبيق Mobile Access	5701	HTTPS	تتلقى الأجهزة المحمولة بيانات اعتماد الهاتف المحمول عبر الإنترنت
الواجهة الخلفية لتطبيق Mobile Access	*	Google Firebase (الإنترنت)	*	HTTPS	تتلقى الأجهزة المحمولة إعلامات منبثقة، يرجى الرجوع إلى وثائق Google Firebase حول إعدادات جدار الحماية https://firebase.google.com/docs/cloud-messaging/concept-options
الكمبيوتر العميل لمستخدم VisMgmt	*	الواجهة الخلفية لتطبيق VisMgmt	5706	HTTPS	أوامر من الكمبيوتر العميل VisMgmt إلى الواجهة الخلفية لتطبيق VisMgmt
كمبيوتر عميل للمستخدم CredMgmt	*	الواجهة الخلفية لتطبيق CredMgmt	5806	HTTPS	أوامر من الكمبيوتر العميل CreMgmt إلى الواجهة الخلفية لتطبيق CredMgmt
كمبيوتر المسؤول	*	الواجهة الخلفية لتطبيق Mobile Access	3389	كمبيوتر سطح المكتب البعيد (RDP)	لأسباب أمنية، يجب السماح بوصول المسؤول إلى كمبيوتر الواجهة الخلفية لتطبيق Mobile Access بشكل مؤقت فقط.

إشعار!
لاحظ أن تطبيق Mobile Access وACS ليس لهما اتصال مباشر، لا واردًا ولا صادرًا.

5.5.1 البرامج والخدمات كاستثناءات جدار الحماية

يمكنك أيضًا تكوين جدار الحماية عن طريق إضافة البرامج والخدمات كاستثناءات

1. ابدأ واجهة مستخدم جدار حماية Windows، وحدد **البدء > الإعدادات > لوحة التحكم > جدار حماية Windows**.
2. حدد علامة التبويب **السماح لتطبيق أو ميزة من خلال جدار حماية Windows.**
3. حدد **السماح لتطبيق آخر** (إذا كان باللون الرمادي، قم بتمكين الزر عن طريق تحديد **تغيير الإعدادات**).
4. يمكنك إضافة البرامج التالية:

البرامج

مسار التثبيت الافتراضي هو `C:\Program Files (x86)\Bosch Sicherheitssysteme\`

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

الخدمات

مسار التثبيت الافتراضي هو :C

\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System

الخدمة	مكان الملف
Bosch.States.Api	States API\[install-path]
Bosch.Map.Api	Map API\[install-path]
Bosch.MapView.Api	Map View API\[install-path]
Bosch.Events.Api	Events API\[install-path]
Bosch.Alarms.Api	Alarms API\[install-path]
Bosch.Ace.IdentityServer	Identity Server\[install-path]
Bosch.Ace.Api	Access API\[install-path]
Bosch.DialogManager.Api	Dialog Manager API\[install-path]
Bosch.Intrusion.Api	Intrusion API\[install-path]
Bosch Ace Visitor Management	\[VM-install-path]
عميل Bosch Ace Visitor Management	\[VM-client-install-path]
Bosch.OSS-SO	OSS-SO\[install-path]
Bosch.OSS-SO.Configurator	OSS-SO.Configurator\[install-path]
Bosch.Access.ProductApi.Api	ProductApi\[install-path]
Bosch.MUM	\[MUM-install-path]

5.5.2 واجهة برمجة التطبيقات (API) لتطبيق Mobile Access

اعتبارًا من الإصدار 5.2 من Mobile Access والإصدارات الأحدث والإصدار 5.2 من Credential Management والإصدارات الأحدث والإصدار 5.2 من Visitor Management والإصدارات الأحدث، تم تقسيم الواجهة الخلفية لتطبيق Mobile Access إلى جزء قناة أمامية وجزء قناة خلفية. يجب أن تتواصل القناة الأمامية مع الهواتف المحمولة بينما تتواصل القناة الخلفية مع Credential Management و/أو Visitor Management.

يسمح هذا الأمر بتعيين مسارات وقواعد جدار الحماية من أجل تنظيم نقل البيانات عبر الشبكة لتعزيز أمن تكنولوجيا المعلومات. يتكون تقسيم واجهة برمجة التطبيقات (API) من رقمين منفصلين للمنفذ. رقم منفذ الهواتف المحمولة هو 5700، بينما يستخدم كل من Credential Management وVisitor Management المنفذ 5701.

يتضمن كل من Credential Management وVisitor Management إعدادين منفصلين لعنوان URL للقناة الأمامية وعنوان URL للقناة الخلفية على التوالي. تطلق عليهم واجهة المستخدم اسم "عنوان الخدمة الإدارية" (القناة الخلفية) و"عنوان خدمة التسجيل" (القناة الأمامية).

المنفذ الافتراضي لـ "عنوان الخدمة الإدارية" (القناة الخلفية) هو 5701. في قاعدة جدار حماية خاصة بالعميل، يجب تكوين هذا المنفذ فقط للاتصال بالجهاز الذي يقوم بتشغيل الواجهة الخلفية لتطبيق Credential Management و/أو الواجهة الخلفية لتطبيق Visitor Management، وهو خادم AMS في معظم الحالات.

المنفذ الافتراضي لـ "عنوان خدمة التسجيل" (القناة الأمامية) هو 5700. في قاعدة جدار حماية خاصة بالعميل، يجب تكوين هذا المنفذ بحيث يمكن الوصول إليه من تطبيقات Mobile Access. في سيناريوهات كثيرة، يمكن الوصول إلى نقطة النهاية هذه من الخارج. ولكن هذا الأمر يتوقف على سيناريو العميل إلى حدٍ بعيدٍ.

إذا كان العميل يجري التحديث من إصدار سابق إلى الإصدار الأحدث من AMS، فيجب تعديل إعدادات Credential Management وVisitor Management. يمكن لدور المسؤول في Visitor Management وCredential Management الوصول إلى هذا الإعداد في صفحة الإعدادات.
يجب أن تكون القناة الخلفية محمية بحيث لا يمكن الوصول إليها من شبكة الإنترنت العامة أو أي شبكة غير مصرح بها.

5.6 أمان تكنولوجيا المعلومات

يمثل أمن نظام التحكم في الوصول لمؤسسة جزءًا حرجًا من بنيتها التحتية. تنصح Bosch بالالتزام الصارم بإرشادات أمان تقنية المعلومات المذكورة لبلد التثبيت.
المؤسسة التي تدير نظام التحكم بالوصول مسؤولة عما يلي على الأقل:

5.6.1 مسؤوليات الأجهزة

- منع الوصول الفعلي غير المصرح به إلى مكونات الشبكة مثل وصلات RJ45.
  - يحتاج المهاجمون إلى وصول فعلي لتنفيذ هجمات "الدخيل".
- منع الوصول المادي غير المصرح به إلى أجهزة تحكم AMC2.
- استخدام شبكة مخصصة للتحكم في الوصول.
  - يستطيع المهاجمون الحصول على إمكانية الوصول عبر أجهزة أخرى داخل الشبكة نفسها.
- استخدام بيانات اعتماد آمنة مثل **DESFire** مع رمز Bosch والمصادقة متعددة العوامل مع القياسات الحيوية.
- التسجيل الفوري، عبر تطبيق **Setup Access**، لأجهزة القراءة الوصول إلى الأجهزة المحمولة مع وحدات BLE (Bluetooth Low Energy). أجهزة القراءة قيد التشغيل وغير المسجلة عرضة للاختراق من قبل جهات خارجية. لمعالجة هذا الاختراق، راجع دليل التثبيت الخاص بالقارئ للحصول على إرشادات حول كيفية إعادة تعيين إعدادات المصنع الافتراضية.
- تقديم آلية للتعامل مع الأعطال وتوفير مصدر طاقة احتياطي لنظام التحكم في الوصول.
- تعقب وتعطيل بيانات الاعتماد التي تم الادعاء بأنها فُقدت أو تم وضعها في غير مكانها.
- الإخراج الملائم من الخدمة للأجهزة التي لم تعد قيد الاستخدام، وخاصة إعادة ضبطها على القيم الافتراضية للمصنع وحذف البيانات الشخصية ومعلومات الأمان.

5.6.2 مسؤوليات البرامج

- صيانة جدار حماية شبكة التحكم في الوصول وتحديثه وتشغيله بشكل ملائم.
- مراقبة الإنذارات التي تشير إلى وقت توقف تشغيل مكونات الأجهزة مثل قارئات البطاقات أو وحدات تحكم AMC2.
  - قد تشير هذه الإنذارات إلى محاولة لتبديل مكونات الأجهزة.
- مراقبة إنذارات اكتشاف التلاعب التي تبدأ التشغيل بواسطة ملامسات كهربائية في أجهزة التحكم في الوصول، مثل أجهزة التحكم والقارئات والخزائن.
- الحد من عمليات بث UDP داخل الشبكة المخصصة.
- التحديثات، وخاصة التحديثات والإصلاحات الأمنية، لبرنامج التحكم في الوصول.
- التحديثات، وخاصة التحديثات والإصلاحات الأمنية، لبرنامج مصنع الأجهزة.
  - لاحظ أنه حتى الأجهزة التي تم تسليمها مؤخرًا قد تتطلب تحديثًا لبرنامج المصنع. راجع دليل الأجهزة للحصول على الإرشادات.
  - لا تتحمل Bosch المسؤولية عن الأضرار الناتجة عن المنتجات الجاري تشغيلها باستخدام برمجيات مصنع متقادمة.
- استخدام اتصال OSDPv2 عبر قناة آمنة.
- استخدام عبارات كلمات مرور قوية.
- فرض تطبيق مبدأ الامتياز الأقل لضمان تمكن المستخدمين الأفراد من الوصول فقط إلى الموارد التي يحتاجون إليها من أجل غرضهم المشروع.
- التعيين والتكوين المناسبين لملفات تعريف المستخدمين للمشغلين لمنع المشغلين العاديين من تعيين تصريحات ذات مستوى أمان عالٍ من دون مبدأ الشخصين.

5.6.3 التعامل الآمن مع بيانات اعتماد المحمول

- لا تترك أجهزة قراءة Mobile-Access التي لم يتم تكوينها بدون حماية.
  - بإمكان المهاجم اختراق القارئ لأنظمة ACS مختلفة. قد يتطلب هذا الأمر تنفيذ إعادة ضبط على إعدادات المصنع باهظة التكاليف.
- في حالة فقدان أو سرقة جهاز محمول يحمل بيانات اعتماد المحمول، تعامل مع هذا الجهاز كبطاقة مفقودة: احظر جميع بيانات اعتماد المحمول الخاصة به أو احذفها في أسرع وقت ممكن.
- توصي Bosch بإجراء مصادقة ثنائية للبيئات عالية الأمان. يتطلب هذا من حامل بيانات الاعتماد إلغاء قفل الجهاز المحمول قبل استخدامه كبيانات اعتماد.
- لا تتم استعادة بيانات اعتماد المحمول عند استعادة الهاتف من نسخة احتياطية. يجب عليك إعادة إرسال جميع الدعوات الحالية إذا تلقى حامل بيانات اعتماد المحمول جهازًا محمولًا جديدًا.
- لمنع الاتصال بأجهزة قراءة الوصول إلى الأجهزة المحمولة، يمكن للمهاجم استخدام جهاز تشويش على الاتصالات. يجب أن يحمل الموظفون الذين يكون وصولهم إلى المناطق أمرًا ضروريًا بيانات اعتماد مادية كنسخة احتياطية.
- كنسخة احتياطية من Mobile Access، استخدم فقط البطاقات المادية ذات التشفير الآمن (مثل كود Bosch).
- قم بحماية خادم Mobile Access من الوصول الفعلي غير المصرح به. توصي Bosch بإجراءات إضافية مثل، على سبيل المثال، إجراء تشفير لقرص BitLocker.
- قم بحماية خادم Mobile Access من هجمات رفض الخدمة (DoS). يجب أن يكون جزءًا من بيئة شبكة آمنة توفر الحماية مثل المحدد المعدل.
- تعامل مع رموز الاستجابة السريعة الخاصة بدعوة المثبت على أنها بيانات اعتماد المسؤول. قد يُمكِّن هاتف المثبِّت المسروق، مع بيانات اعتماد المثبِّت النشطة، المهاجم من إعادة تكوين أجهزة قراءة Mobile-Access بشكل ضار.
  - أرسل دعوات إلى المثبتين في الوقت المناسب تمامًا لإعداد القارئ، وتأكد من حذف بيانات الاعتماد هذه بمجرد اكتمال الإعداد.
  - استخدم وظيفة "مسح رموز الاستجابة السريعة من الشاشة" بدلاً من الدعوات المرسلة عبر البريد الإلكتروني. تأكد من أن المثبت المقصود يقوم بتحميل بيانات الاعتماد على الفور.

5.7 خصوصية البيانات وحمايتها في Bosch

المقدمة

في جميع العمليات التجارية وبطريقة متوافقة مع المتطلبات القانونية المعمول بها، نحن نضمن حماية الخصوصية وحماية البيانات الشخصية والحفاظ على أمان معلومات العمل. من الناحية التقنية والتنظيمية، وخاصة فيما يتعلق بالحماية من الوصول غير المصرح به والخسارة، نحن نطبق معيارًا مناسبًا يعكس أحدث الابتكارات في المجال ويأخذ في الاعتبار المخاطر المرتبطة بها. عند تطوير منتجات Bosch ونماذج الأعمال الجديدة، نحن نتأكد من مراعاة المتطلبات القانونية التي تحكم حماية البيانات وأمن المعلومات في مرحلة مبكرة.

بالإضافة إلى منظمة الامتثال وقسم الشؤون القانونية، فإن جهة الاتصال الأساسية للأسئلة المتعلقة بكيفية التعامل مع البيانات بشكل صحيح هي مسؤول أمن البيانات.

معالجة البيانات الشخصية في تطبيق Mobile Access وفي نظام الواجهة الخلفية لتطبيق Mobile Access

- فئات البيانات الشخصية
  - تحتوي تطبيقات Mobile Access على البيانات الشخصية. هذه هي معلومات رقم البطاقة التي يتم استخدامها للوصول إلى أجهزة القراءة. لا يمكن الوصول إلى البيانات الفعلية للأشخاص الحقيقيين إلا من خلال الاستخدام الإضافي لبرامج AMS أو ACE أو Visitor Management.
  - لا يحتاج إجراء تسجيل المثبت في قائمة **الإعدادات** إلى تخزين البيانات الشخصية. ومع ذلك، قد يتم تخزين بعض معلومات المستخدم، مثل عناوين البريد الإلكتروني، بشكل اختياري.
  - يقوم خادم الواجهة الخلفية لتطبيق Mobile Access بتخزين البيانات الشخصية لإدارة بيانات الاعتماد.
- نقل البيانات

- يتم نقل معلومات بيانات الاعتماد بين نظام الواجهة الخلفية وتطبيق Mobile Access ونظام Visitor Management للتحكم في الوصول إلى أجهزة القراءة.
- تسجيل البيانات
- يحتفظ تطبيق Mobile Access بالسجلات التقنية. ويتم تخزين هذه السجلات محليًا على الجهاز المحمول ويمكن إرسالها إلى جهات خارجية، مثل الدعم التقني، إذا لزم الأمر.
- يحتفظ خادم الواجهة الخلفية أيضًا بالسجلات التقنية. ويتم تخزين البيانات محليًا على نظام الخادم.
- بشكل افتراضي، لا يحذف خادم الواجهة الخلفية ملفات السجلات تلقائيًا. ومع ذلك، يمكن تكوين الحذف التلقائي بالاستناد إلى سعة التخزين المتبقية أو وفقًا لجدول زمني.

ما الذي قمنا به لجعل حماية بيانات المنتج سهلة التطبيق؟

تدير أنظمة التحكم في الوصول من Bosch حقوق الوصول للأشخاص. ولحماية هؤلاء الأشخاص، تتخذ Bosch الإجراءات المناسبة لدمج متطلبات GDPR مباشرة في تطوير المنتج، باتباع نهج "الخصوصية حسب التصميم".

- يتم استخدام التشفير المتطور.
- معلومات بيانات الاعتماد مجهولة الهوية.
- لا يحتاج مستخدم التطبيق إلى إدخال معلومات شخصية لتلقي بيانات الاعتماد الافتراضية عبر رمز الاستجابة السريعة أو البريد.
- يمكن حذف معلومات بيانات الاعتماد من تطبيقات Mobile Access، ومن أنظمة التحكم في الوصول الأساسية، ومن التطبيقات المساعدة مثل Visitor Management وCredential Management.
- يمكن حظر بيانات الاعتماد من قبل مشغلي أنظمة التحكم في الوصول الأساسية والتطبيقات المساعدة في أي وقت.
- بيانات قياس تتبع الاستخدام مجهولة الهوية بحسب التصميم.
- لا يتم نقل ملفات السجلات من الأجهزة المحمولة إلى أطراف أخرى، مثل الدعم التقني، من دون موافقة المستخدم وتعاونه النشط.
- يمكن تكوين الحذف التلقائي المجدول لملفات السجلات في نظام التحكم في الوصول الأساسي.
- لا تطلب Bosch أي تسجيل في متجر التطبيقات أو التطبيق. لا يقوم متجر التطبيقات بإعادة توجيه أي بيانات شخصية إلى Bosch.
- يحتاج التطبيق إلى تقنية Bluetooth لكي يعمل، ولكنه يطلب من المستخدم تنشيط تقنية Bluetooth يدويًا.

أسئلة إضافية

للحصول على المزيد من المعلومات فيما يتعلق بخصوصية البيانات، راجع إشعار خصوصية البيانات في تطبيق Mobile Access، أو اتصل بفريق مشروع Bosch.

5.8 تصريحات أمنية عالية المستوى

5.8.1 مبدأ الشخصين

بدءًا من AMS 5.5 والإصدارات الأحدث، من الممكن تمكين مبدأ الشخصين. الهدف الرئيسي من هذه الوظيفة هو فرض الأمان عند تعيين التصريحات عن طريق إضافة موافق. في Credential Management، بإمكان المشغّل تعيين تصريح واحد أو أكثر لشخص معين. وعلى النقيض من تعيين تصريح نموذجي، الذي يتم تعيينه إلى الشخص على الفور، يتم إرسال التصريحات مع تمكين مبدأ الشخصين كطلب إلى مشغّل آخر لديه حق الموافقة على طلب التصريح أو رفضه. من شأن ذلك أن يمنع التصريحات غير المشروعة حيث يمكن استخدامه لحماية التصريحات الخاصة بالمناطق الحساسة، أي التصريحات التي يمكن تعيينها إلى موظف فقط في حالة موافقة اثنين من المشغّلين (الطالب والموافق).

5.8.2 تكوين تصريحات أمنية عالية المستوى

من أجل تمكين مبدأ الشخصين، المتطلبات التالية إلزامية:

- نظام AMS محدث بالإصدار الأخير.

– يجب أن تكون مسؤول AMS.

إنشاء تصريحات الوصول مع مبدأ الشخصين

في نظام التحكم في الوصول الرئيسي:

مسار مربع الحوار

قائمة AMS الرئيسية > **بيانات النظام** > **التصريحات**

1. امسح حقول الإدخال عن طريق النقر فوق الزر **جديد**  في شريط الأدوات.

   أو، انقر فوق **نسخ**  لإنشاء تصريح جديد استنادًا إلى تصريح موجود.
2. أدخل اسمًا فريدًا للتصريح
3. (اختياري) أدخل وصفًا
4. (اختياري) حدد نموذج الوقت لضبط هذا التصريح
5. (اختياري) اختر **حد عدم النشاط** من القائمة.
6. (إلزامي) عيّن **مدخلاً** واحدًا على الأقل.
7. حدد خانة الاختيار **الموافقة مطلوبة** (هذا الخيار يمكّن مبدأ الشخصين).
8. انقر فوق "حفظ"  لحفظ التخويل.

إشعار!

توصية أمنية

تنطبق هذه الميزة فقط على Credential Management. في AMS، يجب على المسؤولين تعيين وتكوين ملفات تعريف المستخدمين للمشغلين بشكل صحيح كي لا يكون الوصول ممكنًا إلى مربعات الحوار.

سيؤدي هذا إلى منع المشغلين العاديين من تعيين تصريحات ذات مستوى أمان عالٍ من دون مبدأ الشخصين.

لمزيد من المعلومات، راجع أحدث إصدار من دليل تكوين وتشغيل برنامج *Access Management System*.

6 التشغيل

6.1 نظرة عامة على أدوار المستخدمين

تتحدد إمكانيات مستخدمي Credential Management من خلال ملفات تعريف المستخدمين الخاصة بهم في ACS:

نوع المستخدم	حالات الاستخدام
المسؤول	إنشاء إعدادات عامة تخصيص سلوك الأداة وواجهة المستخدم بها بالإضافة إلى جميع حالات استخدام المشغّلين
المشغّل	تعيين وإلغاء تعيين بطاقات الوصول المادية وبيانات الاعتماد الافتراضية للوصول عبر المحمول
مبدأ الشخصين: الطالب	طلب تصريحات ذات مستوى أمان عالٍ
مبدأ الشخصين: الموافق	الموافقة على التصريحات ذات مستوى أمان عالٍ أو رفضها إزالة التصريحات العادية

راجع

- إنشاء مستخدمي *Credential Management* في *ACS*, الصفحة *23*

6.2 استخدام لوحة المعلومات

لوحة المعلومات هي الشاشة الرئيسية - مربع حوار مركزي يؤدي إلى كل مربعات الحوار الأخرى.

الاستخدام العام لجدول الموظفين

يمثل كل صف في الجدول شخصًا. هؤلاء هم موظفون داخليون أو خارجيون يحتاجون إلى بيانات اعتماد للوصول إلى المقر.

- يمكنك تحديد أشخاص فرديين أو عدة أشخاص مرة واحدة، باستخدام تعابير لوحة المفاتيح والماوس:
  - الضغط على مفتاح Ctrl مع النقر للتحديد المتعدد لأسطر فردية.
  - الضغط على مفتاح Shift مع النقر على سطر محدد بالفعل لإزالته من التحديد.
  - الضغط على مفتاح Shift مع النقر للتحديد المتعدد لأسطر متجاورة
- يمكنك إضافة أشخاص جدد إلى الجدول
- يمكنك تعيين وإلغاء تعيين بيانات الاعتماد بالنقر فوق أزرار الإجراءات
  - تعيين بيانات اعتماد مادية
  - تعيين بيانات اعتماد افتراضية (للوصول عبر المحمول)
  - تحرير تفاصيل الشخص
- يمكنك تصدير كافة البيانات إلى ملف CSV. أو XLSX. إذا كنت تحتاج إلى بيانات معينة فقط، فاستخدم وظيفة التصفية. لا يمكن تصدير البيانات المطلوبة عن طريق تحديدها. يمكن تصدير فقط الخطوط التي تمت تصفيتها حاليًا إلى ملف CSV. أو XLSX.

وظائف لوحة المعلومات

التسمية	الوظيفة
(1) **N من الإدخالات**	العدد الإجمالي N من الأشخاص (كل شخص هو صف في الجدول).
(2) **بحث**	البحث عن نص عشوائي ضمن الأشخاص في الجدول
 (3)	تحديد جميع العناصر الموجودة في القائمة
 (4) **حذف**	حذف العناصر المحددة
 (5) **الأحدث**	إظهار الأشخاص الذين تمت إضافتهم مؤخرًا إلى الجدول.
 (6) **إعادة تعيين**	إعادة تعيين الجدول إلى طريقة عرضه الافتراضية واسترجاع كل عوامل التصفية.
 (7) **إلغاء تعيين البطاقة**	فتح مربع حوار لإلغاء تعيين بطاقات تم تعيينها باستخدام قارئ تسجيل متصل.
(8) ...	انقر فوق رمز علامة القطع لقائمة لتصدير الأشخاص والمستندات، إلى تنسيقات ملفات مختلفة، على سبيل المثال، CSV و .XLSX. لأسباب تتعلق بأمان البيانات، لا يمكنك التصدير إلا إذا كان عميلك يعمل في اتصال HTTPS آمن، مع شهادة.
 (9)	فتح مربع حوار لإنشاء مستخدم جديد

أعمدة لوحة المعلومات

العمود	الوصف
الاسم	انقر فوق الارتباط التشعبي لعرض تفاصيل الشخص.
البريد الإلكتروني	
القسم	
الموضع	
الشركة	

العمود	الوصف
أرقام البطاقات	أرقام البطاقات المعينة لهذا الشخص.
الإجراءات	انظر الجدول المنفصل أدناه

الإجراءات التي يجب تنفيذها على سجلات الموظفين في جدول لوحة المعلومات

الأيقونة	الإجراءات
	**تعيين** بطاقة مادية واحدة أو أكثر إلى الشخص
	**تعيين** بيانات اعتماد افتراضية للشخص للوصول عبر المحمول
	**تحرير** التفاصيل الشخصية للشخص. يتم نشر التغييرات في ACS. يتم نشر التغييرات التي يتم إدخالها في ACS في تطبيق CredMgmt.

6.2.1 نظرة عامة على صفحة الشخص

بعد النقر فوق اسم شخص معين، بفتح مربع حوار يتضمن بيانات شخصية. يتضمن مربع الحوار هذا حقولاً يمكن فيها عرض المعلومات الرئيسية للشخص وتحريرها، ولكن المعلومات الشخصية الأساسية تُعرض بشكل دائم على الجانب الأيسر من مربع الحوار.

تظهر المعلومات حول إدخالات القائمة السوداء - إن وجدت - في أسفل عمود المعلومات الشخصية الأساسية هذا.

تلميح: يسمح حقل **العنوان** بالنص الحر إلى جانب الاختيارات المتاحة في القائمة المنسدلة.

في مربع الحوار نفسه، توجد ثلاث علامات تبويب مع طريقة عرض خاصة بها **التفاصيل وبيانات الاعتماد والتصريحات**.

في Credential Management، إذا كان هذا الشخص محظورًا، فسيظهر إشعار برتقالي مع الكلمة **مدرج بالقائمة السوداء**. ويعرض الإشعار أيضًا سبب الإدراج في القائمة السوداء والشخص الذي عيّن هذا الإدراج.

بإمكان المسؤول والمشغل الذي يتمتع بالحقوق المناسبة حظر الشخص من خلال النقر على الزر **إدراج في القائمة السوداء.**

– تفتح نافذة تحذير

1. انقر فوق **نعم**
2. في معالج **السبب** اكتب السبب > **حفظ > موافق**

لاحظ أن الشخص المدرج في القائمة السوداء لا يزال يحتفظ بالتصريحات المعينة له. ولكن هذا الشخص لن يتمكن من فتح مدخل/باب.

لإزالة الشخص من القائمة السوداء، ما عليك سوى النقر على الزر **إزالة X من القائمة السوداء**.

قم بتكوين الحقوق بشكل صحيح. لمزيد من المعلومات حول **حقوق المستخدم**، راجع دليل تكوين وتشغيل برنامج *Access Management System*.

التفاصيل

في علامة التبويب هذه، يمكن إدخال البيانات الشخصية التي لا يلزم أن تكون مرئية باستمرار.

كود PIN

في علامة التبويب **التفاصيل** هذه، يمكن عرض وتغيير أكواد PIN (كود PIN للتأكيد)[1] لحامل البطاقة.

ويمكن تحديد تاريخ انتهاء الصلاحية عند تغيير كود PIN.

ملاحظة: إذا تغير كود PIN أو تغيرت إعداداته، فيجب إعادة كتابة كود PIN للتأكيد.

عند وجود قفل **كود PIN** أو أكثر لبيانات اعتماد الشخص المحدد، سيظهر إشعار في أسفل عمود المعلومات الشخصية الأساسية. عندما ينقر المشغل فوق هذا الإشعار، يتم تحديد علامة التبويب **بيانات الاعتماد**، وسيتمكن المشغل من رؤية المزيد من المعلومات حول قفل **كود PIN**.
عند وجود خطأ في التحقق من الصحة على علامة تبويب، لن يكون من الممكن تحديد صفحة أخرى حتى يتم حل الخطأ.
Credential Management[1] يدعم كود PIN القياسي فقط. أكواد PIN للتعريف وأكواد IDS PIN/أكواد PIN المنفصلة للتفعيل غير مدعومة.
لمزيد من المعلومات حول **أكواد PIN**، راجع دليل تكوين وتشغيل برنامج *Access Management System*.

بيانات الاعتماد
في علامة التبويب هذه، من الممكن تعيين بطاقة مادية من خلال النقر على الزر **قراءة البطاقة** أو تعيين بيانات اعتماد المحمول من خلال النقر على الزر **إضافة الوصول عبر المحمول**. لمزيد من المعلومات، راجع تعيين بيانات اعتماد المحمول وتعيين بيانات اعتماد مادية.
ملاحظة: إذا ظهرت نقطة برتقالية على أيقونة الهاتف، فهذا يعني أن بيانات الاعتماد موجودة بالفعل على الهاتف المحمول ولكنها تحتاج إلى موافقة من الواجهة الخلفية لتطبيق Mobile Access. يتغير لون هذه النقطة إلى الأخضر فقط بعد هذه الموافقة.

التصريحات
في علامة التبويب هذه، يمكن عرض جميع التصريحات المعينة وتعديل التصريحات. لمزيد من المعلومات، راجع تعيين التصريحات من صفحة معلومات الشخصي.
في أي مربع من مربعات حوار علامات التبويب، سيؤدي النقر فوق الزر **حفظ وإغلاق** إلى إعادة التوجيه إلى مربع حوار **لوحة المعلومات**.

6.3 تعيين التصريحات

تعيين التصريحات من صفحة معلومات الشخص
– في مربع حوار لوحة المعلومات، تظهر قائمة بالأشخاص.
1. انقر فوق اسم الشخص.

– يفتح مربع حوار معلومات الشخص.
1. في الزاوية العلوية اليمنى من مربع الحوار، انقر فوق علامة تبويب **التصريحات**.
2. لتعيين تصريح جديد، انقر فوق **تعديل التصريحات**

يظهر معالج يحتوي على قائمة بجميع التصريحات. لقد تم تكوين جميع هذه التصريحات بشكل مسبق في Access Management System. من هذه الخطوة فصاعدًا، اختر التصريحات التي تريد تعيينها.

1. انقر فوق > **تأكيد** > **حفظ**.

ملاحظة: تظهر تصريحات ذات مستوى أمان عالٍ، مع تمكين وظيفة مبدأ الشخصين، مع  .

يفتح مربع حوار لوحة المعلومات. إذا تم تعيين تصريح عادي له، فيمكن التحقق مما إذا تم تعيين التصريح بالفعل من خلال النقر فوق اسم الشخص مرة أخرى وتحديد علامة تبويب **التصريحات**.
إذا تم تعيين التصريح مع مبدأ الشخصين، فستكون عندئذٍ النتيجة مختلفة. وهذا يعني أن التصريح لن يكون نشطًا فورًا بعد حفظه، بل مطلوبًا فقط. في العمودين **التصريحات** و**الإجراءات**، من الممكن معرفة من هي الجهة التي طلبت التصريح.
في علامة تبويب **التصريحات**، تظهر التصريحات بمبدأ الشخصين وكأنها موافق عليها أو مرفوضة. يمكن معرفة الجهة التي طلبت التصريح وتاريخ ووقت الطلب عن طريق تمرير الماوس فوق اسم التصريح. يظهر تعريف الأداة.

بحسب نوع التصريح وبحسب دور المستخدم وحقوق المستخدم، بإمكان أزرار **الإجراءات** المعروضة أن تكون كما يلي:

طلب
سحب - إلغاء طلب تعيين التصريح الخاص بي، والذي لم تتم الموافقة عليه بعد.
موافقة - الموافقة على طلب تعيين التصريح من قبل مشغل آخر.
رفض - رفض طلب تعيين التصريح بواسطة مشغل آخر.
إزالة - إزالة التصريح المعين. يصلح هذا الخيار للتصريحات العادية وللتصريحات ذات مستوى أمان عالٍ.

ملاحظة: لا يكون أي إجراء صالح بالنقر فقط على زر الإجراء. انقر دائمًا فوق **حفظ.**
راجع نظرة عامة على أدوار المستخدم للحصول على المزيد من المعلومات.

في AMS، يجب تكوين **ملفات تعريف المستخدمين** بشكل صحيح مع الحقوق المتاحة لمبدأ الشخصين:
- المسؤول
- المشغّل
- مبدأ الشخصين: الطالب
- مبدأ الشخصين: الموافق

للحصول على المزيد من المعلومات حول كيفية تكوين **ملفات تعريف المستخدمين**، راجع أحدث إصدار من دليل تكوين وتشغيل برنامج *Access Management System*.

طلبات التصريحات المعلقة
بإمكان المشغل الذي يتمتع بحقوق الموافق أو الطالب والمسؤول عرض **طلبات التصريحات** في القائمة. في مربع الحوار هذا، يمكن رؤية جميع **طلبات التصريحات المعلقة** في طريقة عرض واحدة دون الحاجة إلى التنقل عبر اسم كل شخص.
بإمكان المشغل الذي يتمتع بحقوق الموافق الموافقة على التصريحات من خلال مربع الحوار هذا وبإمكان المسؤول سحب التصريحات. بإمكان المشغل الذي يتمتع بحقوق الطالب عرض التصريحات المعلقة فقط. يتعذر على المشغل الذي لا يتمتع بحقوق الموافق والطالب عرض مربع الحوار هذا.
ملاحظة: لا يكون أي إجراء صالح بالنقر فقط على زر الإجراء. بعد النقر فوق زر الإجراء، يصبح لونه رماديًا، ثم انقر فوق **حفظ.**

6.4 تعيين أوراق الاعتماد المادية

الشروط الأساسية
يوصى بشدة بتعيين بيانات اعتماد جديدة للموظفين الجدد، باستخدام بطاقة جديدة وطابعة بطاقات وقارئ تسجيل.

تعيين بطاقة (بحاجة إلى قارئ البطاقات)
الإجراء
يمكن تعيين بطاقة من أيقونة لوحة التحكم إما مباشرة أو من خلال النظرة العامة على صفحة الشخص.
في **لوحة المعلومات**:
1. قم بتجهيز بطاقة وصول مادية لتقديمها إلى قارئ التسجيل.
2. حدد صف الشخص وانقر فوق 
3. اتبع الإرشادات التي تظهر في النافذة المنبثقة لاستخدام قارئ التسجيل.

من النظرة العامة على صفحة الشخص:
1. في **لوحة المعلومات**، حدد اسم الشخص وستفتح النظرة العامة على صفحة الشخص.
2. حدد علامة التبويب **بيانات الاعتماد** > **قراءة البطاقة**.

قم بتعيين بطاقة في محرر بيانات الاعتماد (بحاجة إلى قارئ تسجيل)

1. في لوحة المعلومات، في جدول الأشخاص، حدد شخصًا وانقر فوق  لتحرير بيانات اعتماد ذلك الشخص.
2. انقر فوق **قراءة البطاقة** واتبع الإرشادات التي تظهر في النافذة المنبثقة لاستخدام قارئ التسجيل.
– كرر الخطوات الأخيرة لتعيين المزيد من البطاقات، إذا كان ذلك مطلوبًا.
3. انقر فوق **حفظ** لحفظ الشخص الحالي مع تعيينات البطاقات.

6.5 تعيين بيانات اعتماد المحمول

الشروط الأساسية

– تم تثبيت Mobile Access وتكوينه على نظامك.
– راجع القسم ذي الصلة في فصل التثبيت من هذا المستند للحصول على إرشادات.
– قام الشخص المستلم بتثبيت تطبيق Mobile Access، وهو قيد التشغيل على جهازه الذكي.
– راجع القسم ذي الصلة في فصل التثبيت من هذا المستند للحصول على إرشادات.

الإجراء

يمكن تعيين بيانات اعتماد المحمول إما من أيقونة لوحة المعلومات مباشرة أو من النظرة العامة على صفحة الشخص.

في **لوحة المعلومات:**

1. حدد الصف المخصص للشخص الذي يتلقى بيانات اعتماد الهاتف المحمول
2. في الصف المحدد، انقر فوق 

من النظرة العامة على صفحة الشخص:

1. في **لوحة المعلومات**، حدد اسم الشخص وستفتح النظرة العامة على صفحة الشخص.
2. حدد علامة التبويب **بيانات الاعتماد** > **إضافة وصول عبر المحمول.**

تابع مع التعليمات التالية:

1. حدد إحدى الأيقونات الكبيرة للخيارات:

– **رمز الاستجابة السريعة**

أو

– **بريد الدعوة**

2. إذا حددت الخيار **رمز الاستجابة السريعة**:

– يعرض النظام رمز الاستجابة السريعة
– يقوم الشخص بمسح رمز الاستجابة السريعة ضوئيًا باستخدام تطبيق Mobile Access على جهازه المحمول
– لكي تعمل بيانات الاعتماد، يجب عليك **الموافقة** على الزيارة.
للتعليمات، راجع القسم اعتماد الزيارات ورفضها
– يعمل الجهاز المحمول مثل بطاقة الوصول الفعلية، طالما كان التطبيق قيد التشغيل،

3. إذا حددت الخيار **بريد الدعوة**:

– بشكل افتراضي، يحدد البرنامج عنوان البريد الإلكتروني المحدد للشخص المحدد. أدخل عنوان بريد إلكتروني بديلاً إذا لزم الأمر
– يرسل النظام بريدًا إلكترونيًا إلى العنوان المحدد
– يستلم الشخص البريد الإلكتروني على جهازه المحمول، والذي يقوم بتشغيل التطبيق Mobile Access app
– يفتح الشخص الارتباط في البريد الإلكتروني
– لكي تعمل بيانات الاعتماد، يجب عليك **الموافقة** على الزيارة.
للتعليمات، راجع القسم اعتماد الزيارات ورفضها
– يعمل الجهاز المحمول مثل بطاقة الوصول الفعلية، طالما كان التطبيق قيد التشغيل،

الإجراء في مربعات الحوار "تحرير"

1. حدد الصف المخصص للشخص الذي يتلقى بيانات اعتماد الهاتف المحمول
2. في الصف المحدد، انقر فوق 
– يفتح مربع الحوار "تحرير"
3. في VisMgmt، انقر فوق **التالي** للمتابعة إلى الشاشة **تفاصيل الزيارة**
4. انقر فوق الزر **إضافة Mobile Access**
5. حدد إحدى الأيقونات الكبيرة للخيارات:
– **رمز الاستجابة السريعة**
أو
– **بريد الدعوة**
6. إذا حددت الخيار **رمز الاستجابة السريعة**:
– يعرض النظام رمز الاستجابة السريعة
– يقوم الشخص بمسح رمز الاستجابة السريعة ضوئيًا باستخدام تطبيق Mobile Access على جهازه المحمول
– لكي تعمل بيانات الاعتماد، يجب عليك **الموافقة** على الزيارة.
للتعليمات، راجع القسم اعتماد الزيارات ورفضها
– يعمل الجهاز المحمول مثل بطاقة الوصول الفعلية، طالما كان التطبيق قيد التشغيل،
7. إذا حددت الخيار **بريد الدعوة**:
– بشكل افتراضي، يحدد البرنامج عنوان البريد الإلكتروني المحدد للشخص المحدد. أدخل عنوان بريد إلكتروني بديلاً إذا لزم الأمر
– يرسل النظام بريدًا إلكترونيًا إلى العنوان المحدد
– يستلم الشخص البريد الإلكتروني على جهازه المحمول، والذي يقوم بتشغيل التطبيق Mobile Access app
– يفتح الشخص الارتباط في البريد الإلكتروني
– لكي تعمل بيانات الاعتماد، يجب عليك **الموافقة** على الزيارة.
للتعليمات، راجع القسم اعتماد الزيارات ورفضها
– يعمل الجهاز المحمول مثل بطاقة الوصول الفعلية، طالما كان التطبيق قيد التشغيل،

راجع

- تثبيت *Mobile Access*, الصفحة *11*
- تثبيت تطبيقات *Mobile Access*, الصفحة *19*

6.6 إلغاء تعيين بيانات الاعتماد

إلغاء تعيين بطاقة من لوحة المعلومات (يتطلب قارئ تسجيل)

1. خذ البطاقة المادية من حامل البطاقة وقم بتجهيزها لتقديمها إلى قارئ التسجيل.
2. في شريط الأدوات، انقر فوق  **إلغاء تعيين البطاقة**.
3. اتبع الإرشادات التي تظهر في النافذة المنبثقة لاستخدام قارئ التسجيل.

إلغاء تعيين بطاقة في محرر بيانات الاعتماد

1. في لوحة المعلومات، وفي الجدول الرئيسي، حدد سطرًا من الجدول وانقر فوق  لتحرير حامل البطاقة هذا.

2. في مربع حوار التحرير، وفي عمود **بطاقات الموظفين**، انقر فوق  بجوار البطاقة التي تريد إلغاء تعيينها، وأكد إجراءك في النافذة المنبثقة.
كرر هذه الخطوة إلى أن تلغي تعيين كل البطاقات التي تريد إلغاء تعيينها.
3. انقر فوق **حفظ** لحفظ الزيارة الحالية مع تعيينات البطاقات.

6.7 اعتماد مُثبّتي أجهزة قراءة الوصول إلى الأجهزة المحمولة

المقدمة

يستخدم مُثبّتو قارئات الوصول إلى الأجهزة المحمولة Bosch Setup Access في المسح الضوئي للقارئات وتكوينها عبر BLE.
يرسل المشغلون المصرح لهم لكل من **Credential Management** و**Visitor Management** بيانات اعتماد افتراضية إلى تطبيق المثبت، لتخويل المثبت. يتناول هذا القسم هذا الإجراء.

الشروط الأساسية

- تم تثبيت Mobile Access وتكوينه على نظامك.
- راجع القسم ذي الصلة في فصل التثبيت من هذا المستند للحصول على إرشادات.
- تأكد من أن المُثبّت الذي يتلقى التصريح قد قام بتثبيت Bosch Setup Access، وأنه قيد التشغيل على جهازه الذكي.
- راجع القسم ذي الصلة في فصل التثبيت من هذا المستند للحصول على إرشادات.

الإجراء

1. في القائمة الرئيسية، انقر فوق  لفتح مربع الحوار **إعداد المثبت**.
2. انقر فوق **إضافة** لإضافة مثبت إلى القائمة، أو  لحذف أحد المثبتين الحاليين
- تظهر النافذة المنبثقة **إضافة مثبت**.
3. في النافذة المنبثقة **إضافة مثبت**، أدخل التفاصيل التي تطلبها، على سبيل المثال:
- الأسماء الشخصية واسم الشركة وعنوان البريد الإلكتروني ورقم الهاتف
- ملاحظة: يمكنك النقر فوق  لتعديل التفاصيل الخاصة بالمثبت المحدد في وقت لاحق
4. انقر فوق **التالي**
5. حدد إحدى الأيقونات الكبيرة للخيارات:
- **رمز الاستجابة السريعة**

أو

- **بريد الدعوة**

6. إذا حددت الخيار **رمز الاستجابة السريعة**:
- يعرض النظام رمز الاستجابة السريعة
- يقوم الشخص بمسح رمز الاستجابة السريعة ضوئيًا باستخدام تطبيق Mobile Access على جهازه المحمول
- يؤدي هذا إلى إكمال عملية تسجيل المثبت
- يمكّن الجهاز المحمول من البحث عن أجهزة قراءة Mobile Access وتكوينها بواسطة BLE، طالما أن التطبيق قيد التشغيل
7. إذا حددت الخيار **بريد الدعوة**:
- بشكل افتراضي، يحدد البرنامج عنوان البريد الإلكتروني المحدد للشخص المحدد. أدخل عنوان بريد إلكتروني بديلاً إذا لزم الأمر
- يرسل النظام بريدًا إلكترونيًا إلى العنوان المحدد
- يستلم الشخص البريد الإلكتروني على جهازه المحمول، والذي يقوم بتشغيل Bosch Setup Access
- يفتح الشخص الارتباط في البريد الإلكتروني

- يؤدي هذا إلى إكمال عملية تسجيل المثبت
- يمكّن الجهاز المحمول من البحث عن أجهزة قراءة Mobile Access وتكوينها بواسطة BLE، طالما أن التطبيق قيد التشغيل

إعادة إرسال الدعوات

1. في مربع الحوار "إعداد المثبت"، حدد المثبت المطلوب
2. انقر فوق  في نفس السطر، لإعادة إرسال التصريح إلى المثبت المحدد عن طريق رمز الاستجابة السريعة أو البريد الإلكتروني.

ملاحظة: لا يمكنك إعادة إرسال التصريح إلا إذا كان المثبت لم يقم بعد بتنشيطه.

6.7.1 إعادة تعيين أجهزة قراءة Mobile Access

قد يصبح من الضروري إعادة تعيين أجهزة القراءة الوصول إلى إعدادات المصنع الافتراضية لتمكين إعادة التكوين الخاصة بها.

على سبيل المثال، إذا احتاج أحد المثبتين إلى إعادة تكوين أجهزة قراءة الوصول عبر التي تم تكوينها بالفعل لموقع مختلف، فيجب إعادة تعيين أجهزة القراءة هذه.

راجع دليل قارئ LECTUS select للحصول على وصف لكيفية إعادة تعيين القارئ، باستخدام مفاتيح DIP الخاصة به.

6.8 استخدام تطبيقات Mobile Access على الأجهزة المحمولة

ملاحظة: تم وصف استخدام تطبيقات Bosch Mobile Access بالتفصيل للمستخدمين المعنيين في **أدلة مستخدم سريعة** منفصلة. تتوفر هذه المستندات من كتالوج منتجات Bosch عبر الإنترنت.

المقدمة

توفر Bosch التطبيقات التالية لتطبيق Mobile Access

- Bosch Mobile Access: تطبيق حامل البطاقة لتخزين بيانات الاعتماد الافتراضية ونقلها عبر Bluetooth إلى أجهزة القراءة التي تم تكوينها من أجل Mobile Access. ثم يمنح هذا القارئ الوصول أو يرفضه اعتمادًا على ما إذا كانت إحدى بيانات الاعتماد المخزنة للتطبيق صالحة له.
- Bosch Setup Access: تطبيق مثبت لفحص القراء وتكوينهم عبر Bluetooth.

بإمكان المشغلين المصرح لهم لكل من Visitor Management وCredential Management إرسال بيانات اعتماد افتراضية لكل من تطبيقات حامل البطاقة والمثبت.

إشعار!

هام: لا تقم بتشغيل تطبيقات حامل البطاقة والمثبت في الوقت ذاته
تأكد من عدم استخدام أي شخص لتطبيق المثبت عندما يكون تطبيق حامل البطاقة قيد الاستخدام، والعكس صحيح.

6.8.1 تعيين حدود RSSI في تطبيق Setup Access

المقدمة

يمكن اعتبار حد RSSI ونطاق BLE مفاهيم متكافئة تقريبًا في سياق Bosch Mobile Access.

تنقل أجهزة Mobile access إشارات BLE إلى أجهزة القراءة القريبة. يُعد إعداد حد RSSI لكل قارئ جزءًا مهمًا من تكوين القارئ. هذا الحد هو الحد الأدنى لقوة إشارة BLE، المقاسة بوحدة ديسيبل مللي وات (dBm)، والتي يقبلها القارئ (R) كطلب للدخول. على القارئ أن يتجاهل كل الإشارات الأضعف من BLE.

يمكن أن تختلف قيم RSSI بشكل كبير بناءً على العديد من العوامل، بما في ذلك نوع جهاز الإرسال ومستوى البطارية والمادة وسمك الحوائط المجاورة. لا توجد علاقة خطية بين قيمة RSSI والمسافة بين المرسل والمستقبل.
لهذا السبب، يوفر تطبيق Setup Access أداة لقياس RSSI للقارئ من الموقع الحالي للجهاز المحمول.
يتناول الإجراء أدناه كيفية استخدام هذه الأداة.
عندما تعثر على قيمة حد مناسبة لنطاق BLE، استخدم تطبيق Setup Access لتخزين هذه القيمة في تكوين القارئ.

الإجراء

قم بتكوين **نطاق BLE** باستخدام أحد الخيارين التاليين، A أو B:

أ: استخدام قيم RSSI التي يعكسها القارئ

1. ضع نفسك أمام القارئ، في النقطة التي تتوقع أن يكون فيها مستخدم بيانات اعتماد الهاتف المحمول.
2. انقر فوق **التحقق من النطاق الحالي واستخدامه**

– ستظهر رسالة منبثقة. اضغط على **موافق**

3. ستظهر قيمة RSSI.

– إجراء موصى به: كرر هذه الخطوة عدة مرات من نفس الموضع، للحصول على انطباع عن درجة التباين في قوة الإشارة المتصورة.

4. عندما تجد قيمة حد مناسبة، انقر فوق **حفظ**.

ب: تعيين حد RSSI يدويًا

1. أدخل قيمة في حد RSSI.
انظر جدول الحدود النموذجية أدناه
2. اضغط على **حفظ**

قيم الحدود النموذجية (تقريبية فقط):

المسافة المتوقعة من الجهاز المحمول إلى القارئ	حد RSSI المقترح
القريب (5 - 10 سم)	-30... -40 ديسيبل ملي وات
المتوسط (0.5 - 2 م)	-50... -60 ديسيبل ملي وات
البعيد (> 2 م)	-70... -90 ديسيبل ملي وات

إشعار!

يمكن أن تختلف قيم RSSI بشكل كبير بناءً على العديد من العوامل، بما في ذلك نوع جهاز الإرسال ومستوى البطارية والمادة وسمك الحوائط المجاورة.

المصطلحات

ACS

اسم عام لنظام التحكم في الوصول من Bosch، على سبيل المثال AMS (Access Management System) أو ACE (BIS Access Engine).

BLE

تعتبر Bluetooth Low Energy تقنية شبكة لاسلكية توفر نطاق اتصالات مماثل لنطاق اتصالات Bluetooth، ولكن مع استهلاك أقل للطاقة.

FQDN

اسم المجال المؤهل بالكامل هو اسم مجال شبكة يعبر عن موقعه المطلق في التسلسل الهرمي لـ "نظام اسم المجال" (DNS).

GDPR

إن القانون العام لحماية البيانات (GDPR) هو قانون الخصوصية والأمن الذي وضعه الاتحاد الأوروبي (EU)، ودخل حيز التنفيذ في عام 2018. يفرض هذا القانون التزامات على المؤسسات الموجودة في أي مكان في العالم والتي تعمل على جمع البيانات المتعلقة بالأشخاص في الاتحاد الأوروبي.

Mobile Access

التحكم في وصول الأشخاص الذين يستخدمون بيانات اعتماد افتراضية مخزنة على جهاز محمول مثل الهاتف الذكي للشخص.

OSDP

يمثل Open Supervised Device Protocol "بروتوكول الجهاز الخاضع للإشراف المفتوح" معيار اتصالات التحكم في الوصول، تم تقديمه في عام 2011 من قبل "جمعية صناعة الأمان" (SIA). يوفر مزايا مقارنة بالبروتوكولات القديمة في مجالات التشفير والقياسات الحيوية وسهولة الاستخدام والتشغيل البيني.

RSSI

مؤشر قوة الإشارة المستقبلة (RSSI) هو قوة الإشارة التي يراها جهاز الاستقبال، وتُقاس بوحدة الديسيبل مللي وات (dBm). تعرض الأجهزة المحمولة عادةً RSSI بواسطة رسم شريطي يمثل قوة الإشارة.

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

Building solutions for a better life

202405132108