



# Visitor Management V5.5

مع Mobile Access

ar

ل التشغيل



## جدول المحتويات

5	<b>الأمان</b>	1
6	<b>المقدمة</b>	2
6	عن إدارة الزائرين Bosch	2.1
6	حول Mobile Access	2.2
6	الجمهور المستهدف	2.3
6	كيفية استخدام هذا التوثيق.	2.4
7	<b>نظرة عامة على النظام والطبوغرافيا</b>	3
8	<b>التثبيت وإلغاؤه</b>	4
8	متطلبات البرمجيات والأجهزة	4.1
8	النظام الرئيسي للتحكم في الوصول	4.1.1
9	مثيلة قاعدة بيانات لاستضافة قاعدة بيانات مدير الزائرين	4.1.2
9	مستخدم مخصص للوصول إلى قاعدة بيانات محلية	4.1.3
9	مستخدم مخصص للوصول إلى قاعدة بيانات بعيدة	4.1.4
10	مستخدم مخصص في النظام الرئيسي للتحكم في الوصول	4.1.5
10	تثبيت الخادم	4.2
10	تشغيل برنامج إعداد الخادم	4.2.1
11	ملف Appsettings بصيغة JSON	4.2.2
11	إعداد كمبيوتر عميل VisMgmt	4.3
12	إعداد الوظيفة الإضافية Peripheral Devices	4.3.1
13	شهادات الاتصال الآمن	4.3.2
15	ملف Appsettings بصيغة JSON	4.3.3
16	التحقق من تثبيت الخادم	4.4
16	تثبيت Mobile Access	4.5
16	نظرة عامة على التثبيت والتكوين والاستخدام	4.5.1
17	المتطلبات الأساسية لأجهزة Mobile Access	4.5.2
17	المتطلبات الأساسية لتكوين Mobile Access	4.5.3
18	إجراء التثبيت في نفس الموقع	4.5.4
19	إجراء التثبيت الموزع	4.5.5
22	تثبيت تطبيقات Mobile Access	4.6
22	الأجهزة الطرفية	4.7
23	تسجيل الأجهزة الطرفية باستخدام كمبيوتر العميل	4.7.1
23	إصلاح عمليات تثبيت Mobile Access	4.8
23	إزالة تثبيت البرامج	4.9
25	<b>التكوين</b>	5
25	إنشاء مستخدم إدارة الزائرين في ACS	5.1
26	إنشاء المصادقات وملفات التعريف للزائرين في ACS	5.2
26	إعداد كمبيوتر موظف الاستقبال	5.3
26	إعداد كمبيوتر كشك للزائرين	5.4
26	تسجيل الدخول لمهام التكوين	5.5
27	استخدام قائمة الإعدادات في التكوين	5.6
29	قوالب البريد الإلكتروني	5.6.1
31	وضع المعاينة	5.6.2
31	قوالب المستندات	5.6.3
31	تخصيص واجهة المستخدم	5.7
31	تكوين الخيارات التي ستكون ظاهرة وغير ظاهرة وإلزامية	5.7.1
31	تخصيص نصوص واجهة المستخدم للتطبيقات اللغوي	5.7.2
32	تخصيص وضع الكشك	5.7.3
32	تخصيص شعار الشركة	5.7.4

32	إعدادات جدار الحماية	5.8
33	البرامج والخدمات كاستثناءات جدار الحماية	5.8.1
35	واجهة برمجة التطبيقات (API) لتطبيق Mobile Access	5.8.2
36	أمان تكنولوجيا المعلومات	5.9
36	مسؤوليات الأجهزة	5.9.1
36	مسؤوليات البرامج	5.9.2
36	التعامل الآمن مع بيانات اعتماد المحمول	5.9.3
37	النسخ الاحتياطي للنظام	5.10
38	<b>التشغيل</b>	<b>6</b>
38	نظرة عامة على أدوار المستخدمين	6.1
38	استخدام لوحة المعلومات	6.2
38	نظرة عامة على صفحة الشخص	6.2.1
38	جدول الزيارات	6.2.2
40	أعمدة الجدول وإجراءاته	6.2.3
41	موظف الاستقبال	6.3
41	تسجيل الدخول إلى دور موظف الاستقبال	6.3.1
41	البحث في الزيارات وتصنيفها	6.3.2
41	تسجيل الزيارات	6.3.3
43	اعتماد الزيارات ورفضها	6.3.4
43	تعيين أوراق الاعتماد الفعلية	6.3.5
45	تعيين بيانات اعتماد المحمول	6.3.6
46	إلغاء تعيين بيانات الاعتماد	6.3.7
47	تسجيل الوصول والمغادرة بدون بطاقة	6.3.8
48	الإضافة إلى القائمة المحظورة والإزالة والإعفاء منها	6.3.9
48	الحفاظ على ملفات تعريف الزائرين	6.3.10
49	عرض سجلات الزيارات	6.3.11
49	المستضيف	6.4
49	تسجيل الدخول إلى دور المستضيف	6.4.1
49	البحث والتصنيف	6.4.2
50	تسجيل الزيارات	6.4.3
50	نسخ مواعيد الزيارات	6.4.4
51	زائر	6.5
51	مقدمة إلى وضع الكشك	6.5.1
51	إنشاء ملف تعريف لزائر: تسجيل الوصول الذاتي	6.5.2
51	اعتماد مَثْبُتي أجهزة قراءة الوصول إلى الأجهزة المحمولة	6.6
53	إعادة تعيين أجهزة قراءة Mobile Access	6.6.1
53	استخدام تطبيقات Mobile Access على الأجهزة المحمولة	6.7
53	تعيين حدود RSSI في تطبيق Setup Access	6.7.1
55	<b>المصطلحات</b>	

# الأمان

## 1

### 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](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 إطلافاً مسؤولية أي ضرر ناتج عن تشغيل منتجاتها باستخدام مكونات برمجية قديمة.

## 2 المقدمة

### 2.1 عن Bosch لإدارة الزائرين

Visitor Management، يُشار إليه في ما بعد باسم VisMgmt عبارة عن أداة برمجية تعمل على المستعرض وبالتناغم مع نظم Bosch للتحكم في الوصول. إنه يدير الزيارات إلى موقع تحت التحكم في الدخول، بما في ذلك جدولة الزيارات، والبيانات المهنية للزائر، والمستندات والعقود المرتبطة، وتعيين بيانات اعتماد مؤقتة. واجهة المستخدم قابلة للتخصيص ويجوز لأي مستخدم أن يغير لغته أثناء التشغيل من دون تسجيل الخروج. المستخدمون الرئيسيون وحالات استخدامهم هي:

حالات الاستخدام	نوع المستخدم
تسجيل الزيارات الجديدة والزائرين اعتماد الزيارات ورفضها إدراج زائرين في القائمة المحظورة تعيين بطاقات الزائرين وإلغاء تعيينها إدارة المستندات المرتبطة مراقبة عدد الزائرين على الموقع	موظف الاستقبال
التسجيل الذاتي والمسبق إنشاء ملف تعريف للزائر والمفاظ عليه توقيع المستندات	زائر
إدارة الجداول الزمنية وقوائم الزيارات والزائرين التسجيل المسبق للزيارات	المستضيف
عمل إعدادات عامة تخصيص سلوك الأداة وواجهة المستخدم بها علاوة على: جميع حالات الاستخدام الخاصة بموظف الاستقبال	مسؤول

### 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.

### 2.3 الجماهير المستهدفة

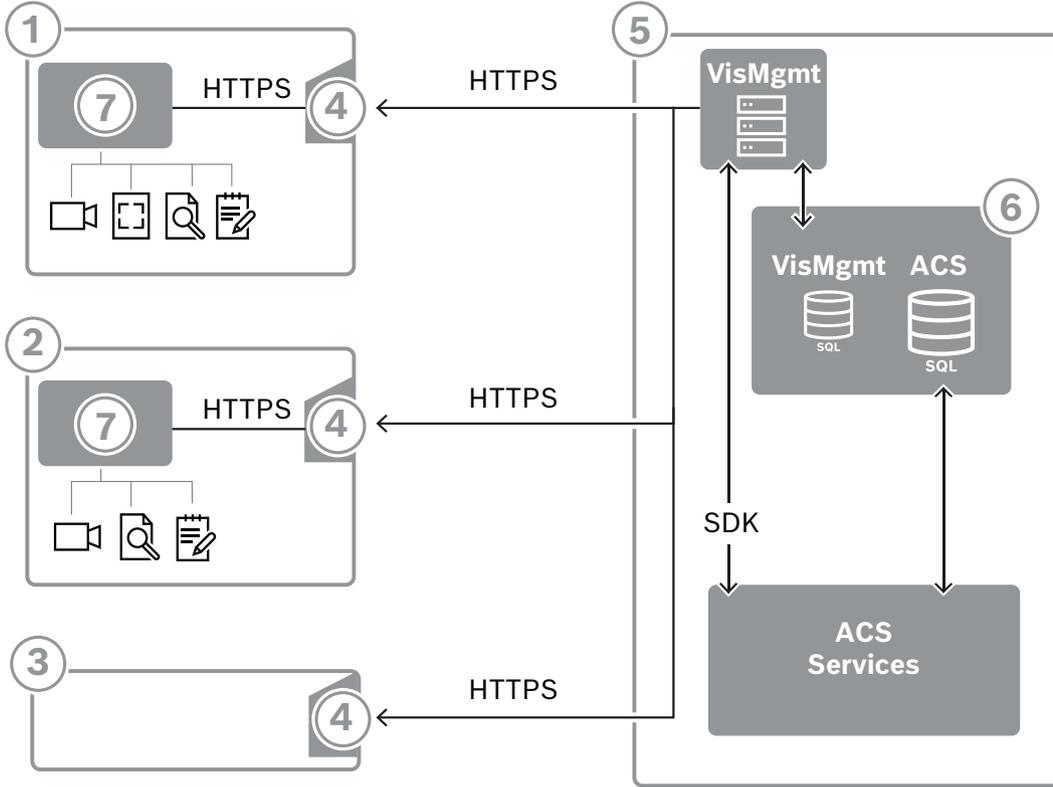
- المثبتون والمسؤولون في Visitor Management
- أنواع المستخدمين الرئيسيين في Visitor Management

### 2.4 كيفية استخدام هذا التوثيق.

- استخدم وظيفة البحث في عارض المساعدة لديك لتحديد موقع المحتوى المعني.
- تُعتبر أقسام النظرة العامة على النظام والتثبيت والتكوين ذات أهمية أساسية بالنسبة إلى مسؤولي النظام
- تُعتبر أقسام التشغيل ذات أهمية أساسية بالنسبة إلى مستخدمي النظام.

## نظرة عامة على النظام والطبوغرافيا

3



الوصف	التسمية
محطة عمل <b>موظف الاستقبال</b> . بإمكان محطة العمل هذه أن تحتوي على أجهزة طرفية اختيارية، مثل قارئ التسجيل وكاميرا الويب والمساحات الضوئية للتوقيعات والمستندات.	1
محطة عمل كشك <b>الزائرين</b> ، مع المستعرض المدعوم في وضع الكشك. بإمكان محطة العمل هذه أن تحتوي على أجهزة طرفية اختيارية، مثل كاميرا الويب والمساحات الضوئية للتوقيعات والمستندات.	2
محطة عمل <b>المضيف</b> ، أي محطة عمل الموظف الذي يستقبل الزائر.	3
المستعرض المدعوم مع موقع ويب VisMgmt	4
خادم ACS (AMS أو BIS)	5
مثيل قاعدة البيانات لخادم ACS (بإمكان هذا المثل أن يكون موجودًا على جهاز كمبيوتر منفصل).	6
<b>الوظيفة الإضافية Bosch Peripheral Devices</b> الاختيارية، التي تدير الاتصال بين المستعرض والأجهزة الطرفية.	7

تحتوي الطبوغرافيا الموصى بها للنظام على خادم VisMgmt على الكمبيوتر نفسه الخاص بخادم النظام الرئيسي للتحكم في الوصول وقاعدة بياناته على مثيل قاعدة البيانات نفسها. يتم تثبيت الوظيفة الإضافية Bosch Peripheral Devices فقط على محطات العمل التي تتطلب الوصول إلى الأجهزة الطرفية. عادةً ما تتطلب محطة عمل المضيف فقط وصول المستعرض إلى خادم VisMgmt.

## 4.1 التثبيت وإلغاؤه متطلبات البرمجيات والأجهزة

- قم بتثبيت خادم VisMgmt على نفس الكمبيوتر حيث تم تثبيت نظام التحكم في الوصول الرئيسي: تنطبق متطلبات البرامج والأجهزة نفسها.
- إذا لم يكن نظام التحكم في الوصول الرئيسي مثبتًا بعد، فتأكد من تثبيته أولاً قبل تثبيت Visitor 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.

### متطلبات الخادم

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 مثل قاعدة البيانات نفسها الذي يستخدمه ACS (نظام التحكم في الوصول الأساسي)
الحد الأدنى لدقة الشاشة	دقة عالية كاملة 1080×1920
المستعرضات المدعومة	Google Chrome، Mozilla Firefox، وMicrosoft Edge (قائم على Chromium) استخدم الإصدار الأحدث من المستعرض لنظام التشغيل Windows. نظام التشغيل.

### متطلبات الوظيفة الإضافية Bosch Peripheral Devices

إن **الوظيفة الإضافية Bosch Peripheral Devices** هي البرنامج الذي يتعامل مع الاتصال الإلكتروني بين المستعرض والأجهزة الطرفية مثل قارئ التسجيل وكاميرا الويب والماسح الضوئي للتوقيعات والماسح الضوئي للمستندات.

كمبيوتر العميل هو الكمبيوتر المتصل فعليًا بالأجهزة الطرفية. وهو يقوم أيضًا بتشغيل المستعرض الذي يتصل بالخادم VisMgmt.

على الرغم من أن الأجهزة الطرفية ليست ضمن المتطلبات الصارمة للتثبيت، لكن يوصى بها بطريقة ملحة لأنها تؤدي إلى زيادة كبيرة في كفاءة عملية تسجيل الزائرين.

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

### 4.1.1 النظام الرئيسي للتحكم في الوصول

#### بدون Mobile Access

إذا لم يكن Mobile Access مطلوبًا، فإن الإصدار 5.5 من VisMgmt يعمل مع أنظمة التحكم في الوصول التالية من Bosch:

- Access Management System (AMS) الإصدار 5.5 والإصدار اللاحق

#### مع Mobile Access

إذا تم اختيار Mobile Access كترخيص إضافي، فإن الإصدار 5.5 من VisMgmt يعمل مع أنظمة التحكم في الوصول التالية من Bosch:

- Access Management System (AMS) الإصدارات 5.5 (يتضمن ملحق Mobile Access) والإصدارات اللاحقة

أكمل عملية تثبيت نظام التحكم في الوصول الرئيسي وتحقق منه، وفقًا لدليل التثبيت الخاص به، قبل متابعة عملية تثبيت VisMgmt.

### 4.1.2 مثيلة قاعدة بيانات لاستضافة قاعدة بيانات مدير الزائرين

يؤدي تثبيت النظام الرئيسي للتحكم في الوصول إلى إنشاء مثيل قاعدة بيانات يمكنك استخدامه لاستضافة ملف قاعدة بيانات dbVisitorManagement، VisMgmt.

يختلف الاسم الافتراضي لهذا المثيل، بحسب ACS

- بالنسبة إلى AMS، الاسم هو ACE

- بالنسبة إلى BIS ACE، الاسم هو BIS\_ACE

### 4.1.3 مستخدم مخصص للوصول إلى قاعدة بيانات محلية

يدخل المستخدم VMUser إلى قاعدة بيانات مدير الزائرين بالنيابة عن تطبيق VisMgmt. ينشئ برنامج تثبيت الخادم VisMgmt مستخدمًا لنظام VMUser على خادم VisMgmt.

### 4.1.4 مستخدم مخصص للوصول إلى قاعدة بيانات بعيدة

إذا كان VisMgmt سيستخدم قاعدة بيانات على خادم قاعدة بيانات بعيدة، فقم بإنشاء وتكوين مستخدم VMUser في Windows وعلى SQL Server كما سيرد وصفه أدناه. مهم: لا تشغل إعداد VisMgmt قبل إتمام هذا الإجراء.

1. على خادم قاعدة البيانات البعيد، أنشئ مستخدم Windows بالإعدادات التالية:

- اسم المستخدم (حساس لحالة الأحرف): VMUser

- كلمة المرور: قم بتعيين كلمة المرور وفقًا لسياسات الأمان التي تنطبق على جميع أجهزة الكمبيوتر لديك. سجل كلمة المرور بتأني لأنها ستكون مطلوبة لإعداد VisMgmt.

- عضو في المجموعة: Administrators

- 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

(إضافة VMUser كتسجيل دخول إلى SQL Server البعيد)

1. فتح SQL Management Studio

2. الاتصال بمثيل SQL البعيد

3. الانتقال إلى الأمان < تسجيل الدخول

4. إضافة VMUser المستخدم مع دور الخادم sysadmin

في وقت لاحق، عندما تقوم بتنفيذ إعداد VisMgmt على خادم VisMgmt، ستحدد خيار كمبيوتر خادم قاعدة البيانات البعيدة وتُدخل كلمة المرور التي حددتها أعلاه لـ VMUser.

## 4.1.5

**مستخدم مخصص في النظام الرئيسي للتحكم في الوصول**

1. في النظام الرئيسي للتحكم في الوصول، قم بإنشاء مستخدم لديه ميزة الاستخدام غير المحدود لواجهة برمجة التطبيقات.  
للاطلاع على إرشادات تفصيلية، انظر الفصل **تعيين ملفات تعريف المستخدم (المشغل)** في دليل المشغل للنظام الرئيسي للتحكم في الوصول.
2. إذا كنت تستخدم BIS ACE، فسجل دخولك إلى عميل BIS الكلاسيكي أو الذكي مرة واحدة مع هذا المستخدم، لتعيين كلمة المرور.
3. قم بتدوين اسم المستخدم وكلمة المرور بعناية لأن معالجات تثبيت VisMgmt ستطلبهما.

## 4.2

**تثبيت الخادم**

لا تبدأ تشغيل برنامج الإعداد قبل أن تقدم كل متطلبات البرمجيات. عند استخدام AMS، Visitor Management، Credential Management، Mobile Access 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.

## 4.2.1

**تشغيل برنامج إعداد الخادم**

1. على خادم VisMgmt المقصود، قم بتشغيل BoschVisitorManagementServer.exe كمسؤول.
2. انقر فوق **التالي** لقبول حزمة التثبيت الافتراضية.
3. إذا كنت توافق على اتفاقية ترخيص المستخدم النهائي (EULA)، فاقبلها وانقر فوق **التالي**.
4. حدد مجلد الوجهة للتثبيت. المجلد الافتراضي هو المجلد المستحسن.
- على شاشة **تكوين خادم SQL**
5. حدد ما إذا كنت ترغب في إنشاء قاعدة بيانات على ميثيل خادم SQL المحلي، أي على ميثيل قاعدة البيانات على الخادم VisMgmt أو على كمبيوتر خادم قاعدة بيانات بعيدة.
- **ملاحظة:** إذا اخترت خادم قاعدة بيانات بعيدة، فيطلب برنامج الإعداد كلمة مرور VMUser، وهو المستخدم المسؤول الذي قمت بإعداده على خادم قاعدة البيانات البعيدة (انظر قسم "متطلبات البرمجيات").
6. تحقق من قيم المعلمات التالية وقيم بتعديلها، إذا لزم الأمر:

اسم كمبيوتر خادم قاعدة البيانات	خادم SQL
اسم ميثيل قاعدة بيانات ACS الرئيسية. هذا هو المكان الذي يتم فيه إنشاء قاعدة بيانات الزائرين. بالنسبة إلى AMS، الاسم هو ACE بالنسبة إلى BIS ACE، الاسم هو BIS_ACE	<b>ميثيل SQL</b>
اسم مستخدم مسؤول للميثيل، وهو عادةً sa	<b>اسم مستخدم SQL</b>
كلمة مرور هذا المستخدم المسؤول.	<b>كلمة مرور SQL</b>

7. انقر فوق **اختبار الاتصال** لاختبار ما إذا كان يمكن الوصول إلى ميثيل قاعدة البيانات باستخدام قيم المعلمات التي أدخلتها. إذا فشل الاختبار، فأعد فحص المعلمات.
8. انقر فوق **التالي** للمتابعة
- في شاشة **تكوين الوصول إلى ACS** (حيث يشير ACS إلى النظام الرئيسي للتحكم في الوصول، وهو AMS أو ACE)
9. أدخل قيمًا للمعلمات التالية:

اسم مضيف ACS	اسم كمبيوتر الذي يتم فيه تشغيل ACS
اسم المستخدم المخصص لنظام ACS مع استخدام غير محدود لواجهة برمجة التطبيقات. انظر قسم متطلبات البرمجيات.	<b>اسم مستخدم ACS</b>
كلمة مرور مستخدم ACS المخصص هذا.	<b>كلمة مرور ACS</b>

10. انقر فوق **التالي** للمتابعة
- على شاشة **تكوين خادم الهوية**
11. أدخل URI لخادم هوية ACS المناظر:  
AMS: HTTPS://<NameOfACSserver>:44333 -  
BIS: HTTPS://<NameOfACSserver>/BisIdServer -
12. انقر فوق **اختبار الاتصال** لاختبار ما إذا كان يمكن الوصول إلى خادم الهوية.
13. انقر فوق **التالي** للاطلاع على شاشة الملخص، ثم انقر فوق **تثبيت** لبدء تثبيت خادم VisMgmt.
14. بعد التثبيت، أعد تمهيد الكمبيوتر.

## ملف Appsettings بصيغة JSON

## 4.2.2

يتم تخزين عدد من معلمات التكوين لخادم VisMgmt في ملف JSON التالي:

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

ليس من الضروري عمومًا تغيير القيم الافتراضية، لكن قد يكون من المفيد تعديل المعلمات التالية في قسم **الإعدادات** في الملف. إذا قمت بضبط المعلمات، فعليك إنشاء نسخة احتياطية من الملف أولاً. ستساعدك النسخة الاحتياطية على التراجع عن التغييرات بسرعة إذا تسببت تغييراتك في حدوث خلل. احفظ تغييراتك وأعد تشغيل خدمة VisMgmt في Windows لتصبح المعلمات المعدلة سارية المفعول. اسم الخدمة هو Bosch Visitor Management.

الوصف	القيمة الافتراضية	اسم المعلمة
أقصى عدد لسجلات الزيارات التي تظهر على الشاشة في المرة الواحدة. عندما يقوم المستخدم بالتمرير، تمتلئ كل صفحة جديدة بهذا العدد من السجلات التي يتم تحميلها من قاعدة البيانات.	20	PageSizeNumberOfVisit
أقصى عدد من وحدات البايت التي يمكن أن يحتوي عليها ملف محمل.	31457289	MaximumUploadFileSizeBytes
ينتظر التطبيق خلال هذا العدد من الثواني إذا توقف المستخدم بشكل مؤقت أثناء إدخال معلومات تسجيل الدخول ثم يطلب الإدخال.	300	StartoverTimeoutAskSeconds
بعد الطلب، ينتظر التطبيق خلال هذا العدد من الثواني قبل أن يعيد تعيين شاشة تسجيل الدخول.	60	StartoverTimeoutResetSeconds

## إعدادات كمبيوتر عميل VisMgmt

## 4.3

يمكن تثبيت الوظيفة الإضافية Bosch Peripheral Devices على كمبيوتر الخادم، لكن يجري تثبيتها في العادة على كمبيوتر العميل في الشبكة نفسها. إذا كان الأمر كذلك، فانسخ شهادة HTTPS من خادم ACS وقم بتثبيتها على كمبيوتر العميل أيضًا. راجع شهادات الاتصال الآمن، الصفحة 13 أدناه للاطلاع على التعليمات.

تُعد الوظيفة الإضافية Bosch Peripheral Devices برنامج الربط للأجهزة الطرفية مثل أجهزة قراءة التسجيل والمساحات الضوئية. إذا لم تكن مثل هذه الأجهزة مطلوبة، على سبيل المثال، للمستخدم المضيف، فإن الوصول إلى المستعرض يكفي لتسجيل الدخول إلى تطبيق VisMgmt وتشغيله.

يتم دعم أجهزة قراءة التسجيل وتنسيقات البطاقات التالية.

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

### راجع

- شهادات الاتصال الآمن، الصفحة 13

## إعداد الوظيفة الإضافية Peripheral Devices

### 4.3.1

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 **سماع** 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.

## 4.3.2

## 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

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

## 4.3.2.1

## 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:

- <ممر ك أقرص 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.
  - افتح 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.

## 4.3.2.2

**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 (chrome://settings) 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**.

## 4.3.2.3

**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 يمنع هذا القارئ الوصول أو يرفضه اعتمادًا على ما إذا كانت إحدى بيانات الاعتماد المخزنة للتطبيق صالحة له.
- Bosch Setup Access: تطبيق مثبت لفحص القراءة وتكوينهم عبر Bluetooth. بإمكان المشغلين المصرح لهم لكل من Visitor Management و Credential 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 تتم 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 و Apple وتثبيتها بالطريقة المعتادة. وأسمائها في متاجر التطبيقات هي:
- Bosch Mobile Access
  - Bosch Setup Access

## 4.3.3

**ملف Appsettings بصيغة JSON**

يتم تخزين عدد من معلمات التكوين لكمبيوتر العميل VisMgmt في ملف JSON التالي:  
 <محرك أقراص التثبيت>: Program Files (x86)\Bosch Sicherheitssysteme\Bosch Visitor Management\appsettings.json  
 ليس من الضروري عمومًا تغيير القيم الافتراضية، لكن قد يكون من المفيد تعديل المعلمات التالية في قسم **AppSettings** في الملف.  
 احفظ تغييراتك وأعد تشغيل خدمة VisMgmt في Windows لتصبح المعلمات المعدلة سارية المفعول.  
 اسم الخدمة هو Bosch Ace Visitor Management Client

الوصف	مثال	اسم المعلمة
العنوان ورقم المنفذ لخادم إدارة الزائرين.	"https://my-vm-server:5706"	CorseOrigins
رقم منفذ COM الذي يتصل به قارئ تسجيل LECTUS. بالنسبة إلى أجهزة قراءة HID OMNIKEY، بإمكان هذه المعلمة أن تكون فارغة.	"com3"	CardReaderPort

## التحقق من تثبيت الخادم

### 4.4

من كمبيوتر في الشبكة نفسها، وباستخدام أحد المستعرضات المدعومة، افتح عنوان URL التالي:  
 https://<كمبيوتر خادم>:5706/main VisMgmt  
 إذا كان الخادم يعمل، فإنه يعرض صفحة تسجيل الدخول إلى التطبيق.

## تثبيت Mobile Access

### 4.5

### المقدمة

توفر خدمة الواجهة الخلفية لتطبيق Mobile Access وظيفة الوصول عبر المحمول لكل من Credential Management و Visitor 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 VisMgmt و CredMgmt، 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.

## نظرة عامة على التثبيت والتكوين والاستخدام

### 4.5.1

يتطلب Mobile Access عدة مكونات للعمل بصورة متسقة. نسرده المراحل الإجمالية هنا، وتتناول 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 حامي 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.

## 4.5.2 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 و W إلى اللونين، الأسود أو الأبيض
- يشير O إلى OSDP
- يشير K إلى وجود لوحة مفاتيح
- يعني الحرف M ملاءمة Mobile Access

## 4.5.3 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 و SQL Server. في أثناء الإعداد الموضوع 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): <MAUser>\ACS-Domain
  - 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 dbcreator و public

### 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.

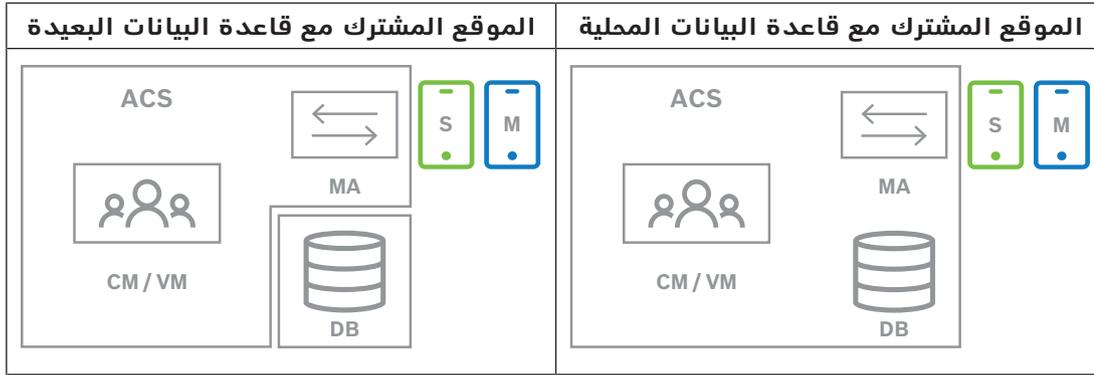
## 4.5.4

### 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 لإجراء التثبيت الموزع.



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" لمثبي ومكوني النظام
M	تطبيق Mobile Access للأجهزة المحمولة لأصحاب بيانات الاعتماد العادية.

### الإجراء

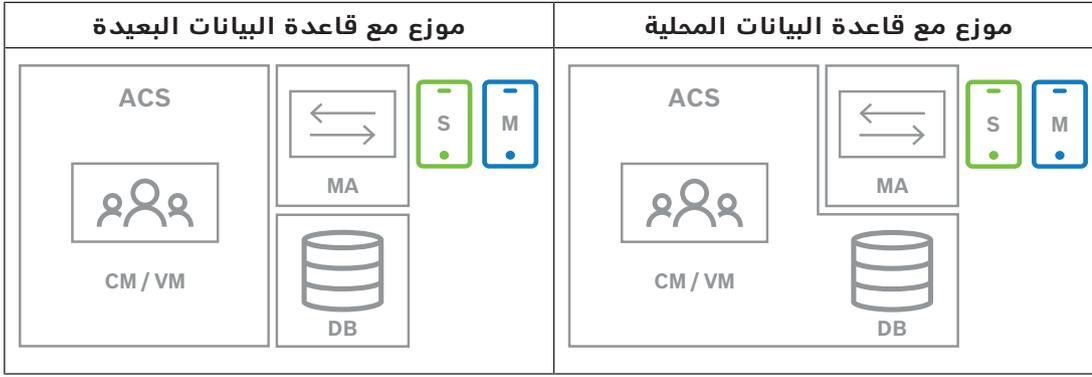
1. على خادم ACS، والذي يعتبر أيضًا خادم Mobile Access للتثبيت في نفس الموقع، قم بتشغيل `BoschMobileAccessBackend.exe` كمسؤول
- افتح برنامج الإعداد
2. على شاشة الموقع، حدد نوع الإعداد: الموقع المشترك
3. في شاشة المكونات، تحقق من تحديد Bosch Mobile Access وانقر فوق التالي
4. على شاشة اتفاقية ترخيص المستخدم 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 الواجهة 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 بديلاً للخطوة التالية:
- البديل 1 خيار **قاعدة البيانات المحلية**:
  - يعثر برنامج الإعداد على قاعدة البيانات المحلية ويحددها مسبقاً.
  - 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 ميثيل 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 مسبقاً) 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.

## 4.5.5

### 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 سماحي".
- 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:
- تثبت **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>



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" لمثبي 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.
  - افتح 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** لاحقاً 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 الواجهة 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 بديلاً للخطوة التالية:
  - البديل 1 خيار **قاعدة البيانات المحلية**:
    - يعثر برنامج الإعداد على قاعدة البيانات المحلية ويحددها مسبقاً.
    - 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 ميثيل 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
  - افتح 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 **تبدال 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 **تبدال 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.

## تثبيت تطبيقات Mobile Access

### 4.6

#### 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 يمنع هذا القارئ الوصول أو يرفضه اعتمادًا على ما إذا كانت إحدى بيانات الاعتماد المخزنة للتطبيق صالحة له.
- Bosch Setup Access: تطبيق مثبت لفحص القراءة وتكوينهم عبر Bluetooth. بإمكان المشغلين المصرح لهم لكل من Visitor Management و Credential 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 و Apple وتثبيتها بالطريقة المعتادة. وأسمائها في متاجر التطبيقات هي:
- Bosch Mobile Access
  - Bosch Setup Access

## الأجهزة الطرفية

### 4.7

تم اختبار أجهزة USB الطرفية التالية واعتمادها للاستخدام مع VisMgmt و CredMgmt في وقت الكتابة. للاطلاع على قائمة محدثة باستمرار للأجهزة الطرفية، راجع جدول البيانات للنظام الرئيسي للتحكم في الوصول.

LECTUS enroll ARD-EDMCV002-USB, HID OMNIKEY 5427 CK	قارئ تسجيل البطاقات
ARH Combo, ARH Osmond	ماسحة ضوئية لمستندات الهوية
signotec LITE, signotec Omega	الماسحة الضوئية للتوقيع

اتبع تعليمات جهة التصنيع لتوصيل هذه الأجهزة بأجهزة الكمبيوتر العميل لديك.

#### أجهزة قراءة التسجيل

يتم دعم أجهزة قراءة التسجيل وتنسيقات البطاقات التالية.

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

### تسجيل الأجهزة الطرفية باستخدام كمبيوتر العميل

4.7.1

لتسجيل الأجهزة الطرفية باستخدام كمبيوتر العميل VisMgmt، قم بتشغيل برنامج إعداد Bosch Peripheral Devices، BoschPeripheralDeviceAddon.exe، على العميل. للحصول على الإرشادات، راجع إعداد الوظيفة الإضافية Peripheral Devices، الصفحة 12.

#### راجع

– إعداد الوظيفة الإضافية Peripheral Devices، الصفحة 12

### إصلاح عمليات تثبيت Mobile Access

4.8

#### 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.
- إعادة إنشاء الشهادة، في شاشة **الشهادات**، حدد زر **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 مستخدم ومثبي Mobile Access إلى شهادة Mobile Access الجديدة.

### إزالة تثبيت البرامج

4.9

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:** تمتوي 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.

## التكوين

### إنشاء مستخدم لإدارة الزائرين في ACS

5

5.1

#### المقدمة

يجب على كل مسؤول أو موظف استقبال أو مستخدم مضيف VisMgmt أن يكون حاملاً لبطاقة بتعريف مُشغّل مستقلّ في ACS، وهو النظام الرئيسي للتحكم في الوصول وتحتوي تعريفات المُشغّل هذه على حقوق VisMgmt خاصة تأتي في شكل **ملفات تعريف المستخدم**. راجع المساعدة عبر الإنترنت في ACS للحصول على معلومات مفصلة وإرشادات بخصوص **ملفات تعريف المستخدم**.

- يجب تحديد مُشغّل منفصل لكل حامل بطاقة يعمل في إدارة الزائرين. لا يُمكنك تعيين حاملي بطاقات متعددين للمُشغّل ذاته.

#### إشعار!

أمن تكنولوجيا المعلومات وحسابات المستخدمين وفقاً لأفضل الممارسات لأمن تكنولوجيا المعلومات، نوصي بأن يعمل كل موظف استقبال ومضيف ومسؤول ضمن حساب Windows الخاص به.



#### إنشاء ملفات تعريف المستخدم لإدارة الزائرين

1. قم بتسجيل الدخول إلى النظام الرئيسي للتحكم في الوصول باستخدام امتيازات المسؤول.
  2. قم بإنشاء ملف تعريف مستخدم (مشغل) واحد أو أكثر لمستخدمي VisMgmt.  
مسار مربع الحوار:
  - **التكوين > المشغّلون ومحطات العمل > ملفات تعريف المستخدمين**
  - مستعرض التكوين > الإدارة > ملفات تعريف مستخدمي ACE
  3. قم بتعيين أحد حقوق المستخدم التالية لملفات التعريف هذه.
  - المسؤول: Visitor Management > Administrator
  - المستضيف: Visitor Management > Host
  - موظف الاستقبال: Visitor Management > Receptionist
- بعد انتهائك من إنشاء ملفات تعريف المستخدمين التي تريدها لأدوار VisMgmt المختلفة (المسؤول، موظف الاستقبال، المستضيف)، يُمكنك تعيين كل ملف تعريف لعدة مُشغلين.

#### تعيين ملفات تعريف المستخدمين لمشغلي ACS وحاملي البطاقات

مسار مربع الحوار:

- **التكوين > المشغّلون ومحطات العمل > حقوق المستخدم**
  - مستعرض التكوين > الإدارة > المشغّلون
1. قم بإضافة نوع مُشغّل جديد (انقر على  أو  ، بناءً على ACS) وأطلق اسمًا عليها بحيث يعكس بوضوح أدوار VisMgmt (المسؤول، أو المضيف، أو موظف الاستقبال).
  2. في علامة التبويب إعدادات المُشغّل العام، حدد ACE Operator من قائمة "التحويل".
  3. في علامة التبويب إعدادات مُشغّل ACE، استخدم أزرار الأسهم لتعيين ملف تعريف مستخدم ACE الذي أنشأته أعلاه.
  4. قم بإلغاء تعيين ملف التعريف الافتراضي UP-Administrator، إلا في الحالة النادرة التي يطلب فيها حامل البطاقة حقوق المسؤول العام في ACS.
  5. في نفس علامة التبويب إعدادات مُشغّل ACE، استخدم الجزء **تعيين الأشخاص** للبحث عن حامل البطاقة في النظام المرشّح لدور VisMgmt.
  5. انقر على **تعيين أشخاص** لإتمام التخصيص إلى حامل البطاقة المُحدد.
  - يجب تحديد مُشغّل منفصل لكل حامل بطاقة يعمل في إدارة الزائرين. لا يُمكنك تعيين حاملي بطاقات متعددين للمُشغّل ذاته.

## 5.2 إنشاء المصادقات وملفات التعريف للزائرين في ACS

### المقدمة

يحدد موظف الاستقبال أو المسؤول في نظام VisMgmt نوع زائر لكل زائر جديد. يستند نوع الزائر هذا إلى نوع شخص محدد مسبقًا يُسمى الزائر في النظام الرئيسي للتحكم في الوصول (ACS) أو إلى نوع فرعي من الزائر أنشأه مسؤولو نظام التحكم في الوصول. يجب على هؤلاء المسؤولين أيضًا تكوين نوع الشخص الزائر وأنواعه الفرعية في نظام التحكم في الوصول باستخدام ملفات تعريف الوصول. تسمح ملفات تعريف الوصول لأنواع الأشخاص هذه بتشغيل الأبواب الحقيقية في الموقع.

## 5.3 إعداد كمبيوتر موظف الاستقبال

يدير كمبيوتر موظف الاستقبال الوظيفة الإضافية **Bosch Peripheral Devices**، مما يسمح باتصالاته الفعلية بالأجهزة الطرفية لقراءة البطاقات والمسح الضوئي لمستندات الهوية والمسح الضوئي للتوقيعات. قم بتوصيل كل الأجهزة الطرفية المطلوبة قبل تثبيت برنامج العميل. تأكد من وجود حماية كافية من الوصول غير المصرح به لكل من الكمبيوتر وأجهزته الطرفية.

## 5.4 إعداد كمبيوتر كشك للزائرين

### المقدمة

عادةً ما يسجل الزائرون زيارتهم ويقومون بإنشاء ملفات تعريفهم على كمبيوتر مفتوح للوصول إليه في منطقة الاستقبال في الموقع الخاضع للتحكم في الوصول. لأسباب أمنية، يعمل مستعرض الويب في الكمبيوتر في وضع الكشك، وهو ما يسمح فقط بالوصول إلى VisMgmt، وليس إلى عدة علامات تبويب أو إعدادات المستعرض أو نظام تشغيل الكمبيوتر. تقدم كل المستعرضات المدعومة وضع الكشك، لكن تكوينه الدقيق يعتمد على المستعرض. يدير كمبيوتر الكشك الوظيفة الإضافية **Bosch Peripheral Devices**، مما يسمح باتصالاته الفعلية بالأجهزة الطرفية لقراءة البطاقات والمسح الضوئي لمستندات الهوية والمسح الضوئي للتوقيعات.

– عنوان URL لوضع الكشك هو 5706: <My\_VisMgmt\_server>: https://

### تكوين المستعرضات لوضع الكشك

تصف الروابط التالية تكوين وضع الكشك للمتصفحات التي يدعمها VisMgmt

تعليمات وضع الكشك	
https://support.google.com/chrome/a/answer/9273974	Chrome
https://support.mozilla.org/en-US/kb/firefox-enterprise-kiosk-mode	Firefox
https://docs.microsoft.com/en-us/deployedge/microsoft-edge-configure-kiosk-mode	Edge

### إشعار!

لأسباب أمنية، قم دائمًا بتعطيل خيار المستعرض الخاص بحفظ كلمات المرور تلقائيًا.



## 5.5 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 VisMgmt ويليهِ نقطتان ورقم المنفذ (الافتراضي 5706)

https://<My\_VisMgmt\_server>:5706/main

تظهر شاشة تسجيل الدخول

2. قم بتسجيل الدخول كمستخدم VisMgmt مسؤول.



3. انقر فوق لفتح قائمة الإعدادات.

## استخدام قائمة الإعدادات في التكوين

5.6

تمتوي قائمة الإعدادات على أقسام فرعية تتيح لك أداء خطوات التكوين التالية:

<p><b>فترة الاحتفاظ (بالأيام):</b> يحكم هذا الإعداد طريقة التعامل مع سجلات الزيارات.</p> <ul style="list-style-type: none"> <li>- عندما تنتضي الفترة لأول مرة، يقوم التطبيق بتحويل السجل إلى سجل مجهول الهوية.</li> <li>- عندما تنتضي الفترة لثاني مرة، يقوم التطبيق بحذف السجل. القيمة الافتراضية هي 365.</li> <li>قم بتعيين 0 لإلغاء تنشيط فترة الاحتفاظ بالكامل. في هذه الحالة، يتم الاحتفاظ بسجلات الزيارات إلى ما لا نهاية.</li> </ul> <p><b>وضع تخزين المستندات:</b> حدد ما إذا كان سيتم تخزين المستندات بشكل ملفات ورقية أم رقمية.</p> <ul style="list-style-type: none"> <li>- <b>أقصى عدد للزائرين</b> مسموح به على الموقع في المرة الواحدة. القيمة الافتراضية هي 100.</li> <li>قم بتعيين 0 لإلغاء تنشيط عدادات الزائرين على لوحة التحكم بالكامل.</li> </ul> <p><b>فترة انتهاء صلاحية المستند (بالأيام):</b> قم بإدخال مدة استمرار صلاحية المستندات التي تم تحميلها مثل اتفاقيات عدم الإفصاح (NDA) وشروط الاستخدام. تسري المدة على كل من الملفات الورقية والرقمية. بعد هذه المدة، توضع علامة على المستندات باعتبارها منتهية الصلاحية في ملف تعريف الزائر (أيقونة الساعة ذات النقطة الحمراء). القيمة الافتراضية هي 365</p> <ul style="list-style-type: none"> <li>- <b>فترة التحذير من انتهاء صلاحية المستند (بالأيام):</b> قم بإدخال طول فترة التحذير السابقة لتاريخ انتهاء الصلاحية. أثناء فترة التحذير هذه، توضع علامة على المستندات في ملف تعريف الزائر (أيقونة الساعة ذات النقطة البرتقالية). قبل فترة التحذير، تحتوي أيقونة الساعة على نقطة خضراء.</li> </ul> <p><b>الشعار:</b> حدد أو قم بإلغاء تحديد خانات الاختيار التي تحدد ما إذا كانت مربعات الحوار تعرض شعارًا مخصصًا أو الشعار الافتراضي وإما لعرض Bosch supergraphic.</p> <ul style="list-style-type: none"> <li>- لمعايير ملفات الشعار المخصصة، انظر: تخصيص شعار الشركة، الصفحة 32</li> </ul> <ul style="list-style-type: none"> <li>- انقر فوق <b>المعاينة</b> لإظهار صفحة الحوار كما ستظهر وفق هذه الإعدادات. انظر القسم التالي للحصول على المزيد من التفاصيل عن وضع المعاينة.</li> </ul> <p><b>اللغات:</b></p> <ul style="list-style-type: none"> <li>- حدد اللغات التي ستوفر في واجهة المستخدم إلى جانب تنسيقات التاريخ والوقت المفضلة لديها.</li> </ul> <p><b>خادم البريد</b></p> <ul style="list-style-type: none"> <li>- 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/TLS إضافية، فاستوردها إلى الجهاز الذي يقوم بتشغيل الواجهة الخلفية لتطبيق Mobile Access. بعد عملية الاستيراد، يجب إعادة تشغيل VisitorManagerServer.</li> </ul>	<p><b>الإعدادات العامة</b></p>
--	--------------------------------

<p><b>قوالب البريد الإلكتروني</b></p> <p>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 <b>قوالب البريد الإلكتروني</b> أدناه.</p> <p><b>Mobile Access</b></p> <p>حدد خانة الاختيار <b>Mobile Access</b> لتنشيط Mobile Access.</p> <p><b>الاتصال:</b> أدخل عنوان خادم Mobile Access (عنوان خدمة التسجيل).  <a href="https://&lt;MyMobileAccessBackendServer&gt;:5700">https://&lt;MyMobileAccessBackendServer&gt;:5700</a>  استخدم (FQDN) لـ &lt;MyMobileAccessBackendServer&gt; في بيانات متعددة المجالات.</p> <p><b>ملاحظة:</b> لاستخدام عنوان IP بدلاً من FQDN، عليك إدخال عنوان IP ضمن <b>إنشاء الشهادة</b>، عندما تقوم بتشغيل معالج إعداد الواجهة الخلفية لـ Mobile Access.</p> <p><b>إعداد المثبت:</b> حدد المعلومات التي تحتاج إليها من المثبتين، لتمكينهم من تكوين أجهزة قراءة الوصول عبر المحمول باستخدام Bosch Setup Access.</p> <p>سجل خروجك من تطبيق الويب، وسجل دخولك من جديد من أجل استخدام ميزة Mobile Access على الفور.</p>	
<p>تحتوي شاشة الإعدادات هذه على خانتي اختيار لكل حقل بيانات في مربعات حوار تسجيل الزائرين الخاصة بموظف الاستقبال.</p> <ul style="list-style-type: none"> <li>- قم بإلغاء تحديد أول خانة اختيار أو حددها للتحكم فيما إذا كان حقل البيانات <b>ظاهرًا</b> في كل مربعات حوار التسجيل.</li> <li>- قم بإلغاء تحديد خانة الاختيار الثانية (عليها علامة نجمة) أو حددها للتحكم فيما إذا كان حقل البيانات <b>إلزاميًا</b>.</li> <li>- قم بتخصيص نصوص الرؤوس الافتراضية في مربعات حوار جمع البيانات. للحصول على المزيد من التفاصيل، راجع تخصيص واجهة المستخدم، الصفحة 31 أدناه.</li> </ul>	<p><b>موظف الاستقبال</b></p>
<p><b>خيار خاص: تمكين تسجيل الوصول/المغادرة بدون بطاقة</b></p> <p>إذا كان لدى الزائرين مرافقون مقربون، أو إذا كان وجودهم يقتصر على الأماكن العامة، فقد تكون البطاقات الفردية للزائرين غير ضرورية. في مثل هذه الحالات، يوجد خيار لتسجيل وصول الزائرين وتسجيل مغادرتهم بدون بطاقات، لأسباب أمنية، هذا الخيار معطل بشكل افتراضي. حدد خانة الاختيار لتمكينه:</p> <ul style="list-style-type: none"> <li>- <b>ملاحظة:</b> إذا كان الخيار ممكنًا، فإن أي <b>زائر</b> يسجل نفسه في كمبيوتر الكشك يوافق بشكل تلقائي على زيارته الخاصة ويسجل وصوله في اللحظة نفسها.</li> <li>- راجع فصل <b>العملية</b> تسجيل الوصول والمغادرة بدون بطاقة، الصفحة 47 في هذا المستند للحصول على تفاصيل حول كيفية قيام <b>موظف الاستقبال</b> بمعالجة الزائرين بدون بطاقات.</li> </ul>	
<p>تظل إعدادات المستخدمين من نوع <b>المضيف</b> و<b>الزائر</b> للقراءة فقط إلى أن تنتهي من تحرير إعدادات <b>موظف الاستقبال</b> وحفظها.</p> <p>يتم بشكل تلقائي تعيين الحقول التي تضع علامة عليها باعتبارها غير ظاهرة في إعدادات <b>موظف الاستقبال</b> باعتبارها غير ظاهرة بالنسبة إلى <b>المضيف</b> و<b>الزائر</b>. بعد ذلك، يكون إجراء التكوين مماثلًا.</p>	<p><b>المضيف</b></p> <p><b>زائر</b></p>

**راجع**

- تعيين أوراق الاعتماد الفعلية, الصفحة 43
- تخصيص واجهة المستخدم, الصفحة 31

**قوالب البريد الإلكتروني****5.6.1**

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. عند تنزيل نموذج للتمرير، يتم نسخه إلى مجلد التنزيلات الافتراضي في المستعرض لديك.

- MobileAccess.html دعوة لحامل بطاقة لاستخدام بيانات الاعتماد المستندة إلى الهاتف الذكي.
- SetupAccess.html دعوة لأحد المثبتين لتكوين أجهزة القراءة من أجل Mobile Access.
- VisitorInvite.html دعوة لأحد الأشخاص بزيارة موقعك، مع خيار إلحاق ملف iCalendar بالبريد الإلكتروني.
- InformHostAboutCheckin.html بريد إلكتروني لإبلاغ المضيف بوصول الزائر.

**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

العنصر النائب	الوصف
{{InviteLink}}	رابط يوفر الوصول عبر المحمول للمثبت لإعداد أجهزة القراءة عبر تطبيق Setup Access

### دعوة الزائر

بريد إلكتروني يُرسل إلى الزائر عند إنشاء زيارة أو تحريرها.

العنصر النائب	الوصف
{{VisitorID}}	رمز بطاقة هوية الزائر، كما تم إنشاؤه بواسطة تطبيق VisMgmt
{{Title}}	لقب الزائر (السيد / الطيب وغيرهما).
{{FirstName}}	الاسم الأول للزائر
{{LastName}}	لقب الزائر
{{CompanyName}}	شركة الزائر
{{HostFirstName}}	الاسم الأول للمضيف
{{HostLastName}}	لقب المضيف
{{ExpArrivalDate}}	التاريخ المخطط للزيارة

### وصول الزائر

البريد الإلكتروني الذي يتم إرساله إلى المضيف عندما يوافق موظف الاستقبال على زيارة

العنصر النائب	الوصف
{{VisitorID}}	رمز بطاقة هوية الزائر، كما تم إنشاؤه بواسطة تطبيق VisMgmt
{{Title}}	لقب الزائر (السيد / الطيب وغيرهما).
{{FirstName}}	الاسم الأول للزائر
{{LastName}}	لقب الزائر
{{CompanyName}}	شركة الزائر
{{HostFirstName}}	الاسم الأول للمضيف
{{HostLastName}}	لقب المضيف
{{ExpArrivalDate}}	التاريخ المخطط للزيارة
{{ArrivalDate}}	التاريخ الفعلي للزيارة

### بطاقة الزائر

مستند يمكن طباعته وتقديمه للزائر. بإمكان هذا المستند أن يحتوي هذا على خريطة للمبنى أو قائمة اختيار.

العنصر النائب	الوصف
{{VisitorID}}	رمز بطاقة هوية الزائر، كما تم إنشاؤه بواسطة تطبيق VisMgmt
{{Title}}	لقب الزائر (السيد / الطيب وغيرهما).
{{FirstName}}	الاسم الأول للزائر

العنصر النائب	الوصف
{{LastName}}	لقب الزائر
{{CompanyName}}	شركة الزائر
{{HostFirstName}}	الاسم الأول للمضيف
{{HostLastName}}	لقب المضيف
{{ExpArrivalDate}}	التاريخ المخطط للزيارة
{{ArrivalDate}}	التاريخ الفعلي للزيارة

### وضع المعاينة

5.6.2

تقدم مجموعات معينة من الخيارات زر **معاينة** ينشط وضع المعاينة لتيح لك رؤية مربعات الحوار كما ستظهر عند تعيين تلك الخيارات. في وضع المعاينة، تسري الشروط التالية:

- يظهر شعار أعلى لوحة المعلومات.

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

- التغييرات التي تتم في لوحة المعلومات أو القوائم لن تُحفظ.
- انقر فوق **إغلاق وضع المعاينة** داخل الشعار لإغلاق وضع المعاينة
- استخدم قائمة **تغيير الدور** داخل الشعار لمعاينة مظهر الواجهة لأنواع المختلفة من المستخدمين.

### قوالب المستندات

5.6.3

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

### تخصيص واجهة المستخدم

5.7

تخصيص واجهة المستخدم في مربعات حوار **لوحة المعلومات > الإعدادات**

### تكوين الخيارات التي ستكون ظاهرة وغير ظاهرة وإلزامية

5.7.1

حدد حقول البيانات التي ستكون ظاهرة في مربعات الحوار والبيانات التي تعتبر إلزامية. مثال:

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

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

### تخصيص نصوص واجهة المستخدم للتطويع اللغوي

5.7.2

يمكنك بسهولة تخصيص نصوص واجهة المستخدم على أساس كل لغة. في الوضع الافتراضي، يحتوي **نص التطويع اللغوي** على العناوين القياسية لكل 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>`

Localization text

General information

Locale

EN ▾

### تخصيص وضع الكشك

5.7.3

إذا كان موقعك لا يحتوي على جهاز أو اثنين من الأجهزة الطرفية، مثل ماسح ضوئي للمستندات، يمكنك تخصيص عملية التسجيل الذاتي للزائرين في وضع الكشك عن طريق إلغاء تحديد مربعات الاختيار الخاصة بخطوات التسجيل المقابلة.

### تخصيص شعار الشركة

5.7.4

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

## إعدادات جدار الحماية

5.8

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 ومنفذ محلية محددة
7. اسم 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

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

## إشعار!

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



## البرامج والخدمات كاستثناءات جدار الحماية

## 5.8.1

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

مكان الملف	البرنامج
AccessEngine\AC\BIN\[Install-path]	acsp.exe
AccessEngine\AC\BIN\[Install-path]	ACTA-3.exe
AccessEngine\AC\BIN\[Install-path]	BioVerify.exe
AccessEngine\AC\BIN\[Install-path]	Bioidentify.exe
Bosch Credential Management\[Install-path]	Bosch.Ace.CredentialManagement.exe
Bosch Mobile Access\[Install-path]	Bosch.Access.MobileAccessBackend.exe
Bosch Visitor Management\[Install-path]	Bosch.Ace.VisitorManagement.exe
AccessEngine\AC\BIN\[Install-path]	CaTa-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\MAC\BIN\[install-path]	DMS.exe
AccessEngine\MAC\BIN\[install-path]	lac.exe

#### الخدمات

مسار التثبيت الافتراضي هو : C

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

مكان الملف	الخدمة
States API\[install-path]	Bosch.States.Api
Map API\[install-path]	Bosch.Map.Api
Map View API\[install-path]	Bosch.MapView.Api

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

## واجهة برمجة التطبيقات (API) لتطبيق Mobile Access

## 5.8.2

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 Visitor Management و Credential Management المنفذ 5701.

يتضمن كل من Credential Management و Visitor 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 بالعمل، 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 بالعمل، 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 العمل إلى حد بعيد.

إذا كان العميل يجري التحديث من إصدار سابق إلى الإصدار الأحدث من AMS، فيجب تعديل إعدادات Credential Management و Visitor Management. يمكن لدور المسؤول في Visitor Management و Credential 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.

## أمان تكنولوجيا المعلومات

### 5.9

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

### مسؤوليات الأجهزة

#### 5.9.1

- 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.

### مسؤوليات البرامج

#### 5.9.2

- صيانة جدار حماية شبكة التحكم في الوصول وتحديثه وتشغيله بشكل ملائم.
- مراقبة الإنذارات التي تشير إلى وقت توقف تشغيل مكونات الأجهزة مثل قارئ 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 والقارئ 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 تحديثاً لبرنامج المصنع. راجع دليل الأجهزة للحصول على الإرشادات.
- لا تتحمل Bosch المسؤولية عن الأضرار الناتجة عن المنتجات الجاري تشغيلها باستخدام برمجيات مصنع متقدمة.
- 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.

### التعامل الآمن مع بيانات اعتماد المحمول

#### 5.9.3

- 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 يُمكن هاتف المثبت المسروق، مع بيانات اعتماد المثبت 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.

## النسخ الاحتياطي للنظام

## 5.10

VisMgmt عبارة عن تطبيق ويب مساعد لنظام رئيسي للتحكم في الوصول. راجع مستندات النظام الرئيسي للتحكم في الوصول المتعلق بالنسخ الاحتياطي لقواعد بيانات النظام.

## التشغيل

### نظرة عامة على أدوار المستخدمين

6

6.1

حالات الاستخدام	نوع المستخدم
تسجيل الزيارات الجديدة والزائرين اعتماد الزيارات ورفضها إدراج زائرين في القائمة المحظورة تعيين بطاقات الزائرين وإلغاء تعيينها إدارة المستندات المرتبطة مراقبة عدد الزائرين على الموقع	موظف الاستقبال
التسجيل الذاتي والمسبق إنشاء ملف تعريف للزائر والحفاظ عليه توقيع المستندات	زائر
إدارة الجداول الزمنية وقوائم الزيارات والزائرين التسجيل المسبق للزيارات	المستضيف
عمل إعدادات عامة تخصيص سلوك الأداة وواجهة المستخدم بها علاوة على: جميع حالات الاستخدام الخاصة بموظف الاستقبال	مسؤول

### استخدام لوحة المعلومات

6.2

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

#### نظرة عامة وعوامل التصفية السريعة

يحتوي الجزء العلوي من لوحة المعلومات على نظرة عامة سريعة على زيارات اليوم. يتيح هذا للمستخدم أن يراقب بسهولة عدد الزائرين على الموقع.

**الزائرون المتوقعون**    **الزائرون الذين سجلوا**    **ما زال على الزائرين أن الزائرون الذين تأخروا**  
**اليوم: %**    **الوصول في: %**    **يسجلوا المغادرة اليوم عن موعد المغادرة**

```
<current count> > <current count> > <current count> > <current count> >
</ <total capacity </ <total capacity
```

انقر فوق أي رؤوس لتصفية جدول الزيارات وفقاً لمعنى الرأس. على سبيل المثال، انقر فوق **الزائرون الذين سجلوا الوصول** لترى فقط الزائرين الذين تم تعيين بطاقة لهم. قيمة `<total capacity>` هي عبارة عن إعداد تكوين يحدده مسؤول النظام. راجع استخدام قائمة الإعدادات في التكوين، الصفحة 27.

#### نظرة عامة على صفحة الشخص

6.2.1

في لوحة المعلومات، انقر فوق اسم شخص معين، وسيفتح مربع حوار يحتوي على بيانات شخصية. تظهر البيانات. في النظرة العامة على صفحة الشخص هذا، هناك أربعة أقسام لحقول البيانات الشخصية:

- صورة الهوية
- مستند الهوية
- معلومات عامة
- المستندات

#### جدول الزيارات

6.2.2

يمثل كل صف في الجدول موعداً لزيارة.

- يمكنك فرز الجدول حسب أي من أعمدته عن طريق النقر فوق رأس العمود.

- يمكنك تحديد زيارات فردية أو عدة زيارات في وقت واحد، 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 زيارات جديدة إلى الجدول
- يمكنك معالجة تفاصيل الزيارات والزائرين عن طريق النقر فوق أزرار الإجراءات
  - الموافقة على الزيارة
  - رفض الزيارة
  - تعيين بطاقات للزائر
  - تحرير تفاصيل الزيارة والزائرين
- 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.

يؤدي شريط الأدوات الأفقي الوظائف التالية:

الوظيفة	التسمية
إجمالي عدد الزيارات (N) (كل زيارة عبارة عن صف في الجدول).	1 N من الإدخالات
ابحث عن نص اعتباطي في الزيارات في الجدول	2 بحث
اعرض الزيارات التي تمت إضافتها مؤخرًا إلى الجدول.	3 L
افتح مربع حوار لتحديد معايير التصفية	4 Y
أعد ضبط الجدول على عرضه الافتراضي واسترجع كل عوامل التصفية.	5 ↶
افتح مربع حوار لإلغاء تعيين بطاقات تم تعيينها باستخدام قارئ تسجيل متصل.	6 إلغاء تعيين بطاقة
افتح مربع حوار لإنشاء إدخال لزيارة جديدة في الجدول	7 +
انقر فوق رمز علامة القطع في قائمة لتصدير الزيارات التي تمت تصفيتها حاليًا، بالإضافة إلى المستندات، إلى تنسيقات ملفات متنوعة، على سبيل المثال، CSV و XLSX. لأسباب تتعلق بأمان البيانات، لا يمكنك التصدير إلا إذا كان عميلك يعمل في اتصال HTTPS آمن، مع شهادة.	...

## أعمدة الجدول وإجراءاته الأعمدة

### 6.2.3

العمود	القيمة	الوصف
الحالة	 هناك زيارة متوقعة  تم اعتماد الزيارة  تم رفض الزيارة  تم تعيين البطاقة  البطاقة منتهية الصلاحية  انتهت الزيارة (لم يعد الزائر يحمل بطاقات وقد غادر المقر)	أيقونة تعكس حالة الزيارة
الاسم	اسم الزائر على شكل ارتباط تشعبي	انقر فوق الارتباط التشعبي لعرض تفاصيل الزائر وزيارته الحالية.
الوصول المتوقع	التاريخ والوقت	التاريخ والوقت المتوقعان لوصول الزائر
المغادرة المتوقعة	التاريخ والوقت	التاريخ والوقت المتوقعان لمغادرة الزائر
الذين سجلوا الوصول	التاريخ والوقت	تاريخ ووقت تعيين أول بطاقة للزائر.
الذين سجلوا المغادرة	التاريخ والوقت	تاريخ ووقت إلغاء تعيين آخر بطاقة من الزائر.
أرقام البطاقات	رقمي	أرقام البطاقات المعينة لهذا الزائر.
الإجراءات	الأيقونات	انظر الجدول المنفصل أدناه

## الإجراءات

الوظيفة	الأيقونة
اعتمد الزيارة. ملاحظة: لا يمكن تعيين بطاقة لزائرين على قائمة الحظر. قم أولاً بإزالة الزائر من قائمة الحظر أو إعفائه منها مؤقتاً. راجع الإضافة إلى القائمة المحظورة والإزالة والإعفاء منها، الصفحة 48	
ارفض الزيارة. تم إلغاء تنشيط هذا الزر بعد تسجيل وصول الزائر، أي عندما كانت لديه بطاقة بالفعل.	
تعيين بطاقة واحدة أو أكثر للزائر	
تحرير حدث الزيارة و/أو بيانات اعتماد الزائرين	

## موظف الاستقبال

6.3

## تسجيل الدخول إلى دور موظف الاستقبال

6.3.1

1. في مستعرضك، افتح [https://<My\\_VisMgmt\\_server>:5706/main](https://<My_VisMgmt_server>:5706/main) لشاشة تسجيل الدخول.
2. قم بإدخال اسم المستخدم لحساب لديه الحقوق المطلوبة لدورك.
3. أدرج كلمة المرور.
4. انقر فوق تسجيل الدخول.

## البحث في الزيارات وتصفيتها

6.3.2

في لوحة معلومات VisMgmt في شريط الأدوات فوق جدول الزيارات.

## بحث

للبحث في الأسماء والمستضيفين، قم بإدخال نص من الحروف والأرقام في مربع البحث واضغط على زر الإدخال.

## التصفية

- لترى الزيارات الأقرب إلى الوقت الحالي، انقر فوق **الأحدث**
- لبناء عامل تصفية مركب من حالة الزيارة وتواريخ تسجيل الوصول وتسجيل المغادرة وأرقام البطاقات، انقر فوق **عامل التصفية**.
- أدخل معايير التصفية المرغوب فيها في مربع الحوار المنبثق
- انقر فوق **تطبيق**
- يختصر النظام جدول الزيارات ليقصر على مواعيد الزيارات التي تحقق معايير عامل التصفية.
- لحذف كل معايير التصفية، انقر فوق **إعادة تعيين**

## تسجيل الزيارات

6.3.3

## المقدمة

يتبع موظف الاستقبال سيناريو هين أساسيين لتسجيل الزيارات:

- **أ:** عندما يستخدم أحد الزائرين كشك الزائرين لإنشاء معرف الزائر الخاص به وتحميل المستندات، لا يحتاج موظف الاستقبال إلا لإكمال أي معلومات وتوقيعات مطلوبة وما زالت مفقودة وتعيين بطاقة للزائر.

- **ب:** عندما يتجاوز أحد الزائرين كشك الزائرين ويتجه إلى مكتب الاستقبال مباشرةً، يستطيع موظف الاستقبال أن يسجل الزيارة من البداية: يجمع المعلومات المطلوبة ويجمع التوقيعات للمستندات المطلوبة ويعين بطاقة للزائر.
- السيناريو أ عبارة عن مجموعة فرعية من السيناريو ب، ولذلك فإن السيناريو الكامل ب مذكور هنا.
- استخدام وضع الكشك بواسطة أحد الزائرين مذكور في القسم الخاص به. راجع مقدمة إلى وضع الكشك، الصفحة 51.

### الإجراء

في لوحة معلومات VisMgmt في شريط الأدوات فوق جدول الزيارات.



1. انقر فوق **+** لإضافة موعد زيارة إلى جدول الزيارات.
2. في مربع حوار **البيانات الشخصية** قم بإدخال البيانات التي يحتاج إليها موقعك من الزائرين. الحقول الإلزامية عليها علامة نجمة (\*).
- يمكنك إدخال البيانات يدويًا، لكن بسرعة ودقة أكبر من خلال الماسحة الضوئية للمستندات إذا كانت متاحة على محطة عمل موظف الاستقبال. انظر الأجهزة الطرفية، الصفحة 22 للاطلاع على تفاصيل بشأن الأجهزة الطرفية المدعومة.

### معلومات عامة

- حدد موقع ملف تعريف كامل للزائر تم إنشاؤه في زيارة سابقة وحمله. لتحديد موقع ملفات



- التعرف، انقر فوق أيقونة (البحث) الموجودة في حقل **الاسم الأخير\***.
- عند إنشاء ملف تعريف زائر، يتلقى رمزًا فريدًا يتكون من حروف وأرقام، وينبغي على الزائر أن يحفظه بعناية لتسريع عملية التسجيل للزيارات المستقبلية.
- بخلاف ذلك، قم بإدخال البيانات باليد.

### صور بطاقة الهوية

- **حمل** صورة من نظام الملفات.
- **التقط** صور الزائر من كاميرا ويب متصلة.
- **مستندات الهوية**
- انقر فوق **مسح المستند ضوئيًا** لقراءة البيانات من ماسحة مستندات ضوئية (إذا كانت متاحة) وأكمل حقول البيانات ذات الصلة في مربع الحوار.
- بخلاف ذلك، أدخل النص باليد، إذا كان النظام لديك لا يحتوي على ماسحة مستندات ضوئية.

### المستندات القانونية

- حمل المستندات التي وقعها الزائر إلكترونيًا في الكشك.
- إذا كان النظام لديك لا يحتوي على كشك زائرين، فاطبع مستندات PDF المطلوبة المخزنة على نظام الملفات وقم بتقديمها (بتوقيع الزائر).
- 3. انقر فوق **التالي** للمتابعة إلى مربع حوار **الزيارات**.
- 4. في مربع حوار **الزيارات** في جزء **الزيارة الحالية** أدخل البيانات التي يتطلبها موقعك. الحقول الإلزامية عليها علامة نجمة (\*).

### حدد نوع زائر.

إنه نوع **زائر** (افتراضي) أو فئة فرعية مخصصة من **الزائر**، ويتم تعريفه باعتباره **نوع شخص** في النظام الرئيسي للتحكم في الوصول.

حدد اسم الموظف الذي يجب زيارته ضمن **المضيف**.

- لاحظ أنك لا تستطيع تحديد إلا حاملي بطاقات النظام الرئيسي للتحكم في الوصول.
- يعرض تلميح أدوات عنوان البريد الإلكتروني للشخص كعامل مساعد في تحديد الهوية.
- إذا كان الزائر يحتاج إلى مرافق عبر المقر، فحدد اسم الموظف المرافق تحت **المرافق**.
- لاحظ أنك لا تستطيع تحديد إلا حاملي بطاقات النظام الرئيسي للتحكم في الوصول.
- يعرض تلميح أدوات عنوان البريد الإلكتروني للشخص كعامل مساعد في تحديد الهوية.
- إذا كان الزائر بحاجة إلى وقت إضافي ليمر عبر باب، فحدد مربع الاختيار **الوقت الممتد لفتح الباب**.
- 5. انقر فوق **حفظ**.

لاحظ أنك لن تتمكن من حفظ البيانات قبل أن تكمل كل الحقول الإلزامية.

## راجع

- الأجهزة الطرفية, الصفحة 22

## اعتماد الزيارات ورفضها

## 6.3.4

## الواجهة الخلفية: الموافقة على البطاقات الفعلية

يجب أن توافق على الزيارة قبل أن تتمكن من تخصيص بطاقات للزائر.

## الواجهة الخلفية: الموافقة على بيانات اعتماد الهاتف المحمول

يمكنك إنشاء بيانات اعتماد الهاتف المحمول ومشاركتها في يوم الزيارة، بشكل مشابه لتعيين بطاقة فعلية.

- **ملاحظة:** لن تعمل بيانات اعتماد الهاتف المحمول حتى توافق على الزيارة.
- بدلاً من ذلك، يمكنك إنشاء بيانات اعتماد الهاتف المحمول ومشاركتها مسبقًا. اعتمد الزيارة، كما هو موضع أدناه، لتفعيل بيانات الاعتماد أخيرًا وذلك عند وصول الزائر إلى مكتب الاستقبال.
- **ملاحظة:** لن تعمل بيانات اعتماد الهاتف المحمول حتى توافق على الزيارة.
- سيتم تطبيق ذلك الوقت إذا كنت قد حددت موعد مغادرة متوقع للزيارة.
- إذا لم تقم بتعيين وقت مغادرة متوقع، فسيتم تطبيق عدد ساعات افتراضي (8). يمكن للمسؤولين تغيير هذا الإعداد الافتراضي في قائمة الإعدادات.

## إجراءات الموافقة والرفض

هناك مكانان لاعتماد زيارة أو رفضها:

- في جدول الزيارات في لوحة المعلومات
- في محرر الزيارة

## في جدول الزيارات في لوحة المعلومات:

- **الاعتماد:** في جدول الزيارات، حدد سطرًا من الجدول وانقر فوق . بعد نافذة منبثقة للتأكيد، تتحول الأيقونة إلى اللون الرمادي لتبين أن الزيارة معتمدة.

- **الرفض:** في جدول الزيارات، حدد سطرًا من الجدول وانقر فوق . بعد نافذة منبثقة للتأكيد، تعود أيقونة الاعتماد إلى اللون الأزرق لتبين أن الزيارة ما زالت بحاجة إلى اعتماد.

## في محرر الزيارة:

1. في لوحة المعلومات، وفي جدول الزيارات، حدد سطرًا من الجدول وانقر فوق  لتحرير الزيارة.
2. في مربع حوار البيانات الشخصية انقر فوق التالي.
3. في مربع حوار الزيارات، انقر فوق زر اعتماد أو رفض.
4. أكد إجراءك في النافذة المنبثقة.

## تعيين أوراق الاعتماد الفعلية

## 6.3.5

## المقدمة

قم بتعيين بطاقة زائر لكل زائر تسمح له بدخول المقر. يمكنك تعيين عدة بطاقات لزائر واحد إذا كان مطلوبًا.

- تاريخ ووقت الزيارة التي سجلت الوصول هو وقت تعيين أول بطاقة.
- تاريخ ووقت الزيارة التي سجلت المغادرة هو وقت إلغاء تعيين آخر بطاقة ما زالت معينة للزائر.

يستطيع موظف الاستقبال أن يعين البطاقة ويُلغِي تعيينها بسهولة من لوحة المعلومات إذا تم توصيل قارئ بطاقات تسجيل بكمبيوتر موظف الاستقبال.  
ومع ذلك، يقدم محرر الزيارات طريقة لتعيين أرقام البطاقات إذا لم يكن هناك قارئ متاح.

### إشعار!

لا يستطيع الأشخاص على قائمة الحظر تلقي بطاقات لا يمكن تعيين بطاقات لزائرين ليسوا على قائمة الحظر. قم بإزالة الزائر من قائمة الحظر أو إنشاء إعفاء مؤقت للزائر قبل محاولة تعيين بطاقة.



### تعيين بطاقة من لوحة المعلومات (يتطلب قارئ تسجيل)

1. قم بتجهيز بطاقة زائر فعلية لتقديمها إلى قارئ التسجيل.
2. في جدول الزيارات، وافق على الزيارة. راجع اعتماد الزيارات ورفضها، الصفحة 43



3. حدد صف الزيارة وانقر فوق
4. اتبع الإرشادات التي تظهر في النافذة المنبثقة لاستخدام قارئ التسجيل.

### 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.

### تعيين بطاقة في محرر الزيارة



1. في لوحة المعلومات، وفي جدول الزيارات، حدد سطرًا من الجدول وانقر فوق لتحرير تلك الزيارة.
2. في مربع حوار **البيانات الشخصية**، انقر فوق **التالي**.
3. في مربع حوار **الزيارات**، إذا لم تكن الموافقة على الزيارة قد تمت بعد، فانقر فوق **موافقة**.
4. إذا كان لديك قارئ تسجيل متصل، فانقر فوق **قراءة البطاقة** واتبع الإرشادات التي تظهر في النافذة المنبثقة لاستخدام قارئ التسجيل.
- وإلا، فانقر فوق **إظهار البطاقات الحرة** لعرض قائمة ببطاقات الزائرين التي لا تزال متوفرة. بدلاً من ذلك، إذا كان لديك بطاقات فعلية لم يتم فرزها وتحمل أرقامًا، فحدد أي بطاقة واستخدم أداة **البحث** للعثور على رقمها بسرعة في القائمة.
- انقر فوق بجوار رقم بطاقة لتعيين تلك البطاقة للزائر الحالي.
- كرر الخطوات الأخيرة لتعيين المزيد من البطاقات، إذا كان ذلك مطلوبًا.
5. انقر فوق **حفظ** لحفظ الزيارة الحالية مع تعيينات البطاقات.



### إلغاء تعيين بطاقة في محرر الزيارة



1. في لوحة المعلومات، وفي جدول الزيارات، حدد سطرًا من الجدول وانقر فوق لتحرير تلك الزيارة.
2. في مربع حوار **البيانات الشخصية**، انقر فوق **التالي**.

3. في مربع حوار **الزيارات**، وفي جزء بطاقات الزائرين، انقر فوق  بجوار البطاقة التي تريد إلغاء تعيينها، وأكد إجراءك في النافذة المنبثقة.
4. كرر هذه الخطوة إلى أن تلغي تعيين كل البطاقات التي تريد إلغاء تعيينها.
5. انقر فوق **حفظ** لحفظ الزيارة المالية مع تعيينات البطاقات.
- عندما تلغي تعيين آخر بطاقة تم تعيينها للزائر، يسجل النظام هذا التاريخ والوقت باعتباره وقت تسجيل مغادرة الزائر.



في جدول الزيارات، تصبح حالة سجل الزيارة هذا

### راجع

- استخدام قائمة الإعدادات في التكوين، الصفحة 27
- تسجيل الزيارات، الصفحة 41
- اعتماد الزيارات ورفضها، الصفحة 43

## تعيين بيانات اعتماد المحمول

### 6.3.6

#### 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 ضوئياً باستخدام تطبيق Mobile Access على جهازه المحمول

- لكي تعمل بيانات الاعتماد، يجب عليك **الموافقة** على الزيارة.

للتعليمات، راجع القسم اعتماد الزيارات ورفضها، الصفحة 43

- 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، الصفحة 43
- 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، الصفحة 43
  - 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، الصفحة 43
  - يعمل الجهاز المحمول مثل بطاقة الوصول الفعلية، طالما كان التطبيق قيد التشغيل،

### راجع

- تثبيت Mobile Access، الصفحة 16
- تثبيت تطبيقات Mobile Access، الصفحة 15

### إلغاء تعيين بيانات الاعتماد

### 6.3.7

#### 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.
3. كرر هذه الخطوة إلى أن تلغي تعيين كل البطاقات التي تريد إلغاء تعيينها.
3. انقر فوق **حفظ** لحفظ الزيارة المالية مع تعيينات البطاقات.

### تسجيل الوصول والمغادرة بدون بطاقة

### 6.3.8

#### المقدمة

إذا كان لدى الزائرين مرافقون مقربون، أو إذا كان وجودهم يقتصر على الأماكن العامة، فقد تكون عندئذٍ البطاقات الفردية للزائرين غير ضرورية. في مثل هذه الحالات، يوجد خيار لتسجيل وصول الزائرين وتسجيل مغادرتهم بدون بطاقات، لأسباب أمنية، هذا الخيار معطل بشكل افتراضي.

#### الشرط الأساسي.

قام مسؤول النظام بتمكين الخيار الخاص **تسجيل الوصول/المغادرة بدون بطاقة** في مربع الحوار **الإعدادات < موظف الاستقبال > الزائرون**. يمكنك مراجعة فصل التكوين استخدام قائمة الإعداد في التكوين، الصفحة 27 للحصول على الإرشادات.

#### العملية

- عند تمكين الخيار، يحدث ما يلي:
- أي زائر يسجل نفسه في كمبيوتر الكشك يوافق بشكل تلقائي على الزيارة ويسجل وصوله في الوقت نفسه.
  - يضبط النظام تاريخ ووقت تسجيل الوصول على لحظة التسجيل.
  - يظهر زر التبديل **تسجيل الوصول/المغادرة بدون بطاقة** في محرر الزيارة ولوحة المعلومات للزيارة نفسها.

#### الإجراء: تسجيل وصول زائر بدون بطاقة

إذا لم يتمكن الزائر من تسجيل نفسه في الكشك، ولكن عليه أن يسجل وصوله بدون بطاقة:

1. سجل الزيارة يدويًا، كما هو موضح في الفصل تسجيل الزيارات، الصفحة 41



2. في لوحة المعلومات، في جدول الزيارات، انقر فوق اسم الزائر في الجدول أو انقر فوق **لتحرير** تلك الزيارة.
3. في مربع حوار **البيانات الشخصية**، انقر فوق **التالي**.
4. في مربع حوار **الزيارات**، في جزء **بطاقات الزائرين**، انقر فوق **تسجيل الوصول بدون بطاقة**

#### الإجراء: تسجيل مغادرة زائر بدون بطاقة

إذا غادر زائر بدون بطاقة المقر:



1. في لوحة المعلومات، في جدول الزيارات، انقر فوق اسم الزائر في الجدول أو انقر فوق لتحرير تلك الزيارة.
2. في مربع حوار **البيانات الشخصية**، انقر فوق **التالي**.
3. في مربع حوار **الزيارات**، في جزء **بطاقات الزائرين**، انقر فوق **تسجيل المغادرة بدون بطاقة**.

### راجع

- تسجيل الزيارات، الصفحة 41

## 6.3.9

### الإضافة إلى القائمة المحظورة والإزالة والإعفاء منها

يمكن وضع الزائرين الذين ليسوا محل ترحيب في الموقع على قائمة محظورة. طالما أن الزائر ليس على قائمة محظورة، لا يمكنك تعيين بطاقة لذلك الشخص. يمكنك إزالة الزائر من القائمة المحظورة في أي وقت أو منحه إعفاء مؤقتاً لكي تعين بطاقة.

### الإدراج بالقائمة السوداء



1. في لوحة المعلومات، وفي جدول الزيارات، حدد سطرًا من الجدول وانقر فوق لتحرير زيارة.
2. في مربع حوار **البيانات الشخصية** انقر فوق **القائمة المحظورة**.
3. في النافذ المنبثقة، قم بتأكيد أنك تريد فعلاً وضع هذا الشخص على القائمة المحظورة.
4. في النافذة المنبثقة التالية، قم بإدخال سبب للإضافة إلى القائمة المحظورة والتأكيد.

**Blacklisted**

- يظهر زران تحت الشعار: أحدهما لإزالة الزائر من القائمة المحظورة وأحدهما لمنع إعفاء مؤقت.
- في جدول الزيارات، يظهر اسم كل زائر على القائمة المحظورة مع مثلث تحذير. على سبيل المثال:

**Yadira Hamill**

### الإزالة والإعفاء

1. في لوحة المعلومات، وفي جدول الزيارات، حدد سطرًا من الجدول حيث توجد علامة الإدراج على



- القائمة المحظورة وانقر فوق لتحرير الزيارة.
2. في مربع حوار **البيانات الشخصية** انقر فوق **التالي**:
- **إزالة** لإزالة الزائر من قائمة الحظر بشكل نهائي.
- **إعفاء** للإبقاء على الزائر على قائمة الحظر مع السماح بتعيين بطاقة لهذه الزيارة فقط.
3. أكد إجراءك في النافذة المنبثقة.

## 6.3.10 الحفاظ على ملفات تعريف الزائرين

## 6.3.10

يحفظ النظام بملفات تعريف الزائرين إلى أن يحذفها الزائرون أنفسهم أو موظفو الاستقبال أو المسؤولون.

بعد فترة احتفاظ محددة في إعدادات النظام (القيمة الافتراضية 12 شهرًا)، يحذف النظام سجلات الزيارة. عندما يبتكر زائر أو موظف استقبال ملف تعريف زائر جديد، يتلقى ملف التعريف رمزًا فريدًا من حروف وأرقام. يستطيع الزائرون تسجيل الدخول باستخدام هذا الرمز عند كشك الزائرين وبذلك يحصلون على إمكانية الوصول للحفاظ على ملفات تعريفهم.



### إشعاراً!

حماية معرفات الزائرين  
قم بحماية معرفات الزائرين بعناية من الوصول غير المصرح به لأنها توفر إمكانية الوصول إلى البيانات الشخصية.

## عرض سجلات الزيارات

6.3.11



- لتحرير تلك
1. في لوحة المعلومات، وفي جدول الزيارات، حدد سطرًا من الجدول وانقر فوق الزيارة.
  2. في مربع حوار البيانات الشخصية انقر فوق التالي
  3. في مربع حوار الزيارة الحالية، انقر فوق إظهار كل الزيارات  
يعرض مربع حوار الزيارة الحالية قائمة بالزيارات السابقة.

## المستضيف

6.4

المستضيفون موظفون يتلقون الزيارات. يمكنهم تسجيل مواعيدهم وتصفح النظام للاطلاع على تفاصيل الزائرين وسجلات زيارتهم: السابقة والحالية والمستقبلية.

### تسجيل الدخول إلى دور المستضيف

6.4.1

1. في مستعرضك، افتح [https://<My\\_VisMgmt\\_server>:5706/main](https://<My_VisMgmt_server>:5706/main) لشاشة تسجيل الدخول.
2. قم بإدخال اسم المستخدم لحساب لديه الحقوق المطلوبة لدورك.
3. راجع مسؤول النظام لديك إذا لم يكن لديك حساب.
3. أدخل كلمة المرور.
4. انقر فوق تسجيل الدخول.

### البحث والتصفية

6.4.2



يحتوي شريط أدوات لوحة المعلومات المستضيفة على الوظائف التالية:

الوظيفة	التسمية
إجمالي عدد الزيارات (N) (كل زيارة عبارة عن صف في الجدول).	1 N من الإدخالات
ابحث عن نص اعتباطي في الزيارات في الجدول	2 بحث
اعرض الزيارات التي تمت إضافتها مؤخرًا إلى الجدول.	3 L
افتح مربع حوار لتحديد معايير التصفية	4 Y

التسمية	الوظيفة
	أعد ضبط الجدول على عرضه الافتراضي واسترجع كل عوامل التصفية.
	افتح مربع حوار لإنشاء إدخال لزيارة جديدة في الجدول

### بحث

للبحث في الأسماء والمستضيفين، قم بإدخال نص من الحروف والأرقام في مربع البحث واضغط على زر الإدخال.

### التصفية

- لترى الزيارات الأقرب إلى الوقت الحالي، انقر فوق **الأحدث**
- لبناء عامل تصفية مركب من حالة الزيارة وتواريخ تسجيل الوصول وتسجيل المغادرة وأرقام البطاقات، انقر فوق **عامل التصفية**.
- أدخل معايير التصفية المرغوب فيها في مربع الموارد المنبثق
- انقر فوق **تطبيق**
- يختصر النظام جدول الزيارات ليقصر على مواعيد الزيارات التي تحقق معايير عامل التصفية.
- لحذف كل معايير التصفية، انقر فوق **إعادة تعيين**

## تسجيل الزيارات

### 6.4.3

لتسجيل موعد زيارة من زائر لأول مرة:  
في لوحة معلومات VisMgmt في شريط الأدوات فوق جدول الزيارات.



1. انقر فوق  لإضافة صف إلى جدول الزيارات.
  2. في مربع حوار **البيانات الشخصية** وفي قسم **المعلومات العامة** قم بإدخال البيانات التي يتطلبها موقعك من الزائرين.
  3. في قسم **تفاصيل الزيارة** أدخل التفاصيل المطلوبة، وهي عادة الوقتان المتوقعان للوصول والمغادرة، إلى جانب سبب الزيارة.
  4. انقر فوق **حفظ** لحفظ موعد الزيارة.
- تظهر الزيارة على لوحة المعلومات على شكل سطر في جدول الزيارات.

## نسخ مواعيد الزيارات

### 6.4.4

لجدولة موعد آخر مع الزائر نفسه  
1. اعثر في لوحة معلومات VisMgmt على موعد قائم مع الزائر نفسه في جدول الزيارات.



2. انقر فوق أيقونة  الأصغر في نهاية الصف.
  3. في مربع حوار **البيانات الشخصية** وفي قسم **تفاصيل الزيارة** أدخل التفاصيل المطلوبة، وهي عادة الوقتان المتوقعان للوصول والمغادرة، إلى جانب سبب الزيارة.
  4. انقر فوق **حفظ** لحفظ موعد الزيارة.
- تظهر الزيارة على لوحة المعلومات على شكل سطر في جدول الزيارات.

## 6.5 زائر

يستطيع الزائرون استخدام النظام في وضع الكشك في المقر لإنشاء ملفات تعريفهم والتوقيع على المستندات المطلوبة قبل الانتقال إلى الاستقبال للحصول على بطاقات الزائرين الخاصة بهم.

### 6.5.1 مقدمة إلى وضع الكشك

عادةً ما يسجل الزائرون زيارتهم ويقومون بإنشاء ملفات تعريفهم على كمبيوتر مفتوح للوصول إليه في منطقة الاستقبال في الموقع الخاضع للتحكم في الوصول. لأسباب أمنية، يعمل مستعرض الويب في الكمبيوتر في وضع الكشك، وهو ما يسمح فقط بالوصول إلى VisMgmt، وليس إلى عدة علامات تبويب أو إعدادات المستعرض أو نظام تشغيل الكمبيوتر. تقدم كل المستعرضات المدعومة وضع الكشك، لكن تكوينه الدقيق يعتمد على المستعرض.

يدير كمبيوتر الكشك الوظيفة الإضافية **Bosch Peripheral Devices**، مما يسمح باتصالاته الفعلية بالأجهزة الطرفية لقراءة البطاقات والمسح الضوئي لمستندات الهوية والمسح الضوئي للتوقيعات.

- عنوان URL لوضع الكشك هو `https://<My_VisMgmt_server>:5706`
- في المقابل، عنوان URL لتسجيل الدخول كمسؤول أو موظف استقبال أو مستضيف هو `https://<My_VisMgmt_server>:5706/main`

### 6.5.2 إنشاء ملف تعريف لزائر: تسجيل الوصول الذاتي

#### الزائرون لأول مرة

لاحظ أن الإجراء الدقيق يعتمد على الأجهزة الطرفية المتوفرة لكمبيوتر الكشك، مثل المساحات الضوئية للمستندات والتوقيعات وكاميرات التصوير.

1. في شاشة الترحيب في كمبيوتر الكشك، انقر فوق **المتابعة من دون معرف الزائر**.
2. في الشاشة التالية، انقر فوق **تسجيل الوصول الذاتي**.
3. في الشاشة التالية، حدد **المسح الضوئي للمستند**.
4. اتبع التعليمات التي تظهر على الشاشة لمعرفة المتطلبات الخاصة بالموقع، مثل:
  - المسح الضوئي لمستندات الهوية،
  - التوقيع على أي مستندات قانونية أخرى مطلوبة،
  - التقاط صورة فوتوغرافية.
5. يعرض النظام المعلومات التي تم جمعها لك لكي تصححها وتكملها.
6. يسأل النظام عما إذا كنت ستفرض مصادقات خاصة على الوصول ويبلغ مكتب الاستقبال بهذا عند الحاجة.
7. في نهاية عملية تسجيل الوصول، تعرض الشاشة معرف زائر متفردًا. خذ هذا المعرف إلى مكتب الاستقبال لتتلقى بطاقتك كزائر.

#### إشعار!

معرف الزائر المتفرد الخاص بك

اكتب معرفك كزائر بعناية وقم بحمايته من الاستخدام غير المصرح به. إنه يمنح إمكانية الوصول إلى ملف تعريفك كزائر. يمكنك استخدامه لتسجيل الدخول على كمبيوتر الكشك مما يؤدي إلى تسريع عملية تسجيل وصولك التالية.



#### الزائرون المتكررون

1. قم بتسجيل الدخول من الكشك باستخدام معرفك المتفرد كزائر.
2. يعرض النظام المعلومات التي تم جمعها لك لكي تصححها وتكملها عند الحاجة.
3. اتجه إلى مكتب الاستقبال لتتلقى بطاقتك كزائر.

## 6.6 اعتماد مُثبتي أجهزة قراءة الوصول إلى الأجهزة المحمولة

#### المقدمة

يستخدم مُثبتي قارئ الوصول إلى الأجهزة المحمولة Bosch Setup Access في المسح الضوئي للقارئ وتكوينها عبر BLE.

يرسل المشغلون المصريح لهم لكل من **Visitor Management** و **Credential Management** بيانات اعتماد افتراضية إلى تطبيق المثبت، لتحويل 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 المُثَبَّت 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  
- يمكن 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  
- يمكن 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.

## 6.6.1

**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.

## 6.7

**استخدام تطبيقات Mobile Access على الأجهزة المحمولة**

**ملاحظة:** تم وصف استخدام تطبيقات Bosch Mobile Access بالتفصيل للمستخدمين المعينين 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 يمنع 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 و Credential Management إرسال بيانات اعتماد افتراضية لكل من تطبيقات حامل البطاقة والمثبت.

**إشعار!**

هام: لا تتم 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.



## 6.7.1

**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 ملي 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):

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

#### 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).

### 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 البيئي.

### RSSI

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

### المستضيف

في سياق إدارة الزائرين، المستضيف هو متلقي الزيارة، أي أنه الشخص الذي يستقبل الزائر.

### وضع الكشك

وضع حظر شديد في استخدام المتصفح يتيح عادةً الوصول فقط إلى تطبيق ويب واحد وليس إلى إعدادات المتصفح أو عدة علامات تبويب أو نظام تشغيل الكمبيوتر.









**Bosch Security Systems B.V.**

Torenallee 49

BA Eindhoven 5617

Netherlands

**[www.boschsecurity.com](http://www.boschsecurity.com)**

Bosch Security Systems B.V., 2024 ©

**Building solutions for a better life**

202405131941