Access Management System V5.5

وين والتشغيل

دليل الاستخدام

ar

جدول المحتويات

1	**الأمان**	**7**
2	**استخدام التعليمات**	**8**
3	**حول هذه الوثائق**	**10**
4	**نظرة عامة على نظام AMS**	**11**
5	**ترخيص النظام**	**12**
6	**تكوين التقويم**	**13**
6.1	تحديد الأيام الخاصة	**13**
6.2	تحديد نماذج اليوم	**15**
6.3	تحديد نماذج الوقت	**16**
7	**تكوين الأقسام**	**19**
7.1	تعيين أقسام إلى أجهزة	**19**
7.2	تعيين أقسام إلى مشغّلين	**20**
8	**تكوين عناوين IP**	**21**
9	**استخدام محرر الجهاز**	**22**
9.1	أوضاع التكوين وتجاوزاته	**23**
10	**تكوين مناطق التحكم في الوصول**	**24**
10.1	تكوين مناطق للسيارات	**25**
11	**تكوين مناطق التسلل ولوحات كشف التسلل**	**27**
11.1	تثبيت واجهة برمجة تطبيقات RPS للاقتحام على كمبيوتر	**28**
11.2	توصيل نظام التحكم في الوصول بلوحات كشف التسلل	**28**
11.2.1	الخطوة 1: تحديد الاتصال بواجهة برمجة تطبيقات RPS	**29**
11.2.2	الخطوة 2: تكوين اتصالات اللوحة	**29**
11.3	إنشاء ملفات تعريف تخويلات اللوحات	**30**
11.4	تعيين ملفات تعريف تخويلات اللوحات لحاملي البطاقات	**31**
11.5	التحكم في الأبواب من خلال وحدات B901 على لوحات الاقتحام	**31**
12	**تكوين المشغّلين ومحطات العمل**	**33**
12.1	إنشاء محطات العمل	**33**
12.2	إنشاء ملفات تعريف محطة العمل	**34**
12.3	تعيين ملفات تعريف محطة العمل	**35**
12.4	إنشاء ملفات تعريف المستخدم (المشغّل)	**35**
12.5	تعيين ملفات تعريف المستخدم (المشغّل)	**36**
12.6	تعيين كلمات مرور المشغّلين	**37**
13	**تكوين البطاقات**	**39**
13.1	تعريف البطاقة	**39**
13.1.1	أنواع البطاقات النشطة	**39**
13.1.2	الإنشاء والتعديل	**39**
13.1.3	تنشيط / إلغاء تنشيط تعريفات البطاقات	**40**
13.1.4	إنشاء بيانات البطاقة في مدير الحوار	**41**
13.2	تكوين رموز البطاقات	**42**
14	**تكوين وحدات التحكم**	**44**
14.1	تكوين MAC وRMAC	**44**
14.1.1	تكوين إعدادات الوصول العمومي لـ MAC	**44**
14.1.2	تكوين جهاز MAC على خادم DMS	**45**
14.1.3	إعداد أجهزة كمبيوتر خوادم MAC لتشغيل أجهزة MAC وRMAC	**46**
14.1.4	تكوين جهاز MAC على خادم MAC الخاص به	**46**
14.1.5	إضافة RMAC إلى MAC	**47**
14.1.6	إضافة المزيد من أزواج MAC/RMAC	**49**
14.1.7	استخدام أداة تثبيت MAC	**50**

14.2	أجهزة التحكم في الوصول	51
14.3	تكوين أجهزة LAC	52
14.3.1	معلمات وإعدادات AMC	53
15	**تكوين DTLS للاتصال الآمن**	68
15.1	نشر DTLS من الأعلى إلى الأسفل	70
16	**تكوين المداخل**	72
16.1	المداخل - مقدمة	72
16.2	إنشاء مداخل	72
16.3	فحوصات مدخل/مخرج إضافية	77
16.4	تكوين المحطات الطرفية في AMC	77
16.5	الإشارات المعرّفة مسبقًا لنماذج الأبواب	83
16.6	المداخل الخاصة	89
16.6.1	المصاعد (DM07)	89
16.6.2	نماذج الأبواب مع إنذارات التسلل (DM14)	91
16.6.3	DIP وDOP في (DM15)	96
16.6.4	نماذج باب الشرَك	97
16.7	الأبواب	99
16.7.1	تحويل REX	102
16.7.2	تكوين الأبواب لإصدار الإنذارات المحلية	103
16.8	أجهزة القراءة	104
16.8.1	تكوين الفحص العشوائي	115
16.9	الوصول بواسطة رمز PIN فقط	115
16.10	لوحات توسيع AMC	116
17	**تكوينات القارئ المخصصة**	121
17.1	المقدمة	121
17.2	خاصية القارئ: معلمات القارئ الموسعة	121
17.3	استيراد مجموعة معلمات القارئ	121
17.4	تطبيق مجموعة معلمات على أجهزة القراءة	122
17.5	إدارة مجموعات معلمات القارئ	123
17.6	حذف مجموعات معلمات القارئ	124
18	**الحقول المخصصة لبيانات الموظفين**	125
18.1	معاينة وتحرير الحقول المخصصة	125
18.2	قواعد خاصة بحقول البيانات.	127
19	**تكوين إدارة مستوى التهديد**	128
19.1	مفاهيم إدارة مستوى التهديد	128
19.2	نظرة عامة على عملية التكوين	128
19.3	خطوات التكوين في محرر الجهاز	129
19.3.1	إنشاء مستوى تهديد	129
19.3.2	إنشاء ملف تعريف أمان باب	129
19.3.3	إنشاء ملف تعريف أمان قارئ	130
19.3.4	تعيين ملفات تعريف أمان الأبواب وأجهزة القراءة للمداخل	131
19.3.5	تعيين مستوى تهديد لإشارة جهاز	132
19.4	خطوات التكوين في مربعات حوار بيانات النظام	132
19.4.1	إنشاء ملف تعريف أمان شخص	132
19.4.2	تعيين ملف تعريف أمان شخص لنوع شخص	133
19.5	خطوات التكوين في مربعات حوار بيانات الموظفين	134
20	**تكوين Milestone XProtect لاستخدام AMS**	135
21	**دمج Otis Compass**	137
21.1	تكوين نظام Compass في محرر الجهاز	138

21.1.1	المستوى 1: إعداد نظام Compass	138
21.1.2	المستوى 2: مجموعات المصاعد، أجهزة DES وDER	139
21.1.3	المستوى 3: أجهزة DET	140
21.2	تكوين حقول مخصصة لخصائص خاصة بـ Otis لحاملي البطاقات	142
21.3	إنشاء تخويلات وتكوينها لمصاعد Otis	144
22	**تكوين IDEMIA Universal BioBridge**	145
22.1	إعداد BioBridge في نظام التحكم في الوصول من Bosch	145
22.2	اختيار تقنيات وتنسيقات البطاقات	146
22.3	اختيار وضع التعريف	150
22.3.1	بطاقة أو بيانات بيومترية	150
22.3.2	بطاقة وبيانات بيومترية	153
22.3.3	بيانات بيومترية فقط	153
22.4	إعداد BioBridge في MorphoManager	153
22.4.1	ملفات تعريف Wiegand	154
22.4.2	تكوين الأجهزة البيومترية	155
22.4.3	الجهاز البيومتري	156
22.4.4	تكوين المستخدم	158
22.4.5	مجموعات توزيع المستخدمين	159
22.4.6	إعداد ODBC لـ BioBridge	160
22.4.7	تكوين نظام BioBridge	164
22.5	تكوين عميل التسجيل BioBridge	166
22.5.1	إضافة مشغّل تسجيل إلى Morpho Manager	167
22.5.2	تكوين أجهزة كمبيوتر عميل MorphoManager لمهام التسجيل	167
22.5.3	اختبار عميل التسجيل	172
22.6	الحدود والملاحظات التقنية	173
23	**تحقيق معايير EN 60839**	176
24	**تعريف تخويلات وملفات تعريف الوصول**	177
24.1	إنشاء تخويلات الوصول	177
24.2	إنشاء ملفات تعريف الوصول	177
25	**إنشاء وإدارة بيانات الموظفين**	179
25.1	الأشخاص	179
25.1.1	خيارات مراقبة البطاقة أو مراقبة المبنى	181
25.1.2	معلومات إضافية: تسجيل المعلومات المعرّفة من قِبل المستخدم	182
25.1.3	تسجيل التواقيع	182
25.1.4	تسجيل بيانات بصمة الإصبع	182
25.1.5	تسجيل بيانات عروق راحة اليد	184
25.2	الشركات	187
25.3	البطاقات: إنشاء وتعيين بيانات الاعتماد والأذونات	187
25.3.1	تعيين بطاقات إلى أشخاص	188
25.3.2	طباعة الشارات	189
25.3.3	علامة تبويب التخويلات	190
25.3.4	علامة التبويب "بيانات أخرى": الاستثناءات والأذونات الخاصة	190
25.3.5	تخويل الأشخاص تعيين وضع المكتب	191
25.3.6	علامة التبويب Smartintego	192
25.3.7	إنشاء بطاقة تنبيه	194
25.4	البطاقات المؤقتة	194
25.5	رموز PIN للموظفين	195
25.6	حظر وصول الموظفين	197
25.7	إدراج بطاقات في القائمة المحظورة	198

25.8	تحرير عدة أشخاص في الوقت نفسه	199
25.8.1	تخويلات المجموعة	200
25.9	تغيير القسم لأشخاص	201
25.10	إعداد المنطقة الأشخاص أو السيارات	202
25.10.1	إجراء لإعادة تعيين موقع جميع حاملي البطاقات والسيارات	202
25.11	تخصيص النماذج وطباعتها لبيانات الموظفين	203
26	**إدارة الزائرين**	204
26.1	بيانات الزائرين	204
26.2	زائر متأخر جدًا	209
27	**إدارة ساحات الانتظار**	211
27.1	تجاوز مدة صف السيارات	211
27.2	تذاكر صف السيارات	211
27.3	تصدير أرقام استخدام أماكن صف السيارات	218
27.4	فحص تصدير "الصلاحية المتنقلة"	218
27.5	تخويلات لمناطق انتظار عديدة	219
27.6	تقرير مكان صف السيارات	220
27.7	إدارة ساحة انتظار السيارات الموسعة	221
28	**إدارة جولات المراقبة والدوريات**	223
28.1	تعريف جولات المراقبة	223
28.2	إدارة الدوريات	224
28.3	مراقبة الجولة (في السابق التحكم في المسار)	225
29	**الفحص العشوائي للموظفين**	227
30	**استخدام عارض الأحداث**	229
30.1	تعيين معايير لتصفية الوقت بالنسبة إلى الحاضر	229
30.2	تعيين معايير التصفية لفاصل زمني	229
30.3	تعيين معايير التصفية بصرف النظر عن الوقت	230
31	**استخدام التقارير**	231
31.1	التقارير: البيانات الرئيسية	231
31.1.1	إعداد تقرير حول المركبات	232
31.2	التقارير: بيانات النظام	234
31.3	التقارير: التخويلات	235
32	**تشغيل إدارة مستوى التهديد**	237
32.1	تشغيل وإلغاء تنبيه تهديد عبر أمر واجهة المستخدم	237
32.2	تشغيل تنبيه تهديد عبر إشارة جهاز	238
32.3	تشغيل تنبيه تهديد عبر بطاقة تنبيه	238
33	**تشغيل مؤشر التمرير**	239
33.1	حالات خاصة	240
34	**النسخ الاحتياطي والاستعادة**	242
34.1	النسخ الاحتياطي للنظام	242
34.2	استعادة نسخة احتياطية	243
34.2.1	استعادة وحدات RMAC إلى تثبيت جديد	245
35	**تكوين بطاقات CEPAS واستخدامها**	246
	المصطلحات	248

1 الأمان

استخدام البرنامج الأحدث

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

توفر الروابط التالية المزيد من المعلومات:

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

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

2 استخدام التعليمات

كيفية استخدام ملف التعليمات هذا.

أزرار شريط الأدوات

الزر	الوظيفة	الوصف
	إخفاء	انقر فوق هذا الزر لإخفاء جزء التنقل (علامات التبويب "المحتويات" و"الفهرس" و"بحث")، بحيث يبقى جزء التعليمات فقط مرئيًا.
	إظهار	عند النقر فوق الزر "إخفاء"، يحل محله الزر "إظهار". انقر فوق هذا الزر لإعادة فتح جزء التنقل.
	رجوع	انقر فوق هذا الزر للرجوع إلى الخلف عبر سلسلة الموضوعات التي تم عرضها مؤخرًا.
	للأمام	انقر فوق هذا الزر للتحرك إلى الأمام مرة أخرى عبر سلسلة الموضوعات ذاتها
	طباعة	انقر فوق هذا الزر من أجل الطباعة. اختر بين "طباعة الموضوع المُحدَد" و"طباعة العنوان المُحدَد وكل الموضوعات الفرعية".

علامات التبويب

المحتويات تعرض علامة التبويب هذه جدول محتويات بتدرج هرمي. انقر فوق أيقونة كتاب لفتحه ثم انقر فوق أيقونة موضوع لعرض ذلك الموضوع.

الفهرس تعرض علامة التبويب هذه فهرس المصطلحات بالترتيب الأبجدي. حدد موضوعًا من القائمة أو اكتب كلمة للعثور على الموضوع (الموضوعات) الذي يحتوي على تلك الكلمة.

بحث استخدم علامة التبويب هذه للعثور على أي نص. أدخِل نصًا في الحقل ثم انقر فوق الزر: **سرد الموضوعات** للعثور على الموضوعات التي تحتوي على كل الكلمات التي تم إدخالها.

تغيير حجم نافذة التعليمات

اسحب زاوية النافذة أو حافتها إلى الحجم المطلوب.

مصطلحات إضافية مستخدمة في هذه الوثائق

- يظهر النص الحرفي (التسميات) من واجهة المستخدم بخط **غامق**.
  على سبيل المثال، **أدوات، ملف، حفظ باسم...**
- يتم ربط النقرات المتتابعة باستخدام الرمز **>** (إشارة أكبر من).
  على سبيل المثال، **ملف > جديد > مجلد**
- تتم الإشارة إلى التغييرات في نوع عنصر التحكم (مثل القائمة وزر الاختيار وخانة الاختيار وعلامة التبويب) ضمن السلسلة قبل تسمية عنصر التحكم مباشرة.
  على سبيل المثال، انقر فوق القائمة: **إضافية > خيارات >** علامة التبويب: **عرض**
- تتم كتابة تركيبات المفاتيح بطريقتين:
  - يعني Ctrl+Z الضغط باستمرار على المفتاح الأول مع الضغط على المفتاح الثاني
  - يعني Alt, C الضغط على المفتاح الأول وتحريره، ثم الضغط على المفتاح الثاني

- تُضاف وظائف أزرار الأيقونات ضمن أقواس مربعة بعد الأيقونة نفسها.
  على سبيل المثال، [حفظ]

3 حول هذه الوثائق

هذا هو دليل برامج Access Management System الرئيسي.
إنه يتناول استخدام برنامج مدير مربع الحوار الرئيسي، المُشار إليه فيما بعد باسم AMS

- تكوين نظام التحكم في الوصول في AMS .
- تشغيل النظام المكوّن بواسطة مشغّلي النظام.

الوثائق ذات الصلة

تم توثيق العمليات التالية بشكل منفصل:

- تثبيت AMS وبرامجه المساعدة.
- تشغيل AMS - Map View.

4 نظرة عامة على نظام AMS

إن Access Management System عبارة عن نظام تحكم في الوصول فعال وحقيقي، يعمل بمفرده أو بالتعاون مع BVMS، نظام إدارة الفيديو المميز من Bosch.

يستمد هذا النظام فعاليته من قدرته على الموازنة الفريدة بين التقنيات الرائدة والمثبتة الفعالية.

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

5 ترخيص النظام

الشروط الأساسية

- تم تثبيت النظام بنجاح.
- سجلت دخولك إلى كمبيوتر خادم AMS، بصفة مسؤول (مستحسن)

الإجراء الخاص بالتراخيص المشتراة

الشروط الأساسية: لقد اشتريت التراخيص استنادًا إلى توقيع الكمبيوتر لهذا الكمبيوتر. اتصل بمندوب المبيعات للحصول على الإرشادات.

تنشيط الترخيص

المسار

- مدير حوار AMS > **القائمة الرئيسية** > **التكوين** > **التراخيص**

1. انقر فوق **إدارة الترخيص**
. عندها سيفتح معالج **إدارة التراخيص**.
2. انقر فوق **حفظ** لحفظ معلومات النظام في ملف.
3. انقر فوق **متابعة**.
4. قم بتسجيل الدخول إلى Remote Portal على العنوان remote.boschsecurity.com باستخدام بيانات اعتماد شركتك.
5. حدد المنتج المراد ترخيصه، واتبع الإرشادات الموجودة في البوابة لإنشاء ملف الترخيص وتنزيله.
6. ارجع الى **إدارة التراخيص**.
7. انقر فوق **متابعة**.
8. انقر فوق **استيراد** لتحديد موقع ملف الترخيص الذي قمت بتنزيله وأضفه إلى نظامك.
9. انقر فوق **إنهاء**.
10. انقر فوق **إعادة تشغيل مدير حوار AMS**.

إشعار!

إذا ظهرت لك أي رسائل خطأ أثناء العملية، فاتصل بدعم Bosch.

إشعار!

نتائج تغييرات الأجهزة والبرامج

بإمكان التغييرات التي يتم إدخالها على أجهزة الخادم أن تؤدي إلى إلغاء صلاحية ترخيصك والتسبب في توقف البرنامج عن العمل. يُرجى مراجعة الأمر مع قسم الدعم التقني قبل إجراء تغييرات على الخادم.

الإجراء الخاص بوضع العرض التوضيحي

يقدم وضع العرض التوضيحي تراخيص لجميع ميزات النظام لفترة وقت محدودة. استخدم وضع العرض التوضيحي فقط في البيئات غير الخاصة بالإنتاج لتجربة هذه الميزات قبل شرائها.

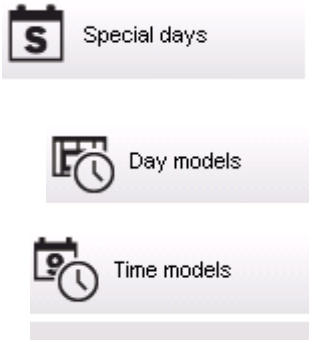
1. سجّل دخولك إلى Access Manager
2. انتقل إلى **التكوين** > **التراخيص**
3. انقر فوق الزر **تنشيط وضع العرض التوضيحي**
4. تأكد من أن الميزات مدرجة في نافذة مربع حوار **التراخيص**.

يتم تنشيط وضع العرض التوضيحي لمدة 5 ساعات. يظهر وقت انتهاء الصلاحية بالقرب من أعلى مربع حوار **التراخيص**، وفي شريط العناوين الموجود في معظم نوافذ مربع الحوار.

6 تكوين التقويم

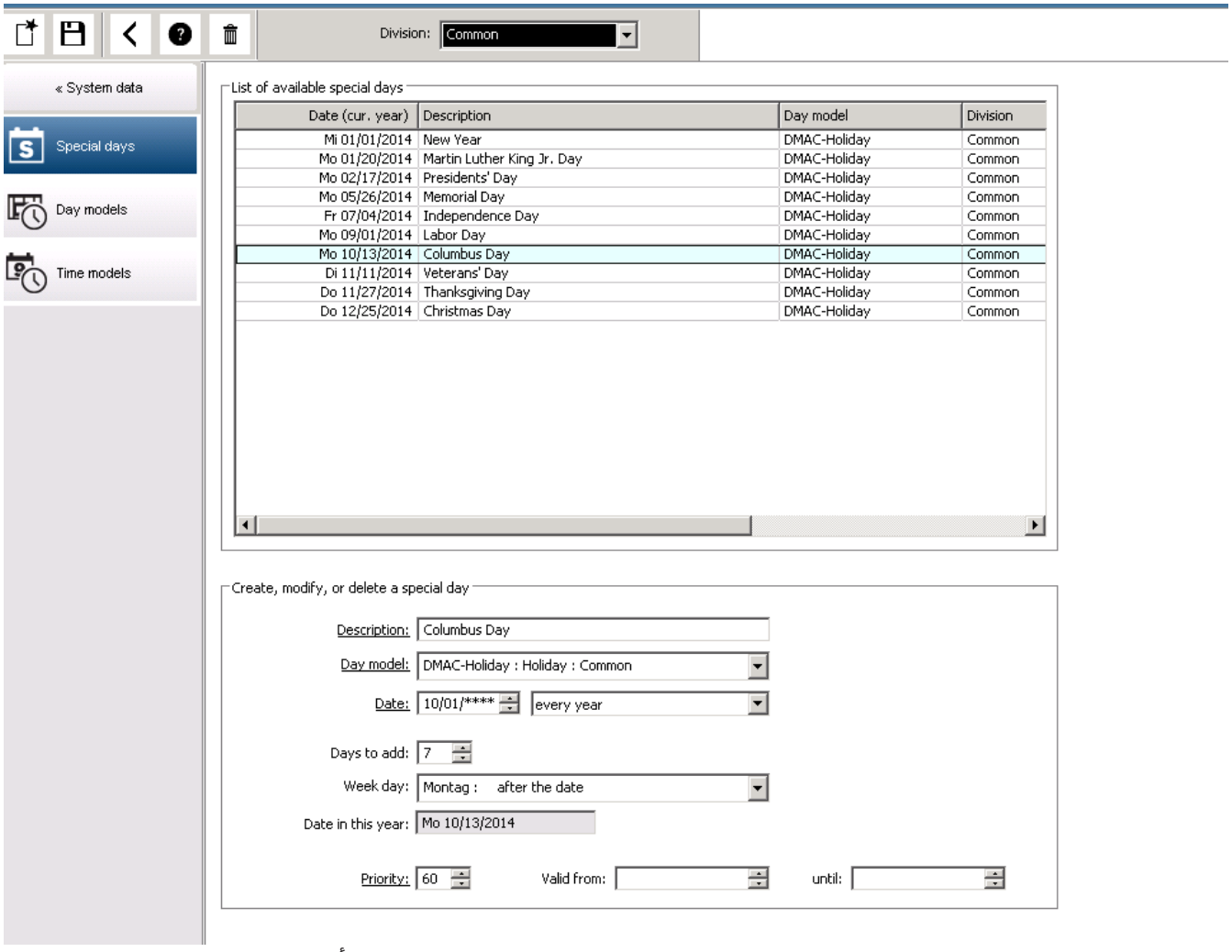
تخضع أنشطة التحكم في الوصول **لنماذج الوقت**.
يُعتبر **نموذج الوقت** تسلسلاً مختصرًا ليوم واحد أو أكثر، يتم وصف كل واحد على أنه **نموذج اليوم**.
تتحكم نماذج الوقت في الأنشطة عندما يتم تطبيقها على **التقويم** الأساسي لنظام التحكم في الوصول.
يستند تقويم نظام التحكم في الوصول إلى تقويم نظام تشغيل الكمبيوتر المضيف، ولكنه يوسّعه بواسطة **أيام خاصة** يحددها مسؤول نظام التحكم في الوصول بشكل اختياري.
يمكن تثبيت الأيام الخاصة على تاريخ معين في التقويم أو يمكن تحديدها بالنسبة إلى حدث ثقافي، مثل عيد الفطر. ويمكنها أن تكون متكررة أو غير متكررة.
تتكوّن عملية تكوين تقويم فعلي لنظام التحكم في الوصول من الخطوات التالية.

1. تحديد **الأيام الخاصة** في التقويم التي تنطبق على موقعك.
2. تحديد **نماذج اليوم** التي تصف الفترات النشطة وغير النشطة لكل نوع من أنواع الأيام. على سبيل المثال، سيكون نموذج اليوم ليوم عطلة رسمية مختلفًا عن نموذج اليوم ليوم عمل عادي. يؤثر أيضًا عمل الورديات على نوع وعدد نماذج اليوم التي تحتاج إليها.
3. تحديد **نماذج الوقت** التي تتكوّن من نموذج يوم واحد أو أكثر.
4. تعيين نماذج الوقت إلى حاملي البطاقات والتخويلات والمداخل.



6.1 تحديد الأيام الخاصة

عند فتح مربع الحوار هذا، تظهر قائمة في حقل القائمة العلوي من مربع الحوار تحتوي على كل العطلات المحددة. يرجى العمل أن كل تواريخ العطلات المعروضة ترتبط بالعام الحالي فقط. ومع ذلك، يتم تحديث التقويم سنويًا بما يتفق مع البيانات التي تم إدخالها.
توجد أسفل القائمة حقول مربعات حوار مختلفة من أجل إنشاء أيام خاصة جديدة، وتغيير الأيام الخاصة الموجودة بالفعل أو حذفها. لإضافة يوم خاص جديد، يجب أن تحتوي ثلاثة حقول على الأقل من حقول الإدخال هذه على بيانات. أولاً، يجب إدخال **وصف** و تاريخ في الحقول المعنية. وثالثًا، يجب تحديد الفئة التي ينتمي إليها هذا اليوم الخاص من القائمة الاختيارية المناسبة.



يتم تحديد التاريخ في عدة خطوات. بادئ ذي بدء، يتم إدخال التاريخ الأساسي في حقل **التاريخ**. عند هذه النقطة، يصف التاريخ حدثًا في العام الحالي. إذا حدد المستخدم الآن معدل الرجوع الدوري في قائمة التحديد الموجودة بجوار حقل التاريخ، يتم استبدال أجزاء التاريخ التي تم تعيينها حسب المعدل الدوري لتحل محلها "أحرف البدل" (*).

مرة واحدة	__.__.____
مرة واحدة كل عام	__.__.****
مرة واحدة كل شهر لمدة عام	__.**.____
مرة واحدة كل شهر كل عام	__.**.****
بحسب عيد الفصح	**.**.****

لا يتم تحديد العطلات التي تتوقف على عيد الفصح بتواريخها، وإنما بفارق الأيام عن أحد الفصح. يُشار إلى تاريخ أحد الفصح للعام الحالي في الحقل **تاريخ ضمن هذا العام** ، ويتم إدخال تباين هذا التاريخ أو تحديده في الحقل **الأيام المطلوب إضافتها**. الحد الأقصى لعدد الأيام هو 188 يومًا، وبهذا يمكنك تحديد كل يوم من العام عن طريق الإضافة أو الطرح.

تُعد البيانات الأخرى، مثل **يوم الأسبوع** للعطلة، اختيارية. ويُرجى ملاحظة أن قائمة أيام الأسبوع تحددها الإعدادات الإقليمية لنظام التشغيل. وهذا يؤدي حتمًا إلى عرض لغات مختلطة على الشاشة حيث تختلف لغة نظام التحكم في الوصول عن لغة نظام التشغيل.

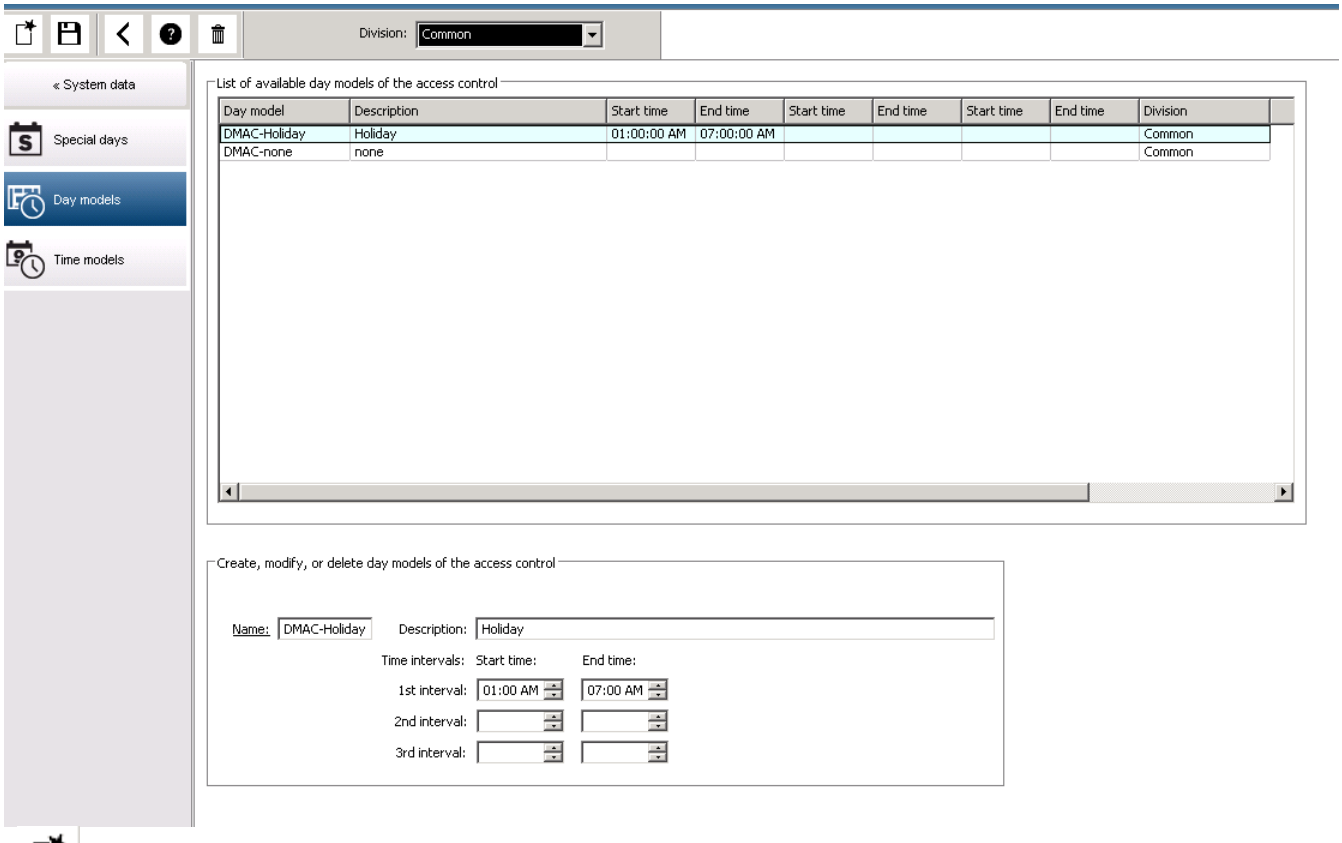
ويُعد أيضًا تعيين **فترة الصلاحية** اختياريًا. وإذا لم يتم تحديد مدة معينة، فإن الإعدادات الافتراضية تجعل الصلاحية بلا حدود بداية من تاريخ الإدخال.

يمكن أيضًا تعيين **أولوية**. وتحدد الأولوية التي تبدأ من 1 إلى 100 العطلة التي سيتم استخدامها وفي حالة وقوع عطلتين في التاريخ نفسه، تأتي العطلة ذات الأولوية الأعلى في المرتبة الأولى. وفي حالة تساوي الأولويات، لن يتم تحديد العطلة التي سيتم استخدامها.
يتم تعطيل العطلة ذات الأولوية "0" ولن يتم استخدامها.
يعرض مربع الحوار **نماذج الوقت** العطلات النشطة فقط، أيْ ذات الأولوية التي تزيد على "0".

إشعار!
بإمكان نموذج الوقت من القسم "عام" أن يستخدم العطلات المخصصة للقسم "عام" فقط.
وبإمكان نموذج الوقت المخصص من القسم "أ" أن يستخدم العطلات المخصصة للقسم "أ" فقط.
ويتعذر وضع العطلات في غير القسم المخصص لها، بمعنى أنه يمكن لكل قسم أن يستخدم العطلات المحددة فقط المخصصة له في نموذج الوقت الخاص به.

6.2 تحديد نماذج اليوم

تحدد نماذج اليوم نمطًا لأي يوم. ويمكن أن تحتوي على ثلاثة فواصل زمنية.
وبمجرد أن يبدأ مربع الحوار، تُعرض كل نماذج اليوم المتوفرة.



استخدم مربع الحوار لتحديد أو تعديل اسم النموذج والمواصفات والفواصل الزمنية. تبدأ الأيقونة نموذجًا جديدًا.
يتم إدخال وقت بدء وانتهاء الفاصل الزمني بالساعات والدقائق. وفور الوصول إلى هذا الوقت، يتم تنشيط الفاصل الزمني أو إلغاء تنشيطه على التوالي. ولجعل هذه الأوقات أكثر وضوحًا بوصفها محددات، يعرضها جزء القائمة بالثواني (دائمًا 00). على سبيل المثال، يسمح التخويل الموجود في نموذج الوقت الذي يحتوي على فاصل يمتد من الساعة 8:00 صباحًا إلى الساعة 3:30 عصرًا بالوصول من 8:00 صباحًا إلى 3:30 عصرًا ولكن يمنع الوصول الساعة 3:30:01. عصرًا.
تخضع أوقات البدء والانتهاء لعمليات التحقق المنطقية عند إدخالها، فمثلاً يجب أن يكون وقت البدء أقل من وقت الانتهاء المرتبط به.

تتمثَّل إحدى النتائج المترتبة على هذا الإجراء في تعذر امتداد الفاصل الزمني إلى ما بعد منتصف الليل، ولكن ينبغي أن ينقسم عند تلك النقطة:

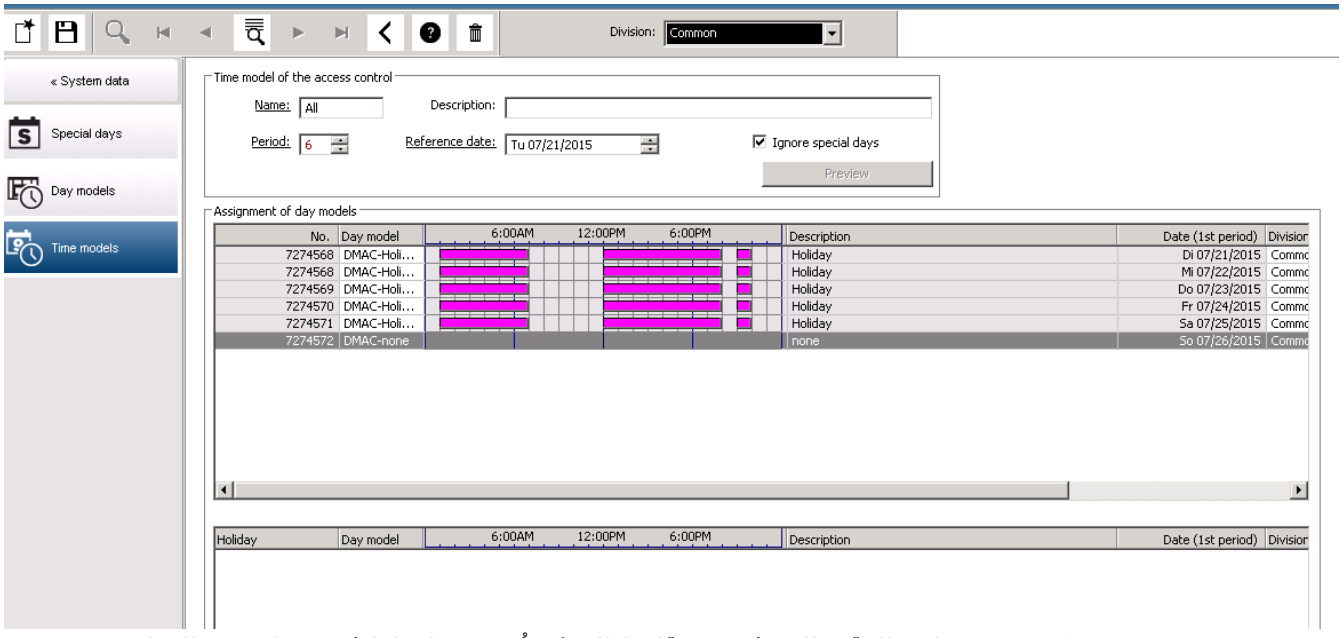
الفاصل الزمني الأول	من:	...	إلى:	12:00 منتصف الليل
الفاصل الزمني التالي	من:	12:00 منتصف الليل	إلى:	...

باستثناء منتصف الليل (12:00) لا يُسمح بحدوث تداخلات بين محددات الفاصل الزمني لنموذج اليوم الفردي. تجدر الإشارة إلى أن هذا الإجراء يمنع إدخال الوقت نفسه للدلالة على انتهاء الفاصل الزمني وبدء الفاصل الزمني التالي.
استثناء: بالرغم من ذلك، تم تعيين وقت بدء وانتهاء الفاصل الزمني الذي يمتد لمدة 24 ساعة على 12:00 منتصف الليل.

إشعار!
تلميح: يمكن التحقق من الفواصل الزمنية بعرضها في مربع الحوار "نماذج الوقت": ينبغي أولاً إنشاء نموذج يوم يحتوي على تلك الفواصل الزمنية (بيانات النظام > التقويم > نماذج اليوم). وبعد ذلك، ينبغي تخصيص نموذج وقت وهمي لنموذج اليوم هذا بحيث يحتوي على فترة يوم واحد (بيانات النظام > التقويم > نماذج الوقت). وبعد ذلك تُعرض الفواصل الزمنية في الرسم البياني الشريطي.
اخرج من مربع حوار "نماذج الوقت" من دون حفظ التغييرات.

يمكن حذف نموذج اليوم فقط إذا لم يتم تخصصيه بيوم معين ولم يتم استخدامه في نموذج يوم ما.

6.3 تحديد نماذج الوقت



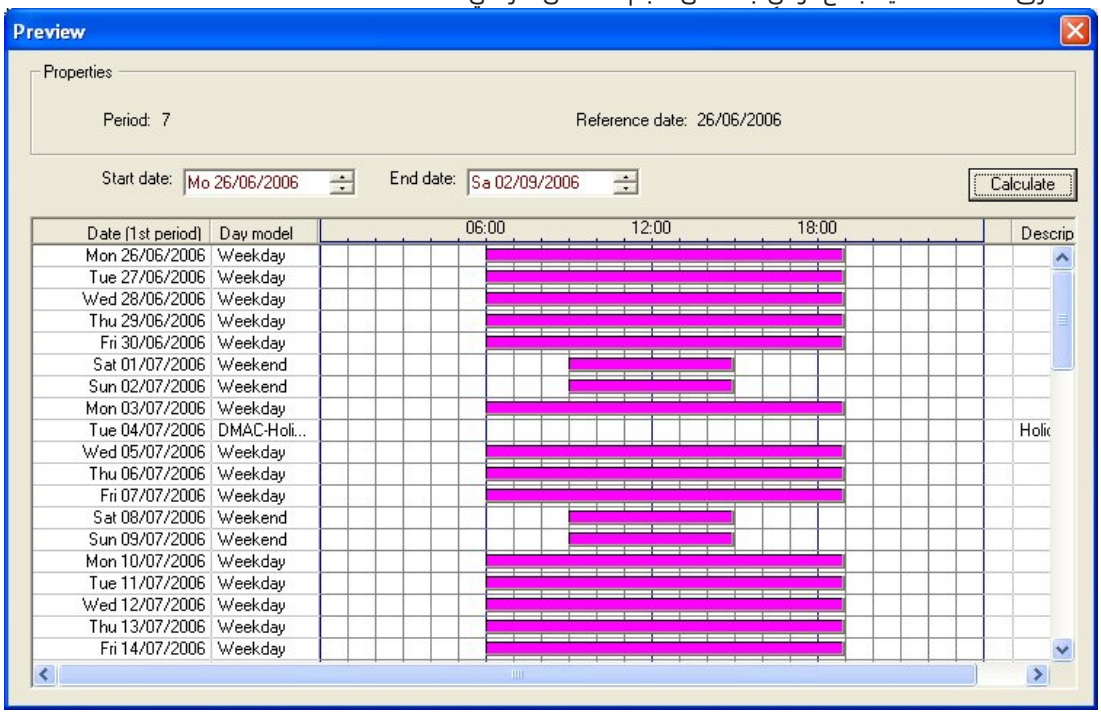
يمكن تحديد نماذج الوقت المتوفرة من قائمة البحث وتُعرض تفاصيلها في حقول مربع الحوار. ويجري تنفيذ أيّ معالجة بالاتساق مع الإجراء لإنشاء نماذج وقت جديدة.
إذا كان القناع فارغًا، يمكن إنشاء نماذج الوقت من البداية. ولتنفيذ هذا الإجراء، يجب أن تدخل **الاسم** وعدد الأيام في **الفترة** وتحدد تاريخًا للبدء **أو تاريخًا مرجعيًا**. وعند تأكيد هذه البيانات (**إدخال**)، تظهر قائمة في حقل مربع الحوار **تعيين نماذج اليوم** أسفل منها. يتوافق عدد الأسطر في هذه القائمة مع عدد الأيام المعيَّن أعلاه، والأعمدة التي تحتوي بالفعل على رقم متدرِّج وتواريخ الفترة، إذ تبدأ بتاريخ البدء المحدد.
بإمكان المستخدم تغيير أو إدراج إدخالات العمود **"الاسم"** فقط في هذه القائمة، كما ذُكر من قبل، وتنشأ الإدخالات في العمودين **"العدد"** و **"التاريخ"** من البيانات الموجودة في رأس مربع الحوار، ويقوم النظام بتعبئة العمود **"الوصف"** باختيار نموذج يوم والتفسيرات التي تمت في مربع الحوار هذا.

من خلال النقر المزدوج على السطر المعني في عمود **نموذج اليوم** ينشط حقل قائمة التحديد. ويمكن تحديد نموذج واحد من نماذج اليوم الموجودة من هذه القائمة. وبهذه الطريقة، يمكن تعيين نموذج يوم محدد لكل يوم من الفترة. وعندما ينتقل المستخدم إلى سطر آخر، يشير النظام إلى الوصف الموجود لنموذج اليوم المحدد في العمود **الوصف**.

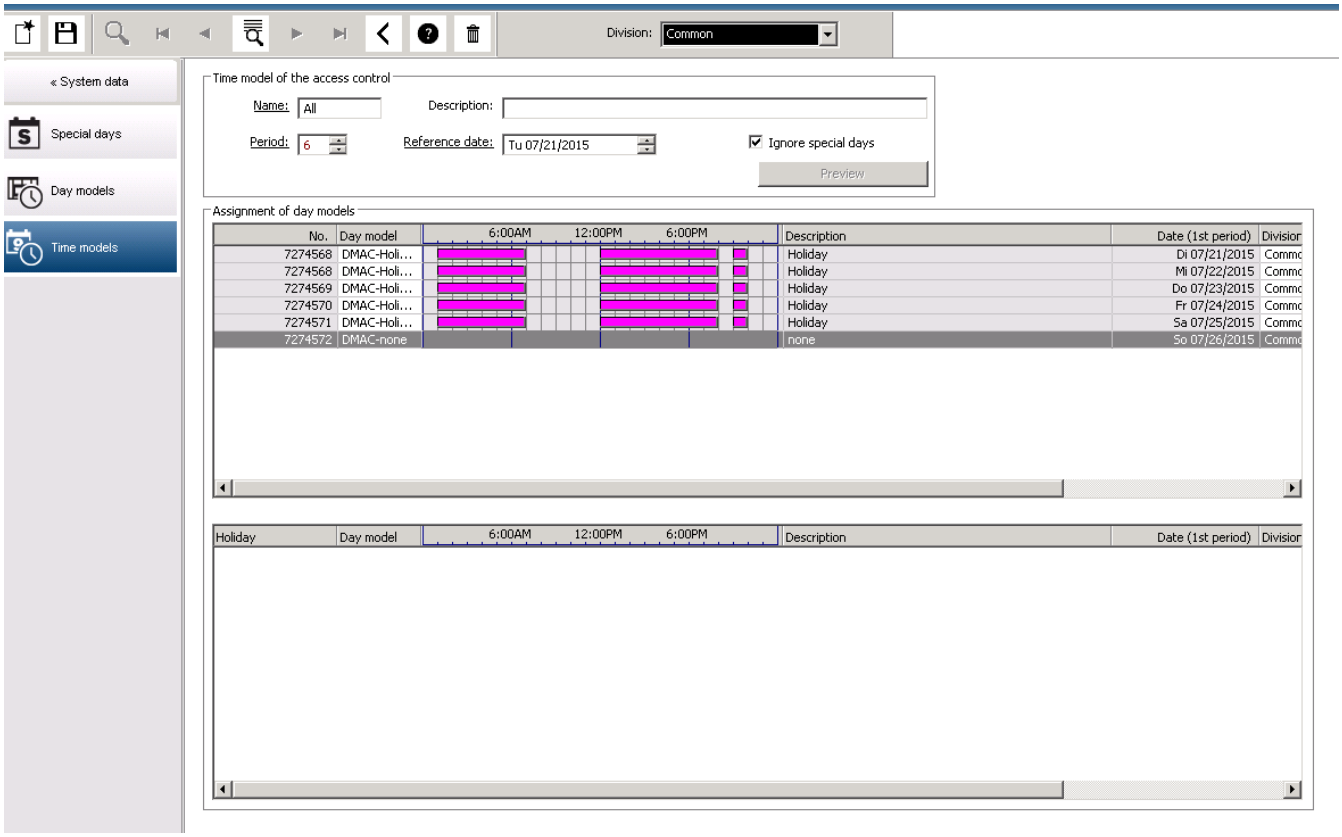
تظهر **العطلات** مسبقة التحديد مع نماذج اليوم ذات الصلة في حقل القائمة السفلي لأغراض التنقل والتحقق. وبالنسبة لنموذج الوقت المحدد أو الذي تم إنشاؤه حديثًا، يمكن تغيير تخصيص نماذج اليوم لعطلات معينة. ومع ذلك، لا تسري هذه التغييرات إلا على نموذج الوقت المعين هذا، ولا يمكن تنفيذ التغييرات العامة التي ينبغي أن تنطبق على كل النماذج الموجودة بالفعل والمستقبلية إلا في مربع الحوار "العطلات". واتساقًا مع هذه الإعدادات، تُمنح أيام الأسبوع نماذج يوم مخصصة، مقابل العطلات.

وبعد ذلك وفقًا لهذه الإعدادات، تُقابل أيام الأسبوع بنماذج اليوم المخصصة في ظل مراعاة الأيام الخاصة. وللتحقق سريعًا من أنه تم استخدام نماذج اليوم وتعيينها بشكل صحيح، لا سيما في العطلات، يحتوي مربع الحوار هذا على **معاينة** تعرض مقدار تخصيص الأيام للفترات المحددة.

وفي النهاية، يفتح مربع حوار مستقل بالنقر على الزر **معاينة** ويمكن تحديد فترة زمنية تبلغ 90 يومًا كحد أقصى بما يشمل العطلات. عند النقر فوق الزر **حساب** ينشأ التقرير ويُعرض كما يظهر فيما يلي، وقد تستغرق هذه العملية بضع ثوانٍ بناءً على حجم الفاصل الزمني.



في الإعداد الافتراضي، تنطبق الأيام الخاصة على نماذج الوقت وفق تعريفاتها. وفي حالة وجود أيام خاصة، بالرغم من ذلك، دون اعتبار بشكل استثنائي، يمكن أن يحدث هذا بتحديد الخيار **تجاهل الأيام الخاصة**. ويتم حذف الإدخالات من القائمتين السفليتين معًا، حتى يتبين للمستخدم على الفور وبشكل واضح أنه لا يوجد استخدام للأيام الخاصة وفئات الأيام في هذا النموذج.


Division:
Common
« System data
Special days
Day models
Time models
Time model of the access control
Name:
All
Description:
Period:
6
Reference date:
Tu 07/21/2015
Ignore special days
Preview
Assignment of day models
No.
Day model
6:00AM
12:00PM
6:00PM
Description
Date (1st period)
7274568 DMAC-Holi... Holiday Di 07/21/2015
7274568 DMAC-Holi... Holiday Mi 07/22/2015
7274569 DMAC-Holi... Holiday Do 07/23/2015
7274570 DMAC-Holi... Holiday Fr 07/24/2015
7274571 DMAC-Holi... Holiday Sa 07/25/2015
7274572 DMAC-none none So 07/26/2015
Holiday
Day model
6:00AM
12:00PM
6:00PM
Description
Date (1st period)

7 تكوين الأقسام

المقدمة

يمكن ترخيص النظام بشكل اختياري لتوفير التحكم في الوصول المشترك لمنشأة يشترك فيها أي عدد من الأطراف المستقلة، وتُسمّى **الأقسام**.

يمكن تعيين قسم واحد أو أكثر لمشغّلي النظام. ولا يرى المشغّلون عندئذ إلا الأشخاص والأجهزة والمداخل الخاصة بهذه الأقسام.

في حالة عدم ترخيص ميزة **الأقسام**، تنتمي جميع الكائنات المدارة من قِبل النظام إلى قسم واحد يُسمى **عام**.

الشروط الأساسية

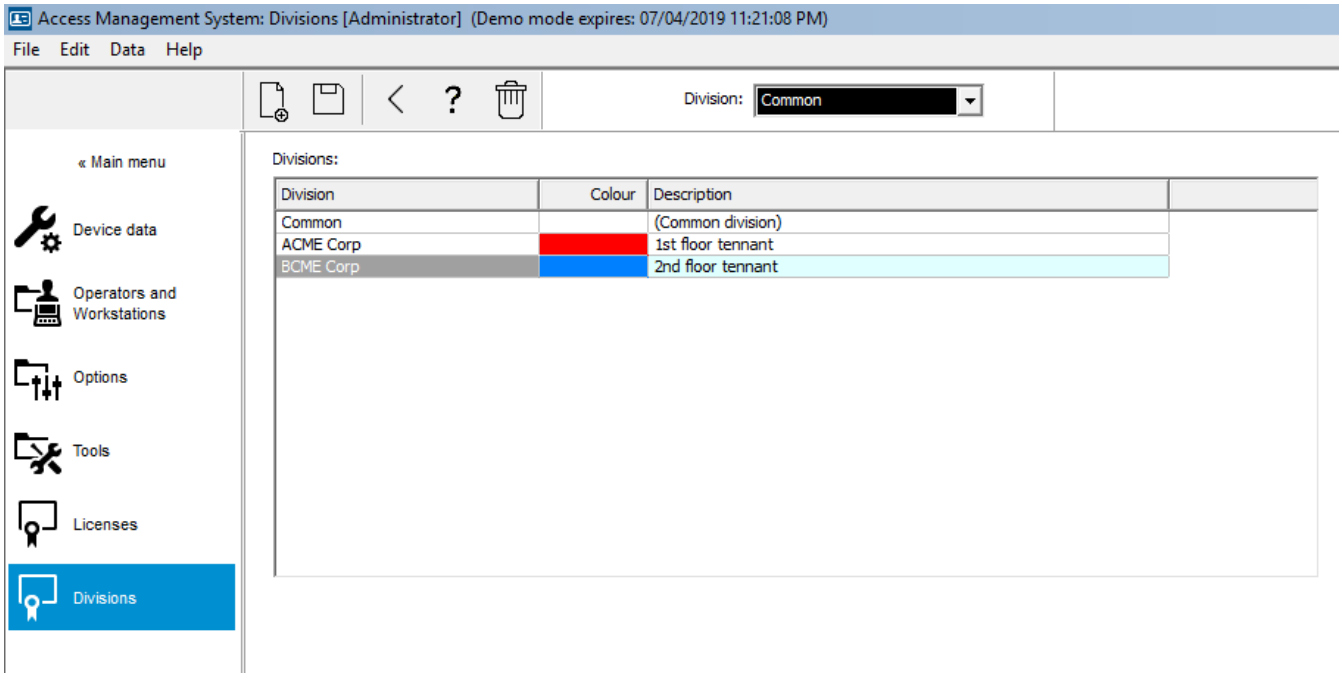
- ميزة "الأقسام" مُرخّصة لعملية التثبيت الخاصة بك.

مسار مربع الحوار

- القائمة الرئيسية > **التكوين** > **الأقسام**
- مستعرض تكوين BIS > **المواقع** > **الأقسام**

الإجراء

1. انقر فوق الزر ✚ أو انقر بزر الماوس الأيمن فوق **عام** وحدد **إضافة قسم جديد** من قائمة السياق.
2. انقر فوق في شريط الأدوات.
   - يتم إنشاء قسم جديد باسم افتراضي.
3. اكتب فوق الاسم الافتراضي ثم (اختياري) أدخِل وصفًا يستفيد منه المشغّلون الآخرون.
4. انقر في عمود **اللون** لتعيين لون للمساعدة في تمييز أصول القسم في واجهة المستخدم.
5. انقر فوق **تطبيق** للحفظ
6. انقر فوق للحفظ



7.1 تعيين أقسام إلى أجهزة

تعيين أقسام إلى أجهزة في محرر الجهاز

مسار مربع الحوار
القائمة الرئيسية > **التكوين** > **بيانات الجهاز**

الشروط الأساسية
- الأقسام مُرخّصة وقيد التشغيل
- تم إنشاء قسم واحد على الأقل.

الإجراء
1. من شجرة الأجهزة، حدد الجهاز من أجل التعيين.
   - يظهر محرر الجهاز في جزء مربع الحوار الرئيسي.
2. من قائمة "الأقسام"، حدد القسم الجديد للجهاز
   - يعكس مربع القائمة القسم الجديد.
3. انقر فوق (حفظ) للحفظ

إشعار!
يجب أن تنتمي جميع مكونات أي مدخل إلى قسم واحد
لن يسمح النظام لك بحفظ أي مدخل حتى تنتمي كل مكوناته إلى القسم نفسه.

7.2 تعيين أقسام إلى مشغّلين

عيّن الأقسام إلى المشغّلين في مربع الحوار **حقوق المستخدم**

مسار مربع الحوار
القائمة الرئيسية > **التكوين** > **المشغّلون ومحطات العمل > حقوق المستخدم**

الشروط الأساسية
- الأقسام مُرخّصة وقيد التشغيل
- تم إنشاء قسم واحد على الأقل.
- تم إنشاء مشغّل واحد على الأقل في النظام

الإجراء
1. من مربع الحوار **حقوق المستخدم**، حدد سجل الموظف للمشغّل المطلوب تعيينه.
2. على علامة التبويب **الأقسام**، استخدم مفاتيح الأسهم لنقل الأقسام من قائمة **الأقسام المتاحة** إلى قائمة **الأقسام المعيَّنة** لهذا المشغّل.
3. انقر فوق (حفظ) للحفظ

8 تكوين عناوين IP

تحتاج وحدات التحكم في الوصول المحلية على الشبكة إلى مخطط متناسق من عناوين IP لكي تتمكن من المشاركة في نظام التحكم في الوصول. تحدد الأداة **AMCIPConfig** مواقع أدوات التحكم على الشبكة، وتوفر واجهة ملائمة لإدارة عناوينها وخيارات أخرى خاصة بالشبكة بطريقة مركزية.

الشروط الأساسية

- يتم تزويد وحدات التحكم في الوصول المحلية بالطاقة وتوصيلها بالشبكة.
- لديك مخطط عناوين IP لأدوات التحكم بالإضافة إلى كلمات مرورها، إذا لزم الأمر.

مسار مربع الحوار

القائمة الرئيسية > التكوين > الأدوات

الإجراء

1. اتبع مسار مربع الحوار أعلاه وانقر فوق **تكوين AMC.**
2. انقر فوق **Scan AMCIPConfig**

يتم إدراج وحدات التحكم في الوصول المحلية المتوفرة على الشبكة، وتتضمن كل واحدة منها المعلمات التالية:

- **عنوان MAC**: عنوان الجهاز لوحدة التحكم. لاحظ أن هذا العنوان **ليس** عنوان وحدة التحكم في الوصول الرئيسية، التي تسمى MAC عن طريق الصدفة فقط.
- **عنوان IP المخزّن**:
- **رقم المنفذ**: الرقم الافتراضي هو 10001
- **DHCP**: القيمة هي **نعم** فقط إذا تم تكوين وحدة التحكم لتلقي عنوان IP من DHCP
- **عنوان IP الحالي**
- **الرقم التسلسلي**

3. انقر نقرًا مزدوجًا فوق AMC في القائمة لتغيير معلماتها في نافذة منبثقة. أو حدد سطر AMC المطلوب وانقر فوق **الأجهزة/تكوين...** لاحظ أن إدخال كلمة مرور قد يكون ضروريًا في حال تم تكوين واحدة للجهاز.

يتم تخزين المعلمات المحددة عندما تنقر فوق "موافق" في النافذة المنبثقة.

4. عندما تنتهي من تكوين معلمات IP لوحدات التحكم، انقر فوق **ملف > خروج** لإغلاق الأداة. سوف تعود إلى التطبيق الرئيسي.

للحصول على معلومات أكثر تفصيلاً، انقر فوق **تعليمات** في الأداة **AMCIPConfig** لعرض ملف التعليمات الخاص بها.

9 استخدام محرر الجهاز

المقدمة

إن "محرر الجهاز" عبارة عن أداة لإضافة المداخل والأجهزة أو حذفها أو تعديلها.

يقدم "محرر الجهاز" طرق عرض للتدرجات الهرمية التالية القابلة للتحرير:

- **تكوين الجهاز**: الأجهزة الإلكترونية ضمن نظام التحكم في الوصول.
- **محطات العمل**: أجهزة الكمبيوتر التي تتعاون فيما بينها في نظام التحكم في الوصول.
- **المناطق**: المناطق الفعلية المقسّم إليها نظام التحكم في الوصول.

الشروط الأساسية

النظام مثبّت ومرخّص بشكل صحيح ويعمل على الشبكة.

مسار مربع الحوار

- **القائمة الرئيسية >التكوين > بيانات الجهاز**
- **مستعرض تكوين BIS > الاتصالات > بيانات الجهاز**

استخدام شريط أدوات محرر الجهاز

تقدم الأزرار على شريط أدوات "محرر الجهاز" الوظائف التالية، بصرف النظر عن طريقة العرض النشطة: **الأجهزة** أو **محطات العمل** أو **المناطق**.

الزر	الاختصار	الوصف
+	Ctrl + N	إنشاء عنصر جديد تحت العقدة المحددة. أو، انقر بزر الماوس الأيمن فوق العقدة لاستدعاء قائمة السياق الخاصة بها.
✕	Del	حذف العنصر المحدد وكل المحتويات تحته
⏮	Ctrl-Page up	العنصر الأول في الشجرة
◀	- Ctrl	العنصر السابق
▶	+ Ctrl	العنصر التالي
⏭	Ctrl-Page down	العنصر الأخير في الشجرة
	Ctrl-A	توسيع وطي الشجرة.
	Ctrl-K	تحديث البيانات عن طريق إعادة تحميلها من قاعدة البيانات. **يتم تجاهل جميع التغييرات غير المحفوظة.**
	Ctrl-S	حفظ التكوين الحالي
	Ctrl-F	فتح نافذة بحث
		فتح شجرة **تكوين الجهاز**

		فتح شجرة **محطات العمل**
		فتح شجرة **المناطق**

في جميع طرق عرض "محرر الجهاز"، ابدأ من جذر الشجرة وأضف العناصر باستخدام أزرار شريط الأدوات أو قائمة كل عنصر أو قائمة السياق لكل عنصر (انقر بزر الماوس الأيمن لاستدعائها). لإضافة عناصر فرعية إلى جهاز، حدد أولاً الجهاز الأصلي الذي يجب أن تظهر تحته العناصر الفرعية.

نسخ أجهزة AMC ولصقها

لنسخ أجهزة AMC من جزء في الشجرة إلى جزء آخر:

1. انقر بزر الماوس الأيمن فوق جهاز AMC، وحدد **نسخ** من قائمة السياق.
2. انقر بزر الماوس الأيمن فوق جهاز أصلي مناسب في أي مكان آخر في الشجرة، وحدد **لصق** من قائمة السياق.
   - يتم نسخ الجهاز إلى الموقع الجديد مع إعداداته وأجهزته الفرعية.
   - **لا** يتم نسخ معلمات الجهاز مثل **عنوان IP** و**الاسم**، الذي يجب أن تكون فريدة.
3. أدخل قيمًا فريدة لمعلمات الجهاز هذه التي تحتاج إليها. لن تتمكن من حفظ شجرة الجهاز حتى تقوم بذلك.

حفظ عملك

عندما تنتهي من إضافة العناصر إلى الشجرة وتعديلها، انقر فوق **حفظ** لحفظ التكوين.
لإغلاق "محرر الجهاز"، انقر فوق **ملف** > **خروج**.

9.1 أوضاع التكوين وتجاوزاته

وضع التكوين هو الحالة الافتراضية لأجهزة التحكم في الوصول في محرر الجهاز. في وضع التكوين، بإمكان أحد مستخدمي AMS أو BIS ACE المخوّلين إجراء تغييرات على الأجهزة في محرر الجهاز، ويقوم نظام ACS بنشر التغييرات على الأجهزة التابعة على الفور.
بإمكان المشغّل **تجاوز** وضع التكوين عن طريق إرسال الأوامر مباشرة للوصول إلى أجهزة التحكم من خارج محرر الجهاز. هذا أمر شائع، على سبيل المثال، عندما يتعامل المشغّل مع الرسائل الواردة والإنذارات.
وإلى أن يقوم المشغّل بإرسال أمر **استعادة التكوين**، يبقى الجهاز في وضع التشغيل .
إذا حدد مستخدم التكوين جهازًا في محرر الجهاز أثناء عمله في وضع التشغيل، فستعرض صفحة الخصائص الرئيسية للجهاز الإشعار.

10 تكوين مناطق التحكم في الوصول

مقدمة إلى المناطق

يمكن تقسيم المنشآت المؤَمَّنة إلى مناطق. وبإمكان المناطق أن تكون ذات مساحات مختلفة: مبنى واحد أو مبانٍ عديدة أو طوابق مفردة أو حتى غرف مفردة.

بعض استخدامات المناطق هي:

- حصر أفراد داخل المنشآت المؤَمَّنة.
- تقدير عدد الأشخاص داخل منطقة معينة، في حال إجراء عملية إخلاء طارئة.
- تقييد عدد الأشخاص أو السيارات في إحدى المناطق:
  عند الوصول إلى الحد الأقصى المحدد مسبقًا للكثافة، يمكن رفض إعطاء أذونات أخرى حتى يغادر الأشخاص أو السيارات المنطقة.
- تطبيق مراقبة تسلسل الوصول ومنع العودة

يميّز النظام بين نوعين من المناطق التي يتم التحكم في الوصول إليها

- مناطق للأشخاص
- مناطق للسيارات (ساحات الانتظار)

قد تتضمن كل منطقة مناطق فرعية لتمكين مراقبتها بشكل أكثر دقة. قد تتضمن المناطق المخصصة للأشخاص 3 مستويات من التداخل، فيما تتضمن ساحات الانتظار مستويين فقط، وتحديدًا ساحات الانتظار ومناطق الانتظار العامة، عددها بين 1 و24.

تسمى المنطقة الافتراضية، التي توجد في جميع عمليات التثبيت، **الخارج**. وتعمل هذه المنطقة كأساس لجميع المناطق التي يحددها المستخدم للنوعين معًا: المناطق المخصصة للأشخاص وساحات الانتظار.

لا تعتبر المنطقة قابلة للاستخدام إلا إذا كان الوصول إليها ممكنًا من خلال مدخل واحد على الأقل.

يمكن استخدام محرر الجهاز، **DevEdit**، لتعيين منطقة موقع ومنطقة وجهة لكل مدخل. عندما يجري أحد الأشخاص مسحًا ضوئيا لبطاقة في قارئ ينتمي إلى مدخل معين، يصبح الموقع الجديد لهذا الشخص منطقة الوِجهة لذلك المدخل.

إشعار!

يتطلب كل من مراقبة تسلسل الوصول ومنع العودة وجود قارئ دخول وخروج في مداخل المنطقة.

يوصى بشدة باستخدام مداخل من نوع الحواجز الدوارة لمنع قيام شخص "بتتبع شخص آخر بدنوّ خطر" عن طريق الخطأ أو عمدًا.

الإجراء الخاص بإنشاء المناطق

الشروط الأساسية

بصفتك مشغّل النظام، فأنت تحتاج إلى تخويل من مسؤول النظام لكي تتمكن من إنشاء المناطق.

مسار مربع الحوار (AMS)

1. في مدير مربع حوار AMS، حدد **القائمة الرئيسية** > **التكوين** > **بيانات الجهاز**
2. انقر فوق "المناطق"
3. حدد العقدة **الخارج**، أو إحدى العقد التابعة لها، وانقر فوق في شريط الأدوات. أو، انقر بزر الماوس الأيمن فوق **الخارج** لإضافة منطقة عبر قائمة السياق التابعة لها.
   تتلقى جميع المناطق التي يتم إنشاؤها اسم **منطقة** فريدًا بالإضافة إلى لاحقة رقمية.
4. حدد نوعها في النافذة المنبثقة، أي **منطقة** للأشخاص أو **ساحة انتظار** للسيارات.
   وحدها منطقة **الخارج** يمكنها أن تتضمن مناطق تابعة من النوعين. وترث أي منطقة فرعية لهذه المناطق التابعة نوع المنطقة الأصل.
   - تتداخل **المناطق** للأشخاص لغاية ثلاث مستويات. ويمكنك تحديد الحد الأقصى للكثافة لكل منطقة أو منطقة فرعية.

- تعتبر **ساحات الانتظار** كيانات افتراضية تتكوّن من **منطقة انتظار** واحدة على الأقل. إذا لم يكن من الضروري تقييد كثافة ساحة الانتظار بواسطة النظام، فسيظهر الرقم 0. بخلاف ذلك، فإن الحد الأقصى لأماكن صف السيارات لكل منطقة هو 9999، ويعرض الجزء الرئيسي لساحة الانتظار مجموع جميع الأماكن في مناطقه.

الإجراء الخاص بتحرير المناطق

1. انقر فوق منطقة في التدرج الهرمي لتحديدها.
2. اكتب فوق سمة أو أكثر من السمات التالية في الجزء الرئيسي من مربع الحوار.

الاسم	الاسم الافتراضي، الذي يمكنك الكتابة فوقه.
الوصف	وصف المنطقة باستخدام نص حر
الحد الأقصى لعدد الأشخاص/السيارات	القيمة الافتراضية 0 (صفر) لعدم وجود أي حد. أو يمكنك إدخال عدد صحيح للحد الأقصى للكثافة.

ملاحظات:

- لا يمكن نقل منطقة عن طريق السحب والإفلات في فرع آخر من التدرج الهرمي. يمكنك حذف المنطقة وإعادة إنشائها على فرع آخر، إذا لزم الأمر.
- حقل **القسم** للقراءة فقط في مربع الحوار هذا. لتغيير أقسام منطقة ما، استخدم مربع حوار **تعيين موضع الكاشفات** وحدد المنطقة في جزء **الأجهزة**.

الإجراء الخاص بحذف المناطق

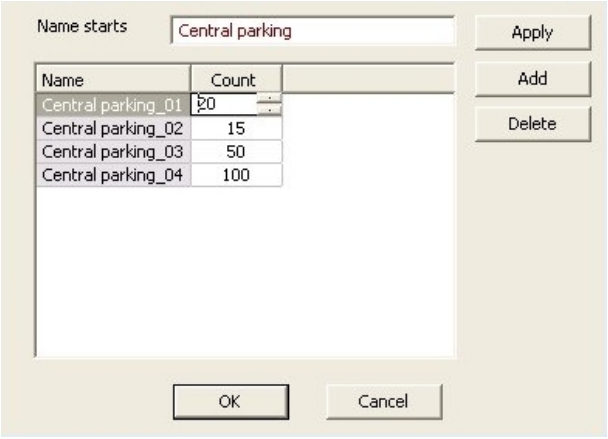
1. انقر فوق منطقة في التدرج الهرمي لتحديدها.
2. انقر **حذف** انقر بزر الماوس الأيمن لحذفها عبر قائمة السياق.

ملاحظة: لا يمكن حذف منطقة إلا بعد حذف جميع المناطق التابعة لها.

10.1 تكوين مناطق للسيارات

إنشاء مناطق للسيارات (ساحة انتظار، منطقة انتظار)

إذا حددت نوع المنطقة **ساحة انتظار**، تظهر نافذة منبثقة.



1. أدخل اسمًا في الحقل **الاسم يبدأ بـ** لإنشاء اسم رئيسي لجميع المناطق الفرعية لصف السيارات أو **مناطق الانتظار**.
   يمكن إنشاء ما يصل إلى 24 **منطقة انتظار** باستخدام الزر **إضافة** ، وستحمل كل منطقة الاسم الرئيسي بالإضافة إلى لاحقة من خانتين رقميتين.
2. إذا تعين على النظام تحديد الكثافة في هذه المناطق، فأدخل عدد أماكن صف السيارات في عمود **التعداد**. إذا لم يكن تقييد الكثافة ضروريًا، فأدخل 0.

ملاحظة: الحد الأقصى للكثافة في ساحة الانتظار بكاملها هو مجموع هذه الأرقام. وحدها مناطق صف السيارات يمكنها أن تحتوي على أماكن لصف السيارات؛ تعتبر **ساحة الانتظار** كيانًا افتراضيًا يتكوّن من **منطقة انتظار** واحدة على الأقل. الحد الأقصى لأماكن صف السيارات لكل منطقة هو 9999.

إنشاء مداخل لساحات الانتظار

تحتاج ساحات الانتظار إلى مداخل، مثلها مثل المناطق العادية. نموذج الباب المناسب هو **Parking lot 05c**.

لمراقبة الكثافة في ساحة انتظار، نحتاج إلى مدخلين مع نموذج الباب هذا على AMC نفسه، أحدهما للدخول والآخر للخروج.

الشرط الأساسي

إنشاء ساحة انتظار مع منطقة انتظار واحدة على الأقل، كما ورد أعلاه.

مسار مربع الحوار

القائمة الرئيسية > **التكوين** > **بيانات الجهاز**

انقر فوق **أجهزة LAC/المداخل/الأجهزة**

الإجراء

1. في التدرج الهرمي للجهاز، أنشئ AMC أو حدد AMC ليس لديه مداخل تابعة.
2. انقر بزر الماوس الأيمن فوق AMC وحدد **مدخل جديد**
3. في النافذة المنبثقة **مدخل جديد** حدد نموذج المدخل **Parking lot 05c** وأضف قارئًا على الجهة الداخلية من النوع المثبت في مدخل ساحة الانتظار.
4. انقر فوق **موافق** لإغلاق النافذ المنبثقة.
5. في التدرج الهرمي للجهاز، حدد هذا المدخل الذي أنشأته حديثًا.
   - لاحظ أن النظام قام بتعيين القارئ كقارئ دخول بشكل تلقائي.
6. في جزء التحرير الرئيسي، على علامة التبويب **Parking lot 05c**، حدد من القائمة المنسدلة **الوجهة** ساحة الانتظار التي أنشأتها في وقت سابق.
7. انقر بزر الماوس الأيمن من جديد فوق AMC، وأنشئ مدخلاً آخر من النوع **Parking lot 05c** كما ورد أعلاه.
   - هذه المرة يمكنك تحديد قارئ على الجهة الداخلية فقط.
   - انقر فوق **موافق** لإغلاق النافذ المنبثقة.
8. في التدرج الهرمي للجهاز، حدد هذا المدخل الثاني الذي أنشأته حديثًا.
   - لاحظ أن النظام قام بتعيين القارئ الثاني كقارئ خروج بشكل تلقائي.

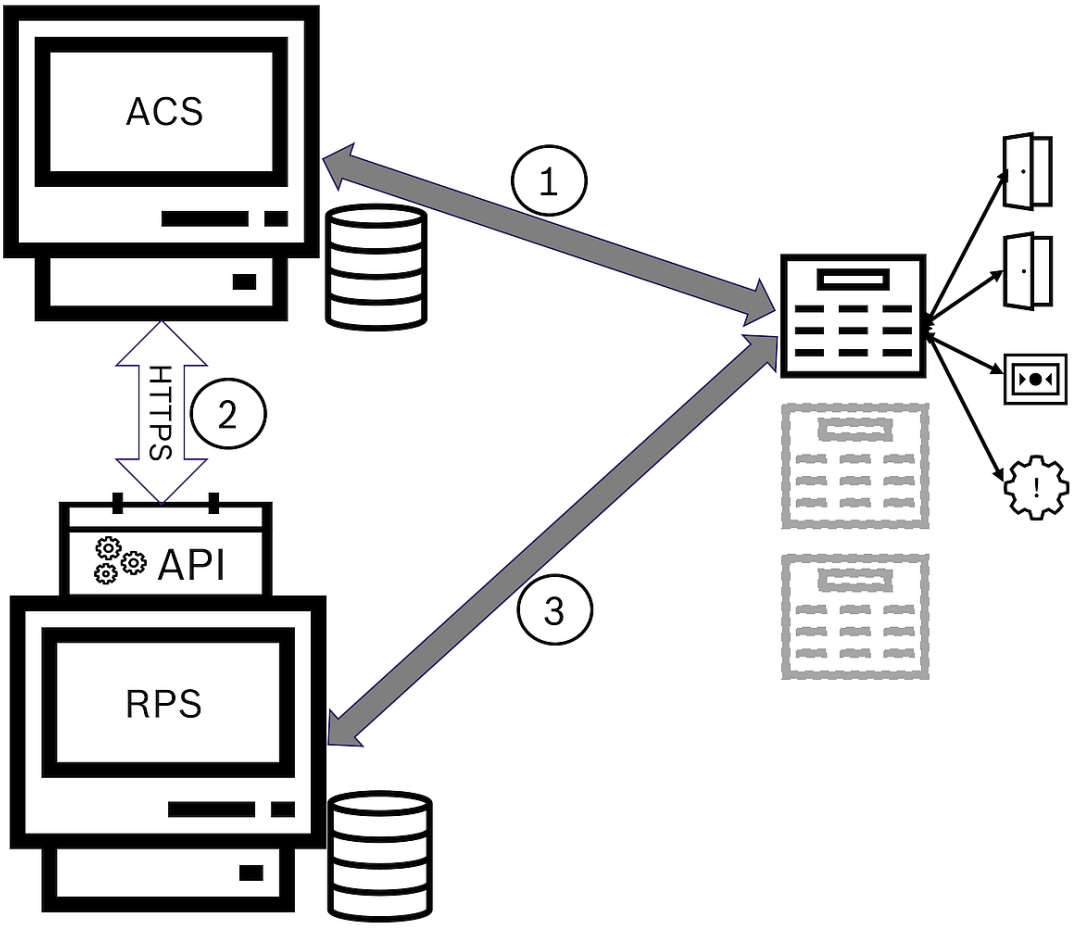
11 تكوين مناطق التسلل ولوحات كشف التسلل

المقدمة

يشارك نظام التحكم في الوصول إدارة وتشغيل لوحات كشف الاقتحام من Bosch. راجع ورقة بيانات نظام التحكم في الوصول للاطلاع على التفاصيل المتعلقة بالطُرز التي يدعمها. يضيف نظام التحكم في الوصول قيمة خاصة لعملية إدارة **مستخدمي** لوحات كشف الاقتحام. هؤلاء المستخدمون هم مجموعة فرعية من حاملي بطاقات نظام التحكم في الوصول الشامل. يمنح مسؤولو نظام التحكم في الوصول حاملي البطاقات تخويلات خاصة لتشغيل لوحات كشف الاقتحام عبر مدير الحوار في ACE.

يتم تكوين لوحات كشف الاقتحام بحد ذاتها وتحديثها كما في السابق من خلال برنامج البرمجة عن بُعد (RPS). يقرأ ACE بشكل مستمر البيانات من RPS، ويعرض اللوحات الموجودة فيها.

يحتوي ACE على مربعات حوار لإنشاء وتعيين ملفات تعريف التخويل، ولإدارة مستخدمي اللوحة على RPS.



الشكل التوضيحي 11.1: طبوغرافيا نظام الاقتحام المبسّط في ACS

ACS	نظام التحكم في الوصول الرئيسي: AMS أو BIS-ACE
API	واجهة برمجة التطبيقات
RPS	نظام البرمجة عن بُعد: تطبيق التحكم في لوحات الاقتحام
1	من ACS إلى اللوحة: أوامر اللوحة. من اللوحة إلى ACS: الأحداث من نقاط الاقتحام.
2	من ACS إلى RPS: بيانات حامل البطاقة
3	من RPS إلى اللوحة: إعدادات التكوين

الشروط الأساسية

- يتم تثبيت RPS للوحات الاقتحام المدعومة من Bosch على كمبيوتر منفصل مع اتصال شبكة بخادم ACE، **وليس** على خادم ACE نفسه. يمكنك مراجعة دليل تثبيت برنامج RPS للحصول على إرشادات التثبيت.
- تم تكوين برنامج RPS مع لوحات كشف الاقتحام التي ستنتمي إلى نظام التحكم في الوصول ACE. يمكنك مراجعة دليل مستخدم RPS أو التعليمات عبر الإنترنت للحصول على الإرشادات.
- تقع الساعات الموجودة على اللوحات على بُعد 100 يوم من الساعة على خادم ACE، لتمكين المزامنة التلقائية.
- تم تعيين بروتوكول الوضع 2 على جميع اللوحات المشاركة.
- بطاقات مع أحد التعريفات القياسية التالية للبطاقات:
  - HID 37 BIT <- Intrusion 37 BIT مع رمز منشأة/موقع من 32767 أو أقل.
  - HID 26 BIT- > Intrusion 26 BIT
  - EM 26 BIT- > Intrusion 26 BIT

نظرة عامة

تتكون عملية التكوين من المراحل التالية، التي ورد وصفها في الأقسام التالية من هذا الفصل:

1. تثبيت واجهة برمجة تطبيقات RPS للاقتحام على كمبيوتر RPS
2. توصيل نظام التحكم في الوصول بلوحات كشف الاقتحام.
   - تحديد الاتصال بواجهة برمجة تطبيقات RPS.
   - تكوين اتصالات اللوحة.
3. إنشاء ملفات تعريف تخويلات اللوحة التي تدير وظائف اللوحات المتصلة التي يمكن استخدامها.
4. تعيين ملفات تعريف تخويلات اللوحات لحاملي البطاقات.
   - وهكذا يتحوّل حامل البطاقة إلى مشغّل للوحات كشف الاقتحام.

11.1 تثبيت واجهة برمجة تطبيقات RPS للاقتحام على كمبيوتر RPS

واجهة برمجة تطبيقات RPS للاقتحام هي قناة الاتصال بين تطبيقات AMS وRPS على أجهزة الكمبيوتر الخاصة بها. يجب عليك أولاً تثبيت واجهة برمجة التطبيقات على كمبيوتر RPS، ثم تثبيت الشهادات التي ينشئها الإعداد على كمبيوتر AMS.

الإجراء

1. قم بتنفيذ ملف إعداد واجهة برمجة تطبيقات RPS وفقًا لوثائقه الخاصة.
   - يوجد ملف الإعداد ووثائقه على وسائط تثبيت AMS:
     `AddOns\Intrusion-RPS-API\Bosch_RPS_API_Setup_v*.exe`
     `AddOns\Intrusion-RPS-API\RPS-API_Application_note_v*.pdf`
   - يقوم برنامج الإعداد بإنشاء شهادتين وحفظهما على كمبيوتر RPS:
     `%AppData%\Roaming\Bosch_RPS_API\BoschRpsAPI.cer`
     `%AppData%\Roaming\Bosch_RPS_API\BoschRpsAPI.pfx` (يتطلب منك تعيين كلمة مرور)
2. انسخ ملفات الشهادتين إلى كمبيوتر AMS.
3. على كمبيوتر AMS، قم بتثبيت الشهادات إلى **موقع المتجر**: `Local Machine` و**مخزن الشهادات**: `Trusted Root Certification Authority`.

11.2 توصيل نظام التحكم في الوصول بلوحات كشف التسلل

المقدمة

يصف هذا القسم كيفية عرض لوحات كشف الاقتحام وجعلها متاحة للتحكم عبر ACE client. يتصل نظام التحكم في الوصول عبر واجهة برمجة التطبيقات بـ RPS على شبكته. من خلال واجهة برمجة التطبيقات، تحتفظ بقائمة داخلية محدثة لألواح الاقتحام المتوافقة المتوفرة.

هناك خطوتان ضروريتان في AMS لربطه بلوحات الاقتحام:

- الخطوة 1: تحديد الاتصال بواجهة برمجة تطبيقات RPS
- الخطوة 2: تكوين اتصالات اللوحة

مسار مربع الحوار

– القائمة الرئيسية > **التكوين** > **اللوحات** ومربعات الحوار الفرعية

11.2.1 الخطوة 1: تحديد الاتصال بواجهة برمجة تطبيقات RPS

في الخطوة 1، ستقدم لنظام التحكم في الوصول عنوان كمبيوتر RPS ومعلومات تسجيل دخول المسؤول.

مسار مربع الحوار

القائمة الرئيسية > **التكوين** > **اللوحات > تكوين RPS API**

الإجراء

1. أدخِل المعلومات التالية:

المعلومات	الوصف
اسم المضيف/عنوان IP	عنوان HTTPS للكمبيوتر حيث يتم تشغيل برنامج RPS، ورقم المنفذ الذي يتصل برنامج RPS من خلاله. استخدام `localhost` غير مسموح به. رقم المنفذ الافتراضي هو `9000`.
اسم المستخدم	اسم المستخدم لمستخدم مسؤول RPS لواجهة API.
كلمة المرور	كلمة مرور مستخدم مسؤول RPS.

2. انقر فوق الزر **اختبار الاتصال** للتأكد من أن برنامج RPS قيد التشغيل ومن صحة اسم المستخدم وكلمة المرور.
3. انقر فوق (حفظ) لحفظ التغييرات.

11.2.2 الخطوة 2: تكوين اتصالات اللوحة

في الخطوة 2، ستكوّن مقدار التحكم المتوفر لدى نظام التحكم في الوصول على لوحات فردية على الشبكة.

مسار مربع الحوار

القائمة الرئيسية > **التكوين** > **اللوحات > إدارة اللوحة**

يحافظ مربع الحوار على قائمة تتضمن لوحات كشف الاقتحام المتوافقة التي قامت واجهة API لبرنامج RPS بتزويد ACE بها.

يتم تحديث القائمة بشكل دوري في الخلفية. بعد فتح مربع الحوار، انقر فوق من وقت إلى آخر، لفرض عملية تحديث فوري يدويًا.

القائمة في وضع القراءة فقط، باستثناء ما يتعلق بعناصر التحكم التي سيرد وصفها في القسم التالي:

الإجراء

1. حدد لوحة من القائمة
2. استخدم عناصر التحكم أدناه لتحديد ما يمكن أن يفعله نظام التحكم في الوصول على لوحة الاقتحام المحددة.

عمود القائمة **إدارة المستخدمين**	حدد خانة الاختيار للتأكد من المحافظة على مستخدمي لوحة كشف الاقتحام في هذا الصف في نظام التحكم في الوصول و**ليس** على اللوحة بحد ذاتها. **مهم**: يتسبب هذا الإعداد في إزالة جميع مستخدمي اللوحة الذين تم إنشاؤهم محليًا في RPS.

عمود القائمة **Map View**	حدد خانة الاختيار لجعل هذه اللوحة متاحة للأمر والتحكم عبر ACE client.
أيقونة الإعدادات (cog) في عمود **بيانات الوصول**.	إذا قمت بتحديد خانة الاختيار في عمود **Map View**، فانقر فوق الأيقونة للدخول – عنوان IP – رقم منفذ (7700 افتراضي) – رمز المرور للوحة الفردية. تم تعيين رمز المرور في RPS.
الزر: **حذف اللوحة المحددة**	إذا تمت إزالة لوحة في برنامج RPS، فستظهر في القائمة وستكون حالتها **تمت إزالتها**. حدد اللوحة وانقر فوق هذا الزر لحذفها بشكل تام من قاعدة البيانات.

11.3 إنشاء ملفات تعريف تخويلات اللوحات

المقدمة

يصف هذا القسم كيفية إنشاء ملفات تعريف تخويلات اللوحات.

إن ملف تعريف تخويل اللوحة عبارة عن مجموعة مخصصة من التخويلات لتشغيل مجموعة مخصصة من لوحات كشف الاقتحام. بإمكان مسؤول ACE إنشاء ملفات تعريف متعددة لتخويلات اللوحات لمسؤوليات مختلفة لمجموعات مختلفة من حاملي البطاقات.

مسار مربع الحوار

– القائمة الرئيسية > **بيانات النظام** > **ملفات تعريف التخويلات للوحات كشف الاقتحام**

الإجراء

1. انقر فوق لإنشاء ملف تعريف جديد
2. (إلزامي) أدخل اسمًا لملف التعريف
3. (اختياري) أدخل وصفًا للوحة يكون عبارة عن نص حر
4. تحت قائمة **اللوحات المعيّنة**، انقر فوق **إضافة...** لإضافة لوحة أو أكثر من قائمة منبثقة تتضمن اللوحات المتوفرة على الشبكة.
   في المقابل، حدد لوحة أو أكثر، وانقر فوق **إزالة** لإزالتها من القائمة.
5. انقر فوق لوحة في قائمة **اللوحات المعيّنة** لتحديدها.
   – في جزء **التخويلات**، تظهر قائمة تتضمن جميع مناطق التسلل التي تنتمي إلى اللوحة المحددة.
6. في قائمة **التخويلات**، في العمود **مستوى التخويل**، حدد مستوى تخويل لكل منطقة تسلل في اللوحة التي يجب تضمينها في ملف التعريف هذا.
   – يتم تحديد مستويات التخويل والمحافظة عليها في RPS. ويمكن أيضًا تخصيصها هناك. تأكد من أنك على اطلاع على تعريف مستوى التخويل في RPS، قبل تعيينه إلى ملف تعريف.
   – بشكل افتراضي، يعتبر **L1** مستوى التخويل الأعلى، مع تقييد متزايد للمستويات **L2** و**L3** وغيرها.
   – إذا تركت خلية فارغة، فإن مستلم ملف التعريف هذا **لن** يحصل على تخويل على منطقة التسلل المحددة في اللوحة المحددة.
7. كرر هذه العملية لجميع مناطق التسلل في جميع اللوحات التي يجب تضمينها في ملف التعريف هذا.
8. (اختياري) من قائمة **مجموعة المستخدمين**، حدد مجموعة مستخدمي اللوحة لتقييد التخويلات بحيث تقتصر على فترات زمنية محددة.
   – يتم تحديد مجموعات المستخدمين والمحافظة عليها في RPS. ويمكن أيضًا تخصيصها هناك. تأكد من أنك على اطلاع على تعريف مجموعة المستخدمين في RPS، قبل تعيين مجموعة المستخدمين إلى ملف تعريف.
9. انقر فوق (حفظ) لحفظ التغييرات.

11.4 تعيين ملفات تعريف تخويلات اللوحات لحاملي البطاقات

المقدمة

يشرح هذا القسم كيفية تعيين ملفات تعريف تخويلات لوحات مختلفة لأنواع أو مجموعات مختلفة من حاملي البطاقات.

الشرط الأساسي

لقد قمت بتعريف ملف تعريف تخويل لوحة أو أكثر في نظام التحكم في الوصول.

مسار مربع الحوار

القائمة الرئيسية > **الأشخاص** > **البطاقات**

الإجراء

1. ابحث عن حامل البطاقة المطلوب من قاعدة البيانات وحدده، باستخدام الطريقة العادية.
2. انقر فوق علامة تبويب **التسلل**.
3. على علامة تبويب **التسلل**، حدد خانة الاختيار **مستخدم اللوحة**.
4. (إلزامي) في حقل **رمز المرور**، اكتب رمز مرور يقوم حامل البطاقة هذا من خلاله بتشغيل لوحات كشف التسلل.
   – استخدم الزر لإنشاء رمز مرور جديد غير مستخدم، إذا لزم الأمر.
5. في قائمة **بطاقة التعريف**، حدد بيانات اعتماد التحكم في الوصول المعينة إلى حامل البطاقة هذا.
6. في حقل **عدد أجهزة التحكم عن بُعد**، أدخل الرقم المطبوع على جهاز التحكم عن بعد الخاص بحامل البطاقة للوحات الكشف عن التسلل.
7. في قائمة **اللغة**، حدد اللغة المفضلة لدى حامل البطاقة لقراءة مربعات حوار اللوحات.
8. إذا كان حامل البطاقة سيستخدم تطبيق الهواتف الذكية من Bosch للوحات التسلل، فحدد خانة الاختيار **الوصول عن بُعد**.
9. من قائمة **ملف تعريف التخويل**، حدد ملف تعريف تخويل لوحة يكون ملائمًا لحامل البطاقة.
10. انقر فوق (حفظ) لحفظ التغييرات.
    – يتم تعيين ملف تعريف تخويل اللوحة هذا، مع جميع لوحاته وتخويلاته، إلى حامل البطاقة. وهكذا يتحوّل حامل البطاقة إلى مشغّل للوحات كشف التسلل.

لاحظ أنه يمكنك استخدام حقول البيانات على مربع الحوار هذا مع الزر للبحث عن حاملي البطاقات في قاعدة البيانات.

11.5 التحكم في الأبواب من خلال وحدات B901 على لوحات الاقتحام

في AMS 4.0.1 والإصدارات الأحدث، يمكن التحكم في وحدات واجهة التحكم في الوصول B901 عبر Map View في AMS.

B901 عبارة عن وحدة تحكم بسيطة في الباب يقوم مسؤول النظام بتوصيلها بلوحات الاقتحام من Bosch. قم بتوصيل لوحة الاقتحام المقابلة بـ AMS كما هو موضح في الأقسام السابقة.

لم تقم بتكوين B901 في محرر الجهاز.

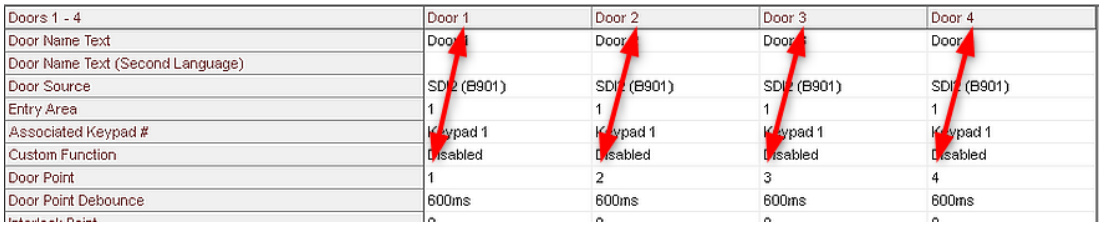
يمكن لـ B901 قفل/فتح، وتأمين/إلغاء تأمين، وتدوير الأبواب، لكنه يوفر معلومات حالة محدودة لنظام التحكم في الوصول. على سبيل المثال، لا يوضح ما إذا كان الباب قد تم فتحه فعليًا أم لا.

مثل جميع أجهزة الاقتحام الأخرى، من أجل إرسال أوامر إلى B901 من Map View في AMS، يجب عليك تمكين Map View للوحة المقابلة في مربع حوار AMS:

القائمة الرئيسية > **التكوين** > **اللوحات > إدارة اللوحة**

مؤشر تمرير Map View وأبواب B901

لتقديم المعلومات الصحيحة إلى تطبيق **مؤشر التمرير** في Map View في AMS، يجب أن تتطابق معرفات أبواب B901 مع معرفات نقاط الأبواب الخاصة بها. وهذا يعني أنه يجب تعيين الباب 1 لنقطة الباب 1، والباب 2 لنقطة الباب 2 وما إلى ذلك.



Doors 1 - 4	Door 1	Door 2	Door 3	Door 4
Door Name Text	Door 1	Door 2	Door 3	Door 4
Door Name Text (Second Language)				
Door Source	SDI2 (B901)	SDI2 (B901)	SDI2 (B901)	SDI2 (B901)
Entry Area	1	1	1	1
Associated Keypad #	Keypad 1	Keypad 1	Keypad 1	Keypad 1
Custom Function	Disabled	Disabled	Disabled	Disabled
Door Point	1	2	3	4
Door Point Debounce	600ms	600ms	600ms	600ms

قم بإجراء هذه التعيينات لوحدة التحكم في الباب B901 في أداة RPS التي تقوم بتكوين لوحات الاقتحام ووحدات التحكم.

12 تكوين المشغّلين ومحطات العمل

مقدمة إلى حقوق إدارة التحكم في الوصول

تحدد حقوق الوصول لنظام التحكم في الوصول مربعات حوار النظام التي قد تكون مفتوحة، والوظائف التي يُحتمل تنفيذها هناك.

يمكن تعيين الحقوق إلى كل من المشغّلين ومحطات العمل.

قد تقوم حقوق محطة عمل بتقييد حقوق مشغّليها بشكل مؤقت، إذ يجب تنفيذ العمليات الأمنية الحرجة فقط من محطات عمل شديدة الأمان.

يتم تعيين الحقوق إلى كل من المشغّلين ومحطات العمل في مجموعات تسمى **ملفات تعريف**. ويتم تخصيص كل ملف تعريف وفق مهام خاصة بنوع معين من أنواع المشغّلين أو محطات العمل.

قد تتوفر لدى كل مشغّل أو محطة عمل ملفات تعريف تخويل متعددة.

الإجراء الشامل ومسارات الحوار

1. أنشئ محطات العمل في محرر الجهاز:

التكوين > **بيانات الجهاز** > **محطات العمل**
2. أنشئ ملفات تعريف محطة العمل في محرر الجهاز:
المشغّلون ومحطات العمل > **ملفات تعريف محطة العمل**.
3. عيّن ملفات التعريف إلى محطات العمل:
المشغّلون ومحطات العمل > **حقوق محطة العمل**.
4. أنشئ ملفات تعريف المشغّلين في محرر الجهاز:
المشغّلون ومحطات العمل > مربع الحوار **ملفات تعريف المستخدم**.
5. عيّن ملفات التعريف إلى المشغّلين في مربع الحوار:
المشغّلون ومحطات العمل > مربع الحوار **حقوق المستخدم**.

12.1 إنشاء محطات العمل

محطات العمل هي أجهزة الكمبيوتر التي يقوم المشغّلون من خلالها بتشغيل نظام التحكم في الوصول. يجب أولاً "إنشاء" محطة عمل، أي الكمبيوتر المسجل ضمن نظام التحكم في الوصول.

مسار مربع الحوار

التكوين > **بيانات الجهاز** > **محطات العمل**

الإجراء

1. انقر بزر الماوس الأيمن فوق **DMS** وحدد **كائن جديد** من قائمة السياق، أو انقر فوق ✚ على شريط الأدوات.
2. أدخل قيمًا للمعلمات.
- يجب أن يتطابق **اسم** محطة العمل مع اسم الكمبيوتر بشكل تام.
- يعتبر **الوصف** اختياريًا. يمكن استخدامه، على سبيل المثال، لوصف وظيفة محطة العمل وموقعها.
- **تسجيل الدخول عبر القارئ** اترك خانة الاختيار هذه غير محددة إلا إذا كان يجب على المشغّلين تسجيل الدخول إلى محطة العمل هذه عن طريق تقديم بطاقات إلى قارئ تسجيل متصل بمحطة العمل هذه. لمزيد من التفاصيل، راجع القسم
- **تسجيل الخروج التلقائي بعد وقت عدم النشاط:** عدد الثواني الذي بعده يتم إنهاء جلسة تسجيل الدخول عبر قارئ التسجيل بشكل تلقائي. يمكنك ترك هذا الإعداد معيّنًا إلى 0 للإشارة إلى وقت غير محدد.

12.2 إنشاء ملفات تعريف محطة العمل

مقدمة إلى ملفات تعريف محطة العمل

يجب تكوين محطة عمل للتحكم في الوصول بشكل متأنٍ فيما يتعلق باستخدامها، استنادًا إلى موقعها الفعلي، على سبيل المثال:

- المشغّلون الذين قد تستخدمهم محطة العمل
- بيانات الاعتماد الضرورية لاستخدامها
- مهام التحكم في الوصول التي يمكن تنفيذها منها

يُعتبر ملف تعريف محطة العمل مجموعة من الحقوق التي تحدد ما يلي:

- قوائم مدير مربع الحوار ومربعات الحوار التي يمكن استخدامها في محطة العمل.
- ملف (ملفات) التعريف الذي يجب أن يكون متوفرًا لدى المشغّل لتسجيل الدخول إلى محطة العمل هذه.

إشعار!

ملفات تعريف محطة العمل تتجاوز ملفات تعريف المستخدم
بإمكان المشغّل استخدام فقط حقوق ملف تعريف المستخدم المضمّنة أيضًا في ملف تعريف محطة العمل للكمبيوتر حيث سجل دخوله. إذا لم يكن لدى محطة العمل والمشغّل أي حقوق مشتركة، فسيفتقد المستخدم لجميع الحقوق في محطة العمل هذه.

مسار مربع الحوار

التكوين > **المشغّلون ومحطات العمل** > **ملفات تعريف محطة العمل**

إنشاء ملف تعريف محطة العمل

1. انقر فوق لإنشاء ملف تعريف جديد
2. أدخل اسمًا لملف التعريف في الحقل **اسم ملف التعريف** (إلزامي)
3. أدخل وصفًا لملف التعريف في حقل **الوصف** (اختياري ولكن مستحسن)
4. انقر فوق أو **تطبيق** لحفظ تغييراتك

تعيين حقوق التنفيذ لوظائف النظام

1. في قائمة **الوظائف**، حدد الوظائف التي يجب أن يكون الوصول إليها ممكنًا في محطة العمل هذه، ثم انقر نقرًا مزدوجًا فوقها لتعيين القيمة في العمود **تنفيذ** إلى `Yes`.
   - تأكد أيضًا من أن الوظائف التي يجب ألا يكون الوصول إليها ممكنًا معيّنة إلى `No`.
2. انقر فوق أو **تطبيق** لحفظ تغييراتك

تعيين ملفات تعريف المستخدم إلى ملفات تعريف محطة العمل

في جزء **ملفات تعريف المستخدم**:

تحتوي قائمة **ملفات التعريف المعيّنة** على جميع ملفات التعريف المصرح لها تسجيل الدخول إلى محطة عمل باستخدام ملف تعريف محطة العمل هذا.

يحتوي حقل **ملفات التعريف المتاحة** على جميع ملفات التعريف الأخرى. وهذه غير مصرح لها بعد تسجيل الدخول إلى محطة عمل باستخدام ملف تعريف محطة العمل هذا.

1. انقر فوق أزرار الأسهم بين القوائم لنقل ملفات التعريف المحددة من قائمة إلى أخرى.
2. انقر فوق أو **تطبيق** لحفظ تغييراتك

إشعار!
لا يمكن حذف أو تغيير ملفات تعريف المسؤول الافتراضية للمستخدم (**مسؤول UP**) ومحطة العمل (**مسؤول WP**).
يرتبط ملف التعريف **WP-Administrator** بطريقة غير قابلة للإلغاء بمحطة عمل الخادم. وهذا يضمن وجود مستخدم واحد على الأقل يمكنه تسجيل الدخول إلى محطة عمل الخادم.

12.3 تعيين ملفات تعريف محطة العمل

استخدم مربع الحوار هذا لإدارة تعيينات ملفات تعريف محطة العمل إلى محطة العمل. يجب أن يكون لدى كل محطة عمل ملف تعريف محطة عمل واحدًا على الأقل. وإذا كان لديها ملفات تعريف متعددة، فستنطبق جميع الحقوق الموجودة في ملفات التعريف هذه.

مسار مربع الحوار
التكوين > **المشغّلون ومحطات العمل** > **حقوق محطة العمل**

الإجراء
تحتوي قائمة **ملفات التعريف المعيّنة** على جميع ملفات تعريف محطة العمل التي تعود إلى محطة العمل هذه.
تحتوي قائمة **ملفات التعريف المتاحة** على جميع ملفات تعريف محطة العمل التي لم يتم تعيينها بعد إلى محطة العمل هذه.

1. في قائمة محطات العمل، حدد محطة العمل التي تريد تكوينها.
2. انقر فوق أزرار الأسهم بين قوائم ملفات التعريف **المعيّنة** و**المتاحة** لنقل ملفات التعريف المحددة من قائمة إلى أخرى.
3. انقر فوق أو **تطبيق** لحفظ تغييراتك

إشعار!
لا يمكن حذف أو تغيير ملفات تعريف المسؤول الافتراضية للمستخدم (**مسؤول UP**) ومحطة العمل (**مسؤول WP**).
يرتبط ملف التعريف **WP-Administrator** بطريقة غير قابلة للإلغاء بمحطة عمل الخادم. وهذا يضمن وجود مستخدم واحد على الأقل يمكنه تسجيل الدخول إلى محطة عمل الخادم.

12.4 إنشاء ملفات تعريف المستخدم (المشغّل)

مقدمة إلى ملفات تعريف المستخدم
ملاحظة: التعبير **مستخدم** هو مرادف للتعبير **مشغّل** في سياق حقوق المستخدم.
يُعتبر ملف تعريف المستخدم مجموعة من الحقوق التي تحدد ما يلي:
- قوائم مدير مربع الحوار ومربعات الحوار التي يستطيع المشغّل رؤيتها.
- القدرات المتوفرة للمشغّل في مربعات الحوار هذه، وبشكل أساسي حقوق تنفيذ وتغيير وإضافة وحذف عناصر مربعات الحوار هذه.

يجب تكوين ملفات تعريف المستخدم بطريقة متأنية، بحسب خبرة الشخص والإذن الأمني الممنوح له ومسؤولياته.

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

الإجراء

1. انقر فوق لإنشاء ملف تعريف جديد
2. أدخل اسمًا لملف التعريف في الحقل **اسم ملف التعريف** (إلزامي)

3. أدخل وصفًا لملف التعريف في حقل **الوصف** (اختياري ولكن مستحسن)
4. انقر فوق أو **تطبيق** لحفظ تغييراتك

إشعار!
اختر أسماء ملفات تعريف تصف بشكل واضح ودقيق قدرات وقيود ملف التعريف.

إضافة حقوق التحرير والتنفيذ لوظائف النظام
1. في جزء القائمة، حدد الوظائف (العمود الأول) والقدرات ضمن تلك الوظيفة (**التنفيذ** و**التغيير** و**الإضافة** و**الحذف**) التي يمكن لملف التعريف هذا الوصول إليها. انقر نقرًا مزدوجًا فوقها لتبديل إعداداتها إلى Yes.
   - تأكد أيضًا من أن الوظائف التي يجب ألا يكون الوصول إليها ممكنًا معيّنة إلى No.
2. انقر فوق أو **تطبيق** لحفظ تغييراتك

12.5 تعيين ملفات تعريف المستخدم (المشغّل)

ملاحظة: التعبير **مستخدم** هو مرادف للتعبير **مشغّل** في سياق حقوق المستخدم.

الشروط الأساسية
- تم تعريف المشغّل الذي سيتلقى ملف تعريف المستخدم هذا **كشخص** في نظام التحكم في الوصول.
- تم تعريف ملف تعريف مستخدم ملائم في نظام التحكم في الوصول.
- لاحظ أنه من الممكن دائمًا تعيين ملف تعريف مستخدم غير مقيّد **مسؤول UP**، ولكن تم استبعاد هذه الممارسة لأسباب أمنية.

مسار مربع الحوار
التكوين > **المشغّلون ومحطات العمل** > **حقوق المستخدم**

الإجراء
1. قم بتحميل سجل الموظف للمستخدم المطلوب في مربع الحوار.
2. حدد صلاحية ملف تعريف المستخدم عن طريق إدخال البيانات في الحقلين **صالح من** و**صالح حتى**.

تعيين ملفات تعريف المستخدم إلى المشغّلين
في جزء **ملفات تعريف المستخدم**:
تحتوي قائمة **ملفات التعريف المعيّنة** على جميع ملفات تعريف المستخدم التي لم يتم تعيينها بعد إلى هذا المستخدم.
يحتوي حقل **ملفات التعريف المتاحة** على جميع ملفات التعريف المتوفرة لتعيينها.

1. انقر فوق أزرار الأسهم بين القوائم لنقل ملفات التعريف المحددة من قائمة إلى أخرى.
2. حدد خانة الاختيار **مسؤول عمومي** لمنح هذا المشغّل حق الوصول للقراءة والكتابة إلى سجلات الموظفين هذه حيث تم تنشيط السمة **إدارة عمومية**. الحق الافتراضي لوصول المشغّل إلى سجلات الموظفين هذه هو للقراءة فقط.
3. انقر فوق لحفظ تغييراتك.

تعيين حقوق استخدام API إلى المشغّلين

بإمكان كود البرنامج الخارجي، إذا تم تكوينه وترخيصه، استدعاء ميزات نظام التحكم في الوصول عبر واجهة برمجة التطبيقات أو API. يعمل البرنامج الخارجي عبر مشغّل وكيل ضمن النظام. تتحكم عناصر تحكم القائمة المنسدلة **استخدام API** بقدرات المشغّل الحالي إذا تم استخدامه كمشغّل وكيل من قبل الكود الخارجي.

التكوين > **المشغّلون ومحطات العمل** > **حقوق المستخدم**

– حدد إعدادًا من قائمة **استخدام API**.
الاختيارات هي:

لا يمكن الوصول	لا يمكن استخدام المشغّل من قِبل واجهة برمجة التطبيقات (API) لتنفيذ وظائف النظام.
للقراءة فقط	يمكن استخدام المشغّل من قِبل واجهة برمجة التطبيقات (API) لقراءة بيانات النظام، ولكن ليس لإضافتها أو تعديلها أو حذفها.
غير محدود	يمكن استخدام المشغّل من قِبل واجهة برمجة التطبيقات (API) لقراءة بيانات النظام وإضافتها وتعديلها وحذفها.

– انقر فوق لحفظ تغييراتك

12.6 تعيين كلمات مرور المشغّلين

كيفية تعيين كلمات مرور آمنة لنفسك وللآخرين.

المقدمة

يحتاج النظام إلى وجود مشغّل واحد على الأقل. يحمل المشغّل الافتراضي في تثبيت جديد اسم المستخدم **Administrator** وكلمة المرور **Administrator**. يجب أن تكون دائمًا الخطوة الأولى في تكوين النظام تسجيل الدخول باستخدام بيانات الاعتماد هذه وتغيير كلمة مرور **المسؤول**، وفقًا لسياسات كلمات المرور المتبعة في شركتك.

بعد ذلك، يمكنك إضافة مشغّلين، مع أو بدون امتيازات.

الإجراء الخاص بتغيير كلمة المرور الخاصة بك.

الشروط الأساسية

سجّلت دخولك إلى مدير مربع الحوار.

الإجراء

1. في مدير الحوار، حدد القائمة: **ملف** > **تغيير كلمة المرور**
2. في النافذة المنبثقة، أدخل كلمة المرور الحالية وكلمة المرور الجديدة ثم كلمة المرور الجديدة مرة أخرى لتأكيدها.
3. انقر فوق **تغيير**.

يعتبر هذا الإجراء الطريقة الوحيدة لتغيير كلمة مرور المسؤول.

الإجراء الخاص بتغيير كلمات مرور المشغّلين الآخرين.

الشروط الأساسية

لتغيير كلمات مرور مستخدمين آخرين، يجب تسجيل الدخول إلى مدير مربع الحوار باستخدام حساب يتمتع بامتيازات المسؤول.

الإجراء

1. في القائمة الرئيسية لمدير مربع الحوار، انتقل إلى **التكوين** > **المشغّلون ومحطات العمل** > **حقوق المستخدم**
2. في جزء الحوار الرئيسي، استخدم شريط الأدوات لتحميل المشغّل الذي تريد تغيير كلمة مروره.
3. انقر فوق **تغيير كلمة المرور**.
4. في النافذة المنبثقة، أدخل كلمة المرور الجديدة وكلمة المرور الجديدة مرة أخرى لتأكيدها.
5. في النافذة المنبثقة، أدخل فترة صلاحية كلمة المرور الجديدة، إما **غير محددة** أو عددًا من الأيام.

– بالنسبة إلى بيئات الإنتاج، من الضروري تعيين فترة صلاحية.

6. انقر فوق **موافق** لإغلاق النافذ المنبثقة.

في نافذة مربع الحوار الرئيسي، انقر فوق أيقونة لحفظ سجل المستخدم.

لاحظ أن منتقيات التاريخ **صالح من** و**صالح حتى**، تحت زر **تغيير كلمة المرور...**، تشير إلى صلاحية حقوق المستخدم في مربع الحوار هذا، وليس كلمة المرور.

معلومات إضافية

اعتمد دائمًا سياسة كلمات المرور المتبعة في مؤسستك لتعيين كلمات المرور. للحصول على إرشادات حول إنشاء مثل هذه السياسة يمكنك مراجعة، على سبيل المثال، الإرشادات التي توفرها شركة Microsoft في الموقع التالي.
/https://www.microsoft.com/en-us/research/publication/password-guidance

13 تكوين البطاقات

13.1 تعريف البطاقة

استخدم مربع الحوار هذا لتنشيط تعريفات البطاقات التي يجب أن يستخدمها نظام التحكم في الوصول أو إلغاء تنشيط هذه التعريفات أو تعديلها أو إضافتها.

مسار مربع الحوار

- مستعرض التكوين > **البنية الأساسية** > **تعريف بطاقة ACE**
- القائمة الرئيسية AMS > **التكوين** > **خيارات** > **تعريف البطاقة**

يتم تزويد النظام بمجموعة من أنواع البطاقات المحددة مسبقًا. تظهر أنواع البطاقات المحددة مسبقًا مع خلفية رمادية في الجدول **أنواع البطاقات المتوفرة** ولا يمكن تعديلها. يمكن نقلها فقط بين **أنواع البطاقات النشطة** و**أنواع البطاقات المتوفرة**.

13.1.1 أنواع البطاقات النشطة

أنواع البطاقات النشطة هي تلك الأنواع التي تتعرّف عليها أجهزة قراء البطاقات في نظام التحكم في الوصول وتعالجها. يصل عدد تعريفات البطاقات التي يمكنها أن تكون نشطة في الوقت نفسه إلى 8 في نظام واحد باستثناء بطاقات CEPAS.

إن بطاقات CEPAS هي نوع من البطاقات الحصرية. وبالتالي، عند استخدام بطاقات CEPAS، لا يمكن تنشيط أي أنواع من البطاقات الأخرى.

بالنسبة إلى أجهزة القراءة المزودة ببروتوكول L-Bus أو BG900، يجب إضافة إدخال القائمة **أجهزة القراءة التسلسلية** تحت **أنواع البطاقات النشطة** في مستعرض التكوين (**البنية الأساسية** > **تعريف بطاقة ACE**) لجعل مربع حوار قناع الإدخال اليدوي (Bosch) متوفرًا في Access Engine لإدخال بيانات البطاقات يدويًا.

13.1.2 الإنشاء والتعديل

انقر فوق الزر ✚ (+ أخضر) فوق مربع القائمة إلى اليسار لإنشاء إدخال قائمة جديد. بشكل مغاير لأنواع البطاقات المعرّفة مسبقًا، تعتبر بيانات الأنواع المُنشأة حديثًا قابلة للتحرير بشكل كامل. انقر نقرًا مزدوجًا فوق حقول **الاسم** و**الوصف** و**عدد وحدات البت** لتحريرها.

بإمكان الاسم أن يتكوّن من 80 حرفًا والوصف من 255 حرفًا كحد أقصى. عدد وحدات البت محدد بـ 64 (إذا تم إدخال عدد أكبر، فسيعاد تعيينه إلى الحد الأقصى فور أن يفقد النص التركيز على الإدخال).

إشعار!

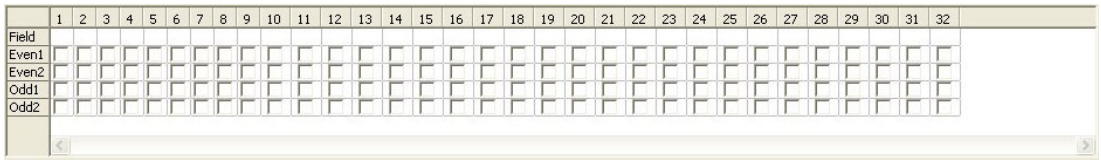
يُستخدم طول البت للتميز بين تعريفات Wiegand. وبالتالي، يلزم وجود طول بت فريد لكل تعريف جديد لم يستخدمه تعريف سابق.

- لتعديل بت بيانات، انقر نقرًا مزدوجًا فوق الحقل ذي الصلة. لحذف بت البيانات، حدده أولاً ثم انقر فوق الزر ✕ (x أحمر).

إشعار!

لا يمكن تعديل أو حذف سوى أنواع البطاقات التي أنشأها المستخدم.

عند تحديد نوع بطاقة واحد (في القوائم إلى أقصى اليمين أو أقصى اليسار)، سيظهر ترميزه في الجزء السفلي من مربع الحوار. تعرض الشاشة وحدات بت البيانات في 5 صفوف، وعدد من الأعمدة يساوي عدد وحدات البت في التعريف.



يمكن إعطاء كل عمود في صف **الحقل** تسمية تحدد كيفية تفسير هذا الجزء من الكود. التسميات المتوفرة هي التالية:

F	المنشأة: وضع علامة على جزء الكود لارتباط المنشأة	
C	رقم الكود: جزء الكود الذي يحتوي على رقم البطاقة الفردية	
E1	زوجي 1: بت لموازنة قناع التماثل الزوجي الأول	يؤدي إقرار هذه القيم إلى تنشيط خانة الاختيار للسطر المناظر.
E2	زوجي 2: بت لموازنة قناع التماثل الزوجي الثاني	
O1	فردي 1: بت لموازنة قناع التماثل الفردي الأول	
O2	فردي 2: بت لموازنة قناع التماثل الفردي الثاني	
1	إصلاح قيم البت الموجودة في الكود	
0		

فيما يتعلق بالتسميات E1 وE2 وO1 وO2، يكفي تحديد خانة الاختيار على الصف المناظر. سيتم تمييز المربع على صف **الحقل** بشكل تلقائي وفقًا لذلك.

التفسير

تتكوّن الإشارة التي يرسلها القارئ عند تقديم بطاقة له من مجموعة من أرقام صفر وواحد. لكل نوع بطاقة، يكون طول هذه الإشارة (أي عدد وحدات البت) محددًا بدقة.

بالإضافة إلى بيانات المستخدم الفعلية، المحفوظة كبيانات الكود، تحتوي الإشارة أيضًا على بيانات تحكم من أجل أ) تعريف الإشارة كإشارة بطاقة وب) التحقق من الإرسال الصحيح.

بشكل عام، تعتبر أرقام الصفر والواحد الثابتة مفيدة لتعريف نوع الإشارة.

تُستخدم وحدات بت التماثل، التي يجب أن تسفر عن صفر (تماثل زوجي) أو واحد (تماثل فردي) كمجموع اختباري على وحدات البت المحددة للإشارة، للتحقق من الإرسال الصحيح. يمكن تكوين وحدات التحكم بحيث تحسب مجموعًا اختباريًا واحدًا أو مجموعين اختباريين للتماثل الزوجي أو مجموعًا اختباريًا واحدًا أو مجموعين اختباريين للتماثل الفردي.

في عنصر تحكم القائمة، يمكن وضع علامة على وحدات البت هذه في الأسطر الخاصة بالمجاميع الاختبارية للتماثل (Even1 وEven2 وOdd1 وOdd2) التي يجب تضمينها في المجموع الاختباري. في السطر العلوي (الحقل) لكل مجموع اختباري مستخدم، يتم تعريف بت لموازنة المجموع الاختباري وفقًا لنوع التماثل. إذا لم يتم استخدام خيار تماثل، فقد يبقى السطر المناظر فارغًا.

13.1.3 تنشيط / إلغاء تنشيط تعريفات البطاقات

يصل عدد تعريفات البطاقات التي يمكنها أن تكون نشطة في الوقت نفسه إلى 8، باستثناء بطاقات CEPAS. يجب نقل التعريفات المراد تنشيطها إلى القائمة اليمنى **أنواع البطاقات النشطة**. يمكن القيام بذلك عن طريق تحديد تعريف أو أكثر (تحديد متعدد) على الجانب الأيسر، والنقر فوق زر السهم إلى اليسار (**>**).

يمكن نقل ثمانية تعريفات فقط مرة واحدة. عند وضع ثمانية تعريفات في مكانها، يتم التخلص من أي تعريفات زائدة من عملية النقل. لإضافة المزيد من التعريفات إلى **أنواع البطاقات النشطة**، سيكون من الضروري حذف تعريف أو أكثر من التعريفات الموجودة عن طريق تحديدها (تحديد متعدد) ونقلها إلى الجانب الأيسر باستخدام الزر (**<**)، وبالتالي إلغاء تنشيطها.

إشعار!
لاستخدام أجهزة القراءة المزودة ببروتوكول L-Bus أو BG900، يجب تنشيط نوع البطاقة **قارئ تسلسلي**. يؤدي ذلك إلى جعل مربع الإدخال اليدوي **Dialog Bosch** متوفرًا لمدير الحوار في نظام التحكم في الوصول.

13.1.4 إنشاء بيانات البطاقة في مدير الحوار

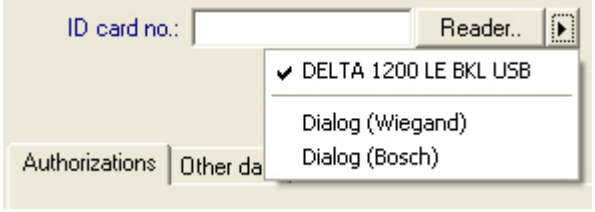
الإدخال اليدوي للبيانات
تُستخدم أساليب إدخال مختلفة لبطاقات Wiegand وBosch.
فيما يتعلق بجميع تعريفات Wiegand (26 HID و35 HID و37 HID و32 Bit CSN)، يسمح لك مربع الحوار **Dialog (Wiegand)** بإدخال **كود العميل** و**رقم البطاقة**.
فيما يتعلق بأجهزة القراءة التسلسلية، يحتوي مربع الحوار **Dialog (Bosch)** على حقول إضافية لكل من **الإصدار** و**كود البلد**.

إدخال البيانات بواسطة قارئ تسجيل
بالإضافة إلى الإدخال اليدوي للبيانات، يمكن تزويد أي محطة عمل بقارئ للحوار لجمع بيانات البطاقات.
استخدم أي قارئ من القائمة في مربع الحوار التالي.
- مستعرض التكوين > **البنية الأساسية** > **قارئ بطاقة ACE**
- القائمة الرئيسية AMS > **التكوين** > **خيارات** > **قارئ البطاقة**

إذا كان القارئ الذي اخترته قارئ إدخالات بطاقات Wiegand، فستكون جميع أنواع بطاقات Wiegand النشطة مدرجة مع القارئ.
- Access Engine > **بيانات الموظفين** > **البطاقات** > زر القارئ > ▶ (سهم إلى اليمين).
- القائمة الرئيسية AMS > **بيانات الموظفين** > **البطاقات** > زر القارئ > ▶ (سهم إلى اليسار).

يجب تحديد أحد أنواع البطاقات هذه للتأكد من حفظ ترميز البطاقات بشكل صحيح. وهذا يعني أنه يتعذر تحديد القارئ بحد ذاته بشكل مباشر بل فقط بشكل غير مباشر عبر اختيار تعريف Wiegand.
إذا لم يظهر نوع البطاقة المطلوب في القائمة المنسدلة، فيجب عليك تنشيطه في مربع حوار تعريف البطاقة.
- مستعرض التكوين > **البنية الأساسية** > **تعريف بطاقة ACE**
- القائمة الرئيسية AMS > **التكوين** > **خيارات** > **تعريف البطاقة**

يمكن تحديد أجهزة قراءة التسجيل HITAG وLEGIC وMIFARE من القائمة بشكل مباشر.



13.2 تكوين رموز البطاقات

يضمن ترميز بطاقات التحكم في الوصول تميّز بيانات جميع البطاقات.

مسار مربع الحوار
القائمة الرئيسية > التكوين > خيارات > تكوين ترميز البطاقة
إدخال الأرقام في مربع الحوار
إدخال الأرقام في مربع الحوار
لتسهيل الأمر، يمكنك إدخال الأرقام بالتنسيق العشري أو الست عشري. حدد الزر التبادلي **ست عشري** أو **عشري** وفقًا للتنسيق المحدد بواسطة الشركة المصنّعة للبطاقة.
تم تقسيم جزء مربع الحوار الرئيسي إلى مجموعتين، يرد وصفهما أدناه بشكل مفصل:
- **بيانات رمز البطاقة الافتراضية**
- **تحقق من قيم العضوية فقط**

بيانات رمز البطاقة الافتراضية
استخدم حقول إدخال النص هذه لتعيين قيم **الإصدار** و**رمز البلد** و**رمز المنشأة**، التي تم تعيينها إلى رقم البطاقة عند تسجيل البطاقة في النظام. إذا لم تكن الحقول قابلة للكتابة، فهذا يعني أنها غير ملائمة لأي من تعريفات البطاقات النشطة. بالنسبة إلى كود Bosch، جميع الحقول قابلة للكتابة.
إذا تم تسجيل البطاقة يدويًا في محطة عمل المشغّل، فسيظهر عندئذٍ مربع حوار يعرض القيم الافتراضية التي يمكن تخصيصها لكل بطاقة.

إدخال بيانات الرمز:
إذا قامت الشركة المصنّعة بتوفير البيانات كقيم عشرية، فحدد الزر التبادلي "عشري" وأدخل القيم المتوفرة، على سبيل المثال:
الإصدار: 2
رمز البلد: 99
رمز المنشأة: 56720
انقر فوق **تطبيق** لتخزين البيانات.

ملاحظات حول إدخال بيانات الرمز الافتراضية:
يتم تخزين البيانات الافتراضية في سجل نظام التشغيل، ويُضاف كل رقم بطاقة تعريف في وقت الترميز.
يتخذ التسجيل شكل قيمة **ست عشرية من 8 خانات رقمية** مع أصفار بادئة، كما تقتضي الحاجة.
إذا تم نقل أرقام الرموز بشكل تام، فقد يقوم النظام بالتحويل من القيم العشرية إلى الست عشرية، ويقوم بتعبئة 8 منازل بأصفار بادئة ويحفظ معلمة النظام المناسبة.
- مثال:
  - المدخل: 56720
  - التحويل: DD90
  - محفوظ على الشكل: 0000DD90

إذا تم نقل أرقام الرموز بشكل منفصل (نموذج مقسّم)، ففي هذه الحالة وفقط في النموذج **العشري**، يتم تحويلها إلى رقم عشري من 10 خانات رقمية، على الشكل التالي.
- الإصدار: خانتان رقميتان
- رمز البلد: خانتان رقميتان
- رمز المنشأة: 6 خانات رقمية
- إذا بقيت أي واحدة من الخانات الرقمية العشر فارغة، فستتم تعبئتها بالأصفار البادئة.

- مثال: 0299056720

يتم تحويل هذه القيمة العشرية المكونة من 10 خانات رقمية وتخزينها كقيمة ست عشرية مكونة من 8 خانات رقمية.

- مثال:
  - القيمة العشرية: 0299056720
  - القيمة الست عشرية: 11D33E50

إشعار!
يتحقق النظام من القيم الست عشرية، في حال وجود أرقام رموز مقسّمة، لمنع إدخال رموز بلدان غير صالحة (أعلى من القيمة الست عشرية 63 أو القيمة العشرية 99) أو رموز منشآت غير صالحة (أعلى من القيمة الست عشرية F423F أو القيمة العشرية 999,999)

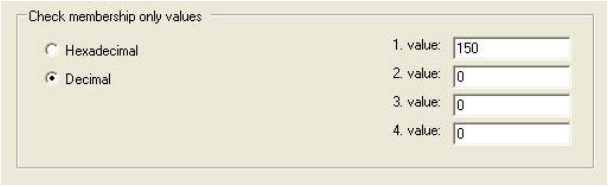
إشعار!
إذا حدث التقاط البطاقة عبر قارئ حوار متصل، فسيتم عندئذٍ تعيين القيم الافتراضية بشكل تلقائي. من غير الممكن تجاوز القيم الافتراضية عند الالتقاط من قارئ.
للقيام بذلك، يجب تبديل نوع الالتقاط إلى **حوار**

الإدخال اليدوي لرقم البطاقة هو بالتنسيق الشعري.
عند حفظ البيانات، يتم إنشاء قيمة عشرية مكونة من 10 خانات رقمية (مع أصفار بادئة)، يتم تحويلها عندئذٍ إلى قيمة ست عشرية من 8 خانات رقمية. تم الآن تخزين هذه القيمة مع بيانات الرمز الافتراضية كرقم رمز البطاقة من 16 خانة رقمية.

- مثال:
  - إدخال رقم البطاقة: 415
  - 10 خانات رقمية: 0000000415
  - محوّل إلى قيمة ست عشرية: 0000019F
  - مجمّع مع بيانات الرمز الافتراضية (انظر أعلاه) ومحفوظ كرقم رمز بطاقة التعريف: 11D33E500000019F

تحقق من قيم العضوية فقط
يعني التحقق من العضوية فقط أنه يتم التحقق من بيانات الاعتماد لعضوية شركة أو مؤسسة فقط، وليس للتعرّف على الأفراد. وبالتالي، لا تستخدم الخيار **تحقق من العضوية فقط** لأجهزة القراءة التي تمنح حق الوصول إلى مناطق ذات مستوى أمان عالٍ.

استخدم مجموعة الخيارات هذه لإدخال ما يصل إلى أربعة رموز شركات أو عملاء. يمكن إدخال البيانات كعشرية أو ست عشرية، ولكن يتم تخزينها كقيم عشرية في سجل نظام التشغيل.



حدد القارئ في محرر الجهاز، DevEdit، وقم بتنشيط معلمة القارئ **تحقق من العضوية**.
تتم قراءة رموز الشركات أو العملاء فقط ضمن بيانات البطاقة ويتم التحقق منها في مقابل القيم المخزنة.

إشعار!
يعمل الخيار **تحقق من العضوية** فقط مع تعريفات البطاقة المعرّفة بشكل مسبق في النظام (خلفية رمادية)، وليس مع التعريفات المخصصة.

14 تكوين وحدات التحكم

المقدمة

تعتبر وحدات التحكم في نظام التحكم في الوصول الأجهزة الافتراضية والفعلية التي ترسل الأوامر إلى الأجهزة الطرفية في المداخل (أجهزة القراءة والأبواب)، وتعيد إرسال الطلبات من أجهزة القراءة والأبواب إلى البرنامج المركزي المسؤول عن اتخاذ القرارات.

تقوم وحدات التحكم بتخزين نُسخ بعض المعلومات من جهاز البرنامج المركزي وحاملي البطاقات، ويمكنها اتخاذ قرارات تتعلق بالتحكم في الوصول، إذا تم تكوينها للقيام بذلك، حتى عندما تكون معزولة بشكل مؤقت عن البرنامج المركزي.

البرنامج المسؤول عن اتخاذ القرارات هو نظام إدارة البيانات .

هناك نوعان من وحدات التحكم:

- وحدة التحكم في الوصول الرئيسية، وتُعرف باسم MAC، ووحدة التحكم في الوصول المكررة والداعمة لها RMAC .
- وحدات التحكم في الوصول المحلية، والتي تُعرف باسم LAC أو AMC.

يتم تكوين وحدات التحكم في محرر الجهاز، DevEdit.

مسار الحوار إلى محرر الجهاز

القائمة الرئيسية > **التكوين** > **بيانات الجهاز** > **شجرة الأجهزة**

استخدام محرر الجهاز، DevEdit

يمكن العثور على وصف للاستخدام الأساسي لمحرر الجهاز، DevEdit، في القسم **استخدام محرر الجهاز**، في الارتباط أدناه.

راجع

- استخدام محرر الجهاز, الصفحة *22*

14.1 تكوين MAC وRMAC

14.1.1 تكوين إعدادات الوصول العمومي لـ MAC

في علامة التبويب **إعدادات الوصول العمومي**، يمكن تعيين قيم المعلمات التالية:

- عامل الوقت للأشخاص ذوي الاحتياجات الخاصة.
- الحد الزمني لوصول المجموعة.
- الحد الزمني لإدخال لوحة مفاتيح المستويات.
- الوقت الذي تنتهي بعده المدة المسموحة لبقاء شخص ما في منطقة ما.

لتعيين المعلمات، اتبع مسار الحوار التالي:

القائمة الرئيسية > التكوين > بيانات الجهاز > شجرة الأجهزة > MAC > DMS > إعدادات الوصول العمومي

لمزيد من المعلومات حول استخدام محرر الجهاز، راجع استخدام محرر الجهاز, الصفحة *22*.

ضع في اعتبارك المعلمات التالية:

- **عامل الوقت للأشخاص ذوي الاحتياجات الخاصة:**
  - يتم ضرب القيمة "الحد الأقصى لمدة النبض حتى طرق الباب" في هذا العامل (الأبواب->علامة التبويب: الخيارات).
  - لتمييز شخص ما كشخص من ذوي الاحتياجات الخاصة.

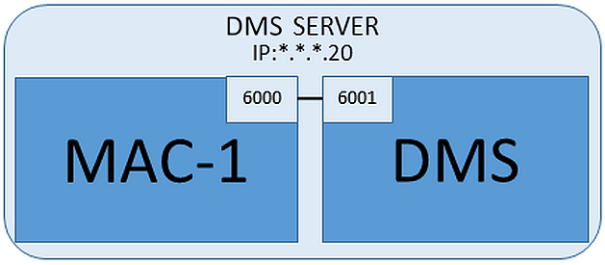
- **الحد الزمني لوصول المجموعة:**
  - الحد الأقصى للوقت حتى تتم قراءة البطاقة التالية لوصول المجموعة.
  - القيمة 0 -> إيقاف الحد الزمني (الوقت اللانهائي).

- **الحد الزمني لإدخال لوحة المفاتيح:**
  - الحد الأقصى لوقت الإدخال على القارئ لكل رقم. (إذا كان لديك رقم تعريف شخصي (PIN) مكون من 4 أرقام وتم تعيين قيمة الحد الزمني على 50 [عشر الثانية] فلديك 20 ثانية (4 مرات 5 ثوانٍ) للإدخال. لن يكون الأمر مختلفًا إذا انتظرت أكثر من 5 ثوانٍ بين رقمين، طالما أن إجمالي وقت الإدخال لا يتجاوز 20 ثانية (قيم المثال مع رقم تعريف شخصي (PIN) مكون من 4 أرقام ووقت إدخال لوحة المفاتيح هو 50 (عشر الثانية)).
  - القيمة 0 -> إيقاف الحد الزمني (الوقت اللانهائي).

- **الوقت الذي تنتهي بعده المدة المسموحة لبقاء شخص ما في منطقة ما:**
  - 0 = تعطيل وظيفة فحص البطاقة (سيبقى الشخص في منطقة ما يجري حجزًا لدى قارئ في منطقة أخرى) -> لا يوجد حد زمني، لا يوجد حجز تلقائي للخارج.
  - يمكن اختيار قيمة بين 0 و168.
  - 1-168: الوقت بالساعات حتى يتم تعيين الشخص بالخارج، إذا لم تكن هناك حجوزات لهذا الشخص لذلك الوقت.
  - سيؤدي اختيار القيمة 0 إلى تعيين وقت البقاء في المنطقة إلى لانهائي.

راجع
- استخدام محرر الجهاز, الصفحة *22*

14.1.2 تكوين جهاز MAC على خادم DMS



فيما يتعلق بالحد الأدنى من متطلبات تكوين النظام، يجب أن يتوفر جهاز MAC واحد. وفي هذا الحالة، باستطاعة MAC أن يقيم على خادم DMS.

الإجراء

على خادم DMS، افتح محرر الجهاز وأنشئ MAC في شجرة الأجهزة، كما ورد في القسم استخدام محرر الجهاز, الصفحة *22*.

حدد MAC في محرر الجهاز. على علامة التبويب **MAC**، قدّم قيم المعلمات التالية:

المعلمة	الوصف
الاسم	الاسم الذي يجب أن يظهر في شجرة الأجهزة، على سبيل المثال MAC-1.
الوصف	وصف اختياري يستفيد منه مشغّلو النظام
مع RMAC (خانة اختيار)	**<اتركه فارغًا>**
منفذ RMAC	**<اتركه فارغًا>**
نشط (خانة اختيار)	**امسح** خانة الاختيار هذه لإيقاف المزامنة في الوقت الحقيقي بشكل مؤقت بين MAC هذا وDMS. يعتبر هذا الأمر مفيدًا بعد تحديثات DMS على الأنظمة الكبيرة الحجم، من أجل تجنب إعادة بدء تشغيل جميع وحدات MAC مرة واحدة.
تحميل الأجهزة (خانة اختيار)	**امسح** خانة الاختيار هذه لإيقاف المزامنة في الوقت الحقيقي بشكل مؤقت بين وحدة MAC هذه والأجهزة التابعة لها.

المعلمة	الوصف
	يؤدي ذلك إلى تقصير الوقت المطلوب لفتح جهاز MAC في محرر الجهاز.
عنوان IP	`Localhost 127.0.0.1`
المنطقة الزمنية	**مهم:** المنطقة الزمنية لجهاز MAC وجميع أجهزة AMC التابعة له.
القسم	(إذا انطبق الأمر) القسم الذي ينتمي إليه جهاز MAC.

نظرًا لعدم وجود جهاز MAC متكرر لتجاوز الفشل لدى جهاز MAC هذا، فمن غير الضروري تشغيل الأداة MACInstaller له. ما عليك سوى ترك معلمتي RMAC على علامة التبويب **MAC** فارغتين.

14.1.3 إعداد أجهزة كمبيوتر خوادم MAC لتشغيل أجهزة MAC وRMAC

يصف هذا القسم كيفية إعداد أجهزة الكمبيوتر كي تصبح خوادم MAC.

بشكل افتراضي، تعمل وحدة التحكم في الوصول (MAC) الأولى في نظام تحكم في الوصول على الكمبيوتر نفسه الذي يعمل عليه خادم إدارة البيانات (DMS)، ومع ذلك، ولتمكين المرونة المحسّنة، من المستحسن أن يتم تشغيل MAC على كمبيوتر منفصل، يمكنه أداء مهام التحكم في الوصول إذا حدث عطل ما في كمبيوتر DMS.

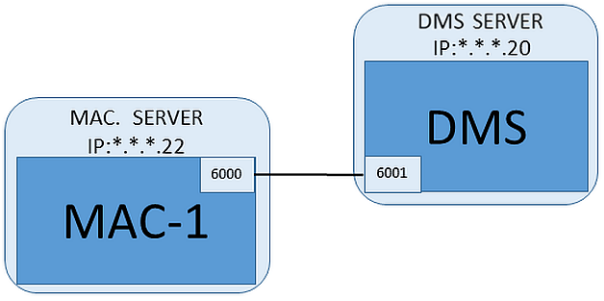
تُعرف أجهزة الكمبيوتر المنفصلة حيث تقيم أجهزة MAC أو RMAC بخوادم MAC، بصرف النظر عن استضافتها جهاز MAC أو RMAC.

من أجل توفير إمكانية تجاوز الفشل، يجب تشغيل أجهزة MAC وRMAC **على** خوادم MAC منفصلة.

تأكد من استيفاء الشروط التالية على جميع خوادم MAC المشاركة:

1. يجب أن تكون أنظمة التشغيل الخاصة بجميع خوادم MAC مدعومة حاليًا من قِبل Microsoft، ويجب أن تكون التحديثات الأخيرة مثبتة فيها.
2. المستخدم المسؤول على جميع الخوادم يستخدم كلمة المرور نفسها
3. سجلت دخولك بصفة مسؤول (إذا كنت تستخدم MSTC، فاستخدم فقط /Admin /Console sessions)
4. تعطيل IP V6. دوّن بتأنٍ عنوان IP V4 لكل خادم.
5. تمكين NET 3.5. على جميع أجهزة الكمبيوتر المشاركة.
   ملاحظة: في نظامي التشغيل Windows 10 وWindows Server، يتم تمكين هذا البرنامج كميزة.
6. أعد تمهيد الكمبيوتر.

14.1.4 تكوين جهاز MAC على خادم MAC الخاص به



- تم إعداد كمبيوتر خادم MAC كما ورد في القسم

1. على كمبيوتر خادم DMS، في محرر الجهاز،
   - انقر بزر الماوس الأيمن فوق MAC وحدد **تعطيل جميع وحدات LAC**
   - قم بإلغاء تنشيط MAC من خلال مسح خانتي الاختيار **تنشيط** و**تحميل الأجهزة** لوحدة MAC هذه.
2. على كمبيوتر خادم MAC، باستخدام برنامج Windows `services.msc`
   - أوقف تشغيل خدمة MAC **AUTO_MAC2**

- عيّن **نوع بدء التشغيل** لخدمة MAC هذه إلى **يدوي**.

3. ابدأ تشغيل `MACInstaller.exe`
   - بالنسبة إلى ACE، يمكن العثور على هذه الأداة في وسائط تثبيت BIS `\AddOns\ACE\MultiMAC\MACInstaller` (راجع القسم, استخدام الأداة MACInstaller أدناه).
   - بالنسبة إلى AMS، يمكن العثور على هذه الأداة في وسائط تثبيت AMS `\AddOns\MultiMAC\MACInstaller` (راجع القسم, استخدام الأداة MACInstaller أدناه).
4. تنقل عبر شاشات الأداة، وقدّم القيم للمعلمات التالية.

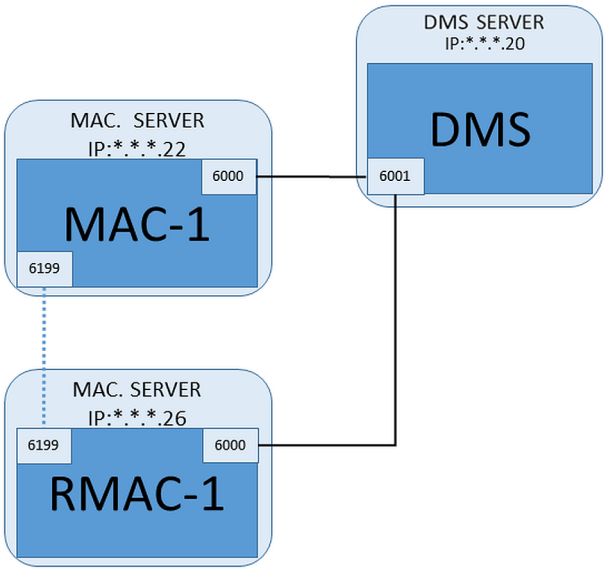
رقم الشاشة	المعلمة	الوصف
3	**مجلد الوجهة**	الدليل المحلي حيث يجب تثبيت جهاز MAC. استخدم الدليل الافتراضي، متى أمكن.
4	**الخادم**	اسم أو عنوان IP للخادم حيث يجري تشغيل DMS.
4	**المنفذ (منفذ إلى DMS)**	المنفذ على خادم DMS الذي سيتم استخدامه لتلقي المراسلات من جهاز MAC**.** استخدم 6001 لجهاز MAC الأول على خادم DMS، مع زيادته بمقدار 1 لكل جهاز MAC آخر.
4	**الرقم (رقم نظام MAC)**	عيّن هذا الرقم إلى 1 لوحدة MAC هذه ولجميع وحدات MAC (بشكل مغاير لوحدات RMAC)**.**
4	**المثيل (اسم أو عنوان IP لوحدة MAC الشريكة)**	اترك هذا الحقل فارغًا طالما كان من غير الضروري أن يكون لوحدة MAC هذه وحدة RMAC.

5. على خادم DMS، حدد MAC في محرر الجهاز.
6. على علامة التبويب **MAC**، قدّم قيم المعلمات التالية:

المعلمة	الوصف
الاسم	الاسم الذي يجب أن يظهر في شجرة الأجهزة، على سبيل المثال MAC-1.
الوصف	وصف اختياري يستفيد منه مشغّلو النظام
مع RMAC (خانة اختيار)	**<اتركه فارغًا>**
منفذ RMAC	**<اتركه فارغًا>**
نشط (خانة اختيار)	حدد خانة الاختيار هذه الآن
تحميل الأجهزة (خانة اختيار)	حدد خانة الاختيار هذه الآن
عنوان IP	عنوان IP لكمبيوتر خادم MAC.
المنطقة الزمنية	**مهم:** المنطقة الزمنية لوحدة MAC وجميع وحدات AMC التابعة لها.
القسم	(إذا انطبق الأمر) **القسم** الذي تنتمي إليه وحدة MAC.

14.1.5 إضافة RMAC إلى MAC

إشعار!
لا تقم بإضافة أجهزة RMAC إلى أجهزة MAC عادية حتى يتم تثبيت أجهزة MAC العادية وتبدأ عملها بشكل صحيح.
بخلاف ذلك، قد يتم منع عملية تكرار البيانات أو إلحاق الضرر بها.



- تم تثبيت جهاز MAC لجهاز RMAC هذا كما ورد في الأقسام السابقة، وهو يعمل بشكل صحيح.
- تم إعداد كمبيوتر خادم MAC لجهاز RMAC كما ورد في القسم

يمكن إقران أجهزة MAC مع أجهزة MAC متكررة (RMAC) لتوفير إمكانية تجاوز الفشل، وبالتالي تمكين المزيد من المرونة للتحكم في الوصول. وفي هذه الحالة، يتم إجراء نسخ متماثل لبيانات التحكم في الوصول بشكل تلقائي بين الجهازين. إذا فشل أحد الجهازين، فسيتمكن الآخر من التحكم في وحدات التحكم في الوصول المحلية التابعة له.

على خادم DMS، في مستعرض التكوين

1. في محرر الجهاز، حدد وحدة MAC الذي يجب إضافة RMAC لها.
2. على علامة التبويب **MAC**، غيّر قيم المعلمات التالية:

المعلمة	الوصف
مع RMAC (خانة اختيار)	**امسح** خانة الاختيار هذه حتى تنتهي من تثبيت RMAC المناظر على خادم الاتصال المتكرر لتجاوز الفشل.
نشط (خانة اختيار)	**امسح** خانة الاختيار هذه لإيقاف المزامنة في الوقت الحقيقي بشكل مؤقت بين MAC هذا وDMS. يعتبر هذا الأمر مفيدًا بعد تحديثات DMS على الأنظمة الكبيرة الحجم، من أجل تجنب إعادة بدء تشغيل جميع وحدات MAC مرة واحدة.
تحميل الأجهزة (خانة اختيار)	**امسح** خانة الاختيار هذه لإيقاف المزامنة في الوقت الحقيقي بشكل مؤقت بين وحدة MAC هذه والأجهزة التابعة لها. يؤدي ذلك إلى تقصير الوقت المطلوب لفتح وحدة MAC في محرر الجهاز.

3. انقر فوق الزر **تطبيق**.
4. اترك محرر الجهاز مفتوحًا، إذ قد نعود إليه حاليًا.

على خادم MAC لجهاز RMAC

لتكوين RMAC، اتبع الخطوات التالية:

- على كمبيوتر خادم MAC المنفصل الخاص به والذي تم إعداده في وقت سابق، قم بتشغيل الأداة MACInstaller (راجع استخدام الأداة MACInstaller) وعيّن المعلمات التالية:
  - **الخادم**: اسم أو عنوان IP لكمبيوتر خادم DMS.
  - **المنفذ**: 6001 (هو نفسه منفذ MAC)
  - **الرقم**: 2 (جميع وحدات RMAC تحمل الرقم 2)

– **مزدوج**: عنوان IP للكمبيوتر حيث يتم تشغيل MAC المثيل.

على خادم DMS، عد إلى محرر الجهاز

1. **مهم:** تأكيد من تشغيل كل من MAC وRMAC، على أجهزة الكمبيوتر الخاصة بهما، ومن أنه باستطاعة كل جهاز رؤية الجهاز الآخر على الشبكة.
2. على علامة التبويب **MAC**، غيّر المعلمات على الشكل التالي:

المعلمة	الوصف
مع RMAC (خانة اختيار)	**محدد** تظهر علامة تبويب جديدة مسماة **RMAC** إلى جانب علامة التبويب **MAC**.
منفذ RMAC	6199 (الافتراضي الثابت) تستخدم جميع وحدات MAC وRMAC هذا المنفذ للتأكد من أن شركاءها فيد التشغيل ويمكن الوصول إليهم.
نشط (خانة اختيار)	**محدد** يمكّن هذا المزامنة بين وحدة MAC هذه والأجهزة التابعة لها.
تحميل الأجهزة (خانة اختيار)	**محدد** يؤدي ذلك إلى تقصير الوقت المطلوب لفتح وحدة MAC في محرر الجهاز.

3. على علامة التبويب **RMAC**، قدّم قيم المعلمات التالية:

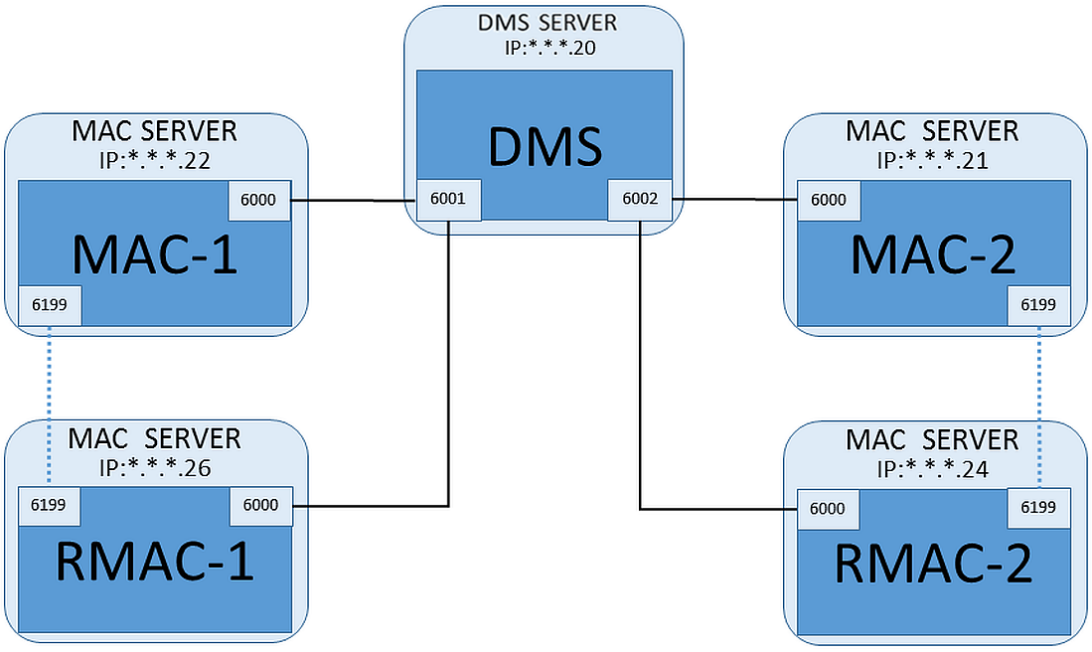
المعلمة	الوصف
الاسم	الاسم الذي يجب أن يظهر في شجرة الأجهزة. على سبيل المثال، إذا كان اسم وحدة MAC المناظرة MAC-01، فسيكون اسم RMAC هذا RMAC-01.
الوصف	وثائق اختيارية لمشغّلي التحكم في الوصول.
عنوان IP	عنوان IP لوحدة RMAC.
منفذ MAC	6199 (الافتراضي الثابت) تستخدم جميع وحدات MAC وRMAC هذا المنفذ للتأكد من أن شركاءها فيد التشغيل ويمكن الوصول إليهم.

راجع

– استخدام أداة تثبيت *MAC*, الصفحة *50*

14.1.6 إضافة المزيد من أزواج MAC/RMAC

يمكن إضافة عدد كبير من أزواج MAC/RMAC إلى تكوين النظام، وهذا يتوقف على عدد المداخل التي يجب مراقبتها ودرجة التسامح مع الخطأ المطلوبة. لمعرفة العدد الدقيق الذي يدعمه الإصدار الذي تستخدمه، يُرجى مراجعة ورقة البيانات المناظرة.



لكل زوج MAC/RMAC إضافي...

1. قم بإعداد أجهزة كمبيوتر منفصلة لكل من MAC وRMAC كما ورد في القسم
2. قم بإعداد MAC كما ورد في القسم
3. قم بإعداد RMAC لجهاز MAC هذا كما ورد في القسم

يرسل كل زوج MAC/RMAC الإشارات إلى منفذ مستقل على خادم DMS. وبالتالي، من أجل المعلمة **منفذ (منفذ إلى DMS)** في `MACInstaller.exe`، استخدم:

- `6001` لجهازي الكمبيوتر في زوج MAC/RMAC الأول
- `6002` لجهازي الكمبيوتر في زوج MAC/RMAC الثاني
- وغير ذلك

في منفذ محرر الجهام، يمكن دائمًا استخدام المنفذ `6199` للمعلمتين **منفذ MAC** و**منفذ RMAC**. ويكون رقم المنفذ هذا محجوزًا من أجل "تأكيد الاتصال" ضمن كل زوج MAC/RMAC، حيث يعلم كل واحد إن كان الوصول ممكنًا إلى شريكه أم لا.

إشعار!
إعادة تنشيط أجهزة MAC بعد ترقيات النظام
بعد إجراء ترقية النظام، يتم إلغاء تنشيط أجهزة MAC وأجهزة AMC المناظرة لها بشكل افتراضي. تذكّر ضرورة إعادة تنشيطها في مستعرض التكوين عن طريق تحديد خانات الاختيار في محرر الجهاز.

14.1.7 استخدام أداة تثبيت MAC

إن `MACInstaller.exe` هي الأداة القياسية لتثبيت وحدات MAC وRMAC على أجهزة الكمبيوتر الخاصة بها (خوادم MAC). وتقوم هذه الأداة بجمع قيم المعلمات لوحدة MAC أو RMAC، وتدخل التغييرات الضرورية في تسجيل Windows.

إشعار!
نظرًا لقيام الأداة بإدخال تغييرات على تسجيل Windows، من الضروري إيقاف أي عملية MAC قيد التشغيل قبل إعادة تكوينها.

يمكن العثور على الأداة MACInstaller في وسائط التثبيت ضمن المسار التالي:

- \AddOns\ACE\MultiMAC\MACInstaller.exe
- \AddOns\MultiMAC\MACInstaller.exe

وهي تجمع القيم للمعلمات التالية من خلال سلسلة من الشاشات.

رقم الشاشة	المعلمة	الوصف
3	**مجلد الوجهة**	الدليل المحلي حيث يجب تثبيت جهاز MAC.
4	**الخادم**	اسم أو عنوان IP للخادم حيث يجري تشغيل DMS.
4	**المنفذ (منفذ إلى DMS)**	رقم المنفذ على خادم DMS الذي سيتم استخدامه للتواصل بين MAC وDMS. **انظر أدناه لمزيد من التفاصيل.**
4	**الرقم (رقم نظام MAC)**	تعيين إلى 1 لجميع وحدات MAC الأصلية. تعيين إلى 2 لجميع وحدات MAC المتكررة لتجاوز الفشل (RMAC).
4	**المثيل (اسم أو عنوان IP لوحدة MAC الشريكة)**	عنوان IP للكمبيوتر حيث يجب أن يتم تشغيل الشريك المتكرر لتجاوز الفشل لخادم MAC هذا. اترك هذا الحقل فارغًا، إذا لم يكن الأمر قابلاً للتطبيق.

المعلمة: المنفذ (منفذ إلى DMS)

تتضمن أرقام المنافذ نظام الترقيم التالي:

- في نظام غير هرمي، حيث يوجد خادم DMS واحد فقط، تقوم كل وحدة MAC ووحدة RMAC مناظرة بإرسال الإشارات من رقم المنفذ نفسه، وهو عادة 6000. بإمكان خادم DMS التواصل فقط مع زوج MAC/RMAC واحد على حدة.
- يتلقى خادم DMS الإشارات من MAC أو زوج MAC/RMAC الأول على المنفذ 6001، ومن MAC أو زوج MAC/RMAC الثاني على المنفذ 6002، وغير ذلك.

المعلمة: الرقم (رقم نظام MAC)

الهدف من هذه المعلمة هو تمييز وحدات MAC الأصلية عن RMAC:

- تحمل جميع وحدات MAC الأصلية الرقم 1
- تحمل جميع وحدات MAC المتكررة لتجاوز الفشل (RMAC) الرقم 2

المعلمة: تكوين فقط (زر تبادلي)

حدد هذا الخيار لتغيير تكوين وحدة MAC على خادم DMS الرئيسي، وتحديدًا لإعلامها بوجود وحدة RMAC جديدة مثبتة على كمبيوتر آخر.

وفي هذه الحالة، أدخل عنوان IP أو اسم المضيف لوحدة RMAC في المعلمة **المثيل**.

المعلمة: تحديث البرنامج (زر تبادلي)

حدد هذا الخيار على كمبيوتر آخر غير خادم DMS الرئيسي، إما لتثبيت RMAC أو لتغيير تكوينه.

وفي هذه الحالة، أدخل عنوان IP أو اسم المضيف لجهاز RMAC المثيل MAC في المعلمة **المثيل**.

14.2 أجهزة التحكم في الوصول

لم تعد وحدات AMC مع دعم DTLS تدعم اتصالات RS485 أو RS232 بين المضيف (MAC) وAMC.

قم بتعطيل جميع وحدات AMC التي تم تكوينها على منافذ COM أو إزالة هذه الوحدات من التكوين.

وإلا، فلن يتمكن محرر الجهاز من إنجاز عملية الترحيل. وبالتالي، يبقى التكوين غير محفوظ.

مع AMS 4.0، تم تحديث برنامج تحميل التمهيد إلى الإصدار 00.62 LCM v02.30.00. سيتم تحديث وحدات AMC تلقائيًا بواسطة AMS 4.0.

لتحديث وحدات AMC يدويًا، يجب استخدام Bosch.AMCIPConfig-Tool.

إذا تضمنت وحدة AMC الإصدار V00.49 من برنامج تحميل التحديث، عليك أولاً التحديث إلى V00.61v01.47.00 ومن هذا الإصدار إلى LCM 00.62 v02.30.00.

إعادة البرنامج الثابت إلى إصدار أقدم
من أجل استخدام وحدة AMC التي تمت ترقيتها إلى BIS 4.9.1 أو AMS 4.0 على نظام تحكم في الوصول أقدم (ACE أو AMS أو APE)، من الضروري إعادة البرنامج الثابت AMC إلى إصدار أقدم.
يجب أولاً إعادة الإصدارات V00.62 من البرنامج الثابت إلى الإصدار V00.61 قبل إعادتها إلى الإصدارات الأقدم.

14.3 تكوين أجهزة LAC

إنشاء وحدة التحكم في الوصول المحلية AMC
تعتبر وحدات التحكم في الوصول النمطية (AMC) وحدات تابعة لوحدات التحكم في الوصول الرئيسية (MAC) في محرر الجهاز.
لإنشاء AMC:

1. في محرر الجهاز، انقر بزر الماوس الأيمن فوق MAC وحدد **كائن جديد** من قائمة السياق
أو
2. انقر فوق الزر ✚.
3. اختر أحد أنواع AMC التالية من مربع الحوار الذي يظهر:

AMC 4W (افتراضي) مع أربع واجهات أجهزة قراءة Wiegand للاتصال بأربعة أجهز قراءة كحدٍ أقصى.

AMC 4R4 مع أربع واجهات أجهزة قراءة RS485 للاتصال بثمانية أجهز قراءة كحدٍ أقصى.

النتيجة: يتم إنشاء إدخال AMC جديد من النوع المختار في التدرج الهرمي لمحرر الجهاز، DevEdit.

AMC 4-W	**و**حدة **ت**حكم **ن**مطية في الوصول مع أربعة أجهزة قراءة Wiegand.	يمكن تكوين أربعة أجهزة قراءة Wiegand كحدٍ أقصى للاتصال بأربعة مداخل. تدعم وحدة التحكم ثماني إشارات مداخل وثماني إشارات مخارج. وبإمكان لوحات التوسيع توفير ما يصل إلى 48 إشارات مداخل ومخارج إضافية.
AMC 2-W	**و**حدة **ت**حكم **ن**مطية في الوصول مع جهازي قراءة Wiegand.	يمكن تكوين جهازي قراءة Wiegand كحد أقصى لتوصيل ما يصل إلى مدخلين. تدعم وحدة التحكم أربع إشارات إدخال وأربعة إشارات إخراج.
AMC 4-R4	**و**حدة **ت**حكم **ن**مطية في الوصول مع أربعة أجهزة قراءة RS485	يمكن تكوين ثمانية أجهزة قراءة RS485 كحدٍ أقصى للاتصال بثمانية مداخل. تدعم وحدة التحكم ثماني إشارات مداخل وثماني إشارات مخارج. وبإمكان لوحات التوسيع توفير ما يصل إلى 48 إشارات مداخل ومخارج إضافية.
AMC_IO08	لوحة توسيع لوحدة AMC مع ثماني إشارات مداخل ومخارج	يمكن جعل إشارات إضافية متوفرة. يمكن توصيل حتى ثلاث لوحات توسيع بوحدة AMC

AMC_IO16	لوحة توسيع لوحدة AMC مع ست عشرة إشارة مداخل ومخارج	
AMC_IO84W	لوحة توسيع لوحدة Wiegand AMC مع ثماني إشارات مداخل ومخارج	

تنشيط/إلغاء تنشيط وحدات التحكم

يكون الخيار (خانة الاختيار) التالي: **تم تمكين الاتصال بالمضيف** محددًا لوحدة التحكم الجديدة عند إنشائها.

يؤدي ذلك إلى فتح اتصال الشبكة بين MAC ووحدات التحكم، بحيث تنتشر في وحدات التحكم الأخرى وبشكل تلقائي بيانات التكوين التي طرأ عليها تغيير أو توسيع.

يمكنك إلغاء تنشيط هذا الخيار لحفظ عرض النطاق الترددي للشبكة، وبالتالي تحسين الأداء، مع إنشاء وحدات تحكم متعددة والأجهزة التابعة لها (المداخل والأبواب وأجهزة القراءة ولوحات التوسيع). عندئذٍ توضع علامة على الأجهزة في محرر الأجهزة بواسطة أيقونات رمادية.

مهم: احرص على إعادة تنشيط هذا الخيار عند اكتمال تكوين الأجهزة. سيسمح ذلك بإبقاء وحدات التحكم محدّثة بشكل مستمر بواسطة أي تغييرات في التكوين تتم على مستويات أخرى.

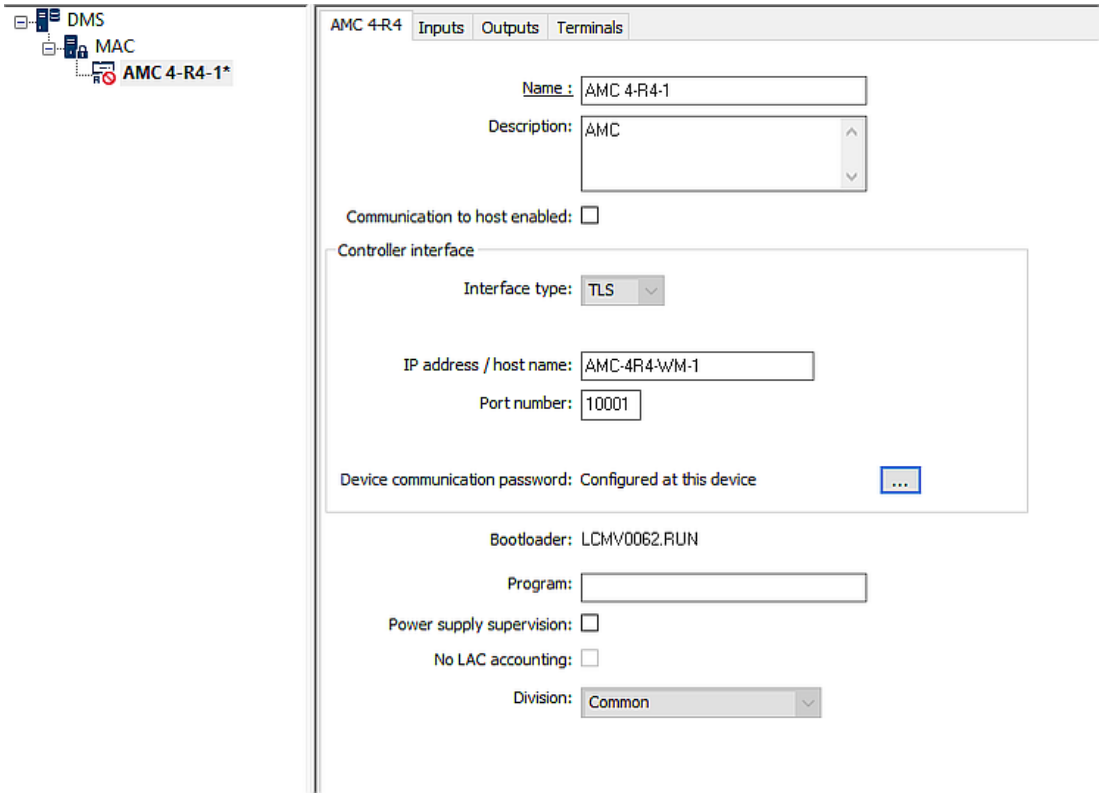
الخلط بين أنواع وحدات التحكم ضمن تثبيت واحد

تكون أنظمة التحكم في الوصول مجهزةً عادةً بنوع واحد من أنواع وحدات التحكم وأجهزة القراءة. وقد تؤدي عمليات تحديث البرامج وعمليات التثبيت المتنامية إلى إبراز ضرورة استبدال مكونات أجهزة موجودة بأخرى جديدة. حتى التكوينات التي تجمع ما بين متغيرات RS485 (AMC 4R4) ومتغيرات Wiegand (AMC 4W) تكون ممكنة، شرط مراعاة التحذيرات التالية:

- تقوم أجهزة قراءة RS485 بإرسال "رسالة تلغرافية" تحتوي على رقم الرمز كمقروء.
- تقوم أجهزة قراءة Wiegand بإرسال بياناتها بطريقة تستوجب فك تشفيرها بمساعدة تعريف بطاقة التعريف بهدف المحافظة على رقم الرمز بشكله الصحيح.
- بإمكان وحدات التحكم المختلطة أن تعمل فقط في حال تم بناء رقمي الرمز بطريقة مماثلة.

14.3.1 معلمات وإعدادات AMC

معلمات AMC العامة



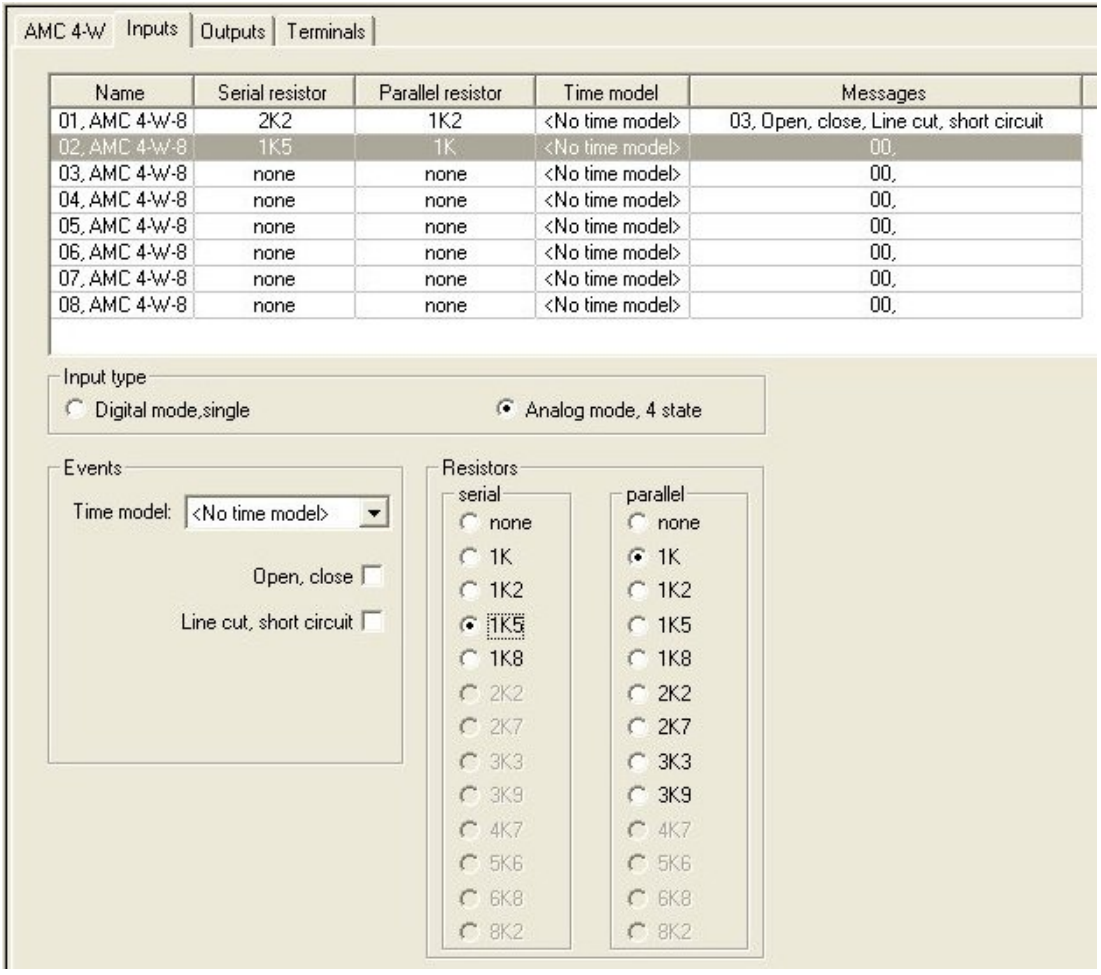
تكوين معلمات AMC

المعلمة	القيم المحتملة	الوصف
اسم وحدة التحكم	مقيد بأحرف أبجدية رقمية: 1 - 16 خانة رقمية	يضمن إنشاء المعرّف (افتراضي) الحصول على أسماء فريدة، ولكن بإمكان المستخدم استبدالها. إذا استبدلت أحد الأسماء، فيجب أن تتأكد من أن المعرّفات هذه فريدة.
وصف وحدة التحكم	أحرف أبجدية رقمية: 0 - 255 خانة رقمية	نص حر.
تم تمكين الاتصال بالمضيف	0 = معطّل (خانة الاختيار غير محددة) 1 = ممكّن (خانة الاختيار محددة)	افتراضي = ممكّن تشير أيقونات التراكب على وحدات التحكم في شجرة الأجهزة إلى حالة الاتصال بالمضيف (ممكّن/معطّل). يؤدي إلغاء تحديد خانة الاختيار إلى نقل AMS إلى وضع عدم الاتصال بشكل مؤقت، وهو مفيد لإعادة التكوين والاختبار. يؤدي تحديث نظام التحكم في الوصول إلى إصدار جديد إلى إلغاء تحديد خانات الاختيار التابعة لجميع أجهزة التحكم بشكل تلقائي. حدد خانات اختيار وحدات AMC وقم بإلغاء تحديدها لاختبارها بشكل فردي في البرنامج المحدّث.

		حدد خانة الاختيار عند استخدام محرر الجهاز لتعيين DCP (كلمة مرور اتصال الأجهزة) على AMC أثناء تنفيذ نشر DTLS "من الأعلى إلى الأسفل". يؤدي ذلك إلى فتح نافذة زمنية مدتها 15 دقيقة لنشر DCP لأسفل وصولاً إلى وحدات AMC. قم بإلغاء تحديد خانة الاختيار وحددها لإعادة تشغيل النافذة الزمنية.
واجهة وحدة التحكم		
نوع الواجهة	TLS	TLS (=أمان طبقة النقل): عند تعيين كلمة مرور اتصال الأجهزة (DCP) لوحدة AMC، يتم الاتصال بوحدة MAC عبر DTLS مع أمان محسّن. تأكد من ضبط مفتاحي DIP الرقم 1 و5 على AMC على وضع التشغيل.
عنوان IP/اسم المضيف	اسم الشبكة أو عنوان IP لوحدة AMC	إذا تم تخصيص عناوين IP بواسطة DHCP، فيجب عندئذٍ توفير اسم الشبكة لوحدة AMC بحيث يمكن تحديد موقع AMC بعد عملية إعادة تشغيل حتى في حال تغيّر عنوان IP. بالنسبة إلى الشبكات من دون DHCP، أدخل عنوان IP.
رقم المنفذ	رقمي: 10001 (افتراضي)	هذا هو منفذ AMC الذي سيتلقى رسائل MAC.
معلمات إضافية		
البرنامج	أبجدي رقمي	اسم ملف البرنامج الذي يجب تحميله إلى AMC. تقع البرامج المتوفرة في دليل BIN في جهاز MAC، ويمكن تحديدها من قائمة. ويظهر أيضًا كل من البروتوكول والوصف لتسهيل الأمر. يتم تعيين هذه المعلمة تلقائيًا أثناء تحميل البرامج تلقائيًا، وهذا يتوقف على أجهزة القراءة المتصلة، ويتم تجاوز المعلمة في حالة عدم تطابق القارئ/البرنامج.
مراقبة مورد الطاقة	0= ملغى تنشيطه (خانة الاختيار غير محددة) 1= منشّط (خانة الاختيار محددة)	مراقبة فولتية مورد الطاقة. إذا توقف مورد الطاقة عن العمل، فستظهر عندئذٍ رسالة إعلامية. يعتبر وجود مورد الطاقة غير المتقطعة (UPS) شرطًا أساسيًا لوظيفة المراقبة، بحيث يمكن إنشاء رسالة. 0 = بدون مراقبة 1 = تنشيط المراقبة
بدون حساب LAC	0= ملغى تنشيطه (خانة الاختيار غير محددة) 1= منشّط (خانة الاختيار محددة)	حدد خانة الاختيار هذه لأجهزة AMC التي تعمل معًا لتوفير حق الوصول إلى مناطق صف السيارات، حيث يحتسب جهاز MAC الأصلي عدد الوحدات القادمة والمغادرة.

		لاحظ أنه إذا تم تحديد هذا الخيار وكان AMC غير متصل بالإنترنت، فسيتعذر على AMC منع الوصول إلى المناطق الشديدة الازدحام، إذ لا يتوفر لديه حق الوصول إلى التعداد الكامل للكثافة.
القسم	القيمة الافتراضية "عام"	تُعد ملائمًا فقط إذا كانت ميزة **الأقسام** مرخصة.

تكوين مداخل AMC



تم تقسيم مربع الحوار هذا إلى أربعة أجزاء:
- قائمة المداخل حسب الاسم
- أنواع المداخل
- الأحداث التي ستتم الإشارة إليها بواسطة المداخل
- أنواع المقاومات المستخدمة مع الوضع التناظري

معلمات المداخل

يرد وصف معلمات مداخل AMC في الجدول التالي:

اسم العمود	الوصف
الاسم	ترقم المدخل (من 01 إلى 08) وتسمية AMC أو AMC-EXT الملائم.
المقاوم التسلسلي	عرض قيمة المقاوم المعينة للمقاوم التسلسلي. "بلا" أو "---" = الوضع الرقمي

المقاوم المتوازي	عرض قيمة المقاوم المعينة للمقاوم المتوازي. "بلا" أو "---" = الوضع الرقمي
نموذج الوقت	اسم نموذج الوقت المحدد
الرسائل	رقم المستند وتسمية الرسائل التي سيتم إنشاؤها 00 = بدون رسائل 01 = إذا تم تنشيط الأحداث **المفتوحة**، **المغلقة** 02 = إذا تم تنشيط الحدثين **انقطاع في الخط**، **قصر في الدائرة الكهربية** 03 = إذا تم تنشيط خياري الأحداث
معيّن	باستخدام نموذج المدخل 15، يظهر اسم إشارة DIP.

استخدم المفتاحين Ctrl وShift عند النقر لتحديد مداخل متعددة في الوقت نفسه. سوف تنطبق أي قيم تقوم بتغييرها على جميع المداخل المحددة.

نماذج الوقت والأحداث

بحسب وضع التشغيل، يتم الكشف عن حالات الأبواب التالية والإعلام عنها: **مفتوح** و**مغلق** و**انقطاع في الخط** و**قصر في الدائرة الكهربية**.

حدد خانات الاختيار التابعة لها لتمكين جهاز AMC من إرسال هذه الحالات كأحداث إلى النظام ككل.

حدد **نموذج وقت** من القائمة المنسدلة بالاسم نفسه لتقييد عملية إرسال الأحداث إلى الأوقات المحددة بواسطة النموذج. على سبيل المثال، قد يكون الحدث **مفتوح** مهمًا فقط خارج أوقات العمل العادية.

نوع المدخل

يمكن تشغيل المقاومات في **الوضع التناظري** أو **الوضع التناظري (الحالة 4)**.

الوضع الافتراضي هو **الوضع الرقمي**: يتم الكشف عن حالتين فقط من حالات الباب **مفتوح** و**مغلق**.

في الوضع التناظري، يتم الكشف عن حالتين من حالات الباب **انقطاع في الخط** و**قصر** في الدائرة الكهربية بشكل تلقائي.

الباب مفتوح	مجموع قيم المقاومات التسلسلية (R_S) والمتوازية (R_P) : $R_S + R_P$
الباب مغلق	يساوي قيم المقاومات التسلسلية: R_S
قصر الدارة	مجموع قيم المقاومات التسلسلية (R_S) والمتوازية (R_P) التي تقترب من اللانهاية.
قصر الدارة	مجموع قيم المقاومات التسلسلية (R_S) والمتوازية (R_P) التي تساوي صفر.

المقاومات

يتم تعيين المقاومات إلى "بلا" أو "---" في **الوضع الرقمي** الافتراضي.

في **الوضع التناظري**، يمكن تعيين قيم المقاومات التسلسلية والمتوازية من خلال تحديد الأزرار التبادلية التابعة لها.

بلا، 1K، 1K2، 1K5، 1K8، 2K2، 2K7، 3K3، 3K9، 4K7، 5K6، 6K8، 8K2 (في 100 أوم)

بحسب قيمة المقاوم المحددة، وحدها النطاقات المقيدة تتوفر للمقاوم المناظر.

تُظهر الجداول التالية في الأعمدة اليمنى القيم المحددة، تُظهر في الأعمدة اليسرى النطاقات المتوفرة للمقاوم الآخر.

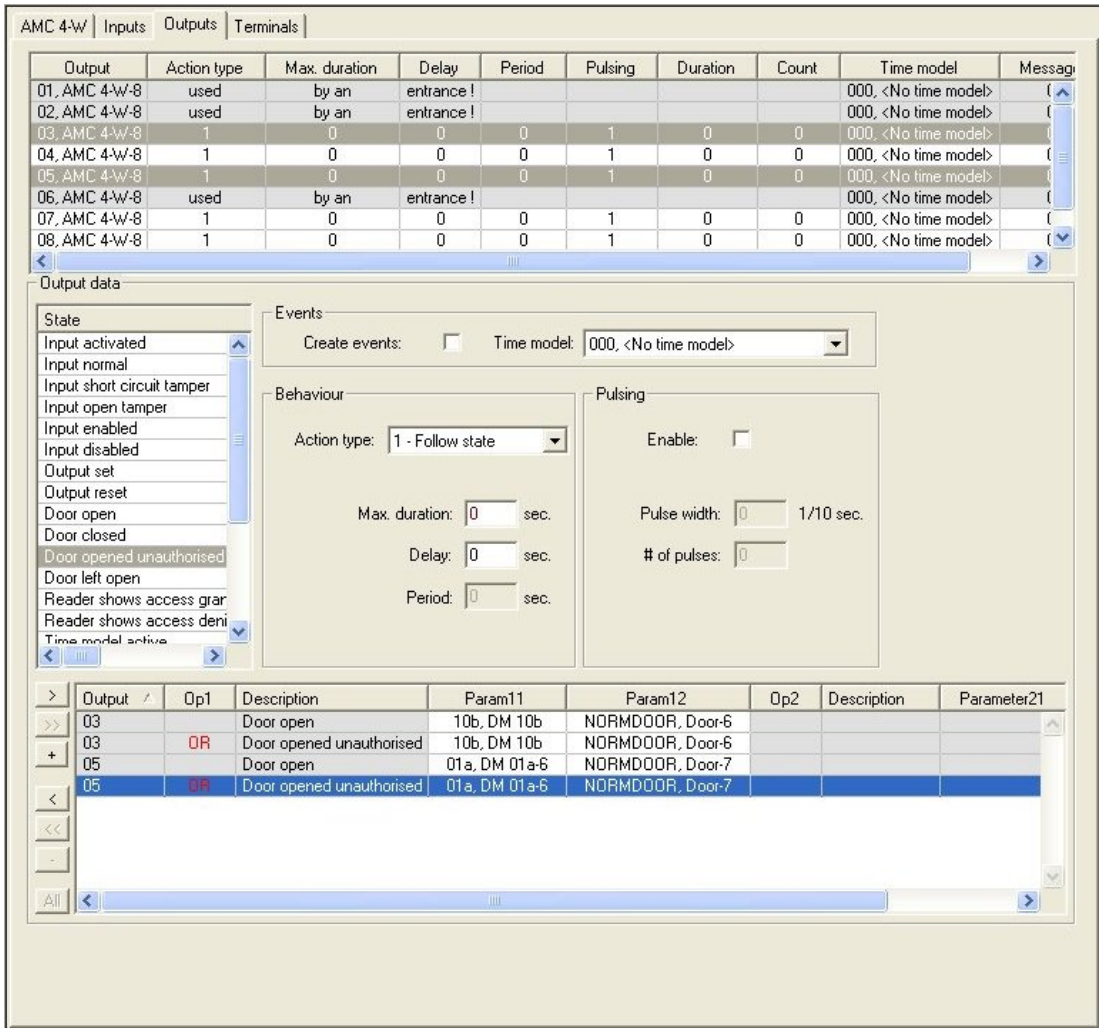
تسلسلي	النطاق		متوازي	النطاق
"بلا" أو "---"	1K إلى 8K2		"بلا" أو "---"	1K إلى 8K2
1K	1K إلى 2K2		1K	1K إلى 1K8
1K2	1K إلى 2K7		1K2	1K إلى 2K7
1K5	1K إلى 3K9		1K5	1K إلى 3K3

1K8	1K إلى 6K8		1K8	1K إلى 3K9
2K2	1K2 إلى 8K2		2K2	1K إلى 4K7
2K7	1K2 إلى 8K2		2K7	1K2 إلى 5K6
3K3	1K5 إلى 8K2		3K3	1K5 إلى 6K8
3K9	1K8 إلى 8K2		3K9	1K5 إلى 8K2
4K7	2K2 إلى 8K2		4K7	1K8 إلى 8K2
5K6	2K7 إلى 8K2		5K6	1K8 إلى 8K2
6K8	3K3 إلى 8K2		6K8	1K8 إلى 8K2
8K2	3K9 إلى 8K2		8K2	2K2 إلى 8K2

تكوين مخارج AMC - نظرة عامة

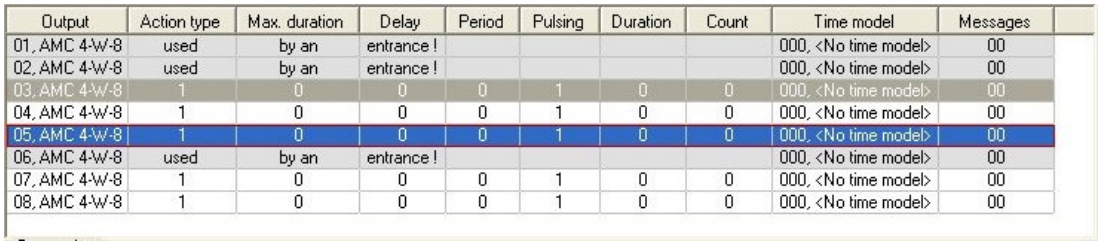
توفر صفحة مربع الحوار هذا تكوين كل مخرج على AMC أو AMC-EXT، وتحتوي على ثلاث مناطق رئيسية.

- مربع قائمة مع نظرة عامة على المعلمة المعينة لكل مخرج
- خيارات التكوين للمخارج المحددة في القائمة
- تعريف شروط تنشيط المخارج



تحديد مخارج AMC في الجدول

لتكوين ملامسات المخارج، حدد أولاً السطر المناظر في الجدول العلوي. استخدم المفتاحين Ctrl وShift عند النقر لتحديد عدة أسطر، إذا لزم الأمر. ستؤثر التغييرات التي يتم إدخالها في الجزء السفلي من النافذة فقط على النافذة التي تحددها.



Output	Action type	Max. duration	Delay	Period	Pulsing	Duration	Count	Time model	Messages
01, AMC 4-W-8	used	by an	entrance !					000, <No time model>	00
02, AMC 4-W-8	used	by an	entrance !					000, <No time model>	00
03, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00
04, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00
05, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00
06, AMC 4-W-8	used	by an	entrance !					000, <No time model>	00
07, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00
08, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00

بالنسبة إلى الأسطر التي تم تعيين مخارجها بواسطة نموذج باب، أو مكان آخر، فهي ستظهر بلون رمادي فاتح مع المعلومات "**مستخدم بواسطة مدخل!**". ولا يمكن إجراء المزيد من عمليات التكوين لهذه المخارج.

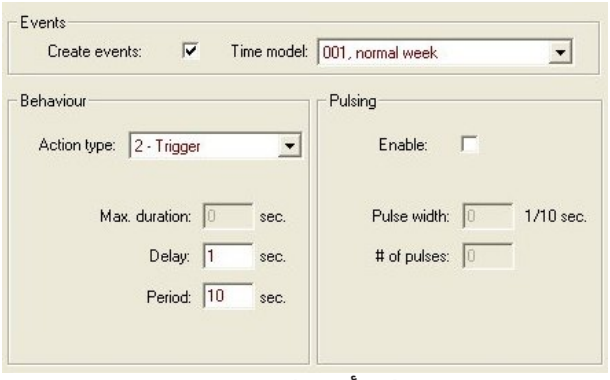
تظهر الأسطر التي تحددها بلون رمادي داكن.

معلمات مخارج AMC

اسم العمود	الوصف
المخرج	الترقيم الحالي للمخارج عند AMC أو AMC-EXT المناظر 01 إلى 08 مع AMC وAMC_IO08 01 إلى 16 مع AMC_IO16
نوع الإجراء	الإشارة إلى نوع الإجراء المحدد 1 = متابعة الحالة 2 = تشغيل 3 = التناوب
المدة القصوى	طول مدة الإشارة بالثواني [1 - 9999؛ 0 = دائمًا، إذا لم تظهر الرسالة المعاكسة] - فقط مع نوع الإجراء "1"
التأخير	التأخير بالثواني حتى إعطاء الإشارة [0 - 9999] - فقط مع نوعي الإجراء "1" و"2"
المدة	المدة بالثواني حتى إعطاء الإشارة - فقط مع نوع الإجراء "2"
النبض	تنشيط النبض - وإلا، ستعطى الإشارة بشكل متواصل
المدة	طول النبض
العدد	عدد النبضات بالثانية
نموذج الوقت	اسم نموذج الوقت المحدد
الرسائل	علامة لنشاط الرسالة 00 = بدون رسائل 03 = يتم الإعلام عن الأحداث
معيّن	باستخدام نموذج المدخل 15، يظهر اسم إشارة DOP.

المخارج: الأحداث، الإجراء، النبض

يتم إنشاء جميع الإدخالات من القائمة أعلاه باستخدام خانات الاختيار وحقول الإدخال في نواحي مربع الحوار **الأحداث** و**الإجراء** و**النبض**. ويؤدي تحديد إدخال قائمة إلى الإشارة إلى الإعدادات المناظرة في هذه النواحي. وينطبق ذلك أيضًا على اختيارات متعددة لإدخالات القائمة، شريطة أن تكون جميع معلمات المخارج المحددة متساوية. ويتم اعتماد التغييرات في إعدادات المعلمات لجميع الإدخالات المحددة في القائمة.



حدد خانة الاختيار **إنشاء أحداث** إذا كان يجب إرسال رسالة للمخرج المحدد. إذا كان يجب إرسال هذه الرسائل خلال فترات محددة فقط، على سبيل المثال، خلال الليل أو عطلة نهاية الأسبوع، فعليك عندئذٍ تعيين **نموذج وقت** ملائم.

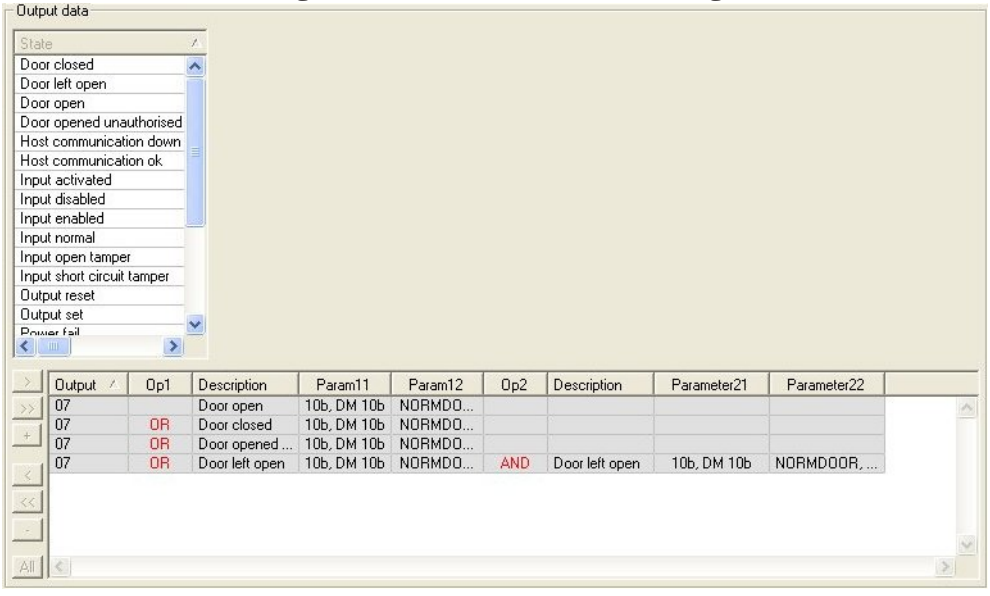
يمكن تعيين المعلمات التالية لأنواع الإجراءات الفردية:

نوع الإجراء	المدة القصوى	التأخير	المدة	النبض/تمكين	عرض النبض	عدد النبضات
متابعة الحالة	0 = دائمًا 1 - 9999	0 - 9999	لا	نعم	1 - 9999	بلا
التشغيل	لا	0 - 9999	0 - 9999 إذا كان النبض **غير** ممكّن	نعم تعطيل الفترة	1 - 9999	1 - 9999
التناوب	لا	لا	لا	نعم	1 - 9999	لا

بيانات مخارج AMC

يحتوي الجزء السفلي من مربع حوار **المخارج** على:

- مربع قائمة مع **الحالات** المتوفرة للمخارج المحددة.
- جدول يتضمن المخارج والحالات المكوّنة لتشغيل هذه المخارج.



تكوين المخارج التي سيتم تشغيلها بواسطة حالات معينة

يمكنك تكوين المخارج المحددة أعلاه بحيث يتم تشغيلها بواسطة حالات فردية أو مجموعات منطقية من الحالات.

- حدد مخرجًا أو أكثر من مربع القائمة العلوي.
- حدد حالة من قائمة **الحالة**.
- في حال وجود عدة أجهزة أو عمليات تثبيت لحالة محددة يمكنها إرسال هذه الحالة فإن الزر » سيكون في وضع التنشيط إلى جانب الزر ›.

انقر فوق › (أو انقر نقرًا مزدوجًا فوق الحالة) لإنشاء مدخل لكل مخرج محدد بتلك الحالة مع الجهاز الأول (على سبيل المثال، AMC، المدخل الأول) والتثبيت (على سبيل المثال، الإشارة الأولى، الباب الأول).

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2

بالنقر فوق »، يتم نقل الحالة المحددة إلى القائمة ويتم إنشاؤها مع عامل OR منطقي لكل جهاز مثبت (على سبيل المثال، جميع مداخل AMC).

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 02, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 03, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 04, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 05, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 06, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 07, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 08, AMC 4-W-2

- يمكن تعيين عدة حالات إلى اختصار OR واحد.

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Door open	06a, Timemgm	<< !!! >>

الاختصارات مع AND ممكنة هي أيضًا:

- يجب أن تكون الحالة معينة هي أيضًا ويُضاف إليها شرط آخر عن طريق تحديده في عمود اختياري.
- بعد ذلك، يتم تحديد حالة أخرى وتوصيلها بالحالة المعلّمة عن طريق النقر فوق ·.

Exit	Operand1	Description	Param11	Param12	Operand2	Description	Parameter21	Parameter22
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2				
04	OR	Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2				
04	OR	Door open	06a, Timemgm	<< !!! >>	AND	Door opened unauthorised	06a, Timemgm	<< !!! >>

إشعار!

يمكن تعيين 128 شرط OR إلى كل مخرج.
بإمكان كل شرط أن يكون لديه **شرط واحد** AND بداخله.

بعد تعيين حالة إلى جهاز أو تثبيت، يمكن أيضًا تعيينها إلى جميع الأجهزة وعمليات التثبيت الأخرى.

- حدد المدخل المعيّن في عمود اختياري.
- يتم إنشاء هذه الحالة لجميع الأجهزة وعمليات التثبيت الموجود عن طريق النقر فوق All.

تعديل معلمات المخارج

يمكنك تعديل الأسطر في القائمة

مع وجود عدة أجهزة أو عمليات تثبيت قد تتطابق معها الحالة المعينة، يتم دائمًا تعيين الأجهزة وعمليات التثبيت الأولى من هذا النوع.
في العمودين **Param11** و**Param21** (مع الاختصارات AND) تظهر الأجهزة (على سبيل المثال، مدخل AMC). يحتوي العمودان **Param12** و**Param22** على عمليات تثبيت خاصة (على سبيل المثال، إشارة المدخل، باب، قارئ).
في حال وجود عدة أجهزة (على سبيل المثال، لوحات الإدخال/الإخراج) أو عدة عمليات تثبيت (على سبيل المثال، إشارات متعددة، أجهزة قراءة)، يتغير مؤشر الماوس أثناء التأشير إلى هذا العمود.

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Door open	06a, Timemgm	<< !!! >>

يؤدي النقر المزدوج فوق إدخال العمود إلى إضافة زر يؤدي إلى ظهور قائمة منسدلة تتضمن إدخالات صالحة للمعلمة.

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Input normal	00, AMC, AMC 4-W-2	01, AMC 4-W-2
04	OR	Door open	06a, Timemgm	

01, AMC 4-W-2
02, AMC 4-W-2
03, AMC 4-W-2
04, AMC 4-W-2
05, AMC 4-W-2
06, AMC 4-W-2
07, AMC 4-W-2
08, AMC 4-W-2

يؤدي تغيير الإدخالات في العمودين **Param11** و**Param21** إلى تحديث الإدخالات في العمودين **Param12** و**Param22**:

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Door open	06a, Timemgm	<< !!! >>
04	OR	Input normal	01, AMC_IO, AMC_IO16_002_1	In, 01, AMC_IO16_002_1

إشعار!
هذا الأمر ممكن فقط بالنسبة إلى الأعمدة **Param11** و**Param12** و**Param21** و**Param22**.
في حال عدم وجود أي خيارات أخرى (على سبيل المثال، بسبب تكوين مدخل واحد فقط)، لا يتغير مؤشر الماوس وتظهر جميع الحقول باللون الرمادي. إذا تم النقر بشكل مزدوج على هذا الإدخال، فسيتم تفسير ذلك على أنه أمر حذف، ويظهر مربع الرسالة للتأكد من عملية الحذف.

حذف الحالات التي تتسبب في تشغيل المخارج
يمكن إزالة التعيينات المحددة عن طريق النقر فوق '**>**' (أو النقر نقرًا مزدوجًا فوق إدخال القائمة). سيظهر مربع رسالة لمطالبتك بتأكيد الحذف.

إذا تم إقران حالات متعددة بمخرج، فيمكن عندئذٍ حذفها كلها معًا كما يلي:
- حدد إدخال القائمة الأول (الإدخال الذي ليس لديه أي إدخال في العمود **Op1**) ثم انقر فوق الزر '**<<**'.
- أو انقر نقرًا مزدوجًا فوق الإدخال الأول.
- تظهر نافذة منبثقة. يمكنك تأكيد عملية الحذف أو إيقافها قبل اكتمالها.
- إذا أكدت عملية الحذف، فستظهر نافذة منبثقة ثانية تسألك إن كنت تريد حذف جميع الإدخالات المقترنة (أجب **نعم**)، أو الإدخال المحدد فقط (أجب **لا**).

لحذف حالات إضافية تعرّف الحالة الأولى بواسطة عامل التشغيل AND في العمود **Op2**، انقر فوي أي مكان في السطر ثم انقر فوق زر "علامة الطرح" ، الذي يكون نشطًا فقط في حال وجود حالة AND معرّفة في ذلك السطر.

وصف الحالة

يوفر الجدول التالي نظرة عامة على جميع الحالات القابلة للتحديد ورقم نوعها ووصفها.
يحتوي حقل القائمة **الحالة** على هذه المعلمات أيضًا - يُشار إليها بالتمرير إلى اليسار على القائمة.

الحالة	النوع	الوصف
المدخل منشّط	1	مدخل يدوي
مدخل عادي	2	مدخل يدوي
التلاعب بقصر دائرة المدخل	3	مدخل محلي مع تكوين بمقاومة
إدخال التلاعب بالفتح	4	مدخل محلي مع تكوين بمقاومة
تعطيل المدخل	5	إلغاء تنشيط مدخل محلي بواسطة نموذج الوقت
تمكين المدخل	6	تنشيط مدخل محلي بواسطة نموذج الوقت
تعيين المخرج	7	مخرج محلي، وليس المخرج الحالي
إعادة تعيين المخرج	8	مدخل محلي، وليس المدخل الحالي
الباب مفتوح	9	GID المدخل، رقم الباب
الباب مغلق	10	GID المدخل، رقم الباب
فتح الباب بشكل غير مصرح به	11	GID المدخل، رقم الباب، يحل مكان "الباب مفتوح" (9)
تم ترك الباب مفتوحًا	12	GID المدخل، رقم الباب
القارئ يُظهر منح صلاحية الوصول	13	عنوان القارئ
القارئ يُظهر رفض الوصول	14	عنوان القارئ
نموذج الوقت نشط	15	نموذج الوقت المكوّن
تلاعب بالقارئ	16	عنوان القارئ
تلاعب بـ AMC	17	---
تلاعب بلوحة الإدخال/الإخراج	18	---
انقطاع الطاقة	19	لجهاز AMC الذي يعمل بطاقة البطارية فقط
جودة الطاقة	20	لجهاز AMC الذي يعمل بطاقة البطارية فقط
اتصال المضيف جيد	21	---
اتصال المضيف معطّل	22	---
رسالة من القارئ	23	عنوان القارئ
رسالة من LAC	24	رقم اللوحة
مراقبة البطاقة	25	عنوان القارئ، وظيفة مراقبة البطاقة

تكوين المخارج

إلى جانب تعيين الإشارات مع نماذج الأبواب أو مع التعيين الفردي، يمكن تعريف الشروط للمخارج التي لم يتم تخصيصها بعد. إذا حدثت هذه الشروط، فسيتم تنشيط المخرج وفقًا للمعلمة المحددة.

يجب أن تقرر ما الذي سيتم تشغيله عبر المخرج. بشكل مغاير للإشارات التي يمكن تعيينها لنموذج باب محدد، وأبوابه، وأجهزة القراءة التابعة له، في هذه الحالة يمكن تطبيق إشارات كل الأجهزة والأدوات المركبة الموصولة بجهاز AMC.

على سبيل المثال، في حال وجود إشارة بصرية، أو صوتية أو رسالة إلى جهاز خارجي يجب تشغيلها بواسطة إشارات المداخل **التلاعب بقصر دائرة المدخل** و**فتح الباب بشكل غير مصرح به**، يتم تعيين هذا المدخل أو المداخل إلى مخرج الوجهة المناظر.

مثال يبيّن ملامس واحد تم تحديده في كل حالة:

Exit	Operand1	Description	Param11	Param12
04		Input short cir...	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Door opened ...	06a, Timemgm	<< !!! >>

مثال يبين كل الملامسات:

Exit	Operand1	Description	Param11	Param12
04		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 08, AMC 4-W-2
04	OR	Door opened unauthorised	06a, Timemgm	---
04	OR	Door opened unauthorised	03a, Entrance B:B	REVDOOR, Revolving Door

مثال يبين الملامسات المحددة:

يتم إنشاء إدخال واحد لكل ملامس بالنقر فوق » أو إزالة الملامسات غير المطلوبة بعد تعيين كل الملامسات:

Exit	Operand1	Description	Param11	Param12
04		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
04	OR	Door opened unauthorised	06a, Timemgm	---
04	OR	Door opened unauthorised	03a, Entrance B:B	REVDOOR, Revolving Door

يمكن تثبيت الظروف نفسها على عدة مخارج إذا تطلب الأمر، على سبيل المثال، إرسال رسالة إلى جهاز خارجي في الوقت نفسه، إذا احتجت أيضًا إلى إشارة صوتية بالإضافة إلى إشارة بصرية:

Exit	Operand1	Description	Param11	Param12
04		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 08, AMC 4-W-2
04	OR	Door opened unauthorised	06a, Timemgm	<< !!! >>
04	OR	Door opened unauthorised	03a, Entrance B:B	REVDOOR, Revolving Door
06		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 08, AMC 4-W-2
06	OR	Door opened unauthorised	06a, Timemgm	<< !!! >>
07		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2

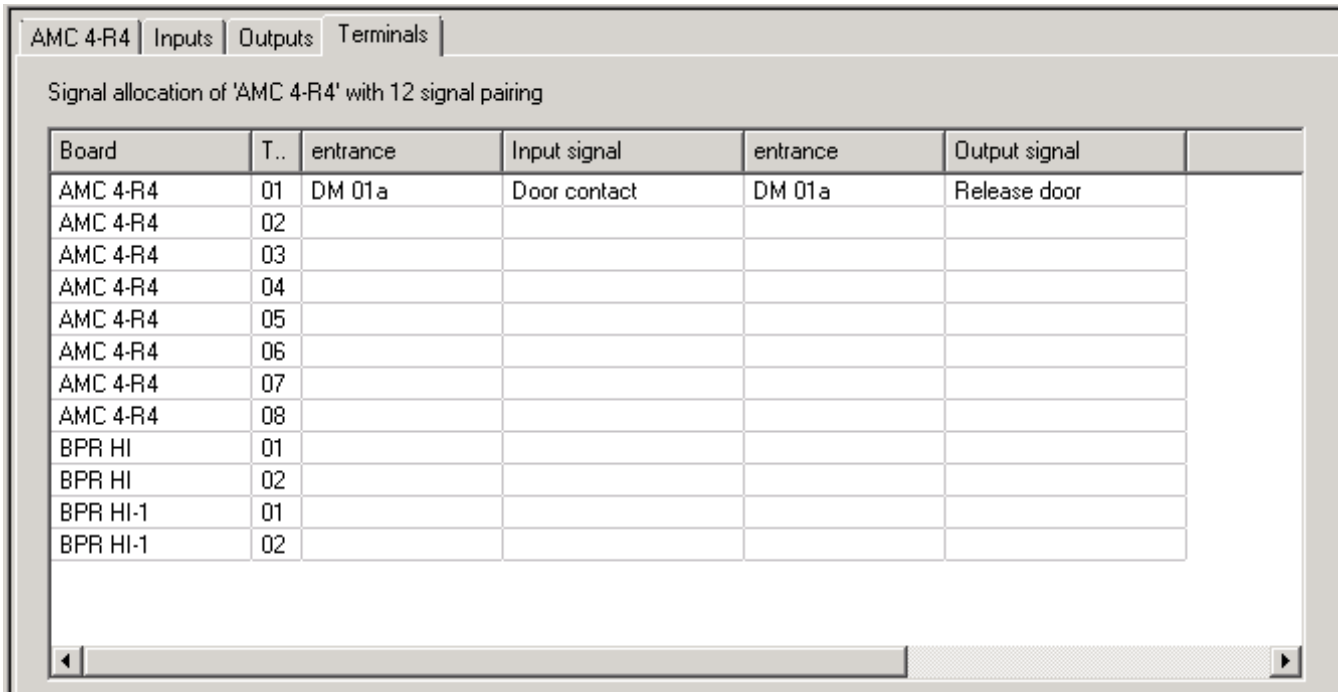
قائمة بكافة الحالات الموجودة مع القيم الافتراضية للمعلمة 11/21 و12/22:

Description	Param11	Param12
Input activated	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input open tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input enabled	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input disabled	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
Output reset	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
Door open	06a, Timemgm	<< !!! >>
Door closed	06a, Timemgm	<< !!! >>
Door opened unauthorised	06a, Timemgm	<< !!! >>
Door left open	06a, Timemgm	<< !!! >>
Reader shows access granted	---	TM-Reader IN
Reader shows access denied	---	TM-Reader IN
Time model active	---	000, <No time model>
Tamper reader	---	TM-Reader IN
Tamper AMC	---	---
Tamper I/O board	---	00, AMC, AMC 4-W-2
Power fail	---	---
Power good	---	---
Host communication ok	---	---
Host communication down	---	---

تحديد الإشارات في تبويب المحطات الطرفية

يسرد تبويب **المحطات الطرفية** تعيين الملامسات على جهاز AMC أو AMC-EXT. حالما يتم إنشاء المداخل، يُشار إلى تعيينات الإشارات بحسب نموذج الباب المحدد.

لا يمكنك إجراء تعديلات في تبويب **المحطات الطرفية** الخاص بوحدة التحكم أو لوحات التوسيع. عمليات التحرير ممكنة فقط في تبويب المحطات الطرفية لصفحة المدخل. لهذا السبب يتم عرض إعدادات المحطات الطرفية على خلفية رمادية. تشير المداخل التي يتم عرضها باللون الأحمر إلى تكوينات إشارات المخارج ذات الصلة.



Board	T..	entrance	Input signal	entrance	Output signal
AMC 4-R4	01	DM 01a	Door contact	DM 01a	Release door
AMC 4-R4	02				
AMC 4-R4	03				
AMC 4-R4	04				
AMC 4-R4	05				
AMC 4-R4	06				
AMC 4-R4	07				
AMC 4-R4	08				
BPR HI	01				
BPR HI	02				
BPR HI-1	01				
BPR HI-1	02				

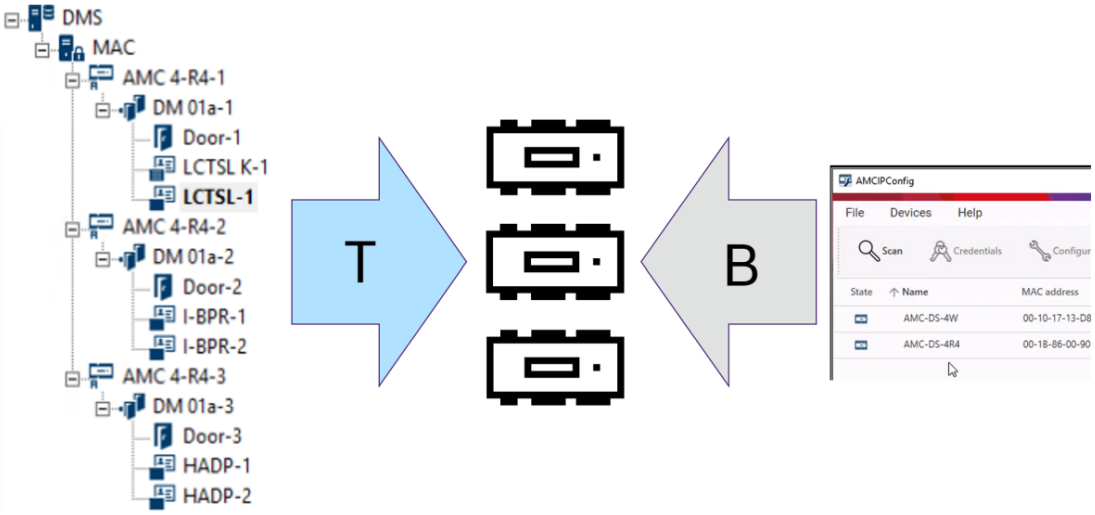
15 تكوين DTLS للاتصال الآمن

المقدمة

يقدم نظام التحكم في الوصول (ACS) اتصالاً آمنًا للغاية بين الأجهزة، محمي بواسطة DTLS. هناك طريقتان رئيسيتان لنشر اتصال DTLS بين الأجهزة في ACS:

النشر من الأعلى إلى الأسفل (T) يتم في محرر الجهاز في ACS.

النشر من الأسفل إلى الأعلى (B) يتم بشكل أساسي في أداة AMCIPConfig، ولكنه يحتاج إلى محرر الجهاز كي يُستكمل.



- يمكن تنفيذ النشر من الأعلى إلى الأسفل (T) بطريقتين بديلتين في محرر الجهاز.
  - باستخدام كلمة مرور واحدة لاتصال الأجهزة (DCP) على مستوى DMS لجميع وحدات AMC.
  - باستخدام عدة كلمات مرور لاتصال الأجهزة (DCP) لفروع مختلفة من شجرة الأجهزة، بدءًا من وحدات MAC أو وحدات AMC
- يمكن أيضًا بدء النشر من الأسفل إلى الأعلى (B) بطريقتين بديلتين في أداة AMCIPConfig.
  - باستخدام مفتاح أجهزة AMC
  - باستخدام مفتاح LCD عشوائي

إشعار!

يحتاج النشر من الأسفل إلى الأعلى (B) إلى إعداد DCP في محرر الجهاز.
يسمح لك النشر من الأسفل إلى الأعلى بتعيين DCP على جهاز AMC. ومع ذلك، يجب عليك تعيين نفس DCP على نفس AMC في محرر الجهاز أيضًا، لتمكين اتصال DTLS الكامل بين MAC وAMC.

ملخص خيارات نشر DTLS

	وصف مختصر	المزايا	العيوب
من الأعلى إلى الأسفل	يقوم مسؤول النظام بإدخال كلمة مرور قوية في **محرر الجهاز**. من كلمة المرور هذه، ينشئ النظام **مفتاحًا رئيسيًا** يقوم بنشره من الأعلى إلى الأسفل عبر شجرة أجهزة التحكم في الوصول، من DMS عبر وحدات MAC إلى وحدات التحكم في الأبواب AMC.	نشر سريع وبسيط	أثناء نشر المفتاح الرئيسي لوحدات التحكم في الأبواب AMC، لا يكون اتصال الأجهزة محميًا بواسطة DTLS.

	وصف مختصر	المزايا	العيوب
	يمكنك تعيين كلمة مرور واحدة لشجرة الأجهزة بالكامل، أو تعيين كلمات مرور مختلفة لفروع مختلفة من شجرة الأجهزة.		
من الأسفل إلى الأعلى باستخدام مفتاح أجهزة AMC	يستخدم مسؤول النظام أداة **AMC IPConfig** لنشر DTLS على مستوى وحدات التحكم في الأبواب AMC.	تمايز أكبر ومرونة في النشر. يتجنب هذا الأسلوب العيب الرئيسي للنشر من الأعلى إلى الأسفل، ألا وهو الاتصال المتقطع غير المحمي للمفتاح الرئيسي. ومع ذلك، فهو يتطلب أن يكون الاتصال من أداة AMCIPConfig إلى AMC آمنًا عند تعيين DCP.	أثناء قيام أداة IPConfig بتعيين DCP على AMC، يجب عليك ضمان الاتصال الآمن بوسائل أخرى. على سبيل المثال، قم بتوصيل AMC مباشرة بالكمبيوتر حيث يتم تشغيل أداة IPConfig. يجب أيضًا تعيين كلمات مرور اتصال الأجهزة (DCP) التي تعيّنها في أداة IPConfig على نفس وحدات AMC عبر محرر الجهاز.
من الأسفل إلى الأعلى باستخدام مفتاح LCD العشوائي		تمايز أكبر ومرونة في النشر. أعلى مستوى من الأمان، بسبب عدم نقل مفتاح LCD عبر الشبكة على الإطلاق؛ وبالتالي يكون نشر بيانات الاعتماد محميًا في جميع الأوقات.	نشر أكثر تعقيدًا وأكثر استهلاكًا للوقت. يجب عليك نقل مفتاح LCD العشوائي المكون من 27 رمزًا عبر بعض الوسائل غير الخاصة بالشبكة إلى أداة IP Config.
يمكن العثور على التفاصيل والإرشادات في الأقسام التالية من هذا الفصل.			

مصطلحات DTLS

DCP (كلمة مرور اتصال الأجهزة)	كلمة مرور واحدة قوية ينشئ منها ACS مفتاحًا رئيسيًا داخليًا. يجب الحفاظ على أمان كلمة المرور نظرًا لعدم تخزينها في ACS.
المفتاح الرئيسي	رمز يقوم النظام بإنشائه من DCP، ويستخدمه لحماية أجهزة التحكم في الوصول. لا يتم عرض المفتاح الرئيسي لأي مستخدم على الإطلاق.
مفتاح LCD عشوائي	رمز أبجدي رقمي مؤقت تقوم وحدة AMC بإنشائه من جديد في كل مرة تقوم فيها بالتمهيد. يمكن عرض المفتاح في شاشة العرض البلورية السائلة (LCD) لوحدة AMC وقد تطلبه الأدوات البرمجية لمصادقة اتصالات الشبكة.
مفتاح أجهزة AMC .	رمز مصادقة داخلي تقوم وحدة AMC بإنشائه من معلمات أجهزة معينة. وهو غير مرئي للمستخدم.

15.1 نشر DTLS من الأعلى إلى الأسفل

الشروط الأساسية

- AMS 4.0 أو BIS-ACE 4.9.1 أو إصدارات لاحقة.
- تم إعداد شجرة أجهزة التحكم في الوصول من DMS إلى وحدات AMC وتم توصيلها بالشبكة بطريقة فعلية، ولكن لم يتم تمكين وحدات AMC. يعني التمكين أن خانات اختيار وحدات AMC **تم تمكين الاتصال بالمضيف** محددة.
- لم يتم تكوين DTLS بالفعل على إحدى وحدات AMC بواسطة أحد أساليب النشر من الأسفل إلى الأعلى عبر أداة IPConfig.

الإجراء: كلمة مرور واحدة لاتصال الأجهزة (DCP) للكل

1. في ACS، ابدأ تشغيل محرر الجهاز
   - مستعرض تكوين BIS > **الاتصالات**
   - قائمة AMS الرئيسية > **التكوين** > **بيانات الجهاز** > **شجرة الأجهزة**
   - تظهر نافذة حوار تدعوك إلى إدخال كلمة مرور قوية لاتصال الأجهزة (DCP).
2. لتعيين كلمة مرور واحدة لاتصال الأجهزة (DCP) لجميع وحدات AMC في شجرة الأجهزة، أدخل كلمة مرور قوية وقم بتأكيدها وفقًا لسياسات كلمة المرور المحلية المتبعة لديك.
   - يقدم مربع الحوار ملاحظات بشأن قوة كلمة المرور، بالاستناد إلى إنتروبيا كلمة المرور.
3. دوّن كلمة المرور بتأنٍ نظرًا لعدم تخزينها في ACS.
4. انقر فوق **موافق** لإغلاق مربع الحوار.

الإجراء البديل: استخدام كلمات مرور لاتصال الأجهزة (DCP) لفروع مختلفة من شجرة الأجهزة

1. في ACS، ابدأ تشغيل محرر الجهاز
   - مستعرض تكوين BIS > **الاتصالات**
   - قائمة AMS الرئيسية > **التكوين** > **بيانات الجهاز** > **شجرة الأجهزة**
   - تظهر نافذة حوار تدعوك إلى إدخال كلمة مرور قوية لاتصال الأجهزة (DCP).
2. انقر فوق **إلغاء** لتعيين كلمات مرور مختلفة لاتصال الأجهزة (DCP) على فروع مختلفة من شجرة الأجهزة (وحدات MAC ووحدات AMC).
   - يعلمك مربع حوار منبثق بعدد وحدات AMC في النظام التي ليس لديها كلمة مرور اتصال الأجهزة (DCP).
   - تفتح شجرة الأجهزة في محرر الجهاز.
3. افتح شجرة الأجهزة لتحديد وحدة MAC أو AMC التي تريد تعيين كلمة مرور اتصال الأجهزة (DCP) لها.
   - إذا قمت بتعيين كلمة مرور اتصال الأجهزة (DCP) على مستوى MAC، فسيتم تعيينها لجميع وحدات AMC التابعة لوحدة MAC.
   - إذا قمت بتعيين كلمة مرور اتصال الأجهزة (DCP) على مستوى AMC، فسيتم تعيينها لوحدة AMC هذه فقط.
4. انقر فوق زر علامة القطع إلى جانب الحقل النصي **كلمة مرور اتصال الأجهزة:**
5. أدخل كلمة مرور قوية وقم بتأكيدها وفقًا لسياسات كلمة المرور المحلية المتبعة لديك.
6. دوّن كلمة المرور بتأنٍ بالإضافة إلى الفرع الذي تنطبق عليه نظرًا لعدم تخزينها في ACS.
7. كرر هذا الإجراء لكل وحدة MAC أو AMC تريد أن تعيّن لها كلمة مرور منفصلة لاتصال الأجهزة (DCP).
8. انقر فوق **موافق** لإغلاق مربع الحوار.

نتيجة النشر من الأعلى إلى الأسفل

يستخدم ACS كلمة (كلمات) مرور اتصال الأجهزة (DCP) لإنشاء مفاتيح داخلية لجميع وحدات AMC تحت DMS أو MAC المحدد.

لا تحتاج إلى تكرار هذا الإجراء ما لم تقم لاحقًا بتغيير كلمة مرور اتصال الأجهزة (DCP) على وحدة AMC أو أكثر باستخدام أداة AMC IPConfig (راجع النشر "من الأسفل إلى الأعلى"). وفي هذه الحالة، يجب أن تقوم على الفور بتعيين كلمة مرور اتصال الأجهزة (DCP) نفسها من الأعلى إلى الأسفل على نفس وحدات AMC في محرر الجهاز.

إذا قمت في وقت لاحق بإضافة أجهزة في شجرة الأجهزة التابعة لأنظمة DMS ووحدات MAC التي لديها كلمات مرور لاتصال الأجهزة (DCP)، فسترث الأجهزة الجديدة تلقائيًا نفس DCP من الأجهزة الأعلى منها.

16 تكوين المداخل

16.1 المداخل - مقدمة

يدل مصطلح المدخل بمجمله إلى آلية التحكم في الوصول عند نقطة دخول:
تشمل عناصر المدخل:
- أجهزة قراءة الوصول - بين 1 و4
- بعض أشكال الحواجز، على سبيل المثال باب، أو حاجز دوار، أو شرَك أو حاجز ذو ذراع.
- إجراء الوصول كما تم تعريفه بواسطة التسلسلات المعرّفة مسبقًا للإشارات الإلكترونية التي تمر بين عناصر الأجهزة.

إن نموذج الباب عبارة عن قالب لنوع معين من المداخل. فهو يصف عناصر الباب الموجودة (عدد أجهزة القراءة ونوعها، ونوع الباب أو الحاجز إلخ.)، ويفرض عملية محددة للتحكم في الوصول مع تسلسل من الإشارات المعرّفة مسبقًا.
تُسهّل نماذج الأبواب إلى حد كبير تكوين نظام التحكم في الوصول.

نموذج الباب 1	باب بسيط أو مشترك
نموذج الباب 3	حاجز دوار قابل للعكس للدخول والخروج
نموذج الباب 5	مدخل أو مخرج ساحة الانتظار
نموذج الباب 6	أجهزة القراءة على الجهة الداخلية/الخارجية للوقت والحضور
نموذج الباب 7	التحكم بالمصعد
نموذج الباب 9	حاجز بذراع وبوابة منزلقة للمركبات
نموذج الباب 10	باب بسيط مع تفعيل/تعطيل IDS
نموذج الباب 14	باب بسيط مع تفعيل/تعطيل IDS وحقوق وصول خاصة
نموذج الباب 15	إشارات مدخل ومخرج مستقلة

- تتضمن نماذج الأبواب 1، 3، 5، 9 و10 خيارًا لأجهزة قراءة بطاقات إضافية على الجهة الداخلية أو الخارجية.
- لا يمكن مشاركة وحدة التحكم في الوصول المحلية المستخدمة ضمن نموذج الباب 05 (ساحة الانتظار) أو 07 (المصعد) مع نموذج باب آخر.
- عندما يتم تكوين مدخل مع نموذج باب وحفظه، سيتعذر تبديل نموذج الباب بآخر. وفي حال تطلب الأمر نموذج باب آخر فيجب حذف المدخل وإعادة تكوينه من البداية.

تتضمن بعض نماذج الأبواب متغيرات (a، b، c، r) مع الميزات التالية:

a	أجهزة القراءة على الجهة الداخلية **و**أجهزة القراءة على الجهة الخارجية
b	قارئ على الجهة الداخلية وزر يعمل بالضغط على الجهة الخارجية
c	قارئ على الجهة الداخلية **أو** قارئ على الجهة الخارجية (وليس الاثنين معًا - مما يجعله المتغير **a**)
r	(نموذج الباب 1 فقط). قارئ واحد لغرض واحد وهو تسجيل الأشخاص في نقطة التجمع، على سبيل المثال في حالة الإخلاء. لا يوجد حاجز فعلي مثبت في نموذج الباب هذا.

يُصبح زر إكمال التكوين **موافق** نشطًا فقط عندما يتم إدخال كافة القيم الإلزامية. على سبيل المثال، تتطلب نماذج الأبواب ذات المتغير (a) أجهزة قراءة على الجهة الداخلية **و** أجهزة قراءة على الجهة الخارجية. ولن يكون بالإمكان حفظ الإدخالات إلا عندما يتم تحديد نوع القارئين.

16.2 إنشاء مداخل

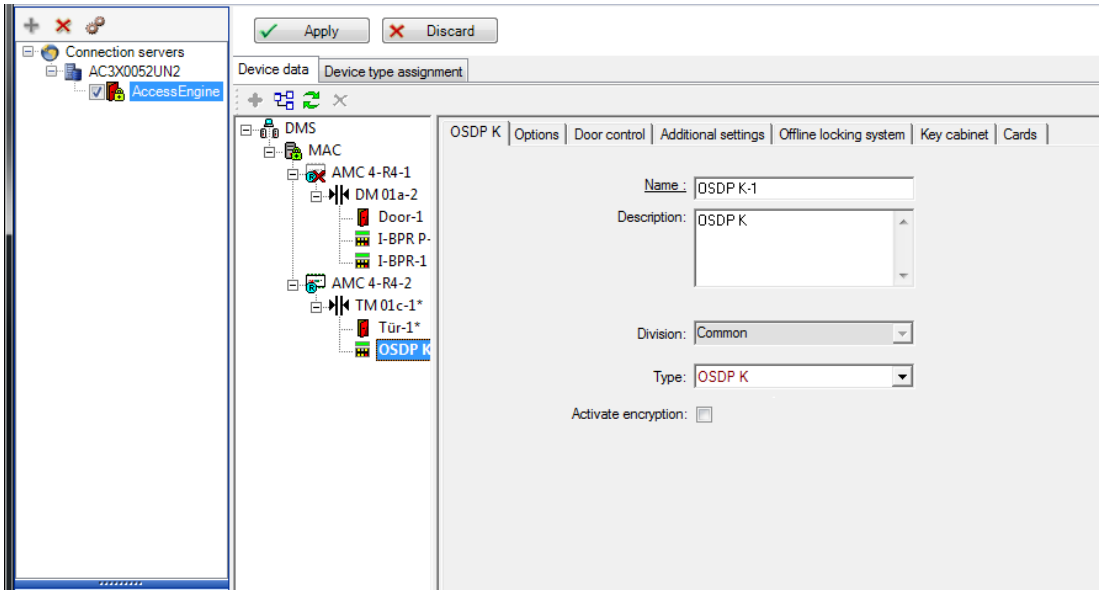
سيتم تخصيص قائمة أجهزة القراءة المعروضة للتحديد منها بحيث تتناسب مع نوع وحدة التحكم التي حددتها.

- بالنسبة إلى أنواع **AMC 4W** تتوفر أجهزة قراءة Wiegand فقط، مع لوحة مفاتيح أو بدونها.
- بالنسبة إلى أجهزة **AMC 4R4**، تتوفر أجهزة القراءة المبينة في الجدول التالي. لا تمزج البروتوكولات في وحدة التحكم نفسها.

اسم القارئ	بروتوكول OSDP	بروتوكول Wiegand	بروتوكول LBUS	بروتوكول HADP
قارئ بصمات الأصابع BEW2	X	X		
قارئ EM Mini Mullion		X		
قارئ HADP	X			
قارئ HADP، لوحة مفاتيح	X			
قارئ HADP، لوحة مفاتيح، شاشة	X			
قارئ HID R15	X			X
قارئ HID R30	X			X
قارئ HID R40	X			X
قارئ HID RK40، لوحة مفاتيح	X			X
قارئ HID RKL55، لوحة مفاتيح وشاشة	X			X
قارئ HID Mini Prox		X		
قارئ HID Prox Pointplus		X		
قارئ LECTUS duo	X	X		
قارئ LECTUS duo، لوحة مفاتيح	X	X		
قارئ LECTUS secure 1000	X	X		
قارئ LECTUS secure 2000	X	X		
قارئ LECTUS secure 4000	X	X		
قارئ LECTUS secure 5000	X	X		
قارئ LECTUS secure 9000		X		
قارئ LECTUS select	X			
قارئ LECTUS select مع لوحة مفاتيح	X			
قارئ Morpho Wave MDPI	X	X		
قارئ OSDP	X			

قارئ OSDP، لوحة مفاتيح	X			
قارئ OSDP، لوحة مفاتيح، شاشة	X			
قارئ SIGMA Lite Bio/ iClass/Prox/Multi	X	X		
قارئ SIGMA Lite/ Lite+iClass/Prox/Multi	X	X		
قارئ لوحة المفاتيح STID	X	X		
قارئ STID قياسي	X	X		
قارئ STID Mullion	X	X		
التعرف على الوجه Vision Pass MDPI	X	X		
قارئ Wiegand		X		
قارئ Wiegand، لوحة مفاتيح		X		
قارئ I-BPR			X	
قارئ I-BPR مع وظيفة الكتابة			X	
قارئ I-BPR، لوحة مفاتيح			X	
HADP				X
HADP K (لوحة مفاتيح)				X
HADP KD (لوحة مفاتيح+شاشة)				X

في حالة **قارئ OSDP** يظهر مربع الحوار كما يلي:



الاتصال الآمن بواسطة OSDP

بشكل افتراضي، تكون خانة الاختيار **تنشيط التشفير** غير محددة. حدد خانة الاختيار هذه إذا كنت تستخدم أجهزة قراءة لديها دعم **OSDPv2 الآمن**.

إذا قمت لاحقًا بإلغاء تنشيط التشفير عن طريق إلغاء تحديد خانة الاختيار، فأعد تعيين جهاز القارئ، وفقًا لإرشادات الشركة المصنعة.

كإجراء احترازي إضافي، تؤدي أي محاولة لمبادلة وحدة قارئ OSDP مكوّنة بوحدة قارئ OSDP مختلفة إلى توليد إنذار في نظام التحكم في الوصول. بإمكان المشغّل أن يتعرف على الإنذار في العميل، وإعطاء إذن المبادلة في الوقت نفسه.

رسالة الإنذار: **رفض مبادلة قارئ OSDP**

الأمر: **السماح بمبادلة قارئ OSDP**

تتوفر الأنواع التالية من أجهزة قراءة OSDP:

OSDP	قارئ OSDP القياسي
لوحة مفاتيح OSDP	قارئ OSDP مع لوحة مفاتيح
لوحة مفاتيح+شاشة OSDP	قارئ OSDP مع لوحة مفاتيح وشاشة

تم اختبار أجهزة قراءة OSDP التالية:

OSDPv1 - وضع غير آمن	LECTUS duo 3000 C - MIFARE classic LECTUS duo 3000 CK - MIFARE classic LECTUS duo 3000 E - MIFARE Desfire EV1 LECTUS duo 3000 EK - MIFARE Desfire EV1
OSDPv2 - وضع غير آمن وآمن	LECTUS secure 2000 RO LECTUS secure 4000 RO LECTUS secure 5000 RO

إشعار!

تحذيرات حول OSDP

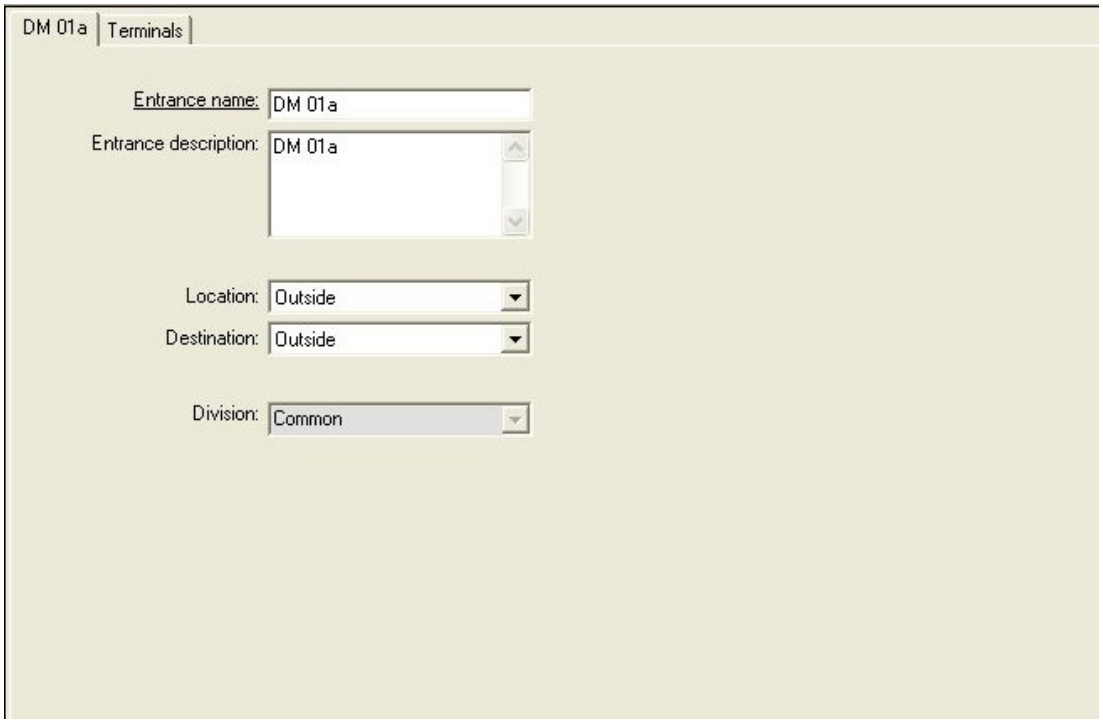
لا تمزج بين عائلات المنتجات، مثلاً **LECTUS duo** و**LECTUS secure** على ناقل OSDP نفسه.

يتم إنشاء مفتاح خاص بالعميل واستخدامه لتشفير بيانات الإرسال إلى قارئ OSDP. تحقق من إجراء عملية نسخ احتياطي للنظام بشكل صحيح.

احتفظ بالمفاتيح في مكان آمن. لا يمكن استرداد المفاتيح المفقودة؛ يمكن إعادة تعيين القارئ إلى إعدادات المصنع الافتراضية فقط.

لأسباب تتعلق بالأمان، لا تمزج بين الأوضاع المشفرة وغير المشفرة على ناقل OSDP نفسه.

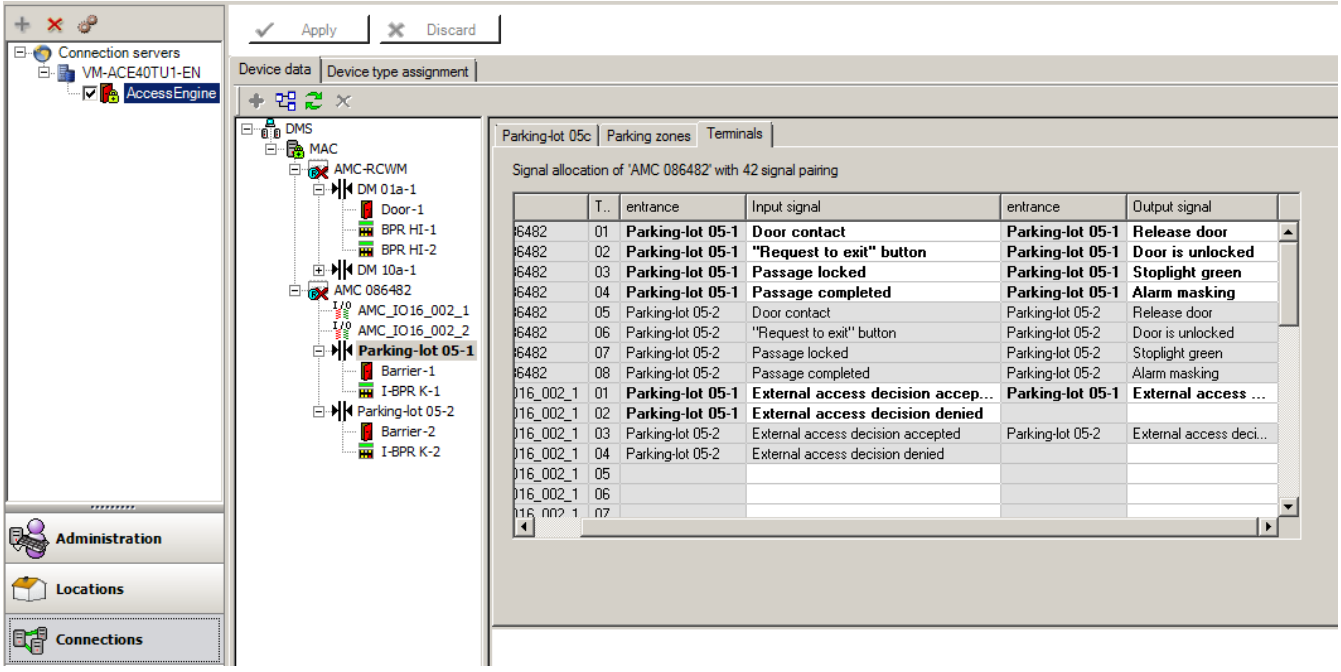
إذا قمت بإلغاء تنشيط التشفير عن طريق إلغاء تحديد خانة الاختيار على علامة تبويب OSDP التابعة للقارئ في محرر الجهاز، فعليك عندئذٍ إعادة تعيين جهاز القارئ، وفقًا لإرشادات الشركة المصنعة.



المعلمة	القيم المحتملة	الوصف
اسم المدخل	أبجدي رقمي، بين 1 و16 حرفًا	ينشئ مربع الحوار اسمًا فريدًا للمدخل، ولكن يمكن الكتابة فوق ذلك الاسم من قِبل المُشغّل الذي يقوم بتكوين المدخل، إذا رغب في ذلك.
وصف المدخل	أبجدي رقمي، من 0 إلى 255 حرفًا	نص وصفي اختياري لعرضه في النظام.
الموقع	أي منطقة محددة (بلا مناطق صف السيارات)	المنطقة المسماة (كما هو محدد في النظام) هي المنطقة التي يتواجد فيها القارئ. تُستخدم هذه المعلومات لمراقبة تسلسل الوصول: إذا حاول شخص استخدام هذا القارئ، ولكن الموقع الحالي لذلك الشخص (حسب تعقبه من قِبل النظام) مختلف عن موقع القارئ، عندئذ يرفض القارئ منح حق الوصول لذلك الشخص.
الوجهة	أي منطقة محددة (بلا مناطق صف السيارات)	المنطقة المسماة، كما هو محدد في النظام، هي المنطقة التي يسمح القارئ بالوصول إليها. تُستخدم هذه المعلومات لمراقبة تسلسل الوصول: إذا استخدم شخص هذا القارئ، فسيتم تحديث موقع الشخص إلى قيمة **الوجهة**.
وقت انتظار قرار الوصول الخارجي	عدد من أعشار الثانية	الوقت الذي تنتظر خلاله وحدة التحكم في الوصول قرارًا من نظام أو جهاز خارجي متصل بأحد مداخلها.
القسم	القسم الذي ينتمي إليه القارئ. القيمة الافتراضية هي **عام**	تُعد ملائمًا فقط إذا كانت ميزة **الأقسام** مرخصة.
منطقة التفعيل (لنموذج المدخل 14 فقط)	حرف واحد: من A إلى Z	سيتم تنشيط المداخل التابعة لمجموعة IDS معًا عن طريق تنشيط أجهزة قراءة المنطقة.

16.3 فحوصات مدخل/مخرج إضافية

بإمكان فحوصات المدخل/المخرج الإضافية، على سبيل المثال، المساعدة في تعريف الزائر استنادًا إلى التعرّف التلقائي على لوحة الرقم (ANPR).
يحصل جهاز AMC على مدخل واحد (1) بواسطة ملامس مدخل/مخرج في AMC:
– فحص مدخل/مخرج إضافي مصرّح به للزائر
يمنع جهاز AMC الوصول في حال وجود إشارة "غير مصرّح به".

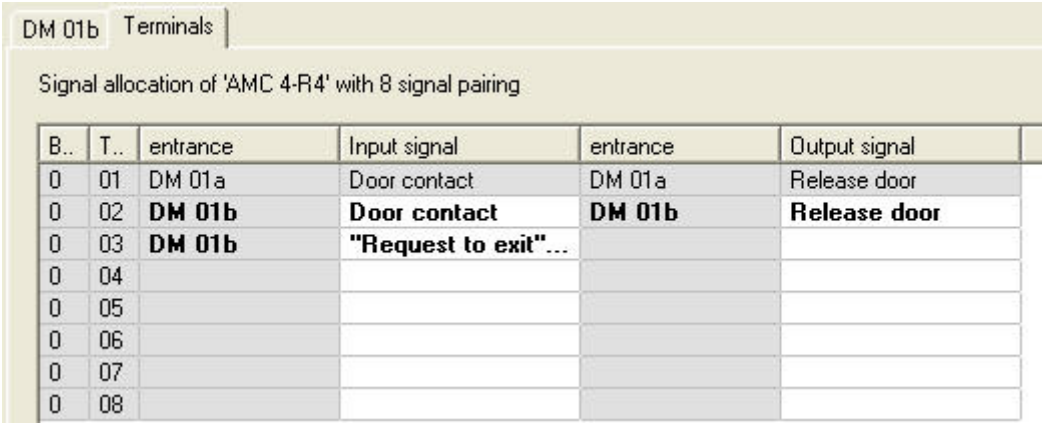


حالة البطاقة	الإشارة = ANPR:1 مصرّح به	الإشارة = 0: ANPR غير مصرّح به
البطاقة المصرّح بها	الوصول	حدث رقم مركبة غير صالح
البطاقة على القائمة المحظورة	غير مصرّح به - قائمة سوداء	غير مصرّح به - قائمة سوداء
البطاقة منتهية الصلاحية	غير مصرّح به - انتهاء الصلاحية	غير مصرّح به - انتهاء الصلاحية
البطاقة غير مصرّح بها لهذا القارئ	غير مصرّح به	غير مصرّح به

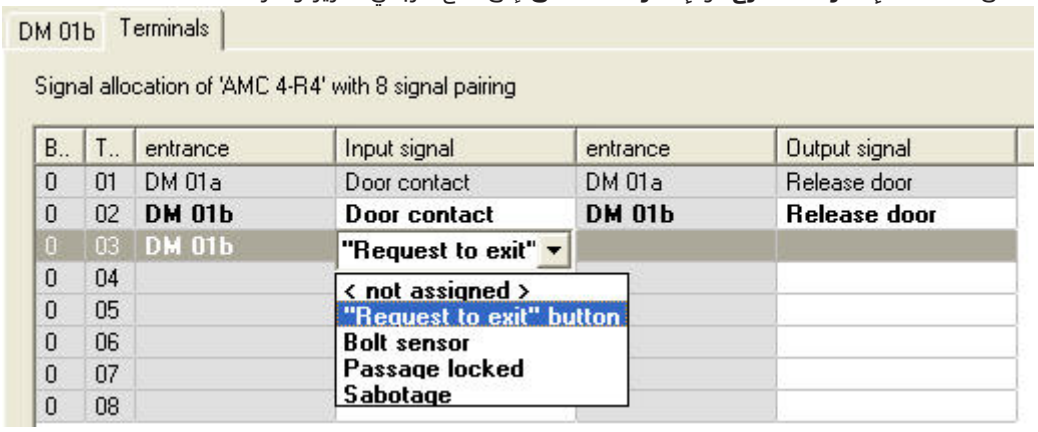
من الممكن فتح الحاجز يدويًا حتى في حال عدم التعرّف على الزائر.
لهذه الوظيفة يتم وصل مفتاح بملامسات مدخل ومخرج وحدة AMC.
تقوم وحدة AMC بتعيين إشارة مخرج **فحص إضافي نشط** قبل إتمام تحليل إشارة المدخل.
إذا لم يكن مالك المركبة ولوحة الترخيص معروفان بعد لدى نظام التحكم في الوصول، فيجب على المشغّل تسجيلهما الآن.

16.4 تكوين المحطات الطرفية في AMC

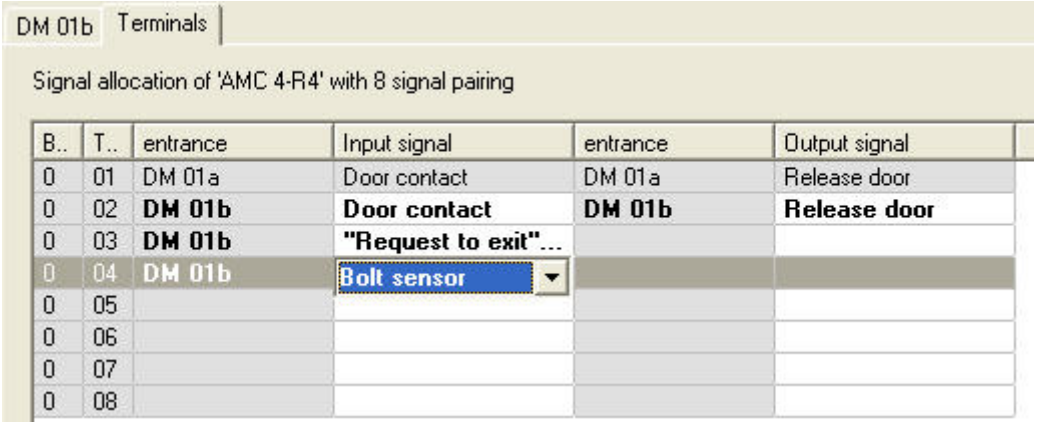
يطابق هذا التبويب بمحتوياته وبنيته تبويب **المحطات الطرفية** في AMC.



مع ذلك، من الممكن هنا إجراء تغييرات في تعيين الإشارات لنموذج المدخل المحدد. يؤدي النقر المزدوج ضمن الأعمدة **إشارة المخرج** أو **إشارة المدخل** إلى فتح مربعي تحرير وسرد.



وبشكل مشابه من الممكن إنشاء إشارات إضافية للمدخل ذي الصلة. ويؤدي النقر المزدوج في أي سطر فارغ إلى ظهور مربع التحرير والسرد المناسب:



تكون تعيينات الإشارات غير المناسبة للمدخل الذي تقوم بتحريره للقراءة فقط، مع خلفية رمادية اللون.
ويمكن تحرير هذه التعيينات فقط عنما يكون المدخل الموافق محددًا.
يتم إعطاء خلفية رمادية مشابهة ولون أمامي باهت لتلك المخارج التي تم تعيين معلماتها في التبويب **مخارج** في جهاز AMC.

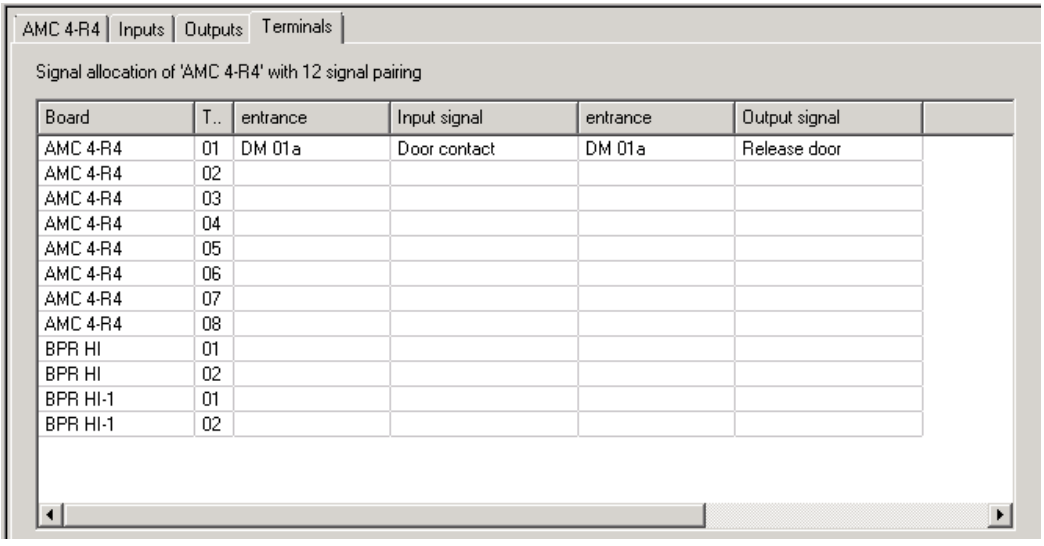
إشعار!
مربعات التحرير والسرد ليست حساسة للسياق بنسبة 100%، وبالتالي من الممكن تحديد إشارات لن تعمل في الواقع الحقيقي. إذا قمت بإضافة أو إزالة إشارات في تبويب **المحطات الطرفية**، فاختبرها كي تتأكد من توافقها فعليًا ومنطقيًا مع المدخل.

تعيين المحطات الطرفية

لكل جهاز AMC وكل مدخل يسرد التبويب **وحدة مرور طرفية** جميع الإشارات لجهاز AMC والتي يبلغ عددها 8 على 8 أسطر منفصلة. ويتم تعليم الإشارات غير المستخدمة باللون الأبيض، والمستخدمة منها باللون الأزرق.

تتضمن القائمة البنية التالية:

- **اللوحة**: ترقيم توسيع Wiegand في AMC وهو (0) أو لوحة توسيع المداخل/المخارج (1 إلى 3)
- **المحطة الطرفية**: عدد الملامسات الموجودة في AMC (من 01 حتى 08) أو لوحة توسيع Wiegand (من 09 إلى 16).
- **المدخل**: اسم المدخل
- **إشارة المخرج**: اسم إشارة المخرج
- **المدخل**: اسم المدخل
- **إشارة المدخل**: اسم إشارة المدخل



Board	T..	entrance	Input signal	entrance	Output signal
AMC 4-R4	01	DM 01a	Door contact	DM 01a	Release door
AMC 4-R4	02				
AMC 4-R4	03				
AMC 4-R4	04				
AMC 4-R4	05				
AMC 4-R4	06				
AMC 4-R4	07				
AMC 4-R4	08				
BPR HI	01				
BPR HI	02				
BPR HI-1	01				
BPR HI-1	02				

تغيير تعيين الإشارات

يتم عرض تعيينات الإشارات المنفصلة فقط (للقراءة فقط) على علامات تبويب المحطات الطرفية التابعة لوحدات التحكم. ومع ذلك، الممكن تغيير أو إعادة وضع إشارات المداخل المحددة على علامات تبويب المحطات الطرفية للمداخل ذات الصلة.

يؤدي النقر المزدوج فوق الإدخال المطلوب تغييره في عمود **إشارة المخرج** أو **إشارة المدخل** إلى تنشيط قائمة منسدلة، بحيث يمكن تحديد قيمة مختلفة كإشارة لنموذج المدخل. إذا حددت **غير معينة**، يتم تحرير الإشارة وبالتالي يمكن استخدامها لمداخل أخرى.

وبالتالي، لا يمكنك تغيير الإشارات فقط، بل يمكنك أيضًا تعيين الإشارات إلى ملامسات أخرى لتحسين استخدام الفولتية المتوفرة. يمكن في وقت لاحق استخدام أي ملامسات حرة أو تم تحريرها لإشارات جديدة أو كوضعيات جديدة للإشارات الموجودة.

إشعار!

مبدئيًا يمكن تحديد كافة إشارات المداخل والمخارج بحرية، ولكن قد لا تكون كل التحديدات مفيدة لكل نماذج الأبواب. على سبيل المثال، من غير المفيد تعيين إشارات IDS إلى نموذج باب (مثل 01 أو 03) لا يدعم IDS. لمزيد من التفاصيل راجع الجدول الموجود في قسم "تعيين الإشارات إلى نماذج الأبواب".

تعيين الإشارات إلى نماذج الأبواب

لتجنب تحديد المعلمات بشكل غير صحيح في القوائم المنسدلة الخاصة بتعيين الإشارات إلى نماذج الأبواب، تقدم تلك القوائم الإشارات المتوافقة مع نموذج الباب المحدد فقط.

جدول إشارات المداخل

إشارات المداخل	الوصف

ملامس الباب	
زر "طلب الخروج"	زر لفتح الباب.
مستشعر المزلاج	تُستخدم للرسائل، فقط. ولا يوجد وظيفة تحكم.
المدخل مقفل	تُستخدم لقفل الباب المقابل في الممرات مؤقتًا. ولكن يمكن استخدامها أيضًا للقفل طويل الأجل.
التلاعب	إشارة تلاعب من وحدة تحكم خارجية.
حاجز دوار في وضع السكون	الحاجز الدوار مغلق.
تم استكمال الممر	تم استكمال الممر بنجاح. وهذه عبارة عن نبضة من وحدة تحكم خارجية.
IDS: جاهز للتفعيل	سيتم التعيين من قِبل IDS، إذا كانت كافة أجهزة الكشف في وضع السكون ويمكن تفعيل IDS.
IDS: مُفعّل	IDS مُفعّل.
IDS: زر طلب التفعيل	زر لتفعيل IDS.
إيقاف الإنذار من الفتح غير المصرح به	سيتم استخدامه في حال أدى ترتيب معين لباب الممر إلى فتح الباب دون تدخل جهاز AMC. لا يُرسل جهاز AMC أي رسالة تتعلق بالاقتحام ولكن رسالة "الباب المحلي مفتوح".
تم قبول قرار الوصول الخارجي	يتم تعيين الإشارة، إذا قبل نظام خارجي الوصول
تم رفض قرار الوصول الخارجي	يتم تعيين الإشارة، إذا رفض نظام خارجي الوصول

جدول إشارات المخارج

إشارات المخارج	**الوصف**
تحرير الباب	
الممر: قفل في الاتجاه المعاكس	قفل الجانب الآخر من الشرَك يتم إرسال هذه الإشارة عندما يُفتح الباب.
إبطال الإنذار	... إلى IDS. يتم تعيينه طالما كان الباب مفتوحًا، ولتجنب ذلك يقوم IDS بإنشاء رسالة تتعلق بالاقتحام.
ضوء التوقف أخضر	مصباح مؤشر - سيتم التحكم به طالما كان الباب مفتوحًا.
انقضى الحد الأقصى لوقت فتح الباب أو تعرض أمان الباب للخطر	إذا تم تثبيت الباب في الوضع المفتوح أو ظل مفتوحًا لفترة طويلة
توصيل الكاميرا	سيتم تنشيط الكاميرا عند بداية الممر.
تحرير الباب الدوار للداخل	
تحرير الباب الدوار للخارج	
الباب غير مقفل	إشارة لإلغاء قفل الباب لفترة مطولة.
IDS: تفعيل	إشارة لتفعيل IDS .
IDS: تعطيل	إشارة لتعطيل IDS.

تم تنشيط قرار الوصول الخارجي	يجب تعيين إشارة لتنشيط نظام الوصول الخارجي

تعيين جدول نماذج الأبواب إلى إشارات المداخل والمخارج

يسرد الجدول التالي التعيينات المفيدة للإشارات ونماذج الأبواب.

نموذج الباب	الوصف	إشارات المداخل	إشارات المخارج
01	باب بسيط مع قارئ للدخول والخروج أجهزة قراءة الوقت والحضور قرار الوصول الخارجي متوفر	- ملامس الباب - زر "طلب الخروج" - مستشعر المزلاج - المدخل مقفل - التلاعب - تمكين الفتح المحلي - تم قبول قرار الوصول الخارجي - تم رفض قرار الوصول الخارجي	- تحرير الباب - الممر: قفل في الاتجاه المعاكس - إبطال الإنذار - ضوء التوقف أخضر - توصيل الكاميرا - انقضى الحد الأقصى لوقت فتح الباب أو تعرض أمان الباب للخطر - تم تنشيط قرار الوصول الخارجي
03	حاجز دوار مع قارئ للدخول والخروج أجهزة قراءة الوقت والحضور قرار الوصول الخارجي متوفر	حاجز دوار في وضع السكون - زر "طلب الخروج" - المدخل مقفل - التلاعب - تم قبول قرار الوصول الخارجي - تم رفض قرار الوصول الخارجي	- الممر: قفل في الاتجاه المعاكس - تحرير الباب الدوار للداخل - تحرير الباب الدوار للخارج - إبطال الإنذار - توصيل الكاميرا - انقضى الحد الأقصى لوقت فتح الباب أو - تعرض أمان الباب للخطر - تم تنشيط قرار الوصول الخارجي
05	مدخل أو مخرج ساحة الانتظار - 24 منطقة انتظار كحد أقصى أجهزة قراءة الوقت والحضور قرار الوصول الخارجي متوفر	- ملامس الباب - زر "طلب الخروج" - المدخل مقفل - تم استكمال الممر - تم قبول قرار الوصول الخارجي - تم رفض قرار الوصول الخارجي	- تحرير الباب - إبطال الإنذار - ضوء التوقف أخضر - انقضى الحد الأقصى لوقت فتح الباب أو - تعرض أمان الباب للخطر - الباب غير مقفل - تم تنشيط قرار الوصول الخارجي
06	أجهزة قراءة الوقت والحضور		
07	المصعد - 56 طابقًا كحد أقصى		
09	قارئ دخول أو خروج العربات وزر يعمل بالضغط	- ملامس الباب - زر "طلب الخروج" - المدخل مقفل - تم استكمال الممر	- تحرير الباب - إبطال الإنذار - ضوء التوقف أخضر

	أجهزة قراءة الوقت والحضور قرار الوصول الخارجي متوفر	- تم قبول قرار الوصول الخارجي - تم رفض قرار الوصول الخارجي	- انقضى الحد الأقصى لوقت فتح الباب أو - تعرض أمان الباب للخطر - الباب غير مقفل - تم تنشيط قرار الوصول الخارجي
10	باب بسيط مع قارئ للدخول والخروج وتفعيل/تعطيل IDS أجهزة قراءة الوقت والحضور قرار الوصول الخارجي متوفر	- ملامس الباب - زر "طلب الخروج" - IDS: جاهز للتفعيل - IDS: مُفعّل - التلاعب - IDS: طلب التفعيل - تم قبول قرار الوصول الخارجي - تم رفض قرار الوصول الخارجي	- تحرير الباب - توصيل الكاميرا - IDS: تفعيل - IDS: تعطيل - انقضى الحد الأقصى لوقت فتح الباب أو - تعرض أمان الباب للخطر - تم تنشيط قرار الوصول الخارجي
14	باب بسيط مع قارئ للدخول والخروج وتفعيل/تعطيل IDS أجهزة قراءة الوقت والحضور	- ملامس الباب - زر "طلب الخروج" - IDS: جاهز للتفعيل - IDS: مُفعّل - التلاعب - IDS: طلب التفعيل	- تحرير الباب - توصيل الكاميرا - IDS: تفعيل - انقضى الحد الأقصى لوقت فتح الباب أو - تعرض أمان الباب للخطر
15	ملامسات رقمية		

تعيين الإشارات إلى أجهزة القراءة

يمكن تحسين أجهزة القراءة التسلسلية (مثل أجهزة القراءة على AMC2 4R4) وأجهزة قراءة OSDP باستخدام إشارات مداخل/مخارج محلية. وبهذه الطريقة، يمكن توفير إشارات إضافية واختصار المسارات الكهربائية إلى ملامسات الباب.

عند إنشاء قارئ تسلسلي يُظهر تبويب **المحطات الطرفية** الخاص بالمدخل المناظر إشارتي مدخل وإشارتي مخرج لكل قارئ تحت وحدة التحكم وإشارات لوحات التوسيع (إن وجدت).

إشعار!

يتم إنشاء إدخالات القائمة هذه لكل قارئ تسلسلي بغض النظر إن كان يتضمن مداخل/مخارج محلية أو لا.

لا يمكن تعيين إشارات القارئ المحلية هذه إلى وظائف وتحديد معلماتها كتلك الخاصة بوحدات التحكم واللوحات. وهي لا تظهر أيضًا على علامتي التبويب **إشارة المدخل** و**إشارة المخرج**، كما لا يمكن استخدامها للمصاعد (مثلاً لتجاوز حد 56 طابقًا). ولهذا السبب فهي مناسبة جدًا للتحكم المباشر بالأبواب (مثل طرق الباب أو تحريره). ومع ذلك، فهذا يؤدي إلى تحرير إشارات وحدة التحكم لتنفيذ وظائف أكثر تعقيدًا ذات معلمات محددة.

تحرير الإشارات

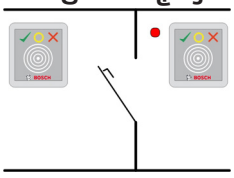
عند إنشاء مدخل يُظهر تبويب **المحطات الطرفية** الخاص بالمدخل المناظر إشارتي مدخل وإشارتي مخرج لكل قارئ تحت وحدة التحكم. يعرض عمود اللوحة اسم القارئ. يتم تعيين الإشارات القياسية للمدخل بشكل افتراضي إلى أول إشارات حرة على وحدة التحكم. ولنقل هذه الإشارات إلى الإشارات الخاصة بالقارئ يجب أولاً حذفها من مواضعها الأصلية. لتنفيذ ذلك حدد إدخال القائمة **<غير معينة>**

انقر نقرًا مزدوجًا ضمن عمود **إشارة المدخل** أو **إشارة المخرج** في القارئ لمشاهدة قائمة بالإشارات المحتملة لنموذج الباب المختار، وبالتالي إعادة وضع الإشارة. يمكن عرض هذه الإشارات، مثلها مثل جميع الإشارات، في تبويب **المحطات الطرفية** لوحدة التحكم، ولكن لن يتم تحريرها هناك.

إشعار!
لا يمكن مراقبة حالة إشارات القارئ.
يمكن استخدامها فقط للباب الذي ينتمي إليه القارئ.

16.5 الإشارات المعرّفة مسبقًا لنماذج الأبواب

نموذج المدخل 01



متغيرات النموذج:

01a	باب عادي مع قارئ دخول **و**خروج
01b	باب عادي مع قارئ دخول وزر يعمل بالضغط
01c	باب عادي مع قارئ دخول **أو** خروج

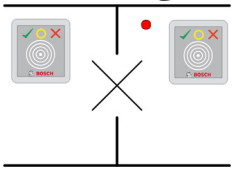
الإشارات المحتملة:

إشارات المداخل	إشارات المخارج
ملامس الباب	تحرير الباب
زر "طلب الخروج"	الممر: قفل في الاتجاه المعاكس
التلاعب	ضوء التوقف أخضر
إيقاف الإنذار من الفتح غير المصرح به	توصيل الكاميرا
	انقضى الحد الأقصى لوقت فتح الباب أو تعرض أمان الباب للخطر

إشعار!
يمكن تحديد معلمات لوظائف منفردة، خصوصًا قفل الاتجاه المقابل، باستخدام نموذج الباب DM 03، فقط.

يتم تنشيط إبطال الإنذار فقط عندما يكون وقت إبطال الإنذار قبل فتح الباب أكبر من 0.
بإمكان نموذج المدخل هذا أن يكون مفيدًا أيضًا لمداخل المركبات، وفي هذه الحالة يُنصح أيضًا بقارئ ثانوي للشاحنات والسيارات.

نموذج المدخل 03



متغيرات النموذج:

03a	حاجز دوار قابل للعكس مع قارئ دخول **و**خروج
03b	حاجز دوار قابل للعكس مع قارئ دخول وزر يعمل بالضغط
03c	حاجز دوار مع قارئ دخول **أو** خروج

الإشارات المحتملة:

إشارة المدخل	**إشارات المخارج**
حاجز دوار في وضع السكون	تحرير الباب الدوار للداخل
زر "طلب الخروج"	تحرير الباب الدوار للخارج
التلاعب	المدخل مقفل
إيقاف الإنذار من الفتح غير المصرح به	توصيل الكاميرا
	انقضى الحد الأقصى لوقت فتح الباب أو تعرض أمان الباب للخطر
إشارات إضافية باستخدام خيار **الشرَك**:	
المدخل مقفل	الممر: قفل في الاتجاه المعاكس
	إبطال الإنذار

ملاحظات تكوين الشرَك:
عندما يكون الباب الدوار في الوضع العادي يتم تشغيل أول إشارة مدخل في كل أجهزة القراءة الموصولة. إذا تم إبراز بطاقة وإذا كان لدى مالكها حقوق وصول لهذا المدخل، عندئذ:
- إذا تم إبرازها عند قارئ الدخول، يتم تعيين إشارة المخرج الأولى عند قارئ الدخول طوال وقت التنشيط.
- إذا تم إبرازها عند قارئ الخروج، يتم تعيين إشارة المخرج الثانية عند قارئ الخروج طوال وقت التنشيط.

عند الضغط على زر طلب الخروج (REX)، يتم تعيين إشارة المدخل الثانية وإشارة المخرج الثانية. خلال هذا الوقت يمكن استخدام الباب الدوار بالاتجاه الممكّن.

نموذج المدخل 05c

متغير النموذج:

05c	قارئ دخول **أو** خروج للوصول إلى ساحة الانتظار

الإشارات المحتملة لنموذج المدخل هذا:

إشارات المداخل	**إشارات المخارج**
ملامس الباب	تحرير الباب

زر "طلب الخروج"	الباب غير مقفل
المدخل مقفل	ضوء التوقف أخضر
تم استكمال الممر	إبطال الإنذار
	انقضى الحد الأقصى لوقت فتح الباب أو تعرض أمان الباب للخطر

يجب تكوين المدخل والمخرج في ساحة الانتظار على وحدة التحكم نفسها. سيتعذر على وحدة التحكم، إذا تم تعيين الوصول إلى ساحة الانتظار لها، التحكم في نماذج الأبواب الأخرى. بالنسبة إلى المدخل الذي يؤدي إلى ساحة الانتظار، يمكنك تعيين قارئ دخول واحد فقط (بدون قارئ خروج). يسمح لك تعيين قارئ دخول ثم تحديد نموذج الباب من جديد بتحديد قارئ الخروج. يمكنك تحديد ما يصل إلى 24 منطقة فرعية لكل ساحة انتظار، ويجب تضمين واحدة منها في تخويلات البطاقة لكي تعمل البطاقة بشكل صحيح.

نموذج المدخل 06

متغيرات النموذج

06a	قارئ دخول **و**خروج للوقت والحضور
06c	قارئ دخول **أو** خروج للوقت والحضور

لا تتحكم أجهزة القراءة التي يتم إنشاؤها باستخدام نموذج الباب هذا بالأبواب أو الحواجز، بل فقط تعيد توجيه بيانات البطاقات إلى نظام تسجيل الوقت والحضور. تقع أجهزة القراءة هذه عادةً في أماكن يخضع الوصول إليها للرقابة.
وبالتالي، لا يتم تحديد أي إشارات.

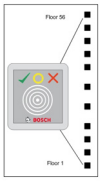
إشعار!
لتمكين إنشاء أزواج حجوزات صالحة (وقت الدخول ووقت الخروج) في نظام الوقت والحضور، من الضروري تحديد معلمات لجهازي قراءة منفصلين بواسطة نموذج الباب 06: أحدهما لتسجيل وقت الدخول والآخر لتسجيل وقت الخروج.

استخدم المتغير **a** عندما لا يكون قارئ الدخول منفصلاً عن قارئ الخروج. استخدم المتغير **c** إذا كان قارئ الدخول منفصلاً عن قارئ الخروج من الناحية المكانية، أو إذا تعذر عليك توصيل جهازي القراءة بوحدة التحكم نفسها. احرص على تحديد أحد جهازي القراءة كقارئ على الجهة الداخلية والآخر كقارئ على الجهة الخارجية.
وكما هو الحال مع أي مدخل، من الضروري إنشاء وتعيين التخويلات. تسرد علامة تبويب **إدارة الوقت** في مربعي الحوار **تخويلات الوصول** و**تخويلات المنطقة/الوقت** جميع أجهزة قراءة الوقت والحضور التي تم تحديدها. يمكنك تنشيط قارئ واحد على الأقل في الاتجاه الداخلي وقارئ واحد في الاتجاه الخارجي.
يمكن تعيين تخويلات أجهزة قراءة الوقت والحضور إلى جانب تخويلات وصول أخرى، أو كتخويلات منفصلة.
عند وجود أكثر من قارئ واحد للوقت والحضور لاتجاه معين، من الممكن عندئذٍ تعيين بعض حاملي البطاقات إلى أجهزة قراءة معينة. سيقوم القارئ بتسجيل وتخزين أوقات الحضور للمستخدمين المعيّنين والمخوّلين فقط.

إشعار!
تؤثر أيضًا ميزات أخرى للتحكم في الوصول على سلوك أجهزة قراءة الوقت والحضور. وبالتالي، بإمكان القوائم السوداء أو نماذج الوقت أو تواريخ انتهاء الصلاحية أن تمنع أيضًا قارئ الوقت والحضور من تسجيل أوقات الوصول.

يتم تخزين أوقات الدخول والخروج المسجلة في ملف نصي في الدليل:
\SW_installation_folder>\AccessEngine\AC\TAExchange>
باسم TAccExc_EXP.txt ويتم الاحتفاظ بها حتى تصديرها إلى نظام تسجيل الوقت والحضور.
تُرسل بيانات الحجز بالتنسيق التالي:
.ddMMyyyy;hhmm[s];Direction [0,1]; AbsenceReason; Personnel-Nr
d=اليوم، M=الشهر، y=السنة، h=الساعة، m=الدقيقة، s=التوقيت الصيفي، 0=خارجي، 1=داخلي
يحتوي ملف التصدير على جميع الحجوزات بترتيب زمني. تُستخدم الفاصلة المنقوطة كفاصل حقول في الملف.

متغيرات نموذج المدخل 07



متغيرات النموذج:

07a	مصعد مع 56 طابقًا كحد أقصى
07c	مصعد مع 56 طابقًا كحد أقصى ونموذج الوقت

نموذج المدخل 07a
الإشارات:

إشارة المدخل	إشارات المخارج
	تحرير <اسم الطابق>
	إشارة مخرج واحدة لكل طابق محدد، مع حد أقصى من 56 طابقًا.

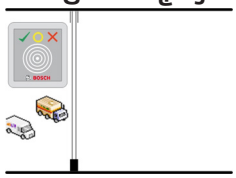
عندما يقوم مالك البطاقة باستدعاء المصعد، يمكنه تحديد فقط تلك الطوابق المخوّلة لهذه البطاقة.
ولا يمكن الخلط بين نماذج أبواب المصعد ونماذج الأبواب الأخرى على وحدة التحكم نفسها. باستخدام لوحات التوسيع، يمكن تحديد عدد من الطوابق يصل إلى 56 طابقًا لكل مصعد على جهاز AMC. ويجب أن تحتوي تخويلات البطاقة على المصعد نفسه وطابق واحد على الأقل.

نموذج المدخل 07c
الإشارات:

إشارة المدخل	إشارة المخرج
مفتاح المدخل <اسم الطابق>	تحرير <اسم الطابق>
يوجد مدخل دخول وخروج لكل طابق محدد - حتى 56 طابقًا.	

عندما استدعاء المصعد والضغط على زر تحديد الطابق (ونتيجة لذلك، الحاجة إلى إشارات المدخل)، يتم التحقق من تخويلات البطاقة للتأكد من أنها تشتمل على الطابق المحدد.
بالإضافة إلى ذلك، يسمح نموذج الباب هذا بتحديد أي طوابق متاحة **للوصول العمومي**، مما يعني أن التخويلات لن تخضع لأي عملية فحص فيما يتعلق بهذا الطابق، وأنه بإمكان أي شخص أن يستخدم المصعد للوصول إليه. ومع ذلك، قد يخضع الوصول العمومي بحد ذاته **لنموذج وقت** يقيّده بحيث يقتصر على ساعات معينة في أيام معينة. وسيتم تنفيذ عمليات فحص التخويلات خارج هذه الساعات كالمعتاد.
ولا يمكن الخلط بين نماذج أبواب المصعد ونماذج الأبواب الأخرى على وحدة التحكم نفسها. باستخدام لوحات التوسيع، يمكن تحديد عدد من الطوابق يصل إلى 56 طابقًا لكل مصعد على جهاز AMC. ويجب أن تحتوي تخويلات البطاقة على المصعد نفسه وطابق واحد على الأقل.

نموذج المدخل 09

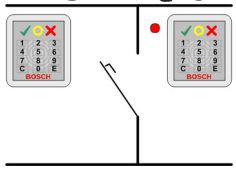


الإشارات المحتملة:

إشارات المداخل	إشارات المخارج
ملامس الباب	تحرير الباب
زر "طلب الخروج"	الباب مفتوح على المدى الطويل
المدخل مقفل	ضوء إشارة المرور أخضر
تم استكمال الممر	إبطال الإنذار
	انقضى الحد الأقصى لوقت فتح الباب أو تعرض أمان الباب للخطر

للتحكم في الحواجز، يُفترض استخدام تحكم أساسي (SPS). يمكنك تكوين هذا المدخل والمخرج على أجهزة AMC مختلفة، بشكل يختلف عن **نموذج الباب 5c**. علاوةً على ذلك، لا توجد مناطق فرعية، ولكن فقط تخويل عام لمنطقة الانتظار.

نموذج المدخل 10



متغيرات النموذج:

10a	باب عادي مع قارئ للدخول **و**الخروج **و**تفعيل/تعطيل نظام اكتشاف الاقتحام (IDS)
10b	باب عادي مع مدخل وزر طلب الخروج (REX) وتفعيل/تعطيل IDS
10e	باب عادي مع مدخل وزر طلب الخروج (REX) وتفعيل/تعطيل IDS غير مركزي

الإشارات المحتملة:

إشارات المداخل	إشارات المخارج
ملامس الباب	تحرير الباب
IDS: مُفعّل	IDS: تفعيل
IDS: جاهز للتفعيل	IDS: تعطيل [10e DM فقط]
زر "طلب الخروج"	توصيل الكاميرا
مستشعر المزلاج	انقضى الحد الأقصى لوقت فتح الباب أو تعرض أمان الباب للخطر
التلاعب	
إيقاف الإنذار من الفتح غير المصرح به	

IDS: زر طلب التفعيل	

إشعار!
يحتاج نموذج الباب هذا إلى أجهزة قراءة مزودة بلوحات مفاتيح. ويحتاج أصحاب البطاقات إلى **رموز PIN** لتفعيل/تعطيل IDS.

يجب تنفيذ إجراءات مختلفة تبعًا لأجهزة القراءة المثبتة.

أجهزة القراءة التسلسلية (بما في ذلك I-BPR وHADP وOSDP)
يمكنك التفعيل بالضغط على المفتاح **7** والتأكيد بالضغط على المفتاح Enter (#). بعد ذلك، قدّم البطاقة، وأدخل رمز PIN وأكد مرة أخرى بالضغط على المفتاح Enter (#).
يمكنك التعطيل عن طريق تقديم البطاقة، وإدخال رمز PIN ثم التأكيد بالضغط على المفتاح Enter (#).

أجهزة القراءة Wiegand (بما في ذلك بروتوكول BPR التسلسلي)
يمكنك التفعيل عن طريق الضغط على 7 وتقديم البطاقة وإدخال رمز PIN. لا حاجة إلى التأكيد بالضغط على المفتاح Enter.
يمكنك التعطيل عن طريق تقديم البطاقة وإدخال رمز PIN. يحدث التعطيل وتحرير الباب في الوقت نفسه.

ميزات خاصة لنموذج الباب DM 10e:
في حين يتميز كل مدخل في نموذجي الأبواب 10a و10b بمنطقة أمان خاصة به، يمكن تجميع مداخل متعددة في وحدات في نموذج الباب 10e. وبإمكان أي قارئ في هذه المجموعة تفعيل أو تعطيل الوحدة بكاملها. ثمة حاجة إلى إشارة المخرج **تعطيل IDS** لإعادة تعيين الحالة التي عيّنها أي واحد من أجهزة القراءة في المجموعة.
الإشارات:
- نموذجا الأبواب 10a و10b:
  - - يتم تشغيل التفعيل بواسطة إشارة ثابتة
  - - يتم تشغيل التعطيل نتيجة انقطاع الإشارة الثابتة.
- نموذج الباب 10e:
  - - يتم تشغيل التفعيل والتعطيل بواسطة نبضة إشارة مدتها ثانية واحدة.

باستخدام مرحّل ثنائي الاستقرار، يمكن التحكم في IDS من عدة أبواب. وللقيام ذلك، تحتاج إشارات جميع الأبواب إلى عملية OR عند المرحّل. يجب تكرار إشارات **IDS مفعّل** و**IDS جاهز للتفعيل** عند كل الأبواب المشاركة.

المداخل الخاصة
بالنسبة لنماذج المدخل ذات الميزات الخاصة، مثل:
- المصاعد
- اكتشاف الاقتحام
- المفاتيح الرقمية أو الثنائية العامة
- الشرَك

راجع الفصل المخصص للمداخل الخاصة.

راجع
- المداخل الخاصة, الصفحة *89*

16.6 المداخل الخاصة

16.6.1 المصاعد (DM07)

ملاحظات عامة حول المصاعد (نموذج المدخل 07)

لا يمكن الخلط بين المصاعد ونماذج الأبواب الأخرى على وحدة تحكم AMC نفسها.

لا يمكن استخدام المصاعد مع خيارات القارئ **وصول المجموعة** أو **يلزم وجود ملاحظ**

يمكن تحديد ما يصل إلى 8 طوابق على جهاز AMC واحد. تقدم لوحة توسيع AMC مخارج إضافية (8 أو 16) لكل لوحة توسيع.

وبالتالي، فإن استخدام العدد الأقصى للوحات التوسيع الأكبر حجمًا يسمح بتكوين ما يصل إلى 56 طابقًا مع أجهزة قراءة RS485 و 64 طابقًا مع أجهزة قراءة Wiegand، إذا تم استخدامها مع لوحة توسيع Wiegand خاصة.

الاختلافات بين نموذجي الأبواب 07a و07c

في مربعات حوار تخويلات الوصول، يمكنك تعيين طوابق معينة يسمح لشخص معين بالوصول إليها.

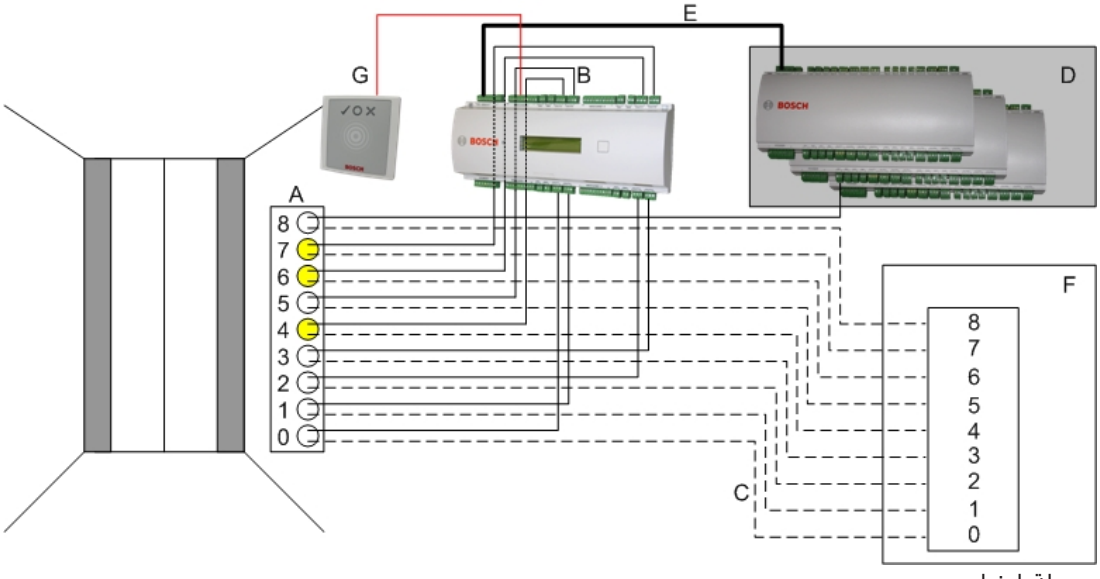
إذا تم إنشاء المصعد باستخدام نموذج المدخل **07a**، يقدم حامل البطاقة بطاقة هويته وتصبح الطوابق التي لديه إذن الدخول إليها متاحة.

فيما يتعلق بنموذج المدخل **07c**، يتحقق النظام من التخويل الممنوح للطابق المحدد بعد اختياره من قِبل الشخص. وتصبح الطوابق التي تحمل علامة **الوصول العمومي** متاحة للجميع بصرف النظر عن التخويل.

ومع نموذج وقت، يمكن أن تقتصر هذه الوظيفة المتاحة للجمهور على نموذج الوقت المحدد. وسيتم فحص التصريحات الممنوحة للطابق المحدد خارج هذه الفترة.

مخطط تمديد أسلاك المصاعد:

تُظهر الصورة التالية مخطط توصيل مصعد باستخدام نموذج الباب 07a.

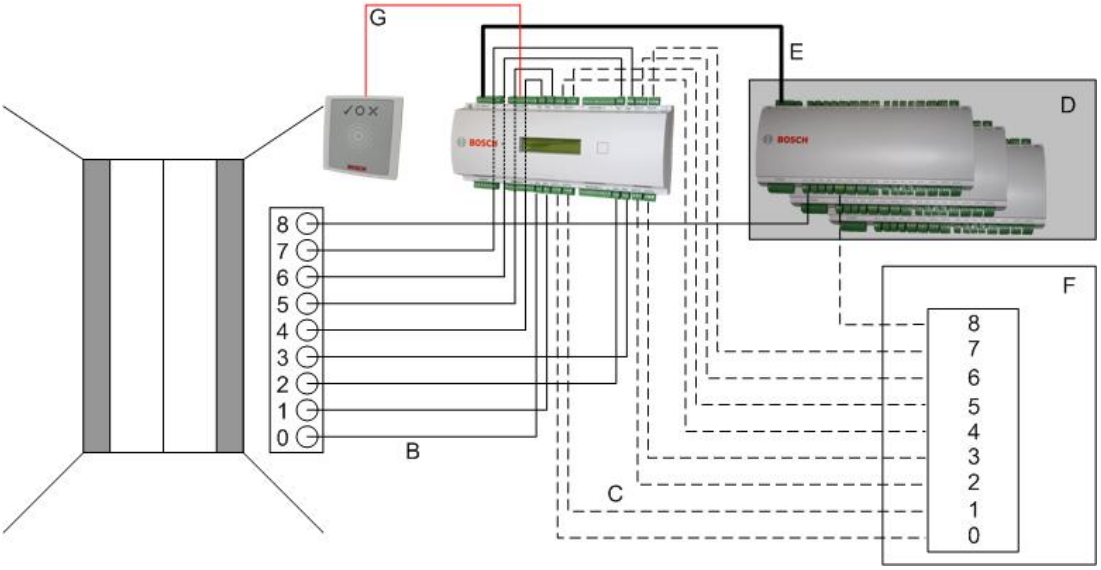


وسيلة إيضاح:

- A = لوحة مفاتيح المصعد
- B = (خط مستمر) إشارات مخارج جهاز AMC
- C = (خط متقطع) وصلة إلى عناصر التحكم بالمصعد
- D = يمكن توصيل ما يصل إلى ثلاث لوحات إدخال/إخراج بجهاز AMC، إذا لم تكن مداخله ومخارجه الثمانية كافية.
- E = التزويد بالطاقة والبيانات من جهاز AMC إلى لوحات الإدخال/الإخراج
- F = محدد الطوابق في المصعد

– G = القارئ. هناك قارئان قابلان للتكوين لكل مصعد.

تُظهر الصورة التالية مخطط توصيل مصعد باستخدام نموذج الباب 07c.



وسيلة إيضاح:

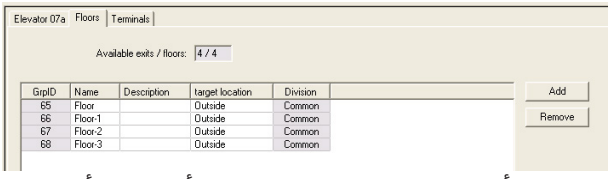
– B = (خط مستمر) إشارات مخارج جهاز AMC
– C = (خط متقطع) وصلة إلى عناصر التحكم بالمصعد
– D = يمكن توصيل ما يصل إلى ثلاث لوحات إدخال/إخراج بجهاز AMC، إذا لم تكن مداخله ومخارجه الثمانية كافية.
– E = التزويد بالطاقة والبيانات من جهاز AMC إلى لوحات الإدخال/الإخراج
– F = محدد الطوابق في المصعد
– G = القارئ. هناك قارئان قابلان للتكوين لكل مصعد.

بشكل مشابه لساحات الانتظار، لدى المصاعد المعلمة **عام.** يمكن تعيين هذه المعلمة لكل طابق بشكل منفرد. إذا تم تنشيط المعلمة **عام** فلن يتم التحقق من تخويلات الوصول - وبالتالي يمكن لحامل البطاقة في المصعد اختيار الطابق.

عند الحاجة، يمكن تعيين نموذج وقت لنموذج المدخل: عندها سيتم التحقق من التخويلات خارج المناطق الزمنية المحددة.

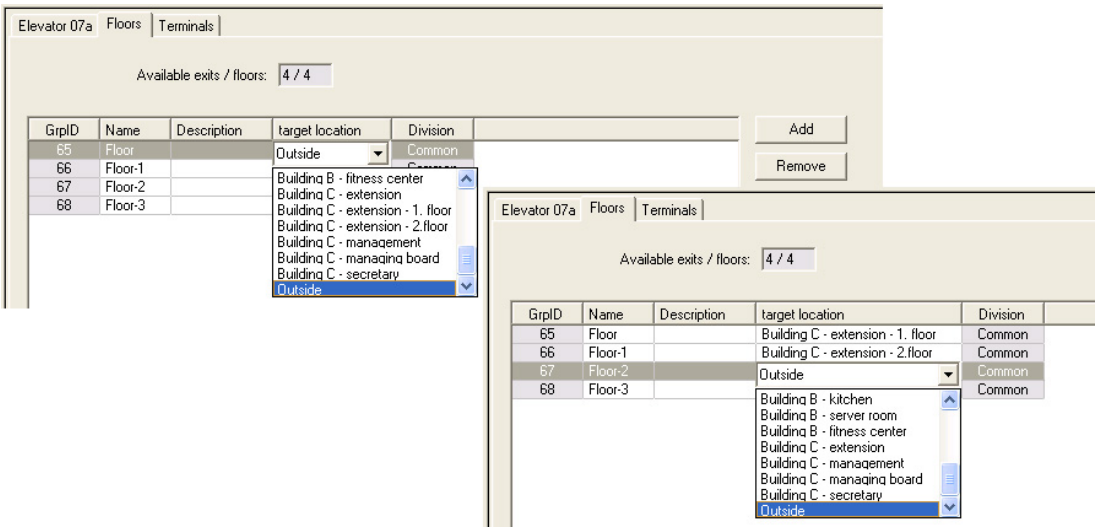
طوابق لنموذج المدخل 07

استخدم التبويب **طوابق** لإضافة وإزالة طوابق للمصعد، باستخدام الأزرار **إضافة** و**إزالة**.

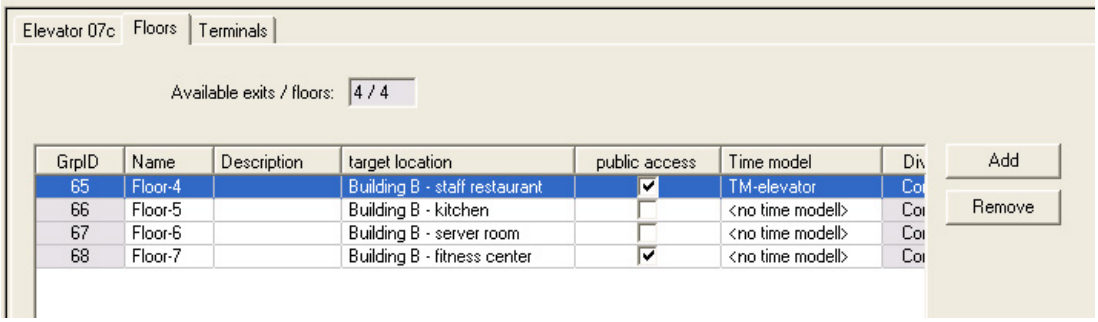


بإمكان الأماكن المستهدفة في الطابق أن تكون أي **مناطق** باستثناء مناطق انتظار السيارات ومناطق صف السيارات.

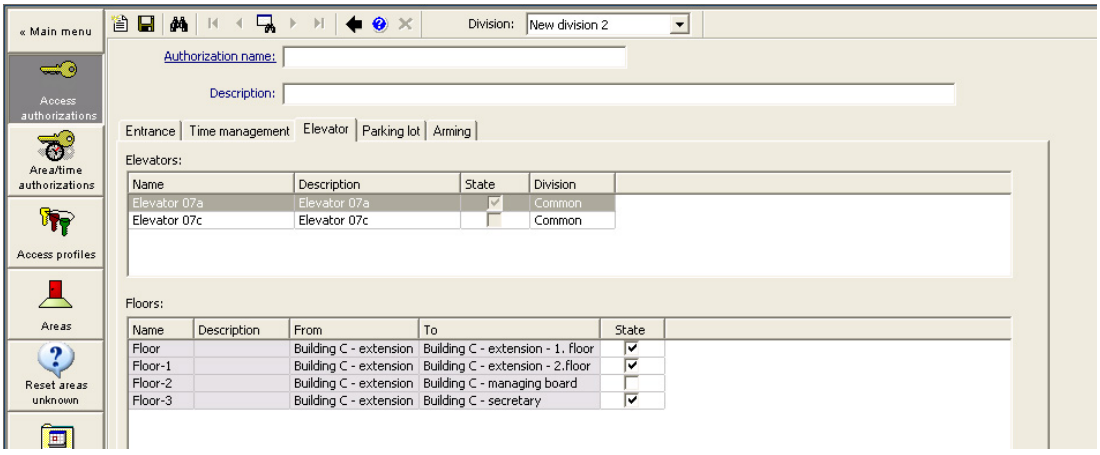
يمكن تعيين منطقة واحدة فقط لكل طابق. ولهذا ينخفض عدد المناطق المتوفرة للاختيار في مربعي التحرير والسرد بعد كل عملية تعيين، وبالتالي يتم تجنب التعيينات المتكررة غير المقصودة.



عند استخدام نموذج المدخل 07a من الممكن جعل طوابق معينة قابلة للوصول من قِبل العموم من خلال تحديد المربع **وصول عام**. في هذه الحالة لن يتم تنفيذ عملية التحقق من التخويلات. وبالرغم من ذلك سيؤدي التعيين الإضافي **نموذج الوقت** إلى تقييد الوصول وفق الفترات المعرّفة مسبقًا.



في علامة تبويب **المصعد** فوق مربع القائمة العلوي في مربعات حوار **تخويلات الوصول** و**تخويلات المنطقة/الوقت**، حدد أولاً المصعد المطلوب، ثم حدد أدناه الطوابق المسموح لحامل البطاقة الوصول إليها.



16.6.2 نماذج الأبواب مع إنذارات التسلل (DM14)

المقدمة

بطريقة مغايرة لنموذج المدخل 10 (DM10)، بإمكان **DM14** تفعيل نظام إنذار التسلل وإلغاء تفعيله، أو IDS في منطقة تفعيل معينة. يمكن أيضًا تفعيل مدخل DM14 لمنح الوصول لحامل البطاقة الذي يلغي التفعيل منه، شريطة أن تتوفر لدى حامل البطاقة جميع الأذونات الأخرى المطلوبة.

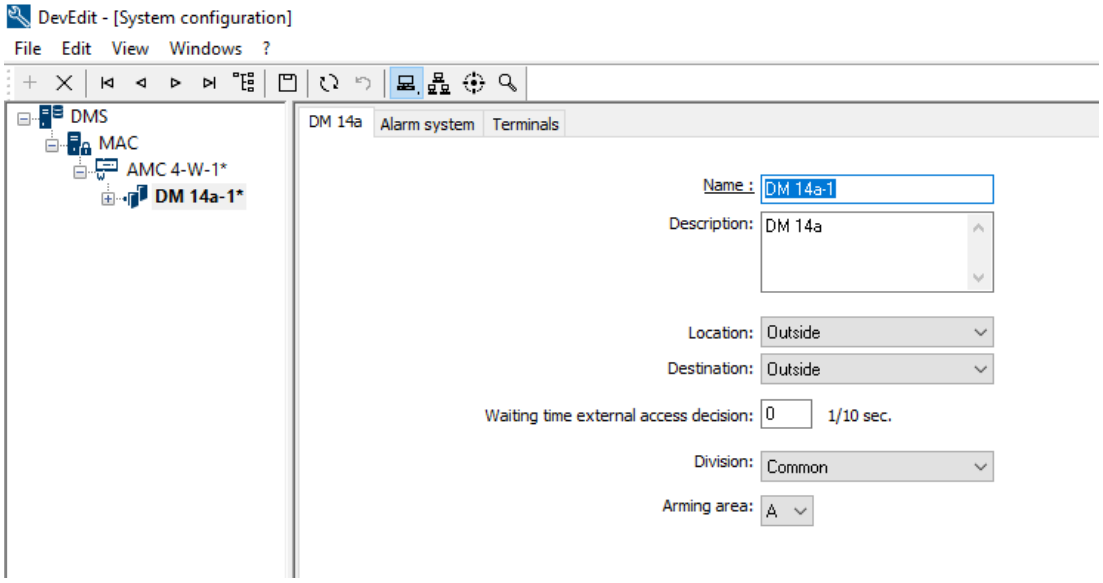
يتضمن إجراء تكوين DM14 في محرر الجهاز ومدير مربع الحوار هذه المهام:

1. تعيين المعلمات العامة لتحديد المدخل ومنطقة تفعيله.
2. تعيين المعلمات الخاصة لتعيين الإجراء الدقيق الخاص بإلغاء تفعيل المنطقة.
3. تحديد إشارات المداخل والمخارج الخاصة بنظام IDS على الوحدات الطرفية في وحدة التحكم في باب المدخل.
4. تضمين أذونات التفعيل/إلغاء التفعيل في تخويلات الوصول لحاملي البطاقات هؤلاء الذين سيقومون بتشغيل مداخل DM 14.

تقدم الأقسام التالية وصفًا للمهام.

المعلمات العامة

على علامة التبويب الأولى، **DM14a** أو **DM14b**، عيّن قيم المعلمات التالية.

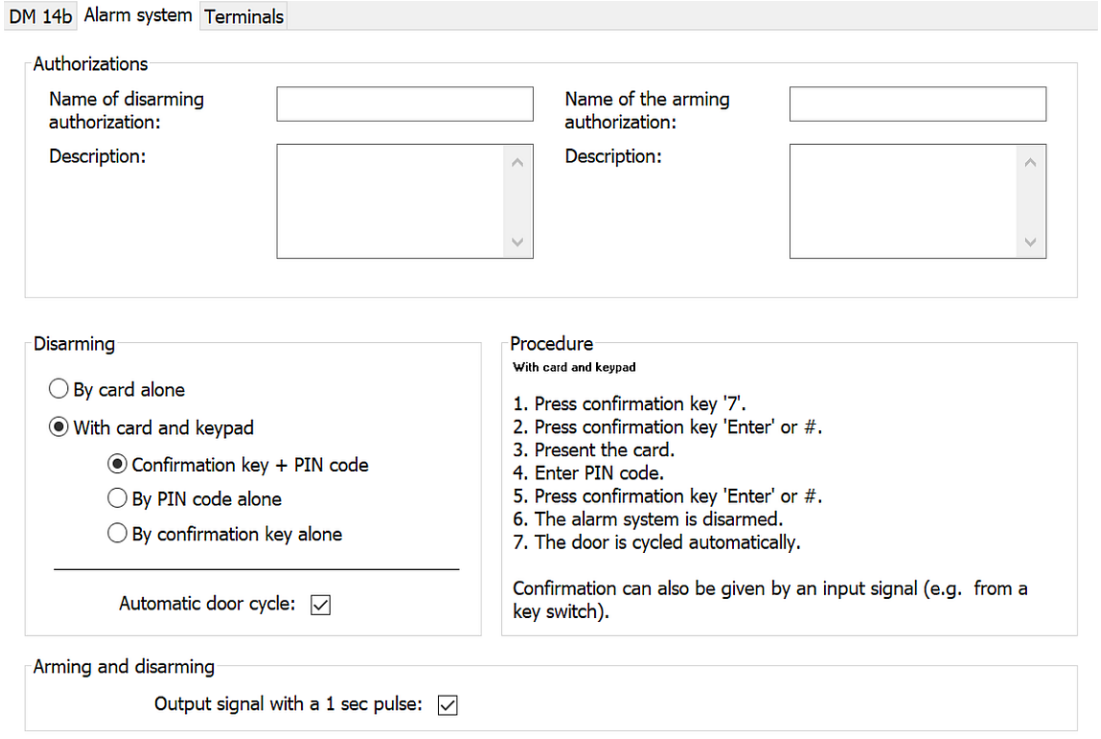


المعلمة	نوع القيمة	الوصف
الاسم	نص حر	اسم المدخل.
الوصف	نص حر، اختياري	وصف المدخل.
الموقع	قائمة المناطق المحددة، إذا تم استخدامها	منطقة الوصول حيث يقع المدخل.
الوجهة	قائمة المناطق المحددة، إذا تم استخدامها	منطقة الوصول التي يؤدي إليها المدخل.

المعلمة	نوع القيمة	الوصف
القسم	قائمة الأقسام المحددة، إذا تم استخدامها	القسم أو المستأجر ضمن نظام التحكم في الوصول الذي ينتمي إليه المدخل.
وقت انتظار قرار الوصول الخارجي	أعشار الثانية	في حال قمت بتوصيل نظام خارجي بالمحطات الطرفية لوحدة AMC، لاتخاذ القرارات بالنيابة عنه، تحدد هذه المعلمة عندئذٍ وقت انتظار استجابة من النظام الخارجي. ملاحظة: يتطلب قرار الوصول تنفيذ **جميع** الشروط المحددة في نظام التحكم في الوصول، على سبيل المثال، تخويلات الوصول، ونماذج الوقت والأقسام (في حال استخدامها). القيمة الافتراضية هي 0، أي، يتم تجاهل المعلمة.
منطقة التفعيل	قائمة الأحرف الكبيرة A...Z	حرف لاستخدامه لتجميع مداخل DM14 في مناطق التفعيل.

معلمات أنظمة الإنذار

على علامة التبويب الثانية **نظام الإنذار**، عيّن قيم المعلمات التالية. تحكم هذه المعلمات بيانات الاعتماد والإجراء الخاص بإلغاء تفعيل IDS، ويؤثر إلغاء التفعيل على جميع المداخل ضمن منطقة التفعيل نفسها، كما هو محدد على علامة التبويب الأولى.



المعلمة	نوع القيمة	الوصف
جزء التخويلات		

المعلمة	نوع القيمة	الوصف
اسم تخويل إلغاء التفعيل	نص حر	اسم يظهر في البروتوكولات والتقارير عندما يقوم حامل بطاقة بإلغاء تفعيل IDS في مدخله.
اسم تخويل التفعيل	نص حر	اسم يظهر في البروتوكولات والتقارير عندما يقوم حامل بطاقة بتفعيل IDS في مدخله.
الوصف (واحد لكل تخويل)	نص حر، اختياري	أوصاف تخويلات التفعيل
جزء إلغاء التفعيل		
بواسطة البطاقة فقط	زر تبادلي	حدد هذا الخيار للسماح بإلغاء تفعيل نطام IDS من خلال تقديم بطاقة للقارئ، من دون مصادقة إضافية.
بواسطة البطاقة ولوحة المفاتيح	زر تبادلي	حدد هذا الخيار للسماح بإلغاء تفعيل نطام IDS من خلال تقديم بطاقة للقارئ، ومنح مصادقة إضافية عبر لوحة مفاتيح القارئ. يتحدد إجراء المصادقة وإلغاء التفعيل الدقيق بواسطة المعلمات الفرعية التالية:
مفتاح التأكيد + رمز PIN	زر تبادلي	يتعين على حاملي البطاقات مصادقة أنفسهم باستخدام بطاقة ومفتاح تأكيد ورمز PIN.
بواسطة رمز PIN فقط	زر تبادلي	يتعين على حاملي البطاقات مصادقة أنفسهم باستخدام بطاقة ورمز PIN.
بواسط مفتاح التأكيد فقط	زر تبادلي	يتعين على حاملي البطاقات مصادقة أنفسهم باستخدام بطاقة ومفتاح تأكيد.
تدوير قفل الباب تلقائيًا	خانة اختيار	حدد خانة الاختيار هذه إذا أردت تدوير قفل الباب عند إلغاء التفعيل، للسماح لحامل البطاقة بإلغاء التفعيل والدخول في الوقت نفسه. **ملاحظة:** لن يتم تدوير القفل إلا إذا توفر لدى حامل البطاقة إذن الوصول إلى هذا الباب.
جزء الإجراء		
بحسب المعلمات التي تم تعيينها في جزء **بإلغاء التفعيل**، يعرض هذا الجزء الإجراء القياسي المتعلق بإلغاء تفعيل IDS. يمكنك نقل هذا الإجراء لحاملي البطاقات الذين سيستخدمون مداخل DM14 في منطقة التفعيل هذه.		
جزء التفعيل وإلغاء التفعيل		
إشارة المخرج مع نبض من ثانية واحدة	خانة اختيار	حدد هذا الخيار إذا كنت تستخدم لوحة كشف تسلل **Bosch B أو G-Series**. التأثير هو إرسال إشارة نبض واحدة لتبديل حالة منطقة التسلل في المدخل، بدلاً من تعيين الإشارة إلى ثابت 1 (تفعيل) أو 0 (إلغاء التفعيل).

المحطات الطرفية لوحدات التحكم في الأبواب

من أجل جعل التفعيل وإلغاء التفعيل ممكنًا مع مدخل DM14، يجب تعريف إشارات مداخل ومخارج IDS التي تريد استخدامها على المحطات الطرفية في وحدات التحكم في باب المدخل.

الخطوة مطلوبة مرة واحدة لكل وحدة تحكم لديها مداخل DM14. سترث جميع مداخل DM14 التالية التي تحددها على وحدة التحكم نفسها ولوحات التوسعة الخاصة بها إشارات من وحدة التحكم المشتركة.

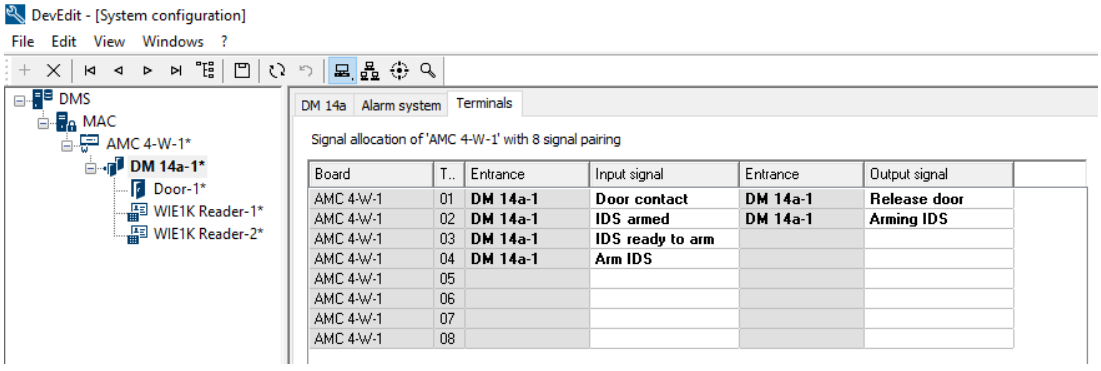
يقدم الجدول التالي وصفًا للإشارات الافتراضية.

الإشارة	داخل /خارج	الوصف
IDS مُفعّل	داخل	IDS مفعّل لمنطقة التسلل هذه.
IDS جاهز للتفعيل	داخل	لا توجد نقاط IDS في حالة خاطئة (مفتوحة أو غير جاهزة).
تفعيل IDS	داخل	طلب لتفعيل IDS.
زر "طلب الخروج" (REX)	داخل	
مستشعر المزلاج	داخل	يراقب مستشعر مزلاج الباب.
التلاعب	داخل	تم الكشف عن تلاعب.
إيقاف الإنذار من الفتح غير المصرح به	داخل	قم بإخماد التنبيه لعدد مكوّن من الثواني الإضافية إذا تم إعطاء إشارة REX بواسطة كاشف حركة. راجع ميزة تحويل REX لمزيد من التفاصيل.
تحرير الباب	خارج	قم بتدوير آلية الباب إلى غير مقفل، ثم إلى مقفل للسماح بالوصول.
تفعيل IDS	خارج	يمكنك تفعيل IDS أو إلغاء تفعيله، بحسب حالته الحالية (تبديل).
توصيل الكاميرا	خارج	قم بتنشيط كاميرا متصلة بالمدخل.
انقضى الحد الأقصى لوقت فتح الباب أو **تعرض أمان الباب للخطر**	خارج	تم تثبيت الباب في وضع الفتح، أو يشتبه النظام في حدوث خرق للأمن عند الباب.

إجراء لتعيين الإشارات إلى المحطات الطرفية

1. افتح علامة التبويب الثالثة، **المحطات الطرفية**.

– تظهر في جدول المحطات الطرفية لوحدة التحكم في باب هذا المدخل، بالإضافة إلى لوحات التوسيع الموجودة فيه.



2. حدد الخط المطابق للوحدة الطرفية التي تريد استخدامها لإشارة المدخل.
3. في الخلية المطابقة، في عمود **إشارة المدخل**، حدد الإشارة المحددة من القائمة المنسدلة. حتى الآن تظهر الإشارات غير المعينة في القائمة.
4. كرر الخطوات السابقة لإضافة أي إشارات مدخل أخرى تحتاجها لهذا المدخل.
5. كرر الإجراء كما تقتضي الحاجة لإضافة إشارات المخارج التي تحتاج إليها إلى عمود **إشارة المخرج**.

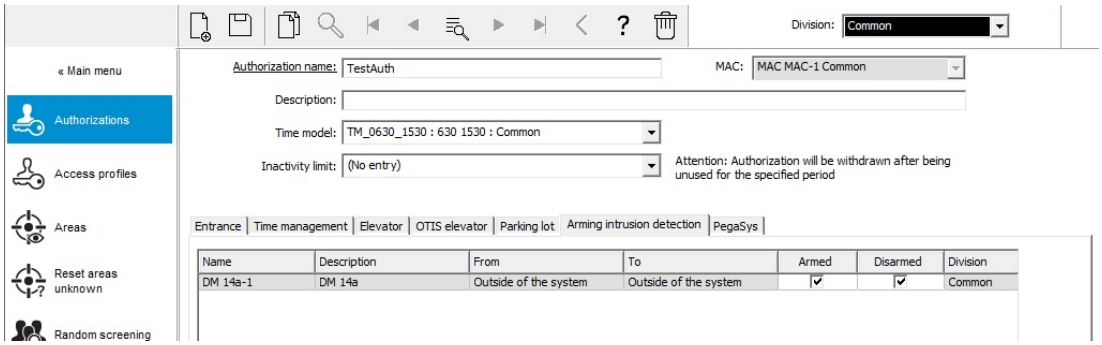
تعريف التخويلات لتفعيل وإلغاء تفعيل مداخل DM14

بعد إنشاء مدخل DM14 في محرر الجهاز، سيكون المدخل متاحًا لتضمينه في تخويلات الوصول.

1. في مدير مربع الحوار، انتقل إلى:

– القائمة الرئيسية > **بيانات النظام** > علامة تبويب **التخويلات** >: **تفعيل الكشف عن التسلل**

2. قم بتحميل تخويل وصول موجود إلى مربع الحوار أو انقر فوق (جديد) لإنشاء تخويل جديد.
3. حدد موقع مدخل DM14 في القائمة، وحدد خانة الاختيار **مفعّل** و/أو **غير مفعّل**.

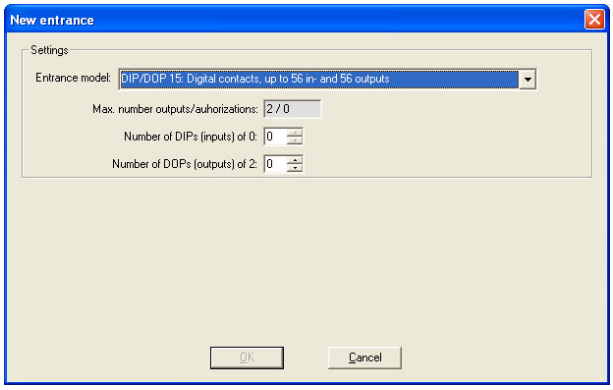


4. انقر فوق (حفظ) لحفظ تخويل الوصول مع الأذونات المحددة.
5. قم بتعيين تخويل الوصول هذا إلى حاملي البطاقات الذين سيقومون بتشغيل مداخل DM 14.

16.6.3 DIP وDOP في (DM15)

إنشاء نموذج المدخل 15:

يُقدم نموذج المدخل هذا إشارات مداخل ومخارج مستقلة.



في حال استخدام كافة واجهات القارئ، سيكون نموذج المدخل هذا فقط متوفرًا. يمكنك تحديد نموذج المدخل هذا عند توفر إشارتين على الأقل.

للتحكم بالمصاعد بأجهزة AMC (نموذج 07) أو بساحات الانتظار (نموذج 05c)، لا يمكن تعيين نموذج المدخل هذا.

نموذج المدخل 15

الإشارات الممكنة: يمكن الكتابة فوق هذه الأسماء الافتراضية.

إشارة المدخل	إشارة المخرج
DIP	DOP
DIP-1	DOP-1
...	...

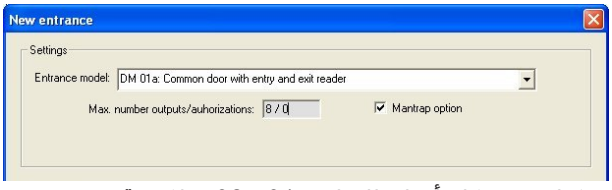
DIP-63	DOP-63

بشكل مخالف لنماذج الأبواب الأخرى، يقوم نموذج المدخل 15 بإدارة إدخالات وإخراجات وحدة التحكم التي ما زالت متوفرة، ويضعها كإدخالات عامة وإخراجات خالية من الفولتية تحت تصرف النظام بالكامل.
بشكل مغاير لملامسات المخارج لنماذج الأبواب الأخرى، يمكن استعراض تلك الخاصة بنموذج المدخل 15 كل على حدة في محرر الجهاز.

إعادة تثبيت DOP بعد إعادة التشغيل
تؤدي عملية إعادة تشغيل MAC أو AMC، عادةً إلى إعادة تعيين قيم الحالة في DOP الثانوي إلى القيم الافتراضية 0 (صفر).
للتأكد من قيام عملية إعادة التشغيل دومًا بإعادة تعيين DOP إلى آخر حالة تم تعيينها يدويًا إليه، حدد DOP في شجرة الأجهزة، وحدد خانة الاختيار **المحافظة على الحالة** في النافذة الرئيسية.

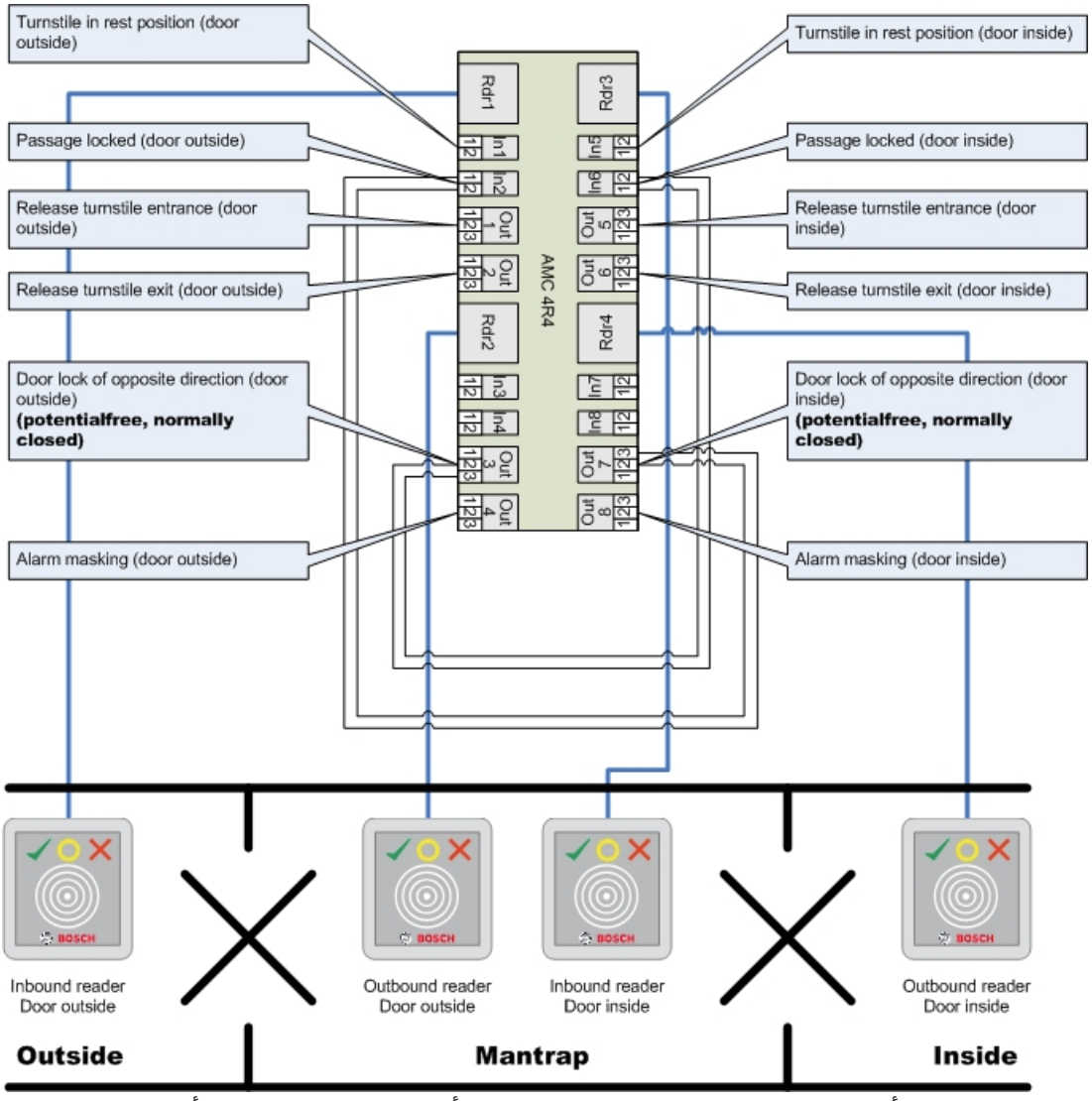
16.6.4 نماذج باب الشرَك

إنشاء الشرَك
يمكن استخدام نماذج المداخل 01 و03 "كشرَك" لمنح الوصول لحاملي البطاقات كل فرد على حدة.
استخدم خانة الاختيار **خيار الشرَك** لتوفير الإشارات الإضافية الضرورية.



يمكنك جمع كل أنواع النماذج 01 و03، ولكن قم بتعيين هذا الخيار على مدخلي الشرَك.
بالإضافة إلى تعيينات الإشارات العادية لنموذج الباب، يتطلب خيار الشرَك تعيينات الإشارات الإضافية الخاصة به.

مثال: شرَك على وحدة تحكم واحدة
تُعتبر الأبواب الدوارة الوسيلة الأكثر شيوعًا لمنح الوصول لحاملي البطاقات كل فرد على حدة. وقد استخدمنا في الأمثلة التالية نموذج الباب 3a (حاجز دوار مع قارئ دخول وقارئ خروج).
تكوين شرَك مع بابين دوارين (DM 03a):



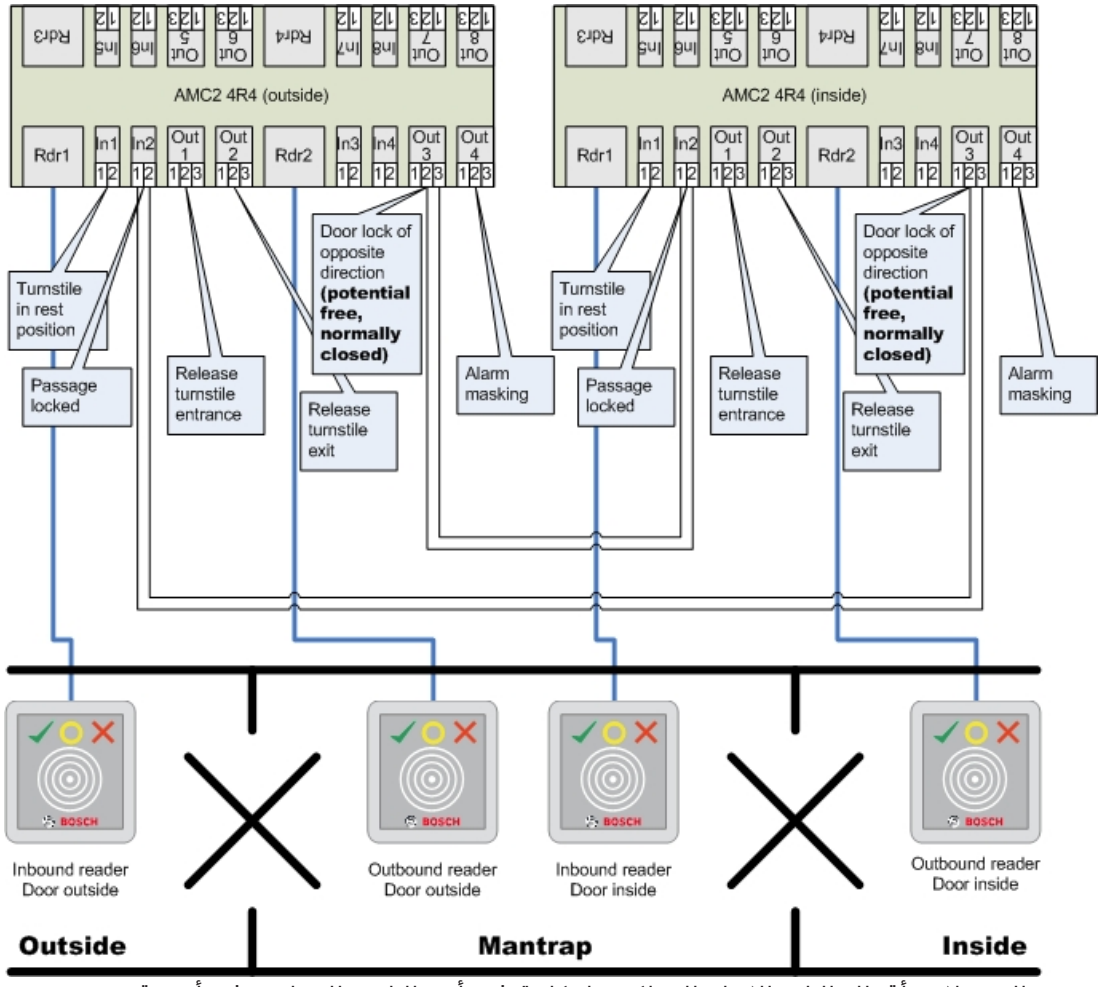
تضمن التوصيلات بأقفال الباب للاتجاه المعاكس إمكانية فتح أحد البابين الدوارين في أي وقت.

إشعار!

يجب تعيين إشارات المخارج (خارج) 3 و7 بحيث تكون خالية من الفولتية (الوضع الجاف)
الإشارة "قفل الباب في الاتجاه المعاكس" نشطة على 0. يجب استخدامها للمخارج 3 و7 (مغلق عادةً").

مثال: شرَك على جهازي تحكم

تكوين شرَك مع بابين دوارين (DM 03a) يتم توزيعهما عبر جهازي تحكم:



تضمن التوصيلات بأقفال الباب للاتجاه المعاكس إمكانية فتح أحد البابين الدوارين في أي وقت.

إشعار!
يجب تعيين إشارة المدخل (خارج) 3 بحيث تكون خالية من الفولتية (الوضع الجاف)
الإشارة "قفل الباب في الاتجاه المعاكس" نشطة على 0. يجب استخدامها للمخرج 3 (مغلق عادةً").

16.7 الأبواب

علامة التبويب: الباب

المعلمة	القيم المحتملة	الوصف
الاسم	رقمي، لغاية 16 حرفًا	يمكن استبدال القيمة الافتراضية المُنشأة باسم فريد، بشكل اختياري.
الوصف	رقمي، لغاية 255 حرفًا	
القسم	القسم الافتراضي هو "عام"	يُعتبر ملائمة فقط إذا كانت ميزة **الأقسام** مرخصة.
فقط لنموذجي الأبواب 01 و03 إذا تم تكوين شرَك		
خيار الشرَك	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	يوجد شرَك في المكان الذي يتم فيه استخدام نموذج الباب 01 أو 03 بواسطة بابين مدمجين. يمكنك تنشيط خيار الشرَك **للبابين** معًا. ستحتاج الأبواب أيضًا إلى تمديد أسلاك مادي خاص:

علامة التبويب: خيارات

المعلمة	القيم المحتملة	ملاحظات
إنشاء رسالة لمفتوح/مغلق	0 = خانة الاختيار غير محددة 1 = خانة الاختيار محددة	0 = لا يتم إنشاء أي رسالة عند فتح الباب (بزاوية من إطار الباب) أو عند إغلاقه (مغلق تمامًا داخل إطار الباب). 1 = يتم إنشاء الرسائل المقابلة في سجل الأحداث.
تعيين الباب إلى يدوي	0 = خانة الاختيار غير محددة 1 = خانة الاختيار محددة	0 = الباب في الوضع العادي (افتراضي)، وهو يخضع للتحكم في الوصول من قِبل النظام ككل 1 = الباب مستثنى من نظام التحكم في الوصول. الباب غير خاضع للمراقبة ولا ينشئ أي رسائل. يمكن فقط قفله أو إلغاء قفله يدويًا. وجميع المعلمات الأخرى لهذا الباب متوقفة عن التشغيل. يجب تعيين هذه المعلمة للباب والقارئ بشكل منفصل.
وضع الباب	0 = الباب في الوضع العادي 1 = الباب غير مقفل 2 = الباب غير مقفل بحسب نموذج الوقت 3 = الباب مفتوح بحسب نموذج الوقت بعد اجتيازه للمرة الأولى 5 = الباب محظور على المدى الطويل 6 = الباب محظور بحسب نموذج الوقت	0 = الوضع العادي (افتراضي) - سيتم إقفال الباب أو إلغاء قفله بحسب حقوق الوصول الممنوحة لبيانات الاعتماد. 1 = غير مقفل لفترة وقت طويلة - التحكم في الوصول معلّق خلال هذه الفترة. 2 = غير مقفل لفترة يحددها نموذج الوقت. التحكم في الوصول معلّق خلال هذه الفترة. 3 = مقفل طالما كان نموذج الوقت نشطًا حتى يحصل الشخص الأول على حق الوصول، ثم يكون مفتوحًا طالما كان نموذج الوقت نشطًا, 5 = محظور (مستبعد من نظام التحكم في الوصول) حتى يتم إلغاء الحظر يدويًا. 6 = محظور (مستبعد من نظام التحكم في الوصول) طالما كان نموذج الوقت نشطًا - الباب لا يخضع لأي مراقبة، ولا يمكن استخدام الباب عندما يكون نموذج الوقت نشطًا,
نموذج الوقت	أحد نماذج الوقت المتوفرة	نموذج الوقت لأوقات فتح الباب. إذا تم اختيار أوضاع الباب 2 و3 و4 و6 و7، سيكون مربع القائمة لنماذج الوقت متوفرًا. ويكون تحديد نموذج الوقت أمرًا مطلوبًا.
الحد الأقصى لمدة النبض حتى طرق الباب:	0 - 9999	الحد الأقصى لمدة إشارة الفتح. الوحدة 1/10 ثانية. القيم الافتراضية: 50 للأبواب، و10 للأبواب الدوارة (نموذج الباب 03)، و200 للحواجز (نماذج الأبواب 05c أو 09c).
الحد الأدنى لمدة النبض حتى طرق الباب:	0 - 9999	الحد الأدنى لمدة إشارة الفتح في 1/10 ثانية. الافتراضي: 10.
إبطال الإنذار المسبق	0 - 9999	إبطال الإنذار الإضافي **قبل** نبض طرق الباب. ($PARAMETER_WAITEMA)

		في حالات نادرة جدًا حيث قد يتفاعل الطرق على الباب بشكل أبطأ من إنذار الاقتحام، فمن الممكن إيقاف الإنذار مؤقتًا قبل إرسال إشارة الفتح إلى الباب. الوحدة: 1/10 ثانية. الافتراضي 0. عادةً ما تكون القيمة 20، أي ثانيتين، كافية حتى للأبواب البطيئة جدًا.
إبطال الإنذار اللاحق	0 - 9999	إبطال الإنذار الإضافي **بعد** نبض طرق الباب. (PARAMETER_OPENINRT$) بعد مرور النبض إلى طرق الباب (إشارة الفتح)، يمكن فتح الباب خلال هذا النطاق الزمني، دون إطلاق إنذار. الوحدة: 1/10 ثانية. الافتراضي: 0.
وضع طرق الباب	إدخال مربع القائمة	0 = يتم تعطيل زر طلب الخروج (REX) بعد وقت التنشيط 1 = يتم تعطيل زر طلب الخروج (REX) على الفور (= افتراضي)
مستشعر إطار الباب موجود	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	0 = ليس لدى الباب ملامس إطار 1 = لدى الباب ملامس إطار يعني الملامس المغلق عادةً أن الباب مغلق. (= افتراضي)
مستشعر المزلاج موجود	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	0 (افتراضي) = ليس لدى الباب مستشعر مزلاج 1 = لدى الباب مستشعر مزلاج تصدر رسالة عند غلق الباب بالمزلاج أو فتح المزلاج.
الوقت الممدد لفتح الباب (للأشخاص من ذوي الإعاقات)	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	0 = تحتوي إشارة الفتح على المدة القياسية، والتي يتم تعيينها على معلمة **الباب** "الحد أقصى لوقت تنشيط القفل"، أي مدة النبض حتى طرق الباب. 1 (افتراضي) = مدة إشارة الفتح مضروبة في العامل المعين إلى معلمة **MAC** "**عامل الوقت للأشخاص من ذوي الإعاقات**" (علامة التبويب: **إعدادات الوصول العمومي**). تضع القيمة 0 في معلمة MAC هذه أوقات فتح الباب الممتدة خارج العملية.

علامة التبويب: أمان الباب

المعلمة	القيم المحتملة	ملاحظات
إنشاء رسالة "فتح الباب بالقوة"	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	0 = لا رسالة تفيد بوجود اقتحام. يُعتبر هذا مفيدًا إذا كان من الممكن فتح الباب من الداخل بحرية تامة. 1 = (افتراضي) عند الفتح غير المصرح به، ستصدر رسالة، متبوعة برسالة أخرى عند غلق الباب.

إنشاء رسالة لـ "الباب مثبت في وضع الفتح" بعد:	0 - 9999	إذا ظل الباب مفتوحًا بعد هذه الفترة الزمنية، فسيتم إصدار رسالة للتحذير من أن الباب ظل مفتوحًا لفترة طويلة. الوحدة: 1/10 ثانية. الافتراضي: 300. 0 = عدم انقضاء الوقت المحدد، لا تصدر أي رسالة.
تمديد إخماد الإنذار لـ "فتح الباب بالقوة"	0 - 9999	مستخدم في ميزة "تحويل REX": الوحدة = 1/10 ثانية. الافتراضي = 0. بعد إشارة REX من كاشف الحركة، إذا أغلق الباب مرة أخرى خلال هذا النطاق الزمني، فسيتم استبدال الرسالة المعتادة `Unauthorized opening of door N` بالرسالة: `Door N opened (in alarm suppression mode)` حيث N هو رقم الباب.
إنشاء إنذار محلي لـ "فتح الباب بالقوة"	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	المتطلب السابق: يتم تحديد خانة الاختيار **إنشاء رسالة لـ "فتح الباب بالقوة"** في مربع الحوار هذا (انظر أعلاه). 0 = (افتراضي) أجهزة القراءة المتصلة بهذا الباب لا تصدر إنذارًا محليًا. 1 = تطلق أجهزة القراء المتصلة بهذا الباب إنذارًا محليًا إذا تم فتح الباب بالقوة.
إنشاء إنذار محلي لـ "الباب مثبت في وضع الفتح" بعد:	0 - 9999	إذا ظل الباب مفتوحًا بعد هذه الفترة الزمنية ، فإن أجهزة القراءة المتصلة بهذا الباب تطلق إنذارًا محليًا. الوحدة: 1/10 ثانية. 0 = (افتراضي) لا يوجد إنذار محلي.

16.7.1 تحويل REX

المقدمة

عند المداخل التي لا يوجد فيها خطر أمني في فتح الباب يدويًا من الداخل، غالبًا ما يحل كاشف الحركة محل زر REX لفتح الباب. بالنسبة لهذا السيناريو الشائع، فإن ACS يوفر وسيلة بسيطة لإطالة مدة إشارة REX من كاشف الحركة، بينما في نفس الوقت يحول (يعلّق) إنذار `Door forced open` .
تُعرف هذه الميزة باسم "تحويلة REX".
عندما تكون الميزة قيد التشغيل، سيُنشئ حاملو البطاقات الذين يغادرون من خلال الباب خلال مدة التحويل حدث الوصول `Door N opened (in alarm suppression mode)` بدلاً من الحدث `Unauthorized opening of door N`.

إشعار!

تحويل REX مع أنظمة كشف الاقتحام المفعّلة
تعمل ميزة تحويل REX على تعليق التنبيهات للمدة المحددة في المعلمة:
محرر الجهاز > ... > **الباب** > علامة التبويب: **أمان الباب** > **تمديد إخماد الإنذار لـ "فتح الباب بالقوة"**
بغض النظر عما إذا كان هذا الباب مفعّلاً حاليًا كجزء من نظام إنذار ضد السرقة.

الشروط الأساسية

- الأبواب المكوّنة من الأنواع التالية: 01a, 01b, 01c, 03a, 03b, 03c, 10a, 10b, 10e, 14a, 14b
- الباب المادي مزود بكاشف للحركة، بدلاً من زر REX، لفتح الباب. قم بتعيين مدة الإشارة من كاشف الحركة إلى ثانية واحدة على الأقل.

مسار مربع الحوار

- **القائمة الرئيسية >التكوين > بيانات الجهاز**
- **مستعرض تكوين BIS > الاتصالات > بيانات الجهاز**

الإجراء

1. في محرر الجهاز، انتقل إلى المدخل المطلوب (عقدة فرعية مباشرة لوحدة تحكم الباب).
2. في علامة التبويب **المحطات الطرفية** للمدخل، قم بإنشاء إشارة إدخال جديدة من النوع:
   `Suppress alarm from unauthorized opening`
3. انقر فوق (حفظ) لحفظ التغييرات.
4. حدد الباب الذي يقع داخل المدخل المطلوب
5. في علامة التبويب **أمان الباب** للباب، قم بتعيين قيمة للمعلمة **تمديد إخماد الإنذار لـ "فتح الباب بالقوة"**
   - القيمة بعُشر من الثانية.
   - القيمة الافتراضية هي 0. وهذا يعني أنه لا يوجد بشكل افتراضي تمديد لإخماد الإنذار بعد أن يغادر حامل البطاقة المنطقة الحساسة من كاشف الحركة.
6. انقر فوق (حفظ) لحفظ التغييرات.

16.7.2 تكوين الأبواب لإصدار الإنذارات المحلية

المقدمة

بالنسبة لحالات الباب التالية، يوفر نظام ACS وسيلة لإصدار الإنذارات في جميع أجهزة القراءة المتصلة بالباب.

الحالة	الاستجابة للإنذارات المحلية
فتح الباب بالقوة	يصدر صوت التنبيه لمدة 17 ثانية أو حتى يغلق الباب.
الباب مثبت في وضع الفتح	يصدر التنبيه حتى يغلق الباب.

الشروط الأساسية

- تستخدم أجهزة القراءة بروتوكول OSDP أو Wiegand
- توجد أجهزة إصدار الإنذار في أجهزة القراءة ومتصلة كهربائيًا بوحدة التحكم في الباب.
- إصدار البرامج الثابتة لـ AMC 02.38 أو أحدث.

أنواع أجهزة القراءة التالية **ليست** مدعومة:

- أجهزة قراءة IDEMIA
- أجهزة قراءة Suprema مع بروتوكول Wiegand
- أجهزة قراءة LBUS
- أجهزة قراءة BG900

مسار مربع الحوار

- **القائمة الرئيسية >التكوين > بيانات الجهاز**
- **مستعرض تكوين BIS > الاتصالات > بيانات الجهاز**

إجراء فتح الباب بالقوة

1. في شجرة الأجهزة، حدد الباب الذي ترغب في تكوينه.
2. في علامة التبويب **أمان الباب** للباب، حدد خانة الاختيار **إنشاء رسالة لـ "فتح الباب بالقوة"**

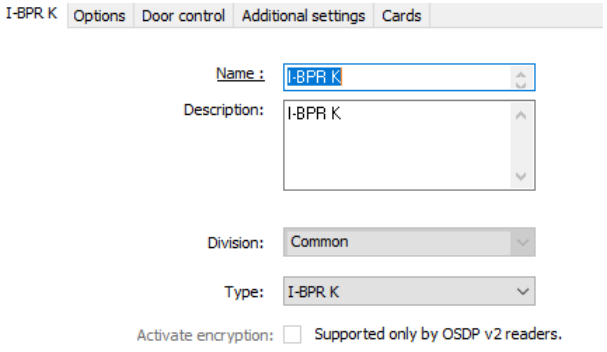
3. حدد خانة الاختيار **إنشاء إنذار محلي لـ "فتح الباب بالقوة"**
. القيمة الافتراضية هي 0 (خانة الاختيار غير محددة). هذا يعني أنه لا يتم صدار أي إنذار محلي بشكل افتراضي.
4. انقر فوق (حفظ) لحفظ التغييرات.

إجراء الباب مثبت في وضع الفتح

1. في شجرة الأجهزة، حدد الباب الذي ترغب في تكوينه.
2. في علامة التبويب **أمان الباب** للباب، قم بتعيين قيمة غير صفرية لـ **إنشاء إنذار محلي لـ "الباب مثبت في وضع الفتح" بعد:**
   - القيمة بعُشر من الثانية.
   - القيمة الافتراضية هي 0. هذا يعني أنه لا يتم صدار أي إنذار محلي بشكل افتراضي.
3. انقر فوق (حفظ) لحفظ التغييرات.

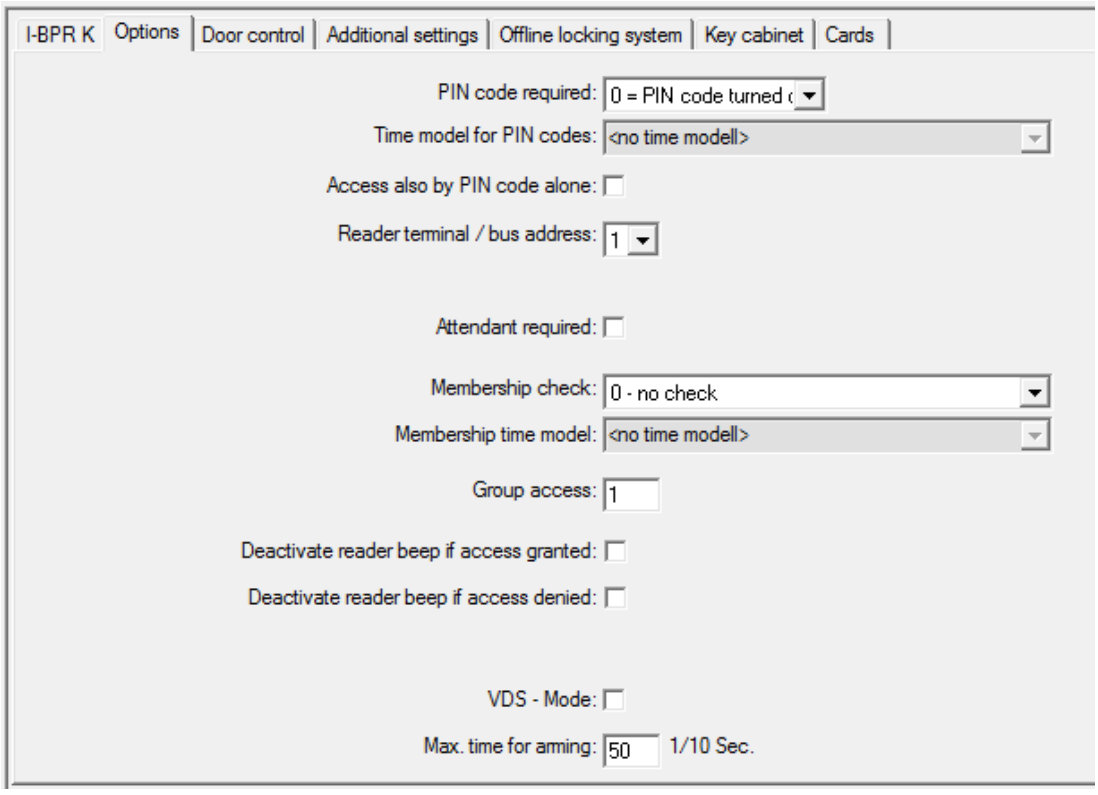
16.8 أجهزة القراءة

تكوين قارئ: المعلمات العامة



المعلمة	القيم المحتملة	الوصف
اسم القارئ	أبجدي رقمي، مقيد بعدد من الأحرف من حرف إلى 16 حرفًا.	يمكن استبدال القيمة الافتراضية باسم فريد.
وصف القارئ	أبجدي رقمي، من 0 إلى 255 حرفًا	وصف باستخدام نص حر.
القسم	القسم الافتراضي "عام".	يُعتبر ملائمًا فقط إذا كانت "الأقسام" مرخصة وقيد الاستخدام.
النوع	أبجدي رقمي، مقيد بعدد من الأحرف من حرف إلى 16 حرفًا.	نوع القارئ أو مجموعة أجهزة القراءة

تكوين قارئ: الخيارات



المعلمة	القيم المحتملة	الوصف
رمز PIN مطلوب	0 = رمز PIN متوقف عن التشغيل - لا حاجة إلى أي إدخال (افتراضي) 1 = رمز PIN قيد التشغيل - الإدخال ضروري دائمًا 2 = يخضع رمز PIN لنموذج الوقت - الإدخال ضروري فقط إذا كان خارج نموذج الوقت	يتم تمكين هذا الحقل فقط إذا تضمن القارئ جهاز إدخال. لاحظ أن عمليات فحص البطاقة لها الأسبقية على صحة رمز PIN، على سبيل المثال التخويلات وتسلسل الوصول (إذا تم تمكينه).
نموذج الوقت لرموز PIN	أحد نماذج الوقت المتوفرة	يعتبر اختيار نموذج الوقت هنا إلزاميًا إذا تم تعيين المعلمة **رمز PIN مطلوب** إلى 2.
الوصول أيضًا بواسطة رمز PIN فقط	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	تحدد هذه المعلمة إن كان هذا القارئ يسمح أيضًا بالوصول استنادًا إلى رمز PIN فقط، أي من دون بطاقة، إذا تم تكوين نظام التحكم في الوصول بهذه الطريقة. راجع
محطة طرفية للقارئ / عنوان الناقل	1 - 4	بالنسبة إلى AMC 4W: الترقيم وفقًا لواجهات Wiegand. بالنسبة إلى AMC 4R4: الترقيم يُشبه عنوان العبور للقارئ.

يلزم وجود ملاحظ	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	0 = لا يحتاج الزائر إلى ملاحظ (افتراضي) 1 = يجب على الملاحظ أيضًا استخدام القارئ
تحقق من العضوية	إدخال مربع القائمة	يُستخدم التحقق من العضوية عادةً في المراحل المبكرة قبل أن يبدأ نظام التحكم في الوصول العمل. هنا يُمنح حق الوصول استنادًا إلى بطاقة هوية الشركة العام لبيانات الاعتماد بدلاً من بطاقة هويتها الشخصية الفريدة الفريد. **مهم** يعمل التحقق من العضوية مع بيانات الاعتمادية المادية فقط حيث يتم تعريف تعريفات البطاقة بشكل مسبق في النظام (خلفية رمادية)، **وليس** مع التعريفات المخصصة أو بيانات الاعتماد البيومترية. **0 - بدون تحقق** التحقق من العضوية متوقف عن التشغيل، ولكن يتم فحص البطاقة للحصول على التخويلات بالشكل المعتاد (افتراضي) **1 - فحص** يجري فحص البطاقة للتأكد من معرّف الشركة فقط، أي من عضوية النظام. **2 - بحسب نموذج الوقت** يجري فحص البطاقة للتأكد من معرّف الشركة (العضوية)، ولكن فقط خلال الفترة المعرّفة في نموذج وقت العضوية.
نموذج وقت العضوية	أحد نماذج الوقت المتوفرة	نموذج الوقت يمكّن/يعطّل التحقق من العضوية. يعتبر تحديد نموذج الوقت إلزاميًا للخيار 2 **تحقق من العضوية**.
وصول المجموعة	1 - 10	**بالنسبة إلى أجهزة القراءة المزوّدة بلوحة مفاتيح:** الحد الأدنى للبطاقات الصالحة التي يجب تقديمها لقارئ البطاقات قبل فتح الباب. تتكوّن المجموعة من عدد من البطاقات يتجاوز هذا العدد؛ وفي هذه الحالة يُستخدم المفتاح ENTER/# للإشارة إلى أن المجموعة كاملة. ونتيجة لذلك، يُفتح الباب. **بالنسبة إلى أجهزة القراءة غير المزوّدة بلوحة مفاتيح:** العدد الدقيق للبطاقات الصالحة التي يجب تقديمها لقارئ البطاقات قبل فتح الباب. القيمة الافتراضية هي 1.
إلغاء تنشيط تنبيه القارئ إذا تم منح حق الوصول	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	في الوضع المنشّط (1) يبقى القارئ صامتًا إذا تم منح حق الوصول لمستخدم مخوّل.

إلغاء تنشيط تنبيه القارئ إذا لم يتم منح حق الوصول	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	في الوضع المنشّط (1) يبقى القارئ صامتًا عند رفض حق وصول مستخدم غير مخوّل.
 تتوقف وظيفة "إلغاء تنشيط تنبيه القارئ" على البرنامج الثابت للقارئ المعني. فقد لا يدعم البرنامج الثابت في بعض أجهزة القراءة هذه الوظائف.		
وضع VDS	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	في الوضع المنشّط (1) سيكون إرسال الإشارات من أحد أجهزة القراءة متوقفًا عن التشغيل.
أقصى وقت للتفعيل	1 - 100 [1/ثانية]	الحد الأقصى لوقت صدور رد فعل من لوحة كشف التسلل للإشارة إلى اكتمال التفعيل.

الشبكة وأوضاع التشغيل

تظهر علامة التبويب هذه فقط لأجهزة القراءة البيومترية المتصلة بشبكة.

تعتبر **القوالب** بمثابة أنماط مخزنة. وبإمكانها أن تكون بيانات بطاقات أو بيانات بيومترية.

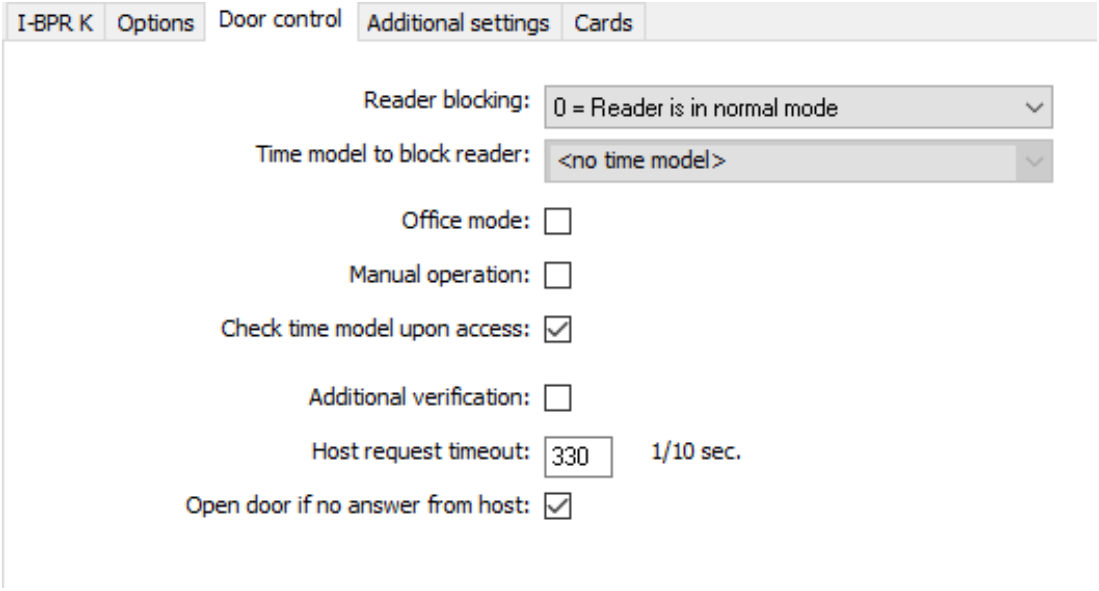
يمكن تخزين القوالب على الأجهزة فوق القارئ في شجرة الأجهزة، وعلى القارئ بحد ذاته. ويتم تحديث البيانات الموجودة على القارئ بشكل دوري بواسطة الأجهزة الموجودة فوقه.

يمكن تكوين القارئ بحيث يستخدم قوالبه الخاصة عند اتخاذ قرارات تتعلق بالوصول، أو فقط لاستخدام القوالب من الأجهزة فوقه.

المعلمة	**الوصف**
عنوان IP:	عنوان IP لهذا القارئ المتصل بشبكة
المنفذ:	المنفذ الافتراضي هو 51211
القوالب على الخادم	
بطاقة فقط	يقرأ القارئ بيانات البطاقة فقط. ويصادق عليها في مقابل البيانات من النظام ككل.
البطاقة وبصمة الإصبع	يقرأ القارئ بيانات البطاقة وبيانات بصمة الإصبع. ويصادق عليها في مقابل البيانات من النظام ككل.
القوالب على الجهاز	
التحقق المعتمد على الشخص	يسمح القارئ لإعدادات حامل البطاقة الفردي بتحديد **وضع التعريف** الذي يستخدمه. تقدم بيانات الموظفين الخيارات التالية: – بصمة الإصبع فقط – بطاقة فقط – البطاقة وبصمة الإصبع سيتم وصف هذه الخيارات لاحقًا في هذا الجدول.
بصمة الإصبع فقط	يقرأ القارئ بيانات بصمة الإصبع فقط. ويصادق عليها في مقابل بياناته المخزنة.

المعلمة	الوصف
بطاقة فقط	يقرأ القارئ بيانات البطاقة فقط. ويصادق عليها في مقابل بياناته المخزنة.
البطاقة وبصمة الإصبع	يقرأ القارئ بيانات البطاقة وبيانات بصمة الإصبع. ويصادق عليها في مقابل بياناته المخزنة.
البطاقة أو بصمة الإصبع	يقرأ القارئ بيانات البطاقة أو بيانات بصمة الإصبع، وهذا يتوقف على البيانات التي يقدمها حامل البطاقة أولاً. ويصادق عليها في مقابل بياناته المخزنة.

تكوين قارئ: مراقبة الباب

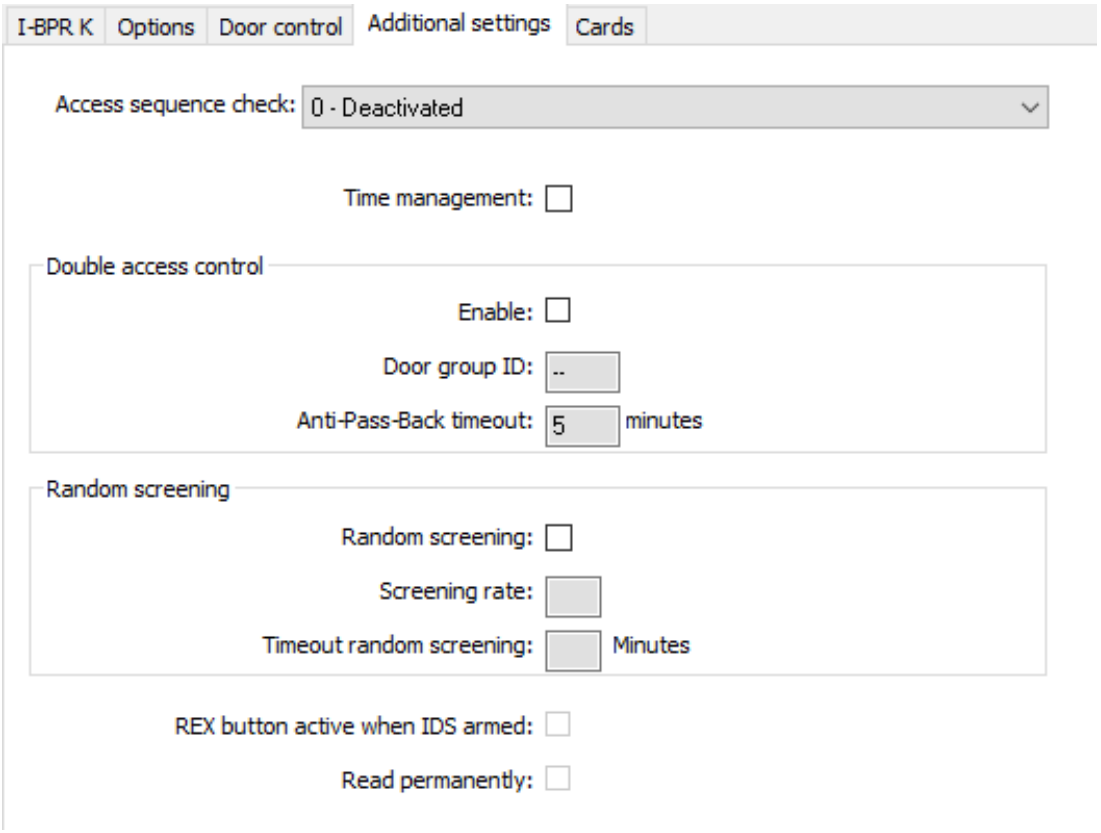


المعلمة	القيم المحتملة	ملاحظات
حظر القارئ	إدخال مربع القائمة	0 = القارئ في الوضع العادي - لا يوجد أي حظر (= افتراضي) 1 = القارئ محظور بشكل دائم - حظر دائم 2 = القارئ محظور بحسب نموذج الوقت - يتم تعيين الحظر وفقًا لنموذج الوقت باستخدام نموذج الوقت لحظر القارئ
نموذج الوقت لحظر القارئ	أحد نماذج الوقت المعرّفة في النظام.	حظر القارئ وفقًا لنموذج الوقت المحدد.
وضع المكتب	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	يسمح لهذا القارئ بتعيين مدخل إلى وضع المكتب. يجب أن يحتوي القارئ على لوحة مفاتيح. عند تنشيط هذه المعلمة، يقوم حامل البطاقة المصرح له بشكل مناسب بتبديل وضع المكتب وإيقاف تشغيله بالضغط على المفتاح 3 قبل تقديم بطاقته. راجع تخويل الأشخاص تعيين وضع المكتب, الصفحة *191*
التشغيل اليدوي	0 = ملغى تنشيطه (خانة الاختيار غير محددة)	0 = القارئ في الوضع العادي (= افتراضي)

	1 = منشّط (خانة الاختيار محددة)	1 = تمت إزالة القارئ بشكل فعلي من نظام التحكم في الوصول، وهو "معطّل". لا يتم استلام أي أوامر. وجميع المعلمات الأخرى لهذا القارئ متوقفة عن التشغيل. يجب تعيين المعلمة للباب والقارئ بشكل منفصل.
التحقق من نموذج الوقت بعد الوصول	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	0 = لن يتم فحص نماذج الوقت. لا توجد أي قيود زمنية تتعلق بالوصول. 1 = في حال وجود نموذج وقت معيّن لحامل البطاقة، إما مباشرةً أو كتخويل مكان زمني، سيتم فحص نموذج الوقت. (= افتراضي)
تحقق إضافي	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	0 = التحقق من المضيف غير مطلوب 1 = التحقق من المضيف مطلوب (افتراضي) (**مهم**: يجب تنشيط هذا الخيار لإجراء تحقق إضافي من الفيديو بواسطة مشغّل نظام Bosch BVMS أو نظام التحكم في الوصول من Bosch).
مهلة طلب المضيف	0 = ملغى تنشيطه	0 = يعمل AMC من دون التحقق من المضيف (لا يعمل مع تغيير المنطقة أو تعداد الأشخاص). يكون عنصر التحكم هذا نشطًا إذا تم إلغاء تنشيط التحقق من المضيف (0) وتم تنشيط فتح الباب في حال عدم تلقي رد من المضيف (1) القيم هي 1 إلى 9999 × 1/10 من الثانية. (الخيار الافتراضي = 330 =33 ثانية). يطلب القارئ الحصول على تأكيد من نظام التحكم في الوصول. إذا لم يتم الحصول على التأكيد خلال فترة الوقت المحددة، فسيقوم نظام AMC بالتحقق من المعلمة **فتح الباب في حالة عدم تلقي إجابة من المضيف** ويمنح حق الوصول أو يرفضه وفقًا لذلك.
فتح الباب في حالة عدم تلقي إجابة من المضيف	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (افتراضي) (خانة الاختيار محددة)	يكون عنصر التحكم هذا نشطًا، إذا تم تعيين المعلمة **التحقق من المضيف**. 0 = لا يفتح الباب إذا لم يقدم النظام المضيف التأكيد المطلوب قبل انقضاء المهلة. 1 (افتراضي) = يفتح الباب بعد انقضاء المهلة إذا لم يقدم النظام المضيف التأكيد المطلوب قبل انقضاء المهلة.
التحقق من أرصدة مناطق صف السيارات	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	في الوضع المنشّط (1) يتم التحقق من أرصدة تذاكر صف السيارات.
التحقق من حالات تجاوز مدة صف السيارات	0 = ملغى تنشيطه (خانة الاختيار غير محددة)	في الوضع المنشّط (1) يتم التحقق مما إذا كانت مدة صف السيارات طويلة جدًا.

	1 = منشّط (خانة الاختيار محددة)	

تكوين قارئ: إعدادات إضافية

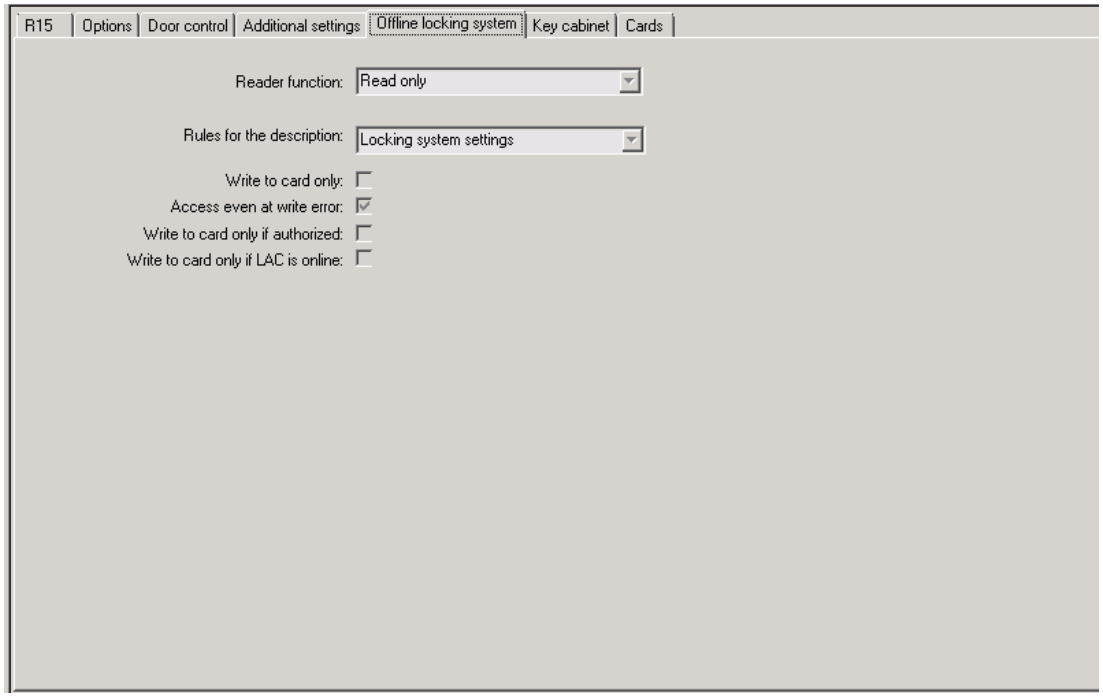


المعلمة	القيم المحتملة	ملاحظات
فحص تسلسل الوصول	0 - ملغى تنشيطه 1 - منشّط؛ إلغاء التنشيط عند حدوث خلل وظيفي في LAC 2 - منشّط؛ تركه نشطًا عند حدوث خلل وظيفي في LAC 3 - منشّط؛ استخدام فحص دقيق لتسلسل الوصول حتى عند حدوث خلل وظيفي في LAC (ملاحظة: تحديث معلومات الشخص يدويًا)	0 = لا يشارك الشخص في فحص تسلسل الوصول (= افتراضي) بإمكان فحص منشّط لتسلسل الوصول أن يتعامل مع الأشخاص الذين تم تعيينهم كأشخاص "غير معروفين" بالطرق التالية: 1 = ستتعطل القراءة الأولى للبطاقة من دون فحص الموقع. يجب أن تكون جميع وحدات التحكم متصلة بالإنترنت. 2 = ستتعطل القراءة الأولى للبطاقة من دون فحص الموقع. 3 = سيتعطل فحص الموقع لكل عمليات قراءة البطاقة أثناء حدوث الخلل الوظيفي في LAC.
يوجد أمر MAC لتنشيط أو إلغاء تنشيط جميع عمليات فحص تسلس الوصول بشكل عام.		

لإلغاء تنشيط فحص تسلسل الوصول لفترة زمنية، يتم إعطاء قيمة بالدقائق مع حد أقصى من 2880 (= 48 ساعة). يؤدي تعيين القيمة إلى "0" إلى إلغاء تنشيط فحص تسلسل الوصول بشكل كامل. **ملاحظة:** بإمكان هذا الأمر تعديل فحص تسلسل الوصول فقط بالنسبة إلى أجهزة القراءة التي تم فيها تعيين المعلمة **تمكين تسلسل الوصول**. وهو لا يقوم بتنشيط/إلغاء تنشيط فحص تسلسل الوصول لجميع أجهزة القراءة.		
إدارة الوقت	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	عند تحديد هذا الخيار، يقوم نظام التحكم في الوصول بجمع بيانات لإدارة الوقت والحضور.
تحكم مزدوج في الوصول (التحكم في منع العودة)		
تمكين	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	0 = من دون تحكم مزدوج في الوصول (= افتراضي) 1 = مع تحكم مزدوج في الوصول في غضون الفترة الزمنية المحددة بواسطة معلمة **المدة**، لا يمكن استخدام هذا القارئ وأجهزة القراءة الأخرى في المجموعة مع البطاقة نفسها. إذا تم تنشيط هذه المعلمة، فيجب استخدام معرّف مجموعة الأبواب، حتى في حال استخدام قارئ واحد فقط.
معرّف مجموعة الأبواب	الأحرف A - Z و a - z و"-" حرفان	يمكن تجميع أجهزة القراءة باستخدام معرّف مجموعة أبواب. سيؤدي تقديم بطاقة عند أحد أجهزة القراءة إلى حظر جميع الحجوزات التالية عند جميع أجهزة القراءة في مجموعة الأبواب (افتراضي = **--**) حتى انقضاء المهلة.
انقضاء مهلة منع العودة	1 - 120	يمكن استخدام القارئ مع البطاقة نفسها بعد انقضاء هذه الفترة الزمنية. وفور استخدام البطاقة عند قارئ من خارج المجموعة، يتم رفع الحظر على الفور. القيم هي الدقائق - افتراضي = 5.
الفحص العشوائي	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	0 = بدون فحص عشوائي 1 = لن يُسمح للفحص العشوائي وفقًا للعامل بالدخول حتى إلغاء الحظر بواسطة مربع الحوار **حظر**.
معدل الفحص	1 - 100	النسبة المئوية للفحص العشوائي في عملية فحص مطولة. يتوفر الخيار فقط في حال تم تنشيط الفحص العشوائي.
مهلة الفحص العشوائي	1 - 120	ضمن الوقت المحدد الذي يخضع فيه المستخدم للفحص العشوائي. القيم هي الدقائق - افتراضي = 5.

زر طلب الخروج (REX) نشط عندما يكون IDS مفعّلاً	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	بالنسبة إلى **DM10** و**DM14** فقط: يتم تعطيل أزرار طلب الخروج (REX) بشكل افتراضي عندما يكون IDS مفعّلاً. سيؤدي ذلك إلى جعل الخروج من المنطقة المراقبة غير ممكن. تقوم معلمة القارئ الجديدة هذه بتمكين زر طلب الخروج (REX) حتى عندما يكون IDS مفعّلاً.
القراءة بشكل دائم	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	يقرأ القارئ بشكل دائم إذا كان يتضمن البرنامج الثابت الخاص بالشركة المصنعة.

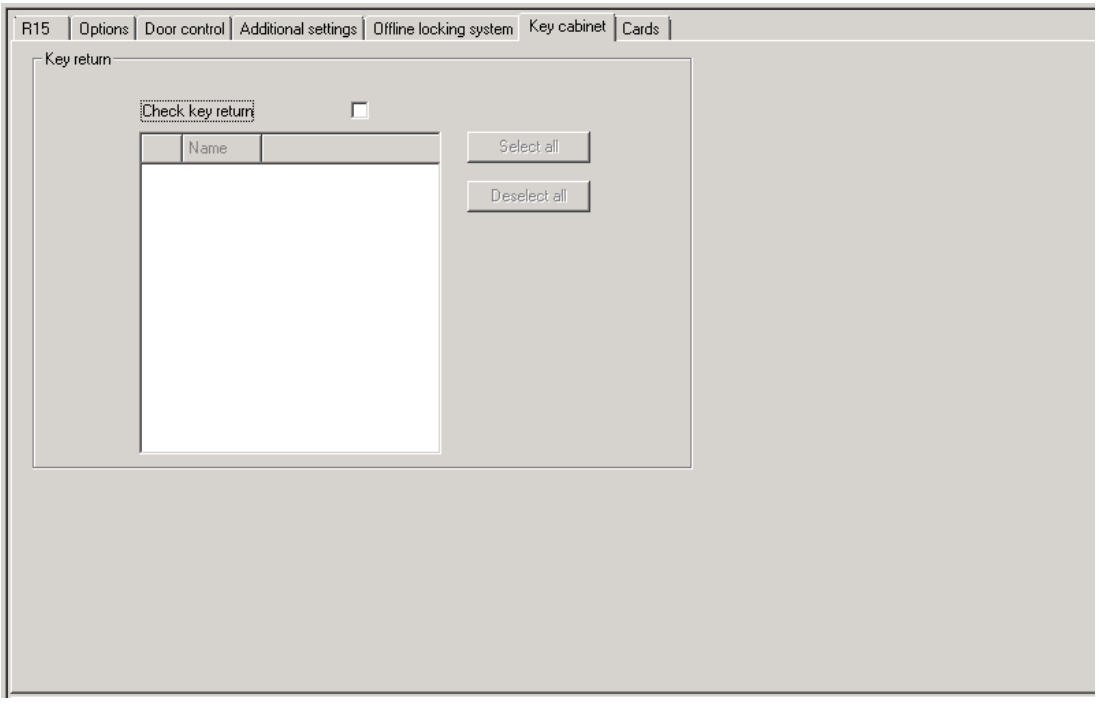
تكوين قارئ: نظام القفل غير المتصل



المعلمة	القيم المحتملة	ملاحظات
وظيفة القارئ		يجب تحديد هذا المربع في حال استخدام قارئ بطاقات آلي
قواعد للوصف		"السحب" يعني جعل البطاقة غير صالحة.
كتابة إلى البطاقة فقط	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	

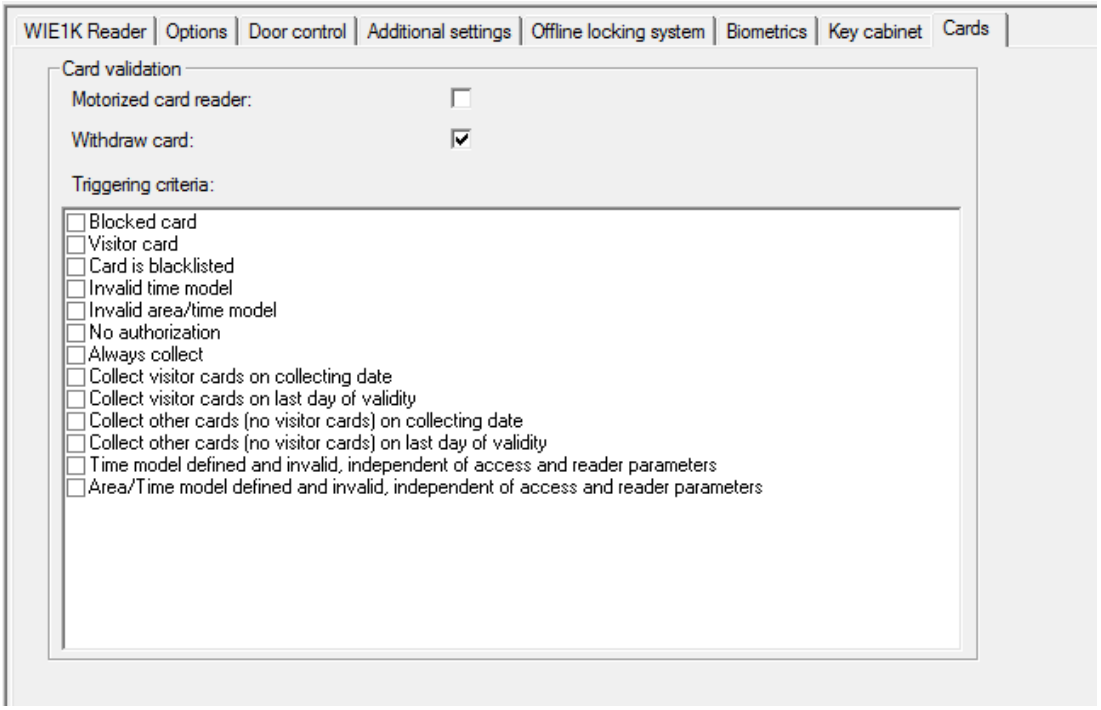
الوصول حتى مع وجود خطأ في الكتابة	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	
الكتابة إلى البطاقة فقط في حالة التخويل بذلك	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	
الكتابة إلى البطاقة فقط إذا كان LAC متصلاً	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	

تكوين قارئ: خزانة المفاتيح



المعلمة	القيم المحتملة	ملاحظات
التحقق من إعادة المفتاح	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	إرشاد نظام التحكم في الوصول للتأكد من إعادة المفتاح إلى خزانة مفاتيح Kemas قبل السماح لحامل المفتاح بمغادرة المقر.

تكوين قارئ: البطاقات



المعلمة	القيم المحتملة	ملاحظات
قارئ بطاقات آلي	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	حدد هذا الخيار عند استخدام قارئ بطاقات آلي.
سحب البطاقة	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	عند استخدام قارئ بطاقات آلي، يعني السحب احتجاز البطاقة فعليًا. عند استخدام أجهزة قراءة أخرى، يعني السحب أن النظام يجعل البطاقة غير صالحة.
معايير التشغيل	0 = ملغى تنشيطه (خانة الاختيار غير محددة) 1 = منشّط (خانة الاختيار محددة)	حدد من هذه القائمة أي معايير يمكن أن تسبب الإجراء **سحب البطاقة**.

إشعار!
يمكن استخدام أجهزة قراءة البطاقات الآلية مع أجهزة قراءة IBPR.

راجع
- تخويل الأشخاص تعيين وضع المكتب, الصفحة *191*

16.8.1 تكوين الفحص العشوائي

يُعتبر الفحص العشوائي طريقة عامة لتحسين أمان المواقع عن طريق اختيار الموظفين بشكل عشوائي في الفحوصات الأمنية الإضافية.

الشروط الأساسية:
- يجب أن يكون المدخل من النوع الذي يشتمل على شرَك أو باب دوّار لمنع قيام شخص "بتتبع شخص آخر بدنوّ خطر" بدون تقديم هويته الخاصة.
- لا بد من وجود قارئ بطاقات لأحد اتجاهات المرور على الأقل.
- يجب تكوين أجهزة القراءة من أجل التحكم العادي في الوصول.
- يمكن تكوين أداة الاختيار العشوائي بصورة مستقلة لكل قارئ.
- يجب أن تكون هناك محطة عمل في محيط المنطقة الأقرب من أجل تحرير أي عمليات حظر قام بها النظام.

الإجراء
1. حدد موقع القارئ المطلوب في محرر الجهاز DevEdit.
2. على علامة التبويب **الإعدادات**، حدد خانة الاختيار **فحص عشوائي**.
3. في مربع **النسبة المئوية للفحص**، أدخل النسبة المئوية للأشخاص الذين سيخضعون للفحص.
4. احفظ إعداداتك.

16.9 الوصول بواسطة رمز PIN فقط

الخلفية

يمكن تكوين أجهزة القراءة المزوّدة بلوحة المفاتيح للسماح بالوصول بواسطة رمز PIN وحده.
عند تكوين أجهزة القراءة، بإمكان مُشغّل التحكم في الصول تعيين رموز PIN فردية لموظفين معينين. ويتلقى هؤلاء الموظفون بالفعل "بطاقة افتراضية" تحتوي فقط على رمز PIN. يسمى هذا رمز PIN للتعريف. وفي المقابل، فإن رمز PIN للتحقق هو رمز PIN يُستخدم مع بطاقة لتشديد الإجراءات الأمنية.

بإمكان المشغّل إدخال رموز PIN للموظفين يدويًا أو أن يخصص لهم رموز PIN مُنشأة بواسطة النظام. لاحظ أنه باستطاعة الموظفين نفسهم متابعة الوصول باستخدام أي بطاقة فعلية مخصصة لهم أيضًا.

الشرط الأساسي للتخويل للمشغّلين

يمكن منح تخويل لحامل بطاقة يسمح له بالوصول بإدخال PIN لوحده فقط بواسطة المشغّلين الذين يحملون ترخيصًا خاصًا لتعيين بطاقات افتراضية. لمنح هذا التخويل لأحد المشغّلين، تابع كما يلي.

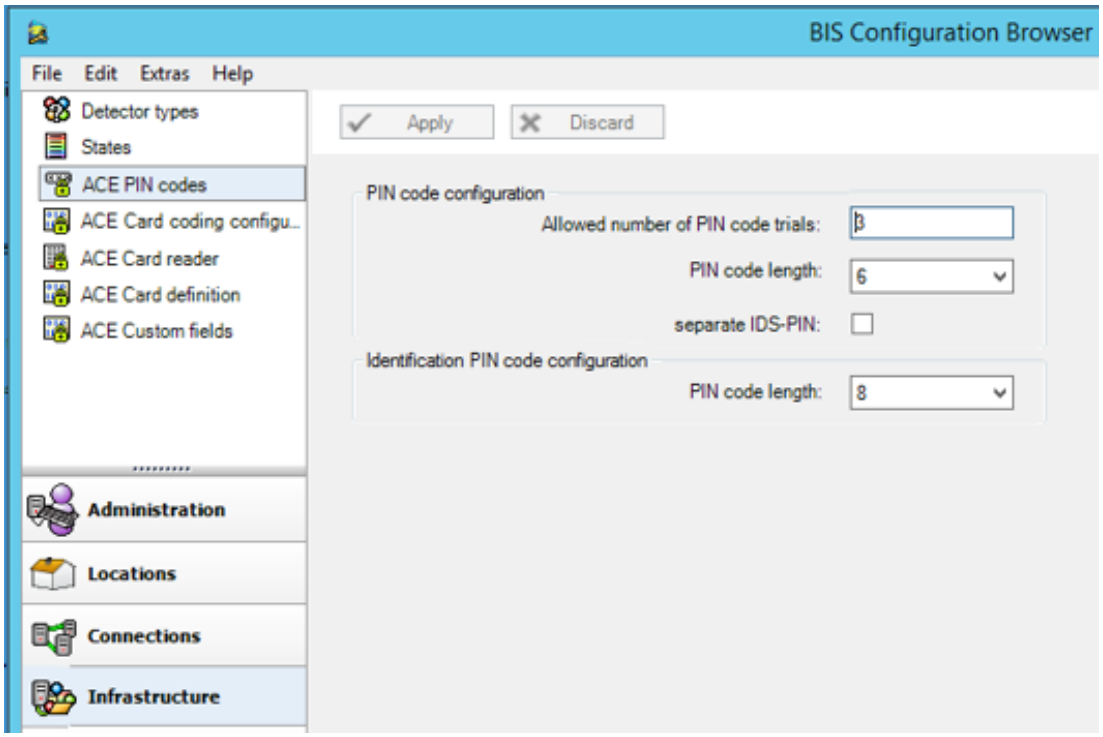
1. في مستعرض تكوين BIS انتقل إلى **الإدارة > ملفات تعريف مستخدمي ACE**
2. انتقل إلى القائمة الرئيسية **التكوين** > **المشغّلون ومحطات العمل** > **ملفات تعريف المستخدم**
3. حدد ملف تعريف المستخدم الذي يُفترض أن يستلم التخويل:
   أدخله في الحقل النصي **اسم ملف التعريف** أو استخدم وسيلة البحث للعثور على ملف التعريف المطلوب.
4. في قائمة مربعات الحوار، انقر فوق الخلية التي تتضمن **البطاقات**
   تظهر نافذة منبثقة تسمى **وظائف خاصة** بالقرب من أسفل جزء النافذة الرئيسية.
5. في جزء الوظائف الخاصة حدد خانة الاختيار **تعيين بطاقات افتراضية (PIN)**
6. انقر فوق أو **تطبيق** لحفظ تغييراتك

تعيين طول رقم التعريف PIN لأنواع أجهزة القراءة المدعومة

طول أرقام PIN التي يتم إدخالها يدوياً أو إنشاؤها من قِبل النظام محكوم بالمعلمة المحددة في تكوين النظام.

- مربع حوار مستعرض تكوين BIS
  البنية > **رموز PIN لـ ACE** > (جزء مربع الحوار السفلي) **تكوين رمز PIN للتعريف** > **طول رمز PIN**

– القائمة الرئيسية > **التكوين** > **خيارات** > **رموز PIN** > **طول رمز PIN**



تكوين قارئ للوصول بواسطة رمز PIN فقط

1. في مستعرض تكوين BIS، انتقل إلى **البنية الأساسية** > **قارئ بطاقة ACE**.

2. انتقل إلى القائمة الرئيسية > شجرة **التكوين** > **بيانات الجهاز** > **محطات العمل**
3. في جزء **محطة العمل**، حدد محطة العمل التي يتصل بها القارئ بشكل فعلي.
4. انقر بزر الماوس الأيمن وحدد قارئًا من النوع **مربع حوار إدخال رمز PIN** أو **مربع حوار إنشاء رمز PIN**.
5. حدد قارئًا في جزء **محطات العمل**.
   يظهر جزء تكوين قارئ مخصص إلى يمين جزء **محطات العمل** .
6. تأكد من أن القائمة المنسدلة **Card usage default** تحتوي على القيمة الافتراضية **بطاقة افتراضية. استخدام رمز PIN كبطاقة**.

7. انقر فوق أو **تطبيق** لحفظ تغييراتك
8. في مستعرض تكوين BIS، انتقل إلى **الاتصالات.**

9. في محرر الجهاز DevEdit، انتقل إلى شجرة **تكوين الجهاز**
10. حدد القارئ في المدخل حيث تريد تكوين الوصول بواسطة رمز PIN فقط.
11. في علامة التبويب **خيارات**، حدد خانة الاختيار **الوصول أيضًا بواسطة رمز PIN فقط.**

12. انقر فوق أو **تطبيق** لحفظ تغييراتك

16.10 لوحات توسيع AMC

إنشاء AMC-I/O-EXT (لوحة توسيع المداخل/المخارج)

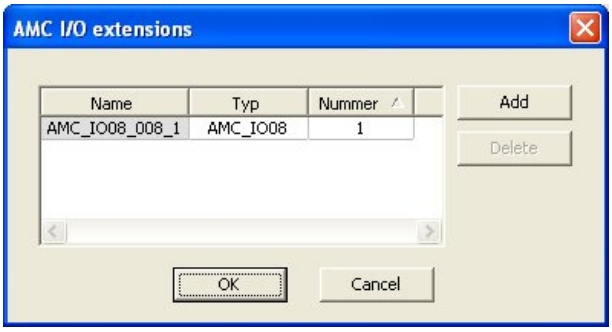
توفر لوحات التوسيع إشارات مداخل ومخارج إضافية، في حال لم تكن الملامسات الثماني الموجودة في AMC كافية لتوصيل الملامسات الضرورية (مع المصاعد مثلاً).

لوحات التوسيع هذه موصولة فعليًا بأجهزة AMC المقترنة بها ويمكن تركيبها تحت أجهزة AMC ذات الصلة فقط في محرر الجهاز. يتم تحديد إدخال AMC المقابل في المستعرض لإنشاء AMC-EXT، ويتم اختيار الإدخال **لوحة توسيع جديدة** في قائمة السياق **كائن جديد**.

إشعار!

يؤدي النقر فوق الزر **+** في شريط أدوات محرر الجهاز إلى إنشاء مداخل جديدة فقط. يمكن تحديد لوحات التوسيع باستخدام قائمة السياق.

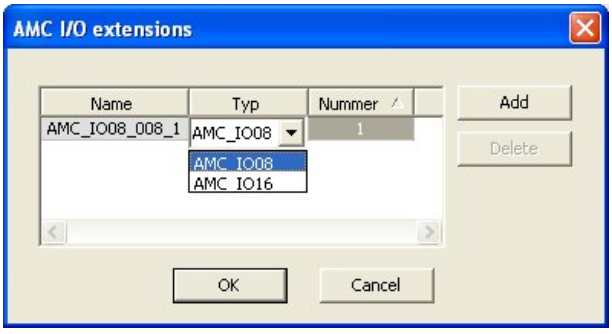
يظهر مربع حوار التحديد لإنشاء لوحات التوسيع.



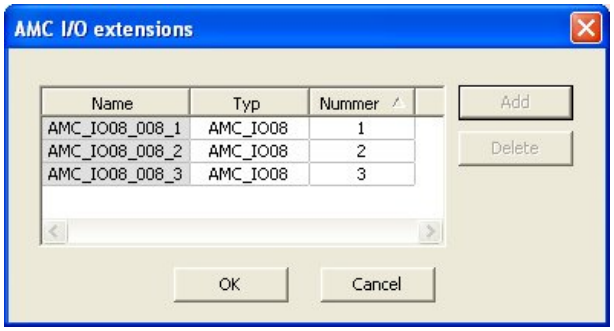
تتوفر AMC-EXT بمتغيرين:

- AMC_IO08: مع 8 مداخل و8 مخارج
- AMC_IO16: مع 16 مدخلاً و16 مخرجًا
- ملحق AMC_4W: مع 8 مداخل و8 مخارج

يتضمن مربع حوار التحديد إدخالاً مع AMC_IO08. من خلال النقر المزدوج فوق مربع القائمة في عمود **النوع**، يمكنك أيضًا وضع AMC_IO16.



يمكن توصيل حتى ثلاث لوحات توسيع بجهاز AMC واحد. ويمكن تشكيل مزيج من متغيرين. انقر فوق **إضافة** لإنشاء إدخالات قائمة إضافية. ويمكن تخصيص كافة إدخالات الأعمدة هذه.



يتم ترقيم لوحات التوسيع 1، 2 أو 3 عند إنشائها. يبدأ ترقيم الإشارات لكل لوحة بالرقم 01. ويُشكّل رقم الإشارة مع رقم اللوحة كمجموعة رقمًا تعريفيًا فريدًا. يمكن أيضًا مشاهدة إشارات لوحات التوسيع في تبويب جهاز AMC الذي تنتمي إليه.
مع إشارات المداخل والمخارج، يمكن توفير ما يصل إلى 56 زوجًا من الإشارات في جهاز AMC.
يمكن إضافة لوحات التوسيع حسب الحاجة بشكل منفرد أو بتاريخ لاحق وصولاً إلى العدد الأقصى (3 لكل جهاز AMC).

إنشاء AMC2 4W-EXT

يمكن تكوين لوحات توسيع خاصة (AMC2 4W-EXT) لوحدات التحكم AMC2 4W ذات واجهات قارئ Wiegand. توفر هذه الوحدات 4 توصيلات أجهزة قراءة Wiegand بالإضافة إلى 8 ملامسات مداخل و8 ملامسات مخارج لكل واحد منها. وبالتالي، يمكن مضاعفة العدد الأقصى لأجهزة القراءة والأبواب القابلة للتوصيل لكل جهاز AMC2 4W إلى 8.

إشعار!

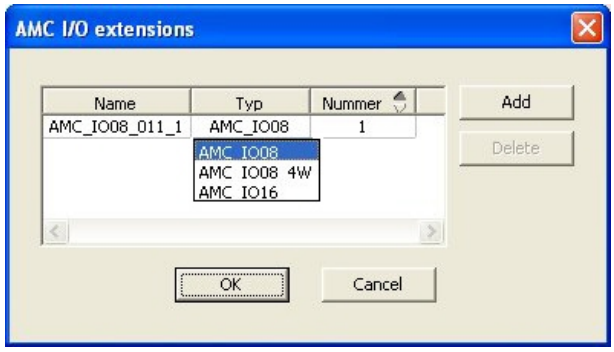
لا يمكن استخدام AMC2 4W-EXT كوحدة تحكم منفصلة، ولكن فقط كملحق لجهاز AMC2-4W. تخضع الأبواب للمراقبة ويتم اتخاذ القرارات المتعلقة بالتحكم في الوصول من قِبل AMC2 4W فقط.

يمكن استخدام AMC2 4W-EXT فقط مع AMC2 4W. وبما أنها تتضمن واجهات قارئ Wiegand فقط، فلا يمكن استخدامها مع متغير AMC، وهو AMC2 4R4
وبطريقة مماثلة للوحات توسيع المداخل/المخارج (AMC2 8I-8O-EXT وAMC2 16I-16O-EXT)، يتم توصيل AMC2 4W-EXT عبر واجهة توسيع AMC2 4W. لا تتوفر لدى لوحة التوسيع ذاكرة أو شاشة خاصة بها، ولكنها تخضع لرقابة AMC2 4W بشكل تام.
يمكن توصيل AMC2 4W-EXT واحدة وحد أقصى من ثلاث لوحات توسيع الإدخال/الإخراج بكل AMC2-4W.
لإنشاء AMC2 4W-EXT في النظام، انقر بزر الماوس الأيمن فوق الجهاز الأصلي المطلوب AMC2 4W في المستكشف وحدد **كائن جديد** > **لوحة توسيع جديدة** من قائمة السياق.

إشعار!

يمكن استخدام الزر ✚ في شريط أدوات محرر بيانات الجهاز لإضافة المداخل فقط. ويمكن إضافة لوحات التوسيع عبر قائمة السياق فقط.

يظهر مربع حوار تحديد مماثل لمربع حوار إنشاء لوحات توسيع الإدخال/الإخراج، باستثناء أن قائمة AMC2 4W تحتوي على العنصر الإضافي AMC_IO08_4W.



يمكن إضافة إدخال قائمة AMC2 4W مرة واحدة فقط، في حين يمكن إضافة ثلاث لوحات توسيع إدخال/إخراج كحدٍ أقصى.

يضيف الزر **إضافة** إدخالات قائمة جديدة. عندما يتعلق الأمر بجهاز AMC2 4W، الحد الأقصى هو 4 في حين يتم إنشاء الإدخال الرابع كلوحة AMC2 4W-EXT,

يتم ترقيم لوحات التوسيع بحسب ترتيب إنشائها 1 أو 2 أو 3. وتتلقى لوحة التوسيع AMC2 4W-EXT الرقم 0 (صفر). يستمر ترقيم الإشارات للوحة التوسيع AMC2 4W-EXT اعتبارًا من ترقيم وحدة التحكم، وتحديدًا من 9 إلى 16، حيث يبدأ ترقيم كل لوحة إدخال/إخراج بالرقم 1. وتظهر أيضًا إشارات جميع لوحات التوسيع على علامة التبويب التابعة لجهاز AMC2 4W ذي الصلة.

مع إشارات المداخل والمخارج لجهاز AMC2 4W، يمكن توفير ما يصل إلى 64 زوجًا من الإشارات.

تعديل لوحات التوسيع وحذفها

تحتوي علامة التبويب الأولى على عناصر التحكم التالية لتكوين لوحات التوسيع.

المعلمة	القيم المحتملة	الوصف
اسم اللوحة	مقيد بأحرف أبجدية رقمية: 1 - 16 خانة رقمية	يضمن التعريف الافتراضي الحصول على اسم فريد، ولكن يمكن الكتابة فوقه يدويًا. يُرجى التأكد من استخدام معرّف فريد. يجب أن تستخدم اتصالات الشبكة بخوادم DHCP اسم الشبكة.
وصف اللوحة	أحرف أبجدية رقمية: 0 - 255 خانة رقمية	يظهر هذا النص في فرع OPC.
رقم اللوحة	1 - 3	رقم اللوحة المتصلة بجهاز AMC. عرض الحقل، فقط
مورد الطاقة	0= ملغى تنشيطه (خانة الاختيار محددة) 1= منشّط (خانة الاختيار محددة)	مراقبة فولتية مورد الطاقة. عند حدوث أعطال في الفولتية، ستظهر رسالة عند انتهاء فترة التأخير. تفترض وظيفة المراقبة استخدام USV، بحيث يمكن إنشاء رسالة. 0 = بدون مراقبة 1 = تنشيط المراقبة
القسم	القيمة الافتراضية **عام**	يُعتبر ملائمة فقط عندما تكون ميزة **الأقسام** مرخصة.

تتضمن علامة تبويب "المداخل" و"المخارج" و"إعدادات الإشارات" التخطيط نفسه والوظيفة نفسها كما في علامات التبويب المناظرة لوحدات التحكم.

حذف لوحات التوسيع

يمكن حذف لوحة توسيع فقط عندما لا تكون أي واحدة من واجهاتها مشغولة. يجب أولاً تكوين الإشارات المقترنة على لوحة مختلفة قبل أن يصبح زر الحذف وخيار قائمة السياق **حذف كائن** قابلين للاستخدام.

AMC2 4W-EXT

نظرًا لعدم إمكانية إزالة أجهزة القراءة التي تشغل لوحات التوسيع أو إعادة تكوينها بشكل فردي، يجب حذفها مع المداخل المطابقة لها. وحتى ذلك الحين، لا يمكن أيضًا إزالة لوحة التوسيع AMC2 4W-EXT.

17 تكوينات القارئ المخصصة

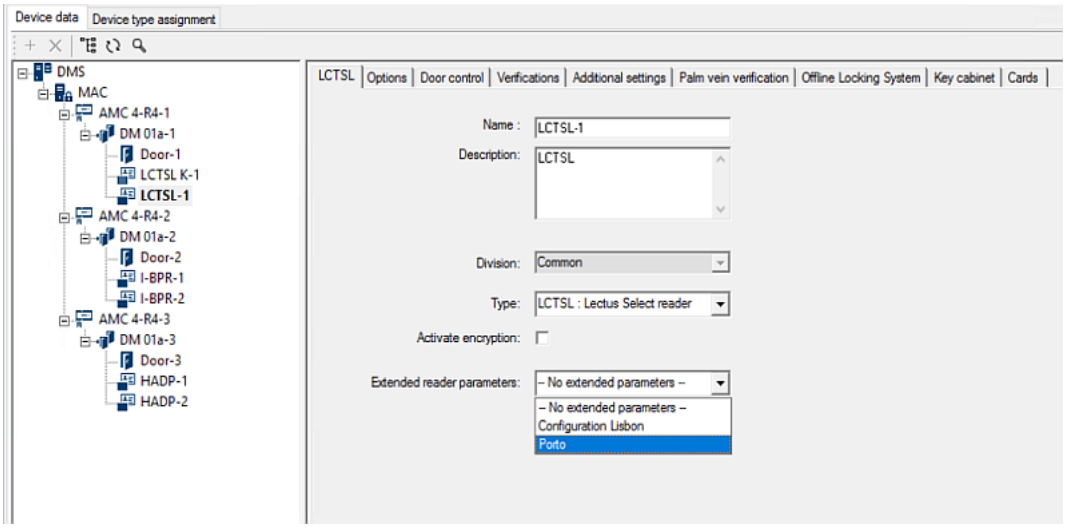
17.1 المقدمة

اعتبارًا من BIS 4.9 و AMS 4.0، تسمح أنظمة التحكم في الوصول من Bosch باستخدام إعدادات MIFARE DESFire المخصصة. يمكنك إنشاء ملفات معلمات مشفرة باستخدام الأداة المساعدة `Bosch.ReaderConfigTool.exe`. هذه الأداة مضمنة في إعدادات BIS ACE 4.9 وAMS 4.0 والإصدارات الأحدث، مع وثائقها الخاصة. راجع هذه الوثائق للاطلاع على القائمة الحالية لأجهزة القراءة المتوافقة.

تصف الأقسام التالية كيفية استخدام محرر الجهاز لاستيراد ملف معلمة مشفر وتطبيقه على أي من أجهزة القراءة المتوافقة أو كلها في التدرج الهرمي لأجهزة التحكم في الوصول.

17.2 خاصية القارئ: معلمات القارئ الموسعة

تظهر مجموعات المعلمات الموسعة المتاحة لأجهزة القراءة المتوافقة على صفحات خصائصها في محرر الجهاز تحت التسمية **معلمات القارئ الموسعة**.



الشكل التوضيحي 17.1: معلمات القارئ الموسعة

القيمة الافتراضية للقائمة المنسدلة هي `No extended parameters`. هذه هي القيمة الوحيدة الممكنة ما لم تقم باستيراد مجموعات معلمات إضافية.

الإجراء

لتطبيق مجموعة معلمات مستوردة على قارئ فردي متوافق:

1. في محرر الجهاز، حدد القارئ في شجرة الأجهزة.
2. حدد علامة تبويب الخاصية الأولى.
3. حدد مجموعة المعلمات المطلوبة من قائمة **معلمات القارئ الموسعة**
4. انقر فوق **تطبيق** أو

17.3 استيراد مجموعة معلمات القارئ

يمكنك استيراد ملفات المعلمات وحذفها فقط على مستوى DMS التدرج الهرمي للجهاز.

الشروط الأساسية

الوصول إلى ملف معلمات موافق عليه لنظام التحكم في الوصول. بشكل افتراضي، الملف من النوع `ReaderConfigSave`.

الإجراء

1. في محرر الجهاز، انقر بزر الماوس الأيمن فوق عقدة DMS وحدد **استيراد مجموعات معلمات القارئ** من قائمة السياق.
تظهر النافذة المنبثقة **استيراد مجموعات معلمات القارئ**.
2. انقر فوق **ملف** وحدد موقع ملف المعلمات باستخدام مستكشف الملفات.
3. أدخل كلمة مرور ملف المعلمات، عند مطالبتك بذلك.
إذا كانت كلمة المرور صحيحة، يتم ملء النصف السفلي من النافذة المنبثقة بالمعلومات التالية:
- قائمة بأنواع أجهزة القراءة التي تنطبق عليها مجموعة المعلمات.
- اسم مجموعة المعلمات. يمكن تحريره في مربع الحوار هذا.
- وصف عبارة عن نص حر، إذا قام منشئ مجموعة المعلمات بتوفيره. يمكنك إضافة وصف أو تحريره في مربع الحوار هذا.
4. انقر فوق **استيراد** لاستيراد مجموعة المعلمات كي يستخدمها في المستقبل نظام التحكم في الوصول.
- يتم استيراد مجموعة المعلمات وتخزينها في نظام التحكم في الوصول.
- وتُضاف إلى قائمة مجموعات المعلمات المتوفرة في أعلى النافذة المنبثقة.
5. انقر فوق **خروج** للخروج من النافذة المنبثقة **استيراد مجموعات معلمات القارئ**.

17.4 تطبيق مجموعة معلمات على أجهزة القراءة

المقدمة

يؤدي استيراد مجموعة معلمات إلى نظام التحكم في الوصول إلى تخزينها لاستخدامها في المستقبل، ولكنه لا يؤدي إلى تطبيقها على أجهزة القراءة في المستقبل. يُعد تطبيق مجموعة المعلمات خطوة إضافية يمكنك تنفيذها على مستويات مختلفة في التدرج الهرمي للجهاز:

- DMS
- MAC
- AMC

عند تطبيق مجموعة معلمات على مستوى DMS أو MAC أو AMC، يمكنها أن تطبّق فقط على أجهزة القراءة التابعة لأنواع أجهزة القراءة التي تم إنشاء المجموعة من أجلها. ولن تتأثر جميع أجهزة القراءة الأخرى التابعة.

الشروط الأساسية

لقد قمت باستيراد مجموعة معلمات القارئ بنجاح.

الإجراء

1. في محرر الجهاز، انقر بزر الماوس الأيمن فوق قارئ أو جهاز (DMS أو MAC أو AMC) تريد وصف أجهزة القراءة الخاصة به بواسطة معلمات.
2. حدد **إدارة مجموعات معلمات القارئ** من القائمة السياقية.
3. في جزء القائمة العلوية، **مجموعات معلمات لأنواع أجهزة القراءة**، حدد مجموعة المعلمات التي تريد تطبيقها.
أجهزة القراءة القابلة للتطبيق مذكورة في الجزء السفلي الأيسر: **أجهزة القراءة القابلة لوصفها بمعلمات بواسطة مجموعة المعلمات هذه**.
4. في القائمة **أجهزة القراءة القابلة لوصفها بمعلمات بواسطة مجموعة المعلمات هذه**، حدد أجهزة القراءة التي تريد تطبيق مجموعة المعلمات المحددة عليها.
- إذا كان عدد أجهزة القراءة كبيرًا، فاستخدم القوائم المنسدلة لتقييد العرض بحيث يقتصر على أجهزة تابعة لوحدة MAC أو AMC معينة.
5. استخدم أزرار الأسهم لنقل أجهزة القراءة المحددة إلى الجزء السفلي الأيمن، **جميع أجهزة القراءة التي تم وصفها بمعلمات بواسطة مجموعة المعلمات هذه**.

إشعار!
عرض أجهزة القراءة المتوافقة
ستكون مدرجة في القائمة فقط أجهزة القراءة المتوافقة مع مجموعة المعلمات. إذا حددت خانة الاختيار **إظهار جميع أجهزة القراءة**، فستظهر أيضًا أجهزة القراءة التي لديها مجموعات معلمات أخرى. إنها تتميز بخلفية رمادية لوضع علامة عليها باعتبارها للقراءة فقط لمجموعة المعلمات المحددة.

6. انقر فوق **موافق** لإغلاق النافذ المنبثقة.

7. بالعودة إلى محرر الجهاز، انقر فوق **تطبيق** أو
يتم تطبيق مجموعة المعلمات على جميع أجهزة القراءة التي تركتها في القائمة **جميع أجهزة القراءة التي تم وصفها بمعلمات بواسطة مجموعة المعلمات هذه** في النافذة المنبثقة.

17.5 إدارة مجموعات معلمات القارئ

المقدمة
يمكنك تغيير تطبيق مجموعات المعلمات على مستويات مختلفة في التدرج الهرمي للجهاز:
- DMS
- MAC
- AMC

بإمكان التغييرات على مستوى DMS أو MAC أو AMC أن تطبّق فقط على أجهزة القراءة التابعة لأنواع أجهزة القراءة التي تم إنشاء المجموعة من أجلها. ولن تتأثر جميع أجهزة القراءة الأخرى التابعة.

الشرط الأساسي
لقد قمت باستيراد مجموعة معلمات القارئ بنجاح.

الإجراء
1. في محرر الجهاز، انقر بزر الماوس الأيمن فوق قارئ أو جهاز (DMS أو MAC أو AMC).
2. حدد **إدارة مجموعات معلمات القارئ** من القائمة السياقية.
3. في جزء القائمة العلوية، **مجموعات المعلمات لأنواع أجهزة القراءة**، حدد مجموعة المعلمات التي تريد تطبيقها.
- أجهزة القراءة القابلة للتطبيق مدرجة في الجزء السفلي الأيسر: **أجهزة القراءة القابلة لوصفها بمعلمات بواسطة مجموعة المعلمات هذه**.
- أجهزة القراءة التي تم تطبيق ملف المعلمات عليها مذكورة في الجزء السفلي الأيمن: **جميع أجهزة القراءة التي تم وصفها بمعلمات بواسطة مجموعة المعلمات هذه**.
4. حدد أجهزة القراءة في أي من القائمتين. استخدم مفاتيح الأسهم لنقل أجهزة القراءة إلى داخل القائمة في الجزء السفلي الأيمن أو خارجها، **جميع أجهزة القراءة التي تم وصفها بمعلمات بواسطة مجموعة المعلمات هذه**.
- مهم: دوّن بتأنٍ أجهزة القراءة التي تخرجها من القائمة، للخطوة الأخيرة في هذا الإجراء.
5. عندما تكمل تغييراتك، انقر فوق **موافق** لإغلاق النافذة المنبثقة.

6. بالعودة إلى محرر الجهاز، انقر فوق **تطبيق** أو
- يتم تطبيق مجموعة المعلمات على جميع أجهزة القراءة التي تركتها في القائمة **جميع أجهزة القراءة التي تم وصفها بمعلمات بواسطة مجموعة المعلمات هذه**.
- تتم إزالتها من أجهزة القراءة التي أخرجتها من هذه القائمة.
7. نفّذ واحدًا مما يلي على جميع أجهزة القراءة التي أخرجتها من هذه القائمة:
- إعادة تعيين إعدادات المصنع الافتراضية باستخدام مفاتيح DIP في جهاز القارئ.
- تطبيق مجموعة معلمات مختلفة عليها.

إشعار!
لا يؤدي حذف مجموعة معلمات إلى إعادة تكوين أجهزة القراءة التي استخدمتها.
سيستمر تكوين القارئ المحذوف في أجهزة القراءة التي استخدمته حتى تعيد تعيين جهاز القارئ، أو تطبيق مجموعة معلمات مختلفة.

17.6 حذف مجموعات معلمات القارئ

يمكنك استيراد ملفات المعلمات وحذفها فقط على مستوى DMS التدرج الهرمي للجهاز.

الشروط الأساسية

تم استيراد ملف معلمات واحد على الأقل إلى نظام التحكم في الوصول.

الإجراء

1. في محرر الجهاز، انقر بزر الماوس الأيمن فوق عقدة DMS وحدد **حذف مجموعات معلمات القارئ** من قائمة السياق.
   تظهر النافذة المنبثقة **حذف مجموعات معلمات القارئ**.
2. في القائمة **مجموعات المعلمات لأنواع أجهزة القراءة**، حدد مجموعة المعلمات التي تريد حذفها.
   - في الجزء السفلي الأيمن من النافذة المنبثقة، تظهر قائمة تتضمن جميع أجهزة القراءة التي تم وصفها حاليًا بمعلمات (تكوينها) بواسطة مجموعة المعلمات هذه.
   - دوّن بتأنٍ أجهزة القراءة هذه، ستحتاج إلى إعادة تعيين أو إعادة تكوين بعد حذف مجموعة المعلمات. للحصول على المزيد من التفاصيل، راجع الخطوة الأخيرة في هذا الإجراء.
3. انقر فوق **حذف**
4. انقر فوق **خروج**

5. بالعودة إلى محرر الجهاز، انقر فوق **تطبيق** أو
6. نفّذ واحدًا مما يلي على جميع أجهزة القراءة التي كانت تستخدمها مجموعة المعلمات المحذوفة:
   - إعادة تعيين إعدادات المصنع الافتراضية باستخدام مفاتيح DIP في جهاز القارئ.
   - تطبيق مجموعة معلمات مختلفة عليها.

إشعار!

لا يؤدي حذف مجموعة معلمات إلى إعادة تكوين أجهزة القراءة التي استخدمتها.
سيستمر تكوين القارئ المحذوف في أجهزة القراءة التي استخدمته حتى تعيد تعيين جهاز القارئ، أو تطبيق مجموعة معلمات مختلفة.

18 الحقول المخصصة لبيانات الموظفين

المقدمة

يمكن تخصيص حقول البيانات للموظفين باستخدام عدة طرق:

- ما إذا كانت **مرئية**، أي ما إذا كانت تظهر في العميل بأي طريقة
- ما إذا كانت **مطلوبة**، أي ما إذا كان من الممكن تخزين سجل بيانات من دون وجود بيانات صالحة في الحقل
- ما إذا كان يجب إبقاء القيم التي تحتوي عليها هذه الحقول **فريدة** ضمن النظام
- نوع البيانات الذي تحتوي عليه هذه الحقول (نص، تاريخ ووقت، عدد صحيح وغير ذلك)
- مكان ظهورها (علامة التبويب، والعمود والصف) في العميل
- مدى كبر الحجم الذي تظهر به
- ما إذا كان يجب استخدام البيانات في التقارير القياسية ومكان استخدامها

يبقى من الممكن، بطبيعة الحال، تعريف حقول بيانات جديدة بالكامل مع جميع السمات المذكورة هنا.

18.1 معاينة وتحرير الحقول المخصصة

مسار مربع الحوار

- في مستعرض التكوين، انتقل إلى قائمة **البنية الأساسية** > **حقول ACE مخصصة**.
- القائمة الرئيسية > **التكوين** > **خيارات** > **حقول مخصصة**

تم تقسيم النافذة الرئيسية إلى علامتي تبويب

نظرة عامة إن علامة التبويب هذه وعلامات التبويب الفرعية التابعة لها (**العنوان وجهة الاتصال وبيانات إضافية خاصة بالشخص وبيانات إضافية خاصة بالشركة وملاحظات وعنصر تحكم البطاقة** و**معلومات إضافية**) هي للقراءة فقط وتوفر لك نظرة عامة تقريبية للبيانات التي ستظهر على علامات التبويب في العميل بحيث أن ما تراه هو ما تحصل عليه (WYSIWYG).

التفاصيل تحتوي علامة التبويب هذه على قائمة ببرامج التحرير، محرر واحد لكل حقل بيانات معرّف مسبقًا أو معرّف بواسطة المستخدم.

المعاينة

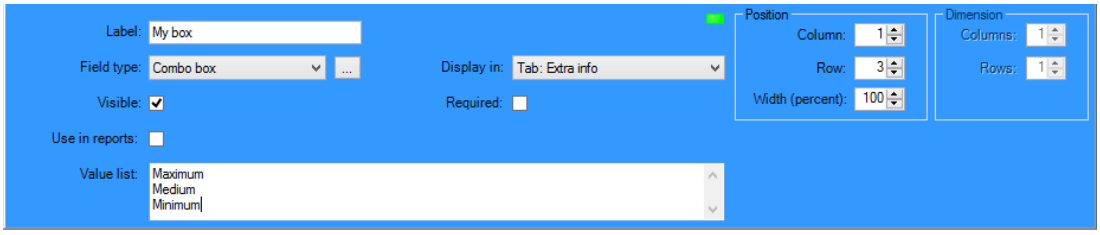
إذا أردت معاينة تأثير أي تغيير تم إدخاله في علامة تبويب **التفاصيل**، انقر فوق الزر **تطبيق** وانتقل إلى علامة التبويب **نظرة عامة** في مستعرض التكوين.

للاطلاع على تأثير هذه التغييرات في عميل ACE، انقر فوق الزر **تطبيق** وافتح مربع الحوار ذات الصلة في عميل ACE. من غير الضروري إعادة تحميل التكوين أو أعادة تشغيل عميل ACE. ومع ذلك، إذا كان مربع الحوار المعدّل مفتوحًا حاليًا في عميل ACE، فسيكون من الضروري إغلاق مربع الحوار هذا وإعادة فتحه.

تحرير حقول البيانات الموجودة

على علامة التبويب **حقول مخصصة** > **التفاصيل**، توجد نافذة محرر لكل حقل بيانات، سواء كان معرّفًا بشكل مسبق أو بواسطة المستخدم، حيث يمكن تعديل سماته.

انقر فوق محرر الحقل الذي تريد تعديله. سيتم تمييز المحرر النشط.



يقدم الجدول التالي شرحًا للسمات القابلة للتحرير للحقول المخصصة.

نص التسمية	الوصف
التسمية	**التسمية** هي تسمية حقل البيانات كما يظهر في العميل. ويمكن الكتابة فوقها، بشكل اختياري، لعكس المصطلحات المستخدمة في موقعك.
نوع الحقل	**نوع الحقل** هو نوع البيانات، ويحدد عنصر تحكم الحوار الذي سيستخدمه المشغّل لإنشاء إدخالات في العميل. يوفر كل نوع حقل عمليات تدقيق التناسق لقيم الإدخال الخاصة به، لضمان الحصول على تواريخ وأوقات وأطوال نص وحدود قيم رقمية صالحة. – **حقل نصي** – انقر فوق زر علامة القطع إلى جانبه لتحديد عدد الأحرف المسموحة. – **خانة اختيار** – **حقل التاريخ** – **الوقت** – **حقل التاريخ والوقت** – **مربع تحرير وسرد** – أدخل القيم الصالحة لمربع التحرير والسرد في الحقل النصي المتوفر. استخدام الفواصل أو أحرف الرجوع للفصل بين القيم. – **إدخال رقمي** – أدخل الحد الأدنى والحد الأقصى لقيم الإدخال الرقمي في مربعات الزيادة والنقصان المتوفرة. – **عنصر تحكم المبنى 1** و**عنصر تحكم المبنى 2** – إنها عناصر تحكم خاصة يمكن إعادة تسميتها هنا (في حقل **التسمية**) وربطها بالأوامر في واجهة مستخدم العميل. وهكذا يمكنك منح مستخدمين معينين إذنًا، عبر بطاقاتهم، يسمح لهم بتنفيذ عمليات خاصة ضمن الموقع. من الأمثلة عن هذه العمليات تشغيل الأضواء الكاشفة أو مراقبة معدات معينة.
مرئي	امسح خانة الاختيار هذه لمنع ظهور حقل البيانات في العميل.
فريد	حدد خانة الاختيار هذه لضمان فرادة القيم المدخلة في هذا الحقل. يرفض النظام عندئذٍ إدخال أي قيمة تم تخزينها لهذا الحقل في قاعدة البيانات. على سبيل المثال، يجب أن تكون أرقام الموظفين فريدة للأشخاص، ولوحات الترخيص فريدة للمركبات.
	يعني الضوء الأخضر أن حقل البيانات **غير** مستخدم حاليًا في قاعدة البيانات. يعني الضوء الأحمر أن حقل البيانات مستخدم حاليًا في قاعدة البيانات.
عرض في	استخدم هذه القائمة المنسدلة لتحديد علامة تبويب العميل حيث يجب أن يظهر حقل البيانات.
مطلوب	حدد خانة الاختيار هذه لجعل حقل البيانات إلزاميًا. على سبيل المثال، يجب إدخال الكنية في سجل كل موظف. وبالتالي، لا يمكن تخزين سجل البيانات من دون إدخال الكنية. تجدر الإشارة إلى أن المحرر لن يسمح بتعيين حقل بيانات مطلوب كغير مرئي عبر خانة الاختيار **مرئي**. لتمكين سهولة الاستخدام في العميل، من المستحسن وضع جميع الحقول المطلوبة على علامة التبويب الأولى.
الموضع	استخدم مربعات الزيادة والنقصان لكل من **العمود** و**الصف** لتعيين موضع حقل البيانات على علامة التبويب المسماة في القائمة المنسدلة **عرض في**. تجدر الإشارة إلى أن المحرر لن يسمح لك بتحديد موضع قيد الاستخدام، أو تغطية حقول البيانات الموجودة.

نص التسمية	الوصف
	استخدم مربع الزيادة والنقصان **العرض (النسبة المئوية)** لتعيين موضع بعض عناصر التحكم القابلة لتغيير الحجم، مثل الحقول النصية. يعني الخيار 100% أن عنصر التحكم سوف يشغل كل الفتحة التي لا تشغلها تسمية حقل البيانات.
البُعد	استخدم مربعات الزيادة والنقصان لكل من **العمود** و**الصف** لتحديد عدد الأعمدة والصفوف التي يجب شغلها على علامة التبويب المسماة في القائمة المنسدلة **عرض في**. تجدر الإشارة إلى أن المحرر لن يسمح لك بتغطية حقول البيانات الموجودة.

إنشاء وتحرير حقول بيانات جديدة

على علامة التبويب **حقول مخصصة** > **التفاصيل**، يوجد جزء محرر لكل حقل بيانات، سواء كان معرّفًا بشكل مسبق أو بواسطة المستخدم، حيث يمكن تعديل سماته.

انقر فوق الزر **حقل جديد** لإنشاء حقل مخصص جديد له محرره الخاص. سيتم تمييز جزء المحرر النشط.

يتضمن المحرر عناصر تحكم الحوار نفسها لتحرير حقول البيانات الموجودة، راجع الجدول أعلاه، بالإضافة إلى عنصري تحكم إضافيين:

استخدام في التقارير (خانة اختيار)	حدد خانة الاختيار هذه لتمكين ظهور حقل البيانات الجديد في التقارير القياسية.
رقم التسلسل (مربع الزيادة والنقصان)	يحدد رقم التسلسل العمود الذي سيشغله حقل البيانات في التقارير القياسية.

إشعار!

أرقام التسلسل الوحيدة القابلة للعنونة حاليًا بواسطة **Badge Designer** و**التقارير** هي أرقام التسلسل 1..10.

18.2 قواعد خاصة بحقول البيانات.

- موقع حقول البيانات
- بإمكان كل حقل أن يظهر على علامة تبويب واحدة فقط.
- بإمكان كل حقل مخصص أن يظهر على أي علامة تبويب قابلة للتحديد.
- يمكن نقل الحقول إلى علامات تبويب أخرى عن طريق تغيير الإدخال في القائمة المنسدلة **عرض في**.
- بإمكان التسمية أن تحتوي على أي نص: الحد الأقصى للطول 20 حرفًا.
- بإمكان حقول البيانات المخصصة أن تحتوي على أي نص: الحد الأقصى للطول 2000 حرف.
- يمكن تحويل أي حقل إلى حقل مطلوب، ولكن يجب تحديد خانة الاختيار **مرئي** التابعة له.

إشعار!

نصائح ضرورية قبل الاستخدام الإنتاجي

وافق على أنواع الحقول واستخداماتها وأنجزها قبل استخدامها لتخزين بيانات الأشخاص.

يتم تعيين كل حقل إدخال بيانات إلى حقل قاعدة بيانات معين بحيث يمكن تحديد موقع البيانات بشكل يدوي وبواسطة منشئي التقارير. عند الانتهاء من تخزين سجلات البيانات من الحقول المخصصة في قاعدة البيانات، سيتعذر عندئذٍ نقل هذه الحقول أو تغييرها من دون التعرض لخطر فقدان البيانات.

19 تكوين إدارة مستوى التهديد

المقدمة

تهدف إدارة مستوى التهديد إلى الاستجابة بفعالية لمواقف طارئة عن طريق إجراء تغيير فوري على سلوك المداخل في كل أنحاء المنطقة المتضررة.

19.1 مفاهيم إدارة مستوى التهديد

- **التهديد** عبارة عن موقف حرج يتطلب استجابة فورية ومتزامنة من بعض المداخل أو كلها في نظام تحكم في الوصول
- يمثل **مستوى التهديد** استجابة النظام لموقف متوقع. ويجب تكوين كل مستوى تهديد بتأنٍّ حتى يعرف كل مدخل من مداخل MAC كيفية الاستجابة.

مستويات التهديد قابلة للتخصيص بشكل كامل، على سبيل المثال يمكن تكوين مستويات التهديد العالي النموذجية كما يلي:

- **القفل الخارجي**: لا يُسمَح بالدخول إلا للمستجيبين الأوائل المتمتعين بمستويات أمان مرتفعة.
- **القفل الداخلي**: يتم قفل كل الأبواب. ويتم رفض الدخول والخروج لكل بيانات الاعتماد التي تقل عن مستوى أمان مُكوَّن.
- **الإخلاء**: يتم فتح كل أبواب الخروج.

- يمكن تكوين مستويات التهديد المنخفض النموذجية كما يلي:
  - **الحدث الرياضي**: يتم فتح الأبواب المؤدية إلى الأماكن الرياضية، بينما يتم تأمين كل الأماكن الأخرى.
  - **اجتماع ولي الأمر**: لا يمكن الوصول إلا إلى بعض الفصول الدراسية والمدخل الرئيسي.
- **تنبيه التهديد**: تنبيه يعمل على تشغيل مستوى تهديد. يمكن للأشخاص المخوّلين الملائمين تشغيل تنبيه تهديد بإجراء سريع، على سبيل المثال من خلال واجهة المستخدم الخاصة بالمشغّل، أو من خلال إشارة جهاز (زر يعمل بالضغط مثلاً)، أو من خلال توفير أي بطاقة تنبيه خاصة في أي قارئ.
- **مستوى الأمان**: سمة تتمتع بها **ملفات تعريف الأمان**الخاصة بحاملي البطاقات وأجهزة القراءة، ويُعبّر عنه كعدد صحيح 0..100. يقوم كل مستوى تهديد بتعيين أجهزة قراءة وحدة التحكم في الوصول الرئيسية (MAC) الخاصة به على مستويات الأمان المُعيّنة. ثم تمنح أجهزة القراءة هذه إمكانية الوصول فقط لبيانات الاعتماد الخاصة بأشخاص لديهم مستوى أمان مساوٍ أو أكبر في ملفات تعريف الأمان لديهم.
- **ملف تعريف الأمان** عبارة عن مجموعات من السمات التي يمكن تعيينها إلى **نوع شخص** (**ملف تعريف أمان شخص**) أو باب (**ملف تعريف أمان باب**) أو قارئ (**ملف تعريف أمان قارئ**).

وتحكم ملفات تعريف الأمان سلوكيات التحكم في الوصول التالية:

- **مستوى الأمان**، حسب تعريفه سالف الذكر، لنوع شخص أو باب أو قارئ
- **معدل الفحص**: النسبة المئوية لاحتمالية تشغيل الفحص العشوائي من قِبل نوع الشخص أو القارئ هذا.

19.2 نظرة عامة على عملية التكوين

تتطلب إدارة مستوى التهديد خطوات التكوين التالية والتي يرد شرحها بالتفصيل بعد هذه النظرة العامة

1. في محرر الجهاز
   - تعريف مستويات التهديد
   - تعريف ملفات تعريف أمان الأبواب
   - تعريف ملفات تعريف أمان أجهزة القراءة
   - تعيين ملفات تعريف أمان الأبواب للمداخل
2. في مربعات حوار بيانات النظام
   - تعريف ملفات تعريف أمان الأشخاص
   - تعيين ملفات تعريف أمان الأشخاص لأنواع الأشخاص
3. في مربعات حوار بيانات الموظفين
   - تعيين أنواع أشخاص للأشخاص
   - تعيين أنواع أشخاص لمجموعات الأشخاص

عند تكوين إدارة مستوى التهديد بنجاح، يمكن مراقبة تنبيهات وحالات وحدة MAC والتحكم فيها من تطبيق Map View. لمزيد من التفاصيل، يُرجى مراجعة تعليمات Map View عبر الإنترنت.

19.3 خطوات التكوين في محرر الجهاز

يصف هذا القسم خطوات التكوين الأساسية في محرر الجهاز.

إشعار!
لا يمكن تحرير بيانات الجهاز في محرر الجهاز بينما يكون مستوى تهديد قيد التشغيل.

19.3.1 إنشاء مستوى تهديد

يوضح هذا القسم كيفية إنشاء مستويات تهديد للاستخدام في موقعك. ويمكن إنشاء ما يصل إلى 15 مستوى.

مسار مربع الحوار
- **القائمة الرئيسية >التكوين > بيانات الجهاز**
- **مستعرض تكوين BIS > الاتصالات > بيانات الجهاز**

الإجراء
1. حدد علامة التبويب الفرعية **مستويات التهديد**
   - يظهر جدول مستويات التهديد. ويمكن أن يحتوي على ما يصل إلى 15 مستوى تهديد، لكل منه اسم ووصف وخانة اختيار لتنشيط مستوى التهديد بعد تكوينه.
2. انقر فوق السطر الذي يقول: **يُرجى إدخال اسم لمستوى التهديد**
3. أدخل اسمًا سيكون مفيدًا لمشغّلي النظام.
4. (اختياري) في عمود **الوصف**، أدخل وصفًا كاملاً لسلوك المداخل عندما يكون مستوى التهديد هذا قيد التشغيل.
5. لا **تحدد** خانة الاختيار **نشط** في هذه المرة. أكمل أولاً جميع خطوات التكوين الأخرى لمستوى التهديد هذا، على النحو المبين في الأقسام التالية.
6. انقر فوق (حفظ) لحفظ مستوى التهديد الجديد.

19.3.2 إنشاء ملف تعريف أمان باب

يوضح هذا القسم كيفية إنشاء ملفات تعريف أمان لأنواع مختلفة من الأبواب، وكيفية تعريف الحالة التي ستتحول إليها كل أبواب ملف التعريف هذا عندما يكون مستوى تهديد قيد التشغيل.

مسار مربع الحوار
- **القائمة الرئيسية >التكوين > بيانات الجهاز**
- **مستعرض تكوين BIS > الاتصالات > بيانات الجهاز**

الشروط الأساسية
- تم تعريف مستوى تهديد واحد على الأقل.
- تم تكوين مدخل واحد على الأقل في شجرة الأجهزة.

الإجراء
1. حدد علامة التبويب الفرعية **ملفات تعريف أمان الأبواب**
   - تتكون نافذة مربع الحوار الرئيسي من جزأين: **التحديد** و**ملف تعريف أمان الباب** (الاسم الافتراضي)
2. انقر فوق **جديد**
   - يتم إنشاء ملف تعريف أمان باب جديد باسم افتراضي

- تتم تعبئة جدول **مستوى التهديد** في جزء **ملف تعريف أمان الباب** بمستويات التهديد التي تم إنشاؤها بالفعل، إلى جانب القيمة **غير محدد** لكل منها في عمود **الحالة**.

3. في جزء **ملف تعريف أمان الباب**، أدخِل اسمًا لنوع الباب الذي سيتم تعيين ملف التعريف هذا له.
   - يظهر اسم ملف التعريف الجديد في جزء **التحديد**. إذا لزم الأمر، يمكن حذفه من التكوين عن طريق النقر فوق **حذف** في ذلك الجزء.
4. (اختياري) أدخل وصفًا لملف التعريف لمساعدة المشغّلين على تعيينه بشكل صحيح.
5. إذا كان يجب تعيين ملف التعريف هذا إلى أبواب دوارة، فحدد خانة الاختيار **باب دوار**.
   - سيوفر هذا خيارات إضافية للحالة المستهدفة للباب عند مستويات تهديد مختلفة، على سبيل المثال خيارات السماح بالدخول أو الخروج وحده أو كليهما معًا.
6. في عمود **الحالة** بجدول **مستوى التهديد**، حدد لكل مستوى تهديد حالة مستهدفة ملائمة لجميع أبواب ملف التعريف هذا، كلما كان مستوى التهديد ذلك قيد التشغيل.
7. انقر فوق (حفظ) لحفظ التغييرات.

كرر الإجراء لإنشاء عدد من ملفات تعريف أمان الأبواب بقدر أنواع الأبواب في تكوينك. قد تكون الأنواع النموذجية للأبواب:

- الباب العمومي الرئيسي
- باب الإخلاء إلى الخارج
- باب الوصول إلى الفصول الدراسية
- الباب العمومي إلى الساحة الرياضية

19.3.3 إنشاء ملف تعريف أمان قارئ

يوضح هذا القسم كيفية إنشاء ملفات تعريف أمان لأنواع مختلفة من أجهزة القراءة. تعرّف ملفات تعريف أمان أجهزة القراءة سمات أجهزة القراءة التالية **لكل مستوى تهديد**:

- أدنى مستوى أمان مطلوب من بيانات اعتماد للحصول على حق الوصول إلى القارئ.
- معدل الفحص، أي النسبة المئوية من حاملي البطاقات التي سيتم اختيارهم عشوائيًا لفحوص الأمان الإضافية.
- **ملاحظة**: يتجاوز معدل الفحص المعيّن في ملف تعريف أمان القارئ معدل الفحص المعيّن في القارئ نفسه.

مسار مربع الحوار

- **القائمة الرئيسية >التكوين > بيانات الجهاز**
- **مستعرض تكوين BIS > الاتصالات > بيانات الجهاز**

الشروط الأساسية

- تم تعريف مستوى تهديد واحد على الأقل.
- تم تكوين مدخل واحد على الأقل في شجرة الأجهزة.

الإجراء

1. حدد علامة التبويب الفرعية **ملفات تعريف أمان أجهزة القراءة**
   - تتكون نافذة مربع الحوار الرئيسي من جزأين: **التحديد** و**ملف تعريف أمان القارئ** (الاسم الافتراضي)
2. انقر فوق **جديد**
   - يتم إنشاء ملف تعريف أمان قارئ جديد باسم افتراضي
   - تتم تعبئة جدول **مستوى التهديد** في جزء **ملف تعريف أمان القارئ** بمستويات التهديد التي تم إنشاؤها بالفعل، إلى جانب القيمة الافتراضية **0** لكل منها في عمودَي **مستوى الأمان** و**معدل الفحص**.
3. في جزء **ملف تعريف أمان القارئ**، أدخِل اسمًا لنوع القارئ الذي سيتم تعيين ملف التعريف هذا له.

- يظهر اسم ملف التعريف الجديد في جزء **التحديد**. إذا لزم الأمر، يمكن حذفه من التكوين عن طريق النقر فوق **حذف** في ذلك الجزء.

4. (اختياري) أدخل وصفًا لملف التعريف لمساعدة المشغّلين على تعيينه بشكل صحيح.
5. في عمود **مستوى الأمان** بجدول **مستوى التهديد**، حدد لكل مستوى تهديد حدًا أدنى لمستوى الأمان (في شكل عدد صحيح 0..100) يجب أن يكون لدى أي مشغّل حتى يتمكن من تشغيل أي قارئ بملف التعريف هذا، كلما كان مستوى التهديد ذلك قيد التشغيل.
6. في عمود **معدل الفحص** بجدول **مستوى التهديد**، حدد لكل مستوى تهديد النسبة المئوية لحاملي البطاقات الذين سيختارهم القارئ عشوائيًا من أجل فحوص الأمان الإضافية كلما كان مستوى التهديد ذلك قيد التشغيل.
7. انقر فوق (حفظ) لحفظ التغييرات.

19.3.4 تعيين ملفات تعريف أمان الأبواب وأجهزة القراءة للمداخل

يوضح هذا القسم كيفية تعيين ملفات تعريف أمان الأبواب وأجهزة القراءة للأبواب وأجهزة القراءة عند مداخل معينة.
الإجراء الفرعي الأول هو تحديد وتصفية مجموعة المداخل التي تريد تعيينها، بينما يعمل الإجراء الفرعي الثاني على إنشاء التعيينات.
بالإضافة إلى ذلك، يمكنك معاينة الحالات ومستويات الأمان ومعدلات الفحص الخاصة بالمداخل المحددة على النحو الذي سيتم تعيينها به حسب مستويات التهديد المتنوعة التي حددتها.

مسار مربع الحوار

- **القائمة الرئيسية >التكوين > بيانات الجهاز**
- **مستعرض تكوين BIS > الاتصالات > بيانات الجهاز**

الشروط الأساسية

- تم تعريف مستوى تهديد واحد على الأقل.
- تم تكوين مدخل واحد على الأقل في شجرة الأجهزة.

الإجراء

1. في شجرة الأجهزة، حدد **DMS** (جذر شجرة الأجهزة)
2. في جزء مربع الحوار الرئيسي، حدد **إدارة مستوى التهديد**
   - يتلقى جزء مربع الحوار الرئيسي عدة علامات تبويب فرعية.

الإجراء الفرعي 1: تحديد مداخل لتعيينها

1. حدد علامة التبويب الفرعية **المداخل**
   - تنقسم نافذة مربع الحوار الرئيسي إلى جزأين: **شروط التصفية** وجدول بكل المداخل التي تم إنشاؤها في النظام حتى الآن.
2. (اختياري) في جزء **شروط التصفية**، أدخل معايير لتقييد مجموعة المداخل التي تظهر في الجدول في النصف السفلي من مربع الحوار، على سبيل المثال:
   - حدد أو امسح خانات الاختيار التي تحدد ما إذا كانت ستظهر في الجدول **أجهزة القراءة على الجهة الداخلية** و/أو **أجهزة القراءة على الجهة الخارجية** و/أو **الأبواب**.
   - أدخل سلاسل الأحرف التي يجب أن تظهر في أسماء المداخل أو المناطق أو أسماء ملفات التعريف أو أسماء أجهزة القراءة لكل المداخل المدرجة في الجدول.
   - حدد أو امسح خانة الاختيار التي تحدد ما إذا كانت ستظهر أيضًا في الجدول الأبواب وأجهزة القراءة التي لم يتم تكوينها بعد.
3. انقر فوق **تطبيق عامل التصفية** لتصفية قائمة المداخل أو **إعادة تعيين عامل التصفية** لإعادة عناصر التحكم في التصفية إلى قيمها الافتراضية.

الإجراء الثانوي 2: تعيين ملفات تعريف الأمان للمداخل المحددة

الشرط الأساسي: تم تحديد المداخل المراد تعيينها وتظهر في الجدول في النصف السفلي من مربع الحوار.
لاحظ أنه عادةً ما يتكون كل مدخل من باب أو حاجز بالإضافة إلى قارئ بطاقات واحد أو أكثر. ولكن قد لا يتوفر ذلك لدى بعض أنواع المداخل التخصصية، مثل **نقاط التجمع**.

1. في العمود **ملف تعريف أمان الباب أو القارئ**، انقر فوق الخلية المقابلة للباب أو القارئ الذي تريد تعيينه.
2. حدد ملف تعريف أمان باب أو قارئ من القائمة المنسدلة للخلية.

(اختياري) معاينة سلوك الأبواب وأجهزة القراءة عند مستويات التهديد
الأعمدة الموجودة بالجانب الأيسر من الجدول للقراءة فقط. وهي تظهر كيف ستكون حالة القفل (**الوضع**) و**مستوى الأمان** و**معدل الفحص** لدى الأبواب وأجهزة القراءة في الجدول إذا كان مستوى التهديد المحدد في قائمة **تحديد مستوى التهديد للحصول على تفاصيل** قيد التشغيل.
الشرط الأساسي: تم تحديد المداخل التي تريد معاينتها وتظهر في الجدول في النصف السفلي من مربع الحوار.

- ▸ من قائمة **تحديد مستوى التهديد للحصول على تفاصيل** حدد مستوى التهديد الذي تريد معاينته.
- ⇦ يعرض الجدول حالة القفل (**الوضع**) لدى الأبواب و**مستوى الأمان** و**معدلات الفحص** لدى أجهزة القراءة على النحو الذي ستكون عليه إذا كان مستوى التهديد المحدد قيد التشغيل.

19.3.5 تعيين مستوى تهديد لإشارة جهاز

يوضح هذا القسم كيفية تعيين إشارة مدخل جهاز لتشغيل تنبيه تهديد أو إلغائه.

مسار مربع الحوار
- **القائمة الرئيسية >التكوين > بيانات الجهاز**
- **مستعرض تكوين BIS > الاتصالات > بيانات الجهاز**

الشروط الأساسية
- تم تعريف مستوى تهديد واحد على الأقل.
- تم تكوين مدخل واحد على الأقل في شجرة الأجهزة.

الإجراء
1. في شجرة الأجهزة، حدد **مدخلاً** أسفل وحدة تحكم AMC التي تريد تعيين إشارات الجهاز الخاصة بها.
2. في نافذة مربع الحوار الرئيسي، حدد علامة التبويب **المحطات الطرفية**.
   - يتم عرض جدول المداخل والإشارات.
3. في صف الإشارة التي تريد تعيينها، انقر فوق خلية **إشارة المدخل**.
   - تحتوي القائمة المنسدلة على أمر **مستوى التهديد: إلغاء تنشيط** بالإضافة إلى **مستوى التهديد:** <name> لكل مستوى تهديد سبق وحددته.
   - سيعمل الأمر **مستوى التهديد: إلغاء تنشيط** على إلغاء أي مستوى تهديد قيد التشغيل حاليًا.
4. قم بتعيين الأوامر لإشارات المداخل المرغوب فيها
5. انقر فوق (حفظ) لحفظ التغييرات.

إشعار!
قيد على DM 15
يتعذر حاليًا استخدام نموذج الباب 15 (DIP/DOP) لتشغيل مستوى تهديد.

19.4 خطوات التكوين في مربعات حوار بيانات النظام

يوضح هذا القسم كيفية إنشاء **ملفات تعريف أمان أشخاص** وتعيينها إلى **أنواع أشخاص**.

19.4.1 إنشاء ملف تعريف أمان شخص

مسار مربع الحوار
- **القائمة الرئيسية > بيانات النظام > ملف تعريف أمان شخص**

– **عميل ACE > بيانات النظام > ملف تعريف أمان شخص**

الشروط الأساسية

تتطلب ملفات تعريف أمان الأشخاص التخطيط والتحديد بتأنٍّ بشكل مسبق لأنها ستكون لها تبعات مهمة بالنسبة الأداء الوظيفي للنظام في المواقف الحرجة.

الإجراء

1. إذا كان مربع الحوار يحتوي بالفعل على بيانات، فانقر فوق (جديد) لمسحها.
2. أدخل اسمًا لملف التعريف الجديد في الحقل النصي "اسم ملف تعريف الأمان":
3. (اختياري) أدخل وصفًا لملف التعريف لمساعدة المشغّلين على تعيينه بشكل صحيح.
4. أدخل عددًا صحيحًا بين 0 و100 في المربع **مستوى الأمان**.
   – بما أن حامل البطاقة مخوّل باستخدام مدخل، فإن العدد 100 كافٍ للحصول على إمكانية الوصول في أي قارئ، حتى لو كان مستوى الأمان الخاص به مُعيّن حاليًا أيضًا على 100.
   – وإلا، يجب أن يكون مستوى الأمان في ملف تعريف أمان الشخص لدى حامل البطاقة مساويًا أو أكبر من مستوى الأمان الحالي لدى القارئ.
5. أدخل عددًا صحيحًا بين 0 و100 في المربع **معدل الفحص**.
   – **ملاحظة**: معدل الفحص الخاص بملف تعريف الشخص ثانوي بالنسبة لمعدل الفحص الخاص بملف تعريف القارئ. يوضح الجدول أدناه التفاعل بين معدلي الفحص الخاصين بملفي التعريف.
6. انقر فوق (حفظ) لحفظ التغييرات.

التفاعل بين معدلي الفحص الخاصين بملفي تعريف أمان الشخص والقارئ.

معدل الفحص (%) في ملف تعريف أمان القارئ R	معدل الفحص (%) في ملف تعريف أمان الشخص P	هل تم تحديد شخص لفحوص أمان إضافية؟
0	أي	**لا**
100	أي	**نعم**
99..1	0	**لا**
99..1	100	**نعم**
99..1	99..1	**ربما** الاحتمالية = MAX(R,P)

19.4.2 تعيين ملف تعريف أمان شخص لنوع شخص

مسار مربع الحوار

– **القائمة الرئيسية > بيانات النظام > نوع الشخص**
– **عميل ACE > بيانات النظام > نوع الشخص**

الإجراء

ملاحظة: لأسباب تاريخية، **هوية الموظف** هنا مرادف **نوع الشخص**

1. في جدول **معرّفات الموظفين المحددة مسبقًا** أو جدول **معرّفات الموظفين المحددة من قبل المستخدم**، حدد الخلية الموجودة في عمود **اسم ملف تعريف الأمان** المقابلة لنوع الشخص المطلوب.
2. حدد ملف تعريف أمان شخص من القائمة المنسدلة.
   – كرّر هذا الإجراء مع جميع أنواع الأشخاص التي تتطلب ملف تعريف أمان شخص.
3. انقر فوق (حفظ) لحفظ تعييناتك

19.5 خطوات التكوين في مربعات حوار بيانات الموظفين

يوضح هذا القسم كيف تتلقى سجلات **الأشخاص** الجديدة التي يتم إنشاؤها في النظام **ملف تعريف أمان شخص** من خلال **نوع الشخص** الخاص بها.

مسارات مربعات الحوار

- **القائمة الرئيسية** > **بيانات الموظفين** > **الأشخاص**
- **القائمة الرئيسية** > **بيانات الموظفين** > **مجموعة الأشخاص**

ملاحظة: لأسباب تاريخية، **هوية الموظف** هنا مرادف **نوع الشخص**

الإجراء

يجب أن يكون لدى كل سجلات **الأشخاص** التي يتم إنشاؤها في النظام **نوع شخص**.

1. تأكد من أن مشغّلي النظام لا يعيّنون إلا **أنواع الأشخاص** التي تم ربطها مع **ملف تعريف أمان شخص** في مربع الحوار **القائمة الرئيسية** > **بيانات النظام** > **نوع الشخص**
2. للحصول على تفاصيل حول ربط **ملفات تعريف أمان الأشخاص** وإنشاء سجلات **أشخاص**، انقر فوق الارتباطات التالية.

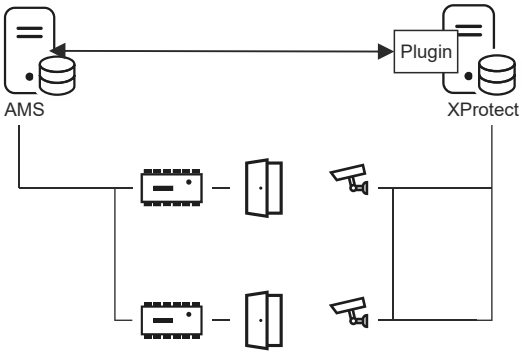
راجع

- تعيين ملف تعريف أمان شخص لنوع شخص, الصفحة *133*
- إنشاء وإدارة بيانات الموظفين, الصفحة *179*

20 تكوين Milestone XProtect لاستخدام AMS

المقدمة

يوضح هذا الفصل كيفية تكوين Milestone XProtect لاستخدام ميزات التحكم في الوصول لدى AMS.
يرسل مكوّن إضافي يوفره AMS، ولكنه مُثبّت على خادم XProtect، الأحداث والأوامر إلى AMS، ثم يرسل النتائج إلى XProtect.



يتألف التكوين من 3 مراحل توضحها الأقسام التالية:
- تثبيت شهادة AMS العامة على خادم XProtect.
- تثبيت مكوّن AMS الإضافي على خادم XProtect.
- تكوين AMS داخل تطبيق XProtect.

إشعار!

عدم التوافق المحتمل للمكونات الإضافية من مصادر مختلفة
ملحقات Milestone XProtect ليست محمية، أي أنها ليست معزولة تمامًا عن بعضها البعض. لهذا السبب، قد تحدث أخطاء في البرامج إذا قمت بتشغيل عدة مكونات إضافية بإصدارات مختلفة من NET. وتبعياتها على نفس خادم XProtect. يمكن أن تضمن BOSCH الأداء الصحيح لملحق AMS فقط إذا كان هو المكون الإضافي الوحيد المثبّت.

الشروط الأساسية

- AMS مُثبّت ومُرخّص.
- XProtect مُثبّت ومُرخّص على الكمبيوتر نفسه أو الكمبيوتر الخاص به.
- يوجد اتصال شبكة بين كلا النظامين.
- تثبيت FQDN غير مدعوم بشكل افتراضي. في حالة التثبيت في بيئة المجال، يوصى بالاتصال بمؤسسة الدعم.

تثبيت شهادة AMS العامة على خادم XProtect

لاحظ أن هذا الإجراء لا يكون مطلوبًا إلا إذا كان AMS يعمل على كمبيوتر مختلف.

1. انسخ ملف الشهادة من خادم AMS
   `C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates\Bosch Security System Internal CA - BISAMS.cer`
   إلى خادم XProtect.
2. على خادم XProtect، انقر نقرًا مزدوجًا فوق ملف الشهادة.
   وسيظهر معالج الشهادة.
3. انقر فوق **تثبيت الشهادة...**
   وسيظهر معالج استيراد الشهادة.
4. حدد **الجهاز المحلي** بوصفه **موقع المتجر** وانقر فوق **التالي**
5. حدد **وضع جميع الشهادات...**

6. انقر فوق **استعراض...**
7. حدد **الشهادات الجذر الموثوقة** وانقر فوق **موافق**
8. انقر فوق **التالي**
9. راجع ملخص الإعدادات وانقر فوق **إنهاء**

تثبيت مكوّن AMS الإضافي على خادم XProtect

1. انسخ ملف الإعداد
`AMS XProtect Plugin Setup.exe`
من وسائط تثبيت AMS المطابقة لإصدار AMS المراد توصيله بخادم XProtect.
2. نفّذ الملف على خادم XProtect.
وسيظهر معالج الإعداد.
3. في معالج الإعداد، تأكد من وضع علامة على مكوّن AMS XProtect الإضافي للتثبيت، ثم انقر فوق **التالي**.
وستظهر اتفاقية ترخيص المستخدم النهائي. انقر فوق **قبول** لقبول الاتفاقية إذا كنت تريد المتابعة.
4. يعرض المعالج مسار التثبيت الافتراضي للمكوّن الإضافي. انقر فوق **التالي** لقبول المسار الافتراضي أو **استعراض** لتغييره قبل النقر فوق **التالي**.
يؤكد المعالج أنه على وشك تثبيت مكوّن AMS XProtect الإضافي.
5. انقر فوق **تثبيت**
6. انتظر تأكيد عملية التثبيت المكتملة، ثم انقر فوق **إنهاء**.
7. أعد تشغيل خدمة Windows المسماة **Milestone XProtect Event Server**.

تكوين AMS داخل تطبيق XProtect

1. في XProtect Management Client، انتقل إلى **التحكم في الوصول**
2. انقر بزر الماوس الأيمن فوق **التحكم في الوصول** ثم حدد **إنشاء جديد...**
وسيظهر معالج المكوّن الإضافي.
3. أدخِل المعلومات التالية في معالج المكوّن الإضافي:
   - **الاسم**: وصف لتكامل AMS-XProtect هذا لتمييزه عن التكاملات الأخرى على نظام XProtect نفسه
   - **المكوّن الإضافي للتكامل**: `AMS - XProtect Plugin` (سيكون هذا الاسم متاحًا في القائمة المنسدلة بعد تثبيت المكوّن الإضافي بنجاح)
   - **نقطة نهاية اكتشاف AMS API**: `https://<hostname of the AMS server>:62904`/ مكان وجود `62904` المنفذ الافتراضي المحدد عند تثبيت AMS API.
   - **اسم المشغّل**: اسم المستخدم الخاص بمشغّل AMS والذي يملك على الأقل أذونات لتشغيل الأبواب المؤدية إلى كاميرات XProtect التي سيتم تعيينها.
   - **كلمة مرور المشغّل**: كلمة مرور AMS الخاصة بالمشغّل.
4. انقر فوق **التالي**
سيتصل مكوّن AMS الإضافي بخادم AMS الذي حددته، ثم يسرد عناصر التحكم في الوصول التي يكتشفها (الأبواب والوحدات والخوادم وأوامر الأحداث والحالات).
5. عند اكتمال شريط التقدم، انقر فوق **التالي**
ستظهر صفحة معالج **إقران الكاميرات**.
6. لإقران الكاميرات مع الأبواب، اسحب الكاميرات من قائمة **الكاميرات** إلى نقاط الوصول في قائمة **الأبواب**.
7. عند الانتهاء، انقر فوق **التالي**.
يحفظ XProtect التكوين ويرسل تأكيدًا عند نجاحه في الحفظ.

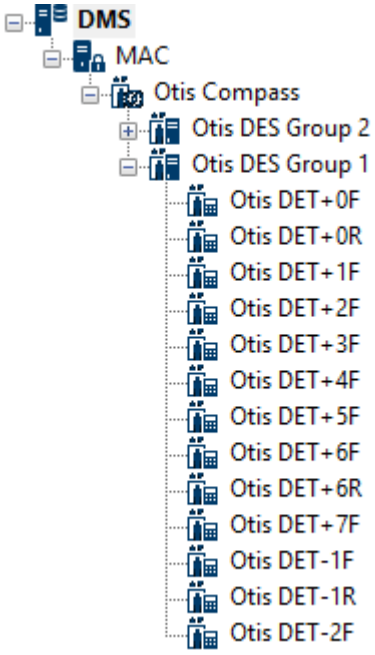
21 دمج Otis Compass

المقدمة

إن **Compass** عبارة عن نظام لإدارة الوجهات من Otis Elevator Company. يعمل هذا النظام على إدارة مجموعات متعددة من المصاعد، وإرسال المصاعد للركاب حتى يتمكنوا من الوصول إلى وجهاتهم بأكبر قدر ممكن من الكفاءة. ولتوفير البيانات الضرورية، لم يعد الركاب بحاجة إلى الضغط على الزرين **أعلى** أو **أسفل**، بل يطلبون وجهاتهم لدى قارئ البطاقات أو شاشة اللمس أو لوحة مفاتيح رقمية. يؤدي التكامل مع أنظمة التحكم في الوصول من Bosch إلى زيادة مستوى الأمان. بناءً على بيانات اعتمادهم ونماذج الوقت قيد التشغيل، يتم نقل الركاب بكفاءة إلى طوابق منازلهم والوجهات الأخرى المسموح بها. ولن يقبل النظام طلبات الطوابق غير الموجودة في ملفات تعريف التخويل الخاصة بالركاب، أو في وقت من اليوم خارج نموذج الوقت الحالي.

طبولوجيا أجهزة نظام Compass

تم تكوين أجهزة نظام Compass من الأعلى إلى الأسفل كتدرج هرمي من 3 مستويات تحت وحدة MAC واحدة في محرر الجهاز.



يعرض التدرج الهرمي أعلاه:
نظام **Otis Compass** على وحدة MAC مخصصة مجموعة مصاعد واحدة يديرها **DES** واحد عدد من المحطات الطرفية (**DET**)، لكل واحدة منها رقم طابق من -2 إلى +7، و F أو R للإشارة إلى الأبواب الأمامية أو الخلفية.

المستوى الأول: (Otis Compass)
نظام إدارة الوجهات. بإمكان كل نظام **Compass** إدارة ما يصل إلى 8 مجموعات من المصاعد.
المعلمات: مجموعة الطوابق و
عناوين الشبكة و
أرقام المنافذ والمهل الزمنية.

المستوى الثاني: (Otis DES/DER)
لغاية 8 مجموعات من المصاعد، يدير كل منها خادم إدخال الوجهة (DES) منطقي واحد يتكوّن من جهاز فعلي واحد أو جهازين فعليين.
علاوةً على ذلك، قد يتضمن هذا المستوى جهازين اختياريين كحدٍ أقصى للتحسين، يُعرفان باسم أجهزة إعادة توجيه إدخال الوجهة (DER).
المعلمات: معرف مجموعة واحدة لكل مجموعة مصاعد.
عنوان IP واحد لكل جهاز.
جدول الطوابق مع أبواب المصاعد وما إذا كانت متاحة للوصول العمومي.

المستوى الثالث: Otis DET
المحطات الطرفية لإدخال الوجهة (DET)
المعلمات: عنوان IP واحد لكل محطة طرفية.
طوابق يمكن الوصول إليها مع أبواب المصاعد لكل محطة طرفية.

نظرة عامة على التكامل في نظام التحكم في الوصول

يقوم مسؤولو نظام التحكم في الوصول بدمج Compass في المراحل التالية، التي سيتم وصفها بشكل مفصل لاحقًا في الفصل:

1. تكوين أجهزة Compass على وحدة MAC واحدة في محرر الجهاز.
2. تكوين حقول مخصصة لخصائص خاصة بـ Otis لحامل البطاقة، مثل طابق المنزل.

3. إنشاء ملفات تعريف التخويل التي تحكم الوصول إلى وجهات مصاعد معينة.
4. تعيين ملفات تعريف التخويل إلى حاملي البطاقات المناسبين
- (راجع دليل تشغيل ACE للاطلاع على هذه الإجراءات القياسية).

21.1 تكوين نظام Compass في محرر الجهاز

يصف هذا القسم الخطوات المتعلقة بتكوين نظام Otis Compass في محرر الجهاز.

مسار مربع الحوار

- **القائمة الرئيسية >التكوين > بيانات الجهاز**
- **مستعرض تكوين BIS > الاتصالات > بيانات الجهاز**

21.1.1 المستوى 1: إعداد نظام Compass

إجراء المستوى 1: إعداد نظام Compass

1. حدد وحدة MAC المطلوبة في طريقة عرض شجرة محرر الجهاز.
2. انقر بزر الماوس الأيمن وحدد **Otis Compass جديد** تتضمن صفحة الخصائص علامتي تبويب.
   - **Otis Compass**
   - **الطوابق**
3. على علامة التبويب **Otis Compass** المعلمات الأكثر أهمية التي يجب تعيينها هي
   - **الاسم** (الاسم الذي يجب أن يظهر في شجرة الأجهزة)
   - **عنوان MAC IP** (عنوان IP لرد الاتصال لنظام Compass، على بطاقة شبكة مخصصة، يتصل من خلاله نظام Compass مع MAC).
     ملاحظة: هذا **ليس** عنوان IP لوحدة MAC بحد ذاتها.
   - **القسم** (فقط إذا كانت الأقسام مرخصة ومستخدمة في عملية التثبيت)

اترك باقي المعلمات على قيمها الافتراضية ما لم يُطلب منك تغييرها بواسطة الدعم التقني المتخصص. سيتم وصفها بشكل مختصر في الجدول التالي:

المعلمة	القيمة الافتراضية	الوصف
عنوان مجموعة MC	234.46.30.7	عنوان IP لمجموعة البث المتعدد
منفذ MC لجهاز DES/DER البعيد منفذ MC لجهاز DES/DER المحلي	48307 47307	منافذ البث المتعدد
منفذ UDP لجهاز DES/DER البعيد منفذ UDP لجهاز DES/DER المحلي	46303 45303	منافذ UDP لأجهزة DES وDER
منفذ UDP لجهاز DET البعيد منفذ UDP لجهاز DET المحلي	45308 46308	منافذ UDP لأجهزة DET
مدة بقاء البث المتعدد (TTL)	5 ثوانٍ	
فاصل النبضات	ثانية واحدة	مقدار الوقت بين إشارات النبضات. تبيّن هذه الإشارات للأجهزة الأخرى أن الجهاز "حي"، أي أنه يعمل.
الحد الأقصى لعدد النبضات الفائتة	3	عدد النبضات التي يمكن تفويتها قبل اعتبار الجهاز متوقفًا عن العمل.
مهلة الرسالة	ثانية واحدة	
المحاولات الجديدة للرسالة	3	

1. على علامة تبويب **الطوابق**، انقر فوق **تغيير مجموعة الطوابق**
2. أدخل الأرقام الأدنى والأعلى للطوابق المطلوب تخديمها من قِبل مجموعات مصاعد نظام Otis Compass.
   - يتراوح النطاق الأقصى من -127 إلى +127
3. انقر فوق (حفظ) لحفظ التغييرات.

21.1.2 المستوى 2: مجموعات المصاعد، أجهزة DES وDER

إجراء المستوى 2: إعداد مجموعات المصاعد (أجهزة DES/DER)

المقدمة

إن خادم إدخال الوجهة (DES) هو الكمبيوتر الذي يدير مجموعة مصاعد. وإذا لزم الأمر، يمكن جمع جاهزي DES فعليين مع عناوين IP منفصلة في جهاز DES منطقي، مع إمكانية تجاوز الفشل.
يقوم جهاز إعادة توجيه إدخال الوجهة (DER) بتوصيل مجموعات المصاعد ويسمح لأجهزة DET عند نقطة دخول مشتركة في المبنى، على سبيل المثال الردهة، بقبول طلبات الوجهة لأي طابق في المبنى. لا يتم تكوين DER للعمل في وضع تجاوز الفشل.

إنشاء أجهزة DES في شجرة الأجهزة:

1. حدد Otis Compass المطلوب في عرض شجرة محرر الجهاز
2. انقر بزر الماوس الأيمن وحدد **Otis DES جديد** تتضمن صفحة الخصائص علامتي تبويب:
   - **Otis DES**
   - **الطوابق**
3. على علامة التبويب **Otis DES**، عيّن المعلمات التالية:
   - **الاسم**: (الاسم الذي يجب أن يظهر في شجرة الأجهزة).
     استخدم نظام تسمية منهجيًا يوفر اتجاهًا واضحًا لأدوات تكوين أجهزة DES وDET لاحقًا في عملية التكوين.
   - **الوصف:** (اختياري) وصف للجهاز عبارة عن نص حر.
   - **المجموعة:** عدد صحيح من 1 إلى 10. اجعل هذا العدد الصحيح فريدًا بين جميع مجموعات المصاعد (المعينة بواسطة أجهزة DER / DES الخاصة بها) داخل نظام Otis Compass هذا.
     لن تتمكن من حفظ تعديلات جهازك إذا كنت تستخدم رقم **المجموعة** نفسه أكثر من مرة واحدة.
   - **عنوان IP الأول:** عنوان IP لجهاز DES هذا.
   - **عنوان IP الثاني:** عند وجود توأم مكرر لجهاز DES هذا، أدخل عنوان IP الخاص به هنا.
   - **القسم** (فقط إذا كانت الأقسام مرخصة ومستخدمة في عملية التثبيت)

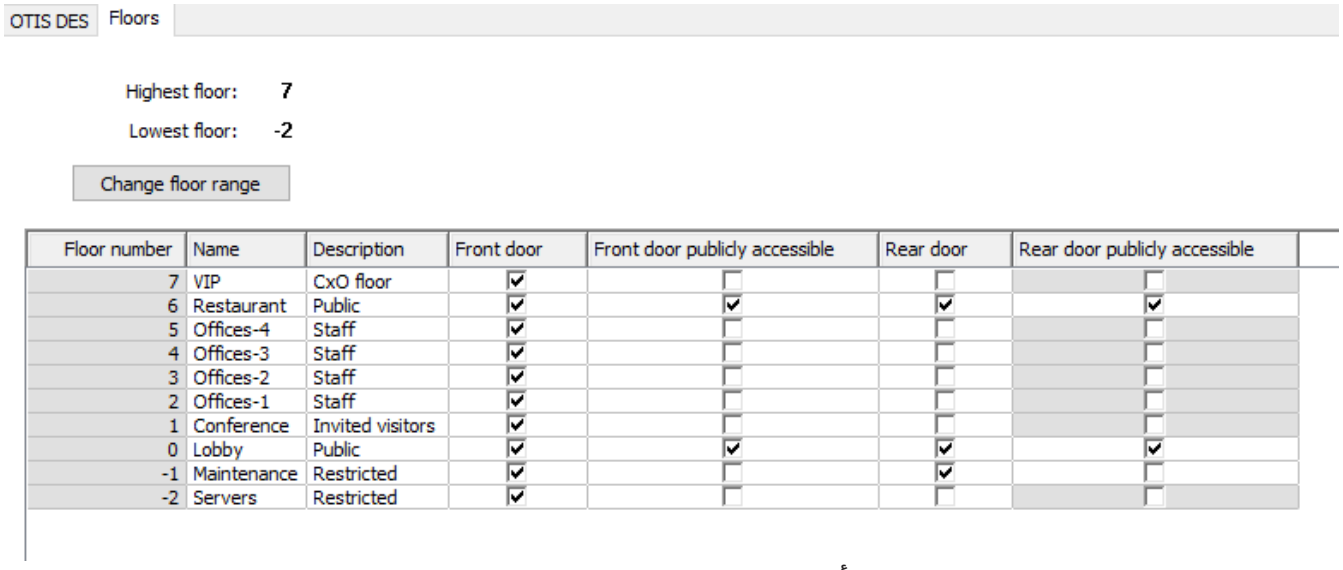
على علامة تبويب **الطوابق**، يتم تقديم الطوابق المحددة للمستوى 1 (نظام Compass) كجدول خلايا قابلة للتعديل.

إنشاء أجهزة DER في شجرة الأجهزة:

يتم إنشاء أجهزة DER تقريبًا بنفس طريقة إنشاء أجهزة DES. الفارق الوحيد هو أن DER لا يحتاج إلى جهاز تجاوز الفشل، وبالتالي لا توجد لديه معلمة **عنوان IP الثاني**.

مثال عن مجموعة مصاعد.

يبيّن المثال أدناه طوابق مجموعة مصاعد من 10 طوابق، مع أبواب أمامية وخلفية، وطوابق أرضية وطوابق سادسة متاحة للوصول العمومي.



Floor number	Name	Description	Front door	Front door publicly accessible	Rear door	Rear door publicly accessible
7	VIP	CxO floor	☑	☐	☐	☐
6	Restaurant	Public	☑	☑	☑	☑
5	Offices-4	Staff	☑	☐	☐	☐
4	Offices-3	Staff	☑	☐	☐	☐
3	Offices-2	Staff	☑	☐	☐	☐
2	Offices-1	Staff	☑	☐	☐	☐
1	Conference	Invited visitors	☑	☐	☐	☐
0	Lobby	Public	☑	☑	☑	☑
-1	Maintenance	Restricted	☑	☐	☑	☐
-2	Servers	Restricted	☑	☐	☐	☐

1. في عمود **الباب الأمامي**، حدد خانات الاختيار لجميع الطوابق التي يتيح فيها المصعد استخدام بابه الأمامي.
2. حدد خانات الاختيار بطريقة مماثلة لعمود **الباب الخلفي**، إن أمكن.
3. في عمود **الباب الأمامي المتاح للوصول العمومي**، حدد خانات الاختيار التابعة للطوابق التي يمكن لجميع ركاب المصعد الوصول إليها من دون أي قيد.
4. حدد خانات الاختيار بطريقة مماثلة لعمود **الباب الخلفي متاحة للوصول العمومي**، إن أمكن.
5. (اختياري) انقر فوق **تغيير مجموعة الطوابق** على علامة التبويب هذه لوضع المزيد من القيود على مجموعة الطوابق التي تم تعيينها على مستوى **Otis Compass**.
6. استبدل الأسماء الافتراضية في عمودي **الاسم** و**الوصف** بأسماء بديلة ذات معنىً.
7. انقر فوق (حفظ) لحفظ التغييرات.

21.1.3 المستوى 3: أجهزة DET

إجراء المستوى 3: إعداد المحطات الطرفية (أجهزة DET)

المقدمة:

يقوم جهاز DET (يُعرف أيضًا باسم DEC -- كمبيوتر إدخال الوجهة) بقراءة بيانات الاعتماد الفعلية أو رموز PIN. يمكن وضع DET في طابق معين خارج الباب الأمامي أو الخلفي للمصعد، أو داخل كابينة المصعد.

إنشاء أجهزة DET في شجرة الأجهزة:

1. حدد جهاز Otis DES/DER المطلوب في عرض شجرة محرر الجهاز.
2. انقر بزر الماوس الأيمن وحدد **محطة طرفية جديدة من Otis**
   - تظهر النافذة المنبثقة **إنشاء محطات طرفية من Otis**
3. أدخل عدد المحطات التي ترغب في تكوينها على DES/DER هذا.
4. اقبل القيم الافتراضية، أو أدخل قيم بداية جديدة للثمانية الرابعة من عنوان IP الخاص بها.
   - لأي ثمانية، ولكن للرابعة عادةً، حدد خانة الاختيار **تزايد تلقائي** إذا أردت أن يقوم النظام بتكوين عنوان IP فريد لكل محطة طرفية عن طريق زيادة الثمانية.
5. انقر فوق **موافق**.
   - يتم إنشاء العدد المطلوب من أجهزة DET في شجرة الأجهزة.
   - تتم زيادة عناوين IP الخاصة بها كما تم تحديده في الخطوة السابقة.

تكوين أجهزة DET

تتضمن صفحة الخصائص لكل جهاز DET علامتي تبويب:

- **المحطة الطرفية من Otis**
- **الطوابق**

1. على علامة تبويب **المحطة الطرفية من Otis**، عيّن المعلمات التالية:
   - **الاسم:** الاسم الذي يجب أن يظهر في شجرة الأجهزة
   - **الوصف** (اختياري) وصف للجهاز عبارة عن نص حر.
   - **عنوان IP** عنوان IP لجهاز DET هذا
   - **الوضع التشغيلي:** `1..4`

   يحدد هذا الوضع كيف تطلب المحطة الطرفية الوجهات من راكب المصعد، ثم تمرّر الطلبات إلى DES/DER للتحقق من صحتها. يقدم الجدول التالي التفاصيل:

الوضع التشغيلي	الوصف	السلوك
1	الطابق الافتراضي	(الوضع التشغيلي الافتراضي) يقدم الراكب بيانات اعتماده أو يدخل رمز PIN. إذا كانت بيانات الاعتماد صالحة أو إذا كان رمز PIN صالحًا، ولم يقم الراكب بأي إدخال إضافي، فعندئذٍ يطلب DET من DES الطابق الافتراضي أو طابق "المنزل" الخاص بالراكب. إذا أدخل الراكب طابق وجهة مختلفًا، عندئذٍ يطلب DET تلك الوجهة من DES.
2	الوصول إلى الطوابق المخوّلة	يقدم الراكب بيانات اعتماده أو يدخل رمز PIN، ثم يدخل طابق الوجهة. يطلب DET تلك الوجهة من DES. يقوم نظام التحكم في الوصول بمنح حق الوصول أو رفضه إلى الوجهة المطلوبة.
3	إدخال المستخدم لطابق الوجهة	يدخل المستخدم طابق الوجهة. إذا كانت الوجهة متاحة للوصول العمومي، عندئذٍ يطلب DET الوجهة من DES. بخلاف ذلك، يطلب DET من الراكب تقديم بيانات اعتماده للتحقق من صحتها.
4	الطابق الافتراضي أو إدخال المستخدم لطابق الوجهة.	يقدم الراكب بيانات اعتماده أو يدخل رمز PIN. إذا كانت بيانات الاعتماد صالحة أو إذا كان رمز PIN صالحًا، عندئذٍ يطلب DET من DES الطابق الافتراضي أو طابق "المنزل" الخاص بالراكب. خلال فترة المهلة المحددة، بإمكان الراكب تجاوز اختيار الطابق الافتراضي واختيار وجهة مختلفة.

   - **سجلات التدقيق:** حدد خانة الاختيار هذه لتسجيل إدخالات الركاب في هذه المحطة الطرفية لسجل الأحداث.
   - **رمز PIN:** حدد خانة الاختيار هذه للسماح باستخدام رمز PIN تعريفي على هذه المحطة الطرفية كبديل لأوراق الاعتماد الفعلية.

     ملاحظة: استخدم أجهزة القراءة للتسجيل من النوع **بطاقة PIN مربع الحوار (إدخال)** لتسجيل رموز PIN لاستخدامها في محطات Otis الطرفية.
   - **نماذج الوقت:** حدد خانة الاختيار هذه للسماح لنماذج الوقت بتقييد الأوقات التي يمكن فيها استخدام هذا المحطة الطرفية.
   - **القسم** (فقط إذا كانت الأقسام مرخصة ومستخدمة في عملية التثبيت)

على علامة تبويب **الطوابق** في صفحة خصائص **المحطة الطرفية من Otis**، يتم تقديم الطوابق المحددة للمستوى 2 (DES/DER) كجدول خلايا قابلة للتعديل.

ملاحظة: يجب أن يوفر نظام التسمية المحدد للمستوى 2 أعلاه توجيهًا كافيًا. إذا لم يكن الأمر كذلك، فإننا نوصي بحفظ عملك والعودة إلى المستوى 2 لإكمال نظام التسمية.

1. حدد كل جهاز DET قمت بإنشائه للتو بدوره في شجرة الأجهزة، وافتح علامة تبويب **الطوابق**.
   – يظهر جدول **الطوابق**
2. في عمود **الباب الأمامي**، حدد خانة الاختيار لكل طابق يمكن الوصول إليه من جهاز DET الحالي.
3. في **عمود الباب الأمامي المتاح للوصول العمومي**، حدد خانة الاختيار التابعة لكل باب أمامي متاح للوصول العمومي، من دون أي تخويل واضح.
4. (اختياري) في عمود **نموذج الوقت للباب الأمامي**، حدد نموذج وقت لتقييد الوصول العمومي إلى الباب الأمامي في ذلك الطابق، إذا لزم الأمر. على سبيل المثال، قد لا يكون الوصول إلى طابق المطعم متاحًا إلا في أوقات معينة من اليوم.
5. كرر تنفيذ الخطوات السابقة، إذا لزم الأمر، لعمود **الباب الخلفي** و **الباب الخلفي المتاح للوصول العمومي** و**نموذج الوقت للباب الخلفي.**
6. انقر فوق (حفظ) لحفظ التغييرات.

مثال:

يبيّن المثال أدناه طوابق مجموعة مصاعد من 10 طوابق، حيث يمكن الوصول إلى هذه الطوابق والأبواب من باب المصعد الأمامي في الردهة. الوصول إلى طابق المطعم مقيد بنموذج الوقت، وذلك لأبواب المصاعد الأمامية والخلفية.

OTIS terminal | Floors

Highest floor: 7

Lowest floor: -2

Change floor range

Floor number	Name	Front door	Front door publicly accessible	Time model for front door	Rear door	Rear door publicly accessible	Time model for rear door	Description
7	VIP	☑	☐		☐	☐		CxO floor
6	Restaurant	☑	☑	Mo_Fr_07-17	☑	☑	Mo_Fr_07-17	Public
5	Offices-4	☑	☐		☐	☐		Staff
4	Offices-3	☑	☐		☐	☐		Staff
3	Offices-2	☑	☐		☐	☐		Staff
2	Offices-1	☑	☐		☐	☐		Staff
1	Conference	☑	☐		☐	☐		Invited visitors
0	Lobby	☐	☐		☐	☐		Public
-1	Maintenance	☑	☐		☑	☐		Restricted
-2	Servers	☑	☐		☐	☐		Restricted

21.2 تكوين حقول مخصصة لخصائص خاصة بـ Otis لحاملي البطاقات

المقدمة

يصف هذا القسم كيفية إنشاء تلك الحقول المخصصة حيث يمكن للمشغّل إدخال خصائص Otis المحددة لحامل بطاقة، وتحديدًا "منزل" حامل البطاقة أو وجهته الافتراضية. يجب تحديد هذا "المنزل" بواسطة **ثلاث إحداثيات**:

1. مجموعة المصاعد
2. الطابق
3. الباب

لاحظ أنه عند تحديد طابق المنزل لحامل البطاقة في عميل نظام التحكم في الوصول، يجب على المشغّل إدخال البيانات بنفس الترتيب: مجموعة المصاعد، الطابق، الباب. ولهذا السبب، يجب وضع الحقول المخصصة الثلاثة بترتيب القراءة، ويفضل أن يكون من الأعلى إلى الأسفل.

انقر فوق **موافق** لتأكيد أي تذكيرات منبثقة بضرورة إنشاء الإحداثيات الثلاث كلها.

حدد الحقول المخصصة الثلاثة الضرورية، بالإضافة إلى أي خيارات Otis خاصة تحتاج إليها، لتظهر على علامة تبويب **المصاعد** من واجهة عميل التحكم في الوصول.

للحصول على معلومات عامة حول تكوين الحقول المخصصة، راجع تعليمات تكوين ACE/AMS في **الحقول المخصصة لبيانات الموظفين**.

مسار مربع الحوار
القائمة الرئيسية >**التكوين** > **خيارات** > **حقول مخصصة**
مستعرض تكوين BIS > **البنية الأساسية** > **حقول ACE مخصصة**

الإجراء
في صفحة خصائص **الحقول المخصصة**، حدد علامة تبويب **المصاعد**.

الإحداثية الأولى: مجموعة مصاعد
1. انقر نقرًا مزدوجًا في خلية على علامة التبويب، وانقر فوق **نعم** لإنشاء حقل إدخال جديد.
2. من القائمة **نوع الحقل**، حدد **تحديد Otis DES**.
3. في حقل **التسمية**، أدخل `Elevator Group`
4. من قائمة **عرض في**، حدد `Tab:Elevators`
5. في مجموعة **الموضع**، حدد موقعًا فريدًا على علامة تبويب **المصاعد**، حيث يجب أن يظهر هذا الحقل المخصص.

الإحداثية الثانية: طابق المنزل
1. انقر فوق **حقل جديد**، لإنشاء حقول مخصصة جديدة
2. من القائمة **نوع الحقل**، حدد **طابق المنزل**.
3. في حقل **التسمية**، أدخل `Home floor`
4. من قائمة **عرض في**، حدد `Tab:Elevators`
5. في مجموعة **الموضع**، حدد موقعًا فريدًا على علامة تبويب **المصاعد**، حيث يجب أن يظهر هذا الحقل المخصص. لتسهيل الاستخدام من قبل مشغّلي النظام، يجب أن يكون تحت الإحداثية السابقة.

الإحداثية الثالثة: باب الخروج
1. انقر فوق **حقل جديد**، لإنشاء حقول مخصصة جديدة
2. من القائمة **نوع الحقل**، حدد **باب الخروج**.
3. في حقل **التسمية**، أدخل `Exit door`
4. من قائمة **عرض في**، حدد `Tab:Elevators`
5. في مجموعة **الموضع**، حدد موقعًا فريدًا على علامة تبويب **المصاعد**، حيث يجب أن يظهر هذا الحقل المخصص. لتسهيل الاستخدام من قبل مشغّلي النظام، يجب أن يكون تحت الإحداثية السابقة.

خيارات Otis خاصة لحاملي البطاقات

المقدمة
تتوفر ثمانية خيارات ثنائية خاصة بـ Otis وفقًا لوظائف Otis القياسية. إذا تم تحديد هذه الخيارات كحقول مخصصة على علامة تبويب **المصاعد**، فستظهر كخانات اختيار على علامة تبويب **بيانات المصعد** لحاملي البطاقات في مربع الحوار **الأشخاص** (القائمة الرئيسية > **بيانات الموظفين** > **الأشخاص**). عندئذٍ يمكن تحديدها وإلغاء تحديدها بواسطة مشغّلي نظام التحكم في الوصول.
كوّن هذه الخيارات فقط وفقًا لإرشادات مندوب Otis.

الإجراء
1. انقر فوق **حقل جديد**، لإنشاء حقول مخصصة جديدة
2. من القائمة **نوع الحقل**، حدد **خيارات Otis**.
3. في حقل **التسمية**، أدخل تسميتك الخاصة، على سبيل المثال `Otis flag 1` أو وفقًا لوثائق Otis.
4. من قائمة **عرض في**، حدد `Tab:Elevators`
5. من قائمة **نوع الوظيفة**، حدد أحد الخيارات من `OTIS option 1` إلى `OTIS option 8`
6. في مجموعة **الموضع**، حدد موقعًا فريدًا على علامة تبويب **المصاعد**، حيث يجب أن تظهر خانة الاختيار هذه.
7. انقر فوق (حفظ) لحفظ التغييرات.

21.3 إنشاء تخويلات وتكوينها لمصاعد Otis

المقدمة

يصف هذا القسم كيفية تضمين حقوق الوصول لمجموعات مصاعد Otis والطوابق وأبواب المصاعد في **تخويل**.

يتم تعيين **التخويلات** إلى حاملي البطاقات مباشرةً، أو بطريقة أكثر شيوعًا، عند جمعها مع تخويلات أخرى في **ملفات تعريف الوصول**، التي يتم عندئذٍ تعيينها إلى حاملي البطاقات.

الشروط الأساسية

تم تحديد نظام Otis Compass على وحدة MAC في محرر الجهاز. إنه مكتمل مع مجموعة مصاعد (ممثلة بجهاز DES الخاص بها) وأزواج طابق+باب (ممثلة بأجهزة DET الخاصة بها).

مسار مربع الحوار

القائمة الرئيسية > **بيانات النظام** > **التخويلات**

الإجراء

1. في حقل **اسم التخويل**، أدخل اسم تخويل موجود، أو انقر فوق (جديد) لإنشاء تخويل جديد.
2. في قائمة **MAC**، حدد اسم MAC الذي تم إنشاء نظام Otis Compass بالاستناد إليه.
3. انقر فوق علامة التبويب **مصعد Otis**
4. في قائمة **مصاعد Otis** حدد DES/DER لمجموعة المصاعد التي ترغب في إضافتها إلى التخويل (لاحظ أنه بإمكان التخويل أن يحتوي على DES/DER واحد فقط).
   - تظهر طواق مجموعة المصاعد المحددة في جزء **الطوابق**.
5. في العمودين **الباب الأمامي** و**الباب الخلفي** في جزء **الطوابق**، حدد الأبواب في تلك الطوابق التي يجب تضمينها في هذا التخويل.
   - لاحظ أن هذه الأبواب والطوابق التي **لم** يتم تحديدها لمجموعة المصاعد هذه، عندما تم تحديدها في محرر الجهاز، ستكون رمادية اللون ولن تكون قابلة للتحديد في مربع الحوار هذا.
6. أو، انقر فوق الزرين **تعيين كل الطوابق** و**إزالة كل الطوابق** لتحديد جميع الطوابق والأبواب أو إلغاء تحديدها مرة واحدة.
7. انقر فوق (**حفظ**) لحفظ التخويل.

22 تكوين IDEMIA Universal BioBridge

يصف هذا القسم تكوين الأجهزة البيومترية IDEMIA للعمل مع أنظمة التحكم في الوصول من Bosch من خلال **MorphoManager** و**BioBridge**.

تتناول هذه الأقسام الفرعية مهام التكوين الضرورية في المجالات التالية:

- نظام التحكم في الوصول من Bosch
- MorphoManager
- عميل التسجيل BioBridge في MorphoManager
- عمليات التكييف لتقنيات وتنسيقات بطاقات مختلفة

22.1 إعداد BioBridge في نظام التحكم في الوصول من Bosch

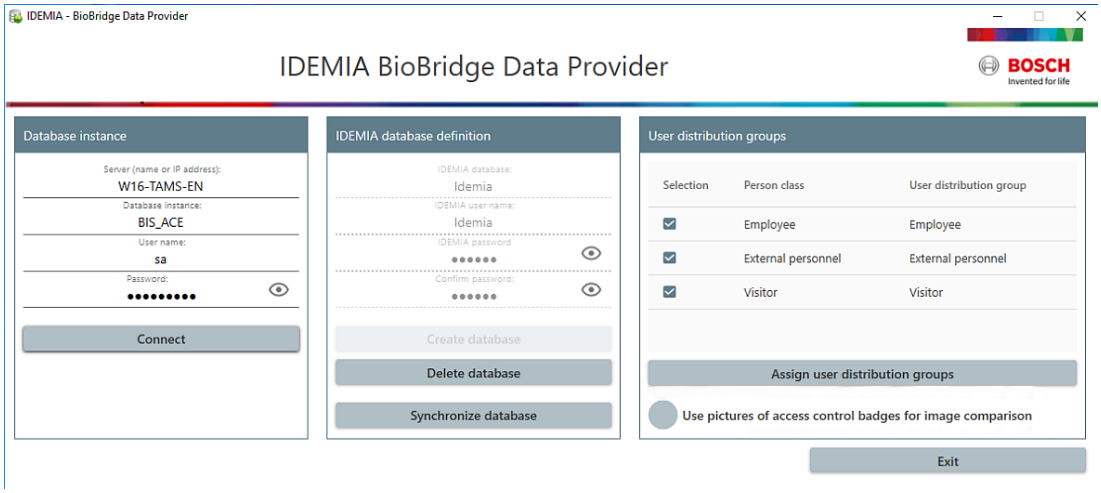
يتم تنفيذ الخطوات التالية في ACS لإنشاء قاعدة البيانات التي تربط الأجهزة البيومترية IDEMIA بنظام التحكم في الوصول من Bosch. تقوم قاعدة البيانات بتعيين كيانات قاعدة البيانات التالية إلى بعضها البعض:

- **فئة شخص** (Bosch) بالإضافة إلى
- **مجموعة توزيع المستخدمين** (IDEMIA).

مسار مربع الحوار

- مستعرض تكوين BIS > **الأدوات** > **قاعدة بيانات IDEMIA لتكوين ACE**
- القائمة الرئيسية AMS > **التكوين** > **الأدوات** > **تكوين قاعدة بيانات IDEMIA**

1. انقر فوق **تكوين قاعدة بيانات IDEMIA**
يظهر مربع الحوار **موفر بيانات IDEMIA BioBridge**.



2. في جزء **مثيل قاعدة البيانات**، أدخل المعلومات التالية:

- **الخادم**: اسم المضيف أو عنوان IP للكمبيوتر حيث يتم تشغيل مثيل قاعدة بيانات SQL Server لـ ACS. قد يكون هذا اسم المضيف المحلي، إذا كان تشغيل SQL Server يتم محليًا.
- **مثيل قاعدة البيانات**: مثيل قاعدة بيانات ACS (الافتراضي: `ACE`).
- **اسم المستخدم**: اسم حساب مسؤول مثيل قاعدة البيانات ACS (الافتراضي: `sa`)
- **كلمة المرور**: كلمة مرور حساب المسؤول، كما تم تكوينها أثناء تثبيت ACS.

3. انقر فوق **اتصال** لاختبار الاتصال. يتم تعطيل جميع عناصر التحكم الأخرى حتى تقوم بذلك.

في جزء تعريف قاعدة بيانات IDEMIA

أول حقلين هما للقراءة فقط:

- **قاعدة بيانات Idemia**: اسم قاعدة البيانات التي تجمع بيانات Bosch وIDEMIA.
- **اسم مستخدم Idemia**: اسم مستخدم قاعدة البيانات الذي ينفذ البرنامج باسمه الأوامر في قاعدة البيانات.

1. أدخل كلمة مرور **اسم مستخدم Idemia** قوية وأكدها.
2. دوّن كلمة المرور بتأنٍ. ستحتاج إليها في مهام التكوين المستقبلية، وسيتعذر استردادها في حال فقدانها.
3. انقر فوق **إنشاء قاعدة بيانات**.
سيؤكد مربع الرسالة ما إذا كانت عملية الإنشاء ناجحة. انقر فوق **موافق**
4. عند إكمال الاختبارات بنجاح، انقر فوق **خروج** لإغلاق مربع الحوار.

في جزء مجموعات توزيع المستخدمين

إن مجموعات توزيع المستخدمين عبارة عن كائنات MorphoManager تقوم بتعيين المستخدمين (حاملي بيانات الاعتماد) إلى مجموعات من أجهزة القراءة البيومترية أو عملاء MorphoManager. نحن نعيّنها إلى **فئات الشخص** في أنظمة التحكم في الوصول من Bosch.

1. في العمود "تحديد"، حدد خانة الاختيار لكل ACE **فئة شخص** تستخدمها عملية التثبيت.
2. لكل سطر قمت بتحديده، انسخ اسم فئة الشخص هذه إلى الخلية المقابلة في عمود **مجموعة توزيع المستخدمين**.
– لاحظ أن أسماء **فئة الشخص** و**مجموعة توزيع المستخدمين** يجب أن تتطابق تمامًا.
3. عند اكتمال التعيين، انقر فوق **تعيين مجموعات توزيع المستخدمين**.

توفير صور بطاقة الهوية للتعرف على الوجوه من VisionPass

للسماح لأجهزة قراءة IDEMIA بتنفيذ التعرف على الوجوه من VisionPass باستخدام صور بطاقات هوية حاملي البطاقات من قاعدة بيانات ACE:

- انقر فوق **استخدم صور شارات التحكم في الوصول لمقارنة الصور** وقم بالتأكيد في النافذة المنبثقة.
تؤكد نافذة **موفر بيانات IDEMIA BioBridge** أن عملية المزامنة قيد التقدم.
لاحظ أنه بناءً على كمية بيانات الصور المعنية، قد يستغرق النقل وقتًا طويلاً.

22.2 اختيار تقنيات وتنسيقات البطاقات

المقدمة

إذا كنت تخطط لاستخدام البطاقات بالإضافة إلى الهوية البيومترية، فعليك إنشاء ملف تعريف (أو "ملف تعريف Wiegand") في MorphoManager يتضمن تنسيق (أو تنسيقات) بطاقات الوصول هذه.
يقدم الجدول التالي نظرة عامة على التنسيقات المدعومة. بالنسبة إلى تقنية MIFARE، تعريف CSN فقط مدعوم.

Card Family	HID Prox	HID Class	HID iClass Seos	MIFARE Classic	MIFARE DESFire EV0	MIFARE DESFire EV1
Card Variant	Prox	2k/2 16k/2 16k/16 32k(16k/2+16k/1) 32k(16k/16+16k/1)	Seos	1K 4-byte NUID 1k 7-byte UID 4k 4-byte NUID 4k 7byte UID	2k 4k 8k	2k 4k 8k

الشكل التوضيحي 22.1: بطاقات IDEMIA المدعومة

الإجراء العام

1. في MorphoManager، انتقل إلى **الإدارة** > **ملف تعريف Wiegand**
2. انقر فوق **إضافة** لإنشاء ملف تعريف Wiegand مخصص
3. في مربعات الحوار ذات الصلة، أدخل معلومات التنسيق وتقنية البطاقة التي يستخدمها النظام.
4. لاستخدام ملف تعريف Wiegand الذي تم تحديده مؤخرًا في النظام، أدخل اسمه في حقل **ملف تعريف Wiegand** في مربعات حوار MorphoManager التالية:
– **الإدارة > ملف تعريف الجهاز البيومتري**
– **الإدارة > سياسة المستخدم**

Mifare Classic CSN

1. أضف عنصر `User CSN Element` Wiegand وأدخل التفاصيل التالية
   - **الاسم**: `CSN` (على سبيل المثال)
   - **الطول** `32`
   - **وضع التحويل:** `Reversed`
2. **ضمن الإدارة > ملف تعريف الجهاز البيومتري**، في صفحة **إعدادات الوضع متعدد العوامل**، حدد خانة الاختيار **MIFARE Classic**

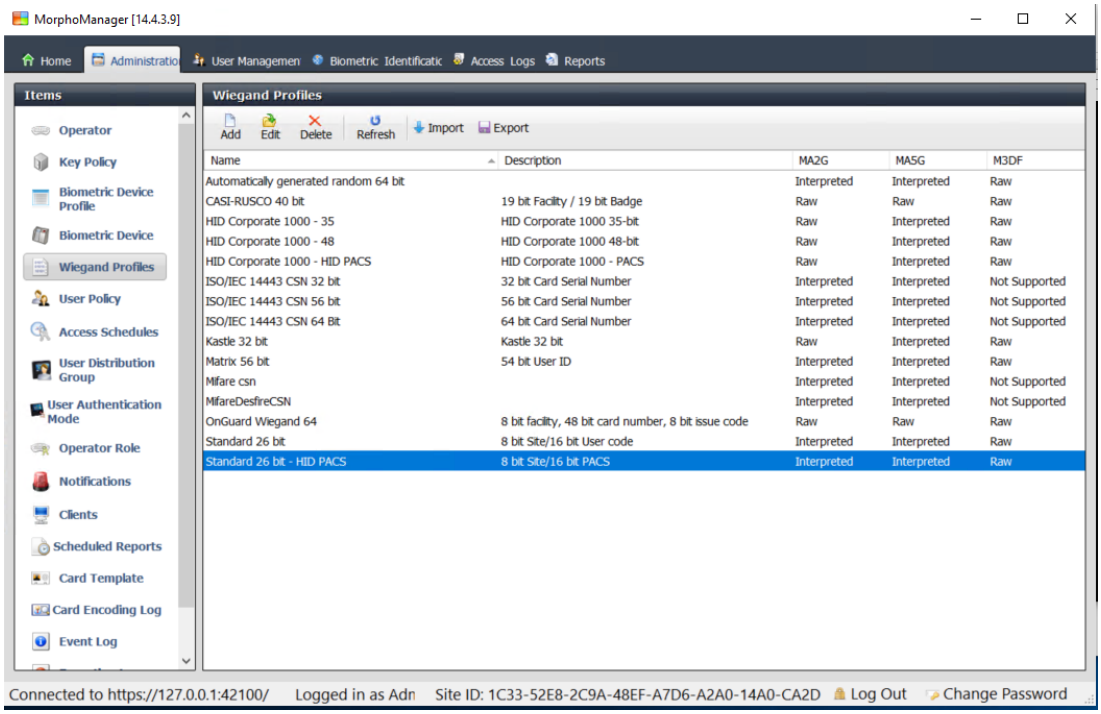
Mifare DESFire CSN

التكوين مماثل لتكوين Mifare Classic باستثناء التفاصيل التالية:

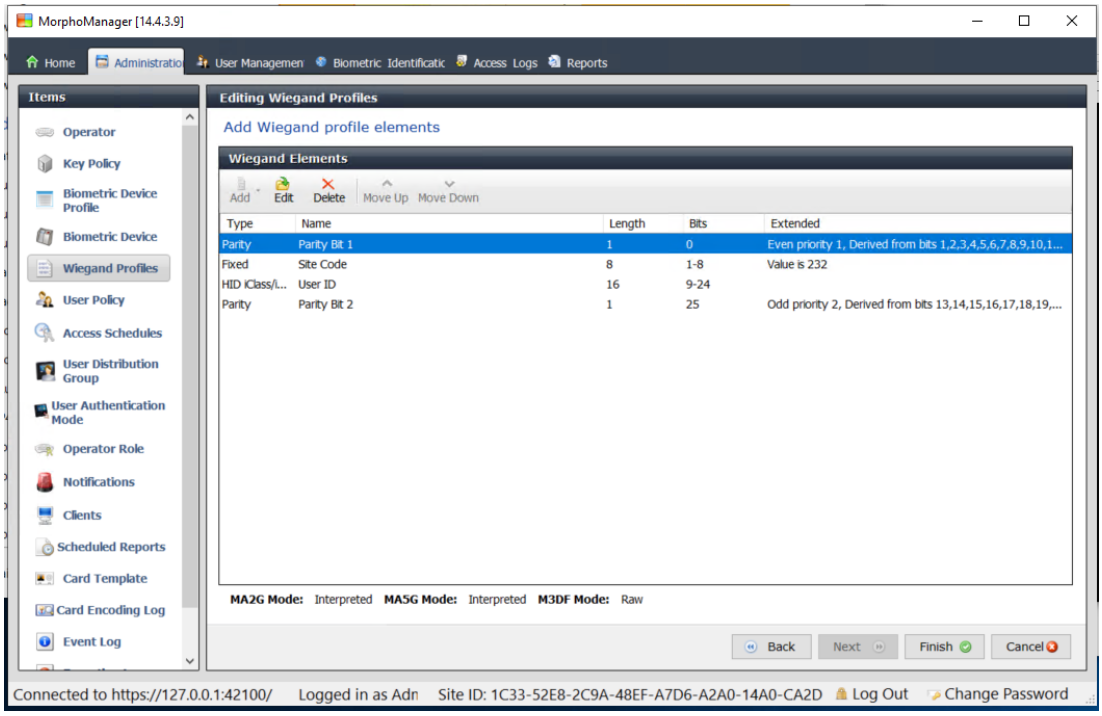
- **الطول:** `56`
- أضف **عنصر CSN لمستخدم عنصر Wiegand**
  - أدخل اسمًا ضمن **الاسم:**
  - في **الطول** أدخل 56
  - في **وضع التحويل:** أدخل `Reversed`
- **ضمن الإدارة > ملف تعريف الجهاز البيومتري**، في صفحة **إعدادات الوضع متعدد العوامل**، حدد خانة الاختيار **Mifare DESFire 3DES**

iClass 26 BIT

1. حدد ملف التعريف المحدد مسبقًا `Standard 26 bit-HID PACS`



2. انقر فوق **تحرير**
3. انقر فوق **التالي**



4. انقر فوق **تحرير**
5. احذف السطر `Fixed Facility Code`
6. حدد السطر `HID iClass SEP User ID`
7. انقر فوق **تحرير**
8. غيّر طول معرف المستخدم من `1..16` إلى `1..24`
9. **ضمن الإدارة > ملف تعريف الجهاز البيومتري**، في صفحة إعدادات الجهاز البيومتري، لملف تعريف Wiegand، حدد `Standard 26 BIT-HID-PACS`
10. **ضمن الإدارة > ملف تعريف الجهاز البيومتري**، في صفحة **إعدادات الوضع متعدد العوامل**، حدد خانة الاختيار `HID iClass`
11. انقر فوق التالي حتى تصل إلى صفحة **المعلمات المخصصة**
12. انقر فوق **إضافة**
13. أضف معلمة مخصصة (حساسة لحالة الأحرف) `wiegand.site_code_propagation`
14. عيّن قيمتها إلى `1`
15. انقر فوق **إنهاء**.
16. أدخل ملف تعريف Wiegand المكتمل هذا ضمن **الإدارة > سياسة المستخدم**

iClass 35 BIT

1. حدد ملف التعريف المحدد مسبقًا `HID Corporate 1000 35 BIT`
2. انقر فوق **تحرير**
3. انقر فوق **التالي**
4. حدد سطر العنصر `Fixed Company ID` واحذفه
5. حدد سطر العنصر `User Card ID Number` واحذفه
6. أضف سطر العنصر `HID iClass/iClass SE PACS Data` وفي تفاصيل العنصر الخاصة به، عيّن ما يلي:
   - الاسم: `Card ID Number`
   - الطول: `32`
   - **ضمن الإدارة > ملف تعريف الجهاز البيومتري**، في صفحة **إعدادات الوضع متعدد العوامل**، حدد خانة الاختيار `HID iClass`
   - انقر فوق **التالي** حتى تصل إلى صفحة **المعلمات المخصصة**
   - انقر فوق **إضافة**

- أضف معلمة مخصصة (حساسة لحالة الأحرف) wiegand.site_code_propagation
- عيّن قيمتها إلى 1
- انقر فوق **إنهاء**.
- أدخل ملف تعريف Wiegand المكتمل هذا ضمن **الإدارة > سياسة المستخدم**

iClass 37 BIT

- **الإدارة > ملف تعريف Wiegand**
- انقر فوق **إضافة ملف تعريف جديد**
- **الطول** 37

1. إضافة بت التماثل:
- **الاسم**: (على سبيل المثال) EvenParityBit 1
- **الأولوية**: 1
- **الطول**: 18
- **الوضع**: Even
- **بت الأساس**: 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18
- انقر فوق **التالي**

2. أضف العنصر User HID iClass/iClass SE PACS Data وفي تفاصيل العنصر، عيّن ما يلي:
- **الاسم:** UserID
- **الطول**: 35
- انقر فوق **التالي**

3. إضافة بت التماثل:
- **الاسم**: (على سبيل المثال): Parity Bits 2
- **الأولوية**: 2
- **الطول**: 19
- **الوضع**: Odd
- **بت الأساس**: 19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37
- انقر فوق **التالي**
- **ضمن الإدارة > ملف تعريف الجهاز البيومتري**، في صفحة **إعدادات الوضع متعدد العوامل**، حدد خانة الاختيار HID iClass
- انقر فوق **التالي** حتى تصل إلى صفحة **المعلمات المخصصة**
- انقر فوق **إضافة**
- أضف معلمة مخصصة (حساسة لحالة الأحرف) wiegand.site_code_propagation
- عيّن قيمتها إلى 1
- انقر فوق **إنهاء**.
- أدخل ملف تعريف Wiegand المكتمل هذا ضمن **الإدارة > سياسة المستخدم**

iClass 48BIT

1. حدد ملف التعريف المحدد مسبقًا HID Corporate 1000 48 BIT
2. انقر فوق **تحرير**
3. انقر فوق **التالي**
4. حدد سطر العنصر Fixed Company ID واحذفه
5. حدد سطر العنصر User Card ID Number واحذفه
6. أضف سطر العنصر HID iClass/iClass SE PACS Data وفي تفاصيل العنصر الخاصة به، عيّن ما يلي:
- الاسم: User
- الطول: 45
7. **ضمن الإدارة > ملف تعريف الجهاز البيومتري**، في صفحة **إعدادات الوضع متعدد العوامل**، حدد خانة الاختيار HID iClass

8. انقر فوق **التالي** حتى تصل إلى صفحة **المعلمات المخصصة**
9. انقر فوق **إضافة**
10. أضف معلمة مخصصة (حساسة لحالة الأحرف) `wiegand.site_code_propagation`
   - عيّن قيمتها إلى `1`
11. انقر فوق **إنهاء**.
12. أدخل ملف تعريف Wiegand المكتمل هذا ضمن **الإدارة** > **سياسة المستخدم**

HID Prox

1. حدد ملف التعريف المحدد مسبقًا `Standard 26 BIT`
2. انقر فوق **تحرير**
3. انقر فوق **التالي**
4. احذف السطر `Fixed Facility Code`
5. انقر فوق **تحرير**
6. غيّر طول معرف المستخدم من `1..16` إلى `1..24`
7. **ضمن الإدارة > ملف تعريف الجهاز البيومتري**، في صفحة إعدادات الجهاز البيومتري، لملف تعريف Wiegand، حدد `Standard 26 BIT`
8. **ضمن الإدارة > ملف تعريف الجهاز البيومتري**، في صفحة **إعدادات الوضع متعدد العوامل**، حدد خانات الاختيار:
   - **بيومتري**
   - **بطاقة القرب**
9. انقر فوق **التالي** حتى تصل إلى صفحة **المعلمات المخصصة**
10. انقر فوق **إضافة**
11. أضف معلمة مخصصة (حساسة لحالة الأحرف) `wiegand.site_code_propagation`
   - عيّن قيمتها إلى `1`
12. انقر فوق **إنهاء**.
13. أدخل ملف تعريف Wiegand المكتمل هذا ضمن **الإدارة** > **سياسة المستخدم**

22.3 اختيار وضع التعريف

المقدمة

يمكن لأجهزة القراءة البيومترية تحديد حاملي بيانات الاعتماد بطرق مختلفة. تُعرف هذه الطرق باسم أوضاع التعريف أو أوضاع المصادقة.

- بواسطة وضع التعريف **بطاقة أو بيانات بيومترية**، بحسب ما يقدمه حامل بيانات الاعتماد إلى القارئ
- بواسطة وضع التعريف **بطاقة وبيانات بيومترية**، أي يجب على المستخدم التأكد من أنه المالك الحقيقي للبطاقة من خلال بيانات الاعتماد البيومترية.
- بواسطة وضع التعريف **بيانات بيومترية فقط**

يوضح هذا القسم كيفية تكوين هذه الأوضاع في MorphoManager.

عندما يتعلق الأمر ببيانات اعتماد البطاقة، من الضروري بطبيعة الحال إنشاء ملف تعريف لتقنية البطاقة وتنسيقها المناسبين.

مسار مربع الحوار

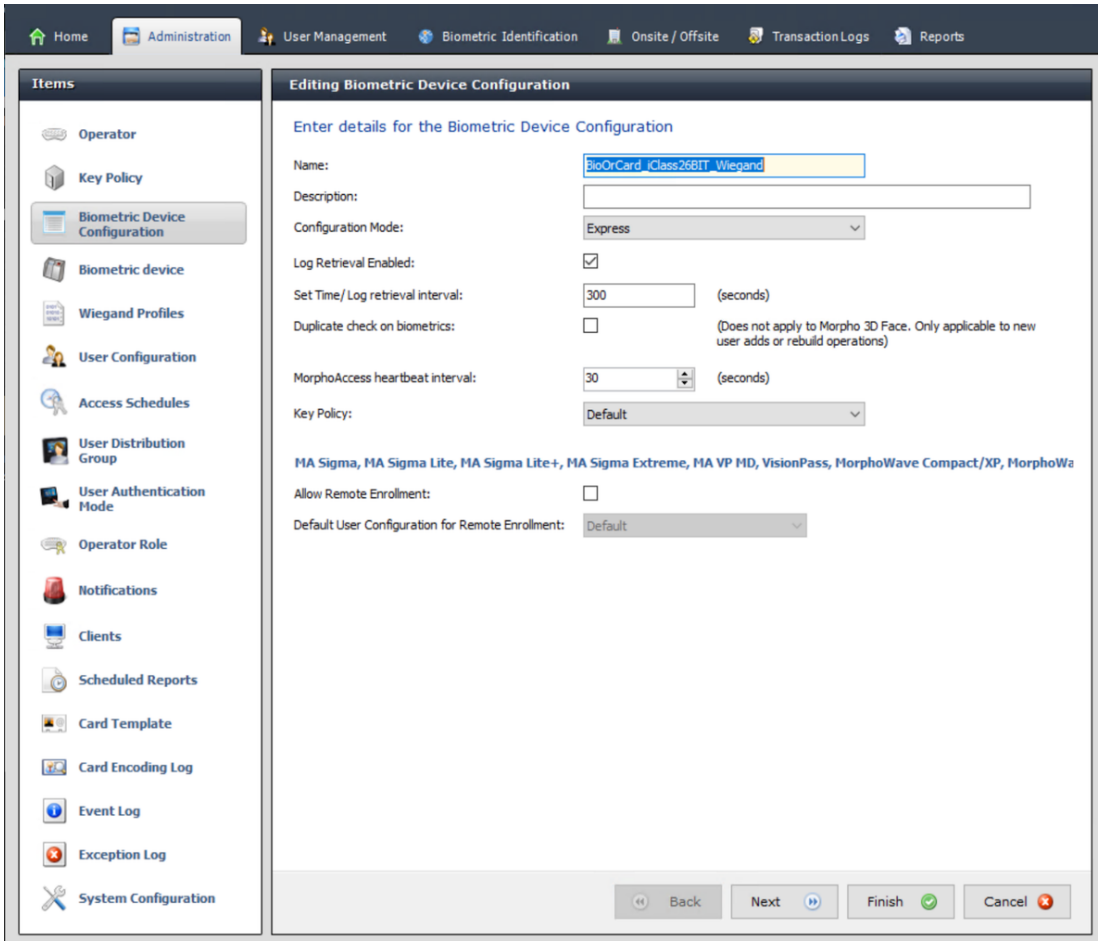
في علامة التبويب **الإدارة** في MorphoManager

22.3.1 بطاقة أو بيانات بيومترية

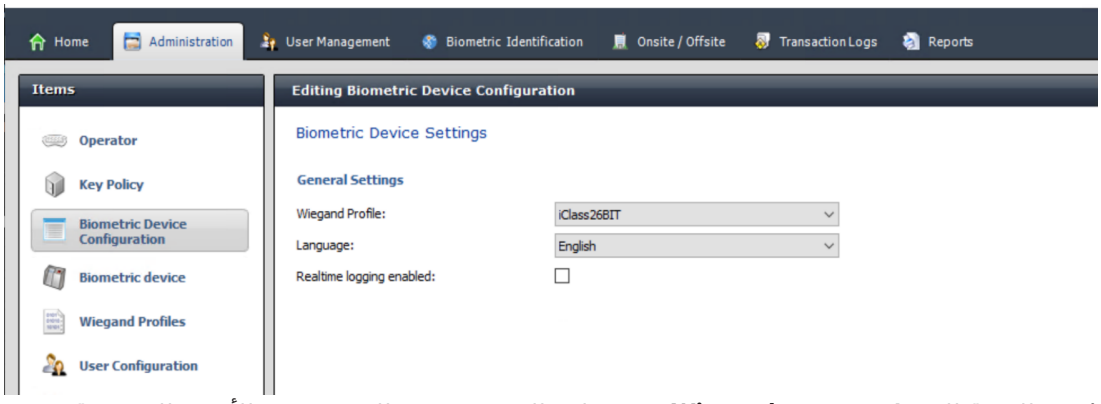
قم بإنشاء وضع المصادقة المخصص هذا إذا أراد المستخدمون تعريف أنفسهم إما بالبطاقة أو عن طريق بيانات الاعتماد البيومترية.

1. في MorphoManager، انتقل إلى **الإدارة** > **بيومتري تكوين الجهاز**

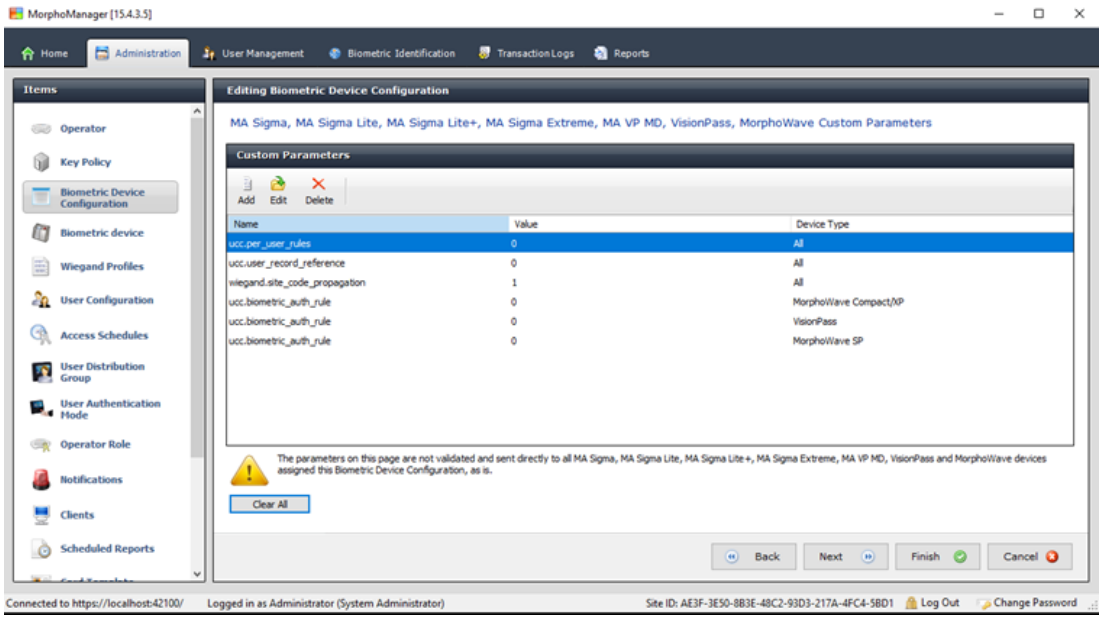
2. أدخل اسمًا لتكوين الجهاز البيومتري هذا، على سبيل المثال `CardORBiometric`



3. انقر فوق **التالي** حتى تصل إلى الصفحة المعنونة **إعدادات الجهاز البيومتري**



4. بالنسبة إلى **ملف تعريف Wiegand**، حدد ملف التعريف نفسه الذي حددته للأجهزة البيومترية عند إعداد BioBridge.
5. انقر فوق **التالي** حتى تصل إلى مربع الحوار **إعدادات الحد البيومتري**.
6. قم بتعيين قيم **الحد البيومتري** وفقًا لظروفك المحلية ووثائق MorphoManager. القيمة الافتراضية هي `Recommended`
7. انقر فوق **التالي** حتى تصل إلى شاشة **إعدادات الوضع متعدد العوامل**.
8. حدد خانة الاختيار **بيومتري**، بالإضافة إلى خانة اختيار تقنية البطاقة التي تستخدمها عملية التثبيت.
9. انقر فوق **التالي** حتى تصل إلى صفحة **المعلمات المخصصة**



10. لكل جهاز تستخدمه:
انقر فوق **إضافة** لإضافة معلمتين مخصصتين.
(إذا تم تعيين هاتين المعلمتين، فسيرسل القارئ بيانات البطاقة مباشرة إلى AMC. من غير الضروري أن يكون المستخدم مسجلاً على قارئ IDEMIA)
   - `ucc.per_user_rules`
   - `ucc.user_record_reference`
11. بالنسبة لجهازي القراءة WAVE وVisionPass، أضف معلمة أخرى:
   - `ucc.biometric_auth_rule=0`
   - في هذه الحالة، حدد لـ **نوع الجهاز** `MorphoWave Compact/XP` أو `MorphoWave SP` أو `VisionPass`
12. انقر فوق **إنهاء**

تعيين وضع مصادقة المستخدم هذا للمستخدمين

في ACS، يجب عليك تعيين بطاقة بها تعريف بطاقة صالح لكل حامل بطاقة.

1. في MorphoManager، انتقل إلى **الإدارة** > **وضع مصادقة المستخدم**.
2. قم بتعيين السمات التالية:
   - قم بتعيين **الوضع** إلى `Enabled`
   - قم بتعيين القائمة **موقع النموذج** إلى `Download to Device`
   - حدد خانة الاختيار **السماح بالبدء بواسطة البيانات البيومترية**
   - حدد خانة الاختيار **السماح بالبدء بواسطة البطاقة من دون تلامس**
   - تعطيل **طلب مطابقة القالب**
3. انتقل إلى **الادارة** > **تكوين المستخدم**
4. انقر فوق **إضافة**
5. بالنسبة **لوضع مصادقة المستخدم**، حدد اسم الوضع الذي قمت بإنشائه أعلاه للبطاقة أو البيانات البيومترية.
6. انقر فوق **إنهاء**

راجع

- اختيار تقنيات وتنسيقات البطاقات, الصفحة *146*

22.3.2 بطاقة وبيانات بيومترية

عيّن الإعدادات التالية إذا كان يجب على المستخدم استخدام بطاقة وبيانات اعتماد بيومترية للتأكد من أنه المالك الحقيقي للبطاقة.

1. في MorphoManager، انتقل إلى **الإدارة** > **بيومتري تكوين الجهاز**
2. انقر فوق **التالي** حتى تصل إلى الصفحة المعنونة **إعدادات الجهاز البيومتري**
3. بالنسبة إلى **ملف تعريف Wiegand**، حدد ملف التعريف نفسه الذي حددته للأجهزة البيومترية عند إعداد BioBridge.
4. انقر فوق **التالي** حتى تصل إلى الصفحة المعنونة **إعدادات الوضع متعدد العوامل**
5. حدد خانة الاختيار لتقنية البطاقة التي تستخدمها عملية التثبيت.
6. انقر فوق **إنهاء**

تعيين وضع مصادقة المستخدم هذا للمستخدمين

في ACS، يجب عليك تعيين بطاقة بها تعريف بطاقة صالح لكل حامل بطاقة.

1. في MorphoManager، انتقل إلى **الإدارة** > **تكوين المستخدم**
2. بالنسبة إلى **وضع مصادقة المستخدم** حدد `Contactless Card ID + Biometric` من القائمة.
3. انقر فوق **إنهاء**.

راجع

- اختيار تقنيات وتنسيقات البطاقات, الصفحة *146*

22.3.3 بيانات بيومترية فقط

عيّن الإعدادات التالية إذا كان يتعين على المستخدمين التعريف عن أنفسهم بواسطة بيانات الاعتماد البيومترية فقط.

1. في MorphoManager، انتقل إلى **الإدارة** > **بيومتري تكوين الجهاز**
2. انقر فوق **التالي** حتى تصل إلى الصفحة المعنونة **تحرير تكوين الجهاز البيومتري**
3. بالنسبة إلى **ملف تعريف Wiegand**، حدد ملف التعريف نفسه الذي حددته للأجهزة البيومترية عند إعداد BioBridge
4. انقر فوق **التالي** حتى تصل إلى الصفحة المعنونة **إعدادات الوضع متعدد العوامل**
5. بالنسبة إلى **الوضع متعدد العوامل**، حدد `Biometric only` من القائمة
6. انقر فوق **إنهاء**

تعيين وضع مصادقة المستخدم هذا للمستخدمين

في ACS، يجب عليك تعيين بطاقة بها تعريف بطاقة صالح لكل حامل بطاقة.

1. في MorphoManager، انتقل إلى **الإدارة** > **تكوين المستخدم**
2. بالنسبة إلى **وضع مصادقة المستخدم** حدد `Biometric(1:many)` من القائمة.
3. انقر فوق **إنهاء**.

22.4 إعداد BioBridge في MorphoManager

الشروط الأساسية

تم تثبيت MorphoManager على خادم MorphoManager في شبكتك. راجع الدليل الخاص بتثبيت MorphoManager والمساعدة عبر الإنترنت.

نظرة عامة

لاستخدام واجهة BioBridge بين أنظمة التحكم في الوصول من Bosch وMorphomanager، تحتاج إلى تكوين ما يلي في MorphoManager:

- **تكوين الأجهزة البيومترية**
- **الجهاز البيومتري**

- **ملفات تعريف Wiegand**
- **تكوين المستخدم**
- **مجموعة توزيع المستخدمين**
- **وضع مصادقة المستخدم**
- **تكوين النظام**

بالإضافة إلى ذلك، يجب إعداد اتصال قاعدة البيانات المفتوح (ODBC) للاتصال بين Morphomanager وقاعدة البيانات BioBridge التي يشاركها مع ACS.
تم وصف جميع مهام التكوين هذه في الأقسام التالية.

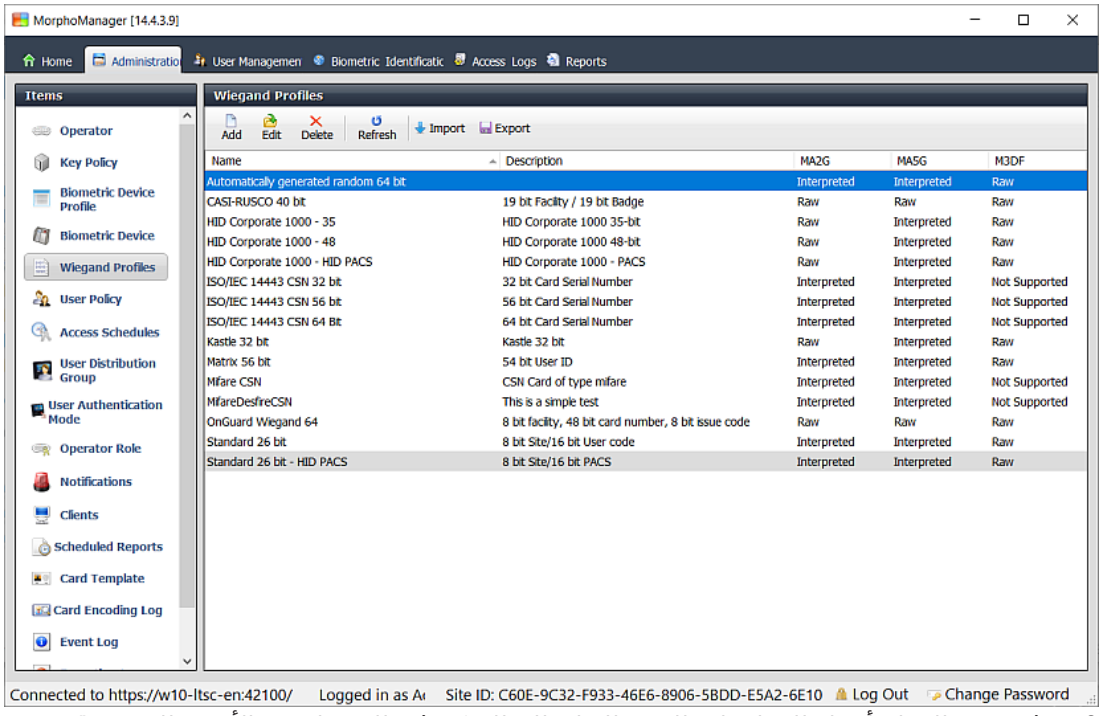
22.4.1 ملفات تعريف Wiegand

إشعار!
تنطبق ملفات تعريف Wiegand، على الرغم من اسمها، على جميع أنواع أجهزة القراءة، بما في ذلك أجهزة قراءة OSDP.

تحدد ملفات تعريف Wiegand المعلومات التي تخرجها الأجهزة البيومترية عبر واجهة Wiegand Out، عندما تحدد هوية المستخدم. تنتقل هذه المعلومات إلى نظام التحكم في الوصول من Bosch، الذي يستخدمها لاتخاذ قرار الوصول.

الإجراء:

1. في MorphoManager، انتقل إلى **الإدارة** > **ملف تعريف Wiegand**.
2. حدد أحد ملفات تعريف Wiegand المحددة مسبقًا، أو انقر فوق **إضافة** لإنشاء ملف تعريف مخصص. بشكل عام، تُعد جميع ملفات تعريف CSN مناسبة لاستخدامها مع أنظمة التحكم في الوصول من Bosch، بالإضافة إلى ملفات تعريف 26 بت القياسية. إذا قدم برنامج التثبيت ملف تعريف لنظامك، فانقر فوق **استيراد** لتحديد موقع الملف الذي تم تقديمه واستيراده، وحدده من القائمة.



3. في مربع الحوار، أدخل المعلومات التي يطلبها نظام التحكم في الوصول من الأجهزة البيومترية.

4. دوّن اسم ملف تعريف Wiegand الذي تقوم بتحديده أو إنشائه هنا. يجب عليك الإشارة إليه في تكوينات MorphoManager في كل من **تكوين المستخدم** و**تكوين الجهاز البيومتري**.

راجع

– اختيار تقنيات وتنسيقات البطاقات, الصفحة *146*

22.4.2 تكوين الأجهزة البيومترية

يحدد تكوين الجهاز البيومتري المعلمات والإعدادات العامة لجهاز بيومتري واحد أو أكثر. عندما تضيف أجهزة بيومترية إلى النظام لاحقًا في قسم **الجهاز البيومتري** في **الإدارة**، ستقوم بتطبيق تكوين جهاز بيومتري عليها.

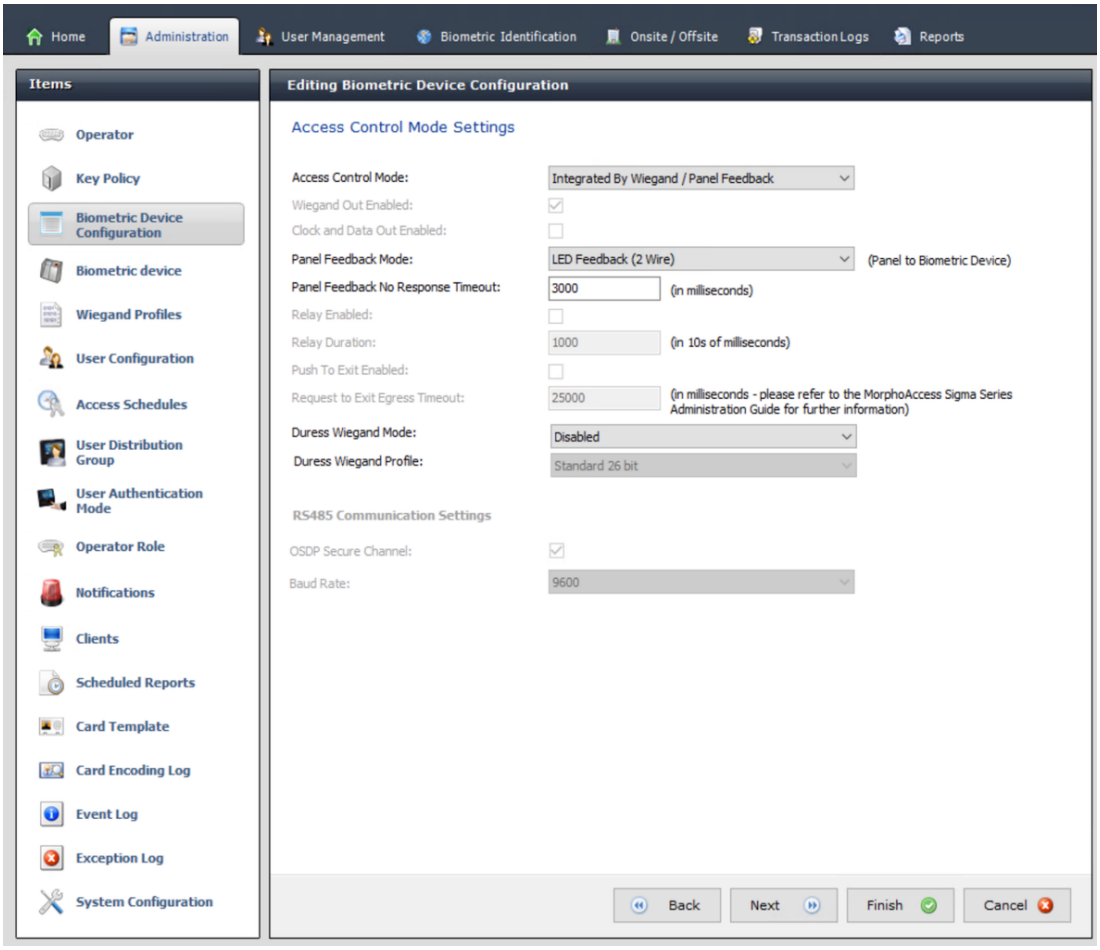
يفترض الإجراء التالي أنك تنشر أجهزة قراءة بيومترية من IDEMIA مع تقنية إضافية لقراءة البطاقات.

الإجراء:

1. في MorphoManager، انتقل إلى **الإدارة** > **تكوين الجهاز البيومتري**.
2. انقر فوق **إضافة** لإنشاء تكوين جهاز بيومتري جديد.
3. على الشاشة التالية، أدخل اسمًا لملف التعريف بالإضافة إلى وصف (اختياري). إذا كنت لا تستخدم حقل الوصف، فإننا نوصي باستخدام اسم يصف النوع وأوضاع التعريف (بيانات بيومترية و/أو بطاقة) لمجموعة من أجهزة القراءة.
4. انقر فوق **التالي** حتى تصل إلى **إعدادات الجهاز البيومتري**

– حدد ملف تعريف Wiegand الذي أنشأته في وقت سابق لعملية التثبيت.

5. انقر فوق **التالي** حتى تصل إلى صفحة **إعدادات وضع التحكم في الوصول**.



في هذه المرحلة، تتباعد إجراءات وحدات AMC لكل من Wiegand وOSDP. اتبع الإجراء أدناه الذي يتوافق مع نوع وحدة تحكم AMC لديك:

بالنسبة إلى وحدات AMC لـ Wiegand

1. عيّن **وضع التحكم في الوصول** إلى `Integrated by Wiegand`
2. عيّن **وضع تعليقات اللوحة** إلى `LED Feedback (2 wire)`
3. انقر فوق **إنهاء**

بالنسبة إلى وحدات AMC لـ OSDP

1. عيّن **وضع التحكم في الوصول** إلى `Integrated by OSDP`
2. عيّن **وضع تعليقات اللوحة** إلى `LED Feedback (2 wire)`
3. حدد خانة الاختيار **قناة OSDP الآمنة**
4. تعيين معدل البث بالباود `9600`
5. لمزيد من التفاصيل، راجع القسم **الجهاز البيومتري**
6. انقر فوق **إنهاء** للخروج من MorphoManager.

استكشاف أخطاء مفاتيح OSDP وإصلاحها

إذا لم تتمكن من إنشاء اتصال آمن بقارئ OSDP، فحاول إعادة تعيين المفتاح الأساسي كما يلي:

1. ابدأ برنامج **MorphoBioToolBox (MBTB)** المنفصل
2. في برنامج MorphoBioToolBox، انتقل إلى **إعدادات الجهاز** > **إعادة تعيين**
3. حدد مفتاح OSDP الأساسي
4. انقر فوق **إعادة تعيين مفاتيح التشفير**
5. قم بإنهاء MorphoBioToolBox

فما يتعلق بحالات أكثر تعقيدًا، اتصل بالدعم التقني لشركة IDEMIA.

راجع

- الجهاز البيومتري, الصفحة *156*

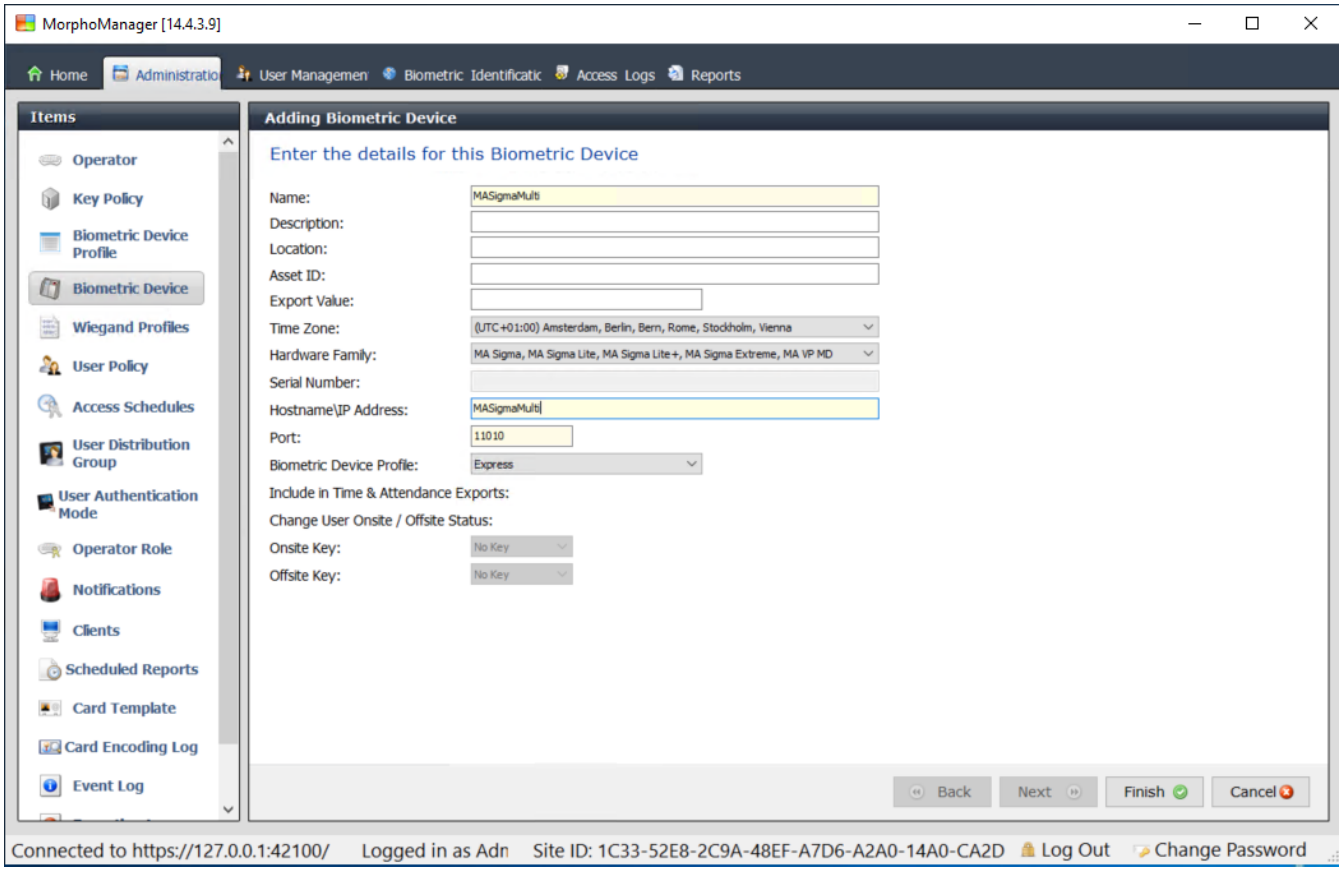
22.4.3 الجهاز البيومتري

تختبر الأجهزة البيومترية ما إذا كانت بيانات الاعتماد البيومترية التي تقرأها مطابقة للسجلات في قاعدة البيانات. وهي تحتفظ أيضًا بسجل لكل حدث استخدام.

الإجراء:

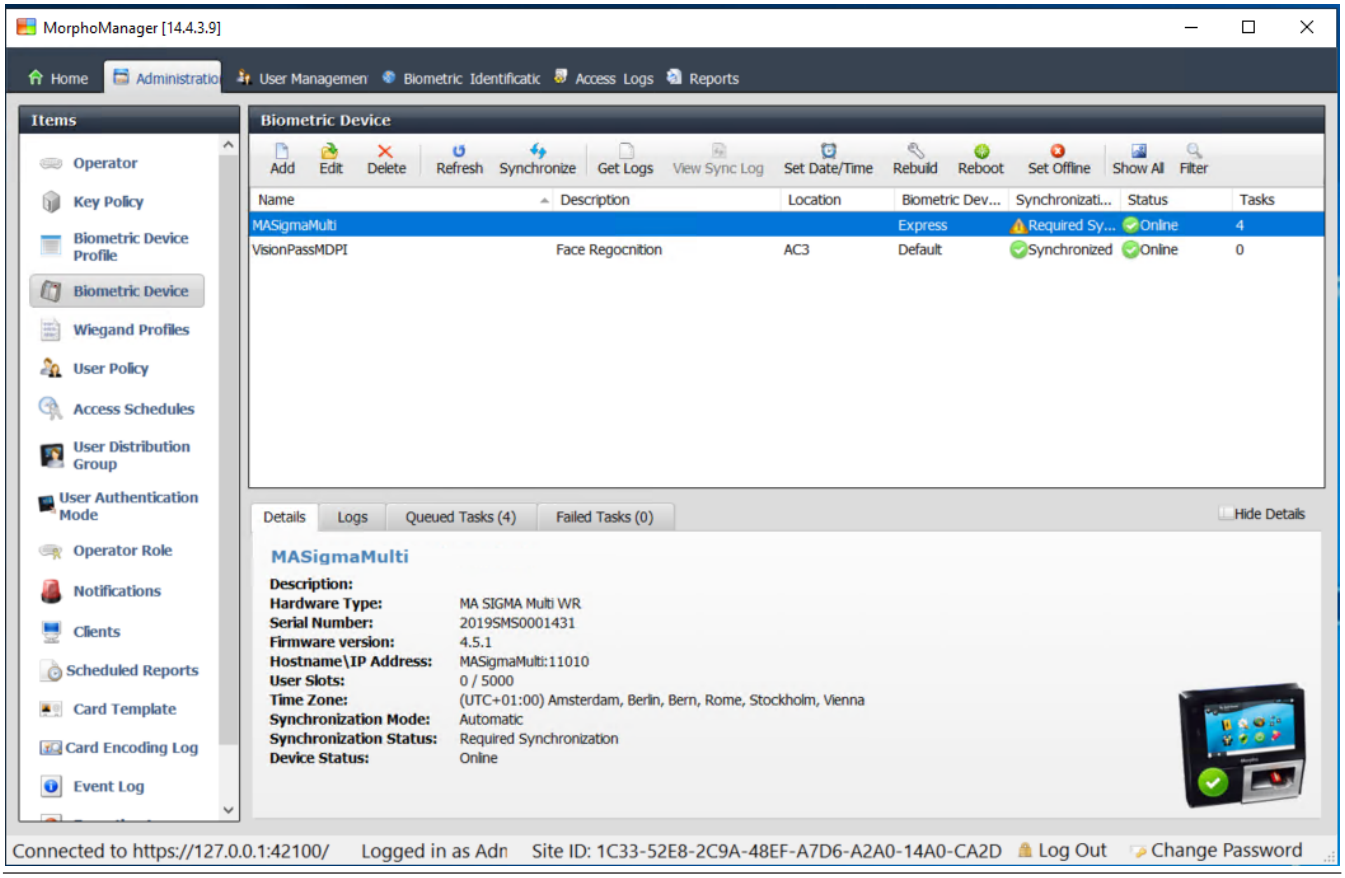
1. في MorphoManager، انتقل إلى **الإدارة** > **الجهاز البيومتري**.
2. انقر فوق **إضافة** لإنشاء جهاز بيومتري جديد.
3. أدخل التفاصيل الأساسية الخاصة بالجهاز على الأقل.

- (من القائمة) **مجموعة الأجهزة**
- **اسم المضيف/عنوان IP**
- (من القائمة) **تكوين الجهاز البيومتري** الذي حددته في وقت سابق



4. انقر فوق **إنهاء**

. يسرد الآن مربع حوار "الجهاز البيومتري" الأجهزة التي سبق أن تم تكوينها:

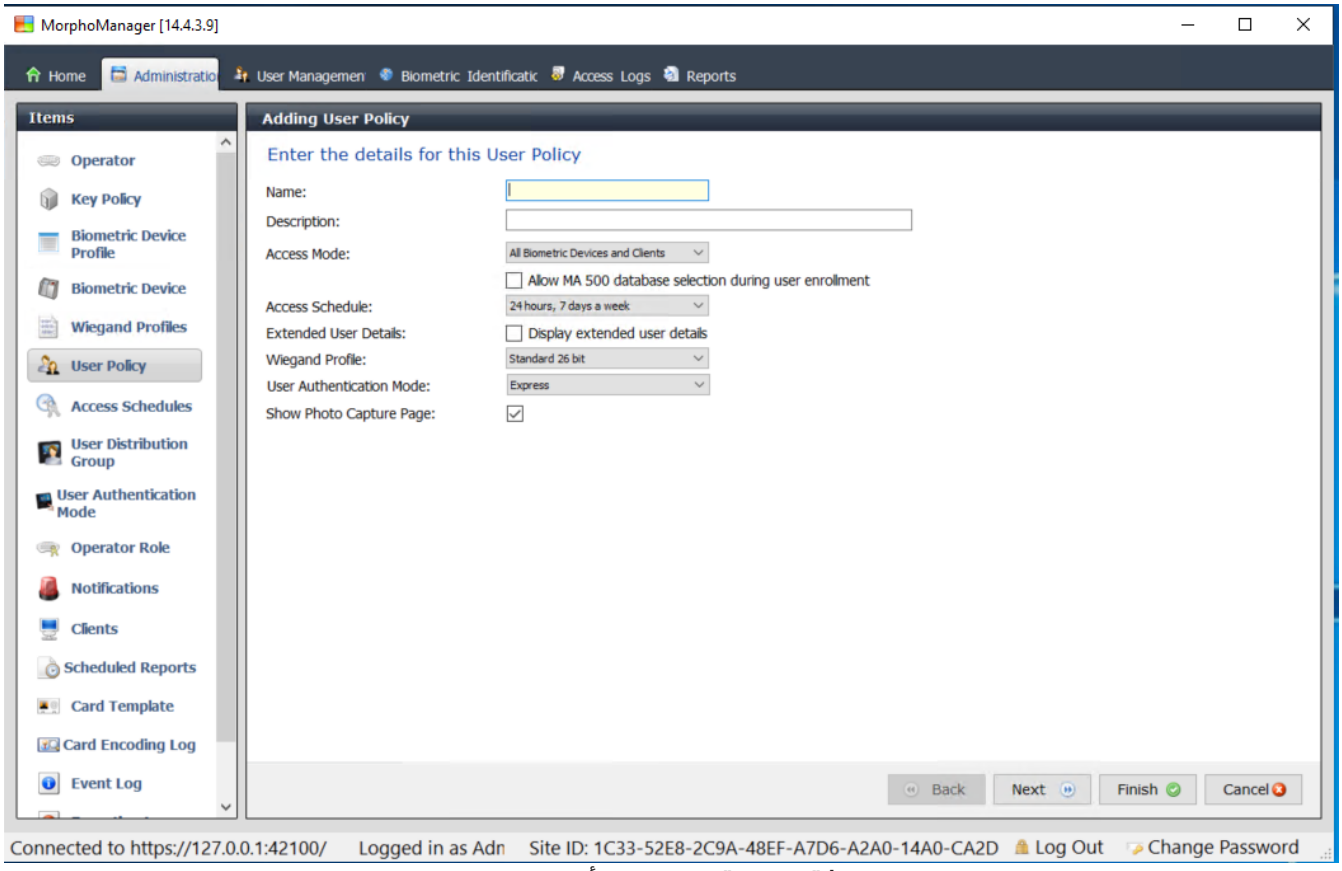


22.4.4 تكوين المستخدم

إن عمليات تكوين المستخدم عبارة عن حزم من حقوق الوصول التي تعيّنها لمستخدمين لديهم متطلبات الوصول نفسها، أي الأجهزة البيومترية التي يُسمح لهم باستخدامها وضمن أي أوضاع وفي أي أوقات.

الإجراء:

1. في MorphoManager، انتقل إلى **الإدارة** > **تكوين المستخدم**.
2. انقر فوق **إضافة** لإنشاء تكوين مستخدم جديد.



3. في مربع الحوار **إضافة سياسة مستخدم**، أدخل المعلومات التالية:
   - **الاسم** لسياسة المستخدم و(اختياريًا) الوصف
   - **وضع الوصول** `Per User`
   - **جدول وصول** يحكم الأيام والأوقات التي يكون فيها الوصول مسموحًا
   - **ملف تعريف Wiegand** نفسه الذي حددته من أجل **ملف تعريف الجهاز البيومتري**.
   - **وضع مصادقة المستخدم**، بحسب الطرق التي سيستخدم بها مستخدمو الجهاز الأجهزة (عن طريق بصمة الإصبع أو الإصبع أو الوجه أو البطاقات وما إلى ذلك). انظر القسم **اختيار وضع التعريف** للحصول على التفاصيل.
4. انقر فوق **إنهاء**

سيكون لسياسة المستخدم الافتراضية وضع مصادقة المستخدم `(Many :1)`. لاستخدام أوضاع المصادقة الأخرى، أنشئ سياسات مستخدم إضافية. راجع دليل مستخدم MorphoManager لمزيد من التفاصيل حول جميع الخصائص المختلفة التي يمكن تعيينها لسياسة المستخدم.

راجع

- اختيار وضع التعريف, الصفحة *150*

22.4.5 مجموعات توزيع المستخدمين

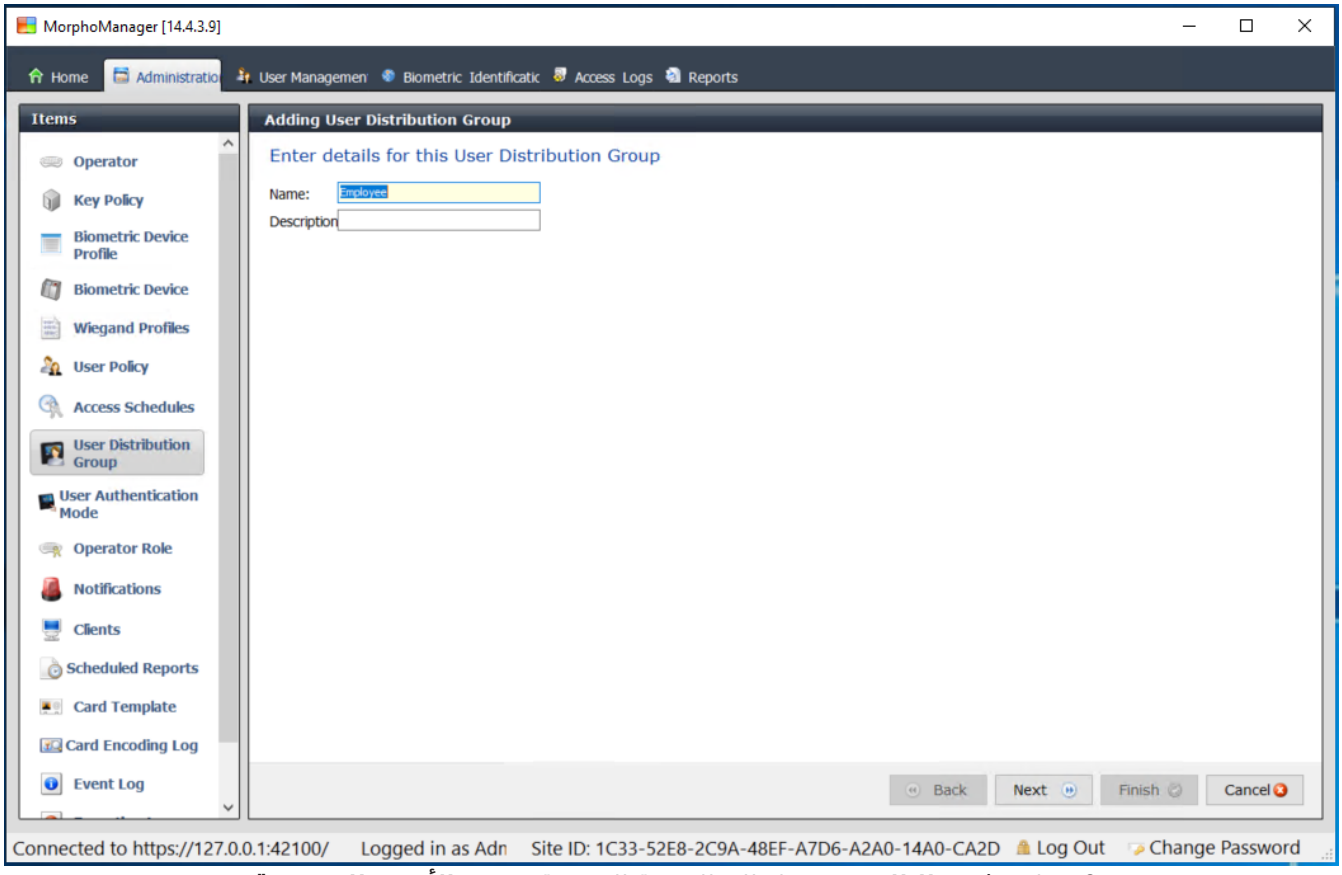
تقوم مجموعات توزيع المستخدمين بتعيين المستخدمين إلى مجموعات من أجهزة القراءة البيومترية أو عملاء MorphoManager.

الشروط الأساسية:

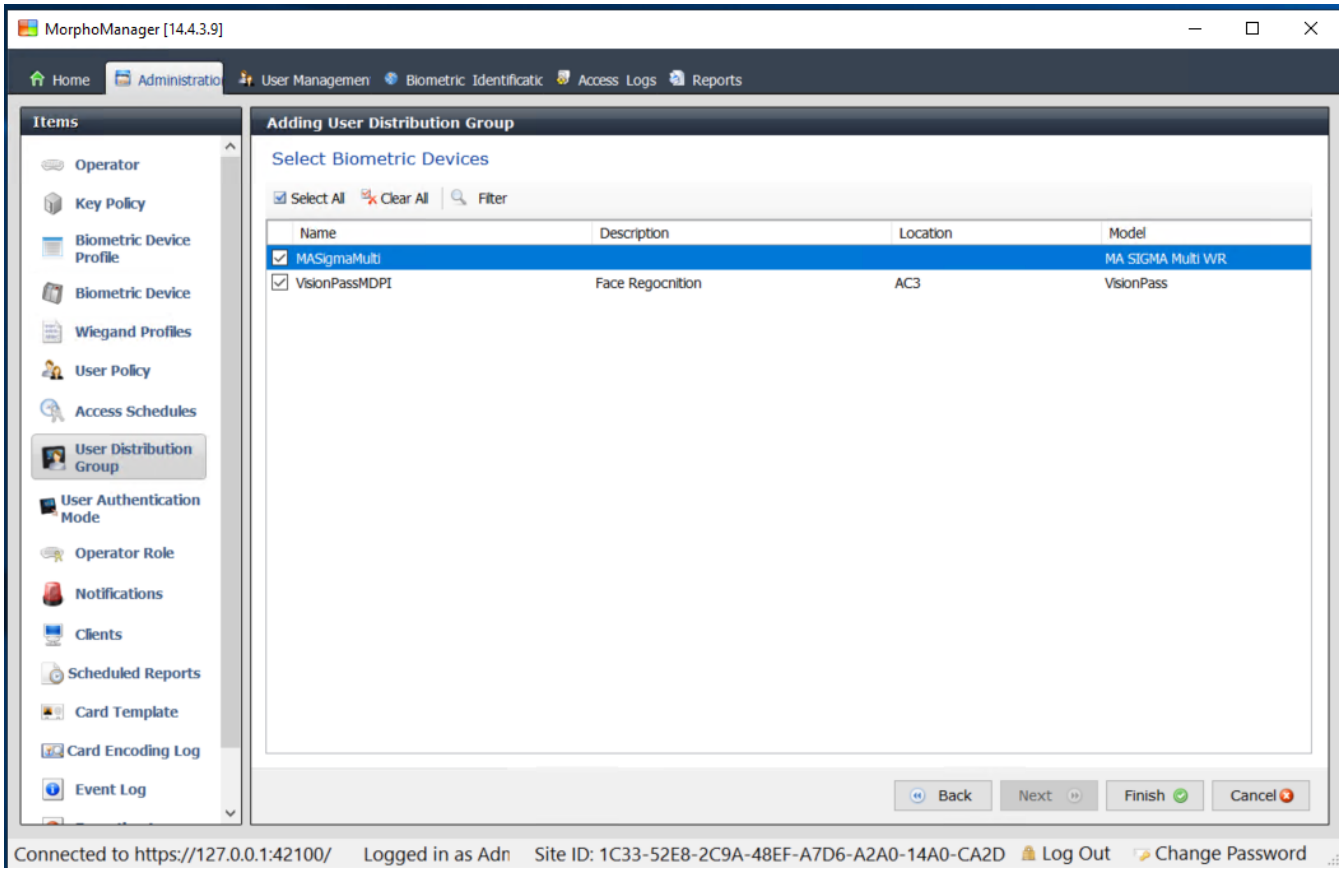
يجب تعيين كل مجموعة من مجموعات توزيع المستخدمين إلى فئة شخص واحدة على الأقل في ACS. وبالتالي، أنشئ مجموعة توزيع مستخدمين واحدة على الأقل لكل فئة شخص تستخدمها.

الإجراء:

1. في MorphoManager، انتقل إلى **الإدارة** > **مجموعة توزيع المستخدمين**.
2. انقر فوق **إضافة** لإنشاء مجموعة توزيع مستخدمين جديدة.



3. انقر فوق **التالي** حتى تصل إلى الصفحة المعنونة **تحديد الأجهزة البيومترية**
4. حدد خانات الاختيار التابعة لهذه الأجهزة البيومترية التي سيستخدمها الأشخاص في مجموعة توزيع المستخدمين هذه.



5. انقر فوق **إنهاء**

22.4.6 إعداد ODBC لـ BioBridge

المقدمة

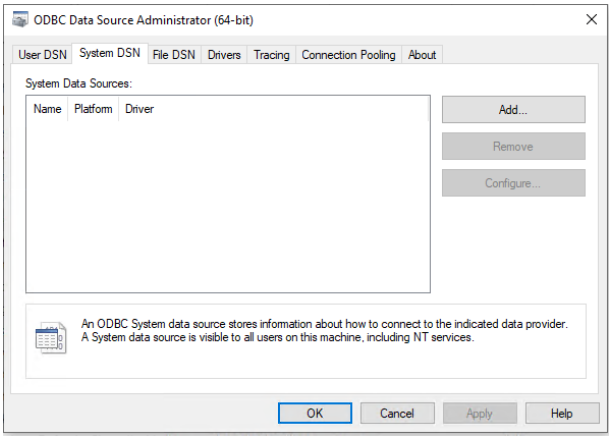
يُعد اتصال قاعدة البيانات المفتوح (ODBC) شرطًا أساسيًا لاستخدام MorphoManager BioBridge.
يشكّل ODBC واجهة برمجة موحدة للوصول إلى قواعد بيانات مختلفة. برنامج التشغيل الموصى به هو `OdbCDriver17SQLServer`

- بالنسبة لـ BIS، يوجد برنامج التشغيل على وسائط تثبيت BIS في `BIS\3rd_Party\OdbCDriver17SQLServer`
- بالنسبة لـ AMS، قم بتنزيل برنامج التشغيل من `www.microsoft.com`

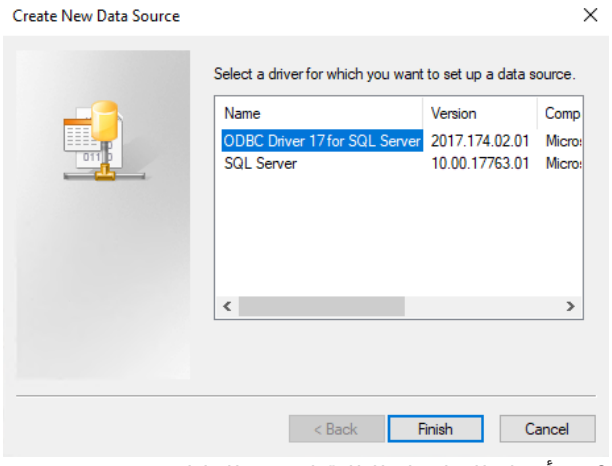
إنشاء مصدر بيانات

إنشاء اسم مصدر بيانات (DSN) لاتصال قواعد البيانات المفتوح (ODBC)

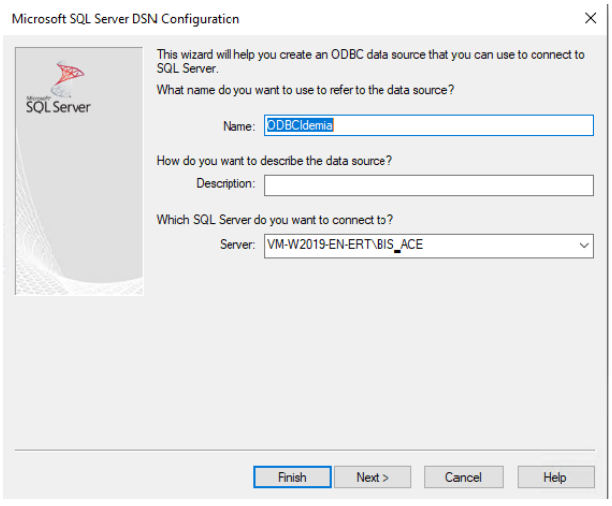
1. في لوحة التحكم في Windows، حدد **أدوات إدارية**.
2. حدد `ODBC Data Sources (64-bit)` من القائمة.
3. حدد علامة التبويب **DSN النظام**.



4. انقر فوق **إضافة** لتحديد برنامج تشغيل.
5. حدد `ODBC Driver 17 for SQL Server` كبرنامج تشغيل، ثم انقر فوق **إنهاء**.

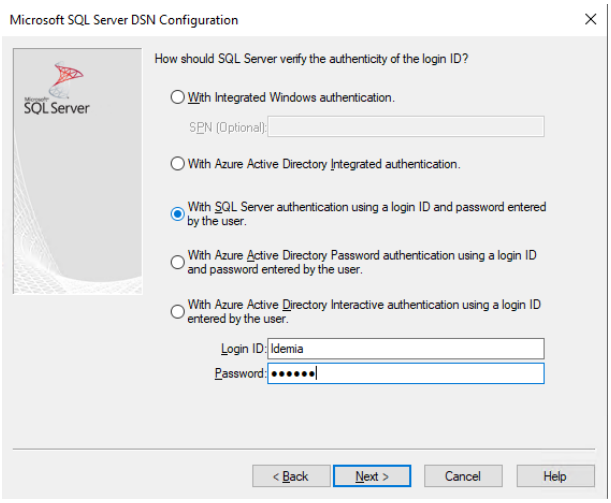


6. أدخل التفاصيل التالية لمصدر البيانات.
- **الاسم**: اسمًا لمصدر البيانات
- **الوصف** (اختياري)
- **الخادم**: اسم الكمبيوتر حيث تم تثبيت قاعدة بيانات ACE واسم قاعدة البيانات (الافتراضي: <خادمACS الخاص بي>\`ACE`)

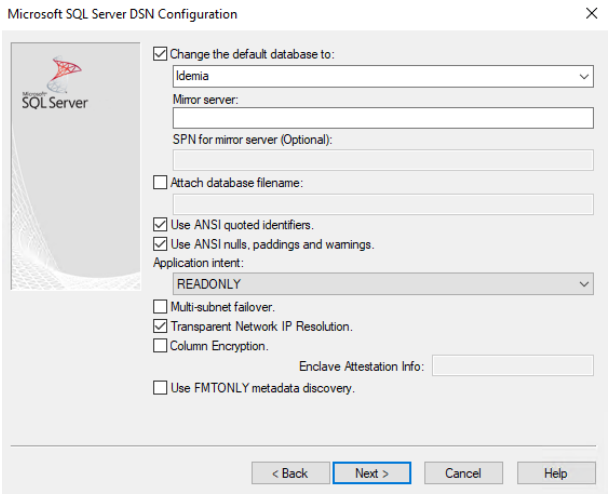


7. انقر فوق **التالي >**

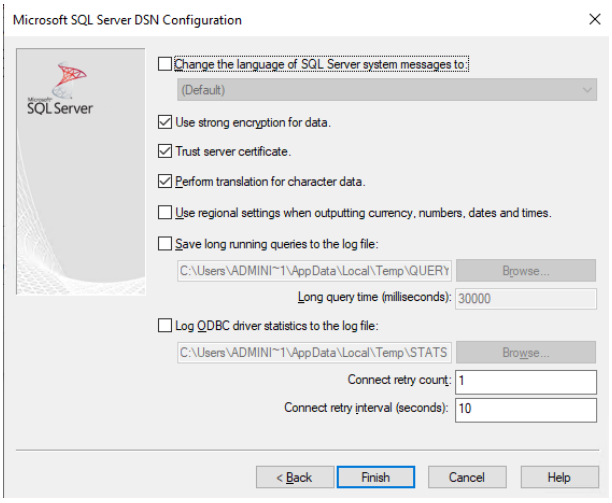
يظهر مربع حوار لجمع معلومات تسجيل الدخول



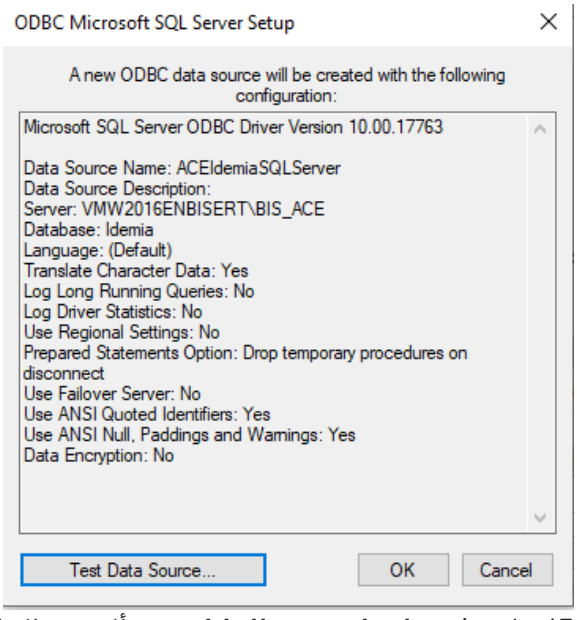
8. حدد **مع مصادقة SQL Server باستخدام معرف تسجيل دخول...**
9. أدخِل المعلومات التالية:
   - **مُعرف تسجيل الدخول**: اسم مستخدم قاعدة بيانات Idemia كما تم تكوينه في ACS. إنه دائمًا `Idemia`.
   - **كلمة المرور**: كلمة المرور التي تم تعيينها لمستخدم قاعدة بيانات Idemia، عند تكوينه في ACS.
10. انقر فوق **التالي >**
11. في مربع الحوار التالي، حدد خانات الاختيار:
    - **تغيير قاعدة البيانات الافتراضية إلى:** و حدد `Idemia`
    - **استخدام معرفات ANSI المقتبسة**
    - **استخدام قيم ANSI الفارغة والهوامش الداخلية والتحذيرات**
    - **دقة IP للشبكة الشفافة**
12. عيّن **القصد من التطبيق** إلى `READONLY`



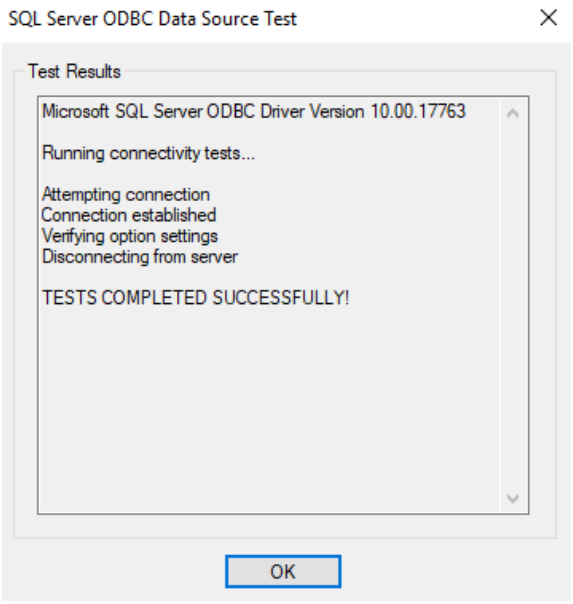
13. انقر فوق **التالي >**
14. في مربع الحوار التالي، حدد خانات الاختيار
    - **استخدام تشفير قوي للبيانات**
    - **تنفيذ ترجمة بيانات الأحرف**
    - **الثقة بشهادة الخادم**



15. انقر فوق **إنهاء**
16. في مربع الحوار التالي، راجع بيانات الملخص



17. انقر فوق **اختبار مصدر البيانات...** وتأكد من إكمال الاختبارات بنجاح.



18. احفظ جميع التغييرات، ثم اخرج من معالج إعداد ODBC.

22.4.7 تكوين نظام BioBridge

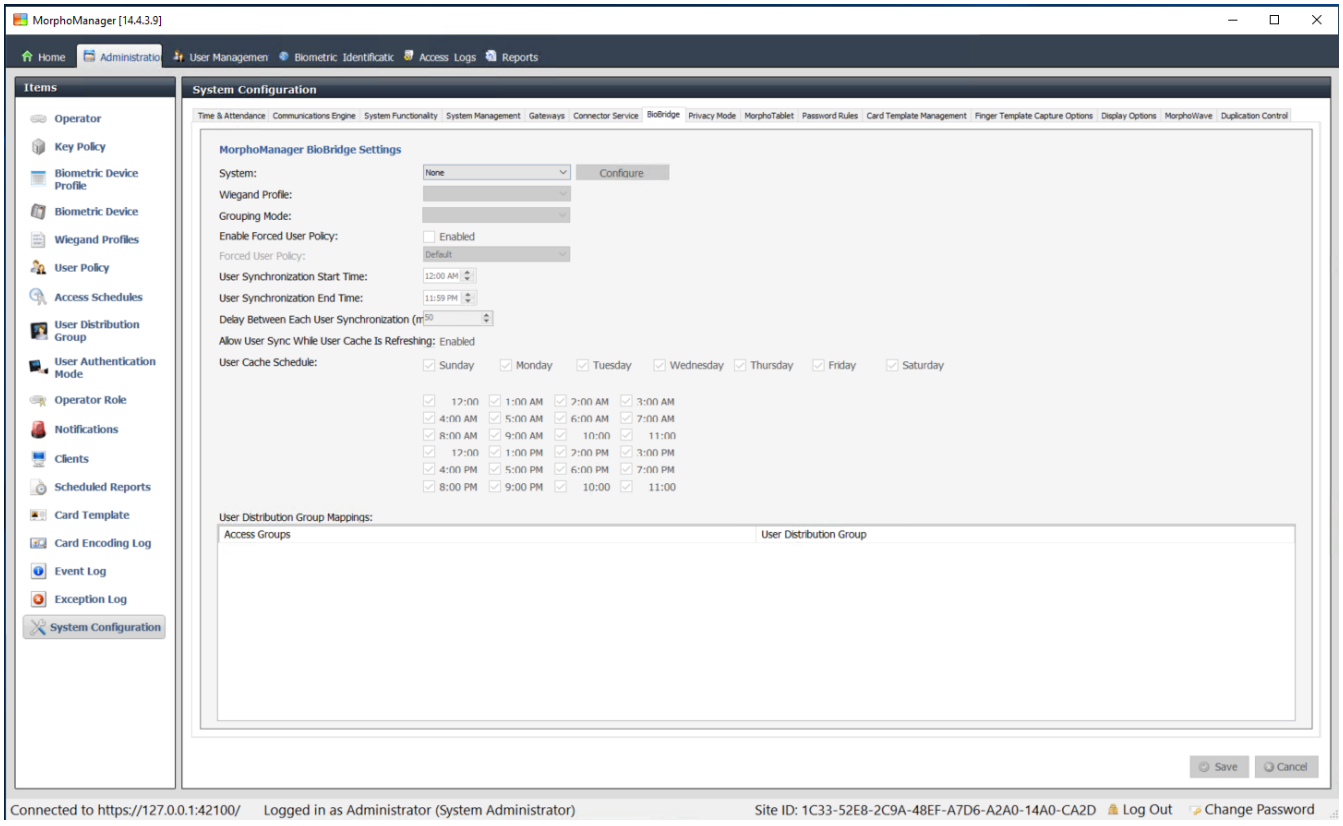
يصف هذا القسم الإعدادات المتبقية المطلوبة لأنظمة التحكم في الوصول لاستخدام واجهة BioBridge.

الشرط الأساسي

يتم إعداد ODBC لـ BioBridge. راجع إعداد *ODBC* لـ *BioBridge*, الصفحة *160*

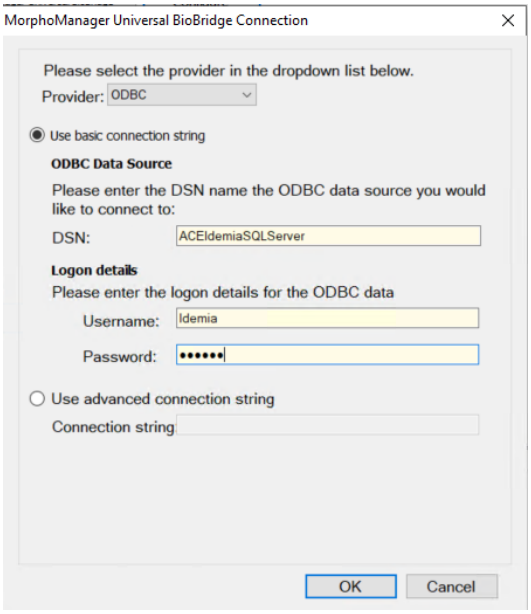
الإجراء:

1. في MorphoManager، انتقل إلى **الإدارة** > **تكوين النظام**.
2. حدد علامة التبويب **BioBridge**



3. في مربع القائمة المنسدلة **النظام**، حدد `MorphoManager Universal BioBridge`
4. انقر فوق **تكوين**

يظهر مربع حوار منبثق.



في النافذة المنبثقة

1. في مربع القائمة المنسدلة **الموفر**، حدد `ODBC`
2. أدخل اسم مصدر البيانات (DSN) من إعداد ODBC.
3. ضمن **تفاصيل تسجيل الدخول**، أدخل اسم المستخدم (`Idemia`) وكلمة المرور كما تم تحديدهما في إعداد ODBC.
4. انقر فوق **موافق** للعودة إلى مربع الحوار **تكوين النظام**.

في مربع الحوار **تكوين النظام**

1. بالنسبة إلى **ملف تعريف Wiegand**: حدد من القائمة ملف تعريف Wiegand الذي حددته في وقت سابق.

وضع التجميع:

يحدد هذا الإعداد كيف يجب على MorphoManager تعيين مستخدمي MM Universal BioBridge إلى مجموعات توزيع مستخدمي MorphoManager. اختر أحد الخيارات التالية:

- **تلقائي**: سيطابق هذا الوضع تلقائيًا **مجموعات مستوى الوصول** من MM Universal BioBridge مع **مجموعات توزيع المستخدمين** في MorphoManager، إذا كان لديها مصطلح التسمية نفسه.
- **يدوي**: إذا لم تكن **مجموعات مستوى الوصول** في MM Universal BioBridge هي نفسها **مجموعة (مجموعات) توزيع المستخدمين** في MorphoManager، فيمكنك في هذه الحالة تنفيذ التعيين يدويًا في **تعيينات سياسة المستخدم**.

الإعدادات الأخرى

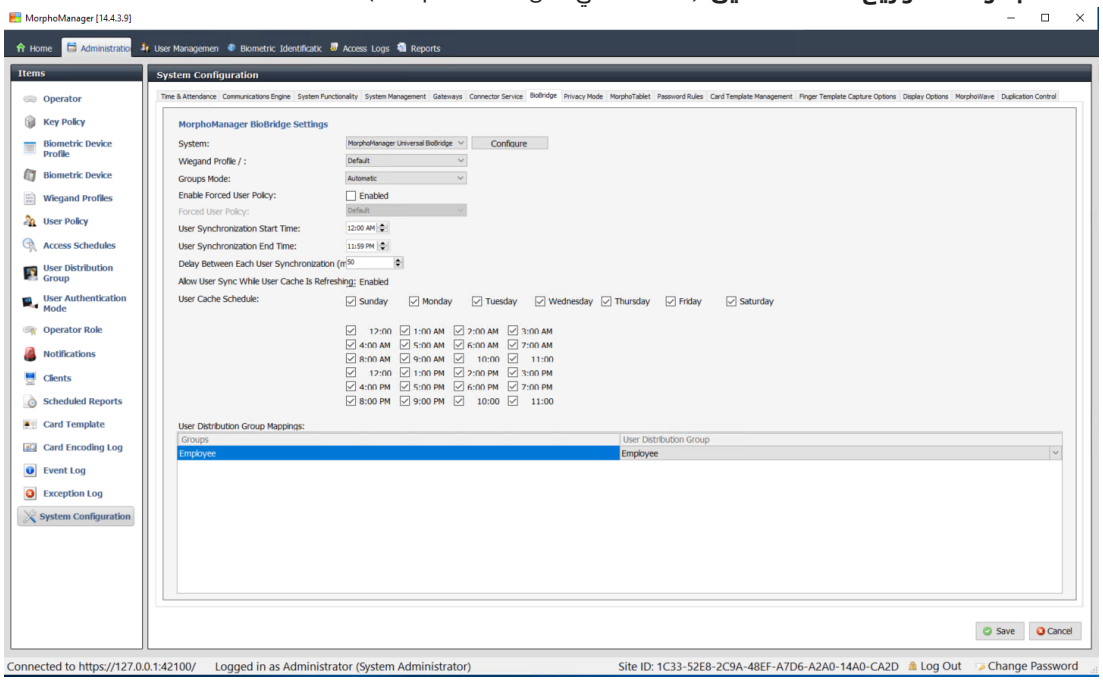
في معظم الحالات، يمكنك ترك الإعدادات التالية عند قيمها الافتراضية:

تمكين سياسة المستخدم المفروضة	عند تحديد هذا الخيار، سيتلقى جميع المستخدمين المسجلين في عميل تسجيل BioBridge سياسة المستخدم المحددة من القائمة المجاورة. إذا حددت خانة الاختيار هذه، فاستخدم دائمًا سياسة المستخدم التي تحمل الاسم `Per User`
وقت بدء ووقت انتهاء مزامنة المستخدم	لن يُسمح بتشغيل محرك مزامنة المستخدم إلا بين هذين الوقتين.

التأخير بين كل عملية مزامنة المستخدم	الفاصل الزمني بين عمليات مزامنة المستخدم. ستؤدي زيادة التأخير إلى توفير موارد النظام، ولكنها ستؤدي إلى زيادة الوقت اللازم لتحديث جميع المستخدمين.
السماح بمزامنة المستخدم أثناء تحديث ذاكرة التخزين المؤقت للمستخدم	عند تمكين هذا الخيار، سيتم تشغيل محرك مزامنة المستخدم بشكل متوازٍ مع تحديث ذاكرة التخزين المؤقت للمستخدم. سيؤدي هذا الأمر إلى زيادة عدد الطلبات على موارد النظام. من المستحسن تعطيل هذا الإعداد عند استخدام قواعد بيانات كبيرة.
جدول تحديث ذاكرة التخزين المؤقت للمستخدم	الأيام والأوقات التي يتم فيها تحديث ذاكرة التخزين المؤقت للمستخدم. للحصول على أعلى مستويات الدقة، يجب أن تكون متوفرة في جميع الأوقات، ولكن فيما يتعلق بأداء الأنظمة ذات قواعد البيانات كبيرة الحجم، تبرز الحاجة إلى تسوية.

تعيينات مجموعة توزيع المستخدمين

- في جدول التعيينات، تأكد من تعيين جميع **المجموعات** (**فئات الأشخاص** المحددة ACS) إلى **مجموعات توزيع المستخدمين** (محددة في MorphoManager).



22.5 تكوين عميل التسجيل BioBridge

المقدمة

إن عميل التسجيل BioBridge هو جهاز كمبيوتر يمكنك من خلاله إنشاء سجلات بيومترية لمستخدمي نظام التحكم في الوصول. تتكوّن عملية إعداد عميل التسجيل BioBridge من 3 أجزاء:

- إضافة مشغّل تسجيل إلى MorphoManager
- تكوين أجهزة كمبيوتر عميل MorphoManager لمهام التسجيل
- اختبار عميل التسجيل

الشروط الأساسية

تثبيت MorphoManager BioBridge على كل محطة عمل ACE تقوم منها بتنفيذ التسجيل البيومتري لأنظمة IDEMIA.

22.5.1 إضافة مشغّل تسجيل إلى Morpho Manager

الإجراء

اتبع التعليمات الواردة في دليل تثبيت عميل MorphoManager.

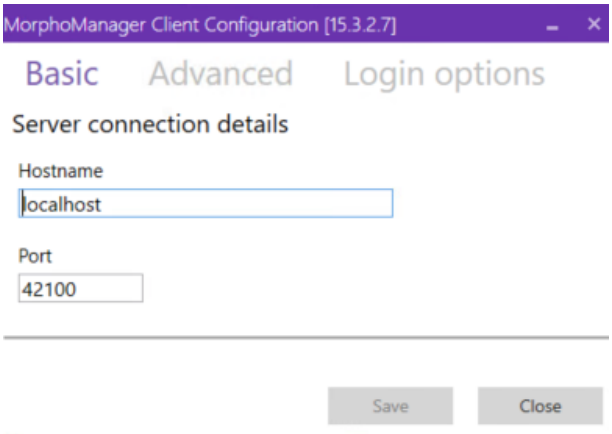
ملاحظة: لأسباب أمنية، تُعد حسابات مستخدمي Active Directory موصى بها.

22.5.2 تكوين أجهزة كمبيوتر عميل MorphoManager لمهام التسجيل

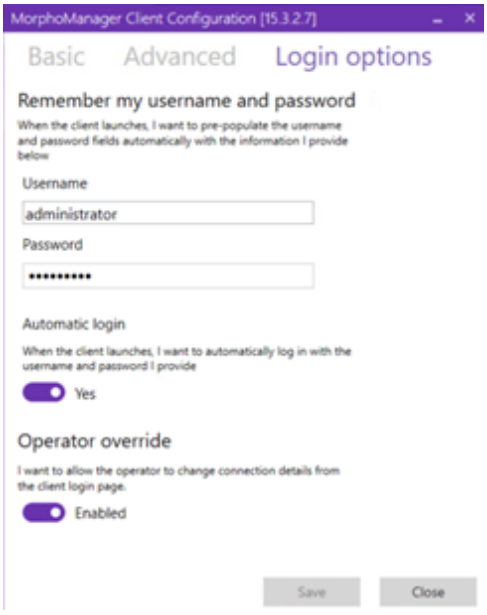
نفّذ هذا الإجراء على كل كمبيوتر تريد استخدامه للتسجيل البيومتري.

الإجراء

1. في دليل تثبيت MorphoManager (الافتراضي: `C:\Program Files (x86)\Morpho\MorphoManager\Client`) نفّذ الملف `ID1.ECP4.MorphoManager.AdvancedClientConfig.exe` كمسؤول

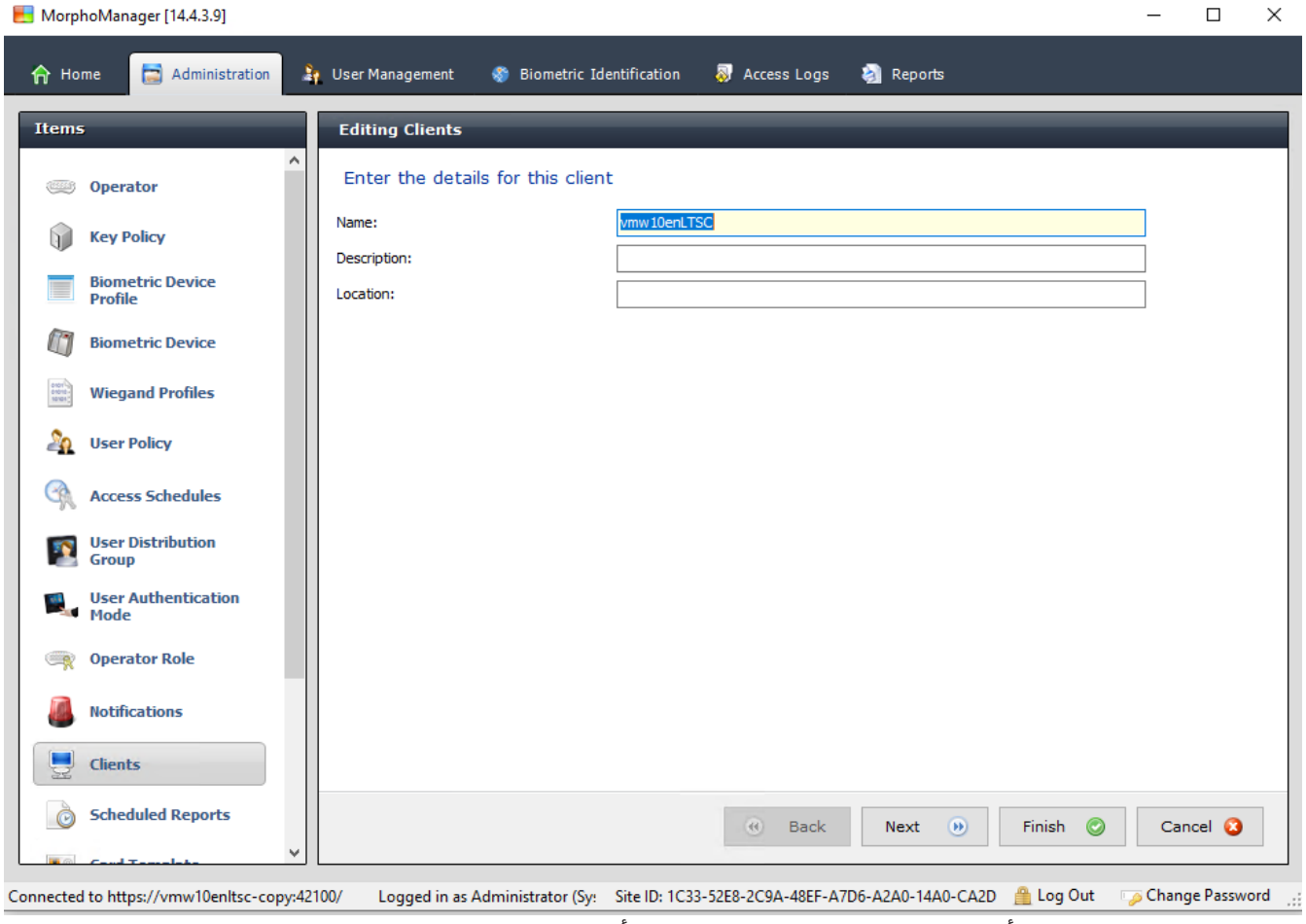


2. في علامة التبويب **أساسي**، أدخل اسم مضيف خادم Morpho ضمن **اسم المضيف**.
3. للتثبيت الآمن، استخدم Active Directory أو اسم المستخدم وكلمة المرور الأصليين، وفقًا لوثائق Morpho.
4. بدلاً من ذلك، [لا يوصى به لعمليات التثبيت عالية الأمان] على علامة التبويب **خيارات تسجيل الدخول**

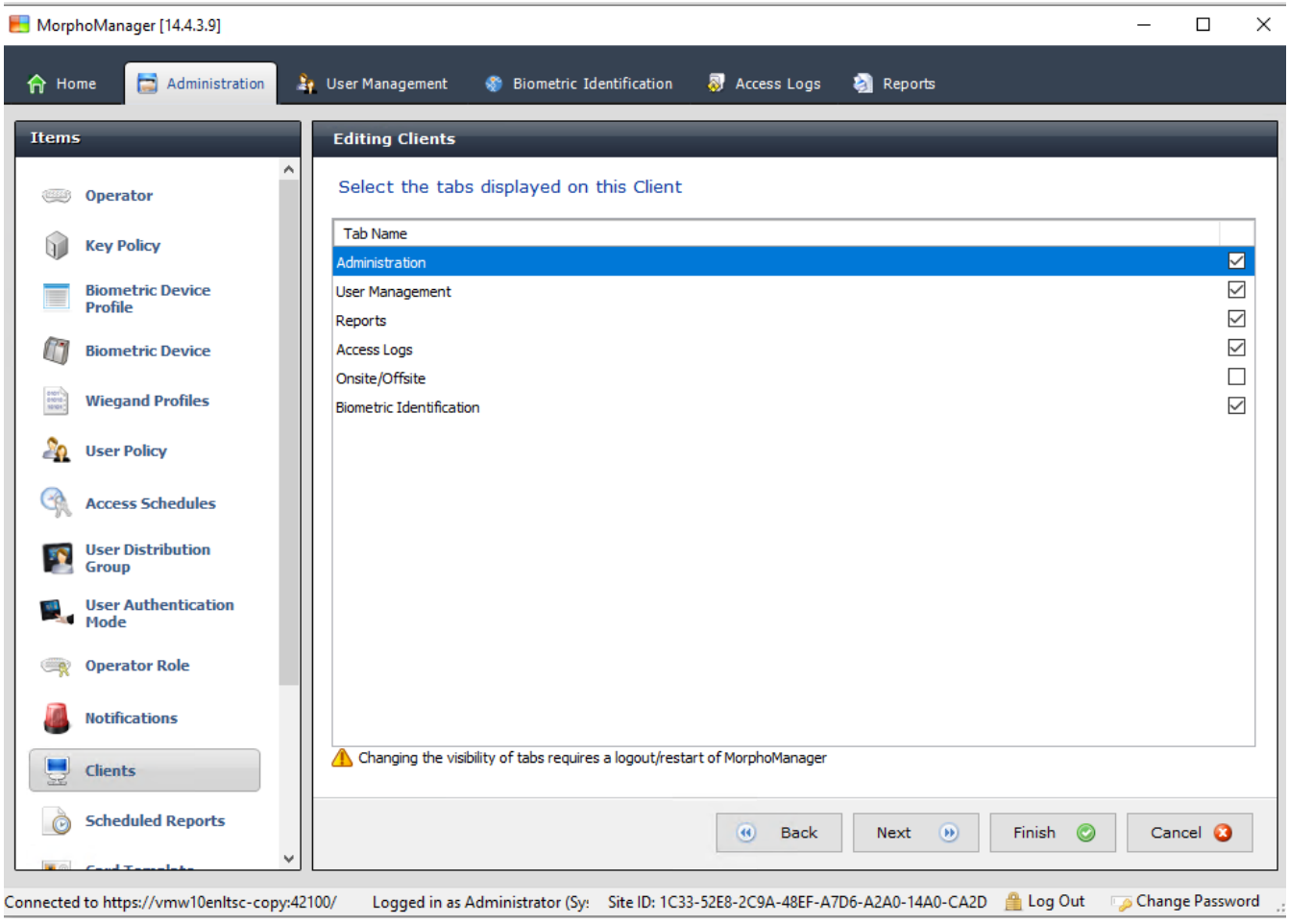


- أدخل اسم المستخدم وكلمة المرور اللذان أدخلتهما لمشغّل التسجيل في القسم السابق
- قم بتعيين مفتاح **تسجيل الدخول التلقائي** إلى `Yes`

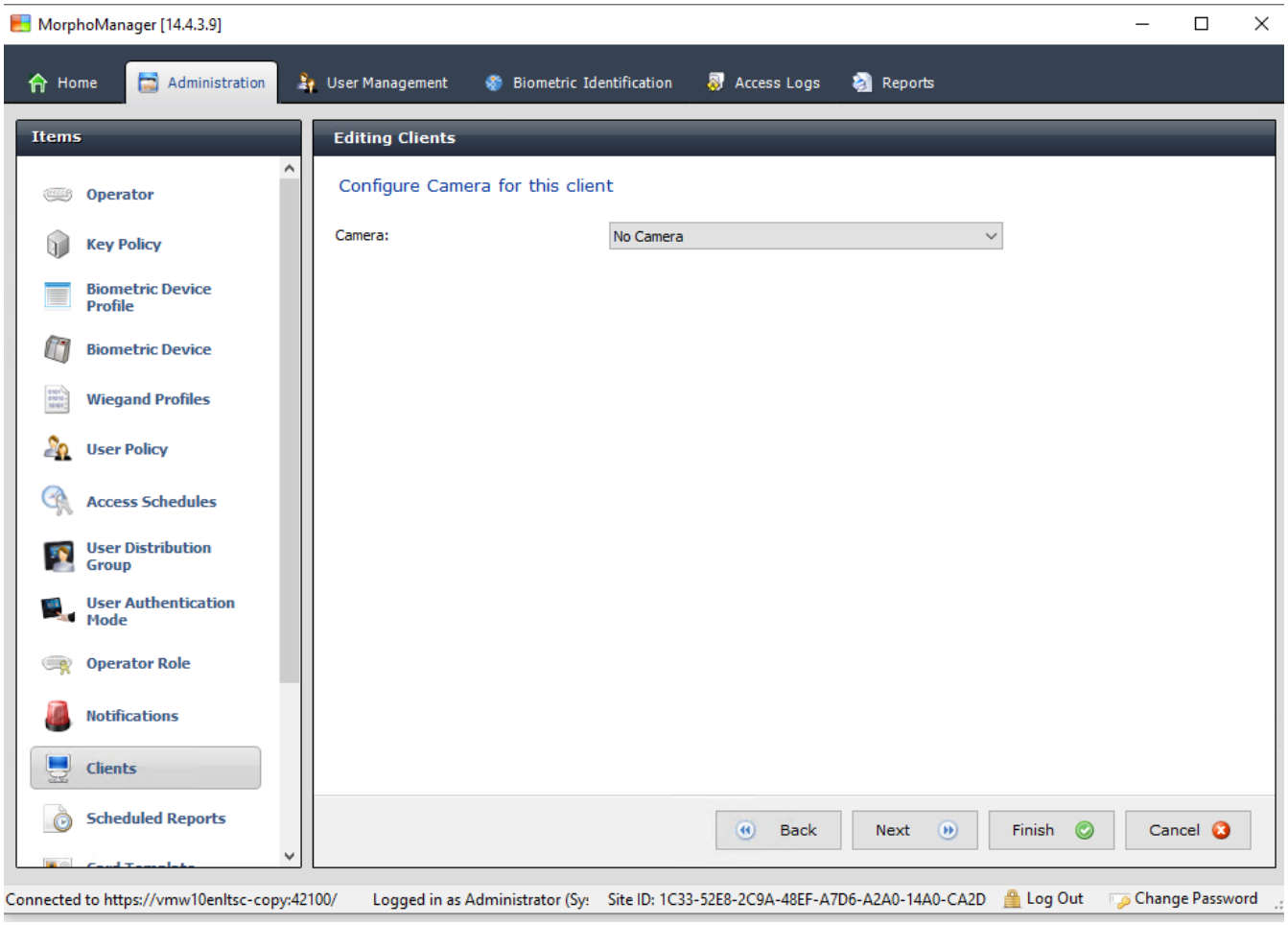
1. في دليل تثبيت MorphoManager (الافتراضي: `C:\Program Files(x86)\Morpho\MorphoManager\Client`)
   نفّذ الملف `Start ID1.ECP4.MorphoManager.Client.exe` كمسؤول
2. انتقل إلى **الإدارة** > **العملاء**
3. حدد كمبيوتر عميل
4. انقر فوق **تحرير**



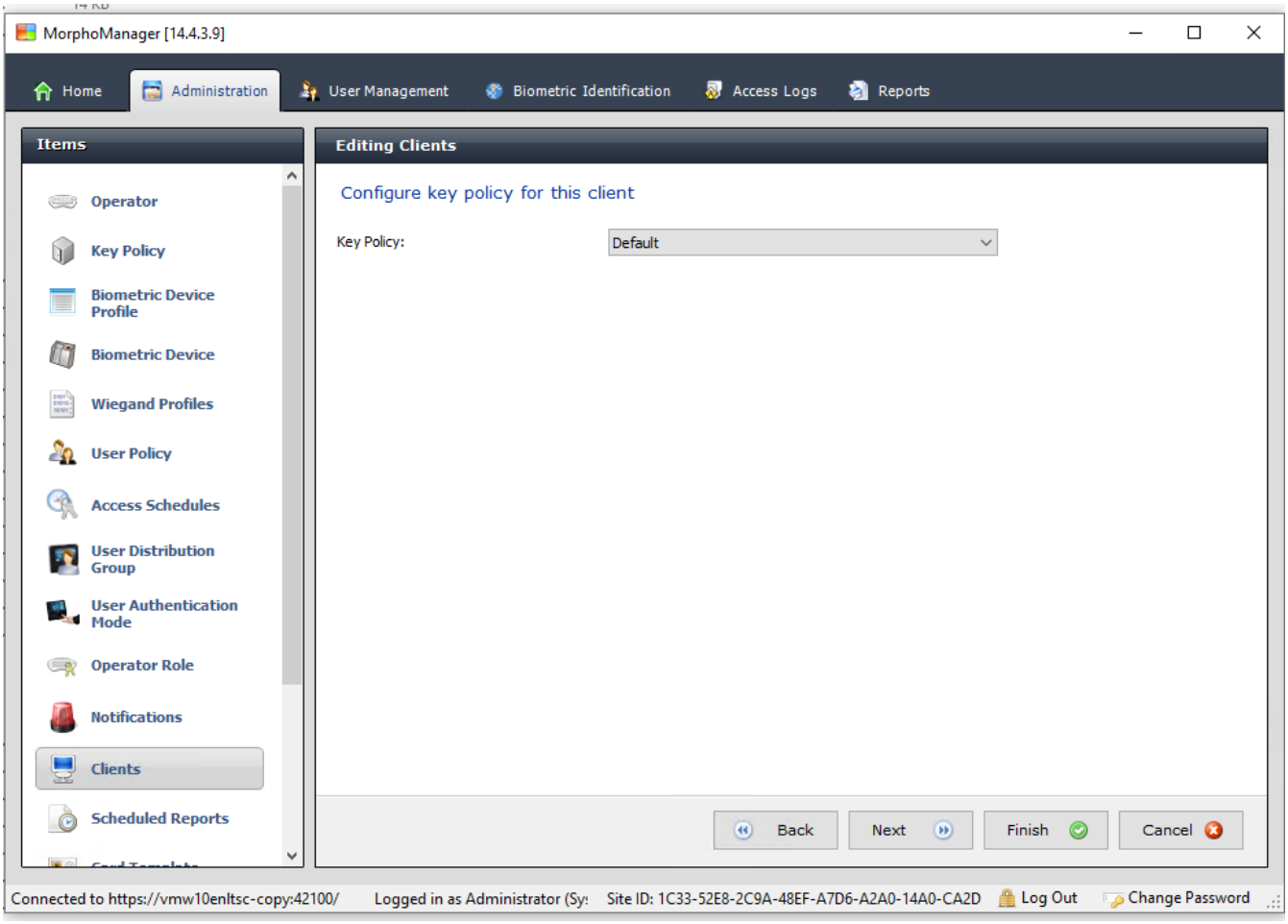
5. أدخل اسم عميل التسجيل المطلوب، وأدخل الموقع والوصف بشكل اختياري
6. انقر فوق **التالي**



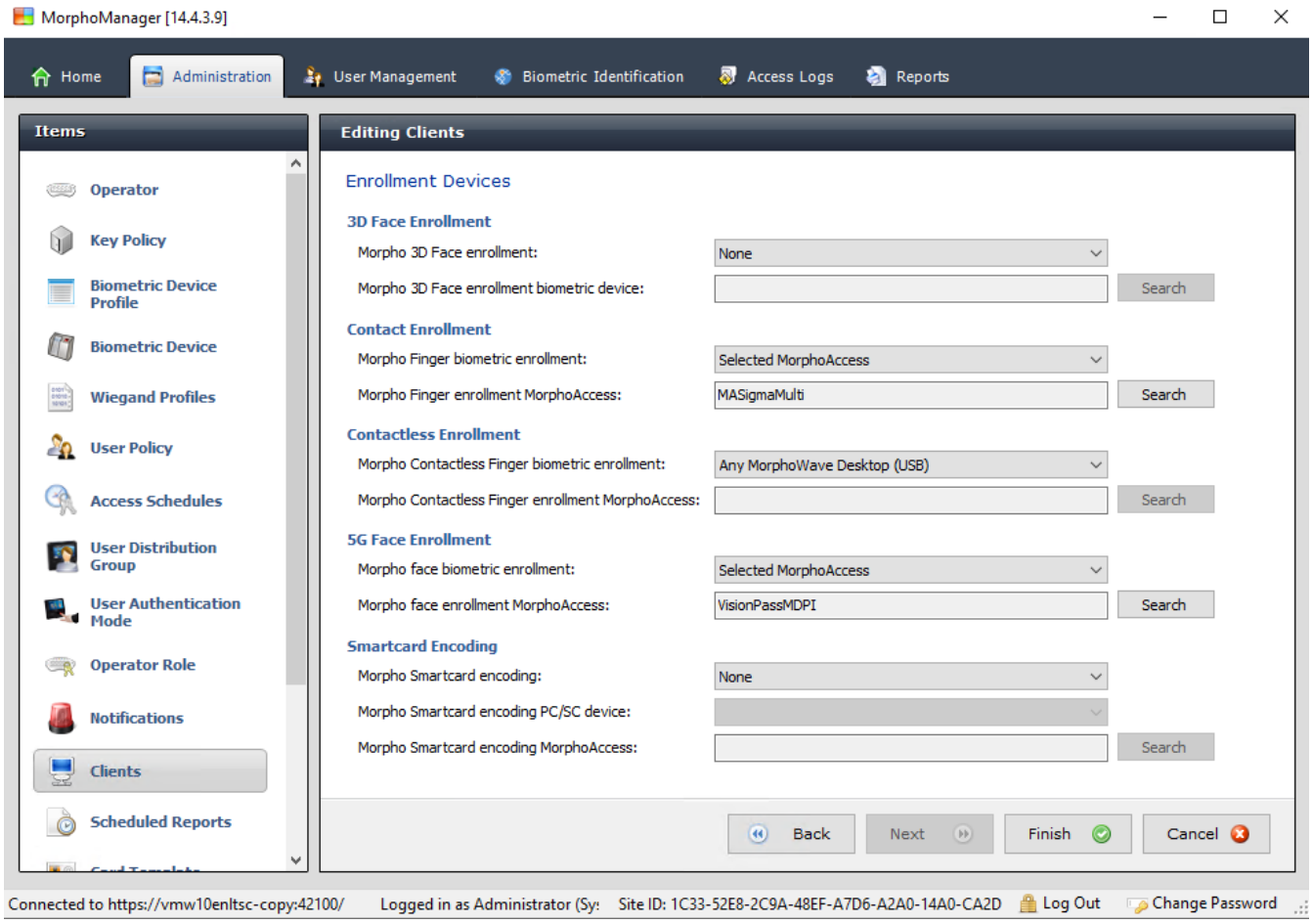
7. حدد خانات الاختيار التابعة لعلامات التبويب التي تريد عرضها على عميل التسجيل:
   - **الإدارة**،
   - **إدارة المسؤولين**،
   - **التقارير**،
   - **سجلات الوصول**،
   - **التعريف البيومتري**
8. انقر فوق **التالي**



9. بالنسبة إلى **الكاميرا:** حدد `No camera` من القائمة
10. انقر فوق **التالي**



11. بالنسبة إلى **السياسة الرئيسية:** حدد `Default` من القائمة
12. انقر فوق **التالي**



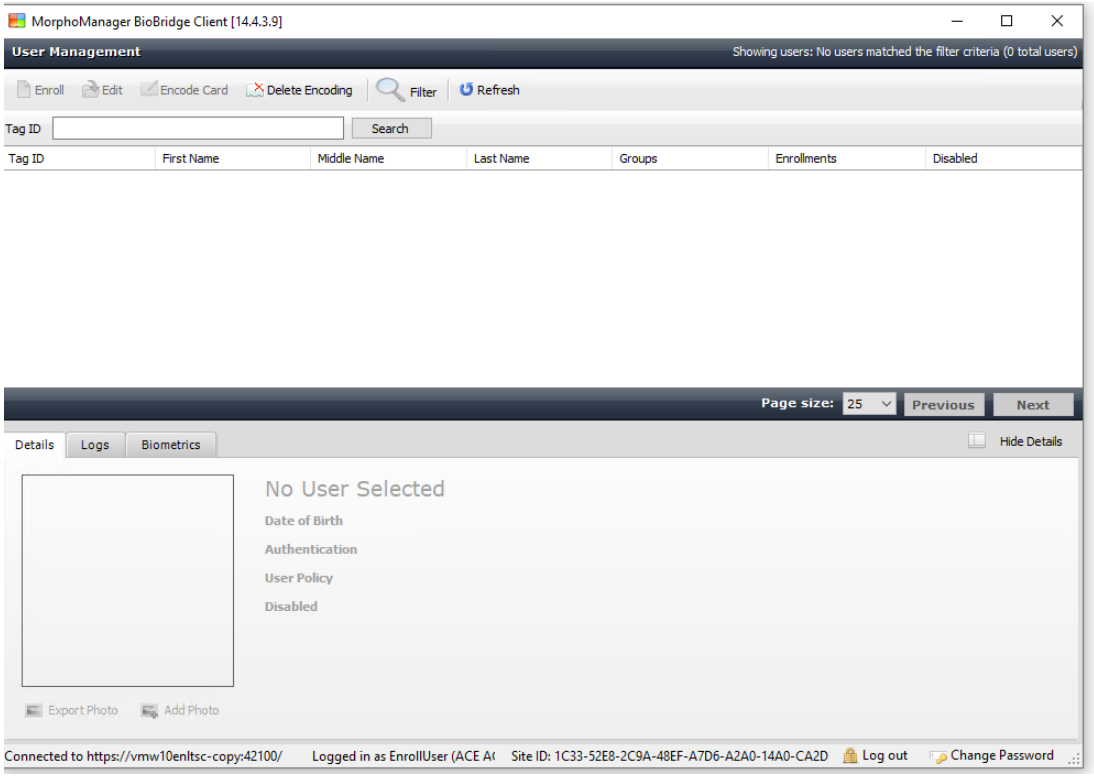
13. حدد قارئ التسجيل البيومتري الذي تريد استخدامه على محطة عمل التسجيل
14. انقر فوق **إنهاء**
15. أغلق تطبيق MorphoManager

راجع

- تكوين عميل التسجيل *BioBridge*, الصفحة *166*

22.5.3 اختبار عميل التسجيل

1. في دليل تثبيت MorphoManager (الافتراضي: `C:\Program Files (x86)\Morpho\MorphoManager\Client`) نفّذ الملف `ID1.ECP4.MorphoManager.BioBridgeEnrollmentClient.exe`



1. تأكد من أنه يمكنك استدعاء شاشة التسجيل من دون الحاجة إلى إدخال اسم المستخدم وكلمة مرور مشغّل التسجيل.

22.6 الحدود والملاحظات التقنية

أنظمة تشغيل Windows المدعومة رسميًا
يدعم IDEMIA إصدارات Windows 10 نفسها التي يدعمها Bosch ACS.

إصدار Microsoft SQL Server المدعوم رسميًا
الإصدار المدعوم هو SQL Server 2017

نظام IDEMIA واحد لكل نظام وصول
بإمكان نظام التحكم في الوصول من Bosch أن يدعم نظام IDEMIA واحدًا فقط

بطاقة IDEMIA واحدة لكل حامل بطاقة.
تدعم أنظمة التحكم في الوصول من Bosch بطاقات متعددة لكل حامل بطاقة، ولكن نظام IDEMIA يدعم بطاقة واحدة فقط وبالتالي، عند التسجيل، وعند المزامنة مع BIS، يتم تعيين أول بطاقة صالحة (أي، حيث الحالة = 1) من النوع "وصول" أو "مؤقت" أو "موقف سيارات" إلى IDEMIA. إذا تم حظر البطاقة لاحقًا، فسيستمر إرسال رقمها والتسجيل في سجل الأحداث.

الحد الأقصى لعدد حاملي بطاقات IDEMIA
بإمكان BioBridge MorphoManager استيعاب ما يصل إلى 100,000 من حاملي البطاقات.

الحد الأقصى لعدد مجموعات الوصول
يدعم نظام IDEMIA ما يصل إلى 5000 من مجموعات الوصول (مجموعات توزيع المستخدمين) ويتم تعيين هذه المجموعات إلى **فئات الشخص** في نظام التحكم في الوصول من Bosch.

أداء القوالب التي تم تنزيلها
- 1000 قالب إلى جهاز واحد: يستغرق التنزيل أقل من دقيقة.
- 1000 قالب إلى مئة جهاز: يستغرق التنزيل بعض الدقائق.

لا يدعم نظام IDEMIA الأقسام
عندما يتم دمج نظام IDEMIA، يتعذر على نظام ACS فحص حاملي البطاقات في قسم واحد بشكل موثوق من مشغّلي التحكم في الوصول من قسم آخر. إذا كانت الخصوصية المطلقة إلزامية بين الأقسام، فلا تدمج نظام IDEMIA.

البطاقات الافتراضية / الوصول بواسطة رمز PIN وحده.
لا يدعم نظام IDEMIA الوصول بواسطة رمز PIN وحده. يجب أن تتوفر بطاقة فعلية.

وظيفة إصبع الضغط في نظام IDEMIA
وظيفة إصبع الضغط في نظام IDEMIA غير مدعومة حاليًا بواسطة وحدات تحكم AMC.

الحد الأدنى من معايير التعريف.
يتطلب التسجيل في نظام IDEMIA معايير التعريف التالية على الأقل:
- الاسم الأول،
- اسم العائلة،
- فئة الشخص
- بطاقة فعلية واحدة معينة إلى حامل البطاقة.

الحالات المعروضة على القارئ
لا تظهر حالة القارئ (على سبيل المثال، الجهاز محظور) على أجهزة قراءة Wiegand وOSDP.

النسخ الاحتياطي والاستعادة
قبل استعادة نسخة احتياطية من IDEMIA، يمكنك أن تقوم بحذف قاعدة بيانات IDEMIA وبإعادة إنشائها باستخدام أداة موفر IDEMIA DataBridge.
في مربع الحوار **الجهاز البيومتري**، تأكد من إرسال جميع عمليات التكوين بشكل صحيح إلى أجهزة قراءة IDEMIA. إذا فشلت إحدى مهام المزامنة، فأعد بناء تكوين القارئ:
1. في MorphoManager، انتقل إلى **الجهاز البيومتري**.
2. حدد الجهاز المتأثر.
3. انقر فوق **إعادة البناء**.

توافق وظائف بطاقة ACS مع أوضاع المصادقة في IDEMIA:

الوظائف	الوضع: البطاقة والسيرة الذاتية	الوضع: البطاقة أو السيرة الذاتية
بطاقات الدخول: إدخال	موافق	موافق
بطاقات الدخول: تحديث	موافق	موافق
بطاقات الدخول: حذف	موافق	موافق
بطاقات الدخول: بطاقات متعددة	البطاقة الأولى فقط	أول بطاقة مستخدمة للبيانات البيومترية.
البطاقة البديلة	موافق	موافق
البطاقات المؤقتة	موافق	موافق
البطاقة المؤقتة: فترة فقط	موافق	موافق

البطاقة المؤقتة: فترة إلغاء تنشيط جميع البطاقات على الفور	موافق	موافق
البطاقة المؤقتة: تنشيط البطاقات تلقائيًا بعد فترة محددة	موافق	موافق
البطاقة المؤقتة: إلغاء تنشيط البطاقات وتفعيلها تلقائيًا	موافق	موافق
بطاقات الإنذار	غير مدعومة	موافق
وضع المكتب	غير مدعومة (*)	غير مدعومة (*)
زائر	من الممكن أن تظل البيانات البيومترية للزائر الأول معينة إلى البطاقة.	من الممكن أن تظل البيانات البيومترية للزائر الأول معينة إلى البطاقة.
مراقب	غير مدعومة	لا تدعم البيانات البيومترية. البطاقة تعمل.
بطاقة وقوف السيارات	موافق	موافق
كود PIN	غير مدعومة (*)	غير مدعومة (*)
التحقق من الصحة بواسطة طرف ثالث	لا يوجد كود PIN (*)	لا يوجد كود PIN (*)
(*) قارئ IDEMIA غير قابل للاستخدام كقارئ لوحة مفاتيح		

23 تحقيق معايير EN 60839

المقدمة

EN 60839 هي مجموعة من المعايير الأوروبية الدولية للأجهزة والبرامج التالية:

- أنظمة الإنذار والأمن الإلكتروني
- أنظمة التحكم في الدخول الإلكتروني

لضمان توافق نظام التحكم في الدخول الخاص بك مع هذا المعيار، قد تحتاج إلى تكييف أجزاء من التكوين. تحتوي القائمة التالية على أهم الأجزاء. للحصول على القائمة الكاملة، يرجى الرجوع إلى المعيار المعتمد في بلدك.

متطلبات استخدام AMS 4.0 كنظام EN 60839 معتمد من الدرجة الثانية

- يفي النظام بمتطلبات منع العودة العمومية من حيث استخدام منطقة واحدة لكل MAC.
- تعتمد مناطق أوقات الاستخدام المختلفة لنظام AMS على عدد وحدات MAC. يمكن استخدام منطقة زمنية منفصلة لكل وحدة MAC.
- يجب ألا تمنع الأسلاك في نقاط تلامس الباب فتح الباب للإخلاء في حالات الطوارئ المشغلة بواسطة نظام منع الحريق أو الاقتحام.
- تستخدم أجهزة قراءة OSDP فقط التشفير على واجهة RS485.
- يجب التحكم بدقة في الوصول إلى وضع التكوين. يمكن تحقيق ذلك، على سبيل المثال، عن طريق تحديد موقع أجهزة الكمبيوتر في مناطق آمنة، ومن خلال انقضاء المهلات في جلسات تسجيل الدخول، لا سيما مهلات عدم النشاط على مستوى التطبيق ونظام التشغيل.
- يجب وضع الشبكة والكابلات الكهربائية في منطقة آمنة أو مغلفة في أنابيب.
- يمكن تركيب أجهزة قراءة البطاقات فقط في مناطق غير آمنة؛ ويجب أن تكون جميع الأجهزة الأخرى في مناطق آمنة.
- يجب تعيين الحد الأدنى لطول رموز PIN للتحقق من بيانات الاعتماد البيومترية أو المادية إلى 4 على الأقل.
- يجب تعيين الحد الأدنى لطول رموز PIN إلى 8 على الأقل.
- يجب مزامنة كمبيوتر الخادم الرئيسي وخوادم الاتصال وخوادم MAC والعملاء مع خادم وقت الشبكة.
- يجب تمكين مراقبة الطاقة على وحدات التحكم في الوصول المحلية (مثل وحدات AMC).
- لا يُسمح بتشغيل وحدات التحكم في الوصول المحلية (مثل وحدة AMC) دون اتصال بالإنترنت إلا أثناء حالات فشل الشبكة. على سبيل المثال ، معلمة AMC **مهلة المضيف** يجب عدم تعيينها إلى 0.

قواعد قوة كلمة المرور

- يجب أن يكون الحد الأدنى لطول كلمة المرور 5 من الحروف على الأقل.

24 تعريف تخويلات وملفات تعريف الوصول

24.1 إنشاء تخويلات الوصول

مسار مربع الحوار
القائمة الرئيسية > **بيانات النظام** > **التخويلات**

الإجراء

1. امسح حقول الإدخال عن طريق النقر فوق الزر **جديد** في شريط الأدوات.
أو انقر فوق **نسخ** لإنشاء تخويل جديد استنادًا إلى تخويل موجود.
2. أدخل اسمًا فريدًا للتخويل
3. (اختياري) أدخل وصفًا
4. (اختياري) حدد نموذج الوقت لضبط هذا التخويل
5. (اختياري) اختر **حد عدم النشاط** من القائمة.
إنها فترة محددة الوقت تتراوح من 14 إلى 365 يومًا. إذا لم يتمكن المستفيد من هذا التخويل من استخدامه خلال الفترة المحددة، فسيخسره. وفي كل مرة يقوم فيها المستفيد من استخدام التخويل، يبدأ المؤقت من الصفر من جديد.
6. (إلزامي) عيّن **مدخلاً** واحدًا على الأقل.
يتم ذكر المداخل الموجودة على علامات تبويب مختلفة، بحسب نماذج الأبواب.
(عام) **المدخل**، **إدارة الوقت**، **المصعد**، **ساحة الانتظار**، **تفعيل اكتشاف الاقتحام**.
حدد مداخل فردية من القوائم على مختلف علامات التبويب، كما سيرد وصفه أدناه.
أو استخدم الزرين **تعيين الكل** و**إزالة الكل** على كل علامة تبويب.
   - على علامة تبويب **المدخل**، حدد أحد المداخل عن طريق تحديد خانة اختيار واحدة أو خانتي الاختيار **داخل** أو **خارج**
   - على علامة تبويب **إدارة الوقت** (لأجهزة قراءة الوقت والحضور) حدد أحد المداخل عن طريق تحديد خانة اختيار واحدة أو خانتي الاختيار **داخل** أو **خارج**
   - على علامة تبويب **المصعد**، حدد مختلف الطوابق
   - على علامة تبويب **ساحة الانتظار** ، حدد انتظار ومنطقة انتظار
   - على علامة تبويب **تفعيل اكتشاف الاقتحام**، حدد **مفعّل** أو **معطّل**.
7. حدد جهاز MAC المناسب من القائمة.
8. انقر فوق "حفظ" لحفظ التخويل.

إشعار!
سوف يتأثر المستفيدون الحاليون من هذه التخويلات عند إدخال تغييرات لاحقة على التخويلات، إلا إذا كان ملف التعريف الذي يضبطها مؤمنًا.
مثال: إذا تم خفض حد عدم النشاط من 60 يومًا إلى 14 يومًا، فسيخسر جميع الأشخاص التخويل في حال عدم استخدامهم له خلال فترة الأربعة عشر (14) يومًا الماضية.
استثناء: إذا كان التخويل جزءًا من ملف تعريف وصول **مقفل** لهوية موظف (نوع الشخص)، فإن الأشخاص من هذا النوع لن يتأثروا بحدود عدم النشاط على التخويل. يمكن تعيين أقفال ملف التعريف باستخدام خانة الاختيار التالية.
القائمة الرئيسية > **بيانات النظام** > جدول **أنواع الأشخاص** >: خانة الاختيار **معرّفات الموظفين المحددة مسبقًا** >: **تم تأمين ملف التعريف**

24.2 إنشاء ملفات تعريف الوصول

ملاحظة: استخدام ملفات تعريف الوصول لتجميع التخويلات
لتمكين التناسق والملاءمة، لا يتم تعيين تخويلات الوصول بشكل فردي، ولكن يتم تجميعها عادةً في **ملفات تعريف الوصول** ويتم تعيينها على هذا الشكل.
- عميل ACE: **بيانات النظام** > **ملفات تعريف الوصول**

– القائمة الرئيسية: **بيانات النظام** > **ملفات تعريف الوصول**

الشروط الأساسية

تم تعريف تخويلات الوصول بشكل مسبق في النظام.

الإجراء

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

أو انقر فوق **نسخ** لإنشاء ملف تعريف جديد استنادًا إلى ملف تعريف موجود.

2. أدخل اسمًا فريدًا لملف التعريف.
3. (اختياري) أدخل وصفًا
4. (اختياري) حدد خانة الاختيار **ملف تعريف الزائر** بحيث يقتصر ملف التعريف هذا على الزائرين
5. (اختياري) عيّن قيمة في **المدة القياسية للصلاحية**.
   – إذا لم يتم تعيين قيمة، فسيبقى ملف التعريف غيّر معين إلى أجل غير مسمى.
   – إذا تم تعيين قيمة، فسيتم استخدامها عندئذٍ لحساب تاريخ انتهاء الصلاحية لأي تعيين لاحق لملف التعريف.
6. (إلزامي) عيّن **تخويلاً** واحدًا على الأقل:
   ستجد التخويلات المتوفرة للتعيين مدرجة على الجانب الأيسر.
   وستجد التخويلات المعيّنة مدرجة على الجانب الأيمن.
   حدد العناصر وانقر فوق الأزرار بين القوائم لنقل العناصر من قائمة إلى أخرى.
   – يعيّن العنصر المحدد.
   – يلغي تعيين العنصر المحدد.
7. انقر فوق "حفظ" لحفظ ملف التعريف.

25 إنشاء وإدارة بيانات الموظفين

مسار مربع الحوار

القائمة الرئيسية > **بيانات الموظفين** > <مربعات حوار فرعية>

الإجراء العام

1. في مربع الحوار الفرعي **الأشخاص**، أدخل بيانات هوية الشخص.
2. في مربع الحوار الفرعي **البطاقات**:
   - عيّن ملفات تعريف الوصول أو تخويلات وصول فردية.
   - عيّن نموذج وقت، إذا لزم الأمر.
   - عيّن بطاقة.
3. في مربع الحوار الفرعي **رمز PIN**: عيّن رمز PIN، إذا لزم الأمر.
4. في مربع الحوار الفرعي **طباعة بطاقات التعريف**، اطبع البطاقة.

في **الزائرين** تابع كما يلي:

- أدخل البيانات الشخصية في مربع حوار **الزائرون** من قائمة **الزائرون** وعيّن مرافقًا (ملاحظًا) إذا لزم الأمر.

إشعار!

لا يُشترَط تعيين بطاقات الهوية وتخويلات الوصول في وقت واحد. ولذلك؛ يمكن تعيين بطاقات هوية للأشخاص بدون تعيين تخويلات وصول أو العكس. غير أنه لا يُسمَح بأي وصول لهؤلاء الأشخاص في كلتا الحالتين.

عملية المسح الضوئي للبطاقات

عند إجراء مسح ضوئي للبطاقات في أجهزة القراءة، ينفذ القارئ عددًا من عمليات الفحص.

- هل البطاقة صالحة ومسجّلة في النظام؟
- هل حامل البطاقة محظور في الوقت الحالي (معطّل في النظام)؟
- هل يمتلك حامل البطاقة تخويل الوصول للدخول في هذا الاتجاه؟
- هل تخويل الوصول مكاني - زمني؟ إذا كان الأمر كذلك، فهل يقع وقت المسح الضوئي ضمن الفترات المعيّنة بواسطة نموذج الوقت؟
- هل تخويل الوصول نشط؛ بمعنى أنه غير **منتهي الصلاحية** أو **محظور** (معطّل)؟
- هل يخضع حامل البطاقة لنموذج وقت؟ إذا كان الأمر كذلك، فهل يقع وقت المسح الضوئي ضمن الفواصل الزمنية المحددة؟
  الشرط الأساسي: يجب تمكين عمليات فحص نموذج الوقت في القارئ المعني.
- هل حامل البطاقة موجود في الموقع الصحيح بحسب مراقبة تسلسل الوصول؟
  الشرط الأساسي: تمكين مراقبة تسلسل الوصول في القارئ المعني.
- هل تم تحديد حد أقصى لعدد الأشخاص في المنطقة الوجهة لهذا القارئ، وهل تم بلوغ هذا الرقم بالفعل؟
- في حال تمكين مراقبة تسلسل الوصول، بما في ذلك منع العودة: هل تخضع هذه البطاقة للمسح الضوئي في القارئ قبل انقضاء وقت الحظر المعيّن بواسطة منع العودة؟
- هل يلزم إدخال رمز PIN إضافي؟ **الشرط الأساسي**: القارئ يشتمل على لوحة مفاتيح.
- إذا كان هناك مستوى تهديد قيد التشغيل، فهل يشتمل **ملف تعريف أمان الشخص** الخاص بحامل البطاقة على **مستوى أمان** يكافئ على الأقل مستوى أمان القارئ عند مستوى التهديد هذا؟

25.1 الأشخاص

يذكر الجدول التالي البيانات التي تظهر بشكل افتراضي في مربع حوار **الأشخاص**. مربعات الحوار قابلة للتخصيص إلى حدٍ بعيد. راجع القسم **الحقول المخصصة لبيانات الموظفين**.

تعتبر كل الحقول تقريبًا حقولاً اختيارية. أما بالنسبة إلى الحقول الإلزامية، فقد تم تعليمها بشكل واضح بواسطة تسميات مسطرة في واجهة المستخدم.

علامة التبويب	اسم الحقل
رأس مربع الحوار	الاسم

	الاسم الأول
	اسم الولادة (أو اسم العائلة قبل الزواج في بعض الثقافات)
	رقم الموظف
	تاريخ الميلاد
	هوية الموظف (المعروف أيضًا بنوع الشخص)
	الجنس
	الشركة
	المسمى الوظيفي
	رقم بطاقة الهوية
	رقم رخصة السيارة
العنوان	الرمز البريدي (أو رمز Zip في بعض الثقافات)
	رقم الشارع
	البلد، الولاية
	الجنسية
بيانات الاتصال	رقم هاتف آخر
	هاتف الشركة
	فاكس الشركة
	الهاتف المحمول
	الهاتف
	البريد الإلكتروني
	عنوان صفحة الويب
بيانات إضافية خاصة بالشخص	اسم شخص مركب (اسم إضافي يُستخدم في الكثير من الثقافات)
	مكان الميلاد
	الحالة الاجتماعية
	بطاقة الهوية الرسمية
	رقم بطاقة الهوية
	صالحة حتى
	الطول
بيانات إضافية خاصة بالشركة	القسم
	الموقع
	مركز التكلفة
	المسمى الوظيفي
	الملاحظ (المرافق)
	سبب الزيارة

	ملاحظات
ملاحظات	(توفير حقل نصي ذي شكل حر للملاحظات حول الشخص.
معلومات إضافية	10 حقول قابلة للتعريف من قِبل المستخدم
التوقيع	أخذ صور للتواقيع وإعادة تسجيلها وحذفها
بصمات الأصابع	أخذ صور بصمات الأصابع وإعادة تسجيلها وحذفها واختبارها كبيانات اعتماد بيومترية تعيين بعض بصمات الأصابع للإشارة إلى الضغط.

راجع

– الحقول المخصصة لبيانات الموظفين, الصفحة *125*

25.1.1 خيارات مراقبة البطاقة أو مراقبة المبنى

نظرة عامة

استخدم **مراقبة البطاقة** لمنح حاملي البطاقات القدرة على تنشيط مخرج عام أو مخرجين عامين من مخارج وحدة التحكم في الوصول بواسطة بطاقتهم. يمكنك تعيين القدرة إلى حامل البطاقة عن طريق تحديد خانة الاختيار **مراقبة المبنى** في مربع حوار **الأشخاص**. تعتبر خانات الاختيار **مراقبة المبنى** (أو **مراقبة البطاقة**) بمثابة حقول مخصصة تظهر على علامة تبويب **مراقبة البطاقة** التابعة للشخص بشكل افتراضي، ولكن يمكن وضعها في أي مكان آخر.

هناك مهمتان رئيسيتان لخيار مراقبة المبنى وسيرد وصفهما أدناه:

– تكوين خانة الاختيار: امنحها تسمية مناسبة، و(إذا لزم الأمر) موضعًا على علامة تبويب أخرى في مربع حوار **الأشخاص**.
– تعيين الوظيفة إلى مخرج على وحدة التحكم في الوصول AMC وخانة اختيار.

الشروط الأساسية

– يكون المخرج على وحدة التحكم في الوصول موصولاً بطريقة كهربائية بالجهاز الذي يجب أن تقوم البطاقة بتنشيطه.

مسار مربع الحوار

– مستعرض تكوين BIS > **البنية الأساسية** > **حقول ACE مخصصة** > علامة التبويب **مراقبة البطاقة**
– القائمة الرئيسية AMS > **التكوين** > **خيارات** > **حقول مخصصة** > علامة التبويب **مراقبة البطاقة**

تكوين خانات الاختيار

1. في صفحة **الحقول المخصصة**، حدد علامة تبويب **التفاصيل** في الجزء العلوي.
2. حدد موقع وظيفة **مراقبة المبنى**، 1 أو 2، التي تريد استخدامها.
3. استبدل التسمية باسم مناسب (مستحسن). يمكنك وضع خانة الاختيار في مكان آخر على علامة تبويب **مراقبة البطاقة**، إذا لزم الأمر. راجع القسم **معاينة الحقول المخصصة وتحريرها** في الارتباط أدناه، للحصول على مزيد من الإرشادات المفصلة.

تعيين الوظيفة إلى مخرج على وحدة التحكم في الوصول وخانة اختيار.

راجع القسم **معلمات وإعدادات AMC** في الارتباط أدناه.

1. في **محرر الجهاز**، في شجرة الأجهزة، حدد وحدة التحكم في الوصول AMC التي تريد استخدام إشارة المخرج الخاصة بها.
2. على علامة تبويب **المخارج**، في الجزء العلوي، حدد المخرج الذي تريد استخدامه.
3. في الجزء الأوسط، **بيانات المخرج**، حدد النوع **25, مراقبة البطاقة**
4. انقر فوق الزر **>** لإضافة المخرج إلى الجزء السفلي.
5. في الجزء السفلي، العمود **Param11**، حدد تسمية وظيفة مراقبة المبنى التي حددتها في الإجراء السابق **تكوين خانات الاختيار**.
6. احفظ شجرة الأجهزة.

راجع
- معلمات وإعدادات *AMC*, الصفحة *53*
- معاينة وتحرير الحقول المخصصة, الصفحة *125*

25.1.2 معلومات إضافية: تسجيل المعلومات المعرّفة من قِبل المستخدم

استخدم علامة التبويب **معلومات إضافية** لتعريف الحقول الإضافية التي لم يتم توفيرها على علامات التبويب الأخرى. إذا لم يتم تعريف حقول إضافية، فستبقى علامة التبويب فارغة.

25.1.3 تسجيل التواقيع

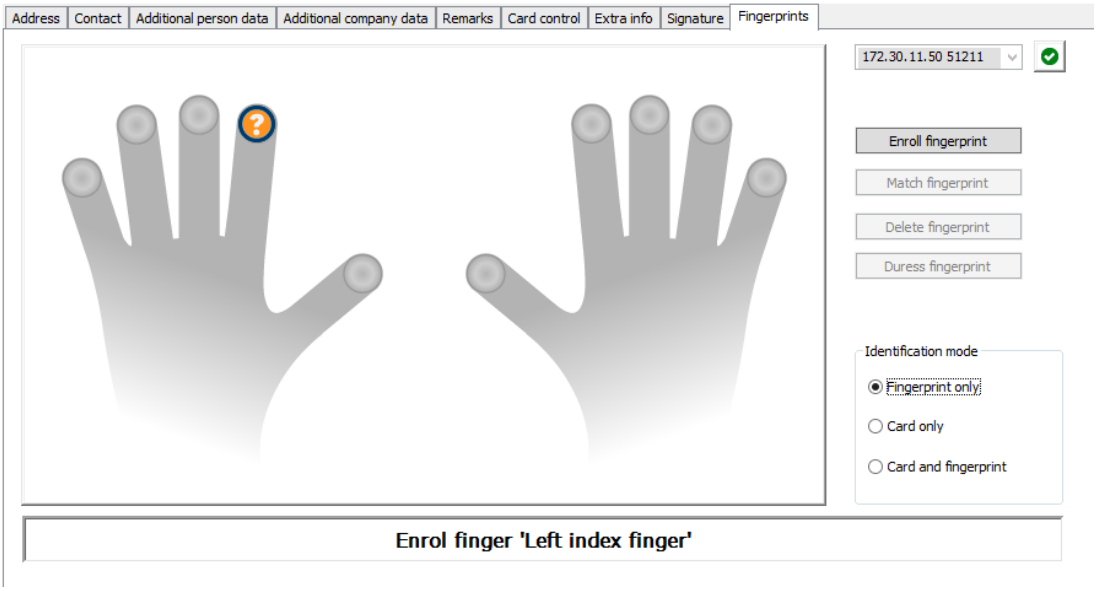
يلزم توصيل لوحة أخذ صورة التوقيع من شركة Signotec وتكوينها في النظام لأخذ صورة التواقيع. في حال وجود أي شك لديك، يمكنك استشارة مدير النظام.

1. انقر فوق علامة التبويب **التوقيع**
2. انقر فوق الزر **أخذ صورة التوقيع** لتسجيل توقيع جديد.
3. وقّع مباشرة على لوحة أخذ الصور باستخدام قلمها الخاص.
4. انقر قوق زر علامة الاختيار على لوحة أخذ الصور للتأكيد.

يظهر التوقيع الجديد الآن على الشاشة (انقر على التوقيع للحصول على عرض مكبّر له).

إجراءات ذات صلة:
- انقر فوق الزر **أخذ صورة التوقيع** من أجل الكتابة فوق توقيع موجود بالفعل.
- انقر فوق الزر **حذف التوقيع** من أجل حذف توقيع موجود بالفعل.

25.1.4 تسجيل بيانات بصمة الإصبع



الشروط الأساسية
- يلزم تكوين قارئ بصمات أصابع واحد أو أكثر في المداخل لتنفيذ تحكم في الوصول بيومتري.
- مهم: تتلقى أجهزة القراءة هذه بشكل دوري بيانات البطاقات وبصمات الأصابع من الخادم وتقوم بتخزينها. وبالتالي تحدد الإعدادات الموجودة على كل قارئ فردي بيانات الاعتماد التي يمكن قبولها. وهي تتجاوز أي إعدادات تم تكوينها هنا للشخص.
- من أجل استخدام بصمات الأصابع كوسيلة (أو بديل) للتحقق من المصادقة القائمة على البطاقة، يلزم إجراء مسح ضوئي لبصمات أصابع جميع حاملي البطاقات.
- يتواجد المسجل أمام قارئ بصمات أصابع تم توصيله وتكوينه لمحطة عملك. يجب **ألا** يكون قارئ تسجيل بصمة الإصبع قارئ وصول.

- بصفتك مشغّل، ستتواصل بشكل مباشر مع المسجل، أي الشخص الذي يجب تسجيل بصمات أصابعه كبيانات اعتماد بيومترية لمنحه حق الوصول.
- لقد تآلفت مع عملية وضع إصبعك بشكل متكرر على القارئ المحدد المستخدم، للسماح له بأخذ صورة لبصمات أصابعك بطريقة فعالة.

الإجراء المتعلق بتسجيل بصمة الإصبع للحصول على حق الوصول

1. انتقل إلى مربع حوار بصمات الأصابع: علامتي التبويب **بيانات الموظفين** > **الأشخاص** >:**بصمات الأصابع** واعمل على إنشاء المسجل أو البحث عنه في قاعدة البيانات.
2. اسأل المسجل عن الإصبع الذي يرغب في استخدامه للوصول العادي عند قارئ بصمات الأصابع.
3. حدد الإصبع المناظر في مخطط اليدين.
   النتيجة: يتم تعليم بصمة الإصبع بواسطة علامة استفهام.
4. انقر فوق الزر **تسجيل بصمة الإصبع**.
5. قدّم للمسجل الإرشادات المتعلقة بكيفية وضع إصبعه على القارئ.
   يمكن قراءة إرشادات موضحة مع أمثلة من جزء مربع الحوار تحت مخطط اليدين، ولكن قد تختلف الإجراءات قليلاً من قارئ إلى آخر بحسب نوع القارئ.
6. إذا نجحت عملية تسجيل بصمة الإصبع، فستظهر نافذة تأكيد.
7. حدد **وضع تعريف**؛ يحدد هذا بيانات الاعتماد التي سيطلبها قارئ بصمات الأصابع من المسجل عندما يطلب حق الوصول. تجدر الإشارة إلى أن الوضع الذي تم تعيينه هنا لن يدخل حيز التنفيذ إلا إذا تم تحديد معلمة القارئ **تحقق يعتمد على الشخص**.
   الخيارات هي:
   - **بصمة الإصبع فقط** - يتم استخدام فقط الماسح الضوئي لبصمة الإصبع في القارئ.
   - **البطاقة فقط** - يتم استخدام فقط الماسح الضوئي للبطاقة في القارئ.
   - **البطاقة وبصمة الإصبع** - يتم استخدام الماسحين الضوئيين في القارئ. يتعين على المسجل تقديم البطاقة والإصبع الذي اختاره إلى القارئ، للحصول على حق الوصول.
8. انقر فوق الزر **قبول** لتخزين بصمة إصبع المسجل ووضع تعريفه.
9. انقر فوق (حفظ) لتخزين بصمة إصبع المسجل ووضع تعريفه.

إشعار!

إعدادات القارئ تتجاوز إعدادات الشخص
تجدر الإشارة إلى أن وضع التعريف الذي تم اختياره في مربع حوار بصمة الإصبع يعمل فقط إذا تم تكوين قارئ بصمات الأصابع بحد ذاته باستخدام الخيار **التحقق المعتمد على الشخص** في محرر الجهاز. في حال وجود أي شك لديك، يمكنك استشارة مسؤول النظام.

الإجراء المتعلق بتسجيل بصمة الإصبع للإشارة إلى الضغط

الشروط الأساسية:

- بإمكان أجهزة قراءة بصمات الأصابع إرسال فقط إشارات تفيد بالتعرض للضغط إذا تم تكوينها في **محرر الجهاز** مع الإعداد التالي: علامة التبويب
  الشبكة وأوضاع التشغيل > **القوالب على الخادم** > **البطاقة وبصمة الإصبع**
- تم تسجيل وتخزين بصمة إصبع واحدة على الأقل للمسجل.
- قارئ بصمة الأصابع متصل بالإنترنت. عندما يكون القارئ غير متصل بالإنترنت، يتعذر عليه، بطبيعة الحال، أن يرسل إلى النظام إشارة تفيد بالتعرض للضغط.

1. اطلب من المسجل اختيار الإصبع الذي يريد استخدامه للإشارة إلى الضغط، أي، في حال تم الضغط عليه من قبل شخص غير مخوّل لاستخدام قارئ بصمات الأصابع.
2. كرر إجراء تسجيل بصمة الإصبع، كما ورد وصفه أعلاه، لهذا الإصبع.
3. عند تسجيل بصمة الإصبع الثانية بنجاح، حددها في مخطط اليدين، وانقر فوق الزر **إصبع الضغط**.
   يتم تعليم الإصبع الذي تم تعيينه كإصبع ضغط بواسطة علامة تعجب في مخطط اليدين.

إذا استخدم المسجل فيما بعد إصبع الضغط في قارئ بصمات الأصابع، ولم يكن القارئ في وضع عدم الاتصال، فإن النظام سيشير إلى الضغط للمسجل، باستخدام نافذة منبثقة.

الإجراء المتعلق باختبار بصمات الأصابع المخزنة

1. في مخطط اليدين، حدد بصمة الإصبع التي تريد اختبارها.
2. قدّم للمسجل الإرشادات المتعلقة بوضع هذا الإصبع على القارئ.
3. انقر فوق الزر **مطابقة بصمة الإصبع** button

النتيجة: ستظهر نافذة منبثقة تؤكد ما إذا كانت بصمة الإصبع المخزنة تطابق أم لا بصمة الإصبع الموضوعة على القارئ. لاحظ أنه قد يتعين عليك تكرار هذا الإجراء لتقليل احتمال حدوث تنبيه خاطئ.

الإجراء المتعلق بحذف بصمات الأصابع المخزنة

1. في مخطط اليدين، حدد بصمة الإصبع التي تريد حذفها.
2. انقر فوق الزر **حذف بصمة الإصبع**.
3. انتظر صدور تأكيد الحذف.

25.1.5 تسجيل بيانات عروق راحة اليد

التحقق البيومتري

يعني التحقق البيومتري عدم السماح لحامل بطاقة بالدخول إلا بعد تقديم إثبات بيومتري بأنه المالك الحقيقي لبطاقة الهوية (أو بيانات اعتماد مكافئة).

ويجب تكوين ما لا يقل عن جهازي قراءة بيومتريين في النظام، قبل السماح بالاستخدام الربحي للتحقق البيومتري من الهويات:

- قارئ متصل بمحطة عمل مشغّل لتسجيل البيانات البيومترية.
- قارئ واحد أو أكثر عند المداخل للتحقق من هويات حاملي البطاقات.

الشروط الأساسية:

- قارئ عروق راحة اليد مُرخّص ومُكوّن في برنامج الشركة المصنّعة. لقد قمت بتعريف ما يلي:
  - عنوان IP الخاص بالقارئ
  - معرّف القارئ (1 أو 2) للتمييز بين أجهزة القراءة في وحدة التحكم البيومترية نفسها.
- سجلت بتأنٍ كلمة مرور القارئ التي قدمها مثبت القارئ.

تكوين قارئ عروق راحة اليد على محطة عمل مشغّل
مسار مربع الحوار

- مستعرض تكوين BIS > **البنية الأساسية** > **قارئ بطاقة ACE**

الإجراء

1. في جزء **محطات العمل**، حدد محطة العمل التي تريد أن يتصل بها قارئ عروق راحة اليد.
2. في جزء **محطات العمل**، انقر فوق أيقونة علامة زائد الخضراء.
3. أدخل البيانات التالية في جزء **قارئ البطاقة**:

- **النوع:** حدد **مستشعر عروق راحة اليد** من القائمة المنسدلة.
- **عنوان IP:** أدخل عنوان IP الخاص بوحدة التحكم في قارئ عروق راحة اليد.
- **معرّف القارئ:** حدد معرّف قارئ عروق راحة اليد من القائمة المنسدلة.
- **كلمة المرور:** أدخل كلمة المرور التي قدمها مثبت القارئ.

4. انقر فوق **تطبيق** لتطبيق التغييرات وحفظها أو
   انقر فوق **تجاهل** لإلغاء التغييرات.

إنشاء وحدة تحكم بيومترية في شجرة الأجهزة
مسار مربع الحوار
– مستعرض تكوين BIS > **الاتصالات**

الإجراء
1. في علامة تبويب **بيانات الجهاز**، انقر بزر الماوس الأيمن فوق جهاز MAC وحدد **وحدة تحكم بيومترية جديدة** من قائمة السياق.
2. أدخل البيانات المطلوبة في مربع حوار وحدة تحكم PCS:
– **الاسم**: أدخل اسم وحدة التحكم.
– **الوصف**: أدخل وصفًا.
– **عنوان IP**: أدخل عنوان IP الخاص بوحدة التحكم في قارئ عروق راحة اليد.
3. انقر فوق **تطبيق** لتطبيق التغييرات وحفظها أو
انقر فوق **تجاهل** لإلغاء التغييرات المُطبّقة أو إزالتها.

إضافة قارئ عروق راحة يد إلى وحدة تحكم بيومترية

1. في علامة تبويب **بيانات الجهاز**، وسّع شجرة الأجهزة وانقر بزر الماوس الأيمن فوق **جهاز وحدة تحكم PCS** وحدد **قارئ عروق راحة يد جديد** من قائمة السياق.
2. أدخل البيانات المطلوبة في مربع حوار عروق راحة يد PCS:
– **الاسم:** أدخل اسم قارئ عروق راحة اليد.
– **الوصف:** أدخل وصفًا (اختياري).
– **القسم:** حدد قسمًا.
– **عنوان الناقل / المحطة الطرفية للقارئ:** أدخل معرّف القارئ، 1 أو 2.
– **عدد مرات إعادة المحاولة**: أدخل الحد الأقصى لعدد مرات إعادة المحاولة المسموح به.
– **كلمة المرور:** أدخل كلمة المرور التي قدمها مثبت القارئ.
3. انقر فوق **تطبيق** لتطبيق التغييرات وحفظها أو
انقر فوق **تجاهل** لإلغاء التغييرات المُطبّقة أو إزالتها.

تسجيل نمط عروق راحة يد للتحقق من الهويات

الشروط الأساسية:
– يتم تكوين قارئ عروق راحة اليد على محطة عمل المشغّل لديك.
– يتم تشغيل قارئ عروق راحة اليد وتوصيله بالشبكة.
يظهر قارئ عروق راحة اليد أضواءً زرقاء ثابتة.
– أنت على دراية بإرشادات الشركة المصنّعة بخصوص عملية التسجيل باستخدام قارئ عروق راحة اليد.
– تم تعريف المسجل بالفعل كحامل بطاقة في النظام.

الإجراء
1. ابدأ تشغيل عميل ACE (مدير مربع الحوار)، أو أغلقه أو أعد تشغيله إذا كان قيد التشغيل بالفعل.
2. انتقل إلى علامة التبويب **بيانات الموظفين** > **الأشخاص** >: **عروق راحة اليد**
– تعني أيقونة علامة التجزئة الخضراء بجانب زر **تسجيل عروق راحة اليد** أن قارئ عروق راحة اليد متصل.
3. قم بتحميل سجل حامل البطاقة المطلوب في مربع الحوار الرئيسي.
4. اسأل المسجل عن راحة اليد التي يرغب في استخدامها في قارئ عروق راحة اليد.
5. حدد راحة اليد المناظرة في مخطط اليدين.
يتم تعليم راحة اليد بواسطة علامة استفهام.
6. قدّم للمسجل الإرشادات المتعلقة بكيفية وضع راحة يده على نموذج قارئ عروق راحة اليد. (قد تتطلب الخطوات التالية بعض التعديل حسب الطراز والنوع).

7. انقر فوق زر **تسجيل عروق راحة اليد**.
تتغير أضواء قارئ عروق راحة اليد للإشارة إلى الاستعداد للقراءة.
- ضَع راحة اليد على قارئ عروق راحة اليد.
- انتظر حتى تومض أضواء القارئ
- أبعد راحة اليد عن القارئ لمدة ثانية تقريبًا، ثم ضَعها من جديد.
- إذا تكرر وميض أضواء القارئ، فكرّر الخطوات السابقة حتى يظهر القارئ إما أضواء خضراء أو حمراء ثابتة.
  - **خضراء**: تم تسجيل نمط عروق راحة اليد بنجاح.
  - **حمراء**: لم يتم تسجيل نمط عروق راحة اليد. تأكد من أن المسجل اتبع إرشادات الشركة المصنّعة وكرّر الإجراء.
8. عند تسجيل نمط عروق راحة اليد بنجاح، تتحول أيقونة علامة الاستفهام في مخطط اليدين إلى أيقونة علامة تجزئة خضراء.
9. انقر فوق (حفظ) لتخزين نمط عروق راحة اليد الذي تمت قراءته.

اختبار نمط عروق راحة يد تم تخزينه

1. انتقل إلى علامة التبويب **بيانات الموظفين** > **الأشخاص** >: **عروق راحة اليد**
2. قم بتحميل سجل حامل البطاقة المطلوب في مربع الحوار الرئيسي.
3. في مخطط اليدين، حدد اليد التي تريد اختبارها.
4. انقر فوق زر **مقارنة عروق راحة اليد**.
تتغير أضواء قارئ عروق راحة اليد للإشارة إلى الاستعداد للقراءة
- ضَع راحة اليد على قارئ عروق راحة اليد.
- انتظر حتى يظهر القارئ إما أضواء خضراء أو حمراء ثابتة.
  - **خضراء**: يطابق نمط عروق راحة اليد النمط المُخزَّن.
  - **حمراء**: لا يطابق نمط عروق راحة اليد النمط المُخزَّن لك.
تأكد من أن المسجل اتبع إرشادات الشركة المصنّعة وكرّر الإجراء إذا لزم الأمر.

حذف نمط عروق راحة يد تم تخزينه

1. انتقل إلى علامة التبويب **بيانات الموظفين** > **الأشخاص** >: **عروق راحة اليد**
2. قم بتحميل سجل حامل البطاقة المطلوب في مربع الحوار الرئيسي.
3. في مخطط اليدين، حدد اليد التي تريد حذف نمط عروق راحتها.
4. انقر فوق الزر **حذف عروق راحة اليد**.
5. انتظر ظهور مربع حوار يؤكد الحذف.

إشارات أضواء LED

لاحظ أن إشارات الأضواء قد تختلف حسب الطراز والنوع.
- **زرقاء (وامضة):** الجهاز قيد التشغيل ولكنه غير متصل بالشبكة.
- **زرقاء (ثابتة):** الجهاز قيد التشغيل ومتصل بالشبكة.
- **زرقاء وباهتة (ثابتة):** الجهاز مستعد لقراءة نمط عروق راحة يد.
- **وميض تحت راحة يد المسجل**: إشارة لإبعاد راحة اليد عن القارئ لمدة ثانية تقريبًا، ثم وضعها من جديد.
- **خضراء (ثابتة)**: تم التعرّف على نمط عروق راحة اليد.
- **حمراء (ثابتة)**: لم يتم التعرّف على نمط عروق راحة اليد.

استخدام قارئ عروق راحة يد عند مدخل

إشعار!
القارئ غير متصل بالإنترنت
إذا كان قارئ عروق راحة اليد يظهر أضواء زرقاء وامضة، فإنه يكون غير متصل بالشبكة ولن يعمل. أعلِم موظفي الأمن.

1. ضَع بطاقتك على قارئ البطاقات.
إذا كان التحقق بواسطة نمط عروق راحة اليد مطلوبًا، فسيصدر قارئ عروق راحة اليد الآن إشارة بالاستعداد للقراءة.
2. ضَع راحة يدك على قارئ عروق راحة اليد حتى يظهر أضواء خضراء أو حمراء.
- **خضراء**: يطابق نمط عروق راحة اليد النمط المُخزَّن لك. يتم منح حق الوصول.
- **حمراء**: لا يطابق نمط عروق راحة اليد النمط المُخزَّن لك. يتم رفض حق الوصول.

25.2 الشركات

- يمكن استخدام مربع الحوار هذا لإنشاء بيانات شركات جديدة وتعديل بيانات شركة موجودة بالفعل أو حذفها.
- يلزم إدخال اسم الشركة واسمها المختصر. ويجب أن يكون الاسم المختصر فريدًا.
- إذا كان إدخال الشركة إلزاميًا في مربع حوار **الأشخاص**، فأنشئ الشركة في مربع الحوار هذا قبل محاولة إنشاء سجلات الموظفين لهذه الشركة.
- لا يمكن حذف الشركات من النظام إذا كانت سجلات الموظفين ما زالت معينة إليها.

25.3 البطاقات: إنشاء وتعيين بيانات الاعتماد والأذونات

يهدف مربع الحوار هذا إلى تعيين **بطاقات** أو **تخويلات وصول** أو مجموعات من تخويلات الوصول تسمى **ملفات تعريف الوصول** إلى سجلات الموظفين.
تُعيَن تخويلات الوصول وملفات تعريف الوصول إلى أشخاص وليس إلى بطاقات.
تتلقى البطاقات الجديدة التي يتم تعيينها إلى شخص تخويلات الوصول المعينة مسبقًا إلى هذا الشخص.

ملاحظة: استخدام ملفات تعريف الوصول لتجميع التخويلات
لتمكين التناسق والملاءمة، لا يتم تعيين تخويلات الوصول بشكل فردي، ولكن يتم تجميعها عادةً في **ملفات تعريف الوصول** ويتم تعيينها على هذا الشكل.
- عميل ACE: **بيانات النظام** > **ملفات تعريف الوصول**
- القائمة الرئيسية: **بيانات النظام** > **ملفات تعريف الوصول**

قائمة البطاقات
تُعرض قائمة البطاقات التي يمتلكها الشخص المحدد في مربع حوار "البطاقات". تشمل السمات الواردة في القائمة:
- نوع استخدام البطاقة.
- علامة تشير إلى ما إذا كانت البطاقة قابلة للاستخدام مع نظام قفل غير متصل تم تكوينه.
- ما إذا كانت البطاقة محظورة بسبب الاستخدام المتكرر لرموز PIN غير صالحة. يتم تمييز هذه الحالة على وجه التحديد.
- تاريخ إنشاء البطاقة
- تاريخ انتهاء صلاحية (تاريخ تحصيل) البطاقة.

ملاحظة: باستطاعة قارئ بطاقات آلي، في حال استخدامه، أن يحجز فعليًا بطاقة منتهية الصلاحية. وإلا، سيتم إبطال البطاقة بكل بساطة.

- تاريخ الطباعة الأخيرة للبطاقة، وعدد البطاقات المطبوعة.
- تفاصيل بيانات الرمز.

الخيار **إدارة عمومية**
يمكن تحرير بيانات الأشخاص الذين لديهم الإعداد **إدارة عمومية** (خانة الاختيار إلى جانب إطار الصورة) فقط من قِبل المشغّلين الذين لديهم الحق الإضافي **مسؤول عمومي**.
البيانات التالية في وضع القراءة فقط للمشغّلين الذين ليس لديهم هذا الحق:
- جميع البيانات في مربع حوار **الأشخاص**، باستثناء علامتي التبويب **ملاحظات، معلومات إضافية** والحقول المخصصة.
- جميع البيانات في مربع الحوار **البطاقات**.
- جميع البيانات في مربع الحوار **رمز PIN**.

يمكن تعيين حق **المسؤول العمومي** هذا في خانة الاختيار التالية:
- قائمة مستعرض تكوين BIS:**الإدارة** > علامة تبويب **المشغّلون** >: خانة الاختيار **إعدادات مشغّل ACE** >: **مسؤول عمومي**.
- القائمة الرئيسية: **التكوين** > **المشغّلون ومحطات العمل** > خانة الاختيار **حقوق المستخدم**>: **المسؤول العمومي**.

25.3.1 تعيين بطاقات إلى أشخاص

المقدمة
يحتاج جميع الأشخاص ضمن نظام التحكم في الوصول إلى بطاقة أو بيانات اعتماد إلكترونية أخرى، يتم تعيينها إلى حاملها في مربع حوار **البطاقات**.
يمكن تعيين أرقام البطاقات يدويًا أو عبر قارئ التسجيل.

مسار مربع الحوار
القائمة الرئيسية > **بيانات الموظفين** > **البطاقات**

الشروط الأساسية
- لقد قمت بتحميل سجل الموظف الذي سيتلقى البطاقة في رأس مربع حوار **البطاقات**.

الإدخال اليدوي لبيانات البطاقة
انقر فوق الزر **تسجيل بطاقة** لتعيين بطاقة هوية إلى شخص ما. عندها يظهر قناع مربع الحوار **تسجيل هوية**. يظهر أحد مربعي حوار الإدخال، وهذا يتوقف على نوع البطاقة ووحدات التحكم وأجهزة القراءة قيد الاستخدام.

أدخل الرقم المطبوع على بطاقة الهوية يدويًا - تتم تعبئة بطاقات الأرقام بالأصفار بشكل تلقائي بحيث يتم تخزينها دائمًا على شكل 12 خانة رقمية. في بعض الأنظمة، لن يتم تعيين أرقام بطاقات هوية جديدة عند ضياع بطاقة الهوية. بدلاً من ذلك، يتم استخدام رقم بطاقة الهوية نفسه، ولكن مع رقم إصدار أعلى.
وتوفر جهة التصنيع رمز البلد ورمز العميل ويجب إدخالهما في ملف التسجيل الخاص بالنظام.
إذا لم يكن رقم الهوية قيد الاستخدام من قِبل النظام، فيمكن تعيينه للشخص. يتم تأكيد التعيين الناجح بواسطة نافذة منبثقة.

استخدام قارئ تسجيل

الشرط الأساسي

– يتم تكوين قارئ التسجيل على محطة العمل.

الإجراء الخاص بالتسجيل

1. انقر فوق الزر ▸ على الجانب الأيمن من الزر **تسجيل بطاقة** لتحديد قارئ تسجيل تم تكوينه.
– لتغيير التحديد على قارئ التسجيل، يجب أن تسجل دخولك إلى مدير حوار ACE كمسؤول.
2. انقر فوق الزر **تسجيل بطاقة** واتبع الإرشادات التي تظهر على الشاشة.
3. بحسب نوع القارئ، يمكنك الآن إدخال تفاصيل البطاقة في مربع الحوار، أو قراءة البيانات من البطاقة عن طريق تقديمها إلى القارئ.

الإجراء الخاص بتغيير البطاقات

1. حدد بطاقة من القائمة.
2. انقر فوق الزر **تغيير البطاقة**.
3. في النافذة المنبثقة
– حدد **استبدال البطاقة** إذا كان البطاقة الأصلية تالفة أو ضائعة بشكل دائم.
– حدد **بطاقة مؤقتة** إذا تغيّر مكان البطاقة الأصلية أو تُركت في البيت، وتحتاج فقط إلى بطاقة بديلة.
– أدخل فترة صلاحية للبطاقة المؤقتة.
– حدد إن كنت تريد إلغاء تنشيط جميع البطاقات الأخرى الآن.
– حدد ما إذا كان يجب إعادة تنشيط البطاقات الأصلية عندما تنتهي صلاحية البطاقة المؤقتة.
4. انقر فوق **موافق** للحفظ.

حذف القائمة

1. حدد بطاقة من القائمة.
2. انقر فوق الزر **حذف بطاقة** لإزالة تعيين شخص إلى بطاقة ما.

ملاحظة: إذا حذفت البطاقة الأخيرة لحامل البطاقة، فستتغير عندئذٍ حالة الشخص إلى **غير مُسجّل** (التسمية الحمراء إلى جانب **مُسجّل** في شريط الحالة). عندئذٍ، لن يعود الشخص خاضعًا لنظام التحكم في الوصول.

25.3.2 طباعة الشارات

الشروط الأساسية

– يجب أن يكون سجل الموظف لحامل البطاقة الجديد موجودًا في النظام.
– محطة عمل تتضمن الأجهزة المتصلة التالية، عادةً عبر USB:
– طابعة شارات
– كاميرا لأخذ صور للهويات.

الإجراء

مسار مربع الحوار

عميل AMS: **بيانات الموظفين** > **طباعة الشارات**

1. قم بتحميل سجل الموظف الذي يجب طباعة بطاقته.
2. في القائمة المنسدلة **التخطيط**، حدد تخطيط البطاقة المطلوب من التخطيطات المخزنة.
3. احصل على صورة معرّف باستخدام أحد الأساليب التالية:
– انقر فوق الزر **أخذ صورة** وحدد الكاميرا المطلوبة من قائمة الكاميرات المتصلة.

- انقر فوق الزر **استيراد صورة** واستخدم إطار الاقتصاص لتحديد جزء الصورة لطباعته على البطاقة.

4. انقر فوق **معاينة** للتأكد من أن البيانات الصحيحة سوف تظهر في التخطيط الصحيح على الشارة.
5. انقر فوق **طباعة** لطباعة الشارة.

الكاميرات المدعومة
جميع أجهزة USB التي يتعرف عليها نظام التشغيل على أنها كاميرا.

25.3.3 علامة تبويب التخويلات

تعيين التخويلات المجمّعة كملفات تعريف الوصول
تعتبر أسهل طريقة لتعيين التخويلات إلى حاملي البطاقات وأكثرها مرونةً تجميعها أولاً في ملفات تعريف الوصول، ثم تعيين ملف التعريف.

- لإنشاء ملفات تعريف الوصول، راجع القسم إنشاء ملفات تعريف الوصول, الصفحة *177*
- لتعيين ملف تعريف الوصول إلى حامل البطاقة هذا، حدد ملف تعريف تم تعريفه من قائمة **ملف تعريف الوصول:**

تعيين تخويلات الوصول بشكل مباشر
على علامة تبويب **التخويلات**:
تظهر كل تخويلات الوصول التي تم منحها إلى الشخص في القائمة إلى اليمين.
تظهر كل تخويلات الوصول المتوفرة للتعين في القائمة إلى اليسار.
حدد العناصر، ثم انقر فوق الأزرار بين القوائم لنقل العناصر من قائمة إلى أخرى.

يعيّن العنصر المحدد.

يلغي تعيين العنصر المحدد.

يعيّن جميع العناصر المتوفرة.

يلغي تعيين جميع العناصر المتوفرة.

الخيار: **إبقاء التخويلات مُعيَنة**
يتوقف تأثير تعيين ملف تعريف الوصول إلى أحد الأشخاص على خانة الاختيار **إبقاء التخويلات مُعيَنة**:

- إذا تم إلغاء تحديد خانة الاختيار، فسيتم **استبدال** أي تحديد أُجري قبل هذا وأي تخويلات وصول تم تعيينها بالفعل عند تعيين ملف التعريف.
- إذا تم تحديد خانة الاختيار، فإن تخويلات ملف التعريف **تُضاف** إلى التخويلات المُعيَنة.

تحديد الفترة الزمنية للتخويلات
استخدم حقول البيانات **صالح من:** و**حتى:** لتحديد أوقات بدء وانتهاء التخويلات وملفات التعريف. إذا لم يتم تعيين أي قيمة، فسيكون التخويل صالحًا على الفور وغير مقيّد بمدة.

انقر فوق لفتح مربع حوار لتعيين مدد تخويلات فردية.

عرض مداخل التخويل
انقر بزر الماوس الأيمن فوق تخويل في أي من القائمتين لعرض قائمة بالمداخل التي تنتمي إليه.

25.3.4 علامة التبويب "بيانات أخرى": الاستثناءات والأذونات الخاصة

تعيين نموذج وقت:
استخدم مربع القائمة **نموذج الوقت** لتحديد ساعات الدخول اليومية لحامل البطاقة، أي، الفترات التي ستقوم خلالها بيانات اعتماد حامل البطاقة بمنح حق الوصول.

استثناء أشخاص من الفحص العشوائي
حدد خانة الاختيار **مُستثنى من الفحص العشوائي** لمنع اختيار هؤلاء الأشخاص بطريقة عشوائية لإخضاعهم لعمليات الفحص عند المداخل والمخارج.

استثناء الأشخاص من عمليات التحقق من رمز PIN
حدد خانة الاختيار **تعطيل التحقق من رمز PIN** لإعفاء هؤلاء الأشخاص من إدخال رموز PIN في أجهزة قراءة رموز PIN خارج ساعات العمل العادية.

إشعار!
يؤثر الاستثناء من رموز PIN في النظام بكامله.
على سبيل المثال، نظرًا لعدم فحص رموز PIN لهؤلاء الأشخاص، فسيتعذر عليهم أيضًا تفعيل أو تعطيل التنبيهات في المداخل في نموذج الباب 10.

زيادة فترة وقت فتح الباب
حدد خانة الاختيار **زيادة فترة وقت فتح الباب** لمنح الأشخاص من ذوي الاحتياجات الخاصة وقتًا إضافيًا (الافتراضي هو 3 مرات) للمرور عبر المدخل قبل إنشاء الحالة **الباب مفتوح لمدة طويلة**.
ملاحظة: يمكن إعادة تعيين عامل التمديد الافتراضي في خصائص MAC في محرر الجهاز.
حدد **إعدادات الوصول العمومي** > **عامل الوقت للأشخاص من ذوي الإعاقات:**

مراقبة الجولة
إن **الجولة** أو **المسار** عبارة عن تسلسل دقيق لأجهزة القراءة تم تحديده في قائمة العميل: **مراقبة الجولة** > مربع الحوار **تحديد المسارات**.
لتعيين جولة إلى حامل بطاقة، حدد خانة الاختيار **مراقبة الجولة**، ثم حدد جولة محددة من القائمة المنسدلة. إذا لم يتم تحديد أي جولة، فستكون خانة الاختيار غير نشطة.
عند تعيين **جولة** إلى حامل بطاقة، تصبح هذه الجولة نشطة فور قيام حامل البطاقة بمسح بطاقته عند أول قارئ في التسلسل. بعد ذلك، يجب استخدام جميع أجهزة القراءة في التسلسل بالترتيب المحدد، حتى اكتمال الجولة. تقضي الاستخدامات النموذجية بفرض تسلسلات وصول دقيقة في البيئات الصناعية النظيفة أو المناطق الخاضعة للمراقبة الصحية أو تلك التي تتميز بمستوى أمان عالٍ.

الإذن بفتح الأبواب
حدد خانة الاختيار للسماح لحامل البطاقة بفتح الأبواب لمدة طويلة، راجع **وضع المكتب**.

راجع
- تخويل الأشخاص تعيين وضع المكتب, الصفحة *191*

25.3.5 تخويل الأشخاص تعيين وضع المكتب

المقدمة
يصف المصطلح وضع المكتب تعليق التحكم في الوصول في مدخل ما خلال ساعات العمل أو المكتب. ويبقى المدخل مقفلاً خلال هذه الساعات، لمنع الوصول العمومي غير المعاق. ينطبق الوضع العادي خارج نطاق هذه الساعات، أي يُمنح حق الوصول إلى الأشخاص الذين يقدمون بيانات اعتماد صالحة للقارئ.
يُعتبر وضع المكتب شرطًا أساسيًا لمرافق البيع بالتجزئة والمرافق التعليمية والطبية.

الشروط الأساسية
لكي يعمل وضع المكتب، يجب تلبية المتطلبات التالية:
في التكوين (شجرة الأجهزة)
- يجب تكوين مدخل واحد أو أكثر للسماح بالفترات الممددة غير المقفلة.
- يجب استخدام قارئ لوحة مفاتيح واحد على الأقل في المدخل.

في العميل (مربعات حوار الأشخاص)
- يجب تخويل حامل بطاقة أو أكثر بإدخال المدخل في وضع المكتب وإخراجه منه.
- يجب أن تكون بطاقاتهم صالحة وتسمح بالوصول إلى المدخل خارج ساعات وضع المكتب.

الإجراءات الخاصة بتخويل الأشخاص تعيين وضع المكتب
الإجراء الخاص بحاملي البطاقات الفرديين
1. انتقل إلى علامتي التبويب: **بيانات الموظفين** > **البطاقات** >:**بيانات أخرى** واعمل على إنشاء حامل البطاقة المعين أو البحث عنه في قاعدة البيانات.
2. حدد خانة الاختيار **الإذن بفتح الأبواب**.
3. انقر فوق أيقونة القرص المرن لحفظ بيانات حامل البطاقة.

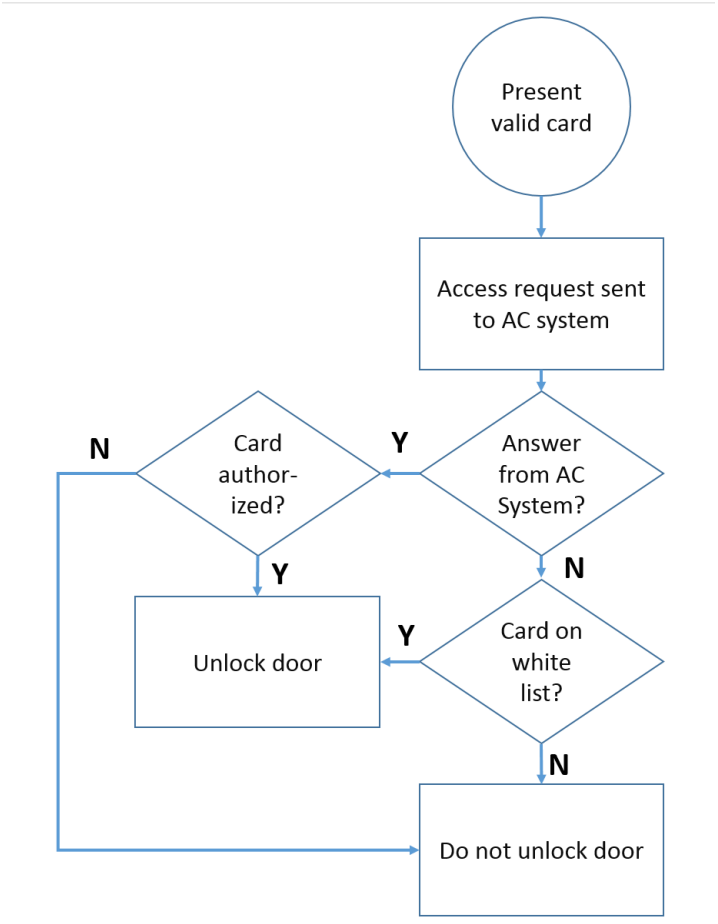
الإجراء الخاص بمجموعة من حاملي البطاقات
1. انتقل إلى: **بيانات الموظفين** > **مجموعات من الأشخاص** واستخدم معايير التصفية لجمع قائمة تتضمن حاملي البطاقات في نافذة القائمة.
2. من القائمة المنسدلة **الحقل المراد تغييره** حدد **فتح الأبواب**
3. حدد خانة الاختيار **فتح الأبواب**.
4. انقر فوق زر **تطبيق التغييرات** لحفظ بيانات حاملي البطاقات.

إرشاد حامل البطاقة إلى كيفية بدء وضع المكتب وإيقافه
لبدء وضع المكتب أو إيقافه في مدخل ما، يضغط حامل البطاقة على **3 #** على لوحة المفاتيح، ثم يقدم بطاقته الحاصلة على تصريح خاص إلى القارئ.
يبقى المدخل مفتوحًا حتى يضغط حامل بطاقة لديه تصريح على **3 #** ويقدم البطاقة من جديد.
لاحظ أنه باستطاعة المراقبين الذين يحملون بطاقة مراقب إيقاف وضع المكتب بالطريقة نفسها، من دون الحاجة إلى إذن خاص.
وضع المكتب مدعوم فقط مع البطاقات الفعلية.

إشعار!
وضع المكتب ومعلمات الجهاز للباب
يتجاوز وضع المكتب معلمة **إلغاء قفل الباب** في علامة التبويب **خيارات** لأحد الأبواب في محرر الجهاز، مما يسمح فقط بالخيارين **0 وضع عادي** و**1 غير مقفل.**

25.3.6 علامة التبويب Smartintego

أنظمة القفل SmartIntego
المقدمة
يحاول قارئ البطاقة SmartIntego أولاً منح تصريح الوصول عبر النظام الأساسي للتحكم في الوصول (AC). وإذا فشل الاتصال، فسيبحث عن رقم البطاقة في القائمة البيضاء المخزنة.



يتم تعيين تصريحات الوصول لنظام القفل SmartIntego بطريقة مماثلة جدًا لأي تصريحات وصول أخرى.

الشروط الأساسية

- تم تكوين نظام قفل SimonsVoss SmartIntego ضمن نظام التحكم في الوصول لديك. يمكنك مراجعة دليل التكوين للحصول على الإرشادات.
- أنواع البطاقات المستخدمة من قِبل حاملي البطاقات هي MIFARE Classic أو MIFARE Desfire. يستخدم النظام SmartIntego الرقم التسلسلي للبطاقة (CSN).

الإجراء الخاص بالتعيين

يصف الإجراء التالي كيفية إضافة رقم بطاقة إلى قائمة بيضاء لنظام SmartIntego، بالإضافة إلى أي تصريحات معينة عبر النظام الأساسي للتحكم في الوصول.

يتم تخزين القوائم البيضاء على أبواب SmartIntego، لتمكين القارئ من منح حق الوصول إلى أرقام البطاقات المدرجة في القائمة البيضاء عند انقطاع الاتصال بجهاز MAC.

ويتم إرسال عمليات الإضافة إلى القوائم البيضاء والحذف منها إلى أجهزة قراءة SmartIntego عندما تُحفظ بيانات حامل البطاقة وعندما يصبح الاتصال متوفرًا.

1. في قائمة عميل ACE، حدد **بيانات الموظفين** > **البطاقات**
2. في قائمة عميل AMS الرئيسي، حدد **بيانات الموظفين** > **البطاقات**
3. حدد الشخص الذي يجب أن يتلقى تخويلات SmartIntego
4. حدد علامة التبويب **SmartIntego.**
5. أنشئ التعيينات:
   - تظهر كل تخويلات الوصول التي تم منحها إلى الشخص في القائمة إلى اليمين.
   - تظهر كل تخويلات الوصول المتوفرة للتعين في القائمة إلى اليسار.

حدد العناصر، ثم انقر فوق الأزرار بين القوائم لنقل العناصر من قائمة إلى أخرى.

يعيّن العنصر المحدد.

 يلغي تعيين العنصر المحدد.

 يعيّن جميع العناصر المتوفرة.

 يلغي تعيين جميع العناصر المتوفرة.

25.3.7 إنشاء بطاقة تنبيه

يوضح هذا القسم كيفية إنشاء بطاقة تنبيه يمكن استخدامها لتشغيل مستوى تهديد.

المقدمة

بطاقة التنبيه عبارة عن بطاقة تشغّل مستوى تهديد معيّنًا عند وجودها في قارئ. لا يمكن إلغاء مستويات التهديد باستخدام بطاقة تنبيه، بل من خلال برنامج التحكم في الوصول فحسب.

الشروط الأساسية

- يتم تكوين قارئ التسجيل على النظام.
- تم تعريف مستوى تهديد واحد على الأقل في النظام.

مسار مربع الحوار

القائمة الرئيسية > **بيانات الموظفين** > **البطاقات** > **بطاقة التنبيه**

الإجراء

1. قم بتحميل سجل الشخص الخاص بالشخص الذي سيتم تعيين بطاقة التنبيه له.
2. انقر فوق "تسجيل البطاقة" في علامة تبويب بطاقة التنبيه.
   - تظهر النافذة المنبثقة: **تحديد مستوى التهديد**
3. في النافذة المنبثقة، حدد مستوى التهديد المطلوب وانقر فوق **موافق**
   - تظهر النافذة المنبثقة: **تسجيل معرّف بطاقة التعريف**
4. أدخل بيانات البطاقة المعتادة بما يتوافق مع تثبيت موقعك، وانقر فوق **موافق**
   - تظهر بطاقة التنبيه التي سجلتها في القائمة على علامة التبويب **بطاقة التنبيه**.

25.4 البطاقات المؤقتة

البطاقة المؤقتة عبارة عن بديل مؤقت لبطاقة تم تغيير موضعها بواسطة حامل بطاقة عادي. إنها بطاقة مكررة تحتوي على جميع التخويلات والقيود الموجودة في البطاقة الأصلية، بما في ذلك حقوق الأبواب غير المتصلة بالإنترنت.

لمنع سوء استخدامها، يستطيع النظام حظر بطاقة واحدة لحامل البطاقة أو جميع بطاقاته الأخرى لفترة وقت محددة، أو حتى إلغاء حظرها يدويًا.

وبالتالي، تُعتبر البطاقات المؤقتة **غير ملائمة** للاستخدام كبطاقات زائرين.

الشروط الأساسية

- يتوفر لدى المشغّل حق الوصول إلى قارئ تسجيل تم تكوينه على محطة العمل حيث يعمل.
- تتوفر بطاقة فعلية ملائمة للتسجيل في النظام كبطاقة مؤقتة.

عميل ACE: انقر فوق **بيانات الموظفين** > **البطاقات**

القائمة الرئيسية > **بيانات الموظفين** > **البطاقات**

الإجراء: تعيين البطاقات المؤقتة

1. قم بتحميل سجل الموظف المطلوب في مربع حوار **البطاقات**.
2. في قائمة البطاقات، حدد البطاقة أو البطاقات التي تحتاج إلى بديل مؤقت.
3. انقر فوق **تغيير البطاقة**
4. في النافذة المنبثقة **تغيير البطاقة**، حدد **بطاقة مؤقتة**
5. في قائمة **المدة**، حدد أحد الخيارات التالية:
   - **اليوم**
   - **اليوم وغدًا**
   - **إدخال عدد الأيام**

6. عند استخدام الخيار الأخير، أدخل عددًا صحيحًا للأيام في المربع.
تجدر الإشارة إلى أن **المدة** تنتهي صلاحيتها دائمًا عند منتصف ليل اليوم ذي الصلة، في الحالات الثلاث كلها.
7. حدد خانة الاختيار **إلغاء تنشيط جميع البطاقات الآن**، إذا لزم الأمر.
– عند تحديد هذا الخيار، سيتم حظر جميع البطاقات التي تعود إلى حامل البطاقة هذا.
– عند مسح هذا الخيار، سيتم حظر البطاقة المحددة أعلاه فقط.
8. حدد خانة الاختيار **تنشيط البطاقة (البطاقات) تلقائيًا بعد مدة زمنية**، إذا لزم الأمر.
– سيتم إلغاء حظر البطاقات المحظورة بشكل تلقائي عندما تنتهي صلاحية **المدة** المحددة أعلاه.
9. ضع البطاقة المؤقت على قارئ التسجيل.
10. انقر فوق **موافق**
يتم تسجيل معرّف بطاقة التعريف بواسطة قارئ التسجيل.
– تظهر البطاقة المؤقتة كنشطة ✓ في قائمة البطاقات، إلى جانب مدة صلاحيتها وبيانات الرمز.
– تظهر البطاقة أو البطاقات الأخرى كمحظورة ×، وهذا يتوقف على الإعداد المحدد أعلاه: **إلغاء تنشيط جميع البطاقات الآن**.
11. (اختياري) في قائمة البطاقات، انقر فوق العمود **تاريخ التجميع** للبطاقة المؤقتة، وحدد تاريخًا لاستردادها من حامل البطاقة.
القيمة الافتراضية هي **أبدًا**.

الإجراء: حذف البطاقات المؤقتة

عندما يتم العثور على البطاقة الأصلية التي تم تغيير موضعها، احذف البطاقة المؤقتة كما يلي:

1. قم بتحميل سجل الموظف المطلوب في مربع حوار **البطاقات**.
2. في قائمة البطاقات، حدد البطاقة المؤقتة.
3. انقر فوق **حذف البطاقة**
تُحذف البطاقة المؤقتة من القائمة، ويُلغى حظر البطاقة أو البطاقات التي كانت تحل مكانها على الفور.

الإجراء: إزالة الحظر المؤقت على البطاقات

إذا لم يعد حظر البطاقة الأصلية مطلوبًا، فاحذف الحظر كما يلي:

1. انتقل إلى مربع الحوار **حظر**: **بيانات الموظفين** > **حظر**.
2. في قائمة البطاقات، حدد البطاقة الشخصية المعلّمة كبطاقة محظورة في العمود **قفل (أقفال)**.
3. انقر فوق **تحرير القفل المؤقت**
لاحظ أن إزالة **الحظر** لا تزيل البطاقات المؤقتة. ستنتهي صلاحية البطاقات المؤقتة بشكل عادي بعد انتهاء فترات صلاحيتها. يمكنك حذفها يدويًا، إذا لزم الأمر.

ملاحظات حول البطاقات المؤقتة

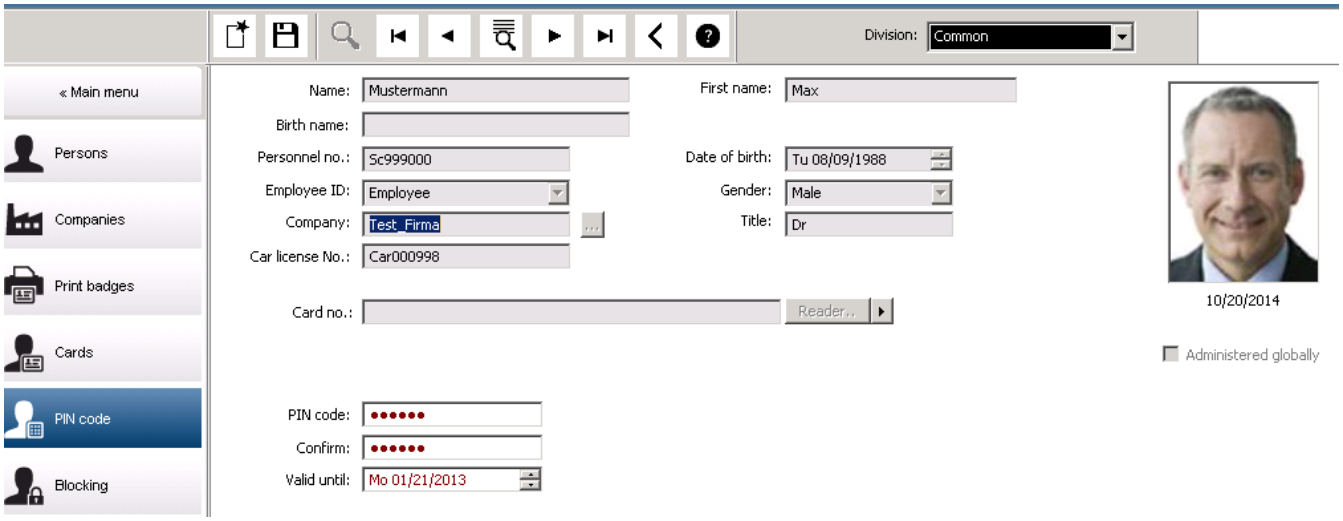
– لا يسمح النظام بأن يتم استبدال البطاقات المؤقتة ببطاقات مؤقتة أخرى.
– لا يسمح النظام بحصول بطاقة شخصية على أكثر من بطاقة مؤقتة واحدة.
– للاطلاع على ملخص سريع لجميع البطاقات المتوفرة لدى حامل بطاقة، مرّر الماوس فوق الجزء الصغير إلى أقصى اليمين الذي يحمل التسمية **مسجّلة**، في شريط الحالة في نافذة مربع الحوار الرئيسي.

25.5 رموز PIN للموظفين

مربع الحوار: رمز PIN

للوصول إلى المناطق ذات متطلبات السلامة المشددة، قد لا يكون تخويل الوصول كافيًا. هنا أيضًا يجب إدخال رمز PIN. يمكن لكل شخص أو بطاقة هوية الحصول على رمز PIN صالح لجميع المناطق. ويحظر النظام استخدام رموز سهلة للغاية (مثلاً: 123456 أو متناظر عند القراءة من الاتجاهين مثل 127721). ويمكن تقييد الصلاحية ويتم تحديدها لكل شخص في مربع الحوار.
في حالة حظر رمز PIN ما أو انتهاء صلاحيته، يُمنع الوصول إلى المنطقة التي تحتم استخدام الرمز حتى لو كانت بطاقة الهوية صالحة لجميع المناطق الأخرى.

في حالة إدخال رمز غير صحيح ثلاث مرات متتابعة، وهو الإعداد الافتراضي ويمكن تكوينه بقيم تتراوح من 1 إلى 99، يتم حظر هذه البطاقة أي يُمنع الوصول إلى جميع المناطق. لا يمكن إلغاء حظر أي بطاقة تم حظرها بهذه الطريقة إلا من خلال مربع الحوار الحظر.



أدخل رمز PIN جديد في حقل إدخال **رمز PIN** وأعد كتابته لتأكيده. يقوم مسؤول النظام بتكوين طول رمز PIN، (ما بين 4 و9 أرقام، القيمة الافتراضية 6).

إشعار!

تتوقف الطريقة التي يستخدمها حامل البطاقة لإدخال أكواد PIN في أجهزة قراءة البطاقات على نوع أجهزة القراءة التي تم تكوينها في النظام:

لجميع البروتوكولات (RS485 وWiegand وLBUS)، يدخل حامل البطاقة `<the PIN>` **# 4**

وضع التفعيل ووضع المكتب مدعومان فقط مع البطاقات الفعلية.

احرص على إعلام حاملي البطاقات بالطريقة التي عليهم اتباعها لإدخال أكواد PIN. في حال وجود أي شك لديك، يمكنك استشارة مسؤول النظام.

رمز PIN لتفعيل إنذارات أنظمة اكتشاف الاقتحام (IDS)

أدخل رمز PIN من 4 إلى 8 أرقام (العدد الافتراضي هو 6 أرقام أي نفس طول رمز PIN للتحقق).

سيستخدم رمز PIN هذا لتفعيل إنذارات نظام اكتشاف الاقتحام (IDS).

يمكن عرض هذا الحقل بواسطة تمثيله بالمعلمات. يكون عنصر التحكم **رقم IDS-PIN منفصل** فقط إذا تم تنشيطه.

- مستعرض التكوين > **البنية الأساسية** > **تكوين النظام** > **رموز PIN لـ ACE**
- القائمة الرئيسية > **التكوين** > **خيارات** > **رموز PIN**

حدد تاريخ انتهاء صلاحية، إذا لزم الأمر.

إذا لم تتوفر حقول الإدخال الخاصة بإدخال رمز IDS PIN، فيمكن استخدام رمز PIN لتفعيل IDS وتعطيله أيضًا. ولكن إذا تم إظهار حقول الإدخال في مربع الحوار هذا، فيمكن استخدام رمز PIN للتفعيل لنظام IDS فقط.

الإعداد الافتراضي: تكون حقول الإدخال لرمز PIN للتفعيل غير مرئية.

رموز PIN للإنذارات (الضغط)

باستطاعة الأشخاص تحت الضغط تشغيل إنذار صامت عبر رمز PIN خاص. ونظرًا لضرورة بقاء الإنذار الصامت غير ملحوظ من قِبل المهاجم، يتم منح حق الوصول، ولكن يتم تنبيه مشغّلي النظام إلى الضغط الذي يتعرض له أحد الأشخاص.

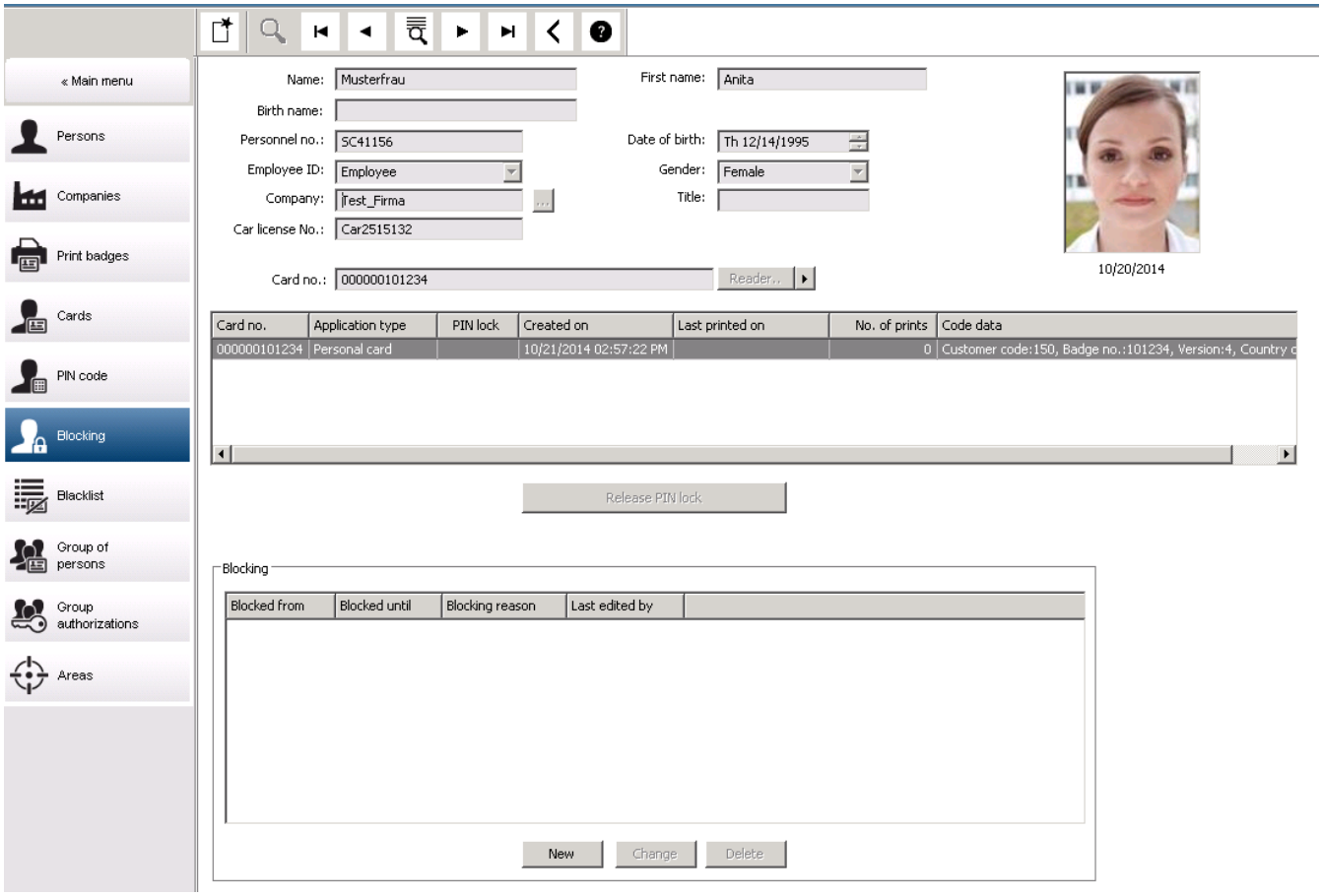
يتوفر متغيران يتم تنشيطهما في نفس الوقت ويمكن للشخص الذي يتعرض للتهديد الاختيار بينهما:
- إدخال رمز PIN بترتيب معكوس (على سبيل المثال: 321321 بدلاً من 123123).
- زيادة رمز PIN بمقدار "1" (على سبيل المثال: 123124 بدلاً من 123123). إذا كان الرقم الأخير 9، فيمكن زيادة رمز PIN، ونتيجة لذلك، سيكون رمز PIN بعد زيادته 123130 إذا كانت قيمته 123129.

25.6 حظر وصول الموظفين

مربع الحوار:الحظر

في مواقف معينة، من الضروري منع حق وصول أحد الأشخاص مؤقتًا أو إزالة حظر مفروض من وحدة التحكم MAC، على سبيل المثال، بسبب إدخال رموز PIN غير صحيحة ثلاث مرات أو بسبب الفحص العشوائي.

ويعني الحظر منع الشخص من الوصول إلى أي مكان بشكل مطلق، بصرف النظر عن بيانات الاعتماد المستخدمة.



1. حدد الشخص كالمعتاد.
2. في جزء الحظر، انقر فوق **جديد** أو أنشئ حظرًا للشخص المحدد حاليًا.
3. أدخل معلومات إضافية في مربع الحوار المنبثق.
   - **محظور من / حتى**: (إذا لم يتم تحديد وقت انتهاء، يتم حظر الشخص حتى يُرفع الحصار يدويًا.)
   - **نوع الحظر:**
   - **سبب الحظر:** (لسجل الشخص، إذا كان نوع الحظر `Manual`)
4. انقر فوق **حفظ** في مربع الحوار المنبثق لحفظ الحظر.

- حدد حظرًا من القائمة، إذا لزم الأمر، وانقر فوق **تغيير** أو **حذف** لتغييره أو حذفه.

إذا تم اختيار **القفل اليدوي** كنوع حظر، فأدخل **سبب الحظر** لسجل الشخص.

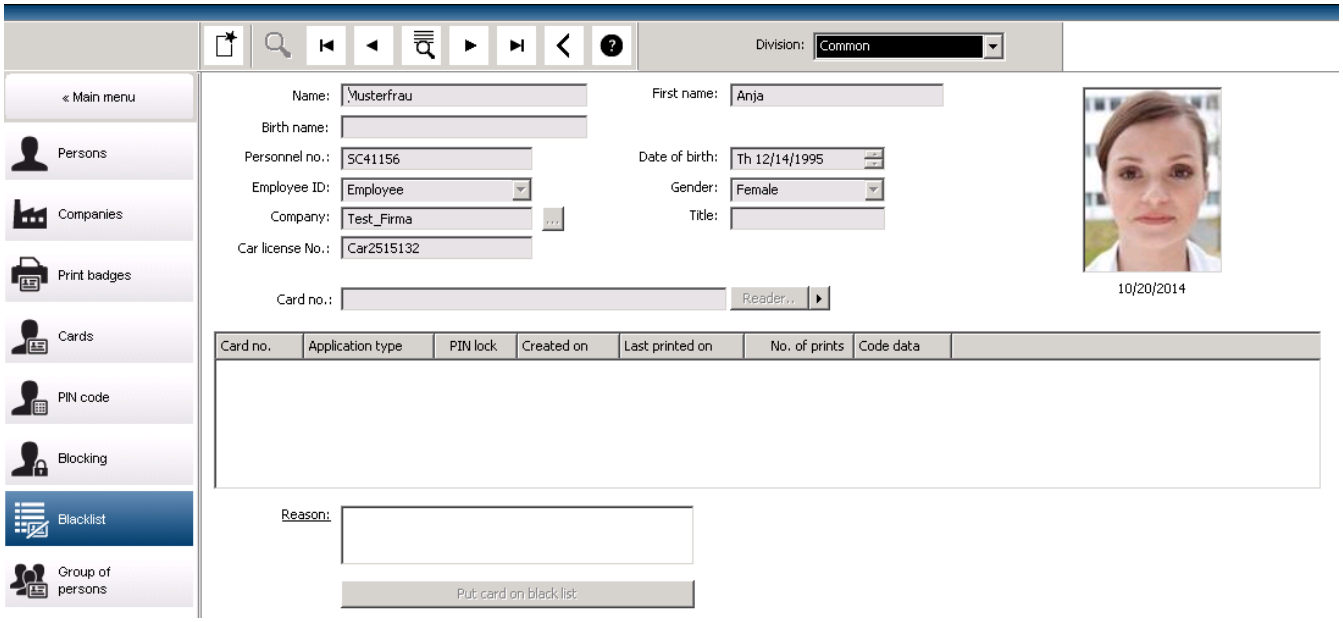
إشعار!
ينطبق الحظر على الشخص وليس على بيانات اعتماد معينة. وعليه من غير الممكن إلغاء الحظر أو تجنبه عن طريق إعطاء بطاقة هوية جديدة.

25.7 إدراج بطاقات في القائمة المحظورة

مربع الحوار: القائمة المحظورة
يتم إدخال أي بطاقة لا يجب استخدامها مرة أخرى مطلقًا، مثل البطاقات المسروقة أو المفقودة، في جدول قائمة سوداء.
يتم إدراج بطاقات الاعتماد في القائمة المحظورة، وليس الشخص.

إشعار!
والعملية لا يمكن عكسها، فالبطاقات المدرجة في القائمة المحظورة لا يمكن إلغاء حظرها مطلقًا ولكن يجب استبدالها بدلاً من ذلك.

لا تمنح البطاقات المدرجة بالقائمة المحظورة صلاحية الوصول. وفي المقابل يتم تسجيل محاولة استخدامها في ملف السجل، ويُطلق إنذار.



القائمة الرئيسية > **بيانات الموظفين** > **قائمة سوداء**

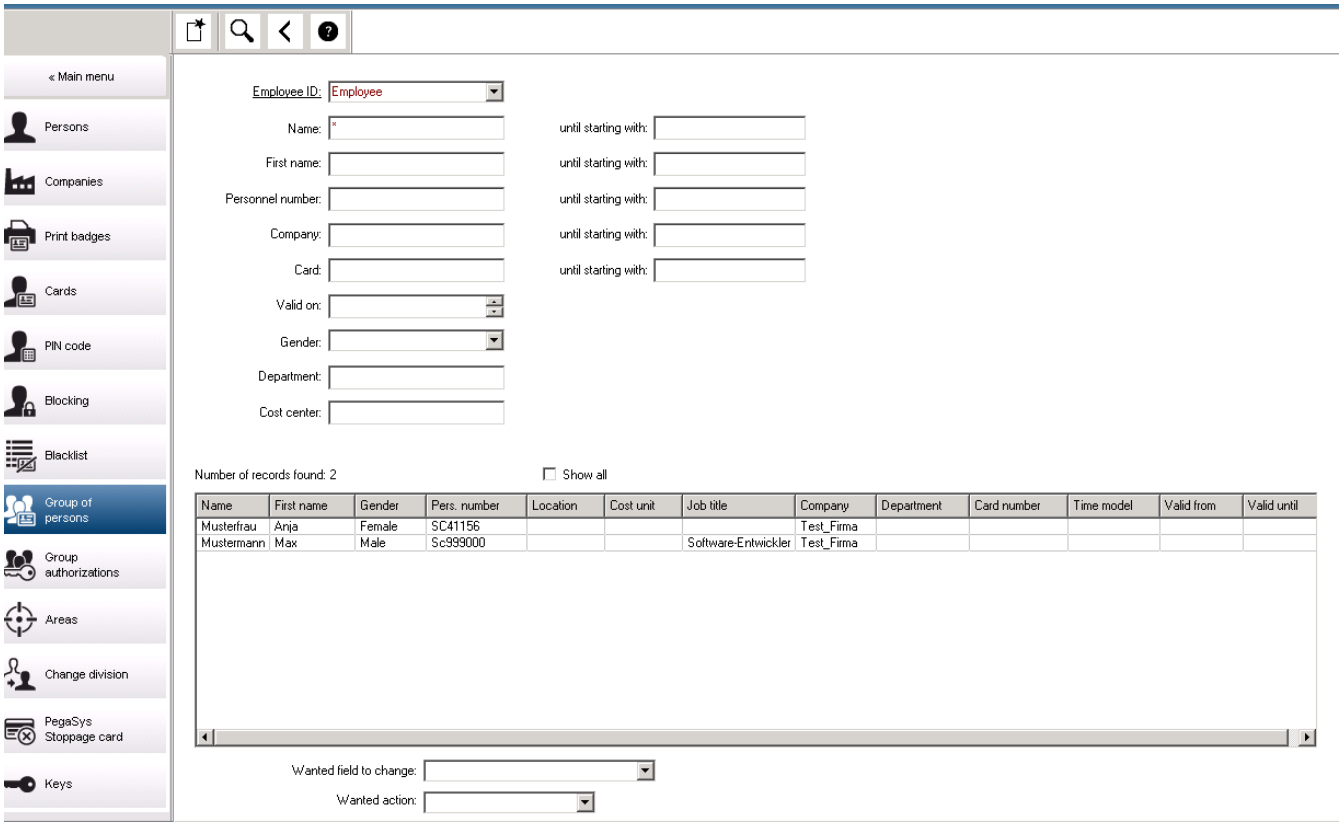
1. حدد الشخص المراد إدراج بطاقة هويته في القائمة المحظورة.
2. وفي حالة وجود أكثر من بطاقة واحدة مخصصة إلى حامل البطاقة هذا، فحدد البطاقة في القائمة **رقم بطاقة الهوية**.
3. أدخل سبب إدراج هذه البطاقة بالقائمة المحظورة في حقل الإدخال **السبب**.
4. انقر فوق الزر **إدراج هذه البطاقة في القائمة المحظورة**.
5. أكد الإدراج في القائمة المحظورة في النافذة المنبثقة.

النتيجة: يتم إدراج البطاقة بالقائمة المحظورة مع التفعيل الفوري.

إشعار!
ويؤثر الإدراج بالقائمة المحظورة على البطاقات **لا** حامليها.
ولا يتم حظر أي بطاقات أخرى لنفس الشخص غير مُدرجة بالقائمة المحظورة.

25.8 تحرير عدة أشخاص في الوقت نفسه

مجموعة أشخاص



يتيح مربع حوار آخر تحديد مجموعة من الأشخاص يمكن تعريف تعديلات المجموعة عليها. وللاستمرار في التحكم في مجموعة الأشخاص المحددة، يتم إدراج أول عشرة أشخاص بالأسماء والبيانات الفعلية من قاعدة البيانات (البيانات الفعلية: إذا تم تحديد "ST-AC" كقسم، يتم عندها عرض "ST-ACS" و"ST-ACX"). بالإضافة إلى ذلك، يتم عرض عدد الأشخاص بالمجموعة المحددة.
بعد تحديد مجموعة من الأشخاص يمكن تحديد الإدخالات التالية:

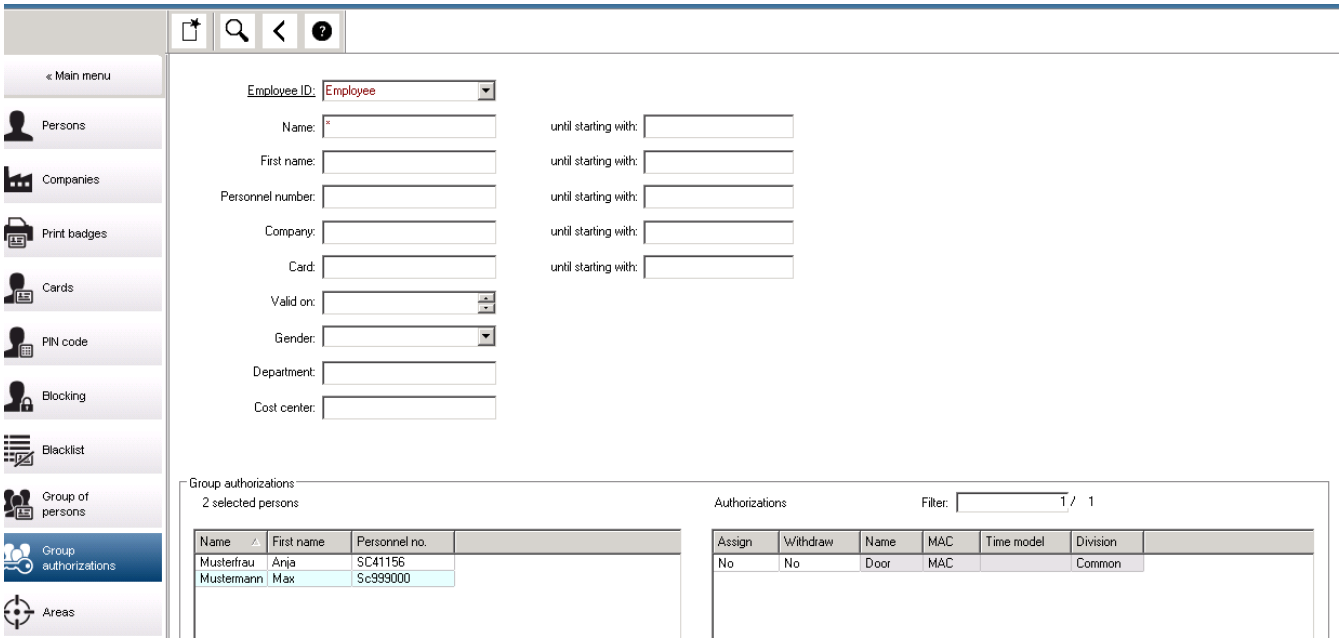
- هوية الموظف
- الاسم
- الاسم الأول
- رقم الموظف
- الشركة
- البطاقة
- صالح في
- الجنس
- القسم
- وحدة التكلفة
- حقول احتياطية في حالة تعريفها

يمكن تحديد خيار التعديلات:
- الحقل المطلوب تغييره
- الإجراء المطلوب
- القيمة القديمة
- القيمة الجديدة

ومن ثم يتم إدخال القيم المصممة في الحقل **القيمة القديمة** أو **القيمة الجديدة** على التوالي. وعند تحديد الزر **تطبيق التغييرات** وتأكيد سؤال الأمان **هل ترغب في تطبيق التغييرات على جميع الأشخاص المحددين؟** يكتمل الإجراء، أي لا يمكن استخدام مربع الحوار أثناء تنفيذ الإجراء. ويحتمل أن تستغرق الإجراءات التي تم تشغيلها بواسطة الحقول من *1 إلى *4 وقتًا أطول من الحقول الأخرى، (بدون نجمة)، ولا يُسمح بجميع التعديلات. وعليه مثلاً، لا يمكن مقارنة الحقل **الإجراء المطلوب** مع الحقل **القيمة الجديدة**، لأن هذين الإدخالين غير مشمولين في المنتج القياسي. ويمكن أن تختلف حقول **القيمة القديمة** و**القيمة الجديدة** على التوالي.

25.8.1 تخويلات المجموعة

تخويلات المجموعة



يدعم عنصر القائمة **[تخويلات المجموعة]** معايير البحث التالية:
- هوية الموظف
- الاسم
- الاسم الأول
- رقم الموظف
- الشركة
- البطاقة
- صالح في
- الجنس
- القسم
- وحدة التكلفة
- حقول احتياطية في حالة تعريفها

بعد ذلك، تظهر قائمة في الجزء الأسفل من مربع الحوار حيث تعرض جميع الأشخاص المحددين (مع الاسم والاسم الأول ورقم الموظف). وتُعرض جميع التخويلات التي ينطبق عليها وصف التخويل أسفل الجزء السفلي الأيسر، مع وصف التخويل ونموذج الوقت والأعمدة **[تعيين]** و**[سحب]**. وعند فتح قائمة التخويلات تظهر التخويلات الحالية وتتم إعادة تعيين الأعمدة **[تعيين]** و**[سحب]** إلى "لا". والآن، يمكن تعيين تخويلات الأفراد عن طريق النقر المزدوج فوق الحقل في أي عمود مما يغير الإدخال "لا" إلى "نعم" أو العكس. يؤدي النقر فوق "تنفيذ التغييرات" إلى إضافة جميع التخويلات التي تم تعيينها باستخدام الخيار "نعم" إلى جميع الأشخاص المحددين أو يتم سحبها تباعًا. وتظل جميع التخويلات الأخرى للأشخاص دون تغيير، فعادة لا يملك الأشخاص المحددين تخويلات متطابقة تمامًا.

25.9 تغيير القسم لأشخاص

المقدمة

يعتبر مربع الحوار **تغيير القسم** مربع حوار فعالاً لتغيير قسم خاص بمجموعة من سجلات الموظفين في النظام.

إشعار!

استخدم هذه الميزة بتأنٍ فائق!
ينطوي التغيير في القسم على تداعيات واسعة النطاق على سجلات الموظفين التي تقوم بتغييرها.

الشروط الأساسية

يجب أن تتوفر لدى المشغّل الذي يغيّر قسم سجلات الموظفين تخويلات تسمح له بتحرير هؤلاء الأشخاص بالإضافة إلى القسمين المعنيين.

مسار مربع الحوار

القائمة الرئيسية > **بيانات الموظفين** > **تغيير القسم**

الإجراء

1. في جزء **تصفية الأشخاص**، أدخل معايير التصفية في حقل أو أكثر من الحقول التالية:

تصفية	الملاحظات / الوصف
اللقب	استخدم علامة نجمية واحدة لمطابقة جميع الأشخاص، أو استخدم أحرفًا **من دون** علامات نجمية
رقم الموظف من/ إلى	استخدم الحقلين لتحديد مجموعة من القيم
هوية الموظف (نوع الموظف)	حدد من القائمة
القسم	يُظهر الزر "تطبيق عامل التصفية" الأشخاص من هذا القسم فقط
الشركة	حدد من ضمن الشركات المتوفرة
القسم	
رقم البطاقة (من/ إلى)	استخدم الحقلين لتحديد مجموعة من القيم

2. انقر فوق **تطبيق عامل التصفية**
يظهر جميع الأشخاص الذين يتطابقون مع عامل التصفية في قائمة **الأشخاص المحددون.**
3. لتنقية مجموعة الأشخاص المحددين، انقر فوق سطر أو أكثر في قائمة **الأشخاص المحددون**، ثم انقر فوق الزر **إزالة**. استخدم المفتاحين Ctrl وShift لتحديد عدة سجلات مرة واحدة.

- **مهم:** قبل المتابعة، تأكد من أن قائمة **الأشخاص المحددون** تحتوي فقط على الأشخاص الذين تريد تغيير قسمهم.

4. في القائمة **قسم جديد**، حدد القسم الوجهة للأشخاص المحددين.
5. انقر فوق **تغيير قسم الأشخاص**

يُنقل جميع الأشخاص في قائمة **الأشخاص المحددون** إلى **قسم جديد**.

تأثير التغيير من قسم إلى آخر

الأشخاص

- تخويلات الوصول والتحكم في المسار
- تم حذف الروابط إلى القسم السابق.
- تم الاحتفاظ بالروابط إلى بيانات الفئة "عام".

الشركات

- تم حذف الروابط إلى شركات القسم السابق.

تأثير التغيير من "عام" إلى قسم آخر

- تخويلات الوصول والتحكم في المسار
- تم الاحتفاظ بالروابط إلى الفئة "عام" والقسم الجديد.
- تم حذف الروابط إلى القسم الآخر.

تأثير التغيير من قسم إلى "عام"

تم الاحتفاظ بكل الروابط.

25.10 إعداد المنطقة الأشخاص أو السيارات

المقدمة

يصف هذا القسم كيفية تغيير الموقع المسجل لحامل بطاقة أو سيارته من منطقة محددة إلى أخرى. قد يصبح هذا الأمر ضروريًا إذا انتقل حامل البطاقة من منطقة إلى أخرى من دون إجراء مسح ضوئي لبطاقته. في مثل هذه الحالات، ترفض أنظمة منع العودة الصارمة دخول حامل البطاقة إلا عندما يتطابق موقعه الفعلي مع موقعه المسجل.

الشروط الأساسية

- تم تعريف مناطق الوصول في النظام، وهي قيد الاستخدام. للاطلاع على الوثائق، انظر الرابط أدناه.
- بصفتك المشغّل، يمكنك تعديل بيانات حامل البطاقة.

إجراء لإعادة تعيين موقع حاملي بطاقات فرديين وسيارات فردية

مسار مربع الحوار

القائمة الرئيسية > **بيانات الموظفين** > **المناطق**

1. حدد حامل البطاقة من قاعدة البيانات كالمعتاد.
2. في قائمة **الموقع**، حدد موقعًا جديدًا

أو

3. في قائمة **موقع السيارة**، حدد موقعًا جديدًا لسيارة حامل البطاقة.
4. انقر فوق للحفظ

راجع

- تكوين مناطق التحكم في الوصول, الصفحة *24*

25.10.1 إجراء لإعادة تعيين موقع جميع حاملي البطاقات والسيارات

قد يصبح هذا لإجراء ضروريًا، على سبيل المثال، بعد تجربة إخلاء. يتم تعيين جميع المناطق إلى **غير معروفة** لتمكين استئناف مراقبة تسلسل الوصول ومنع العودة.

الإجراء
مسار مربع الحوار
القائمة الرئيسية > **بيانات النظام** > **إعادة تعيين المناطق غير المعروفة**

- انقر فوق **تعيين مناطق كل الأشخاص الموجودين إلى "غير معروف"**

أو

- انقر فوق **تعيين مناطق كل مركبات الانتظار إلى "غير معروف"**

25.11 تخصيص النماذج وطباعتها لبيانات الموظفين

نظرة عامة
استخدم **النماذج** لتخصيص النماذج لطباعة بيانات حاملي البطاقات من قاعدة البيانات. قد تكون هذه الوظيفة مطلوبة من جانب القوانين المحلية لحماية خصوصية البيانات.
يتم توفير نماذج القوالب. ويمكن تصدير هذه القوالب كملفات HTML وتخصيصها وفقًا لمتطلباتك وإعادة استيرادها لاستخدامها في مدير الحوار.
أنشئ مثيلاً من هذه النماذج واطبعها من مربع الحوار **بيانات الموظفين** > **طباعة الشارات**.

مسار مربع الحوار
- القائمة الرئيسية AMS > **التكوين** > **خيارات** > **النماذج**

تخصيص نموذج
1. في مربع حوار **النماذج**، في قائمة **النماذج المتوفرة**، حدد القالب الذي تريد تخصيصه، عادةً `AllPersonalData_EN`، الذي يحتوي على جميع حقول بيانات الموظفين في قاعدة البيانات.
2. انقر فوق **تصدير** لحفظ النموذج إلى ملف HTML جديد على النظام.
3. استخدم محرر HTML لتخصيص ملف HTML وفقًا لمتطلباتك.
4. في مربع حوار **النماذج**، انقر فوق **إدراج** لاستيراد ملف HTML المخصص إلى مدير الحوار.
   - (اختياري) إذا كان النموذج صالحًا لقسم معين فقط، فحدد قسمًا من عمود **القسم**.
   - (اختياري) انقر فوق **معاينة** لعرض النموذج الذي لم يتم إنشاء مثيل له في عارض HTML.
   - (اختياري) انقر فوق **حذف** لحذف نموذج من القائمة.

إنشاء مثيل من نموذج وطباعته
1. في مدير الحوار، انتقل إلى
   - القائمة الرئيسية AMS > **بيانات الموظفين** > **طباعة الشارات**
2. قم بتحميل سجل الموظف المطلوب إلى النموذج.
3. حدد نموذجًا قائمة **النماذج**.
4. انقر فوق الزر **طباعة نموذج**.
   - يتم إنشاء مثيل للنموذج بواسطة بيانات الموظف المحدد، ويتم إرسالها إلى الطابعة التي تختارها.

26 إدارة الزائرين

يحظى الزائرون بحالة خاصة في نظام التحكم في الوصول، وتبقى بياناتهم منفصلة عن بيانات الموظفين الآخرين. لهذا السبب، يجري إنشاء بيانات الزائرين وحفظها في مربعات حوار منفصلة.

26.1 بيانات الزائرين

مقدمة

يدعم النظام إدارة بيانات الزائرين بسرعة وسهولة. وعليه يمكن إدخال بيانات الزائرين المعروفين بالفعل وتعيين تصاريح الوصول قبل حضور الزائرين. وعند حضور الزائرين، لا يتبقى سوى تخصيص البطاقة. في نهاية الزيارة عند إعادة البطاقة، تُحذف الصلة بين بطاقة الهوية والشخص مرة أخرى وتُسحب التصاريح تلقائيًا.

إذا لم يحذف المستخدم بيانات الزائر، فسيتم ذلك بواسطة النظام في نهاية الوقت المُكوّن (وهو 6 أشهر بشكل افتراضي) بعد المرة الأخيرة التي تم فيها إعادة البطاقة.

وتتم إدارة الزائرين الخارجيين من خلال مربعي حوار.

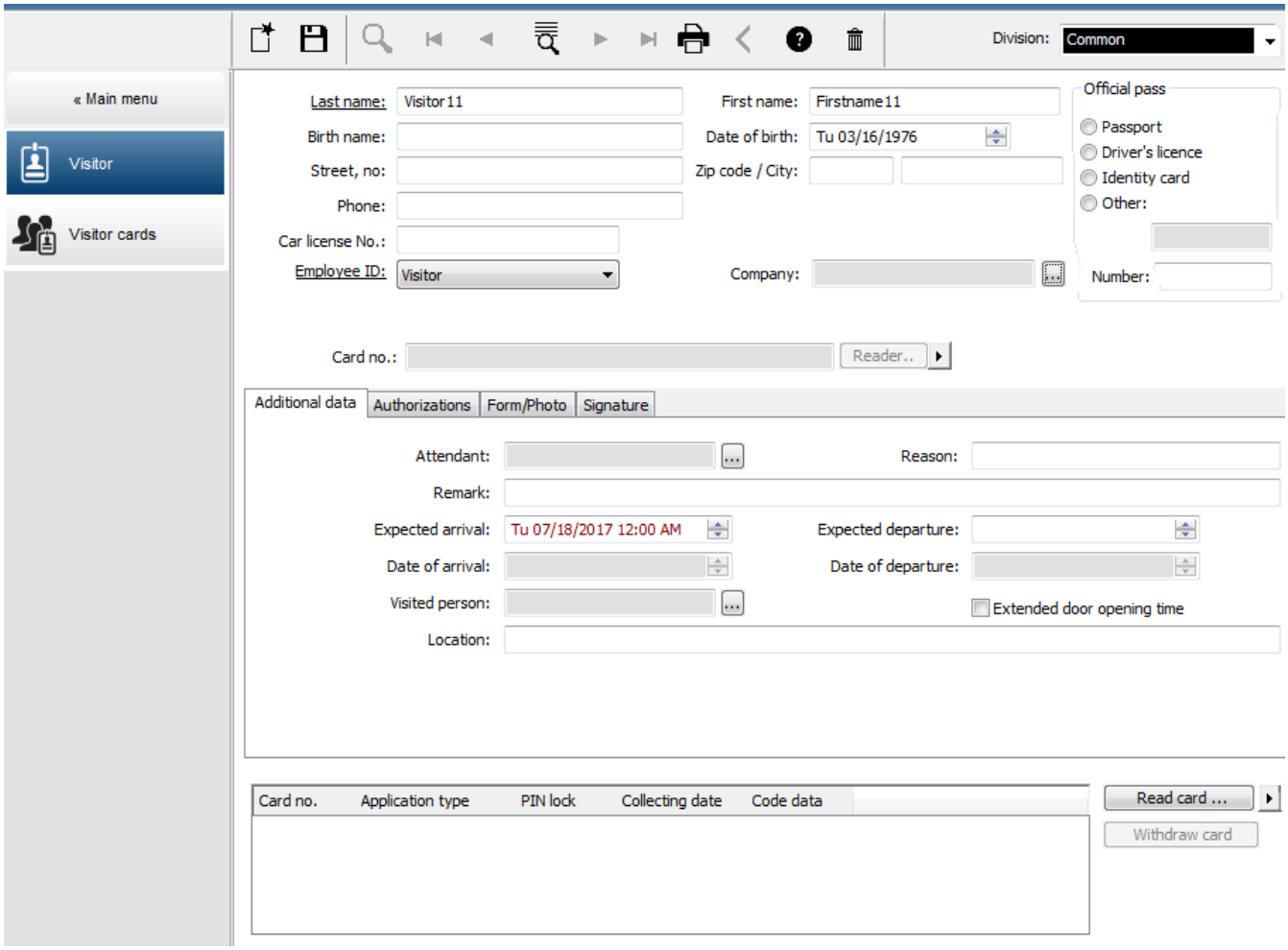
- يتم استخدام مربع حوار **الزائرون** لإدخال بيانات الزائرين وتصاريح الوصول الخاصة بهم.
- وينظم مربع حوار **بطاقات الزائرين** تسجيل بطاقات الزائرين وحذفها.

مربع الحوار: الزائرون

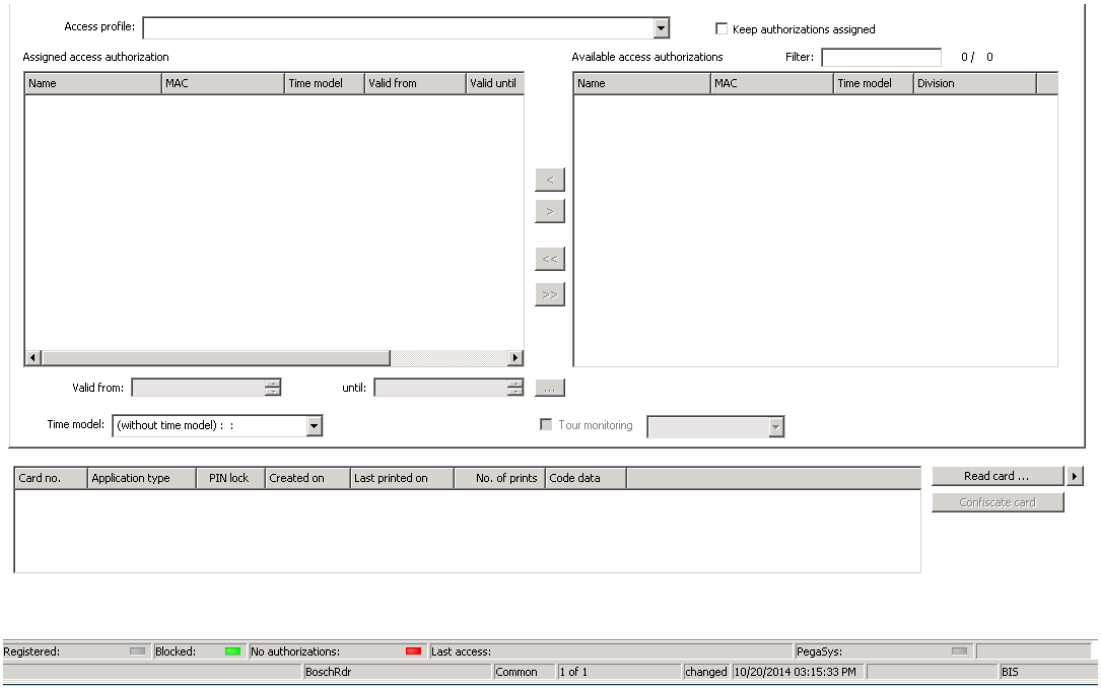
تكون الحالة المعينة للزائرين منفصلة تمامًا بشكل صارم عن الأشخاص الآخرين وبالتالي تتم معالجتها في مربع حوار منفصل. ولا يمكن إنشاء الأشخاص الذين لديهم هويات **زائر** في مربع الحوار **الأشخاص** كما لا يمكن تسجيل بطاقات هوية لهم في مربع الحوار المخصص لهذا الغرض.

ومن ضمن أشياء أخرى، لا يوجد حقل إدخال **هوية الموظف** في مربع الحوار **الزائرون**. وبما أن هناك جدول قاعدة بيانات منفصل للزائرين، فإن الأشخاص الذين يتم إنشاؤهم في مربع الحوار الموضح هنا كزائرين يتم التعرف عليهم تلقائيًا. ومن ثم فهذا يعني عدم إمكانية إنشاء أي أشخاص هنا بخلاف الزائرين. وفقًا لذلك، لا تتم عمليات التحديد إلا في مربع الحوار هذا في جدول قاعدة البيانات ذي الصلة. وفي المقابل، فإن جميع الأشخاص المُسجلين بالنظام يمكن تحديدهم في مربعات الحوار الأخرى لبيانات الموظفين، ولكن قد لا يكون استخدامهم ممكنًا دائمًا للزائرين (مربع الحوار **البطاقات**).

بينما يمكن إدخال بيانات الزائرين غير المعروفين، بشكل كامل أو جزئي في النظام قبل حضور الزائرين. وهذا يوفر حدًا أدنى من وقت الانتظار للزائرين الذين تم بالفعل تسجيل بياناتهم.



يمكن إدخال **السبب** من الزيارة و**الموقع** الذي يزوره الزائرون و**ملاحظة** ما في حقول الإدخال أدناه.
إذا أردت إدخال بيانات في الحقول **تاريخ الوصول المتوقع** و**تاريخ المغادرة المتوقع** فإن هذه التواريخ ستظهر أيضًا في الحقول **صالح من** و**حتى**.
ويتم إدخال التواريخ ذات الصلة في الحقول **تاريخ الوصول** و**تاريخ المغادرة** بواسطة النظام عند تعيين بيانات الزائرين إلى كل منهم وفصلها من بطاقة هوية الزائر.
وكما هو الحال مع مربع الحوار **البطاقات**، هناك أيضًا إمكانية تعيين أوقات أطول لفتح الأبواب للزائرين وذلك لضمان وصول أسهل، على سبيل المثال، لذوي الاحتياجات الخاصة.



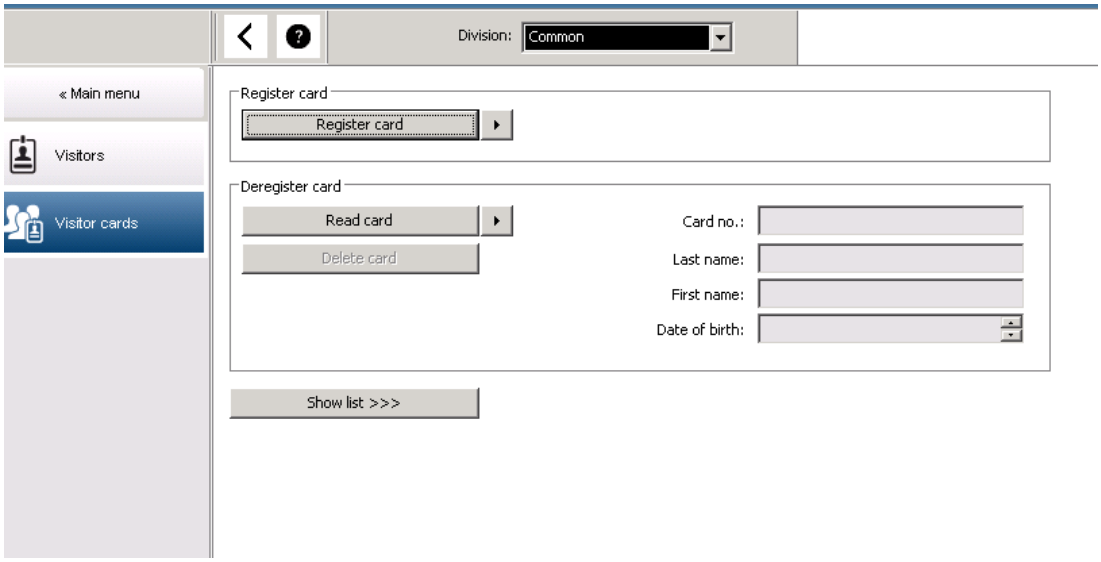
في حقل مربع الحوار **تعيين التخويل**، يمكن تحديد ملف تعريف زائر، موجود بالفعل، في قائمة التحديد المتشابهة في الحروف، أو يمكن تحديد تخويلات الوصول الفردية من القائمة **تخويل الوصول المتاح** في القائمة **تخويل الوصول المعيّن** إلى اليمين عن طريق وضع علامة عليها ونقلها من القائمة اليسرى.
في مربع الحوار هذا، لا يمكن تحديد سوى ملفات تعريف الوصول المميزة كملفات تعريف خاصة بالزائرين. وعلى هذا الأساس، يتم تجنب منح الزائرين الوصول إلى مناطق خاصة عن طريق إعطاء تخويلات عامة.
ويمكن تعيين التحقق من صلاحية تخويلات الوصول، لكل تخويل على حده.
في حالة وجود خطأ في قراءة البطاقة، يمكن أيضًا إدخال رقم بطاقة الهوية يدويًا. ويتم تخزين التاريخ الحالي باعتباره تاريخ الوصول في نفس الوقت.
ويُعيد الزائر بطاقة هويته بعد انتهاء الزيارة. أثناء قراءة بطاقة الهوية في قارئ البطاقات أو أثناء أو إدخال رقمها يدويًا، يتم تحديد الشخص ذي الصلة وعرض بياناته على الشاشة.
يؤكد المشغّل إعادة البطاقة. وتتم إزالة الاقتران بين بطاقة الهوية والزائر عن طريق النقر فوق الزر **مصادرة البطاقة**. ويتم تخزين تاريخ ووقت هذا الإجراء كتاريخ مغادرة.

مربع الحوار: بطاقات الزائرين

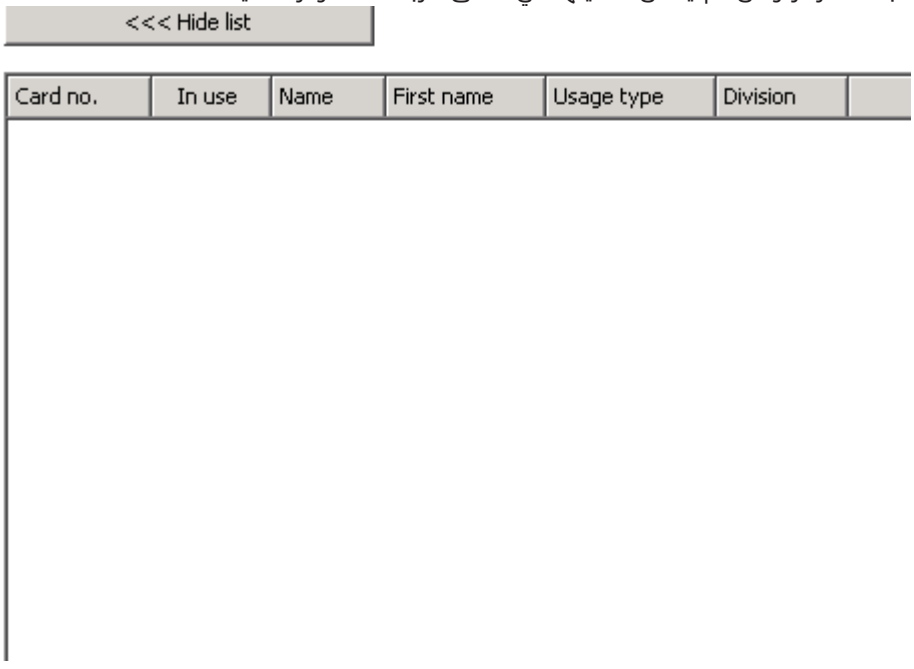
يتم حجز بعض البطاقات في النظام كبطاقات زائرين. ويتم عادة تعيين بطاقة زائر إلى زائر قادم وتتم إعادتها عند مغادرته، وعندئذ يمكن إعادة استخدام البطاقة. يجب تسجيل مثل هذه البطاقات كبطاقات زائرين قبل تعيينها إلى الزائرين.

إشعار!

بشكل عام، يتم إنشاء بطاقات الزائرين بدون اسم أو صورة، لكي تكون قابلة لإعادة الاستخدام.



انقر فوق الزر **تسجيل بطاقة هوية** لإجراء التسجيل.
عندئذ يتم اتباع إجراء الإدخال الموضح سابقًا (بالأقسام **الأشخاص** و**بطاقات الهوية** في الفصل **بيانات الموظفين**) مع رقم بطاقة الهوية بهدف اكتشاف البطاقة. وهذا يتيح للنظام التعرف على بطاقة الهوية كبطاقة زائر ومن ثم يمكن تفعيلها في نطاق مربعات الحوار التالية.



لإجراء عملية تعيين بطاقات هوية الزائرين بشكل أسرع، يُوصى بمسح جميع بطاقات الهوية الحالية ضوئيًا حتى يتم تعيين هذه البطاقات للزائرين كل على حده في مربع الحوار التالي.
وفي نهاية الزيارة، يُعيد الزائر بطاقة الهوية. وعند مسح بطاقة الهوية هذه لدى قارئ مربع حوار أو غير إدخال رقم بطاقة الهوية، يتم تحديد الشخص المخصص له البطاقة وتظهر بياناته على الشاشة. [لإدخال رقم بطاقة الهوية يدويًا والتحويل لاستخدام أجهزة القراءة، الرجاء مراجعة التوضيح الموجود في **مربع الحوار: البطاقات** و**مربع الحوار: الزائرون**.] يقوم المستخدم بتأكيد إعادة بطاقة الهوية. وتتم إزالة الصلة بين بطاقة الهوية وبيانات الموظف الخاصة بالزائر عن طريق الضغط على الزر. ويتم تخزين التاريخ الحالي باعتباره تاريخ المغادرة.

طباعة نموذج زائر

يحتوي شريط الأدوات في مربع الحوار **الزائرون** على زر إضافي من أجل طباعة شهادة الزائر. وفي جملة أمور أخرى، يستطيع الشخص الذي يستقبل الزائر استخدام شهادة الزائر هذه للتأكد من وصول الزائر ووقت وصوله ومغادرته.

Visitor pass

Entry	Exit

First- and lastname
Steven Visitor

Company

☐ Proof of authority for plant area

Registration plate

Passed card

Contact person | Phone | Department

Reason of visit

Visit appointment
☐ Yes ☐ No

Type of official
Passport

Number of offical document

I accept the terms and conditions overleaf

Location, date | Sign of visitor

Identy card with photo seen ?
☐ Yes ☐ No

Sign of plant protective force

To complete from visited person
Arrival at
Departure at

To sign on visited person

26.2 زائر متأخر جدًا

تسمح طريقة العرض **زائر متأخر جدًا** للمشغّل بالتحقق من موقع الزائرين في المقرّ، وما وإذا تجاوزوا وقت المغادرة المجدولة.

- كي يتمكن المشغّلون من عرض صفحة html، يجب أن يكون رابط هذه الصفحة المكوّن على شاشة البدء لديهم.
- يمكن إنشاء مشغّل إنذار في BIS للرد على الرسالة **زائر متأخر جدًا**. بإمكان المشغّل عندئذٍ فتح صفحة html التي تتضمن بيانات الزائر.

الأحداث التي تؤدي إلى إنشاء رسالة "زائر متأخر جدًا":

عند تعيين بطاقة إلى زائر، يقوم المشغّل بإدخال الوقت المتوقع للمغادرة. وعندما تنتهي الزيارة، يعيد الزائر البطاقة إلى مكتب الاستقبال، حيث يقوم المشغّل بإلغاء البطاقة.

أو، يمكن استخدام قارئ بطاقات آلي كقارئ خروج للزائرين، ويمكن تكوينه للاحتفاظ ببطاقة الزائر عندما يغادر المقر.

إذا لم يعيد الزائر البطاقة قبل وقت المغادرة الذي تم ترتيبه مسبقًا، وبصرف النظر عن استمرار وجود الزائر في المقر، فسيتم إنشاء الرسالة **زائر متأخر جدًا** بواسطة النظام.

يتم تنفيذ عملية التحقق من التأخير في إعادة البطاقات عند فواصل زمنية منتظمة (على سبيل المثال، كل دقيقة). وسيتم إنشاء الرسالة **زائر متأخر جدًا** بواسطة كل عملية تحقق حتى إعادة البطاقة. يمكن تكوين الفاصل الزمني في سجل الخادم، ضمن: `HKLM\Software\Micos\SPS\Default\VLDP\Interval`

إشعار!

يمكن إلغاء تنشيط إنشاء هذه الرسالة في سجل الخادم، ضمن:
`HKLM\Software\Micos\SPS\Default\VLDP\Active`

تعمل هذه الميزة على تمكين العميل من اكتشاف أي زائر لا يقابل الموظف المخصص أو لا يعود مرة أخرى إلى الاستقبال وإبقاء موظفيه على اطلاع أو لا يخرج من البوابة بعد مقابلة الموظف خلال المدة الزمنية المحددة.

ما يتم التحقق منه:

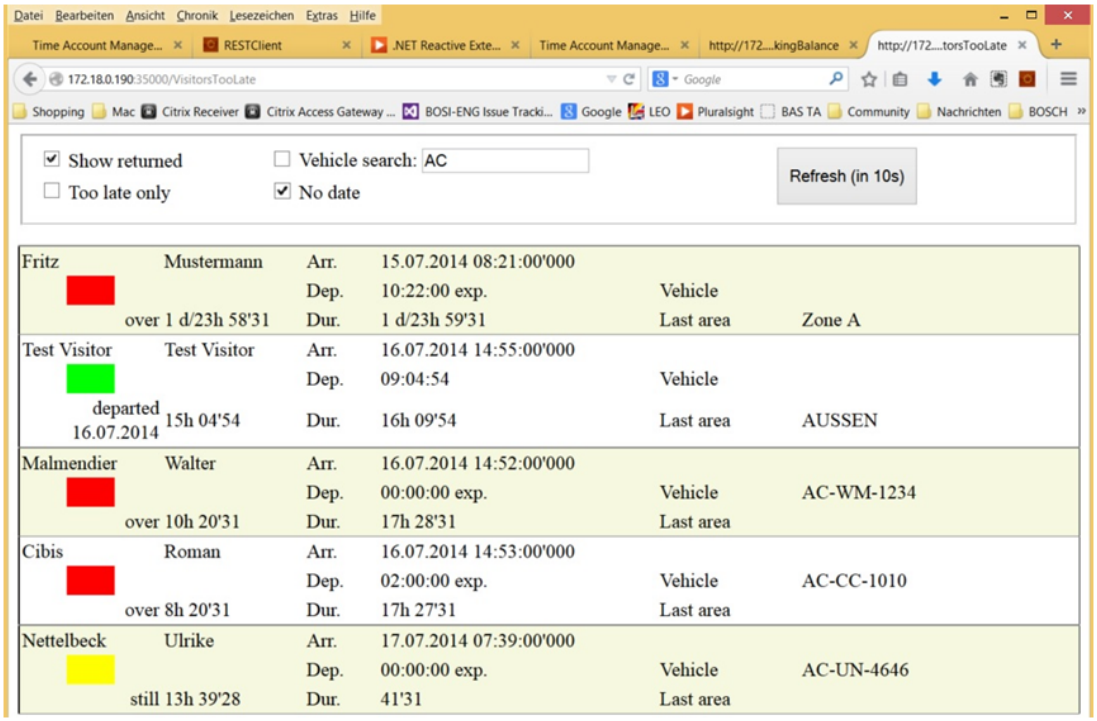
- ما هي أخر منطقة أُستخدمت فيها شارة الوصول إلى المبنى الخاصة بالزائر.
- إذا كان الزائر قد سحب شارة الوصول إلى المبنى.
- إذا كان الزائر قد سحب شارة المركبة، إذا كان ذلك منطبقًا.

يتم إنشاء تقرير يشمل **زائر متأخر جدًا** و**مركبة متأخرة جدًا**.

وفي حالة عدم الإعادة، يمكن طبع المنطقة الحالية للشارة في التقرير "زائر متأخر جدًا".

تُعرض حالة الزائر على موقع الويب مع أشرطة ملونة:

- **أخضر:** أعاد الزائر جميع بطاقات الوصول.
- **أصفر:** لم تنتهِ الزيارة بعد ولم ينتهِ الوقت.
- **أحمر:** لم تنتهِ الزيارة بعد والوقت انتهى، أي **زائر متأخر جدًا**.



يتم تحديث الصفحة تلقائيًا كل 30 ثانية. ويمكن تكوين وقت التحديث من داخل صفحة الويب. بالإضافة إلى ذلك، يمكن تعديل طريقة عرض المُشغّل باستخدام عوامل التصفية **إظهار البطاقات المُعادة** و**المتأخر جدًا فقط** و**بحث المركبات**.

27 إدارة ساحات الانتظار

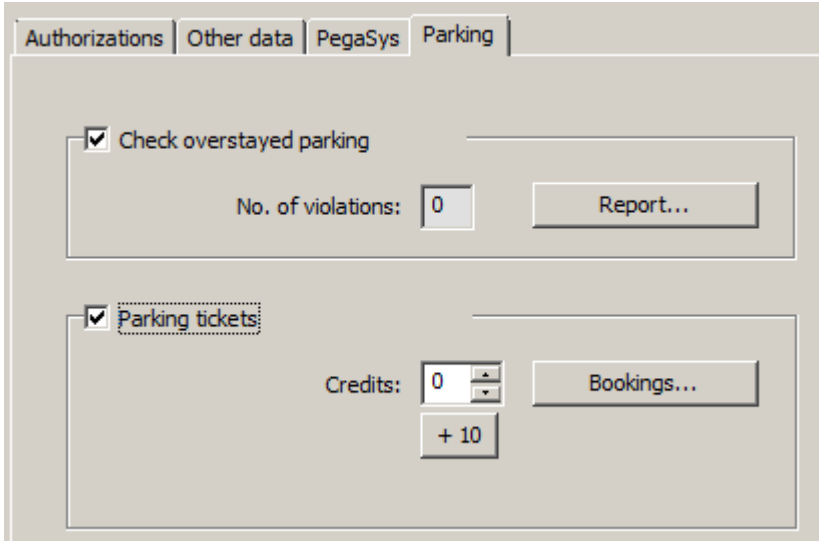
27.1 تجاوز مدة صف السيارات

تتيح هذه الميزة للمشغّل القيام بما يلي:
- اكتشاف حالات تجاوز مدة صف السيارات
- إظهار المخالفات على المحطات الطرفية لإدارة صف السيارات.
- السماح بخروج سيارة تجاوزت مدة الصف بعد إطلاق سراحها يدويًا فقط.
- الاحتفاظ بسجل المخالفات.
- التدقيق في حالات تجاوز مدة صف السيارات في أجهزة قراءة محددة،
- استثناء أشخاص بعينهم من عمليات التدقيق في حالات تجاوز مدة صف السيارات.

بإمكان ميزة إدارة أماكن صف السيارات الكشف عن المستخدمين الذين تركوا سياراتهم في موقف السيارات لمدة 24 ساعة أو أكثر.

في حالة تجاوز الحد الأقصى من الوقت، سيظل الحاجز مغلقًا عند تمرير البطاقة ويُمنع الخروج. وتظهر رسالة في محطات عمل مشغّل موقف السيارات. ويجب على المُشغّل قبول الرسالة مما يؤدي إلى تنشيط بث مباشر بالفيديو للمخرج المقصود. يظهر رقم هاتف المخرج لدى المشغّل ليتمكن من الاتصال بالسائق بشكل مباشر.

بعد الاتصال بالسائق والتحقق منه، يستطيع المشغّل إزالة الحاجز يدويًا من خلال الواجهة لديه ولكن عليه إدخال تعليق. سيتم تسجيل الحادث مع وقت الدخول ووقت الخروج والتعليق.



اكتشاف حالات تجاوز مدة صف السيارات والتعامل معها

يسجل النظام أوقات الدخول والخروج لكل مركبة، إذا كان النظام بأكمله متصلاً بالإنترنت. إذا لم يكن LAC متصلاً بالإنترنت، فسيسمح بالدخول أو يرفضه استنادًا إلى بياناته المخزنة.
- إذا كان السائق معفىً من عمليات التدقيق في حالات تجاوز مدة صف السيارات، فسيسمح MAC بالخروج من خلال الحاجز في أي حالة.
- إذا لم يكن السائق معفىً من عمليات التدقيق، فستتم مقارنة وقت الخروج من إدخال وقت دخول العربة الأخير المسجّل.
  - إذا كانت مدة الإقامة بكاملها أقل من الحد الأقصى المسموح به، فسيُسمح بالخروج.
  - وبخلاف ذلك، يبقى الحاجز مغلقًا وسيتعين على السائق الاتصال بمسؤول ساحة الانتظار لفتح الحاجز يدويًا.

إحصاءات حول تجاوز مدة صف السيارات

توفر هذه الميزة نظرة عامة على عدد المركبات التي تجاوزت مدة صف السيارات في ساحة الانتظار.

27.2 تذاكر صف السيارات

تتيح هذه الميزة الفرصة للعملاء بإصدار تذاكر لصف السيارات المتعدد لعدد محدد من إجراءات صف السيارات الأحادية (قابلة للتكوين).

يحصل المستخدم المصرح به على تذكرة لصف السيارات تسمح له بدخول ساحة انتظار واحدة من الساحات المعينة.
قبل الإقرار بالوصول إلى ساحة الانتظار، يقوم النظام بمراجعة إذا كان هناك على الأقل إجراء واحد من إجراءات صف السيارات على التذكرة أم لا.

- إذا كان الأمر كذلك، فسيتم السماح بالوصول وستقل الأصول الموجودة على التذكرة بمعدل أصل واحد
- أما إذا لم يكن الأمر كذلك، فسيتم رفض الوصول.

عند دخول ساحة انتظار السيارات، سيتم تحديد الفاصل الزمني الذي سيتم السماح لمالك التذكرة خلاله بدخول الساحة ومغادرتها كما يشاء. ويمتد هذا الفاصل الزمني بحيث يساوي الحد الأقصى لفترة الانتظار داخل ساحة السيارات (الإعداد الافتراضي: 24 ساعة).
يشير امتلاك تذكرة لصف السيارات إلى امتلاكك لإذن استخدام أي من ساحات الانتظار المسموح بها لمدة يوم واحد (24 ساعة). وخلال هذه الفترة الزمنية، من الممكن أيضًا تغيير ساحة الانتظار أو مكان صف السيارات

- في حالة تجاوز مالك تذكرة صف السيارات المتعدد للحد الأقصى للفترة الزمنية المسموح بها لانتظار السيارات، ستتناقص الأصول الموجودة على تذكرة صف السيارة تبعًا لذلك. وقد يؤدي ذلك أيضًا إلى تناقص الأصول والوصول إلى أصول سالبة! وفي هذه الحالة، تنطبق القاعدة نفسها كما هي الحال مع صف السيارات المتأخر: يجب تحرير المخرج يدويًا وسيتم تسجيل الحادث.
- في حالة تجاوز مالك تذكرة الصف المتعدد للسيارات للفترة الزمنية الأولية (على سبيل المثال، الدخول والمغادرة بشكل متكرر) دون تجاوز الحد الأقصى للفترة الزمنية المسموح بها لانتظار السيارات، ستتناقص الأصول بمعدل أصل واحد، وسيتم السماح بالخروج.

إدارة أرصدة التذاكر

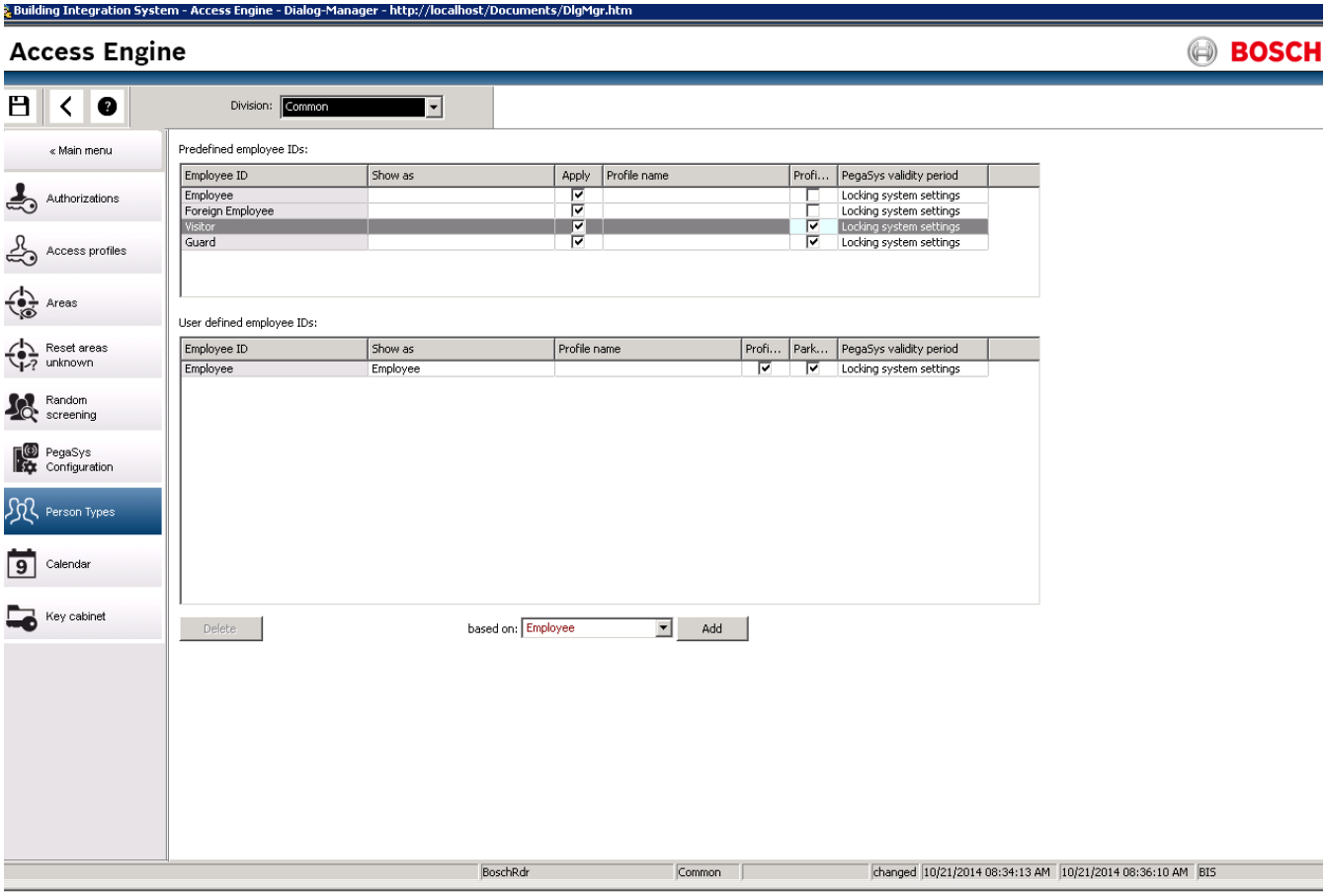
يتم حفظ الأصول الحالية لشخص ما في قاعدة بيانات خاصة بمالكي تذاكر صف السيارات المتعدد. يعرض حقل الإدخال **أرصدة صف السيارات** الموجود في مربع الحوار **البطاقات** القيمة الحالية ويمكن تحريرها. سيتم تسجيل جميع التعديلات الموجودة في هذا الحقل وحفظها في قاعدة البيانات.
لا يمكن تحرير أرصدة صف السيارات إلا في حالة امتلاك المشغل لإذن خاص لمربع حوار البطاقات (راجع **إذن مربع الحوار** الموجود في "مستعرض التكوين").
يلزم توفر الإذن الخاص نفسه لاستخدام مربع حوار البيانات الشاملة لهذا الغرض.

إشعار!
يمكن لحامل البطاقة حمل بطاقات عديدة. تتمثل الأصول الخاصة بصف السيارات في حفظ ما يتعلق بالشخص، ولذلك لا يؤدي تغيير البطاقة إلى أي مشكلة بالنسبة لحساب الأصول.

تعيين تذاكر صف السيارات المتعدد

بالنسبة لتعيين تذاكر صف السيارات المتعدد، ينطبق ما يلي:

- الأشخاص الحاصلون على الدورات التدريبية المخصصة المحددة في مجال شؤون الأفراد هم فقط المصرح لهم بالحصول على تذكرة للصف المتعدد للسيارات. ويمكن التعبير عن ذلك بواسطة المعلمات في مربع حوار **أنواع الأشخاص**.



- في حالة وقوع الأصول الموجودة على التذكرة دون القيمة المضبوطة (القيمة الافتراضية = 4)، سيتم إخطار المالك تلقائيًا عن طريق البريد الإلكتروني.

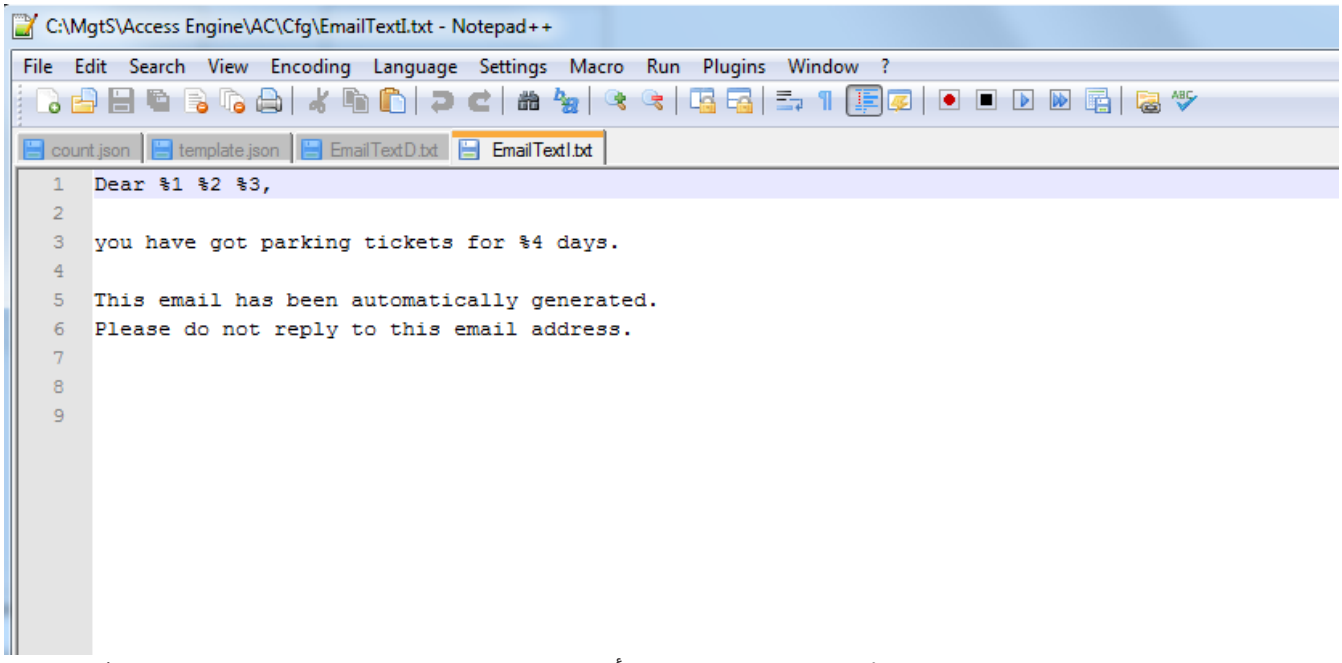
يتسنى للمشغل التحقق من الأصول الموجودة بالتذكرة في أي وقت وإجراء التصحيحات إن لزم الأمر. سيتم تسجيل جميع التصحيحات وحفظها في قاعدة البيانات.

يسمح النظام بزيادة الأصول لمجموعات الموظفين الكاملة حسب القيمة (س). وسيتم إخطار المالكين عن طريق البريد الإلكتروني.

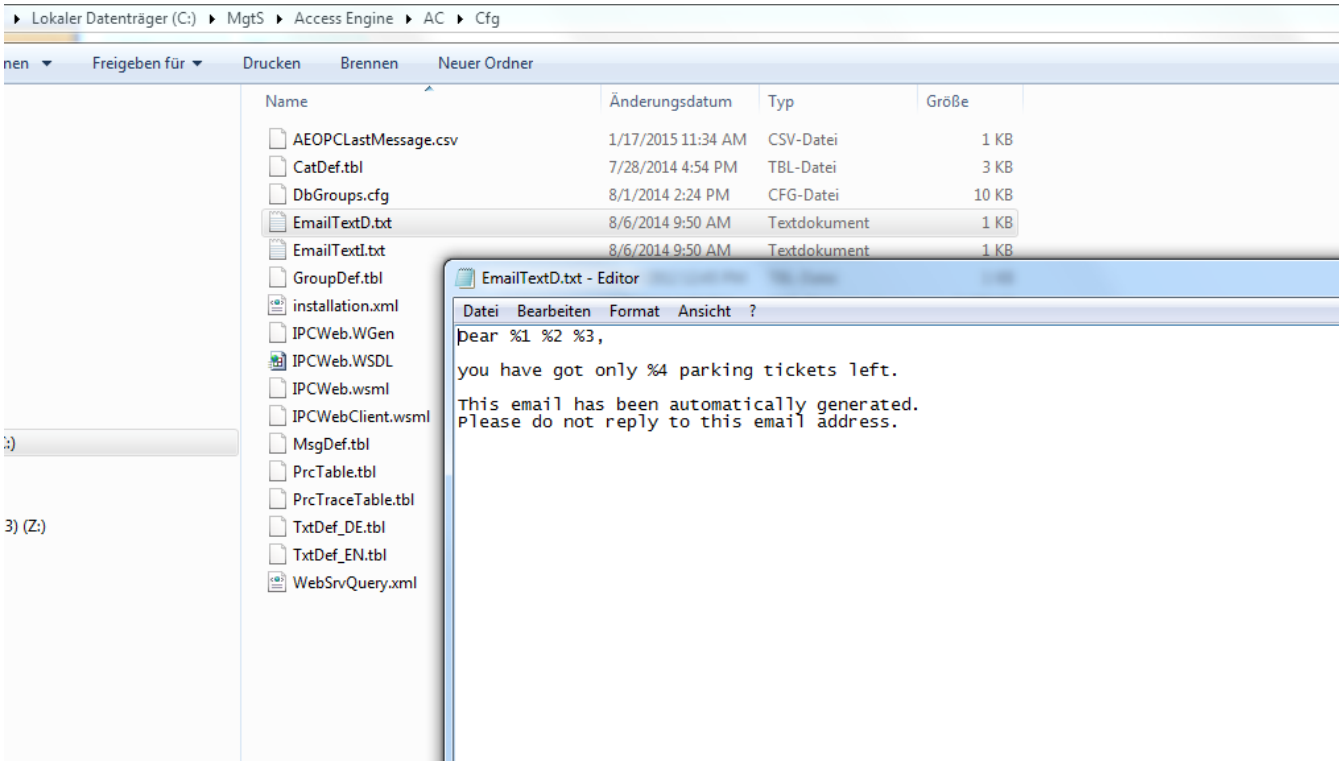
لتكوين رسالة البريد الإلكتروني، انتقل إلى دليل التثبيت الخاص بـ BIS ACE لديك. حدد الدليل: **<مسار التثبيت لديك>\MgtS\AccessEngine\AC\Cfg\.**

في هذا الدليل، سيتوفر أمامك خياران:

- تحرير **EmailTextI.txt** لإنشاء نص رسالة بأن حساب التذكرة قد تمت زيادته:



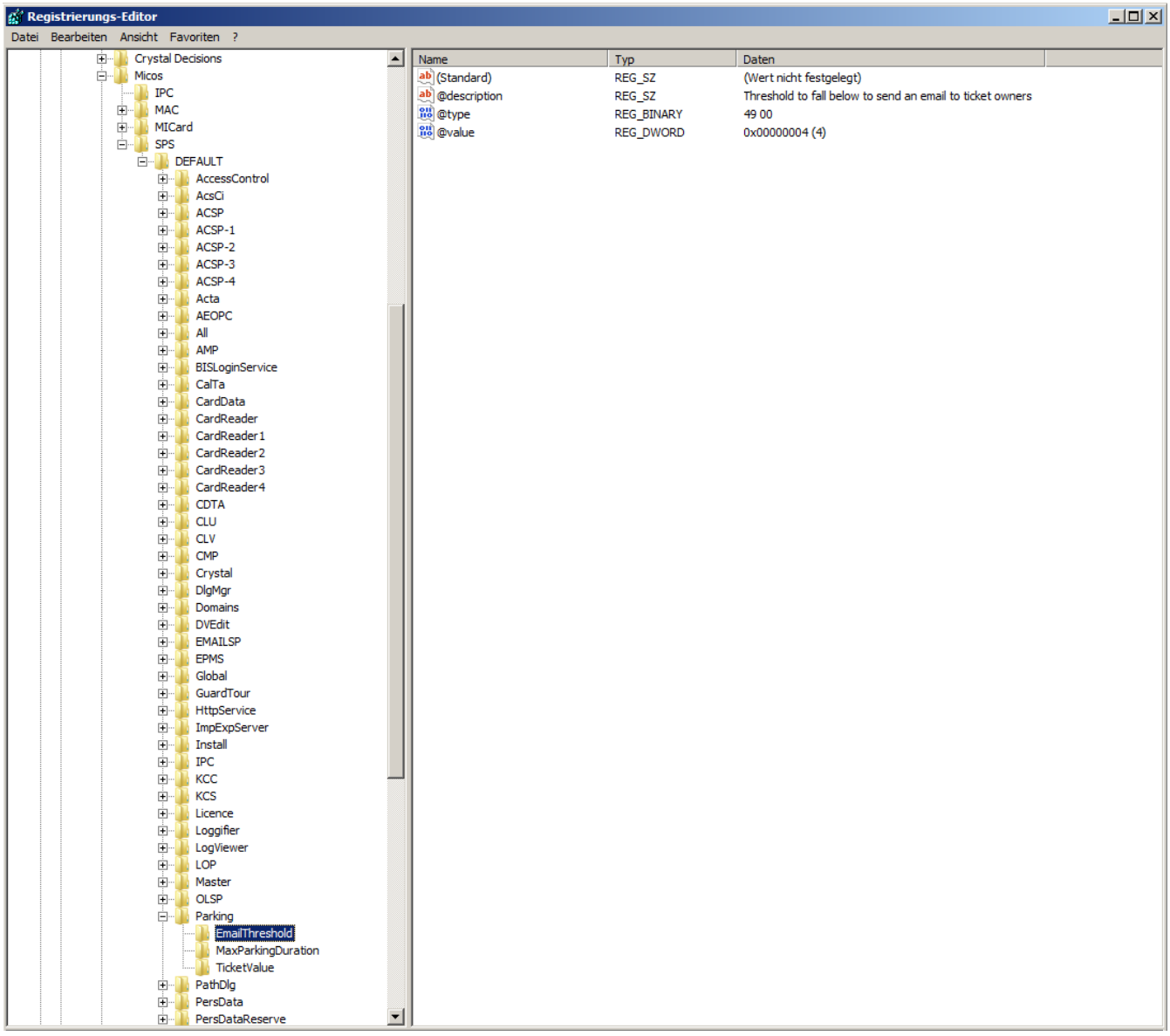
- تحرير **EmailTextI.txt** لإنشاء نص رسالة بأنه تم بلوغ حد البريد الإلكتروني الذي تم تكوينه (4 في المثال):



إشعار!

تشير أحرف البدل 1% و2% و3% في السطر الأول من الرسائل إلى مخاطبة المستخدم، وستتم تعبئتها بالبطاقة المعنية، على سبيل المثال "السيد/ سعيد سالم،".

يمكن تعيين القيمة الحدية نفسها في "سجل صف السيارات" ضمن **:Micos\SPS\DEFAULT\Parking\EmailThreshold**



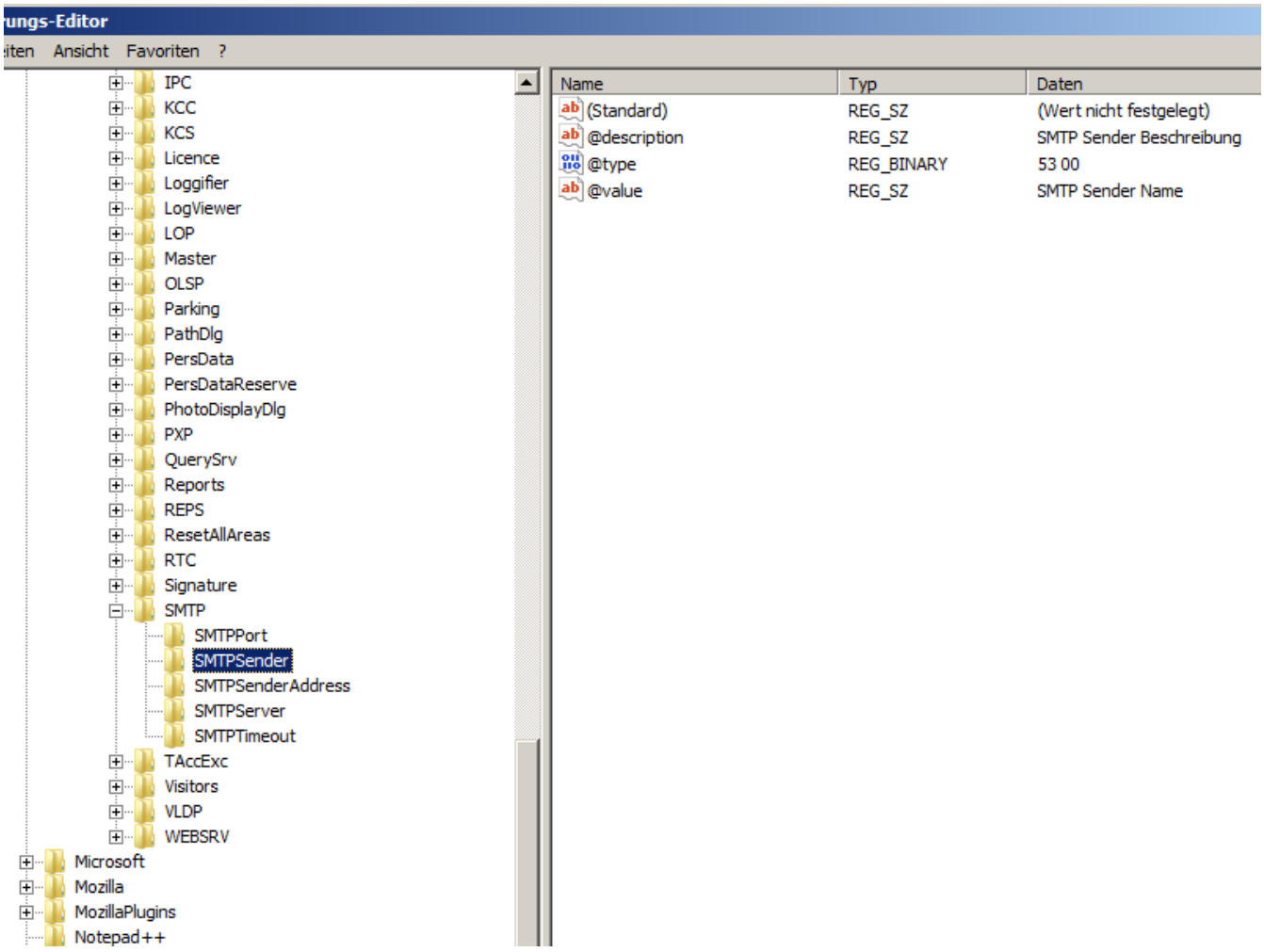
يوضح المثال الإعداد الافتراضي المتمثل في 4.

وعلى هذا المنوال، يمكن تعيين الميزتين الأخريين ضمن **صف السيارات**:

- **MaxParkingDuration**: الإعداد الافتراضي هو 23:59 ساعة
- **TicketValue**: الإعداد الافتراضي هو 10 مرات لصف السيارات.

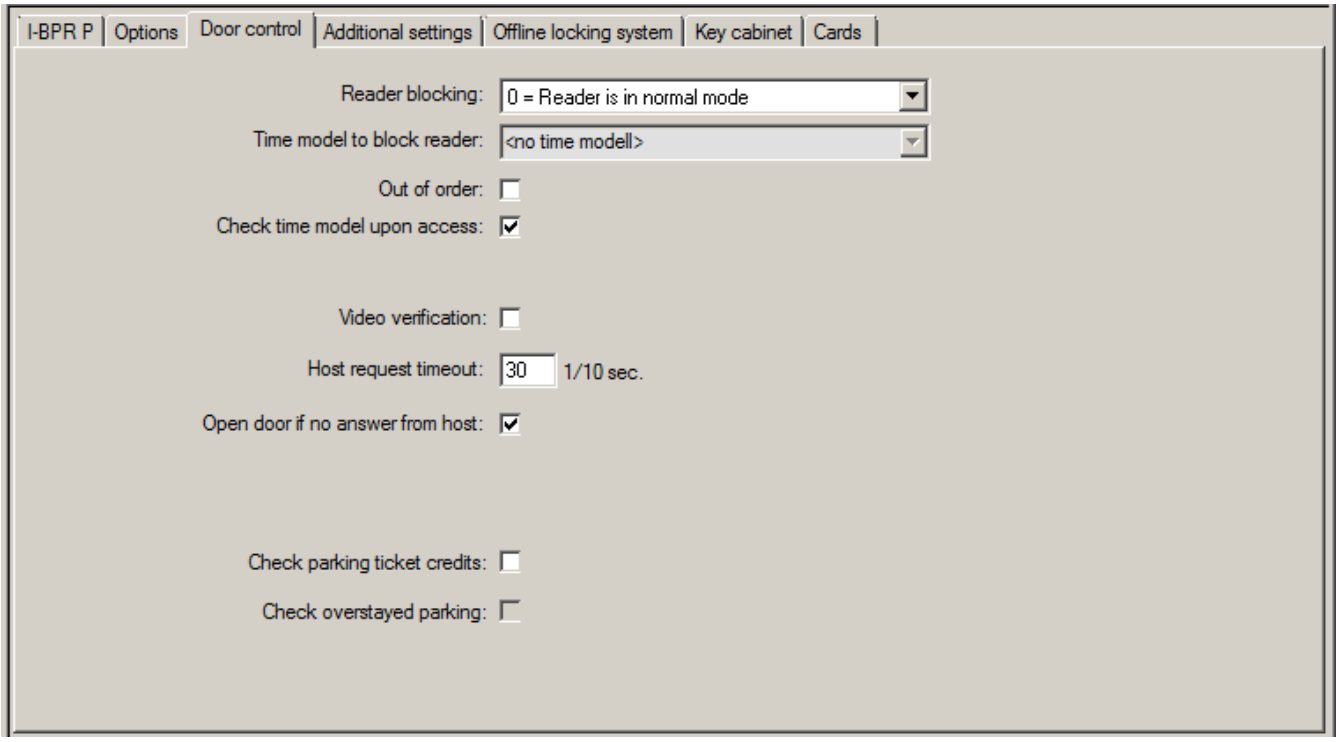
إعدادات SMTP

استخدم محرر التسجيل لتكوين **إعدادات SMTP**: لاستخدام البريد الإلكتروني في بيئة إدارة صف السيارات



تحديث الأرصدة عند الوصول

عند وصول مالك تذكرة الصف المتعدد للسيارات، يقوم النظام بتحديد التذكرة لتقليل عدد الأصول. أما إذا كانت الأصول تبلغ صفرًا أو أقل، فسيتم رفض الوصول.



- لتكوين فحص التذكرة، قم بتنشيط خانة الاختيار **التحقق من أرصدة تذاكر الانتظار.**
- **للتحقق من الانتظار الذي يتجاوز الفترة المحددة، قم بتنشيط خانة الاختيار "التحقق من الانتظار الذي يتجاوز الفترة المحددة".**

قبل الإقرار بالوصول إلى ساحة الانتظار، يتحقق النظام من بقاء إجراء واحد من إجراءات صف السيارات على التذكرة أم لا.

- إذا كان الأمر كذلك، فسيتم السماح بالوصول وستقل الأصول الموجودة على التذكرة بمقدار أصل واحد ما لم يحدث أي تغيير في منطقة الانتظار خلال الفترة الزمنية المسموح بها (24 ساعة).
- أما إذا لم يكن الأمر كذلك، فسيتم رفض الوصول.

إرسال إخطار البريد الإلكتروني في حالة بلوغ عدد الأصول دون الحد الأدنى

في حالة وقوع الأصول الموجودة على التذكرة دون القيمة المعينة المحددة (على سبيل المثال 4)، سيتم إخطار مالك التذكرة تلقائيًا عن طريق البريد الإلكتروني.

في حالة تعذر وصول البريد الإلكتروني لمالك التذكرة، سيتم إرسال رسالة خطأ إلى BIS.

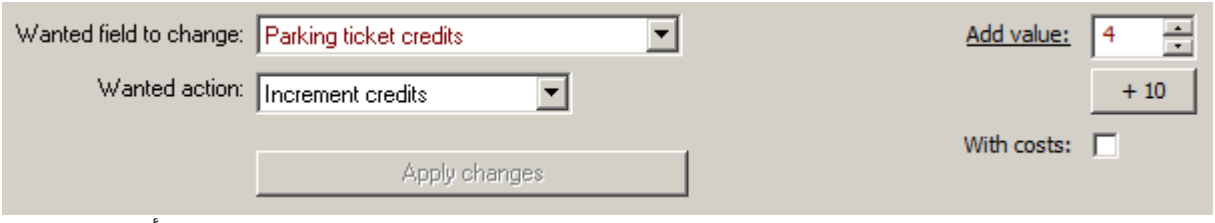
أرصدة التذاكر

يتم عرض الأصول الشخصية لمالك تذكرة صف السيارات المتعدد في أحد الحقول في "مربع حوار البيانات الرئيسية" ضمن **أرصدة تذاكر صف السيارات**.

يتسنى للمشغل تحرير قيمة أصول التذكرة في أي وقت. سيتم تسجيل أي تعديلات ووضعها في قاعدة البيانات.

ويمكن تعديل أصول التذكرة أيضًا لمجموعات كاملة من الأفراد. بالنسبة لهذا الأمر، يتوفر حقل الإدخال **أرصدة تذاكر صف السيارات** في مربع الحوار **البيانات الشاملة**. يتم تحديد مجموعة من الأشخاص عبر وظائف التصفية في مربع الحوار **البيانات الشاملة**. وبعد ذلك، يتم إدخال قيمة دلتا (على سبيل المثال، "ن") في الحقل **أرصدة تذاكر صف السيارات**.

ويؤدي ذلك إلى زيادة قيمة أصول صف السيارات حسب القيمة "ن"، ويتلقى الأشخاص المشاركون في ذلك الأمر بريدًا إلكترونيًا يعلمهم بالأمر.



في حالة عدم وصول البريد الإلكتروني لمالكي التذكرة، سيتم إرسال رسائل خطأ إلى BIS.
سيتم جمع كل التعديلات الخاصة بأصول صف السيارات في قاعدة بيانات ACE وتقديمها كتقرير في مربع الحوار الموجود أسفل **أرصدة تذاكر صف السيارات**.

27.3 تصدير أرقام استخدام أماكن صف السيارات

تعمل هذه الميزة على تمكين المشغّل من تقييم استخدام أماكن صف السيارات بشكل إحصائي. يقوم نظام التحكم في الوصول بتصدير أرقام استخدام أماكن صف السيارات إلى ملف CSV كما هو محدد مسبقًا بواسطة المشغّل.
يحتوي التصدير إلى ملف CSV على بيانات حول استخدام جميع ساحات انتظار السيارات من قِبل مالكي بطاقات متعددين مقسمين إلى فئات - على سبيل المثال، فئات الموظفين. يتم أخذ القيم تبعًا لفواصل زمنية دورية قابلة للتعيين بحيث لا يتعدى الحد الأقصى لطول الفاصل الزمني 15 دقيقة.
تشتمل بيانات أي نقطة في الوقت على ما يلي:

- التاريخ
- الوقت
- موقف السيارات
- عدد السيارات المتوقفة، مقسمة إلى:
  - مناطق انتظار
  - مجموعات المستخدمين (فئات الموظفين)

إشعار!
إذا قام حامل بطاقة فردي بتغيير فئة الموظفين، فستستمر بيانات التقرير من فترة سابقة ت في عرض التخصيص القديم.

يمكن تعيين مسار التصدير في محرر معلمة النظام ضمن **Default\TAccExc\PB-Dir. بمجرد إدخال دليل صالح، سيتم تصدير سعة واحدة لكل موقف سيارات.**

27.4 فحص تصدير "الصلاحية المتنقلة"

تسمح هذه الميزة للمشغّل بالتحقق من تصريحات صف السيارات في أماكن صف السيارات.
يتم إنشاء ملف CSV عند فواصل زمنية منتظمة تضم جميع مالكي التذاكر معًا إلى جانب معلومات إضافية حول مناطق صف السيارات. .
لإجراء التكوين، حدد محرر معلمة النظام ضمن **Default\PXP\Task0001...** وقم بتشغيل مسار التصدير واسم الملف ووضوح التصدير (أو إيقاف تشغيله على التوالي).

يتم تنفيذ التصدير عند فواصل زمنية قابلة للتكوين. تشتمل البيانات المصدرة على ما يلي:

- صلاحية البطاقة (حقل الإدخال **صالح حتى** في **أشخاص AC**)
- اسم الشخص المصرح له
- رقم تسجيل السيارة
- أرقام البطاقات المسجلة
- رقم الهاتف
- حالة البطاقة
- اسم ساحة انتظار السيارات أو منطقة صف السيارات إن أمكن
- حقول احتياطية (اختيارية في حالة تكوينها)

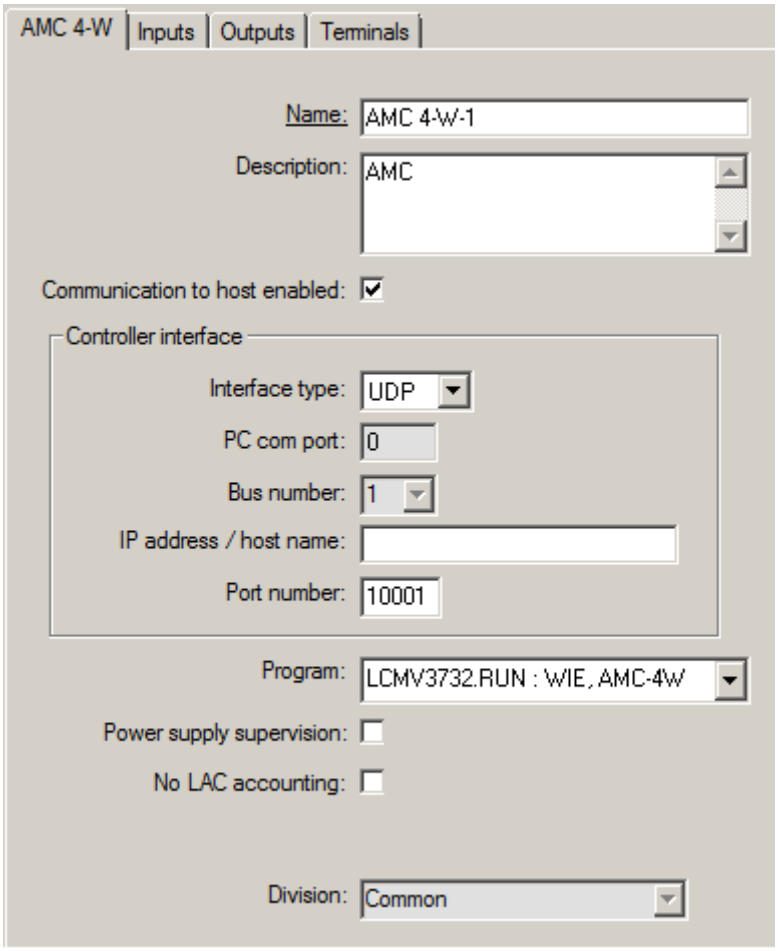
27.5 تخويلات لمناطق انتظار عديدة

تشتمل بعض ساحات انتظار السيارات على سائقين معاقين وأصحاء على السواء. وفي هذه الحالة، تنطبق القواعد التالية:

- يُسمح لمالكي التذاكر الموسمية فقط بالقيادة طالما هناك حارات متوفرة لصف السيارات للأشخاص الأصحاء من غير المعاقين.
- يُسمح للأشخاص المعاقين بالقيادة طالما هناك حارات متوفرة لصف السيارات للمعاقين وغير المعاقين على السواء.

إشعار!
يفترض هذا مسبقًا أن مالكي التذاكر يتبعون اللوائح المنصوص عليها. وهذا يعني بصفة خاصة ما يلي:
لا يقوم الأشخاص غير المعاقين بصف السيارات في الحارات المخصصة للمعاقين
يستخدم الأشخاص المعاقون حارات صف السيارات الخاصة بهم حال توافرها

يتسنى للشخص ممن يمتلك تصريحات عديدة الوصول إلى كلا النوعين سواء تلك الخاصة بالأصحاء أو المعاقين. يحاول AMC حجز الشخص تبعًا للترتيب التسلسلي الذي تم تكوينه لمناطق صف السيارات. وفي حالة امتلاء إحدى المناطق تمامًا، سيتم البحث عن المنطقة المتوفرة التالية المصرح بها.
حساب العداد في MAC وAMC:
1) يتحكم جهاز AMC واحد في كل عمليات الدخول والخروج من منطقة صف السيارات:
=> يقوم جهاز AMC بالعد على طريقته الخاصة ويمكن تصحيحه من خلال جهاز MAC عند الاتصال بالإنترنت.
2) يتم توزيع عمليات الدخول إلى إحدى مناطق صف السيارات والخروج منها على أجهزة AMC مختلفة:
=> يقوم جهاز MAC بالعد لصالح جهاز AMC في حالة التشغيل عبر الإنترنت. عند التشغيل في حالة عدم الاتصال بالإنترنت، تسمح أجهزة AMC بالوصول (حال تكوينها تبعًا لذلك) ولكن لا يتم العد.
إذا كانت وحدات AMC متعددة تراقب منطقة صف سيارات واحدة، فيمكنك تنشيط خانة الاختيار **بدون حساب LAC** في تكوين جهاز AMC



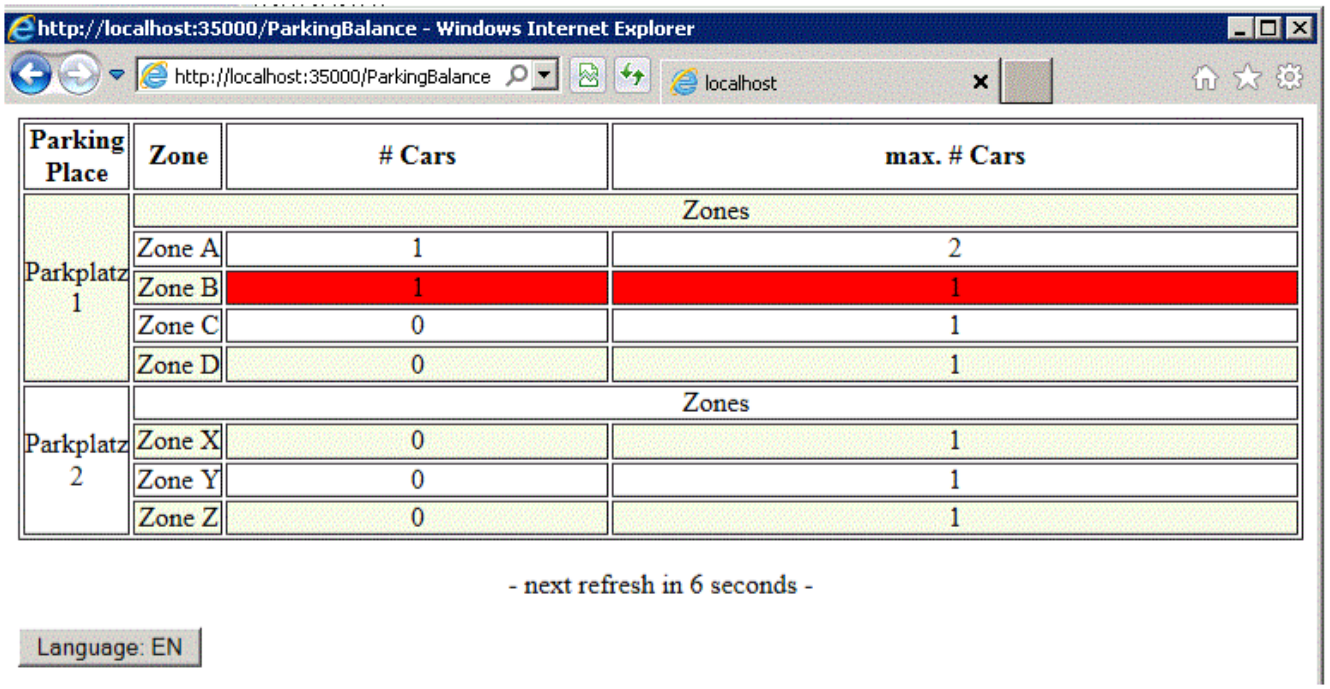
27.6 تقرير مكان صف السيارات

Parking lot list

Date 08.11.2013 , 14:51:23
Page 1

Parking area	Zone	Vehicle count	State
Main Park		51	
	Zone A	30	full
	Zone B	9	--
	Zone C	12	--
Building A		39	
	Zone A	30	full
	Zone B	9	--
Building B		39	
	Zone A	30	full
	Zone B	9	--

يعرض المثال الثاني **توازن صف السيارات** الأمور الممكنة من خلال خادم الويب. يتم عرض جميع الأماكن المخصصة لانتظار السيارات بما في ذلك عدادات الاستخدام الحالي لكل ساحات الانتظار. علاوةً على ما سبق، يشتمل المثال على زر اختيار اللغة لعرض مدى سهولة التبديل بين اللغتين العربية والإنجليزية. وتتم عملية الترجمة داخل صفحة الويب فقط.



27.7 إدارة ساحة انتظار السيارات الموسعة

المقدمة

بإمكان المشغّل ضبط عدد أماكن صف السيارات في منطقة لصف السيارات للتعويض للمركبات ذات الحجم غير القياسي، على سبيل المثال:

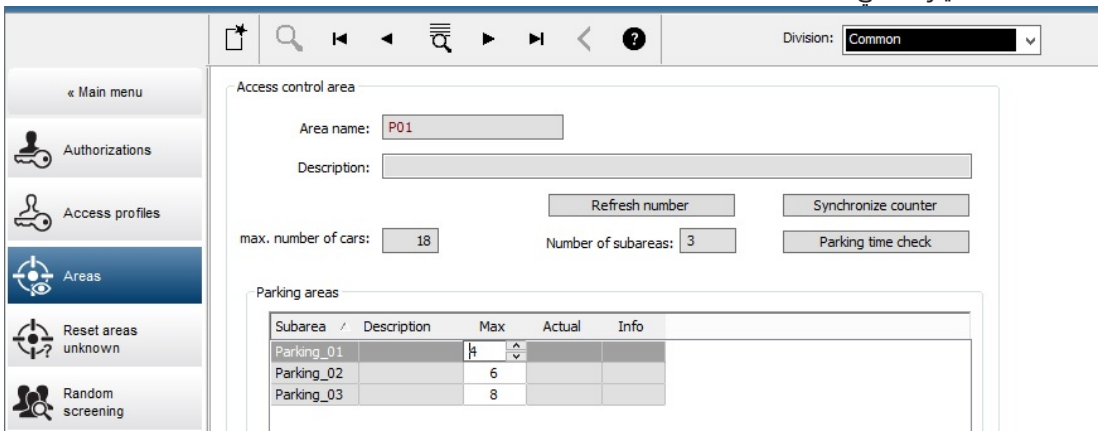
- الشاحنات
- وصول الأشخاص من ذوي الإعاقات
- الدراجات النارية

مسار مربع الحوار

القائمة الرئيسية > **بيانات النظام** > **المناطق**

الإجراء

1. تحديد منطقة صف السيارات
2. في جزء **مناطق صف السيارات**، اضبط القيمة في عمود **الحد الأقصى** إلى العدد الجديد لأماكن صف السيارات في هذه المنطقة.



ملاحظات:

- تُبطل الإعدادات في العمود **المدة القصوى** الإعدادات في تكوين **المناطق**. حدد **تكوين مناطق للسيارات** في الارتباط أدناه.

- تعني القيمة الصفرية 0 في عمود **المدة القصوى** غير محددة، جميع عمليات تعداد السيارات متوقفة عن التشغيل

راجع

- تكوين مناطق للسيارات, الصفحة *25*

28 إدارة جولات المراقبة والدوريات

مقدمة إلى جولات المراقبة

إن **جولة المراقبة** عبارة عن مسار حول المقر الرئيسي، تتخلله أجهزة قراءة البطاقات، حيث يتعين على الأشخاص من النوع **مراقب** تقديم بطاقة مراقب خاصة لإثبات زيارتهم للقارئ بطريقة فعلية.

ليس باستطاعة بطاقات المراقب فتح المداخل، ولكن يتم استخدامها لأغراض التعقب فقط. ولكي يتمكن المراقب من فتح المداخل، فهو يحتاج أيضًا إلى بطاقة وصول.

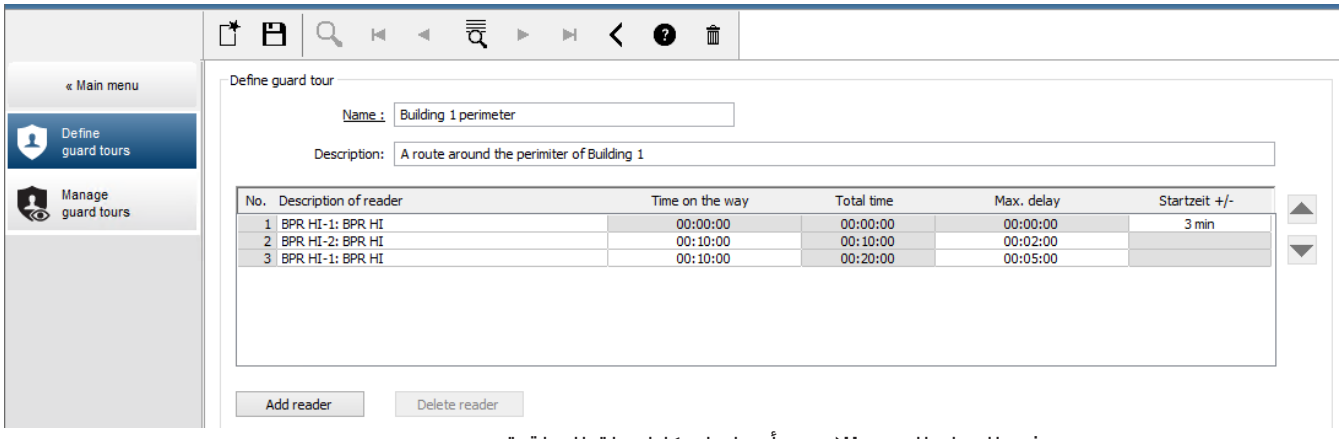
تتكوّن جولة المراقبة من مجموعة من أجهزة القراءة مع وقت السير التقريبي بينها. الحد الأقصى من التأخير المسموح به بين أجهزة القراءة والانحراف المسموح به (+/-) من وقت البدء هما أيضًا عن سمات جولة المراقبة. باستطاعة الانحرافات التي تقع خارج مستويات السماح المحددة هذه تشغيل الإنذارات على الأرجح، ويتم تسجيلها في **الدوريات**.

مقدمة إلى الدوريات

إن **الدورية** عبارة عن عبور لجولة المراقبة في وقت وتاريخ معينين. ويتم إنشاء كل دورية وتسجيلها ككيان فريد في النظام، لأغراض تتعلق بالبحث القضائي.

28.1 تعريف جولات المراقبة

حدد **جولات المراقبة** > **تعريف جولات المراقبة**

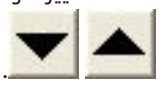


- في الحقل النصي **الاسم**، أدخل اسمًا لجولة المراقبة.
- في الحقل النصي **الوصف** ، أدخل اسمًا أكثر تفصيلاً للمسار (اختياري).

إضافة أجهزة قراءة إلى جولة المراقبة:

1. انقر فوق الزر **إضافة قارئ**.
   يتم إنشاء سطر في الجدول.
2. في العمود **وصف القارئ**، حدد قارئًا من القائمة المنسدلة.
3. أدخل قيمًا للانحرافات المسموح بها:
   - إذا كان هذا القارئ الأول في التسلسل، فأدخل في مربع **وقت البدء +/-** عددًا من الدقائق قبل وقت البدء أو بعده تبقى مسموحة كوقت بدء الدورية خلال جولة المراقبة.
   - إذا **لم يكن** هذا القارئ الأول في التسلسل، فأدخل، ضمن **الوقت على الطريق** الوقت (س س:د د:ث ث) المطلوب لانتقال المراقب بين القارئ الأول وهذا القارئ.
     يتم تجميع وقت الجولة الإجمالي في عمود **الوقت الإجمالي**.
4. ضمن **مهلة التأخير القصوى** أدخل الحد الأقصى الإضافي من **الوقت المستغرق في الطريق** الذي ما زال مسموحًا والذي يحول دون وضع علامة **متأخر** على الدورية.
5. أضف العدد الذي تريده من أجهزة القراءة. لاحظ أنه يمكن ظهور القارئ نفسه أكثر من مرة واحد في حال مرور جولة المراقبة عبره مرات متعددة أو في حال عودتها إليه.

- لحذف قارئ من التسلسل، حدد السطر وانقر فوق زر **حذف القارئ**.
- لتغيير موضع قارئ في التسلسل، حدد السطر وانقر فوق الزرين للأعلى/للأسفل



28.2 إدارة الدوريات

حدد **جولات المراقبة** > **إدارة جولات المراقبة**

جدولة دورية جديدة

لجدولة دورية مع جولة مراقبة معينة، تابع على الشكل التالي:

1. تأكد من أن بطاقة المراقب المطلوبة للدورية موجودة لديك، وانتقل إلى قارئ بطاقات وصول مكوّن أو قارئ تسجيل متصل بشكل مباشر.
2. في عمود **جولات المراقبة**، حدد إحدى جولات المراقبة التي تم تعريفها.
3. انقر فوق الزر **دورية جديدة...**.
   تظهر نافذة منبثقة.
4. في النافذة المنبثقة، غيّر جولة المراقبة في القائمة المنسدلة، إذا أردت ذلك.
5. إذا كان يجب أن تتضمن الدورية وقت بدء تم تحديده بشكل مسبق، فحدد **تعيين وقت البدء:**
   - أدخل تاريخ ووقت البدء.
   - إذا لزم الأمر، انقر فوق مربع الزيادة والنقصان **وقت البدء +/-** لضبط السماح بحالات البدء المتأخر أو المبكر.
6. انقر فوق السهم لليمين وحدد القارئ الذي تريد استخدامه لتسجيل بطاقة المراقب. تجدر الإشارة إلى وجوب تكوين القارئ مسبقًا في النظام قبل أن يظهر هنا للتحديد.
7. انقر فوق زر علامة الجمع الخضراء لبدء قراءة بطاقة المراقب، وضع البطاقة على القارئ واتبع الإرشادات التي تنبثق.
   يتم تسجيل بطاقة المراقب لاستخدامها في الدورية.
8. كرر الخطوة السابقة لتسجيل بطاقات المراقب البديلة لهذه الدورية. لاحظ مع ذلك أن أول بطاقة يجب تقديمها خلال الدورية يجب أن تُستخدم في كل أجهزة القراءة خلال هذه الدورية.
9. انقر فوق الزر **موافق**. سيتم وضع علامة **مخططة** على جولة المراقبة المحددة في القائمة.

تعقب دورية

تنتقل جميع الدوريات النشطة والمخططة إلى أعلى القائمة. وفي حال وجود عدة دوريات مخططة أو نشطة، توضع الدورية المحددة في إطار أحمر اللون. انقر على الإطار للحصول على مزيد من المعلومات.
تبدأ الدورية عندما يقدم المراقب بطاقته عند أول قارئ في جولة المراقبة. يجب استخدام هذه البطاقة للقسم المتبقي من الدورية، حتى لو تم تحديد بطاقات بديلة للدورية.
تتغير **حالة** الدورية إلى **نشطة**.
يتلقى كل قارئ يتم الوصول إليه في الموعد المحدد علامة اختيار خضراء اللون - ✔. يظهر الوقت المجدول والوقت الفعلي بين أجهزة القراءة في الدورية المحددة حاليًا في النصف السفلي من نافذة مربع الحوار.
يتلقى كل قارئ يتم الوصول إليه في موعد متأخر عن الوقت المحدد بالإضافة إلى **مهلة التأخير القصوى** علامة اختيار حمراء اللون ⊘. وتوضع العلامة **متأخر** على الدورية.
في هذه الحالة، يتصل المراقب بالمشغّل لتأكيد عدم وجود أي مشكلة. عندئذٍ، ينقر المشغّل فوق الزر **استئناف الدورية**. يتلقى القارئ علامة اختيار خضراء اللون بالإضافة إلى "ج" إضافي - ✔C. باستطاعة المراقب الآن متابعة الدورية عند القارئ التالي.
عند حدوث تأخير عرضي ولكن غير ضار في دورية نشطة، يستطيع المراقب الاتصال بالمشغّل لضبط الجدول. أدخل عدد دقائق التأخير في مربع الزيادة والنقصان **التأخير (بالدقائق)** وانقر فوق الزر **تطبيق**.

إذا تعذر إكمال دورية كما هو مجدول، يستطيع المشغّل إيقافها قبل اكتمالها بالنقر فوق زر **مقاطعة**. تتغير **حالة** الدورية إلى **تم الإيقاف قبل الاكتمال**، وستسقط تحت جولات المراقبة النشطة والمخططة في القائمة.

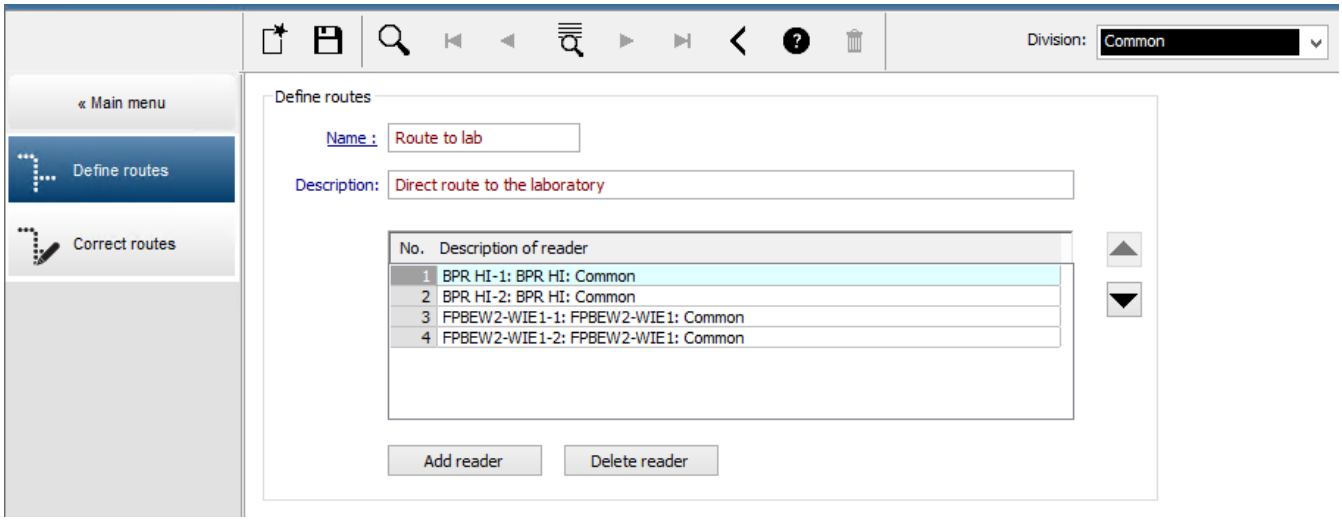
28.3 مراقبة الجولة (في السابق التحكم في المسار)

المقدمة

إن المسار (أو الجولة) عبارة عن تسلسل أجهزة قراءة يمكن فرضه على الأشخاص المحددين في نظام التحكم في الوصول، لتوجيه حركاتهم في المقر الرئيسي، بصرف النظر عن التخويلات الممنوحة للشخص. تقضي الاستخدامات النموذجية بفرض تسلسلات وصول دقيقة في البيئات الصناعية النظيفة أو المناطق الخاضعة للمراقبة الصحية أو تلك التي تتميز بمستوى أمان عالٍ.

تحديد المسارات

1. في القائمة الرئيسية، حدد **مراقبة الجولة** > **تحديد المسارات**
2. أدخل اسمًا للمسار (لغاية 16 حرفًا)
3. أدخل وصفًا أكثر تفصيلاً (اختياري)
4. كما هو الحال مع جولات المراقبة، انقر فوق الزر **إضافة قارئ** لإضافة تسلسل أجهزة القراءة. استخدم أزرار الأسهم لتغيير موضع قارئ في التسلسل، وانقر فوق الزر **حذف القارئ** لإزالته.



تعيين مسار إلى شخص

لتعيين مسار إلى شخص، تابع على الشكل التالي:

1. في القائمة الرئيسية، انقر فوق **بيانات الموظفين** > **البطاقات**
2. قم بتحميل سجل الموظف للشخص الذي يجب تعيينه.
3. على علامة التبويب **بيانات أخرى**، حدد خانة الاختيار **مراقبة الجولة**
4. من القائمة المنسدلة إلى جانبها، حدد مسارًا محددًا (لتحديد مسار، راجع القسم السابق).
5. احفظ سجل الموظف.

يتم تنشيط المسار عندما يقدم الشخص المعين بطاقته لدى أول قارئ في المسار. يجب أن يتم الآن استخدام أجهزة القراءة الأخرى في المسار بالتسلسل المحدد، أي أن القارئ التالي فقط في التسلسل سوف يمنح حق الوصول. بعد الانتهاء من عبور المسار بشكل كامل، باستطاعة الشخص أن يحجز لدى أي قارئ آخر ضمن تصريحاته.

تصحيح المسارات ومراقبتها

1. في القائمة الرئيسية، حدد **مراقبة الجولة** > **تصحيح المسارات**
2. قم بتحميل سجل الموظف للشخص الذي تم تعيينه إلى المسار.

3. لتحديد موقع ذلك الشخص على المسار، انقر فوق الزر **تحديد موقع**.
4. تتلقى أجهزة القراءة التي تم اجتيازها بطريقة ناجحة علامة اختيار خضراء ✔ في القائمة.
5. لإعادة تعيين موقع شخص على المسار أو لتصحيح موقعه، انقر فوق الزر **تعيين موقع**.

29 الفحص العشوائي للموظفين

عملية الفحص العشوائي

1. يقدم حامل البطاقة بطاقته إلى قارئ تم تكوينه لإجراء فحص عشوائي.

ملحوظة

وحدهم الأشخاص المصرح لهم بالمرور من المدخل في الاتجاه المحدد هم الذين يمكن اختيارهم عشوائيًا. نظرًا لإخضاع التخويلات للفحص قبل إجراء الفحص العشوائي، فسيُحظر أي شخص غير مصرح له على الفور، ولن تتضمنه عملية الاختيار.

2. إذا اختارت أداة الاختيار العشوائي هذا الشخص من أجل الفحص، فستُحظَر بطاقته عبر النظام بالكامل.
   - ويُسجَل الحدث في سجل أحداث النظام.
   - يتلقى مربع الحوار **الحظر** إدخالاً لفترة زمنية غير محدودة عليه علامة **فحص عشوائي**. [الشكل أدناه - رقم 1]
   - يعرض شريط الحالة الخاص بمربعات حوار بيانات الموظفين "مؤشرات LED" المحظورة (الضوء الأحمر) ومعها "الفحص العشوائي" (الضوء البنفسجي الوامض).

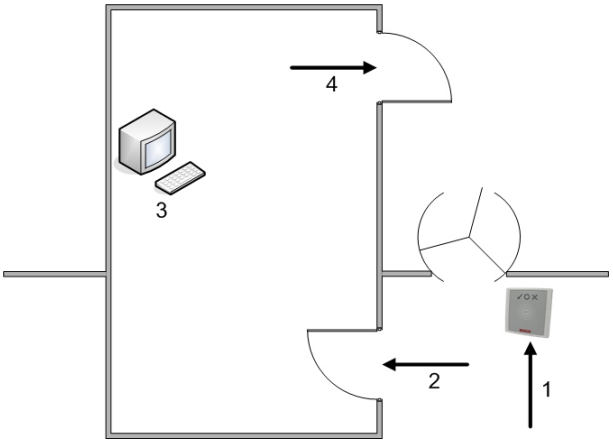
إشعار!

الأشخاص الذين تم تعيين معلمة **مُستثنى من الفحص العشوائي** لهم (في مربع حوار **البطاقات**، علامة التبويب **بيانات أخرى**) لا تشملهم عملية الفحص.

3. ويُدعى الشخص الذي تم اختياره عشوائيًا إلى فحوصات أخرى في خزانة أمنية منفصلة.
4. بعد إجراء هذه الفحوصات، يعيد حارس الأمن تعيين الحظر في مربع الحوار **الحظر** على النحو التالي:
   - حدد الحظر المناسب في قائمة **الحظر** بأدوات تحكم القائمة.
   - انقر فوق الزر **حذف**.
   - أكّد الحذف عن طريق النقر فوق **نعم**.

يستطيع الآن الشخص الذي خضع للفحص معاودة استخدام بطاقته في كل أجهزة القراءة التي صُرح له باستخدامها.

مثال على تخطيط غرفة الفحص العشوائي



1 - تقديم البطاقة - الفحص - الحظر عبر كل قطاعات النظام
2- يدخل حامل البطاقة الخزانة الأمنية
3= يخضع حامل البطاقة للتفتيش ثم يُرفع الحظر عن بطاقته عبر مربع الحوار.
4 = يغادر حامل البطاقة الخزانة الأمنية، من دون تقديم بطاقته إلى القارئ مرة أخرى.

إشعار!

تتحقق النسبة المئوية للفحص بطريقة تراكمية مع مرور الوقت. على سبيل الوصول، عند وصول الفحص العشوائي إلى 10%، يستمر وجود احتمال (1 في 100، أي 1/10 1/10 x) باختيار شخصين متتاليين.

30 استخدام عارض الأحداث

المقدمة

يسمح "عارض الأحداث" لمشغّلين ملائمين مخولين بفحص الأحداث التي تم تسجيلها بواسطة النظام، وبإنتاج تقارير مطبوعة أو على الشاشة أو كملفات .csv.

لاسترداد وعرض السجلات المطلوبة من قاعدة بيانات سجلات الأحداث، عيّن معايير التصفية، وانقر فوق **تحديث** . قد تستغرق هذه العملية بعض الدقائق، وهذا يتوقف على كمية البيانات المطلوبة.

يمكن تعيين معايير التصفية بطرق مختلفة:

نسبي لتحديد أحداث بالنسبة إلى الوقت الحالي.

الفاصل الزمني لتحديد أحداث ضمن فاصل زمني قابل للتحديد بطريقة اختيارية

الإجمالي لتحديد أحداث بصرف النظر عن وقت حدوثها

الشروط الأساسية

سجّلت دخولك إلى مدير مربع الحوار.

مسار مربع الحوار

القائمة الرئيسية في مدير مربع الحوار > **التقارير** > **عارض الأحداث**

30.1 تعيين معايير لتصفية الوقت بالنسبة إلى الحاضر

1. ضمن **الفترة الزمنية**، حدد الزر التبادلي **نسبي**
2. في المربع **بحث ضمن آخر**، حدد عدد وحدات الوقت التي يجب البحث فيها، واختر الوحدات التي يجب استخدامها، على سبيل المثال، الأسابيع، الأيام، الساعات، الدقائق، الثواني.
3. في قائمة **أنواع الأحداث**، حدد فئة الأحداث التي يجب البحث فيها، ثم أنواع الأحداث التي تثير اهتمامك.
4. في قائمة **العدد الأقصى**، حدد عدد الأحداث التي يحاول عارض الأحداث تلقيها. لأسباب تتعلق بالأداء، **من غير** المستحسن ترك القيمة **(غير محددة)**.
5. حدد معايير تصفية أخرى تهمك:
   - اسم العائلة
   - الاسم الأول
   - الرقم الشخصي
   - رقم البطاقة
   - المستخدم (أي مشغّل النظام)
   - اسم الجهاز
   - اسم المنطقة.

- انقر فوق **تحديث** لبدء تجميع الأحداث، وفوق **إلغاء** للتوقف.
- انقر فوق لحفظ النتائج، أو فوق لطباعتها.
- انقر فوق لمسح النتائج لإجراء بحث آخر.

30.2 تعيين معايير التصفية لفاصل زمني

1. ضمن **الفترة الزمنية**، حدد الزر التبادلي **الفاصل الزمني**

2. في منتقيات التاريخ **الوقت من، الوقت حتى** ، حدد بداية ونهاية الفترة التي يجب البحث فيها عن أحداث.
3. في قائمة **أنواع الأحداث**، حدد فئة الأحداث التي يجب البحث فيها، ثم أنواع الأحداث التي تثير اهتمامك.
4. في قائمة **العدد الأقصى**، حدد عدد الأحداث التي يحاول عارض الأحداث تلقيها. لأسباب تتعلق بالأداء، **من غير** المستحسن ترك القيمة **(غير محددة)**.
5. حدد معايير تصفية أخرى تهمك:
   - اسم العائلة
   - الاسم الأول
   - الرقم الشخصي
   - رقم البطاقة
   - المستخدم (أي مشغّل النظام)
   - اسم الجهاز
   - اسم المنطقة.

- انقر فوق **تحديث** لبدء تجميع الأحداث، وفوق **إلغاء** للتوقف.
- انقر فوق لحفظ النتائج، أو فوق لطباعتها.
- انقر فوق لمسح النتائج لإجراء بحث آخر.

30.3 تعيين معايير التصفية بصرف النظر عن الوقت

1. ضمن **الفترة الزمنية**، حدد الزر التبادلي **الإجمالي**
2. في قائمة **أنواع الأحداث**، حدد فئة الأحداث التي يجب البحث فيها، ثم أنواع الأحداث التي تثير اهتمامك.
3. في قائمة **العدد الأقصى**، حدد عدد الأحداث التي يحاول عارض الأحداث تلقيها. لأسباب تتعلق بالأداء، **من غير** المستحسن ترك القيمة **(غير محددة)**.
4. حدد معايير تصفية أخرى تهمك:
   - اسم العائلة
   - الاسم الأول
   - الرقم الشخصي
   - رقم البطاقة
   - المستخدم (أي مشغّل النظام)
   - اسم الجهاز
   - اسم المنطقة.

- انقر فوق **تحديث** لبدء تجميع الأحداث، وفوق **إلغاء** للتوقف.
- انقر فوق لحفظ النتائج، أو فوق لطباعتها.
- انقر فوق لمسح النتائج لإجراء بحث آخر.

31 استخدام التقارير

يصف هذا القسم مجموعة من وظائف التقارير التي يمكن استخدامها لتصفية بيانات سجل النظام والأحداث، ولتقديمها بتنسيقات واضحة.

مسار مربع الحوار

القائمة الرئيسية > **التقارير**.

استخدام شريط أدوات التقارير

انقر فوق لعرض معاينة قبل الطباعة.

تحتوي المعاينة على شريط أدوات خاص بها:

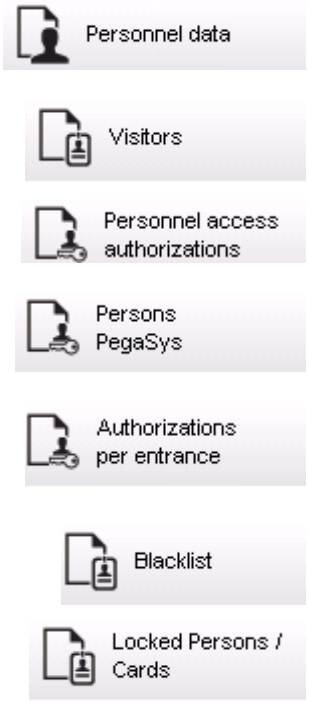
- انقر فوق ✕ للخروج من المعاينة قبل الطباعة.
- استخدم مفاتيح الأسهم ◀ ▶ 2 of 17 ◀ ▶ في شريط أدوات المعاينة للاستعراض للأمام وللخلف أو لتحديد صفحات فردية حسب رقم الصفحة.

- انقر فوق للطباعة على الفور، باستخدام طابعتك الافتراضية.
- انقر فوق للطباعة عبر مربع الحوار "إعداد الطباعة"، الذي يوفر لك المزيد من خيارات الطباعة.
- انقر فوق لتصدير التقرير إلى مجموعة من تنسيقات الملفات، بما في ذلك PDF وRTF وExcel.
- يمثل العدد الموجود إلى يسار شريط الأدوات:
  - العدد الإجمالي لإدخالات قاعدة البيانات الموجودة التي تتطابق مع معايير التصفية.
  - النسبة المئوية لإدخالات قاعدة البيانات هذه التي تظهر في المعاينة.

31.1 التقارير: البيانات الرئيسية

نظرة عامة على التقارير - البيانات الرئيسية

تتضمن تقارير البيانات الرئيسية كل البيانات المتعلقة بالأشخاص والزائرين والبطاقات وتخويلات الوصول الخاصة بهم. وعلاوة على ما سبق، يمكن عرض بيانات الجهاز وبيانات الشركة.



التقرير: بيانات الموظفين
يمكن تطبيق عاملي تصفية عند إنشاء التقارير.
تصفية الأشخاص: هنا، يجري المشغّل عملية التصفية استنادًا إلى حقول بيانات الموظفين العادية.
تصفية بطاقات الوصول: بإمكان المشغّل هنا إجراء التصفية استنادًا إلى أرقام البطاقات ونطاقات من الأرقام والحالة وحالة الحظر.

التقرير: الزائرون
بطريقة مماثلة لبيانات الموظفين، يمكن إنشاء تقارير الزائرين هنا. عند القيام بذلك، يبقى الوصول إلى كل بيانات الزائرين التي تم إنشاؤها ممكنًا، أيْ يمكن اختيار الزائرين المسجَّلين بالفعل ولكنهم لم يصلوا بعد.

التقرير: تخويلات وصول الموظفين
يقدم هذا التقرير نظرة عامة على تخويلات الوصول المسجَّلة على النظام ويعرض أيضًا الأشخاص الذين مُنحوا هذه التخويلات.
وفي إطار تطبيق عوامل التصفية، يمكن استخدام البيانات الشخصية وتحديد تخويلات معينة:
- بيانات الموظف: اللقب، الاسم الأول، رقم الموظف.
- التحقق من صلاحية كل التخويلات.
- اسم التخويل الذي ينطبق على المدخل.
- اسم نموذج الوقت - إن وجد.
- اتجاه المدخل.
- التحقق من صلاحية التخويل الخاص.

التقرير: القائمة المحظورة
في مربع الحوار هذا، يمكن طباعة قائمة تذكر بالتفصيل كل بطاقات الهوية أو مجموعة من بطاقات الهوية المختارة المراد إدراجها في القائمة المحظورة لأسباب متعددة.

التقرير: الأشخاص المحظورون/البطاقات المحظورة
يمكن استخدام مربع الحوار هذا لإنشاء تقارير تحتوي على بيانات حول كل الأشخاص المحظورين.
استخدم التواريخ للعثور على كتل ضمن فترات زمنية محددة.

التقرير: بيانات الجهاز
يمكن استخدام مربع الحوار هذا لإنشاء تقارير تستند إلى بيانات الجهاز، على سبيل المثال، اسم الجهاز أو نوعه.

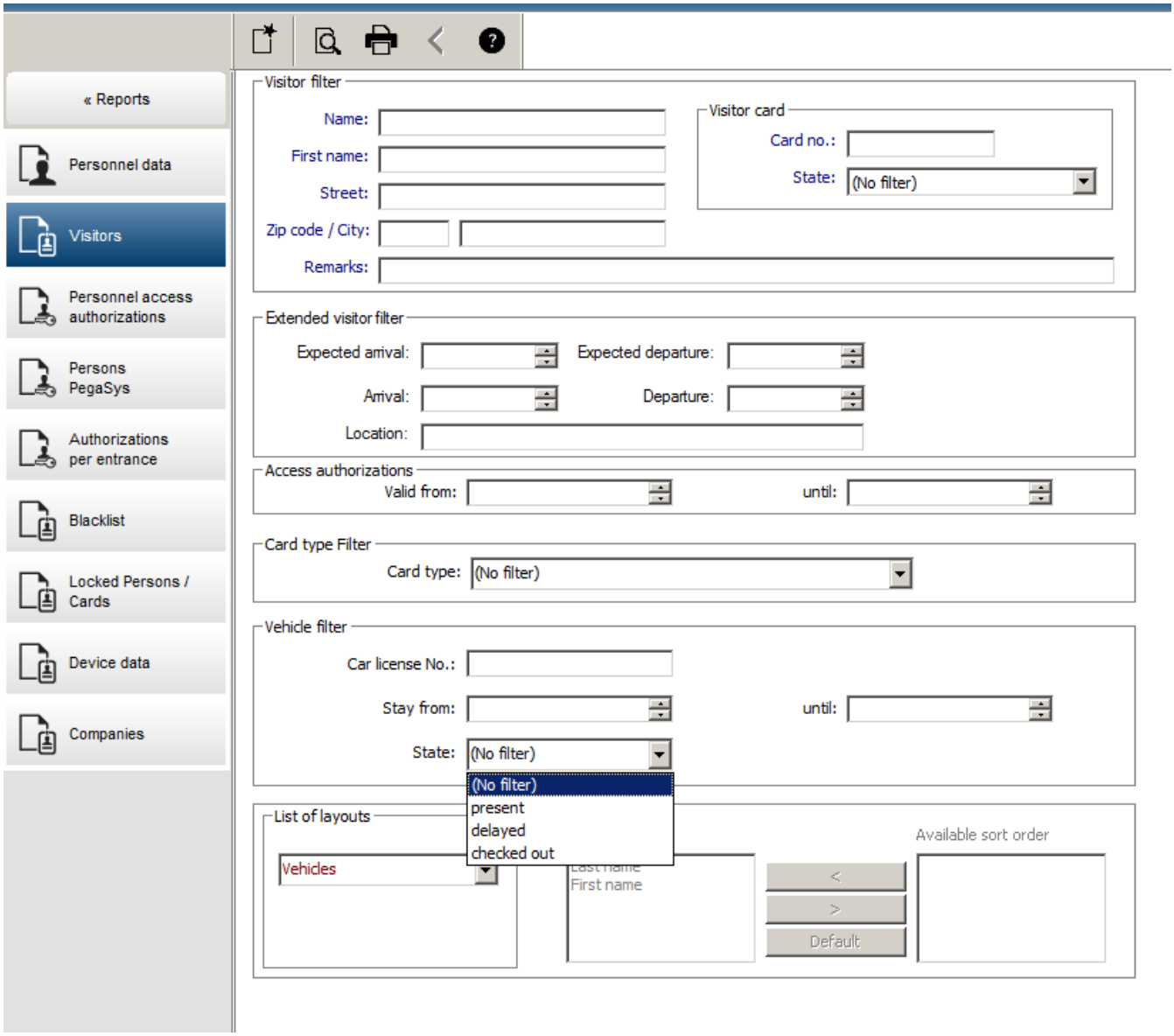
التقرير: الشركات
يُستخدم مربع حوار "تقرير الشركات" لدمج بيانات الشركة في قائمة ما.
استخدم العلامات النجمية، على سبيل المثال، للبحث عن شركات تبدأ بحرف معين.

31.1.1 إعداد تقرير حول المركبات

في مربع الحوار **التقارير > الزائرون** يمكن تحديد **المركبات** من قائمة التخطيط. وبمجرد تحديد **المركبات** تنشط منطقة مربع الحوار **عامل تصفية المركبات** ويمكن أن يستخدمها المشغِّل لتصفية المركبات وحالاتها.

وتُعرض الحالية وفق ما يلي:

- حاضر:لم تنته الزيارة ولا الوقت بعدُ.
- متأخر:لم تنته الزيارة بعدُ ولكن انتهى الوقت.
- سجَّل الخروج: أعاد الزائر كل بطاقات الوصول.



ويتوفر **التقرير الخاص بالمركبات** فقط للزائرين، بسبب أن عناصر تاريخ الوصول المتوقع وتاريخ المغادرة المتوقع وتاريخ الوصول وتاريخ المغادرة لا تتوفر إلا للزائرين في جدول قاعدة بيانات **الزائرون**.

ويذكر التقرير أرقام المركبات فقط والتي تُخزَّن في جدول قاعدة البيانات **الأشخاص**. ولذلك بمجرد تغيير رقم المركبة، يعرض التقرير نتائج أخرى.

ويجري حساب الفترة وفق ما يلي:

- إذا كان الزائر قد سجَّل المغادرة بالفعل، يُعرض الفرق بين وقت الوصول والمغادرة بالدقائق.
- إذا لم يسجّل الزائر المغادرة بعد، يُعرض الوقت المنقضي من وقت الوصول إلى الوقت الحالي بالدقائق.

Access Engine

Vehicle

Datum 02.07.2014 , 14:26:14
Seite 1

Lastname	Firstname Status	Arrival Departure Duration	Vehicle Last area	Person Last area
Neuer Besucher mit Langem Namen	**Vorname** present	02.07.2014 14:21 02.07.2014 14:30 0h 5'	AC BB 5678 parkplatz_01	ASB
Test	**Visitor** too late	01.07.2014 09:10 02.07.2014 12:00 29h 16'	AC AA 1234 parkplatz_01	ISB
Testbesucher mit sehr lagem Namen	**Besucher mit gaaaaaanz langem namen** departed	01.07.2014 07:30 01.07.2014 12:00 4h 30'	AC AA 2345 AUSSEN	AUSSEN

31.2 التقارير: بيانات النظام

التقارير - بيانات النظام

خلافًا للبيانات الرئيسية، تُعد بيانات النظام معلومات مخصصة للنظام ولا ترتبط بالأشخاص ولا بطاقات الهوية ولا الشركات. ويتم شرح هذه التقارير بتفصيل أكثر فيما يلي.

التقرير: المناطق

يُستخدم مربع الحوار هذا لدمج المواقع في تقرير. ويحتوي هذا التقرير على عامل تصفية واحد فقط للمنطقة، ويعرض المباني المختلفة والمناطق الأخرى للتحديد.

ويتم تحديد المنطقة المعنية بالنقر على زر الماوس الأيسر. بإمكان المستخدم عرض التقرير على الشاشة باستخدام الزر **المعاينة** قبل أن يبدأ عملية الطباعة باستخدام **طباعة**.

هناك تخطيطان متوفران.

	القياسي	الأشخاص الموجودون في الموقع - بدون ساحات الانتظار
	شغل ساحة الانتظار	الأشخاص الموجودون في الموقع - ساحات الانتظار فقط

للتحقق من أن مجموعة البيانات المعروضة محدَّثة، يتم ذكر عمليات المسح الضوئي الأخيرة للبطاقات الخاصة بالمناطق أيضًا.

وبالتالي، يمكن إعطاء معلومات موثوقة بشأن مواقع الأفراد لأحداث مختلفة.

التقرير: تكوين المناطق

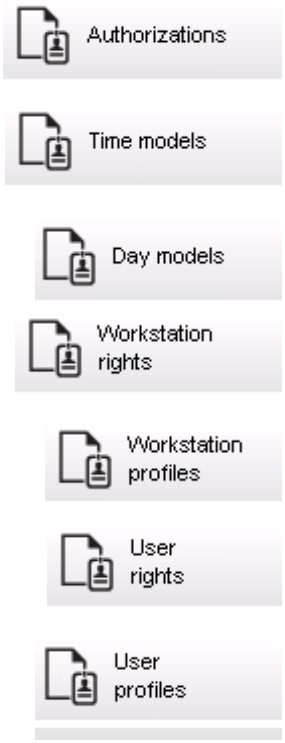
مناطق محددة ومناطق فرعية تابعة لها مع أعلام خاصة بساحات الانتظار وحد أقصى لعدد الأفراد أو السيارات

التقرير: قائمة التجمع في المنطقة
وكما يمكن ذكر الأفراد وفق البيانات الرقمية الواضحة، يمكن أيضًا ذكر الأفراد الموجودين في المنطقة بحسب الاسم.
وبالإضافة إلى أوقات المسح الضوئي للمناطق المنفردة، تحتوي هذه التقارير أيضًا على الأوقات الخاصة بكل شخص بعينه.

التقرير: إجمالي قائمة التجمع
مبدئيًا، ترتبط قوائم التجمع بمربع حوار **المناطق**، ومع ذلك، فهي تقدم قوائم للمناطق المحددة والتي تقدم معلومات حول عدد الأفراد الموجودين حاليًا في المنطقة وفق التحكم في الوصول.

31.3 التقارير: التخويلات

نظرة عامة
في عنصر القائمة هذا، يتم تقديم ملخص حول التخويلات المتنوعة المذكورة في مربعات الحوار ذات الصلة:



التقرير: التخويلات
يمكن استخدام مربع الحوار هذا لعرض تخويلات الوصول المحددة في النظام. كما يتم ذكر المداخل المرتبطة بتخويلات الوصول الفردية. ويتم عرض اسم نموذج الوقت المحدد. علاوة على ما سبق، يعرض هذا التقرير عدد الأفراد الذين تم تعيين تخويلات لهم.

التقرير: نماذج الوقت
يمكن استخدام هذا التقرير لعرض نماذج الوقت المحددة في النظام بحسب التحديد. ويعرض هذا التقرير كل البيانات المقترنة بالنموذج علاوة على عدد الأفراد الذين يتعلق بهم النموذج.

التقرير: نماذج اليوم
يعرض هذا التقرير كل نماذج اليوم المحددة بحسب أسمائها ومواصفاتها والفواصل الزمنية التي تتضمنها.

التقرير: حقوق محطة العمل
يمكن استخدام مربع الحوار هذا لعرض حقوق محطة العمل المخصصة لمحطات العمل المحددة في النظام.

التقرير: ملفات تعريف محطة العمل
يمكن استخدام مربع الحوار هذا لعرض ملفات تعريف محطات العمل المحددة في النظام، وهذا يسمح بتقديم عمليات النظام، الممكنة في محطات العمل المستقلة، في تنسيق واضح.

التقرير: حقوق المستخدم
يمكن استخدام مربع الحوار هذا لعرض ملفات تعريف المستخدم المخصصة للمستخدمين المحددين في النظام.

التقرير: ملفات تعريف المستخدم
يمكن استخدام مربع الحوار هذا لعرض مربعات الحوار المخصصة وحقوق مربعات الحوار لملفات تعريف المستخدم المحددة في النظام.

32 تشغيل إدارة مستوى التهديد

يوضح هذا القسم الطرق المتعددة لتشغيل مستوى تهديد وإلغائه. للحصول على معلومات خلفية، راجع القسم تكوين إدارة مستوى التهديد, الصفحة *128*

المقدمة

يتم تنشيط مستوى التهديد بواسطة تنبيه التهديد. ويمكن تشغيل تنبيهات التهديد بإحدى الطرق التالية:

- من خلال أمر في واجهة مستخدم البرنامج
- من خلال إشارة مدخل يتم تعريفها على وحدة تحكم محلية في الوصول، على سبيل المثال زر يعمل بالضغط.
- من خلال تمرير بطاقة تنبيه في قارئ

لاحظ أنه يمكن إلغاء تنبيهات التهديد بواسطة أمر واجهة المستخدم أو إشارة الجهاز، وليس من خلال بطاقة تنبيه.

راجع

- تكوين إدارة مستوى التهديد, الصفحة *128*

32.1 تشغيل وإلغاء تنبيه تهديد عبر أمر واجهة المستخدم

يوضح هذا القسم كيفية تشغيل تنبيه تهديد في AMS Map View.

مسار مربع الحوار

- AMS Map View > (شجرة الأجهزة)

الشروط الأساسية

- تم تعريف مستوى تهديد واحد على الأقل.
- تم تعليم مستوى تهديد واحد على الأقل بعلامة "نشط" في محرر الجهاز.
- تملك الأذونات الضرورية بصفتك أحد مشغّلي Map View وAMS:
  - لتشغيل مستويات التهديد
  - لعرض وحدة MAC أو وحدات MAC في القسم الذي يراد تشغيل تنبيه التهديد فيه.

الإجراء المُتبع لتشغيل تنبيهات التهديد

1. في شجرة الأجهزة في AMS Map View، انقر بزر الماوس الأيمن فوق جهاز MAC الذي تريد تشغيل تنبيه التهديد فيه.
   - تظهر قائمة سياق تحتوي على الأوامر التي يُخوّل لك بتنفيذها في MAC
   - إذا لم يكن هناك مستوى تهديد قيد التشغيل، فستشمل القائمة عنصرًا واحدًا أو أكثر تحت اسم **تنشيط مستوى التهديد** "<name>"، حيث يكون اسم مستوى التهديد مُعرّفًا في محرر الجهاز.
2. حدد مستوى التهديد الذي تريد تشغيله.
   - وسيعمل مستوى التهديد.

الإجراء المُتبع لإلغاء تنبيهات التهديد

الشرط الأساسي: مستوى التهديد قيد التشغيل بالفعل.

1. في شجرة الأجهزة في AMS Map View، انقر بزر الماوس الأيمن فوق جهاز MAC الذي تريد إلغاء تنبيه التهديد فيه.
   - تظهر قائمة سياق تحتوي على الأوامر التي يُخوّل لك بتنفيذها في MAC
2. حدد **إلغاء تنشيط مستوى التهديد**. من قائمة السياق.
   - يتم إلغاء تنشيط مستوى التهديد الحالي.

32.2 تشغيل تنبيه تهديد عبر إشارة جهاز

يوضح هذا القسم كيفية إرسال إشارة مدخل جهاز لتشغيل تنبيه تهديد.

الشروط الأساسية

- تم تعريف مستوى تهديد واحد على الأقل.
- تم تكوين مدخل واحد على الأقل في شجرة الأجهزة.
- تم تعريف إشارات الجهاز على AMC، وتم توصيل جهاز بالمحطة الطرفية الصحيحة في AMC هذه والتي ستنقل إشارة إليه. إذا لزم الأمر، فانقر فوق الارتباط في نهاية هذا القسم لمعرفة إرشادات حول كيفية تكوين إشارة المدخل أو تواصل مع مسؤول النظام لديك.

الإجراء

قم بتنشيط الجهاز المتصل بـ AMC، عادةً من خلال زر يعمل بالضغط أو مفتاح جهاز.
لإلغاء تنبيه التهديد، قم بتنشيط الجهاز الذي يرسل إشارة المدخل المعرّفة بما يلي: **مستوى التهديد: إلغاء تنشيط**.

راجع

- تعيين مستوى تهديد لإشارة جهاز, الصفحة *132*

32.3 تشغيل تنبيه تهديد عبر بطاقة تنبيه

يوضح هذا القسم كيفية تشغيل تنبيه تهديد عبر بطاقة تنبيه.

الشروط الأساسية

- تم تعريف مستوى تهديد واحد على الأقل.
- تم تكوين مدخل واحد على الأقل في شجرة الأجهزة.
- تم إنشاء بطاقة تنبيه لحامل بطاقات معيّن. إذا لزم الأمر، فانقر فوق الارتباط في نهاية هذا القسم لمعرفة إرشادات حول كيفية إنشاء بطاقة تنبيه أو تواصل مع مسؤول النظام لديك.

الإجراء

1. يضع حامل البطاقة بطاقة التنبيه الخاصة في أي قارئ **بخلاف أجهزة قراءة بصمات الأصابع** في الموقع.
   - يتم تنشيط مستوى التنبيه الذي تم تعريفه أو تلك البطاقة.
2. عند انتهاء التهديد، ألغ مستوى التهديد عبر أمر واجهة المستخدم أو مفتاح الجهاز. من الناحية التصميمية، لا يمكن إلغاء مستوى تهديد عبر بطاقة تنبيه.

راجع

- إنشاء بطاقة تنبيه, الصفحة *194*

33 تشغيل مؤشر التمرير

المقدمة

مؤشر التمرير عبارة عن أداة تساعد مشغّلي Map View على مراقبة مَن يدخل أو يخرج من المقر في الوقت الحقيقي.

نظرة عامة

ومؤشر التمرير تطبيق داخل AMS Map View يعرض آخر 10 دقائق من أحداث الوصول في قائمة تمرير ديناميكية. يتم عرض ما يصل إلى 50 حدث وصول، ويتم إبعاد الأحداث الأقدم من 10 دقائق من القائمة تلقائيًا. يمكن للمشغّل مراقبة جميع أجهزة القراءة في النظام أو تحديد مجموعة فرعية.

يحتوي كل سجل في القائمة على تفاصيل الحدث وبيانات الاعتماد المُستخدَمة، على سبيل المثال:

- اسم حامل البطاقة وصورته المُخزّنة للتأكد المرئي من الهوية.
- الطابع الزمني.
- اسم الشركة و/أو القسم إن كان مُخزّنًا.
- المدخل والقارئ الذي تم استخدام بيانات الاعتماد فيهما.
- فئات الأحداث التي تحمل تسمية ملونة:
  - خضراء: وصول كامل ببيانات اعتماد صالحة
  - صفراء: وصول غير كامل ببيانات اعتماد صالحة، على سبيل المثال بدّل حامل البطاقة القفل ولكنه لم يفتح الباب
  - حمراء: محاولة وصول فاشلة ببيانات اعتماد غير صالحة. يظهر نوع عدم الصلاحية، على سبيل المثال كون بيانات الاعتماد مدرجة بالقائمة المحظورة أو غير معروفة أو منتهية الصلاحية

لا يحتفظ مؤشر التمرير بأرشيفاته الخاصة، بل يستخرج أحداث الوصول ويعرضها من قاعدة بيانات النظام.

يمكن إيقاف التمرير الديناميكي مؤقتًا لدراسته عن قرب أو فتحه في نافذة منفصلة للاستخدام المتوازي مع تطبيقات Map View الأخرى.

إشعار!

زمن الانتقال بعد عمليات التحرير

تحتاج عادةً التغييرات التي يتم إدخالها على صور الهويات وبيانات أخرى خاصة بحامل البطاقة في AMS إلى بضع دقائق كي يتم نشرها إلى مؤشر التمرير. وإلى حين حدوث المزامنة، يستمر شريط التمرير في التفاعل في الوقت الفعلي مع البيانات القديمة.

الشروط الأساسية

ويتطلب ملف تعريف المستخدم تخويلاً خاصًا لتشغيل مؤشر التمرير.

1. في تطبيق AMS الرئيسي، انتقل إلى القائمة: **التكوين** > **ملفات تعريف المستخدم**
2. قم بتحميل اسم ملف التعريف الخاص بالمشغّل المطلوب.
3. في الجدول، حدد **خرائط Access Manager** > **الوظائف الخاصة** > مؤشر التمرير

بدء تشغيل مؤشر التمرير

- في Map View، انقر فوق لبدء تشغيل الأداة.

تحديد أجهزة قراءة للمراقبة

إذا لم يتم تحديد أجهزة قراءة بالفعل، أو إذا كنت تريد تغيير التحديد، فتابع كما يلي:

1. في نافذة مؤشر التمرير، انقر فوق (الإعدادات).
   تفتح نافذة **تصفية الأجهزة**.

2. من شجرة الأجهزة، حدد خانات اختيار المداخل أو أجهزة القراءة التي تريد مراقبتها. تتصرف خانات الاختيار كما يلي:
إذا حددت مدخلاً، فسيتم افتراضيًا تحديد جميع أجهزته التابعة.
ويمكن بعد ذلك مسح خانات اختيار الأجهزة التابعة الفردية إن لم تكن مطلوبة.
إذا تم تحديد **كل** الأجهزة الفرعية لجهاز أصلي، تكون خانة اختيار الأصل بيضاء. إذا تم تحديد **بعض** الأجهزة الفرعية فحسب، تكون خانة اختيار الأصل رمادية.
3. انقر فوق **موافق** لإنهاء تحديد أجهزة القراءة وإغلاق نافذة **تصفية الأجهزة**.

عرض أجهزة القراءة المحددة على الخريطة

- انقر نقرًا مزدوجًا فوق سجل في مؤشر التمرير.
⇦ يتم تلقائيًا إيقاف مؤشر التمرير مؤقتًا.
⇦ يظهر في Map View في النافذة الرئيسية مشهد الخريطة الأول ذي الصلة في التدرج الهرمي لخريطته ويتم تمييز القارئ الذي نقرت نقرًا مزدوجًا فوقه.

إيقاف مؤشر التمرير مؤقتًا

- في نافذة مؤشر التمرير، انقر فوق ، أو انقر نقرًا مزدوجًا فوق سجل في القائمة لإيقاف العرض الديناميكي مؤقتًا.
⇦ يتجمد العرض الديناميكي. يتم تخزين سجلات الأحداث الواردة دون عرضها.
⇦ يتم تشغيل إشعار في أعلى القائمة بأن تدفق الأحداث قم تم إيقافه مؤقتًا.

استئناف مؤشر تمرير تم إيقافه مؤقتًا

- في نافذة مؤشر التمرير، انقر فوق لاستئناف العرض الديناميكي.
⇦ تعرض القائمة الديناميكية بترتيب زمني (الأجدد أولاً) جميع أحداث الوصول التي وقعت عند أجهزة القراءة المحددة في آخر 10 دقائق، بحد أقصى 50.
⇦ تتم إزالة أحداث الوصول الأقدم من أجدد 50 أو أقدم من 10 دقائق من القائمة.
⇦ ويتم من جديد عرض أحداث الوصول الجديدة في الوقت الحقيقي أثناء وقوعها.

تكرار مؤشر التمرير في نافذة منفصلة

لاحظ أنه لا يمكن فتح إلا نافذة مؤشر مكررة واحدة في المرة الواحدة.

1. في نافذة مؤشر التمرير، انقر فوق (نافذة إضافية).
النافذة المنفصلة عبارة عن تكرار **وليست** مستقلة عن المؤشر في النافذة الرئيسية. وتخضع للإعداد نفسه.
يمكن الآن تشغيل تطبيقات Map View الأخرى، مثل قائمة التنبيهات، بالتوازي في النافذة الرئيسية.
2. عند الانتهاء من النافذة المنفصلة، استخدم شريط العنوان لإغلاقها.

33.1 حالات خاصة

مؤشر تمرير Map View وأبواب B901

لتقديم المعلومات الصحيحة إلى تطبيق **مؤشر التمرير** في Map View في AMS، يجب أن تتطابق معرفات أبواب B901 مع معرفات نقاط الأبواب الخاصة بها. وهذا يعني أنه يجب تعيين الباب 1 لنقطة الباب 1، والباب 2 لنقطة الباب 2 وما إلى ذلك.

Doors 1 - 4	Door 1	Door 2	Door 3	Door 4
Door Name Text	Door 1	Door 2	Door 3	Door 4
Door Name Text (Second Language)				
Door Source	SDI2 (B901)	SDI2 (B901)	SDI2 (B901)	SDI2 (B901)
Entry Area	1	1	1	1
Associated Keypad #	Keypad 1	Keypad 1	Keypad 1	Keypad 1
Custom Function	Disabled	Disabled	Disabled	Disabled
Door Point	1	2	3	4
Door Point Debounce	600ms	600ms	600ms	600ms

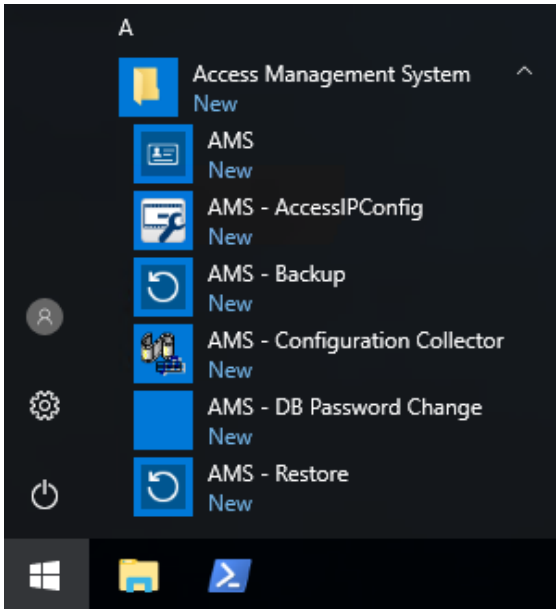
قم بإجراء هذه التعيينات لوحدة التحكم في الباب B901 في أداة RPS التي تقوم بتكوين لوحات الاقتحام ووحدات التحكم.

34 النسخ الاحتياطي والاستعادة

تسمح لك أداة **النسخ الاحتياطي والاستعادة** بنقل نظامك مع بياناته إلى إصدار جديد من AMS أو إلى كمبيوتر جديد.

يمكن تشغيل أداة **النسخ الاحتياطي والاستعادة** فقط على الجهاز حيث تم تثبيت خادم AMS. هناك اختصاران في قائمة البدء في Windows:

- **AMS - نسخ احتياطي** لإنشاء نسخة احتياطية
- **AMS - استعادة** لاستعادة نسخة احتياطية:

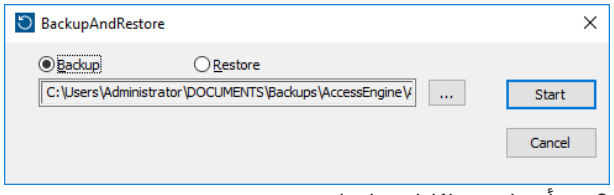


34.1 النسخ الاحتياطي للنظام

يصف هذا القسم كيفية إنشاء نسخة احتياطية لتطبيق AMS وتحديد موقع ملفات نسخة SQL Server الاحتياطية.

إنشاء نسخة احتياطية لتطبيق AMS

1. في قائمة البدء في Windows، انقر بزر الماوس الأيمن فوق **AMS - نسخ احتياطي** وحدد **تشغيل كمسؤول**.
   - يبدأ تشغيل أداة **النسخ الاحتياطي والاستعادة** مع تحديد مسبق لخيار **النسخ الاحتياطي**.



2. أدخل مسارًا لحفظ ملف `.GZ`.
3. انقر فوق **بدء** لبدء تشغيل النسخ الاحتياطي.
   - تنشئ أداة **النسخ الاحتياطي والاستعادة** ملف `.GZ` واحدًا، وتعرض التقدم الذي حققته في نافذة منبثقة.
4. انسخ هذا الملف إلى مساحة تخزين آمنة على كمبيوتر آخر. لحماية البيانات، **لا** تترك النسخة الاحتياطية الوحيدة على خادم DMS.

تحديد موقع ملفات نسخة SQL Server الاحتياطية ونسخها.

1. باستخدام مستكشف ملفات على كمبيوتر خادم AMS، انتقل إلى الموقع حيث يحتفظ SQL Server بملفات `.BAK`.

- مسار الملفات هو على الشكل التالي، حيث <version> و<instance name> عبارة عن متغيرات تعتمد على نظامك:

```
C:
\Program files\Microsoft SQL Server\MSSQL<version>.<instance name>\M
\SSQL\Backup
```

- أسماء الملفات هي على الشكل التالي:

```
acedb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
Bosch.AlarmDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
Bosch.EventDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
Bosch.MapDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
Bosch.MapViewDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
Bosch.StatesDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
```

2. انسخ **جميع** ملفات .BAK إلى مساحة تخزين آمنة على كمبيوتر آخر. لحماية البيانات، **لا** تترك النسخ الوحيدة على خادم DMS.

إشعار!
المسار الافتراضي إلى سجل أحداث AMS هو:
\C:\Program Files (x86)\Access Management System\Access Engine\AC\LgfLog

34.2 استعادة نسخة احتياطية

الشروط الأساسية

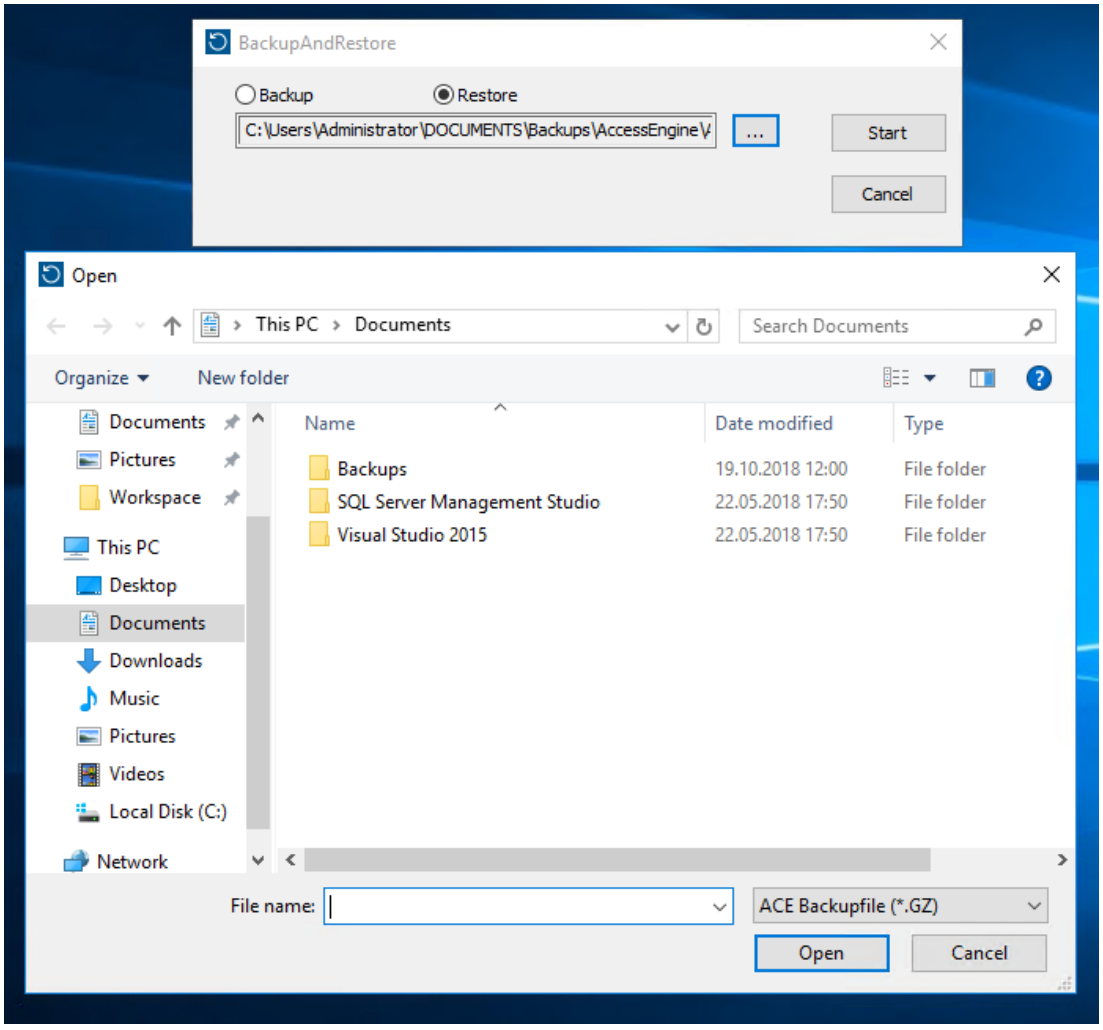
- ملف GZ الذي تم إنشاؤه بواسطة أداة **النسخ الاحتياطي والاستعادة**
- ملفات .BAK التي أنشأها SQL Server والتي حفظتها أثناء إجراء النسخ الاحتياطي.
- حساب SQL مع حقوق **sysadmin** ، مثل sa.
- كمبيوتر هدف تم إعداده بشكل ملائم بالنسبة إلى **التراخيص** و**الشهادات**:
- **التراخيص**: يحتاج الكمبيوتر الهدف (الكمبيوتر الذي تستعيد إليه النسخة الاحتياطية) إلى تراخيص تكون معادلة على الأقل لتراخيص الكمبيوتر حيث تم إجراء النسخ الاحتياطي.
- **الشهادات**: سيحتاج أي عميل من عملاء الكمبيوتر الهدف إلى الشهادات الجديدة التي أنشأتها عملية التثبيت على الكمبيوتر الهدف، وليس إلى تلك التي أنشأتها عملية التثبيت على الكمبيوتر الأصلي.
راجع **دليل تثبيت AMS** للاطلاع على إنشاء شهادات العميل وتثبيتها.

الإجراء

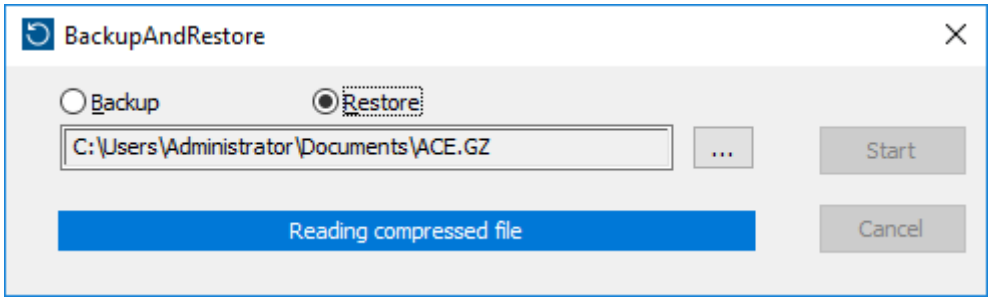
1. في برنامج AMS، انقر فوق **ملف** > **خروج** لإيقاف تطبيق AMS.
2. عند إنهاء البرنامج، قم بتشغيل تطبيق **خدمات** Windows وتأكد من توقف جميع خدمات Access Engine وAccess Management System. أو، أوقفها هنا.
3. **إذا وفقط إذا كنت** تقوم بتشغيل RMAC (MAC متكرر لتجاوز الفشل) مع MAC .1 أو الرئيسي، فانتقل إلى الفصل الفرعي التالي ونفّذ الإجراء الذي ورد وصفه هناك، قبل العودة إلى هذه الخطوة.
4. انسخ ملفات .BAK MSSQL التي حفظتها من الكمبيوتر الأصلي إلى المسار نفسه تمامًا على الكمبيوتر الجديد.
- مسار الملفات هو على الشكل التالي، حيث <version> و<instance name> عبارة عن متغيرات تعتمد على نظامك:

```
C:
\Program files\Microsoft SQL Server\MSSQL<version>.<instance name>\M
\SSQL\Backup
```

5. في قائمة البدء في Windows، انقر بزر الماوس الأيمن فوق **AMS - استعادة** وحدد **تشغيل كمسؤول**.
   - يبدأ تشغيل أداة **النسخ الاحتياطي والاستعادة** مع تحديد مسبق لخيار **الاستعادة**.
6. انقر فوق الزر **[...]** لتحديد موقع ملف النسخ الاحتياطي GZ في نظام الملفات، وانقر فوق **فتح** لتحديده.



7. انقر فوق **بدء** لبدء عملية الاستعادة.
8. عند مطالبتك بإدخال بيانات اعتماد الخادم، أدخل بيانات اعتماد مستخدم MSSQL sysadmin مثل sa، وليس بيانات اعتماد كمبيوتر الخادم.
   - تبدأ عملية الاستعادة



9. عند اكتمال عملية الاستعادة، قم بتشغيل **خدمات**Windows وأعد تشغيل جميع خدمات Access Engine وAccess Management System يدويًا.
10. نفّذ برنامج إعداد الخادم AMS Server Setup.exe كمسؤول لإعادة مزامنة البيانات التي تم إنشاء نسخة احتياطية لها مع بيانات النظام الحالية.

راجع

– النسخ الاحتياطي للنظام, الصفحة *242*

34.2.1 استعادة وحدات RMAC إلى تثبيت جديد

ملاحظة: يتعلق هذا الإجراء فقط بالحالة حيث تعمل على استعادة النسخة الاحتياطية لنظام يتضمن وحدات MAC وRMAC إلى أجهزة أخرى.

المقدمة

إذا قمت باستعادة النسخة الاحتياطية إلى أجهزة كمبيوتر جديدة، فعليك عندئذٍ إعادة تكوين عناوين IP لوحدة MAC ووحدة RMAC التي تم تخزينها في ملف النسخ الاحتياطي إلى عناوين IP للأجهزة الجديدة.
يمكنك تنفيذ هذا التكوين عن طريق تشغيل الأداة MACInstaller على الأجهزة الجديدة.
يمكن العثور على الأداة MACInstaller على وسائط التثبيت على
`AddOns\MultiMAC\MACInstaller.exe\`
يمكن العثور على وصف مفصل للأداة MACInstaller في الفصل استخدام أداة تثبيت *MAC*, الصفحة *50*

الإجراء

1. شغّل الأداة MACInstaller على الكمبيوتر حيث يتم تشغيل MAC.1. قد يكون هذا الكمبيوتر خادم DMS أو خادم مخصص لوحدة MAC.1.
   – في الأداة، عيّن عناوين IP الجديدة لوحدة MAC الرئيسية (هذا الكمبيوتر) وRMAC.
2. شغّل الأداة MACInstaller على الكمبيوتر حيث يتم تشغيل RMAC.
   – في الأداة، عيّن عناوين IP الجديدة لوحدة MAC الرئيسية وRMAC (هذا الكمبيوتر).
3. عد إلى الخطوة حيث تركت الإجراء **إجراء الاستعادة**.

راجع

– استخدام أداة تثبيت *MAC*, الصفحة *50*

35 تكوين بطاقات CEPAS واستخدامها

يُستخدم نوع بطاقة CEPAS في سنغافورة. حجم أرقام البطاقات أكبر من الحجم العادي؛ وبالتالي، تم تقديم نوع خاص من بطاقات CEPAS في برنامج الوصول.
يوضح الوصف التالي كيفية تكوين نوع بطاقة CEPAS، بما في ذلك تسجيل نوع البطاقة هذا في مربع حوار يدوي و/أو بواسطة جهاز قارئ USB خاص.
لتكوين بطاقة CEPAS في نظام التحكم في الوصول (AMS):

مسار مربع الحوار

– في القائمة الرئيسية **تكوين**، انقر فوق **تعريف البطاقة.**

لتنشيط بطاقة CEPAS، انتقل `CEPAS 64 Bit` من قائمة **أنواع البطاقات المتوفرة** في الجانب الأيمن إلى قائمة **أنواع البطاقات النشطة** في الجانب الأيسر بالنقر على زر السهم الأيسر **[<].**

ملاحظة: إذا تم تنشيط أي نوع آخر من أنواع بيانات البطاقة، فلا يمكن أيضًا تنشيط نوع البطاقة CEPAS 64 Bit. وبطريقة مماثلة، أنه إذا تم تنشيط نوع البطاقة CEPAS 64 Bit، فلن يكون من الممكن بعد ذلك تنشيط نوع بيانات بطاقة مختلف.

بعد التكوين والتسجيل، يظهر رقم البطاقة الأطول كاملاً في مربعات حوار الوصول وفي تقارير تطبيق مدير الحوار.

يُظهر الوصف التالي أهم التغييرات في مربعات الحوار إذا تم تكوين CEPAS:

– انتقل إلى القائمة الرئيسية AMS > **بيانات الموظفين** > **الأشخاص**

1. أنشئ شخصًا أو قم بتعديل شخص موجود. لمزيد من المعلومات، اقرأ إنشاء بيانات الموظفين وإدارتها.
2. احفظ

– في القائمة، انقر فوق **البطاقات**

3. انقر في المساحة الفارغة **رقم البطاقة**.
4. حدد قارئ مربع الحوار لتسجيل البطاقة
5. انقر فوق **تسجيل البطاقة**

– سيفتح مربع حوار `Recording badge ID`. يوصى بشدة باستخدام قارئ USB لإدخال رقم البطاقة. بخلاف ذلك، يمكن إدخال أرقام بطاقة CEPAS التي يبلغ عددها 16 رقمًا يدويًا.

6. انقر فوق **رقم البطاقة**
7. قدم بطاقة CEPAS على قارئ NFC USB الذي سيقرأ رقم البطاقة

– يجب أن يكون رقم البطاقة هو نفسه الرقم الموجود على بطاقة الشخص.

8. انقر فوق للبحث عن البطاقة
9. حدد القارئ
10. أثناء النقر فوق **القارئ...**، قدم البطاقة على قارئ NFC USB

– سيتم العثور على البطاقة المنشّطة وعرضها بشكل صحيح.

كي يتم منحك حق الوصول باستخدام البطاقة المنشّطة، يجب مراعاة ما يلي:

مسار مربع الحوار

– القائمة الرئيسية AMS > **القائمة الرئيسية AMS** > **بيانات الجهاز**

1. حدد AMC-4W. لمزيد من المعلومات، راجع استخدام محرر الجهاز.
2. حدد نموذج الباب. لمزيد من المعلومات، راجع تكوين المداخل.
3. احفظ

– القائمة الرئيسية AMS > **بيانات النظام** > **التخويلات**

4. أنشئ تخويلاً جديدًا، وقم بتعيينه إلى المدخل الذي تم إنشاؤه في وقت سابق.
5. احفظ

– القائمة الرئيسية AMS > **بيانات الموظفين** > **البطاقات**

6. حدد الشخص، وعيّن إليه التخويل الذي تم إنشاؤه في وقت سابق.

7. احفظ

قيود بطاقات CEPAS في AMS:

- إذا تم تنشيط بطاقات CEPAS في مربع حوار تعريف البطاقة، فلا يمكن استخدام أنواع بطاقات أخرى بالإضافة إلي هذا النوع.
- لا تدعم الأنظمة الخارجية مثل IDEMIA وSuprema وIntrusion boards وSimonsVoss ومصاعد KONE وخزائن Deister وPegaSys وOSS-SO نوع بطاقة CEPAS ولا يمكن دمجها في نظام AMS واحد.

المصطلحات

MAC.1 (أول MAC)

وحدة التحكم في الوصول الرئيسية (MAC) في BIS Access Engine (ACE) أو نظام إدارة الوصول (AMS). بإمكانها أن تقيم في الكمبيوتر نفسه مثل DMS، ولكن يمكنها أ، تقيم أيضًا كوحدة تحكم في الوصول رئيسية (MAC) إضافية، على كمبيوتر منفصل كخادم MAC.

ACS

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

CSN

رقم اختيار البطاقة.

DCP

كلمة مرور ينشئ منها نظام التحكم في الوصول مفتاحًا رئيسيًا يُستخدم لتشفير اتصال الشبكة إلى جميع وحدات التحكم في الوصول المحلية التابعة، عادةً أجهزة AMC.

DSN

اسم مصدر البيانات. اسم مصدر بيانات في اتصال قاعدة البيانات المفتوح (ODBC).

DTLS

إن بروتوكول أمان طبقة نقل مخطط البيانات (Datagram Transport Layer Security) عبارة عن بروتوكول الاتصالات الآمنة الذي يحمي من التنصت والتلاعب.

IDS

نظام اكتشاف الاقتحام، المعروف أيضًا بنظام الإنذار ضد السرقة.

IPConfig tool

برنامج مساعد منفصل لتكوين الشبكة وإعدادات أمان الشبكة للأجهزة داخل نظام التحكم في الوصول.

MAC (وحدة التحكم في الوصول الرئيسية)

في أنظمة التحكم في الوصول، برنامج خادم يعمل على التنسيق بين وحدات التحكم في الوصول المحلية والتحكم فيها، عادةً وحدات التحكم النمطية في الوصول (AMC).

REX

"طلب الخروج". إشارة لطلب فتح باب هذا الباب من الداخل للسماح بالخروج. عادةً ما يتم تشغيل الإشارة بواسطة زر ضغط أو شريط داخل المدخل؛ وفي بعض الأحيان بواسطة كاشف حركة.

RMAC

وحدة تحكم في الوصول رئيسية (MAC) مكررة، وهي عبارة عن توأم متزامن لوحدة التحكم في الوصول الرئيسية الموجودة، وتأخذ على عاتقها إدارة بياناتها في حال فشل وحدة التحكم في الوصول الرئيسية الأولى أو في حال انقطاع اتصالها.

RPS

برنامج البرمجة عن بُعد. برنامج يدير لوحات تحكم الكشف عن الحريق أو التسلل على الشبكة.

SmartIntego

نظام إقفال رقمي من Simons Voss technologies. يتكامل SmartIntego مع بعض أنظمة التحكم في الوصول من Bosch.

التعرّف التلقائي على لوحة الرقم (ANPR)

استخدام تقنية الفيديو لقراءة لوحات الأرقام ومعالجتها، عادةً للعربات على الطرقات.

القائمة البيضاء (SmartIntego)

القائمة البيضاء عبارة عن قائمة بأرقام البطاقات يتم تخزينها محليًا على أجهزة قراء البطاقات لنظام قفل SmartIntego. إذا لم يكن MAC القارئ متصلاً بالإنترنت، فإن القارئ يمنح حق الوصول فقط إلى البطاقات التي تم إدراج أرقامها في قائمته البيضاء المحلية.

المدخل

يُشير مصطلح المدخل في مجمله إلى آلية التحكم في الوصول عند نقطة دخول: يشتمل على أجهزة القراءة، شكل من أشكال الحاجز القابل للقفل وإجراء وصول كما هو محدد بواسطة تسلسلات الإشارات الإلكترونية التي تمر بين عناصر الأجهزة.

المفتاح الرئيسي

رمز يقوم النظام بإنشائه من كلمة مرور اتصال الأجهزة (DCP)، ويستخدمه لحماية أجهزة التحكم في الوصول. لا يتم عرض المفتاح الرئيسي لأي مستخدم على الإطلاق.

المنطقة (تفعيل)

مجموعة من المداخل لنموذج مدخل 14 في نظام التحكم في الوصول. يكون تأثير تفعيل نظام كشف التسلل أو إلغاء تفعيله في أحد هذه المداخل في الوقت نفسه هو نفسه التأثير في جميع المداخل حيث معلمة منطقة "التفعيل" لها التعيين نفسه من حرف واحد.

النقطة

مستشعر للكشف عن تسلل في منطقة خاضعة لمراقبة التسلل. تسمى النقاط في سياقات معينة مناطق أو أجهزة استشعار.

الوضع العادي

بطريقة مغايرة لوضع المكتب، يمنح الوضع العادي حق الوصول فقط إلى الأشخاص الذين يقدمون بيانات اعتماد صالحة للقارئ.

إنتروبيا كلمة المرور

قياس قوة كلمة المرور يتم حسابه من عوامل مثل عشوائيتها وعدد الرموز المتاحة والعدد الفعلي للرموز المستخدمة.

تتبع آخر بدنوّ خطر

التحايل على التحكم في الوصول عن طريق قيام شخص ما بمتابعة حامل بطاقة مصرّح له عن قرب عبر مدخل دون تقديم بيانات الاعتماد الخاصة به.

تنبيه التهديد

تنبيه يعمل على تشغيل مستوى تهديد. يمكن للأشخاص المخوّلين الملائمين تشغيل تنبيه تهديد بإجراء سريع، على سبيل المثال من خلال واجهة المستخدم الخاصة بالمشغّل، أو من خلال إشارة جهاز (زر يعمل بالضغط مثلاً)، أو من خلال توفير أي بطاقة تنبيه خاصة في أي قارئ.

جهاز إعادة توجيه إدخال الوجهة (DER)

عبارة عن كمبيوتر على المستوى نفسه لخادم إدخال الوجهة (DES) في نظام Otis CompassPlus. وهو يتصل بجميع مجموعات المصاعد ووظيفته هي تعزيز كفاءة أجهزة DES.

خادم MAC

الجهاز: كمبيوتر (غير خادم DMS) في Access Engine (ACE) أو نظام إدارة البيانات (AMS)، حيث يتم تشغيل MAC أو RMAC.

خادم إدخال الوجهة (DES)

كمبيوتر يدير مجموعة مصاعد لتحسين أوقات السفر.

رقم PIN المخصص للتحقق

يُستخدم رقم التعريف الشخصي (PIN) بالإضافة إلى بيانات الاعتماد المادية لفرض مزيد من الأمن.

رقم التعريف الشخصي

يُعد رقم التعريف الشخصي (PIN) بيانات الاعتماد الوحيدة المطلوبة للوصول.

قم بالتحويل

لتعليق الإنذار في ظروف محددة بشكل خاص.

مجموعة المصاعد

مجموعة مصاعد تخدّم نفس الطوابق معًا. تخضع كل مجموعة مصاعد لإدارة خادم إدخال الوجهة (DES).

محطة طرفية لإدخال الوجهة (DET)

جهاز حيث يمكن لركاب المصعد إدخال طلبات الوجهة لمجموعة مصاعد.

مراقبة تسلسل الوصول

تعقب شخص أو عربة من منطقة محددة إلى أخرى عن طريق تسجيل كل مسح ضوئي لبطاقة الهوية، ومنح الوصول فقط من المناطق التي تم فيها مسح البطاقة ضوئيًا.

مفتاح LCD عشوائي

رمز أبجدي رقمي مؤقت تقوم وحدة AMC بإنشائه من جديد في كل مرة تقوم فيها بالتمهيد. يمكن عرض المفتاح في شاشة العرض البلورية السائلة (LCD) لوحدة AMC وقد تطلبه الأدوات البرمجية لمصادقة اتصالات الشبكة.

مفتاح أجهزة AMC

رمز مصادقة داخلي تقوم وحدة AMC بإنشائه من معلمات أجهزة معينة. وهو غير مرئي للمستخدم.

منع العودة

شكل بسيط من مراقبة تسلسل الوصول يتم فيه منع حامل البطاقة من دخول منطقة ما مرتين خلال فترة زمنية محددة، ما لم يتم مسح البطاقة ضوئيًا للخروج من تلك المنطقة خلال تلك الفترة. تقوم وظيفة منع العودة بمنع شخص من تمرير بيانات الاعتماد للعودة عبر مدخل لاستخدامها من قِبل شخص آخر غير مصرّح له.

نظام إدارة البيانات (DMS)

عملية على مستوى عالٍ لإدارة بيانات التحكم في الوصول في النظام. يقوم نظام إدارة البيانات (DMS) بتوفير البيانات لوحدات التحكم في الوصول (MAC) الرئيسية، التي تقوم بدورها بتوفير البيانات لوحدات التحكم في الوصول (AMC عادةً) المحلية.

نظام إرسال الوجهات (DDS)

يُعرف أيضًا باسم نظام إدارة الوجهات، ولكنه يستخدم الاختصار DDS فقط. نظام Otis CompassPlus هو نوع من DDS.

نقطة التجمع

مكان محدد يُطلب من الناس الانتظار فيه بعد إخلاء المبنى.

نموذج الباب

قالب برمجي مخزّن لنوع مدخل معين. تُسهّل نماذج الأبواب تعريف المداخل في أنظمة التحكم في الوصول.

وحدة التحكم في الوصول المحلية (LAC)

جهاز يُرسل أوامر الوصول إلى أجهزة التحكم في الوصول الطرفية، مثل أجهزة القراءة والأقفال، ويعالج الطلبات القادمة من تلك الأجهزة لنظام التحكم في الوصول الشامل. وحدة التحكم في الوصول المحلية (LAC) الأكثر شيوعًا هي وحدة التحكم النمطية في الوصول أو AMC.

وضع التشغيل

حالة جهاز تحكم في الوصول في محرر الجهاز أثناء استجابته للأوامر الصادرة من خارج محرر الجهاز. تدخل تغييرات التكوين حيّز التنفيذ بعد انتهاء وضع التشغيل واستعادة وضع التكوين.

وضع التكوين

الحالة الافتراضية لأجهزة التحكم في الوصول في محرر الجهاز. تدخل التغييرات حيّز التنفيذ وتنتشر في الأجهزة التابعة على الفور.

وضع المكتب

تعليق التحكم في الوصول في مدخل ما خلال ساعات العمل أو المكتب.

Bosch Security Systems B.V.
Torenallee 49
BA Eindhoven 5617
Netherlands
www.boschsecurity.com
Bosch Security Systems B.V., 2024 ©

Building solutions for a better life

202405241055